Actuator fault tolerant control: a receding horizon set-theoretic approach

Giuseppe Franzè, Francesco Tedesco and Domenico Famularo

***Abstract*—In this note a novel actuator Fault Tolerant Control strategy for constrained discrete time linear systems subject to bounded disturbances is proposed. The scheme consists of three modules: a bank of estimators, each one associated with healthy and faulty model configurations, a logic mechanism for identifying healthy-to-faulty and faulty-to-healthy transitions and an estimate based control reconfiguration unit. The idea is to abstractly describe healthy and faulty plant configurations by means of a switching paradigm and sequences of pre-computed inner approximations of one-step controllable sets. Such regions are then on-line exploited together with a switching logic to determine the current plant configuration on the basis of the state estimate provided by the observers.**

I. Introduction

Modern technological systems rely on sophisticated control schemes designed to meet performance and safety requirements. Traditional feedback control algorithms could exhibit significant loss of performance or even instability in the occurrence of actuators, sensors or other system components anomalies. In particular, noticeable contributions have rephrased actuator faults as command input saturation constraints , see e.g. [2], [11], [9] and references therein. A more systematic way to address these issues is to exploit Fault Tolerant Control (FTC) schemes which need to be implemented to steer/hold the plant to/into a safe and acceptable state whenever undesirable fault events occur [3], [16]. FTC is currently an important research area as testified by several recent papers, see e.g. [5] and references therein.

Of interest here are the results from [14] and [15] where a set-theoretic approach for designing MPC sensor-based FTC schemes are proposed. In these contributions, the idea relies on the separation of "healthy" attractive invariant sets, where appropriate fault residual signal variables remain under healthy operations, from "under-fault" sets which instantaneously capture the behaviour of the residuals when abrupt faults occur in one or more groups of sensors. An important property of this "set-based" approach is that the resulting scheme can be guaranteed to be "resilient" under severe sensor faults. Along this research line, it is worth to note that FTC approaches based on the MPC philosophy have only been recently developed. deal with an incipient actuator faults is developed.

Here, we propose a novel FTC scheme for input constrained systems which exploits the one-step controllable set concept within a plant subject to unpredictable events on actuators by means of a hybrid system paradigm. A family of one-step controllable set sequences associated to a predetermined family of nominal plant configurations (derived with respect to the fault category) is first computed. When the plant deviates from its normal behaviour the corresponding linearized configuration is identified and the *reconfigured* control action is obtained by means of a receding horizon strategy originally developed for multi-model linear plants [1]. In spite of its simplicity, such an idea involves two critical aspects in the authors' opinion: the former is the capability of the proposed FTC scheme to discriminate amongst all the system configurations and the second is the correct model switching procedure so as to maintain closed-loop stability and constraints fulfilment. To this end the proposed FTC scheme consists of three interconnected modules: a bank of observers each one tuned with respect to the system configuration related to all the possible fault occurrences, a *certainty equivalence* based switching logic (see [12]) which is in charge to on-line generate the plant mode estimate and a reconfiguration unit for computing the proper control action.

Finally, simulations on an interconnected tank system provide comparisons with the recent MPC-based FTC scheme of Yetendje *et al.* [15] under the occurrence of critical faults.

G. Franzè, F. Tedesco and D. Famularo are with DIMES, Universitá della Calabria, Via Pietro Bucci, Cubo 42-C, Rende (CS), 87036, ITALY {franze,ftedesco,famularo}@dimes.unical.it

Notations

Given a set $S \subseteq X \times Y \subseteq \mathbb{R}^n \times \mathbb{R}^m$, the projection of the set S onto X is defined as $\text{Proj}_X(S) := \{x \in X \,|\, \exists y \in Y \text{ s.t. } (x,y) \in S\}$. Moreover, we denote with 0_q the vector of q zero entries.
Let $M = [\text{col}_i(M)]_{i=1}^m \in \mathbb{R}^{n\times m}$ and $N = [\text{col}_i(N)]_{i=1}^m \in \mathbb{R}^{n\times m}$ be given matrices, we shall denote with $M \subset (\subseteq) N$ the inclusion operator such that

$$\{\text{col}_1(M), \ldots, \text{col}_{q_M}(M)\} \subset (\subseteq)\{\text{col}_1(N), \ldots, \text{col}_{q_N}(N)\},$$

with $\text{col}_i(M) \neq \text{col}_k(M), \forall i \neq k$, $\text{col}_i(N) \neq \text{col}_k(N), \forall i \neq k$, and $\text{col}_i(M) \neq 0_n$, $\text{col}_j(N) \neq 0_n$, $\forall i = 1, \ldots, q_M$, $\forall j = 1, \ldots, q_N$.

II. Problem formulation

We consider plants described by the following linear discrete-time model

$$\begin{array}{rcl} x(t+1) & = & Ax(t) + Bu(t) + B_d d(t) \\ y(t) & = & Cx(t) \end{array} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ denotes the state, $u(t) \in \mathbb{R}^m$ the input and $d(t) \in \mathbb{R}^d$ the process disturbance. It is assumed that $d(t) \in \mathcal{D} \subset \mathbb{R}^d$, $\forall t \in \mathbb{Z}_+ := \{0, 1, ...\}$, with $\mathcal{D}$ a compact set with $0_d \in \mathcal{D}$. Moreover the plant is assumed to be stabilizable and detectable and the control input is subject to the following saturation constraints

$$u(t) \in \mathcal{U},\ \forall t \geq 0,\ \ \mathcal{U} := \{u \in \mathbb{R}^m \,|\, u^T u \leq \bar{u}\}, \tag{2}$$

with $\bar{u} > 0$ and $\mathcal{U}$ a compact subset of $\mathbb{R}^m$ containing the origin as an interior point.
In the sequel, we fix our attention to the case of damaged actuators by leaving out loss of effectiveness occurrences. An FTC strategy capable to regulate (1) by selecting a step-by-step control law complying with the prescribed constraints and with any possible fault actuator occurrence is then proposed. Moreover in order to characterize the plant dynamics due to a generic $i-th$ actuator fault occurrence, the following state space description is considered

$$x(t+1) = Ax(t) + B^i u(t) + B_d d(t) \tag{3}$$

where $B^i = B \cdot \text{diag}([\alpha_1^i, \ldots, \alpha_m^i])$, with $\alpha_i \in \{0,1\}$. The meaning of (3) is that if a single or multiple actuators are no longer available, the plant is driven by the remaining healthy devices associated with the input map B^i. Therefore, all admissible fault events can be abstractly collected into a switching system consisting of a finite number of subsystems (3):

$$\Sigma_\sigma : \begin{cases} x(t+1) = & Ax(t) + B^i u(t) + B_d d(t) \\ y(t) = & Cx(t), \ i \in \mathcal{I} := \{0,1,\ldots,l\} \end{cases} \quad (4)$$

with $B^0 \equiv B$ being the healthy condition. The finite state machine (switching logic), that orchestrates switchings between these subsystems, generates a proper signal which is described as classes of piecewise constant sequences $\sigma : \mathbb{Z}_+ \to \mathcal{I}$ and the index $i = \sigma(t)$ is the *active mode* at the time instant t.
The problem to solve can be stated as follows.

Actuator Fault Tolerant Control (AFTC) Problem - *Given the plant (1), at each time instant t compute an FTC strategy consisting of an estimation actuator fault module capable to detect the current switching system (4) active mode $i(t)$ and a control reconfiguration algorithm such that the regulated plant (1) is asymptotically stable and satisfies input-saturation constraints regardless of any disturbance occurrence.* □

III. The FTC strategy

Here we use set-theoretic ideas (see [2] for a comprehensive tutorial) within a system framework subject to unpredictable events. To this end, the initial idea is to design a set of one-step controllable sets each one associated to the $i-th$ mode of the switching system (4). When an anomaly on the plant behaviour is detected and the corresponding $j-th$ mode identified, the *reconfigured* control action is achieved via the receding horizon strategy developed in [1]. Such a strategy involves two critical points: **1)** How to discriminate amongst the l configurations (4)? **2)** How to ensure a correct model configuration switching ($i \to j$, $i \neq j$,) such that the closed-loop stability and constraint fulfilment are preserved?

To deal with these questions, we propose the FTC scheme depicted in Fig. 1 and consisting of three modules: a bank of $l+1$ estimator devices each one associated to the $i-th$ system configuration, a *Switching logic* whose output $\hat{\sigma}(\cdot)$ is an estimate of the switching signal $\sigma(\cdot)$ and a *Reconfiguration unit* for computing the proper control action $u(\hat{x}_{\hat{\sigma}(\cdot)})$ on the basis of the state estimate $\hat{x}_{\hat{\sigma}(\cdot)}$.

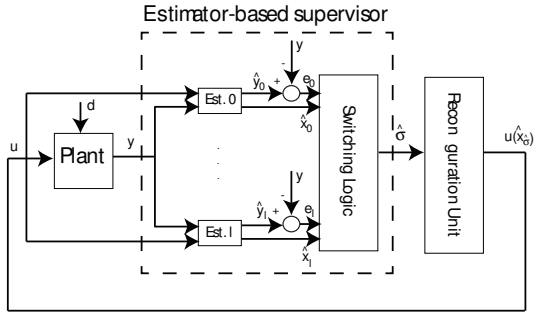

Fig. 1. The AFTC strategy scheme

A. Estimator-based supervisor

In this section we describe the basic ingredients of an estimator-based supervisory whose main ideas have been developed in the seminal papers of Morse *et al.* [8], [12].

A family of control laws is designed for each model configuration (4) such that the control action produced by the selected controller would yield the desired behaviour if the configuration were exactly known. Then, the supervisor is composed of a set of observers and a switching logic scheme where each estimator numerically identifies the actual plant output in either one of the healthy or faulty configurations. Performance are evaluated by computing a norm of the output estimation error related to the observer yielding the smallest performance index corresponding to the current working mode. The controller is then selected on the basis of the current estimate thanks to the *certainty equivalence* principle. Also, the value of $\hat{\sigma}(\cdot)$ at each time instant should coincide with the index of the smallest output error norm. In what follows we will design a certainty equivalence based FTC scheme which does not require the introduction of any dwell-time mechanism as one of its main merits.

1) Estimators: We consider a bank of estimators of the following form

$$\begin{array}{rcl} \hat{x}_i(t+1) & = & A\hat{x}_i(t) + B^i u(t) + L_i(y(t) - \hat{y}_i(t)) \\ \hat{y}_i(t) & = & C\hat{x}_i(t), \ \ i = 0,1,\ldots,l, \end{array} \quad (5)$$

where the gains $L_i \in \mathbb{R}^{n \times p}$, $i = 0,1,\ldots,l$, are such that $(A - L_i C)$ are Schur matrices and the disturbance effects are mitigated. When the estimator represented by the system (5) is connected to the plant (1), the error $e_i(t) := x(t) - \hat{x}_i(t)$ satisfies the following state space equation

$$\begin{array}{l} e_i(t+1) = (A - L_i C)e_i(t) + (B - B^i)u(t) + B_d d(t), \\ e_{y_i}(t) := y(t) - \hat{y}_i(t), \ \ i = 0,\ldots,l. \end{array} \quad (6)$$

Since there exists an unavoidable model mismatch on the input maps (see (6)), the design of the gain matrices L_i is performed by treating the command $u(t)$ as an additional disturbance.

2) Switching logic: The switching logic module identifies at each time instant t the current active mode of (4) by using the output estimation errors $e_{y_i}(t)$. In virtue of the *certainty equivalence principle* and by denoting with $\pi_i := \|e_{y_i}\|$, $i = 0,1,\ldots,l$, the output error norms, an estimate $\hat{\sigma}(t)$ of the switching signal $\sigma(t)$ is obtained by selecting the smallest value amongst all the π_i :

$$\hat{\sigma}(t) = \min_i \ \pi_i(t) \quad (7)$$

The main drawback of such an approach relies on the use of a set of nominal plant models that can give rise to chattering phenomena. In the sequel, we will show that this undesired behaviour will be strongly mitigated by resorting to a set-theoretic approach [2].

B. Reconfiguration unit

The core of the proposed strategy consists in exploiting the computation of the families of one-step controllable sets for each model configuration (4), i.e. $\{\mathcal{T}_i^j\}_{i=0}^N$, $j = 0,1,\ldots,l$, where the integer N defines the saturation level for the sequence growth, see [2] for detailed definitions.

To extend such a concept to the proposed framework, it is mandatory to notice that:

1) the switching signal $\hat{\sigma}(\cdot)$ is generated by using the state estimates, in order to ensure that effectively $\hat{x}_j$ lies into $\mathcal{T}_i^j$, this set must be computed by considering the augmented state $x_j^{aug} := [x_j^T \ \hat{x}_j^T]^T$, where x_j refers to the state evolution associated to the $j-th$ model configuration (4);

2) at each time instant t, the control input $u(\hat{x}_{\sigma(t)})$ is performed by using the active mode $\sigma(t)$. If a fault/recovery event jointly occurs with the application of this command, then the one-step state evolution $x_{\sigma(t)}^{aug}(t+1)$ could not belong to anyone element of the sequences $\{\mathcal{T}_i^{aug^j}\}_{i=0}^N$, $j=0,1,\ldots,l$, in the extended space x_j^{aug}. The latter straightforwardly comes out by noticing that a data incoherence in the observation pair $(u(\hat{x}_{\sigma(t)}), y(t))$, used for estimation purposes in (5), comes out: the first element $u(\hat{x}_{\sigma(t)})$ complies with the actual mode $\sigma(t)$, the second is retrieved instead by a different model configuration.

The point 1) implies that for each computation of the set sequences $\{\mathcal{T}_i^{aug^j}\}_{i=0}^N$ the following state space description has to be considered:

$$x_j^{aug}(t+1) = A_j^{aug}x_j^{aug}(t)+B_j^{aug}u(t)+B_{d_j}^{aug}d(t)+E_j^{aug}e_j(t) \tag{8}$$

where

$$A_j^{aug} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix},\ B_j^{aug} = \begin{bmatrix} B^j \\ B^j \end{bmatrix},$$

$$B_{d_j}^{aug} = \begin{bmatrix} B_d \\ 0 \end{bmatrix},\ E_j^{aug} = \begin{bmatrix} 0 \\ L_jC \end{bmatrix}$$

On the other hand, the reasoning in 2) gives rise to the following recursions for computing the sequences

$$\{\mathcal{T}_i^j\}_{i=0}^N := \text{Proj}_{\hat{x}_j}\{\mathcal{T}_i^{aug^j}\}_{i=0}^N,\ j=0,1,\ldots,l.$$

Let $\mathcal{T}_0^j$, $j=0,1,\ldots,l$, be robustly invariant terminal sets, then we have:

$$\begin{aligned}\mathcal{T}_i^0 :=& \text{Proj}_{\hat{x}_0}\{x_0^{aug} \in \mathbb{R}^{2n} : \exists\, u \in \mathcal{U} : \\ &\text{Proj}_{\hat{x}_0}\{A_0^{aug}x_0^{aug} + B_0^{aug}u + B_{d_0}^{aug}d + E_0^{aug}e_0\} \in \mathcal{T}_{i-1}^0, \\ &\forall e_0 \in \mathcal{E}_0, \text{Proj}_{\hat{x}_0}\{A_j^{aug}x_0^{aug} + B_j^{aug}u + B_{d_j}^{aug}d + E_j^{aug}e_j\} \\ &\in \mathcal{T}_{i-1}^j, \forall d \in \mathcal{D},\ \forall e_j \in \mathcal{E}_j, j=1,\ldots,l\},\end{aligned} \tag{9}$$

$$\begin{aligned}\mathcal{T}_i^j :=& \text{Proj}_{\hat{x}_j}\{x_j^{aug} \in \mathbb{R}^{2n} : \exists u \in \mathcal{U} : \\ &\text{Proj}_{\hat{x}_j}\{A_j^{aug}x_j^{aug} + B_j^{aug}u + B_{d_j}^{aug}d + E_j^{aug}e_j\} \in \mathcal{T}_{i-1}^j, \\ &\forall d \in \mathcal{D}, \forall e_j \in \mathcal{E}_j\}, j=1,\ldots,l.\end{aligned} \tag{10}$$

Recursions (9) compute the set sequence related to the healthy condition by including all the possible fault occurrences and, essentially, healthy-to-faulty transitions are guaranteed. The rationale behind formulas (9) can be better clarified by means of the next Fig. 2 where an illustrative scenario of healthy-to-faulty transitions of three system configurations is depicted: healthy, faulty-1 and faulty-2. There, the state estimate $\hat{x}_0$ obtained by using the *Estimator 0* (see Fig. 1) belongs to $\mathcal{T}_2^0$ and the command input $u(\hat{x}_0)$ is computed on the basis of the healthy model configuration ($\hat{\sigma}=0$). When $u(\hat{x}_0)$ is applied to (1), three situations could arise:

No failures: (Fig. 2 continuous path): the model configuration of (1) is unchanged and therefore the one-step state evolution $x(t+1)$ is driven to $\mathcal{T}_1^0$ thanks to the set-membership requirement: $\text{Proj}_{\hat{x}_0}\{A_0^{aug}x_0^{aug} + B_0^{aug}u + B_{d_0}^{aug}d + E_0^{aug}e_0\} \in \mathcal{T}_1^0$;

Fault 1 occurrence: (Fig. 2 dashed path): the plant (1) assumes the model configuration (4) with $l=1$. Then, $x(t+1) \in \mathcal{T}_1^1$ because of the requirement in (9)

$$\text{Proj}_{\hat{x}_0}\{A_1^{aug}x_0^{aug} + B_1^{aug}u + B_{d_1}^{aug}d + E_1^{aug}e_1\} \in \mathcal{T}_1^1$$

Fault 2 occurrence: (Fig. 2 dotted path): the same reasoning of ii) with $l=2$ and $x(t+1) \in \mathcal{T}_1^2$.

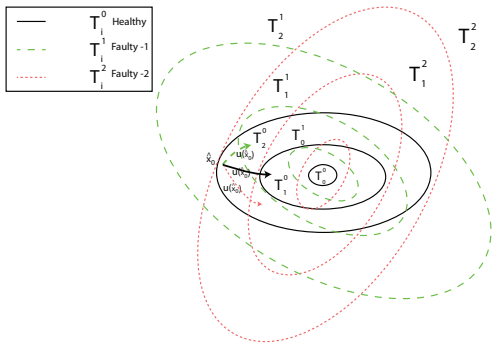

Fig. 2. Healthy-to-faulty transitions

Let us analyze recursions (10) allowing faulty-to-healthy transitions. The following set inclusions hold true by construction

$$\mathcal{T}_i^0 \subset \mathcal{T}_i^j, \forall j=1,\ldots,l, \text{ and } \forall i=0,\ldots,N. \tag{11}$$

Then, if a recovery from the $j-th$ fault configuration occurs, the faulty-to-healthy transition will take place by exploiting the property (11) as follows. The computed command $u(\hat{x}_j)$ will drive the state evolution $x(t+1)$ to $\mathcal{T}_{i-1}^j$ and, because of (11), it is guaranteed that in a finite time $x(t+\bar{t})$, $\bar{t} \geq 1$ will belong to $\mathcal{T}_i^j \cap \mathcal{T}_k^0$ for some $\mathcal{T}_k^0$ and an admissible, though not optimal, command input, say u^H. Such a command for the $j-th$ fault configuration can be computed by referring to the healthy set $\mathcal{T}_k^0$. The plant (1) is under the action of u^H with the consequence that the estimators and the switching logic will be able to retrieve the recovery phase via $\hat{\sigma}(\cdot)$.

Moreover, note that the one-step controllable ellipsoids defined by (9)-(10) are straightforwardly obtained by resorting to the LMI arguments and the projection formula exploited in [1]. Therefore, the pertaining computational complexity grows quadratically with the state and input dimensions.

Remark 1 - The error bound sets $\mathcal{E}_j$, $j=0,1,\ldots,l$, can be characterized by resorting to the arguments in [2]. A possible way to proceed is to compute invariant sets $\mathcal{E}_j$ (ultimate observer error) for (6), i.e. $e_j(0) \in \mathcal{E}_j \rightarrow e_j(t) \in \mathcal{E}_j$. Unfortunately, the condition $e_j(0) \in \mathcal{E}_j$ should be not ensured. Then, by imposing that $e_j(0) \in \mathcal{E}_j^0$, with $\mathcal{E}_j^0$ a region not necessarily invariant, a viable solution is that of computing the smallest invariant set including $\mathcal{E}_j^0$ by propagating the set $\mathcal{E}_j^0$ along the dynamics (6) and by deriving the reachable sets $\mathcal{E}_j^k$ with bounded inputs, see [2]. Because $A-L_jC$ is a stability matrix, in a finite time we have that $\mathcal{E}_j^{\bar{k}} \subset \mathcal{E}_j^0$ and the convex

hull of the union of the set

$$\tilde{\mathcal{E}}_j := conv\left\{\bigcup_{k=0}^{\bar{k}} \mathcal{E}_j^k\right\} \tag{12}$$

is a positively invariant set which provides an over-bound for the error e_j. □

Finally, the above developments prescribe the off-line computation of the gain observer matrices $L_j, j = 0,1,\ldots,l$, the terminal regions $\mathcal{T}_0^j$, $j = 0,1,\ldots,l$, and the corresponding stabilizing state feedback laws K_j, $j = 0,1,\ldots,l$, by considering the augmented system dynamics (8). This can be achieved by using stability arguments for switching systems proposed in [4] and technicalities developed in [6]:

Proposition 1: Given the switching system (4), there exist the triplets $(L_j, \mathcal{T}_0^j, K_j)$, $j = 0,1,\ldots,l$ with $\mathcal{T}_0^j \neq \emptyset$ robustly invariant sets and with each K_j a stabilizing state feedback law for each model configuration of (4) complying with the input constraints (2), if the following requirements in the extended space $x_j^{aug} := [x_j^T \ \hat{x}_j^T]^T$ are satisfied:

$$\left(A_j^{aug}+B_j^{aug}K_j^{aug}\right)\mathcal{T}_0^{aug_j}+B_{d_j}^{aug}\mathcal{D}+E_j^{aug}\tilde{\mathcal{E}}_j \subset \mathcal{T}_0^{aug_j},\ j=1,\ldots,l, \tag{13}$$

$$K_j^{aug}\mathcal{T}_0^{aug_j} \subset \mathcal{U},\ j=1,\ldots,l, \tag{14}$$

$$\left(A_0^{aug}+B_0^{aug}K_0^{aug}\right)\mathcal{T}_0^{aug_0}+B_{d_0}^{aug}\mathcal{D}+E_0^{aug}\tilde{\mathcal{E}}_0 \subset \mathcal{T}_0^{aug_0}, \tag{15}$$

$$\mathcal{T}_0^{aug_0} \subset \mathcal{T}_0^{aug_j} \text{ and } K_j^{aug}\mathcal{T}_0^{aug_j} \subset \mathcal{U},\ j=1,\ldots,l, \tag{16}$$

where $K_j^{aug} = [0 \ \ K_j]$ and $\mathcal{T}_0^j = \text{Proj}_{\hat{x}_j}\mathcal{T}_0^{aug_j}$.
Proof - See [7]. □

C. Healthy-to-Faulty transitions: correctness and admissibility

At each time instant t, the Estimator-based supervisor determines an estimate of the switching signal $\hat{\sigma}(t)$ from which the reconfigured control strategy $u(\hat{x}_{\hat{\sigma}(t)})$ will be computed, see Fig. 1. An important question arises on the correctness of the estimate $\hat{\sigma}(t)$, because this may give rise to an erroneous reconfiguration procedure.

Let $x(t) \in \mathcal{T}_{curr}^0$ be the current healthy state with $curr$ the current set-membership index, by construction at the each time instant t one of the following set-membership events can occur (see Fig. 3):

- **(1)** $\hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_i^{\hat{\sigma}(t)}$ and $\hat{x}_{\hat{\sigma}(t)}(t) \notin \mathcal{T}_i^j, \forall j \neq \hat{\sigma}(t)$ with $i \leq curr$;
- **(2)** $\hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_i^0 \cap \mathcal{T}_i^{\hat{\sigma}(t)} \cap \mathcal{T}_i^{j_1} \cap \mathcal{T}_i^{j_2} \cap \cdots \cap \mathcal{T}_i^{j_q}$, with $j_q \leq l$ and $i \leq curr$;
- **(3)** $\hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_i^{\hat{\sigma}(t)} \cap \mathcal{T}_i^{j_1} \cap \mathcal{T}_i^{j_2} \cap \cdots \cap \mathcal{T}_i^{j_q}$, with $\forall j_k \neq 0$, $j_q \leq l$ and $i \leq curr$.

Note that if **(1)** holds then the switching logic has correctly identified the model configuration because the candidate state estimate $\hat{x}_{\hat{\sigma}(t)}$ belongs only to the ellipsoid $\mathcal{T}_i^{\hat{\sigma}(t)}$ with $i \leq curr$. As a consequence the faulty occurrence is safely detected and $j^* := \hat{\sigma}(t)$.
The event **(2)** refers to the fact that the candidate state estimate $\hat{x}_{\hat{\sigma}(t)}$ belongs to the intersection of more ellipsoidal families including the healthy configuration $\mathcal{T}_i^0$ and the switching to the mode $\hat{\sigma}(t)$ cannot be safely pursued. On the other hand, by construction the inclusion property (11) is always true and the reconfigured control strategy $u(\hat{x}_0)$ obtained by using the healthy configuration ($j^* = 0$) can be still used because it is an admissible, though not optimal, choice.
Finally the scenario **(3)** prescribes that $\hat{x}_{\hat{\sigma}(t)}$ belongs to the intersection of several faulty ellipsoidal families not including the healthy configuration, which ensures unlike **(2)** that a fault is occurring. Also even if in this case the model configuration cannot be changed, nonetheless an admissible reconfigured control law can be achieved by resorting to the following arguments:
-) notice that a generic state $x \in \mathbb{R}^n$ can belong to different faulty ellipsoidal sequences, e.g. $x \in \mathcal{T}_i^{j_1} \cap \mathcal{T}_i^{j_2}$, if the model configurations generating $\{\mathcal{T}_i^{j_1}\}$ and $\{\mathcal{T}_i^{j_2}\}$ are such that

$$B^{j_1} \subset B^{j_2} \text{ or } \textit{viceversa} \tag{17}$$

In fact, by construction (see Fig. 2) a non-empty intersection amongst $\mathcal{T}_i^{j_1}$ and $\mathcal{T}_i^{j_2}$ implies that there exists a common set of healthy actuators such that each admissible command input pertaining to $\mathcal{T}_i^{j_1} \cap \mathcal{T}_i^{j_2}$ is capable to steer $\hat{x}_{\hat{\sigma}(t)}(t+1)$ to $\mathcal{T}_{i-1}^{j_1}$ or to $\mathcal{T}_{i-1}^{j_2}$ when the $j_1 - th$ or the $j_2 - th$ mode respectively occurs;
-) when the event **(3)** occurs the admissible reconfigured control strategy $u(\hat{x}_{j^F}), j^F \in \{\hat{\sigma}(t), j_1, j_2, \ldots, j_q\}$, $j_q \leq l$, is selected by satisfying the following input map inclusion

$$B^j \subseteq B^{j^F},\ \forall j \in \{\hat{\sigma}(t), j_1, j_2, \ldots, j_q\},\ j_q \leq l. \tag{18}$$

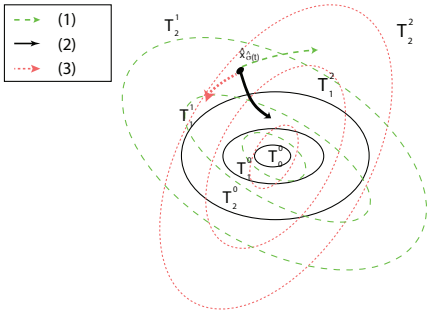

Fig. 3. Switching signal estimate: the set-membership events

Remark 2 - The following event occurrence

$$\hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_i^{\tilde{j}}, \tilde{j} \neq \hat{\sigma}(t), \text{ with } i \leq curr$$

may happen and the use of $\hat{\sigma}(t)$ may give rise to wrong decisions. In this case, the reconfigured control action is computed as in **(3)**, because the scenario is the same except for the set-membership to $\mathcal{T}_i^{\hat{\sigma}(t)}$. □

IV. The FTC Algorithm

We will provide an FTC Receding Horizon Control algorithm by using the previous arguments.

AFTC-RHC-Algorithm

Off-line:

1: Compute the invariant regions $\tilde{\mathcal{E}}_j$, the observer gains L_j, the robust invariant ellipsoids $\mathcal{T}_0^j \subset \mathbb{R}^n$ and the stabilizing state feedback gains $K_j,\ j = 0, 1, \ldots, l$;
2: Generate the sequences of N one-step controllable sets $\mathcal{T}_i^j,\ j = 1, \ldots, l$ via the recursions (9)-(10);
3: Store the ellipsoids $\{\mathcal{T}_i^j\}_{i=0}^N$, $j = 0, 1, \ldots, l$.
4: $t \leftarrow 0$

On-line:
5: $\hat{\sigma}(t) \leftarrow \min_i\ \pi_i(t)$
6: $i(t) \leftarrow \min\{i : \hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_i^{\hat{\sigma}(t)}\}$
7: **if** $\hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_{i(t)}^{\hat{\sigma}(t)}$ and $\hat{x}_{\hat{\sigma}(t)}(t) \notin \mathcal{T}_{i(t)}^j,\ \forall j \neq \hat{\sigma}(t)$ **then**
8: $\quad j^*(t) \leftarrow \hat{\sigma}(t)$;
9: **end if**
10: **if** $\hat{x}_{\hat{\sigma}(t)}(t) \in \left(\mathcal{T}_{i(t)}^0 \cap \mathcal{T}_{i(t)}^{\hat{\sigma}(t)}\right) \cap \bigcap_q \mathcal{T}_{i(t)}^{j_q}$ **then**
11: $\quad j^*(t) \leftarrow 0$;
12: **else** $\quad \triangleright\ \hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_{i(t)}^{\hat{\sigma}(t)} \cap \bigcap_q \mathcal{T}_{i(t)}^{j_q}$
13: $\quad j^*(t) \leftarrow j^F$ $\quad \triangleright\ j^F$ satisfies (18)
14: **end if**
15: **if** $j^*(t) = 0$ **then**
16: $\quad$ **if** $i(t) = 0$ **then**
17: $\quad\quad u(t) \leftarrow K_0\, \hat{x}_{\hat{\sigma}(t)}(t)$
18: $\quad$ **else**
19: $$u(t) \leftarrow \arg\min J_{i(t)}(\hat{x}_{\hat{\sigma}(t)}(t), u) \quad (19)$$
$$\text{s.t. } A\hat{x}_{\hat{\sigma}(t)}(t) + B^{j^*} u \in \mathcal{T}_{i(t)-1}^{j^*(t)},\ u \in \mathcal{U}; \quad (20)$$
20: $\quad$ **end if**
21: **else**
22: $\quad$ **if** there exists k such that $\hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_{i(t)}^{j^*(t)} \cap \mathcal{T}_k^0$ **then**
23: $\quad\quad$ **if** $k = 0$ **then**
24: $\quad\quad\quad u(t) \leftarrow K_0\, \hat{x}_{\hat{\sigma}(t)}(t)$
25: $\quad\quad$ **else**
26: $\quad\quad\quad$ solve (19)-(20)
27: $\quad\quad$ **end if**
28: $\quad$ **end if**
29: **end if**
30: **Apply** $u(t)$ to the plant (1);
31: $t \leftarrow t + 1$; goto 5

Observe that the running cost $J_{i(t)}(\hat{x}_{\hat{\sigma}(t)}(t), u)$ is chosen without loss of generality as follows:

$$J_{i(t)}(\hat{x}_{j^*}(t), u) = \|A\hat{x}_{\hat{\sigma}(t)}(t) + B^{j^*(t)}u\|^2_{P_{i(t)-1}^{j^*(t)}} \quad (21)$$

with $P_{i(t)-1}^{j^*(t)} > 0$ the shaping matrix of $\mathcal{T}_{i(t)-1}^{j^*(t)}$.

Proposition 2: Let the sequences of sets $\mathcal{T}_i^j$ be non-empty and $x(0) \in \bigcup_{j=0}^{l} \mathcal{T}_N^j$. Then, the **AFTC-RHC** algorithm satisfies the prescriptions of the **AFTC** problem by ensuring constraints fulfilment and closed-loop asymptotic stability.

Proof - The existence of a solutions at time t implies existence of the solution at time $t + 1$, because the optimizations in steps 19 and 26 are always feasible. First, let us consider that at the generic instant t the estimate state $\hat{x}_0(t) \in \mathcal{T}_{i(t)}^0$ (Healthy condition). Then, by construction of (9) there exists an input vector u satisfying the input constraints (2) such that the one-step state evolution $A\hat{x}_0(t) + Bu$ belongs to $\mathcal{T}_{i(t)-1}^0$. If a $j-th$ fault occurs, by construction of the sequence $\mathcal{T}_i^0$ the state evolution $A\hat{x}_0(t) + Bu$ will belong to $\mathcal{T}_{i(t)-1}^j$ so that the viability property is preserved. This means that a transition healthy-to-faulty occurs and the plant dynamics is characterized by $j-th$ model configuration of (4). Conversely if $\hat{x}_j(t) \in \mathcal{T}_{i(t)}^j$ (Faulty condition), recursions (10) guarantee the existence of a command vector u such that $A\hat{x}_j(t) + Bu \in \mathcal{T}_{i(t)-1}^j$ or to $\mathcal{T}_{i(t)-1}^0$ (Faulty-to-Healthy transition). Therefore, at $t + 1$, the existence of a solution $u(t+1)$ for the steps 19 and 26 is ensured and the asymptotic stability achieved. □

V. Illustrative example

We present results on the effectiveness of the proposed **AFTC-RHC** strategy and make comparisons with the FTC scheme of [15] both in terms of fault detectability capabilities and control performance.

We focus our attention on the two-tanks water system discussed in [13]. Specifically, two tanks with levels h_1 and h_2 are interconnected through lower and upper valves, u_L and u_U , and the first tank is filled via a pump input command u_P. By defining the state $x = [h_1\ h_2]^T$ and the input vector $u = [u_P\ u_L\ u_U]^T$, the linearized model is described by the following matrices:

$$A = \begin{bmatrix} 0.9931 & 0.0035 \\ .0068 & 0.9823 \end{bmatrix}, B = \begin{bmatrix} 0.0081 & -0.0032 & -0.0034 \\ 0.000 & 0.0032 & 0.0034 \end{bmatrix}$$

$$B_d = -\begin{bmatrix} 0.9966 \\ 0.0034 \end{bmatrix} \cdot 10^{-3}$$

Moreover a leak d belonging to the set $\mathcal{D} := \{d : |d| \leq 10^{-3}\}$ acts on the first tank and the following component-wise constraints on the input vector u are prescribed $|u_P| \leq 1$, $|u_L| \leq 1$, $|u_U| \leq 1$. We consider faults on the two valves that according to (4) are identified together with the healthy condition by the following input maps:

$$B^0 = \begin{bmatrix} 0.0081 & -0.0032 & -0.0034 \\ 0.000 & 0.0032 & 0.0034 \end{bmatrix},$$
$$B^1 = \begin{bmatrix} 0.0081 & 0 & -0.0034 \\ 0.000 & 0 & 0.0034 \end{bmatrix}, B^2 = \begin{bmatrix} 0.0081 & -0.0032 & 0 \\ 0.000 & 0.0032 & 0 \end{bmatrix}$$

The estimator and terminal state-feedback gains have been computed by solving the BMI optimization problem resulting from *Proposition 1* and following the technicalities of [6]. For each (healthy and faulty) configuration, a family of 10 ellipsoids has been computed. The control problem is to track constant set-points on the two tank levels starting from the initial condition $x(0) = [0.4\ 0.06]^T$ and under the following fault occurrences:

Fault scenario - *At $t = 220\,sec.$ and at $t = 710\,sec.$ faults on the lower valve and on the upper valve respectively occur. At $t = 450\,sec.$ a recovery phase from the lower valve malfunctioning is prescribed.*

The FTC algorithm of [15] has been implemented by using an horizon length $N_c = 5$. All the numerical results are summarized in the next Figs. 4-6. First, the proposed **AFTC-RHC** scheme is capable to ensure good tracking capabilities despite of any fault events, see Fig. 4, while the competitor

MPC strategy (dot-dashed line) presents remarkable discrepancies from the set-points when both faults occur. Similarly comments are pertinent for the input behaviours, see Fig. 5, where it is also important to underline that at $t = 450\,sec.$ the recovery from the lower valve fault (see $u_L(\cdot)$) is not detected by the scheme developed in [15] and its action is the same of that corresponding to the faulty condition. The latter explicitly results in Fig. 6 where the upper graph depicts the *effective* switching signal $\sigma(\cdot)$ compared with both the estimates $j^*(\cdot)$ resulting from the Switching logic module (see Fig. 1) and from [15]. There, it is interesting to note that dwell-times are not necessary:

- Healthy-to-Faulty transition at $t = 220\,sec$: $\hat{x}_1(220) \in \mathcal{T}_5^1$, $\hat{x}_1(220) \notin \mathcal{T}_5^0$ and $\hat{x}_1(220) \notin \mathcal{T}_5^2$;
- Faulty-to-Healthy transition at $t = 450\,sec$: $\hat{x}_0(450) \in \mathcal{T}_0^1 \cap \mathcal{T}_8^0$;
- Healthy-to-Faulty transition at $t = 710\,sec$: $\hat{x}_2(710) \in \mathcal{T}_4^2$, $\hat{x}_2(710) \notin \mathcal{T}_4^0$ and $\hat{x}_2(710) \notin \mathcal{T}_4^1$.

Numerical burdens confirms the improvement provided by the proposed scheme: **Off-line phase** (overall CPU time): $78.5\,sec.$ (**AFTC-RH**) $1962.54\,sec.$ ([15]); **On-line phase** (average CPU time/step): $0.08\,sec.$ (**AFTC-RH**) $0.32\,sec.$ ([15]).

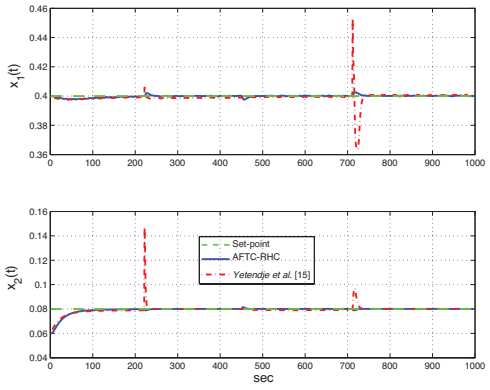

Fig. 4. State evolution

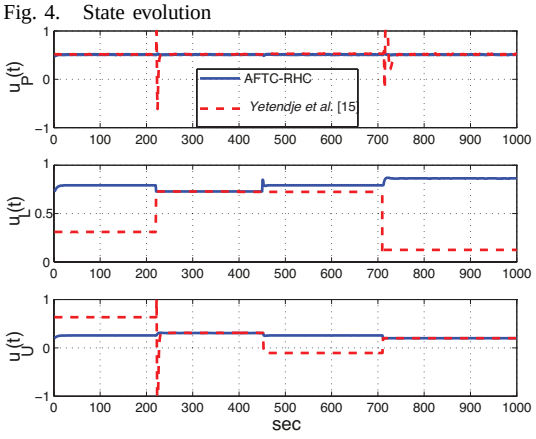

Fig. 5. Command input signals

VI. Conclusions

In this paper, a novel fault tolerant reconfiguration strategy for linear discrete-time systems subject to input saturations and actuator fault occurrences has been proposed. The key idea was to develop a framework based on set-invariance concepts

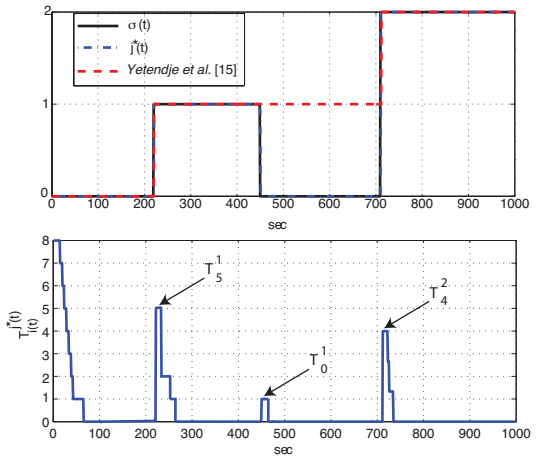

Fig. 6. Switching signals

to properly manage actuator fault occurrences. Comparisons with a recent MPC-based FTC solution have proved that the proposed approach favourably compares both in terms of achievable performance and computational efforts.

References

[1] D. Angeli, A. Casavola, G. Franzè and E. Mosca, "An Ellipsoidal Off-line MPC Scheme for Uncertain Polytopic Discrete-time Systems", *Automatica*, Vol. 44, pp. 3113–3119, 2008.

[2] F. Blanchini and S. Miani, "Set-Theoretic Methods in Control", *Birkäuser*, Boston, 2008.

[3] M. Blanke, M. Kinnaert, J. Schröder and J. Lunze, "Diagnosis and Fault Tolerant Control", *Springer Verlag*, 2006.

[4] J. Daafouz, P. Riedinger and C. Iung, "Stability analysis and control synthesis for switched systems: a switched Lyapunov function approach", *IEEE Trans. Aut. Contr.*, Vol. 47, No. 11, pp. 1883-1887, 2002.

[5] D. Efimov, J. Cieslak and D. Henry, "Supervisory fault-tolerant control with mutual performance optimization", *Int. J. of Adap. Contr. and Sign. Proc.*, DOI: 10.1002/acs.2296, 2013.

[6] D. Famularo and G. Franzè, "Output Feedback Model Predictive Control of Uncertain Norm-Bounded Linear Systems", *International Journal of Robust and Nonlinear Control*, Vol. 21, No. 8, pp. 838-862, 2011.

[7] G. Franzè, F. Tedesco and D. Famularo, "An actuator fault tolerant control strategy", *DIMES-UNICAL, Technical Report*, DIMES-12/04, *http://tedescof.files.wordpress.com/2013/12/tech-ftc.pdf*, 2013.

[8] J.P. Hespanha and A.S. Morse, "Certainty equivalence implies detectability", *Systems & Control Letters*, pp. 1-13, 1999.

[9] T. Hu, A. Teel, and L. Zaccarian, "Stability and performances for saturated systems via quadratic and nonquadratic lyapunov functions", *IEEE Trans. Aut. Contr.*, Vol.51, No. 11, pp. 1770–1786, 2006.

[10] L. Lao, M. Ellis and P. D. Christofides, "Proactive Fault-Tolerant Model Predictive Control", *AIChE Journal*, Vol. 59, No. 8, pp. 2810–2820, 2013.

[11] B. Milani, "Piecewise-affine Lyapunov functions for discrete-time linear systems with saturating controls", *Automatica*, Vol. 38, No. 12, pp. 2177–2184, 2002.

[12] A.S. Morse, "Supervisory control of families of linear set-point controllers, Part 1: exact matching", *IEEE Trans. Aut. Contr.*, pp. 1413-1431, 1996.

[13] J.H. Richter and J. Lunze, "H_∞-based virtual actuator synthesis for optimal trajectory recovery", *In 7th IFAC Safeprocess09*, pp. 1587-1592, Barcelona, Spain, 2009.

[14] M. M. Seron, J. A. De Dona and S. Olaru, "Fault tolerant control allowing sensor healthy-to-faulty and faulty-to-healthy transitions", *IEEE Trans. Aut. Contr.*, Vol. 57 , No. 7, pp. 1657–1669, 2012.

[15] A. Yetendje, M.M. Seron and J.A. De Doná, "Robust multiactuator fault-tolerant MPC design for constrained systems", *International Journal of Robust and Nonlinear Control*, Vol. 23, No. 16 pp. 1828–1845, 2013.

[16] Y. Zhang and J. Jiang, "Bibliographical review on reconfigurable fault-tolerant control systems", *Annual Reviews in Control*, Vol. 32, pp. 229–252, 2008.