Fault-Tolerant Model Predictive Control for a $Z(T_N)$-Observable Linear Switching Systems

Abir SMATI, Wassila CHAGRA and Moufida KSSOURI
University of Tunis El-Manar, Science Faculty of Tunis
Laboratory of Analysis and Control Systems, 1060 Tunis, Tunisia

Abstract—**This work considers the control and the state observation of a linear switched systems with actuators faults. A particular problem is studied: the occurrence of non-observable subsystem in the switching sequence. Hence, the accuracy of the state estimations will decrease affecting the observer-based fault detection algorithms. In this paper, we propose a solution based on a constrained switching control in a predictive scheme. An extension to fault-tolerant control is derived, using several hybrid observers for estimation and fault detection and a reconfigurable finite control set model-predictive controller. The paper includes experimental results applied to a multicellular converter to demonstrate the efficiency of the method.**

Keywords—*Switching systems; $Z(T_N)$-Observability; finite control set predictive control; fault tolerant control; multicellular converter*

I. INTRODUCTION

Hybrid dynamic systems (HDS) represent a particular type of supersystems that contain both continuous and discrete subsystems. A linear switching system (LSS) is a class of HDS in which the interaction between its linear subsystems follows a discrete switching law [1]. The first proposed classical approaches are based on pulse width modulation (PWM) as an open loop control. Its drawback is the presence of several oscillations around the set points. Others approaches can be found in the litterature with additional purposes like in [2], the author proposes a binary Lyapunov-based control with a commutation limiting constraint to extend switching components durability. Also, finite control set predictive control (FCS-PC) are presented in [3].

Continuous and descrete state estimation need the LSS observability, which led the researchers to find solutions to different problems caused by its switching behavior. Some of those problems suppose that the continuous and discrete states are unknoun and were treated using a sliding mode observer [4]. The other problems consider only the estimation of discrete states where some of the proposed solutions use either a sliding mode input reconstruction [5] or Petri networks [6]. These approaches use output measurements and the estimated continuous state to determine the operating discrete state of the LSS. In a different context, Luenberger-based observer structures for HDS are researched in [7]. All these works assume that all LSS subsystems are observable. In the general case, this is not always true. Some LSS contain unobservable subsystems. Consequently, an extension of the observability property for HDS called $Z(T_N)$-observability is investigated in [8] to allow observer design with partial observability of the targeted LSS.

A particular domain of interest in the HDS control research topic is the fault tolerant control (FTC). Faults are symptoms of noncritical abnormal behaviors of the system. However, if a fault persists it may lead to a failure (critical anomaly) that may destroy the system. The dynamic of HDS may involve high commutation frequencies, reducing switching component lifespan and causing occasional malfunctions. The switch is stuck open or stuck closed, reducing the ability to control the HDS. Solutions are needed to minimize faults impact, to prevent failures and to ensure acceptable performance level of the faulty HDS.

Two major approaches investigate FTC for HDS, passive and active. Passive schemes are based on robust control schemes with limited need to observers, but active schemes involve some kind of fault detection isolation and estimation (FDIE) algorithm to ensure appropriate fault compensation by the FTC module. The isolation and estimation parts require the observability of the HDS. Partial observability or unobservability of some HDS subsystem will hinder the ability of FTC design using classical controller design approaches. In some cases, only fault detection (FD) or fault isolation (FDI) are possible. $Z(T_N)$-observability comes handy in this case, allowing performant active FTC designs if favourable control sequences are ensured.

Getting back to the FDIE step, a popular solution is to design a bank of residual generators. Residual generators are particular observers designed to react only to a specified subset of faults and ignoring the remaining ones. Fault detection is ensured if the residual signals react and converge to a pattern called fault signature, and fault isolation is possible if multiple distinct patterns exist, with a one-to-one ratio with the faults to detect. Fault estimation is achieved if some laws exist linking residual amplitudes with fault severity. Observer based FDIE are model-based, requiring knowledge of the targeted system. One should note that some authors address the FDIE problem in a more general fault detection and diagnosis (FDD) context. Rigorously speaking, diagnosis is performed after system failures and involve artificial intelligence approaches to reconstruct failure causes, while FDIE and FTC are running in real-time and should (hopefully) avoid failures with appropriate actions.

The HDS FTC is complex, since different model types are involved. HDS FTC designs are usually hybrid also. In [9], an observation technique with a higher order sliding mode is used to estimate the residual vector. Additionally, the system is modeled as a discrete automaton and a diagnoser (event-based fault reconstructor [10]) is designed to detect continuous faults.

It can be said, considering the previous works on the

topic that an observability ensuring constraint of the switching sequence can lead to a guaranteed performance of the FTC for HDS. Finite control set predictive control (FCS-PC) is a suitable framework to deal with multiple constraints on the control and will be the basis of the proposed contribution.

In this paper, a predictive active FTC scheme for LSS is used to limit the impact of faults and to maintain an acceptable accuracy of the supporting FDI module. Several predictive control algorithms associated with each expected fault are designed. The suitable controller is selected upon the evaluation of the residual vector obtained from the residual generators bank designed according to [11]. The strategy adopted in this article is multilayered and covers several areas: FDI, observation and control of LSS. The main motivation is to propose an FTC solution for partially observable LSS. In the predictive scheme, a constraint is maintained in the algorithm to ensure $Z(T_N)$-observability and to increase the FDIE convergence rate.

The rest of the paper is organized as: Section 2 presents the proposed FTC strategy. Section 3 presents the Finite control set predictive control algorithm. Section 4 discusses the observability aspect and contains a background for $Z(T_N)$-observability. Section 5 presents FDI procedure. Section 6 includes the experimental results and validates the proposed strategy. Finally, conclusions are given in Section 7.

II. FAULT TOLERANT CONTROL SCHEME

Consider a linear continuous switched system described by:

$$\begin{cases} \dot{x}(t) = A(u(t))x(t) + B(u(t)) \\ y(t) = Cx(t) \end{cases} \quad (1)$$

Where, $x(t) = [x_1(t), x_2(t), ..., x_n(t)]$ the state vector, $y(t) \in \mathbf{R}^l$ is the measured output vector, $u(t) = [u_1(t), u_2(t), ..., u_m(t)]$ with $u_i = \{0, 1\}$ is a discrete input. C is $1 \times$ n matrix and $A(u), B(u)$ are respectively n$\times$ n, n$\times$ 1 matrices that change for every new set of the vector $u(t)$.

From (1) and (2) it is possible to deduce another state representation of the switched system described by the following subsystem:

$$\begin{cases} \dot{x}(t) = A_s x(t) + B_s \\ y(t) = Cx(t) \end{cases} \quad (2)$$

Where, $s = \{0, 1, ..., N - 1 = 2^m - 1\}$ is a discrete state or a configuration mode corresponding to a set of $u(t)$ and A_s, B_s are respectively n$\times$ n, n$\times$ 1 constant matrices.

In general, the failures that may happen when dealing with the switched systems are of two types. Failures with effects on the continuous states of the system and failures that affect the hybrid behavior or the discrete states which are treated in this work.

When a fault occurs on a discrete input, a change may appear in the transition to a configuration mode that should not be used by the system under normal circumstances. Also, some of the subsystems may be unobservable and the fault may alter the switching sequences that make the continuous states

observable and consequently, the state estimation becomes inaccurate.

In this paper, we focus on failures affecting the discrete states of a switching system. The procedure followed here is to detect the failure in a first step, then to use an input sequence enabling its isolation in a second step and finally to reconfigure the controller to take into account the changes in the system behavior. The isolation sequence is needed because the failure may affect the controller that may choose some sequences making the system non observable. Therefore, after fault detection, a different control sequence must be used to satisfy the $Z(T_N)$-observability until the fault is isolated.

The fault tolerant control strategy adopted here is based on two major blocs as presented in Fig. 1 the controller bloc and the fault detection bloc.
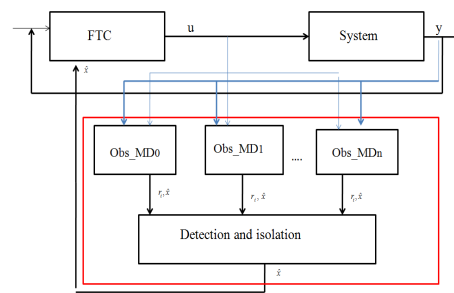

Fig. 1. Fault tolerant control scheme.

The controller bloc is based on several predictive algorithms where each one is related to a predetermined fault model of the process. Whereas, the fault detection bloc is constituted of several hybrid observers Obs_MD_i where $i = 0, 1, ..., m$ is the ith actuator fault, with a detection and isolation bloc. Each observer is associated with a faulty model of the process (Obs_MD_0 is associated to the healthy system), and generates two outputs: the estimated state vector $\hat{x}$ and a residual estimate r_i. The fault detection and isolation procedure is used to detect and identify the fault based on the estimated residual given by all the observers and delivers to the controller bloc the estimated states and the fault if any. The latter reconfigures the control algorithm after receiving the information about the nature of the fault, otherwise the bloc uses the healthy system control algorithm. In order to obtain good results with the proposed FTC scheme, the process must present some redundancies that enable the controller to find solutions to compensate the fault. Further informations about each bloc of the FTC strategy are given in the following sections.

III. FINITE CONTROL SET PREDICTIVE CONTROL FOR SWITCHED SYSTEMS

Generally, the predictive control algorithm is based on a discrete model. In the case of hybrid systems it is possible to use several discrete models where each one corresponds to a different configuration mode of the system. Suppose that the system states are accessible, the discrete sub-models can be obtained from the next approximation for one step horizon:

$$\dot{x}(t) \simeq \frac{\hat{X}(k + 1, s^{k+1}) - X(k)}{T_e} \quad (3)$$

Where, $\hat{X}(k+1, s^{k+1})$ denotes the predicted state over an horizon $H_p = 1$ for a future active mode s^{k+1} and T_e is the sampling time.

After replacing the subsystem (2) into (3) and having $x(t) = X(k)$ when $t = kT_e$, one can obtain the following approximated discrete subsystems:

$$\hat{X}(k+1, s^{k+1}) \simeq (I + T_e A_{s^{k+1}})X(k) + T_e B_{s^{k+1}} \quad (4)$$

Where, $I \in \mathbb{R}^{n \times n}$ is the identity matrix. Note that for N subsystems, one has N future possibilities. When $H_p = 2$, there will be others N future possibilities for every mode in the previous horizon ($H_p = 1$). So, in total there will be N^2 future possibilities to be selected by the controller leading to N^2 discrete models to be computed. If one expand even more the prediction horizon, it will lead to N^{H_p} discrete models to be computed. That will increase the complexity of the algorithm without having a major improvement [3]. In the following, H_p will be equal to 1 to avoid complexity in the control algorithm.

If the LSS system is controllable, then a cost function for every subsystem is needed to ensure a minimal difference between the outputs and its references. Its expression has the following form:

$$F_{s^{k+1}} = (\hat{X}(k+1, s^{k+1}) - X_{ref}) Q (\hat{X}(k+1, s^{k+1}) - X_{ref})^T \quad (5)$$

Where, X_{ref} is a vector containing the reference output and $Q \in \mathbb{R}^{n \times n}$ is a weighting matrix. The results are N cost functions for every future mode $s = 0, 1, ..., N - 1$. The configuration associated to the minimal cost function will be selected by the controller and will be applied on the process each sample time following the next steps:

- Get $X(k)$

- Compute $F_{s^{k+1}}$ for all $s = 0 \dots N$
- Apply $s_{opt} = argmin[F_{s^{k+1}} : s = 0 \dots N]$ to the process.

Stability analysis and proof can be found in [12] and experimental control results with measured continuous state are presented in [13] to attest the efficacy of the predictive algorithm. As reported previously, this paper considers the case where the continuous states are estimated and the LSS is subject to actuator fault. Therefore, feedback control with measured states is not the objective here.

IV. OBSERVER DESIGN FOR HYBRID SYSTEMS

Matrices $A(u)$ and $B(u)$ in (1) can be expressed as follows:

$$A = \overline{A}_0 + \overline{A}_1 u_1 + \dots + \overline{A}_j u_j \quad (6)$$
$$B = \overline{B}_1 u_1 + \dots + \overline{B}_j u_j \quad (7)$$

Where, $\overline{A}_{j=1,\dots,m}$ are n× n constant matrices and $\overline{B}_{j=1,\dots,m}$ are n× 1 constant matrices.

Then, the switched system (1) can be rewritten as follows [14]:

$$\dot{x}(t) = \overline{A}_0 x(t) + \sum_{j=1}^{m} u_j(t)(\overline{A}_j x(t) + \overline{B}_j) \quad (8)$$

Let consider that for some values of the vector $u(t)$, the state vector is not fully observable, meaning that some of its elements are not observable. Moreover, some elements are observable for another combination of $u(t)$.

The system is then said to be $Z(T_N)$-observable, and verifies the following conditions [15]:

(1) Each element of the state vector is observable within at least one time interval.

(2) The components of the state vector that are not observable in a time interval where another one is observable must remain constant during that time.

(3) A time trajectory T_N including time intervals verifying conditions **1** and **2** is used in a way that all the components of the state vector are observable within it.

Remark 4.1: In the case of system (8) the first condition is met if each element of the vector state $x(t)$ is observable for at least one value of $u(t)$. Then the second condition is verified if for the same input $u(t)$ the elements that are unobservable are constant. Finally, the third condition is verified if the sequence of inputs used to control the system contains all the combinations that meet the two previous conditions for all the elements of $x(t)$. The system (8) is said to be Z(T_N) observable.

The observers used in our predictive strategy are based on a hybrid observer proposed in [16]:

$$\dot{\hat{x}}(t) = \overline{A}_0 \hat{x}(t) + \sum_{j=1}^{m} (u_j(t)(\overline{A}_j \hat{x}(t) + \overline{B}_j + K_j(y - \hat{y})) \quad (9)$$

Where, K_j are the correction matrix gains.

From the above equations the dynamics of the error $e = x(t) - \hat{x}(t)$ are:

$$\dot{e}(t) = \tilde{A}_0 e + \sum_{j=1}^{m} u_i \tilde{A}_j e \quad (10)$$

With $\tilde{A}_j = \overline{A}_j - K_j C$ for all $j = 0, 1 \dots m$.

The Lyapunov function is given by: $V(x(t)) = e(t)^T H e(t)$ where H is a positive-definite matrix i.e $(H > 0, H^T = H)$.

The dynamic of the Lyapunov function is given by:

$$\dot{V} = e^T ((\tilde{A}_0^T H + H \tilde{A}_0) + \sum_{i=1}^{m} u_i (\tilde{A}_i^T H + H \tilde{A}_i)) e \quad (11)$$

It can be seen from equation (11), that if we manage to find H and K_j that verifies $\dot{V} < 0$, we can achieve error convergence of the observer.

Remark 4.2: It can be noted that the decreasing rate of the estimation error depends not only on the parameter of the observer but also on the chosen configuration sequences, because of the $Z(T_N)$-observability of the system. Indeed, the difference $x_j - \hat{x}_j$ decreases rapidly if the combinations of $u(t)$ for which x_j is observable are used more often. Otherwise, the difference decreases more slowly. When using estimated values as feedback in a closed loop predictive control strategy,

if the $Z(T_N)$-observability is not taken into account through a convenient sequence of control, then estimation and control results will be affected negatively. A modification to the control algorithm is needed to use adequate control sequence in order to improve the state estimation.

V. FAULT DETECTION AND ISOLATION

The fault detection and isolation procedure is based on the following equation:

$$R_i(k+1) = |r_i(k+1) + \lambda R_i(k)|; 0 < \lambda < 1; i = 1, ..., m \tag{12}$$

With $R_i(0) = r_i(0)$, λ a forgetting factor, $r_i = y - \hat{y}_i$ is the residual given by the observer associated to the ith fault and $\hat{y}_i$ is the estimated measured output given by the same observer ($i = 0$ corresponds to a no fault status).

Remark 5.1:

• When a fault i occurs, it sets the value of u_i of the switched system to a permanent value.

• An observer associated to a fault i is based on equation (9) with its input u_i equal to the value set by the fault.

Remark 5.2 : The observer associated to the healthy system is not affected by the fault occurrence, its input u_i remains connected to the controller.

Assumption 5.1:

• The discrete fault i is detectable, meaning that its occurrence causes a change in the dynamic behavior of the system.

• The occurrence of the discrete fault i improves the estimated states given by the observer related to the fault i.

Theorem 5.1: Assuming that each observer is well defined, if there is not a fault occurrence then there is a real positive value ε_0 such that:

$$lim_{k \to +\infty} R_0 \leq \varepsilon_0 \tag{13}$$

Given **assumption 5.1**, the occurrence of a fault i leads to:

$$lim_{k \to +\infty} R_i \leq \varepsilon_i \tag{14}$$
$$lim_{k \to +\infty} R_0 \geq \varepsilon_0 \tag{15}$$
$$lim_{k \to +\infty} R_{j \neq i} \geq \varepsilon_{j \neq i} : j = 1, ..., m \tag{16}$$

Proof: In the case of a healthy system when the fault $i = 0$, then **remark 4.2** is verified leading to:

$$|r_0(+\infty)| < ... < |r_0(k)| < |r_0(k-1)| < ... < |r_0(0)| \tag{17}$$

So, there exists a real value r_{max} such that:

$$lim_{k \to +\infty} |r_0(k)| \leq r_{0_{max}} \tag{18}$$

Also, (**??**) can be expanded to become:

$$R_i(k+1) = |r_i(k+1) + \lambda r_i(k) + \lambda^2 r_i(k-1)$$
$$+ \lambda^3 r_i(k-1) + ... + \lambda^{k+1} r_i(0)|; 0 < \lambda < 1;$$

Since $0 < \lambda < 1$, so $lim_{k \to +\infty} \lambda^k = 0$, then:

$$lim_{k \to +\infty} R_0(k+1) \leq |r_{0_{max}} + R_{0_{max}}| \tag{19}$$

Where, $R_{0_{max}}$ is a maximum real value containing the weighted sum of the r_0 new values (the residual values that are close to the instant $(k+1)$ which proves (**??**).

Following **remark** 5.1, in the case of a fault occurrence, the same reasoning can be followed to prove (**??**) because the input u_i of the faulty system and that of the observer associated to the fault i are equal, which leads to:

$$lim_{k \to +\infty} R_i(k+1) \leq |r_{i_{max}} + R_{i_{max}}| \tag{20}$$

Where, $r_{i_{max}}$ and $R_{i_{max}}$ are real values.

Also, following **Remark 5.2**, for every control input u_i different from the value set by the fault the observer related to the healthy system does not take it into account leading to:

$$lim_{k \to +\infty} R_0(k+1) \geq |r_{0_{max}} + R_{0_{max}}| \tag{21}$$

Which proves (**??**) That also can be said about the other observers that have an input $u_{j \neq i}$ set permanently to a fixed value, see **Remark 5.1**, but their other inputs are connected to the controller. So, for every control input value u_j different from the value of u_j of the jth observer, the latter does not take it into account leading to:

$$lim_{k \to +\infty} R_j(k+1) \geq |r_{j_{max}} + R_{j_{max}}| \tag{22}$$

Where, $r_{j_{max}}$ and $R_{j_{max}}$ are real values, which prove equation (16).

From **Theorem 5.1**, let consider $\tilde{R}_i$ as a threshold value of R_i used to generate a localization signature of the ith fault as follows:

$$sg_i = \begin{cases} 0 \ if R_i > \tilde{R}_i \\ 1 \ if R_i < \tilde{R}_i \end{cases} \tag{23}$$

Where, $sg_i = 1$ corresponds to the appearance of the ith fault and $sg_i = 0$ means that the corresponding fault did not occur.

The choice of λ in (12) affects the sensibility of the detection. Indeed, a small value attenuates the contribution of the residual's old values and increases the variation speed of R_i, which let appear several peaks that can alter the detection of the fault. In the contrary, a bigger value attenuates the peaks and slow down the variation speed of R_i. Thus, the time taken in the procedure of detection and isolation of the fault is slower but the accuracy is better.

VI. APPLICATION TO A THREE CELLULAR CONVERTER

The FTC developed above is applied on a real three cellular converter located in LAMIH (Laboratory of Industrial and Human Automation Control, Mechanical Engineering and Computer Science), Valenciennes, France. Multicellular converters are typical examples of hybrid systems, constituted of the association of several cells separated by capacitors. Each cell is formed by two complementary switches where each one has a binary value (0 if open and 1 if closed), which results in a hybrid behavior of the process. Its main objective is to decrease the power supply to a sustainable level for the load when the power source is so elevated. The converter distributes the elevated power between several cells

which limits the constraint voltages on the semiconductor components. Moreover, it is possible to control the output current if the semiconductors are manipulated using a suitable control technique. A three cell converter, Fig. 2, has two capacitors, eight operating modes for every combination value of its switches, see Table I, and four output voltage levels.

TABLE I.   Mode Configuration of a Three Cells Converter

	u_3	u_2	u_1	V_s
Mode 0	0	0	0	0
Mode 1	0	0	1	V_{c1}
Mode 2	0	1	0	V_{c1}
Mode 3	0	1	1	V_{c2}
Mode 4	1	0	0	V_{c1}
Mode 5	1	0	1	V_{c2}
Mode 6	1	1	0	V_{c2}
Mode 7	1	1	1	E
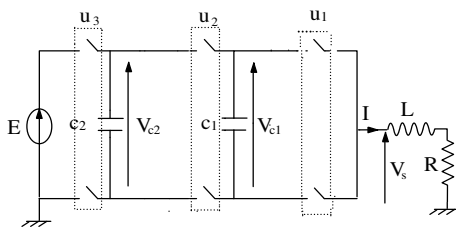
Fig. 2.   Structure of a three cell converter with RL load.

The process is described by the following equation:

$$\begin{pmatrix} \frac{dV_{c_1}}{dt} \\ \frac{dV_{c_2}}{dt} \\ \frac{dI}{dt} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \frac{u_2-u_1}{C_1} \\ 0 & 0 & \frac{u_3-u_2}{C_2} \\ \frac{u_1-u_2}{L} & \frac{u_2-u_3}{L} & -\frac{R}{L} \end{pmatrix} \begin{pmatrix} V_{c_1} \\ V_{c_2} \\ I \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \frac{E}{L}u_3 \end{pmatrix}$$
$$(24)$$

Where, $u_i \in \{0,1\}$ with i = 1, 2, 3 are binary input variables, $X = [V_{c1} \ V_{c2} \ I]^T$ is the state vector containing the capacity voltages and the output current, E is the the supply voltage, C_1, C_2 are the capacity values and $R - L$ represents the load.

In general, industrials use an open loop control when dealing with the multicellular converters to reduce the cost of the capacitor voltage sensors. The drawback is the appearance of several oscillations in the output responses with a slow dynamic before attaining the output references. Therefore, an alternative solution would be using closed loop controller with state observers to estimate the capacitor voltages. But, it can be deduced from (**??**) that the system is not observable for any combination input, as the rank of the observability matrix is inferior to 3. Fortunately, the three cell converter presents several transition modes that meet $Z(T_N)$-observability [17]. That will be exploited by the FCS-PC algorithm in order to achieve a proper estimation and acceptable reference tracking. As discussed in **Remark 5.2**, as long as the sequences insure the $Z(T_N)$- observability of the process, the estimation error decreases resulting in an improvement of the real output responses. But, in our case the predictive controller may choose some input combinations that will slow down the convergence rate like mode 0 and mode 7, because they do not satisfy the

first condition of $Z(T_N)$ observability mentioned in Section 4. Also, the transitions between mode 1 and mode 6 and between mode 3 and mode 4 do not satisfy the third condition of the $Z(T_N)$ observability. Because in the first transition, both mode 1 and mode 6 have $\dot{V}_{c_2} = 0$, and in the second transition, mode 3 and mode 4 have both $\dot{V}_{c_1} = 0$ as can be seen in (**??**). Moreover, the convergence is greatly affected by the switches commutation frequencies. Indeed, for a high frequency the observer cannot lose its minimum dwell time in the estimation. Two step are needed to overcome this problem: the first one is to remove mode 0 and mode 7 from the control algorithm. The controller will rely on the input redundancy of the converter to find alternative solutions to attain its objective. The second one is to use a restriction in the same algorithm to prevent transition between the modes having the commutation of two or three switches simultaneously which will decreases the commutation frequency and in the same time will prohibit the transitions not satisfying the $Z(T_N)$-observability. The resulting switching sequences that will be used by the controller is given in Fig. 3. One can find in [3], the modifications in the control algorithm that can be made to allow or to prohibit transitions between operating modes.
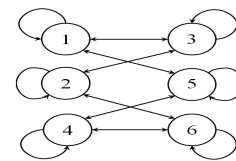

Fig. 3.   Transitions allowed to use from a current mode to a future mode.

A. Materials and methods

The process used to validate the presented FTC approach is constituted of three legs connected to a R-L load ($R = 200\Omega, L = 1H$). We used a three-cell converter, located in the first leg, see Fig. 4. The value of the capacitors between
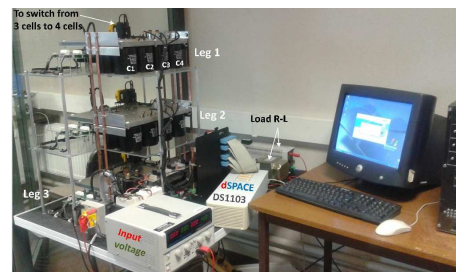

Fig. 4.   Photography of the experimental setup.

the cells are $C_1 = C_2 = 720\mu F$. The switches are bipolar transistors (IGBTs) model SKM100GB12V. The current and the voltage measurements are obtained from voltage sensors and current transduction. The source voltage of the converter is $E = 30V$ supplied by a rectifier.

A Matlab program file containing the FTC algorithm was compiled and run by a DSPACE card DS1103. The latter will be used to control the switch gates via its binary outputs after receiving the measurements of the current.

B. Experimental results

1) Predictive control for three-cell converter: Hereafter, the experimental results obtained after using control sequences that meet the conditions of the converter $Z(T_N)$-observability, see Fig. 5 that shows a zoomed view of the inputs switching. Fig. 6 shows, respectively, the capacity voltages V_{c_1}, V_{c_2} and the current load I where the output references are $V_{c1ref} = 10\,V$, $V_{c2ref} = 20\,V$, $I_{ref} = 0.08\,A$. The sampling period used is $T_e = 7\ 10^{-4}s$.

The parameters of the observer (9) are obtained by pole placement [16] as follows:

$$K_0 = 10^2 \begin{pmatrix} 0 \\ 0 \\ 8.55 \end{pmatrix}, K_1 = 10^4 \begin{pmatrix} 13.4625 \\ -6.75 \\ 0 \end{pmatrix},$$

$$K_2 = 10^4 \begin{pmatrix} -6.7125 \\ 6.7125 \\ 0 \end{pmatrix}, K_3 = 10^4 \begin{pmatrix} -6.75 \\ -13.4625 \\ 0 \end{pmatrix}$$

The matrices $\overline{A}_0, \overline{A}_1, \overline{A}_2, \overline{A}_3, \overline{B}_1, \overline{B}_2$ and $\overline{B}_3$ for three cell converter can be found in [16]. The error estimation of V_{c_1} and
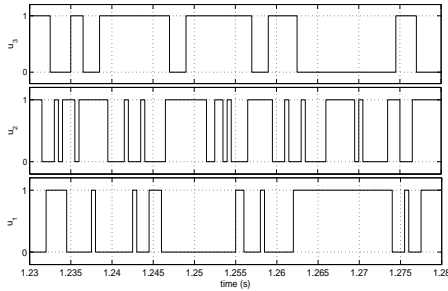
Fig. 5. Control inputs with transitions satisfying the $Z(T_N)$ observability.
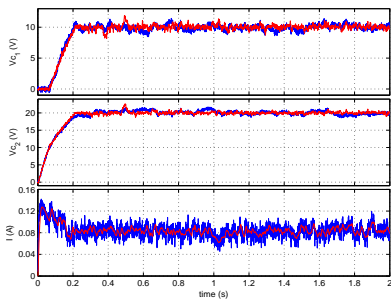
Fig. 6. Experimental results of the capacitor voltages and the output current; (blue line) measured values and (red line) estimated values.

V_{c_2} displayed in Fig. 7 are acceptable and in the same time, the real outputs values in Fig. 5 follow closely enough their references. However, the imposed restrictions on the control algorithm do not come without drawbacks, as it can be seen in the current I response where the fluctuation rate around its reference is significant but remains acceptable.
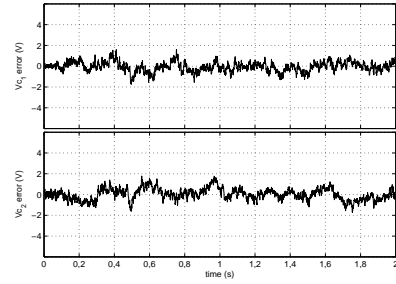
Fig. 7. V_{c_2} and V_{c_1} estimation error.

2) Fault tolerant predictive control: Hereafter, the results of the proposed fault tolerant control strategy are shown. As discussed previously, the study focuses on the discrete failure that may happen to the multicellular converter when one or several switches fail to open or to close when needed.

In the literature, very few works cover the problem. In fact, some studies are only restricted to the fault identification without considering the control of the system. One of the reasons can be related to how we can use the remaining operating modes after the appearance of the fault. That issue was solved here using several predictive control algorithms, hence the contribution made in this paper.

The application is restricted to the case where one cell is stuck closed (stuck open, respectively) with a different cell each time to cover all the potential cases. To that end, 7 observers were used, where three are affected respectively to the failure stuck closed of u_1, u_2 and u_3, three to the failure stuck open and the last one affected to the non faulty converter. All the observers are based on (**??**), where the faulty input $u_{i=\{1,2,3\}}$ of every observer is equal to 1 if stuck closed or 0 if stuck open and the non faulty inputs are driven by the controller.

TABLE II. CAPACITY VOLTAGES RESPONSES AFTER THE APPEARANCE OF A FAILURE

	$u_3 u_2 u_1$	modes	$\dot{V}_{c_2}$	$\dot{V}_{c_1}$
	1 0 0	4	I/c	0
u_3 stuck close	1 1 0	6	0	I/c
	1 0 1	5	I/c	$-I/c$
	0 1 0	2	$-I/c$	I/c
u_2 stuck close	0 1 1	3	$-I/c$	0
	1 1 0	6	0	I/c
	0 0 1	1	0	$-I/c$
u_1 stuck close	0 1 1	3	$-I/c$	0
	1 0 1	5	I/c	$-I/c$
	0 1 1	3	$-I/c$	0
u_3 stuck open	0 0 1	1	0	$-I/c$
	0 1 0	2	$-I/c$	I/c
	0 0 1	1	0	$-I/c$
u_2 stuck open	1 0 1	5	I/c	$-I/c$
	1 0 0	4	I/c	0
	0 1 0	2	$-I/c$	I/c
u_1 stuck open	1 0 0	4	I/c	0
	1 1 0	6	0	I/c

All the potential failures and their consequences on the system states are described by Table II. Note that the current I always flows in one direction because of the load. Considering that, one can see that in some cases it is possible to control at least two states of the system. For example, when u_3 is

stuck close, V_{c_2} can increase or remain invariable but cannot decrease. However, V_{c_1} is not affected by the failure of u_3, as can be seen from equation (24), so it is controllable and the same can be said for the current since it depends on V_{c_1}. Also, when u_1 is stuck close, V_{c_1} cannot increase and V_{c_2} is not affected by the failure, so it is controllable along with the output current.

There are other cases where it is not possible to control any of the outputs of the converter. For example, when u_2 is stuck closed (respectively stuck open), we can see that V_{c_1} cannot decrease and V_{c_2} cannot increase (respectively V_{c_1} cannot increase and V_{c_2} cannot decrease) and consequently the current I is not controllable.

When u_3 is stuck open, the current source is disconnected and the current I provided by the capacities will obviously decrease until disappearing. When u_1 is stuck open, V_{c_2} is not affected, so we can suppose that it is controllable unlike V_{c_1}. But, in reality that is not true because the path enabling the discharge of the capacities are cut off, so V_{c_2} cannot decrease. Further explanation on that case will be given after displaying the states responses of the converter.

The detection and isolation of the fault in this experimentation is based on Table III where $\tilde{R}_0$ and sg_0 are associated to the healthy mode, $\tilde{R}_1$, $\tilde{R}_2$, $\tilde{R}_3$ and sg_1, sg_2, sg_3 are respectively associated to u_1, u_2, u_3 stuck closed and $\tilde{R}_4$, $\tilde{R}_5$, $\tilde{R}_6$ and sg_4, sg_5, sg_6 are respectively associated to u_1, u_2, u_3 stuck open. Following **Theorem 5.1**, it is save to

TABLE III.   Fault Detection and Localization

$\tilde{R}_0 = 1.2$	sg_0	1	0	0	0	0	0	0
$\tilde{R}_1 = 1.3$	sg_1	x	1	0	0	0	0	0
$\tilde{R}_2 = 1.3$	sg_2	x	0	1	0	0	0	0
$\tilde{R}_3 = 1.3$	sg_3	x	0	0	1	0	0	0
$\tilde{R}_4 = 1.3$	sg_4	x	0	0	0	1	0	0
$\tilde{R}_5 = 1.3$	sg_5	x	0	0	0	0	1	0
$\tilde{R}_6 = 1.3$	sg_6	x	0	0	0	0	0	1
current fault	f	0	1	2	3	4	5	6

prioritize the signature of the healthy system over the others signatures. So, when $sg_0 = 1$ all the other signatures are ignored and the current fault f is 0 meaning that the converter operates properly. When sg_0 pass from 1 to 0 that means the appearance of a fault. In that case, sg_0 will hold to its value and an isolation input sequence will replace the control sequence for a time delay corresponding to the minimum dwell time for the stabilization of R_i related to all the observer. After that, the faulty cell and its type is identified (stuck close if $1 \le f \le 3$ or stuck open if $4 \le f \le 6$).

The application will proceed as follows: initially, the three cell converter will operate without fault. After 4 seconds $u_{i=\{1,2,3\}}$ is stuck close (open respectively). When the signature sg_0 pass from 1 to 0, a PWM (pulse wave modulation) input sequence is triggered to isolate the faulty cell, and when that happens the controller will be reconfigured to an appropriate control algorithm. The PWM signal was chosen with a duty cycle qual to 0.5 because the input sequence in that case does not use mode 0 or mode 7 [17]. That choice will improve the estimation since it will reduce the use of sequence unfavourable to $Z(T_N)$-observability. Also, a switching frequency $fs = 5hz$ of the PWM sequence was chosen to offer the time needed for the convergence of the

observer associated to the failure and the divergence of the others.

The detection and localization results of some fault cases are displayed in Fig. 8, 9 and 10 when u_1 is stuck closed and in Fig. 11, 12 and 13 when u_3 is stuck closed.
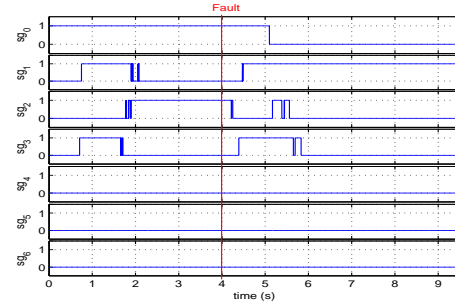

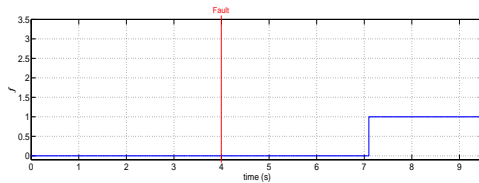Fig. 8.   Signature evolutions when u_1 is stuck closed.

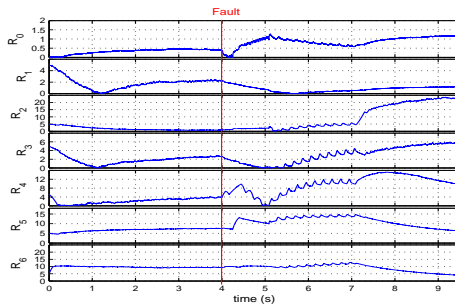Fig. 9.   Fault localization when u_1 is stuck closed.

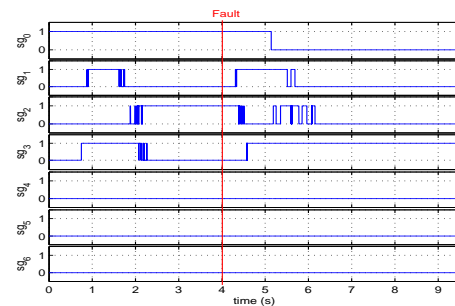Fig. 10. R_i evolution when u_1 is stuck closed.

Fig. 11.   Signature evolutions when u_3 is stuck closed.

We can see that some signatures commute to 1 even when there is no fault or there is a different fault. For example, Fig. 11 where we have sg_2 equal to 1 when the converter operates
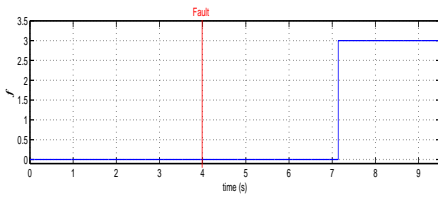
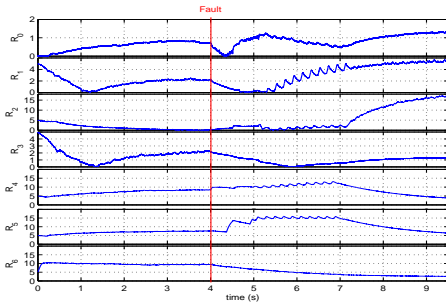Fig. 12. Fault localization when u_3 is stuck closed.

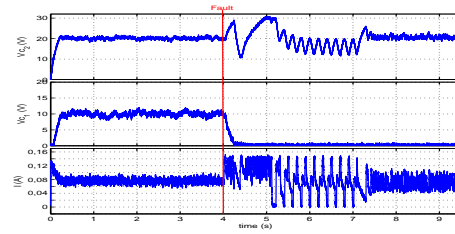Fig. 13. R_i evolution when u_3 is stuck closed.

Fig. 14. Experimental results using the proposed FTC when u_1 is stuck closed.

Fig. 15. Experimental results for inputs control applied to the converter when u_1 is stuck closed.

correctly. That is because R_2 increases until reaching its threshold value, see Fig. 13, which is caused by the controller setting u_2 to 1. In that case the observer of the converter and the one related to the fault are similar since they use the same (??) with the same input $u_2 = 1$. When the controller set u_2 to 0, R_2 will increase because its corresponding observer has u_2 equal to 1, sg_2 changes to 0 when the controller maintains $u_2 = 0$ for enough time until R_2 increases over its threshold.

The fault localization was set to 3.1 seconds after the fault detection (i.e., when $sg_0 = 0$) to identify accurately the fault. The reason is related to the slow variation of $R_{i=0,...,6}$ because the value of λ in equation (12) was taken big enough to filtrate the measurement noises that can tamper the results. However, some faults can be isolated after only 2.1 seconds, like when u_1 or u_3 are stuck closed. Indeed, each fault changes the input sequences favourable to $Z(T_N)$-observability, so the isolation time is not the same for each different fault.

When a fault occurs, some transitions will be discarded which compels the system to use a very reduced number of configuration modes. Table II includes the remaining configuration modes to use for each fault case.

When the failure is identified, the control algorithm will consider only those modes and removes the others when computing the minimal value of the cost function. That will prevent the use of wrong sequences that target a healthy process and use only the sequences that aim to control the corresponding faulty process. Also, in order to improve the control results, the one commutation restriction on the switches used when the converter operates correctly was removed from the algorithm.

The input control and the outputs of the converter are shown in Fig. 15 to 24. It can be seen the change in the shape of the switching commutation after the appearance of the fault, then the PWM sequence is used, and finally the switching sequence to control the faulty system.

The output results when u_1 is stuck closed are presented in
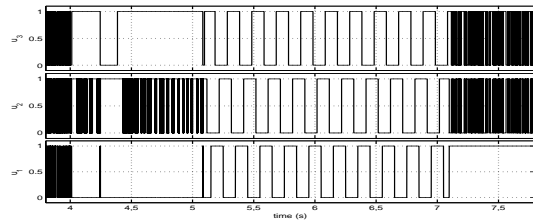
Fig. 14 where it can be seen after the appearance of the fault that the responses move away from their references for 3.1 seconds where only R_1 is under its threshold value, in that instant the information is given to the controller to modify its algorithm taking into account the fault as can be seen in Fig. 15. The FTC is able then to return V_{c_2} and I to their reference values but was not able to do the same to V_{c_1}. The latter cannot increase because it is connected permanently to the load so when $u_2 = 0$ the capacity C_1 discharges and when $u_2 = 1$ it will not charge because the current heads to the load without passing through C_1.
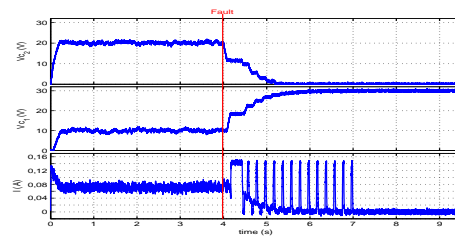

Fig. 16. Experimental results using the proposed FTC when u_2 is stuck closed.
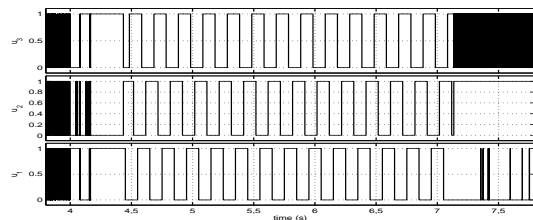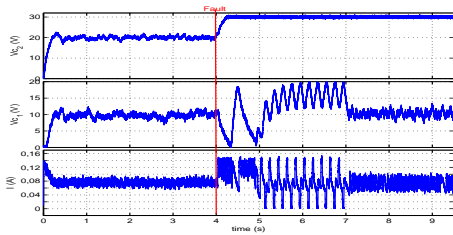

Fig. 17. Inputs control applied to the converter when u_2 is stuck closed.

Fig. 16 describes the evolution of the system states when u_2 is stuck closed. It can be seen in Fig. 17 that there is not a single input combination able to control V_{c_1} and V_{c_2} as explained previously in Table II, but we can also see that there is one combination for which the current increases very

fast, that is when all the superiors switches are closed. So, the voltage output commutes between $0Volt$ and E and so I commute between 0 A and E/R.

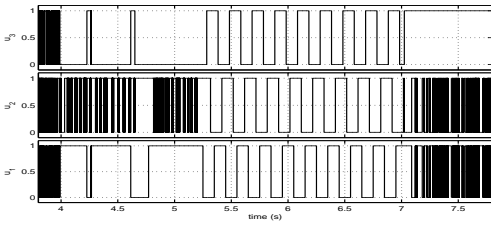Fig. 18.   Experimental results using the proposed FTC when u_3 is stuck closed.

Fig. 19.   Inputs control applied to the converter when u_3 is stuck closed.

The output results when u_3 is stuck closed are presented by Fig. 18. It can be seen after the appearance of the failure that the responses lose their tracks and remain that way until R_3 pass under its threshold value and the others are above their threshold values. At that time, the information is given to the controller to modify its algorithm taking into account the fault as can be seen in Fig. 19. The FTC is able then to return V_{c_1} and I to their reference values but was not able to do the same to V_{c_2} because the latter cannot decrease. That makes sense since the capacity C_2 is connected permanently to the source E because of the failure.
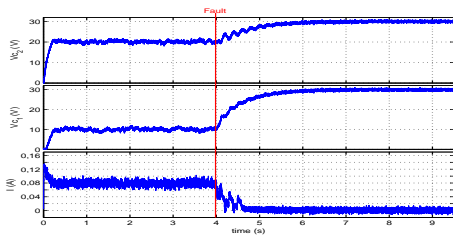

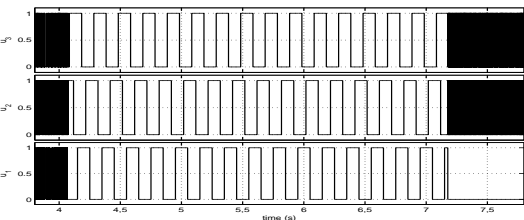Fig. 20.   Experimental results using the proposed FTC when u_1 is stuck open.

Fig. 21.   Inputs control applied to the converter when u_1 is stuck open.

Fig. 20 shows the evolution of the system states without a possibility to be controlled after the appearance of the fault

as can be seen in Fig. 21. Indeed, even if V_{c_2} can increase or decrease (see Table II) which is not the case with V_{c_1} since it can only increase leading at some point to $V_{c_1} \geq V_{c_2}$. At that instant, the current I stops flowing from C_2 to C_1 so it becomes equal to zero and V_{c_2} becomes invariable.
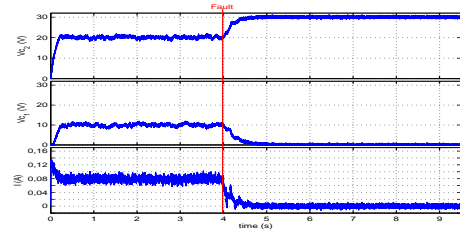

Fig. 22.   Experimental results using the proposed FTC when u_2 is stuck open.
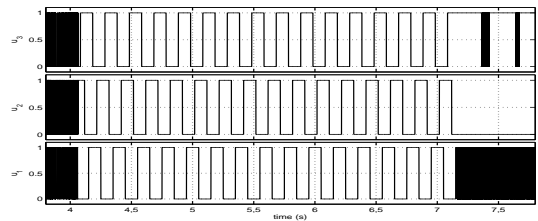

Fig. 23.   Inputs control applied to the converter when u_2 is stuck open.

The analysis in the case of u_2 is stuck open in Fig. 22 and 23 is analog to that when u_2 is stuck closed the two capacity voltages are not be controllable C_1 and C_2. The first cannot decrease and the second cannot increase. Thus, the current can not controllable.
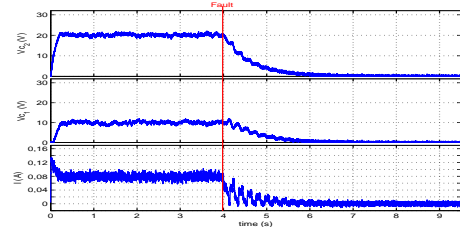

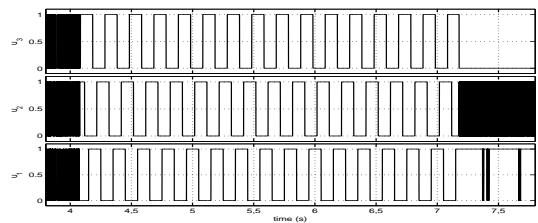Fig. 24.   Experimental results using the proposed FTC when u_3 is stuck open.

Fig. 25.   Inputs control applied to the converter when u_3 is stuck open.

In the case where u_3 is stuck open, see Fig. 24 and 25, the source power is disconnected so V_{c_2} decreases and the current that remains in the capacities will gradually decrease until reaching zero.

As can be seen, after the appearance of the fault, the proposed FTC strategy is able to control some of the system's

states when they are controllable. But in the other cases, the system states are not controllable, either because of the disconnection of the power source, or because of the path allowing the discharge of the capacities are cut off. A solution can be found with a modification in the structure of the converter similar to the solution suggested in [18]. For example it is possible to incorporate alternative switchers for used when u_1 is stuck open to allow the discharge of the capacities and another one is used when u_3 is stuck open to prevent the disconnection of the power source. In that case, the converter will operate with two cells leading to another new configuration that did not exist before the fault.

Nevertheless, the results in the controllable fault cases are acceptable, the load current along with the remaining controllable capacitor voltage is well maintained around their references.

VII. Conclusion

The presented work covers multiple areas: control, observation, fault detection and isolation of hybrid systems. The main objective is to build an FTC strategy based on a predictive controller having a finite control set to apply on a linear switching system.

This paper focuses on a certain class having non-observable subsystems, hence the contribution made in this work. A solution can be found when using the $Z(T_N)$-observability approach in order to identify the fault. However, controlling the system after that is another difficult problem. In fact, the fault compel the controller to use a very reduced number of operating modes. Consequently, the objective was partially reached because of the non controllability of the system's states in some fault cases. A part from that, the proposed method is able to control the hybrid system despite its $Z(T_N)$-observability nature before and after the appearance of a failure as shown by the experimental results. Future works can focus on reducing the detection and isolation time and search a FTC strategy based on a different control technique than the predictive algorithm.

References

[1] D. Liberzon and A.S. Morse, *Basic problems in stability and design of switched systems*, IEEE Control Systems, Vol.19, No.5, pp.59–70, 1999.

[2] J.V Gorp, M. Defoort and M. Djemai, *Binary signals design to control a power converter*, 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), pp.6794–6799, 2011.

[3] A. Smati, D. Berdjag, W. Chagra, M. Defoort and M. Ksouri, *Predictive control for multicell converter*, 2nd International Conference on Automation,Control, Engineering and Computer Science Proceedings of Engineering and Technology (PET), 2015.

[4] J.V. Gorp, M. Defoort, K. Veluvolu and M. Djemai, *Hybrid sliding mode observer for switched linear systems with unknown inputs*, Journal of the Franklin Institute, vol.351,(7), pp.3987–4008, 2014.

[5] N. Orani, A. Pisano, M. Franceschelli, A. Giua and E. Usai, *Robust reconstruction of the discrete state for a class of nonlinear uncertain switched systems*, Nonlinear Analysis : Hybrid Systems, vol.5,(2), pp.220–232, 2011.

[6] F. Arichi, M. Djemai and B. Cherki, *Active mode detection for a class of hybrid dynamic systems*, International Conference on Systems, Signal Processing and Electronics Engineering (ICSSEE'2012), pp.210–215, 2012.

[7] A. Alessendri and P. Coletta, *Design of Luenberger observers for a class of hybrid linear systems*, IHybrid systems: computation and control. Lecture notes in computer science, pp.7–18, 2001.

[8] A. Balluchi, L. Benvenuti, M. D. Di Benedetto, A. L. Sangiovanni-Vincentelli, *Design of observers for hybrid systems*, Hybrid Systems: Computation and Control, pp.76–89, 2002.

[9] J.V. Gorp, M. Defoort, M. Djemai and N. Manamanni, *Hybrid Observer for the Multicellular Converter*, 4th IFAC Conference on Analysis and Design of Hybrid Systems, pp.259–264, 2012.

[10] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen and D. Teneketzis, *Failure diagnosis using discrete event models*, Decision and Control, Proceedings of the 33rd IEEE Conference on, vol.3,(2), pp.3110–3116, 1994.

[11] A. Takrouni, N. Zanzouri, V. Cocquempot and M. Ksouri, *Robust Diagnosis for Hybrid Dynamical Systems*, International Journal of Engineering and Innovative Technology, Vol. 3, (9), pp. 312–318, 2014.

[12] M. S. Branicky , *Multiple Lyapunov functions and other analysis tools for switched and hybrid systems*, IEEE Transactions on Automatic Control, vol.43, pp.475–482, 1998.

[13] P. Lezana, R. Aguilera and D. E. Quevedo , *Model Predictive Control of an Asymmetric Flying Capacitor Converter*, IEEE Transactions on Automatic Control, Vol.56, No.6 pp.1839 –1846, 2009.

[14] L. Hetel, M. Defoort and M. Djema, *Binary Control Design for a Class of Bilinear Systems: Application to a Multilevel Power Converter*, IEEE Transaction on control systems technology, Vol. 24, pp. 719 – 726, 2015.

[15] J. Lygeros, K. Johansson, S. Simic, J. Zhang and S. Sastry, *Dynamical Properties of Hybrid Automata*, IEEE Transactions on Automatic Control, Vol.48, pp.2–17, 2003.

[16] P. Riedinger, M. Sigalotti, J. Daafouz, K. Johansson, S. Simic, J. Zhang and S. Sastry, *On the algebraic characterization of invariant sets of switched linear systems*, Automatica, Vol.46, No.6, pp.1047–1052, 2010.

[17] J.V. Gorp, M. Defoort, M. Djemai and N. Manamanni, *Hybrid Observer for the Multicellular Converter*, 4th IFAC Conference on Analysis and Design of Hybrid Systems, pp.259–264, 2012.

[18] S. Meradi, K. Benmansour, M. Djemai, M. Tadjine and M.S. Boucherit, *Fault Detection and sliding mode reconfiguration for the Multi-cellular Converter three cells*, 4th International conference on electrical engeneering, pp. 615–620, 2012.