2015 IEEE 54th Annual Conference on Decision and Control (CDC)
December 15-18, 2015. Osaka, Japan

Multiple stuck positions actuator faults: a model predictive based reconfigurable control scheme

Domenico Famularo, Giuseppe Franzè and Walter Lucia
DIMES - Università della Calabria
Rende (CS), 87036, ITALY
{domenico.famularo,giuseppe.franze,walter.lucia}@unical.it

Abstract— **This paper presents a Fault Tolerant Control scheme for constrained discrete time linear systems against stuck actuators and bounded disturbances. The results here proposed are a significant generalization of a similar algorithm which has been designed only to manage healthy/out-of-service in the actuator units. A first key feature is the capability to exploit existing methods based on polyhedral algebra and computational geometry in order to characterize the reconfiguration logic of the proposed fault tolerant architecture. This is achieved by defining a set of a finite number of piecewise affine systems capable to cover all of the admissible faulty stuck scenario. It is then proved that one-step sequences of controllable sets can be formally defined within a piecewise affine system paradigm under the key property that each region is a polygon.**

I. Introduction

Current technological advances tend towards more demanding performance requirements to design more complex and sophisticated regulation/tracking control units for physical plants. Faults (unknown actuator/sensor malfunctioning or component impairments) are undesired, often fatal phenomena occurring in any complex system. In most practical safety-critical applications, flight control systems as an example, this fault tolerance aspect is crucial, see e.g. [16] and references therein. A 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, see [1], [5].

Along these lines, an extremely interesting fault scenario is represented by stuck actuators prescribing that, once occurred, the affected actuators can no longer respond to the control inputs and have fixed constant outputs. Although studied from different perspectives, the related FTC problem is currently considered hard to be approached mainly because the structure of the original system could substantially change according to the nature of this class of fault occurrences, see the following relevant contributions [9], [3], [15], [14] and [13].

Moving from these considerations, a more general FTC scheme for constrained systems subject to unpredictable stuck events on the actuation units is proposed. The starting idea is of resorting to the low demanding Model Predictive Control (MPC)-based FTC framework, recently proposed in [8], for linear time invariant systems whose failure actuator occurrences are described by means of a switching system paradigm and the reconfigured control action is obtained via set-theoretic arguments. To this end, two aspects need to be carefully taken into consideration: the hybrid system paradigm and one-step ahead controllable regions.

As the first question is concerned, the idea here pursued is to describe the stuck actuator occurrences by exploit the affine structure deriving from these faults in order to artificially built-up a set of piecewise affine (PWA) systems. Specifically by fixing the attention to a sequence of l stuck values each one related to a single actuator, a switching affine system description consisting of $l+1$ modes including also the healthy mode comes out. Then, the union of the robust positively invariant regions pertaining to $l+1$ system configurations is partitioned so that an adequate polyhedral cover is achieved and used as the domain of the function describing the switching affine system. As a consequence, a well-posed PWA description results.

Based on these developments, the second issue leads to provide a novel one-step controllable set characterization that allows to explicitly exploit the algebra arguments presented in [11] for the computation of such sets by means of polyhedral algebra concepts.

To prove the benefits of the proposed approach, numerical simulations dealing with the attitude control problem of a light utility aircraft are provided.

Notations and preliminaries

Definition 1: A polyhedron is the intersection of a finite number of closed and/or open half-spaces. A polygon is the union of a finite number of polyhedra.

Definition 2: A family of sets $\mathcal{P} := \{\mathcal{P}_r \,|\, r \in \mathcal{R}\}$ is a closed polyhedral cover of a closed polygon $\mathcal{X} \subset \mathbb{R}^n$ if the index set $\mathcal{R}$ is finite and $\mathcal{X} = \bigcup_{r\in\mathcal{R}} \mathcal{P}_r$.

Definition 3: A function $f : \mathcal{X} \to \mathbb{R}^n$ is piecewise affine on the polyhedral cover $\mathcal{P}$ of the polygon $\mathcal{X}$ if the restriction $f|_{\mathcal{P}_r} : \mathcal{X} \to \mathbb{R}^n$ is affine for all $r \in \mathcal{R}$.

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 $\text{Proj}_X(S) := \{x \in X \,|\, \exists y \in Y \text{ s.t. } (x, y) \in S\}$.

II. PROBLEM FORMULATION

In this paper, we consider plants described by the following linear discrete-time model

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

where $x(t) \in \mathbb{R}^n$ denotes the state, $u(t) \in \mathbb{R}^m$ the input, $d(t) \in \mathbb{R}^d$ an exogenous plant disturbance and $y(t) \in \mathbb{R}^p$ the output. 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, (1) is subject to the following set-membership state and input constraints

$$u(t) \in \mathcal{U},\ \forall t \geq 0,\ x(t) \in \mathcal{X},\ \forall t \geq 0, \quad (2)$$

with $\mathcal{X}$ and $\mathcal{U}$ compact subsets of $\mathbb{R}^n$ and $\mathbb{R}^m$, respectively.

The *Robustly Positively Invariance* and *Set precedessor* definitions will be instrumental throughout the paper and are here provided:

Definition 4: A set $\Xi \subseteq \mathcal{X}$ is Robustly Positively Invariant (RPI) for (1) if there exists a control law $u(t) \in \mathcal{U}$ such that once the closed-loop solution $x_{CL}(t)$ enters inside that set at any given time t_0, it remains in it for all future instants, i.e. $x_{CL}(t_0) \in \Xi \rightarrow x_{CL}(t) \in \Xi, \forall d(t) \in \mathcal{D}, \forall t \geq t_0$. □

Definition 5: Given a set $\Xi \subseteq \mathcal{X}$, the predecessor set $Pre\,(\Xi)$, is the set of states for which there exists a causal control $u(t) \in \mathcal{U}$ such that $\forall d \in \mathcal{D}$ the one-step state evolution is in Ξ, i.e.

$$Pre\,(\Xi) := \{x \in \mathcal{X} : \exists u \in \mathcal{U} : Ax + Bu + B_d d \in \Xi, \forall d \in \mathcal{D}\}$$

Then, let Ξ be a target set it is possible to determine the sets of states i-step controllable to Ξ via the following recursion (see [2]):

$$\Xi_0 := \Xi, \quad \Xi_i := Pre\,(\Xi_{i-1}) \quad (3)$$

Moreover, we shall refer to the class of the stuck actuator faults that can modelled as follows:

Definition 6: A stuck fault on the $i-th$ actuator of the plant model (1) is defined as an instantaneous change on the input map B such that a blockage occurs on the $i-th$ actuation channel, i.e.

$$Bu(t) \leftarrow B^i u(t) + F^i \bar{u}_F^{ij}, \quad (4)$$

where

$$\begin{aligned} B^i &:= B \cdot \text{diag}([1 \ldots 1, \overbrace{0}^{i-th} 1 \ldots 1]), \\ F^i &:= B \cdot \text{diag}([0 \ldots 0, \overbrace{1}^{i-th} 0 \ldots 0]) \end{aligned}$$

and $\bar{u}_F^{ij} \in \mathcal{U}_F^i \subset \mathbb{R}$, being $\mathcal{U}_F^i$ a set of a finite number of blockage positions. □

Then, the plant dynamics due to a generic $i-th$ stuck actuator fault occurrence can be described as follows:

$$x(t+1) = Ax(t) + B^i u(t) + B_d d(t) + F^i \bar{u}_F^{ij},\ \forall \bar{u}_F^{ij} \in \mathcal{U}_F^i \quad (5)$$

The meaning of (5) is that if an actuator is blocked at any position $\bar{u}_F^{ij} \in \mathcal{U}_F^i$, then the plant is driven by the remaining healthy devices whose the input map B^i is associated. Let $f^i := card\left(\mathcal{U}_F^i\right)$ the cardinality of the sets $\mathcal{U}_F^i$, $i \in \mathcal{I} := \{0, 1, \ldots, l\}$, then all the admissible fault events can be abstractly collected into a switching affine system that consists of a finite number of subsystems (5):

$$\Sigma_\sigma : \begin{cases} x(t+1) = Ax(t) + B^i u(t) + B_d d(t) + F^i \bar{u}_F^{ij}, \\ \quad\; y(t) = Cx(t), \\ \qquad\quad i \in \mathcal{I}, \\ \qquad\quad j \in \mathcal{J} := \{1, \ldots, f^i\}, \end{cases} \quad (6)$$

where $B^0 \equiv B$ and $\mathcal{U}_F^0 \equiv \emptyset$ describes the healthy condition. Notice that the rule that orchestrates the switching between these subsystems generates a switching signal $\sigma : \mathbb{Z}_+ \rightarrow \mathcal{I} \times \mathcal{J}$, while the resulting pair index $(i, j) = \sigma(t)$ is known as the active mode at the time instant t.

Then, the following control reconfiguration problem will be taken under consideration:

Stuck Actuator Fault Tolerant Control (SAFTC) Problem - *Given the plant (1), at each time instant t design an FTC strategy consisting of an estimation actuator fault module capable to individuate the actual active mode $(i(t), j(t))$ of the affine switching system (6) and a control reconfiguration algorithm such that the feedback plant (1) is asymptotically stable and satisfies state and input constraints regardless of any disturbance occurrence.* □

In the sequel, the **SAFTC** Problem is addressed by adapting the ellipsoidal set-theoretic approach presented in [8] to the system family (6), see the basic scheme of Fig. 1. Specifically, three interconnected units are designed to derive an FTC scheme based on the one-step controllable set concept: a bank of $1 + \sum_{i=1}^{l} f^i$ observers each one tuned with respect to the $(i, j) - th$ system mode (healthy and faulty configurations), a *certainty equivalence* switching logic whose output $\hat{\sigma}(\cdot)$ is an estimate of the switching signal $\sigma(\cdot)$ and a reconfiguration algorithm for computing the more adequate control action $u(\hat{x}_{\hat{\sigma}(\cdot)})$ compatible with the state estimate $\hat{x}_{\hat{\sigma}(\cdot)}$.

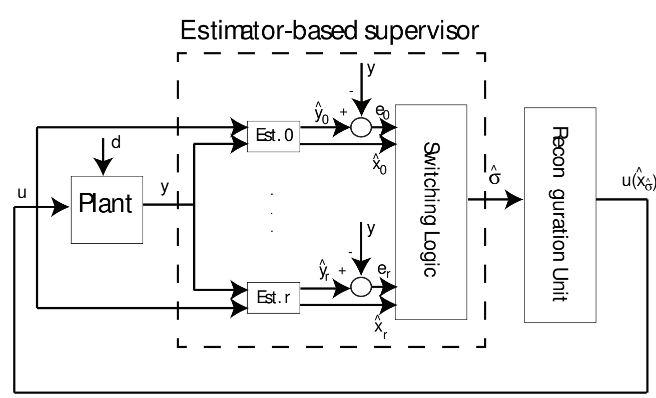

Fig. 1. The FTC architecture

III. A STUCK ACTUATOR ORIENTED FTC ARCHITECTURE

In this section, the three modules of the basic FTC approach of [8] will be properly described in order to comply with the model description (6). First, note that the structure of the *Estimator-based supervisor* essentially remain the same: in fact again this element is in charge to select the *current working mode* according to the *certainty equivalence* principle [10] that allows to discriminate amongst all the system configurations of (6) by evaluating $\hat{\sigma}(\cdot)$ as the smallest output error norm. Specifically, the ingredients of the supervisor are:

Luenberger state observers - A bank of state estimators:

$$\begin{aligned} \hat{x}_{ij}(t+1) = &\ A\hat{x}_{ij}(t) + B^i u(t) + F^i \bar{u}_F^{ij} + \\ &\ L_{ij}(y(t) - \hat{y}_{ij}(t)) \\ \hat{y}_{ij}(t) = &\ C\hat{x}_{ij}(t), i = 0, 1, \ldots, l,\ j = 1, \ldots, f_i, \end{aligned} \tag{7}$$

where the gains $L_{ij} \in \mathbb{R}^{n \times p}$, $i = 0, 1, \ldots, l, j = 1, \ldots, f_i$, are such that $(A - L_{ij}C)$ are Schur matrices, and with the error $e_{ij}(t) := x(t) - \hat{x}_{ij}(t)$ governed by the following equations

$$\begin{aligned} e_{ij}(t+1) = &\ (A - L_{ij}C)e_{ij}(t) + (B - B^i)u(t) + \\ &\ B_d d(t) - F^i \bar{u}_F^{ij}, \\ e_{y_{ij}}(t) := &\ y(t) - \hat{y}_{ij}(t), i = 0, \ldots, l,\ j = 1, \ldots, f_i. \end{aligned} \tag{8}$$

Note that for the sake of notational congruence, we assume that also the healthy mode is double indexed, i.e. when $i = 0$ implies that $j = 0$.

From a computational point of view, the matrices L_{ij} are designed by mitigating the effects due to the exogenous disturbance $d(t)$ and the model mismatch arising both from the input map $B - B^i$ and the stuck occurrence $F^i \bar{u}_F^j$;

Switching logic - At each time instant t the active mode of (6) is identified by using the output estimation errors $e_{y_{ij}}(t)$. In virtue of the *certainty equivalence principle* and by denoting with $\pi_{ij} := \|e_{y_{ij}}\|,\ i = 0, 1, \ldots, l, j = 1, \ldots, f_i$, 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_{ij} :

$$\hat{\sigma}(t) := \arg \min_{i \in \mathcal{I},\, j \in \mathcal{J}} \pi_{ij}(t) \tag{9}$$

A. Reconfiguration algorithm

Differently from the developments of [8], the occurrence of stuck events pose some questions that could prevent their application within the present context:

- As pointed out in (8), each stuck position gives rise to a further model uncertainty whose processing could require to interpret it as an additional disturbance: if it be so, the region of attraction deriving from the computed one-step controllable family for each model configuration (6) should be significantly conservative;
- For each $i - th$ actuation channel several stuck events (cardinality of $\mathcal{U}_F^i$) can occur, therefore if the inner ellipsoidal approximations exploited in [8] were used for computing one-step controllable sets, very poor control performance will result.

A way to overcome these difficulties is to resort to the methodology presented in [11] where a computational framework for the computation of predecessor sets based on piecewise affine plant descriptions and on the polyhedral cover concept is provided.

Hence, the following arguments are exploited to both fit FTC prescriptions and the piecewise affine framework. First, the computation of the one-step controllable sequences $\{\mathcal{T}_k^{ij}\}_{k=0}^N$, $i = 0, 1, \ldots, l, j = 1, \ldots, f^i$, has to be performed by using the augmented state space $x_{ij}^{aug} := [x_{ij}^T\ \hat{x}_{ij}^T]^T$, with x_{ij} a state variable accounting for the $(i, j) - th$ dynamical evolution of (6):

$$\begin{aligned} x_{ij}^{aug}(t+1) = &\ A_i^{aug} x_{ij}^{aug}(t) + B_i^{aug} u(t) + B_{d_i}^{aug} d(t) + \\ &\ E_{ij}^{aug} e_{ij}(t) + F_i^{aug} \bar{u}_F^{ij} \end{aligned} \tag{10}$$

where

$$A_i^{aug} = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix},\ B_i^{aug} = \begin{bmatrix} B^i \\ B^i \end{bmatrix},$$

$$B_{d_i}^{aug} = \begin{bmatrix} B_d \\ 0 \end{bmatrix}, F_i^{aug} = \begin{bmatrix} F^i \\ F^i \end{bmatrix}, E_{ij}^{aug} = \begin{bmatrix} 0 \\ L_{ij}C \end{bmatrix}$$

This becomes necessary in order to ensure that the state estimate $\hat{x}_{ij}$ effectively belongs to the computed $\mathcal{T}_k^{ij}$.

Then, the augmented model (10) can be recast as piecewise affine systems on polyhedral covers as prescribed in [11].

Let $\mathcal{E}^{ij}$, $i = 0, 1, \ldots, l, j = 1, \ldots, f^i$ be the error bound sets for (8) that can be determined as follows (see [2]):

- Choose a region $\mathcal{E}_0^{ij}$, not necessarily invariant, such that $e_{ij}(0) \in \mathcal{E}_0^{ij}$;
- Compute the smallest invariant set including $\mathcal{E}_0^{ij}$ by propagating the set $\mathcal{E}_0^{ij}$ along the dynamics (8) and by deriving the reachable sets $\mathcal{E}_k^{ij}$ with bounded inputs;
- Since $A - L_{ij}C$ is a stability matrix, in a finite time it is guaranteed that $\mathcal{E}_{\bar{k}}^{ij} \subset \mathcal{E}_0^{ij}$ and the convex hull of the union of the set
$$\tilde{\mathcal{E}}^{ij} := conv \left\{ \bigcup_{k=0}^{\bar{k}} \mathcal{E}_k^{ij} \right\} \tag{11}$$
is a positively invariant set which provides an overbound for the error e_{ij}.

Then, the triplets consisting of gain observer matrices L_{ij}, $i = 0, 1, \ldots, l, j = 1, \ldots, f^i$, terminal regions $\mathcal{T}_0^{ij}$, $i = 0, 1, \ldots, l, j = 1, \ldots, f^i$, and corresponding stabilizing state feedback laws K_{ij}, $i = 0, 1, \ldots, l, j = 1, \ldots, f^i$, are achieved as follows:

Proposition 1: Given the switching system (6), there exist the triplets $(L_{ij}, \mathcal{T}_0^{ij}, K_{ij})$, $i = 0, 1, \ldots, l, j = 1, \ldots, f^i$, with $\mathcal{T}_0^{ij} \neq \emptyset$ robust positively invariant (RPI) sets and with each K_{ij} a stabilizing state feedback law for each model configuration of (6) complying with the constraints (2), if the following requirements in the extended space $x_{ij}^{aug} := [x_{ij}^T\ \hat{x}_{ij}^T]^T$ are satisfied:

$$\begin{aligned} &(A_i^{aug} + B_i^{aug} K_{ij}^{aug}) \mathcal{T}_0^{aug_{ij}} + B_{d_i}^{aug} \mathcal{D} + E_{ij}^{aug} \tilde{\mathcal{E}}^{ij} + F_i^{aug} \bar{u}_F^{ij} \\ &\subset \mathcal{T}_0^{aug_{ij}} \subseteq \mathcal{X}^{aug}, i = 1, \ldots, l, j = 1, \ldots, f^i, \end{aligned} \tag{12}$$

$$K_{ij}^{aug} \mathcal{T}_0^{aug_{ij}} \subset \mathcal{U}, i = 1, \ldots, l, j = 1, \ldots, f^i, \tag{13}$$

$$\begin{aligned} &(A_0^{aug} + B_0^{aug} K_{00}^{aug}) \mathcal{T}_0^{aug_{00}} + B_{d_0}^{aug} \mathcal{D} + E_{00}^{aug} \tilde{\mathcal{E}}^{00} \\ &\subset \mathcal{T}_0^{aug_{00}} \subseteq \mathcal{X}^{aug}, \end{aligned} \tag{14}$$

$$\mathcal{T}_0^{aug_{00}} \subset \mathcal{T}_0^{aug_{ij}} \text{ and } K_{00}^{aug}\mathcal{T}_0^{aug_{00}} \subset \mathcal{U}, \quad i=0,1,\dots,l, j=1,\dots,f^i, \tag{15}$$

where $\mathcal{X}^{aug} := \mathcal{X} \times \mathcal{X}$, $K_{ij}^{aug} = [0 \ K_{ij}]$ and $\mathcal{T}_0^{ij} = \text{Proj}_{\hat{x}_{ij}} \mathcal{T}_0^{aug_{ij}} \subseteq \mathcal{X}$.

Proof - The proof is standard and follows by exploiting *S-procedure* technicalities as proposed in [6] and stability arguments for switching systems as provided in [4]. □

By defining an admissible stuck actuator configuration as a $l-$tupla of indices, i.e. $seq\_stuck := (j_1, j_2, \dots, j_l)$, with $seq\_stuck(0) \equiv 0$, associated to constant actuator positions $\bar{u}_F^{i,j_i} \in \mathcal{U}_F^i$, we can refer to the model (10) under the restriction imposed by seq_stuck :

$$x_{i,seq\_stuck(i)}^{aug}(t+1) = A_i^{aug} x_{i,seq\_stuck(i)}^{aug}(t) + B_i^{aug}u(t) + E_{i,seq\_stuck(i)}^{aug} e_{i,seq\_stuck(i)}(t) + B_{d_i}^{aug}d(t) + F_i^{aug}\bar{u}_F^{i,seq\_stuck(i)} \tag{16}$$

that can be viewed as a piecewise affine system on a polyhedral cover according to *Definition* 3. In fact given the family of RPI regions $\mathcal{T}_0^{i\,seq\_stuck(i)}$ of the $l+1$ subsystems (16), it is always possible to determine the polyhedral cover of the inner polygonal approximation of $\bigcup_{i=0}^{l} \mathcal{T}_0^{aug_{i,seq\_stuck(i)}}$ hereafter named as $\mathcal{P}^{\mathcal{X}^{seq\_stuck}}$. Hence, we have that

$$\begin{aligned} & g^{seq\_stuck}(x_{(\cdot),seq\_stuck}^{aug}, u, d, e_{(\cdot),seq\_stuck}) := \\ & A_i^{aug} x_{i,seq\_stuck(i)}^{aug}(t) + B_i^{aug}u(t) + \\ & E_{i,seq\_stuck(i)}^{aug} e_{i,seq\_stuck(i)}(t) + \\ & B_{d_i}^{aug}d(t) + F_i^{aug}\bar{u}_F^{i,seq\_stuck(i)}, \\ & \forall (x_{i,seq\_stuck(i)}^{aug}, u, d, e_{i,seq\_stuck(i)}) \in \mathcal{P}_i^{\mathcal{X}^{seq\_stuck}}, \\ & i \in \mathcal{R}^{\mathcal{X}^{seq\_stuck}}, \end{aligned} \tag{17}$$

is a piecewise affine system description on the polyhedral cover $\mathcal{P}^{\mathcal{X}^{seq\_stuck}}$. The same reasoning applies for all the admissible stuck actuator configurations.

According to the piecewise model description (16), we would determine families of one-step controllable sequences $\{\mathcal{T}_k^{ij}\}_{k=0}^N$, $i = 0, 1, \dots, l$, $j = 1, \dots, f^i$, such that if the application of the current command $u(\hat{x}_{ij})(t)$, computed w.r.t. the active mode $(i(t), j(t))$, jointly occurs with a fault/recovery event, does not give rise to a one-step state evolution $x(t+1)$ outside the region $\bigcup_{i=0}^{l} \bigcup_{j=1}^{f^i} \bigcup_{k=0}^{N} \mathcal{T}_k^{ij}$.

All the above developments lead to the main result:

Theorem 1: Let seq_stuck and $\mathcal{P}^{\mathcal{X}^{seq\_stuck}}$ be an admissible stuck actuator configuration and the polyhedral cover of $\bigcup_{i=0}^{l} \mathcal{T}_0^{i,seq\_stuck(i)}$, respectively. Then, the sequence of one-step ahead controllable sets $\{\mathcal{T}_k^{i,seq\_stuck(i)}\}$ complying with *healthy-to-faulty* and *faulty-to-healthy* transitions is given via recursions (18)-(19).

Corollary 1: All the admissible healthy-to-faulty and faulty-to-healthy transitions are covered by the family of the $\prod_{i=1}^{l} f^i$ piecewise affine subsystems (17) deriving from the stuck actuator configurations.

Then, the following computable algorithm results.

SAFTC-Algorithm

Off-line:

1: Compute the invariant regions $\tilde{\mathcal{E}}^{ij}$, the observer gains L_{ij}, the robust invariant regions $\mathcal{T}_0^{ij} \subset \mathbb{R}^n$ and the stabilizing state feedback gains K_{ij}, $i = 0, 1, \dots, l; j = 1, \dots, f^i$, by means of *Proposition 1*;

2: Generate the sequences of N one-step controllable sets $\mathcal{T}_k^{i,seq\_stuck(i)}$ according to the prescriptions of *Theorem 1* and *Corollary 1*;

3: Store the $\prod_{i=1}^{l} f^i$ sequences $\{\mathcal{T}_k^{i,seq\_stuck(i)}\}_{k=0}^N$.

4: $t \leftarrow 0$

On-line:

5: $\hat{\sigma}(t) \leftarrow \min_{i,j} \pi_{ij}(t)$

6: $k^{i,j}(t) \leftarrow \min\{k : \hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_k^{i,j}\}, \forall (i,j)$

7: **if** $\hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_{k(t)}^{\hat{\sigma}(t)}$ **then**

8: $\quad (i^*(t), j^*(t)) \leftarrow \hat{\sigma}(t)$;

9: **else**

10: $\quad$ **if** $\hat{x}_{\hat{\sigma}(t)}(t) \in \mathcal{T}_{k^{0,0}(t)}^{00}$ **then**

11: $\quad\quad (i^*(t), j^*(t)) \leftarrow 0$;

12: $\quad$ **else**

13: $\quad\quad (i^*(t), j^*(t)) \leftarrow \arg\min_{i_q, j_q} k^{i,j}$ s.t. $\hat{x}_{\hat{\sigma}(t)}(t) \in \bigcap_q \mathcal{T}_{k^{i_q,j_q}(t)}^{i_q,j_q}$;

14: $\quad$ **end if**

15: **end if**

16: $k^* \leftarrow k^{i^*(t),j^*(t)}$;

17: **if** $(i^*(t), j^*(t)) = (0,0)$ **then**

18: $\quad$ **if** $k(t) = 0$ **then**

19: $\quad\quad u(t) \leftarrow K_{00}\, \hat{x}_{\hat{\sigma}(t)}(t)$

20: $\quad$ **else**

21: $\quad\quad u(t) \leftarrow \arg\min J_{k^*}(\hat{x}_{\hat{\sigma}(t)}(t), u)$ s.t.
$A\hat{x}_{\hat{\sigma}(t)}(t) + B^{i^*(t)}u + F^{i^*(t)}\bar{u}^{i^*(t),j^*(t)} \in \mathcal{T}_{k^*-1}^{i^*(t),j^*(t)}$,
$A\hat{x}_{\hat{\sigma}(t)}(t) + B^{i}u + F^{i}\bar{u}^{i,seq\_stuck(i)} \in \mathcal{T}_{k^{i,seq\_stuck(i)}-1}^{i,seq\_stuck(i)}$,
$i = 1, \dots, l, \ \ u \in \mathcal{U}$;

22: $\quad$ **end if**

23: **else**

24: $\quad$ solve $u(t) \leftarrow \arg\min J_{k^*}(\hat{x}_{\hat{\sigma}(t)}(t), u)$ s.t.
$A\hat{x}_{\hat{\sigma}(t)}(t) + B^{i^*(t)}u + F^{i^*(t)}\bar{u}^{i^*(t),j^*(t)} \in \mathcal{T}_{k^*-1}^{i^*(t),j^*(t)}$,
$A\hat{x}_{\hat{\sigma}(t)}(t) + B^{i}u + F^{i}\bar{u}^{i,seq\_stuck(i)} \in \mathcal{T}_{k^{i,seq\_stuck(i)}-1}^{i,seq\_stuck(i)}$,
$\forall i \,|\, \mathcal{T}_{k^{i,seq\_stuck(i)}-1}^{i,seq\_stuck(i)} \cap \mathcal{T}_{k^*-1}^{i^*,seq\_stuck(i^*)} \neq \emptyset, \ \ u \in \mathcal{U}$;

25: **end if**

26: **Apply** $u(t)$ to the plant (1);

27: $t \leftarrow t + 1$; goto 5

$$\mathcal{T}_k^{00} := \mathrm{Proj}_{\hat{x}_{00}}\{x_{00}^{aug} \in \mathcal{X}^{aug} : \exists\, u \in \mathcal{U} : \mathrm{Proj}_{\hat{x}_{00}}\{A_0^{aug}x_{00}^{aug} + B_0^{aug}u + B_{d_0}^{aug}d + E_0^{aug}e_{00}\} \in \mathcal{T}_{k-1}^{00},$$
$$\mathrm{Proj}_{\hat{x}_{00}}\{A_i^{aug}x_{00}^{aug} + B_i^{aug}u + B_{d_i}^{aug}d + E_{i,seq\_stuck(i)}^{aug}e_{i,seq\_stuck(i)} + F_i^{aug}\bar{u}_F^{i,seq\_stuck(i)}\} \in \mathcal{T}_{k-1}^{i,seq\_stuck(i)},$$
$$\forall d \in \mathcal{D},\ \forall e_{i,seq\_stuck(i)} \in \tilde{\mathcal{E}}^{i,seq\_stuck(i)},\ i = 1,\ldots,l\}, \tag{18}$$

$$\mathcal{T}_k^{i,seq\_stuck(i)} := \mathrm{Proj}_{\hat{x}_{i,seq\_stuck(i)}}\{x_{i,seq\_stuck(i)}^{aug} \in \mathcal{X}^{aug} : \exists u \in \mathcal{U} :$$
$$\mathrm{Proj}_{\hat{x}_{i,seq\_stuck(i)}}\{A_i^{aug}x_{i,seq\_stuck(i)}^{aug} + B_i^{aug}u + B_{d_i}^{aug}d + E_{i,seq\_stuck(i)}^{aug}e_{i,seq\_stuck(i)} + F_i^{aug}\bar{u}_F^{i,seq\_stuck(i)}\}$$
$$\in \mathcal{T}_{k-1}^{i,seq\_stuck(i)}, \forall d \in \mathcal{D}, \forall e_{i,seq\_stuck(i)} \in \tilde{\mathcal{E}}^{i,seq\_stuck(i)},$$
$$\mathrm{Proj}_{\hat{x}_{i',seq\_stuck(i')}}\{A_{i'}^{aug}x_{i',seq\_stuck(i')}^{aug} + B_{i'}^{aug}u + B_{d_{i'}}^{aug}d + E_{i',seq\_stuck(i')}^{aug}e_{i',seq\_stuck(i')} + F_{i'}^{aug}\bar{u}_F^{i',seq\_stuck(i')}\}$$
$$\in \mathcal{T}_{k-1}^{i',seq\_stuck(i')}, \forall d \in \mathcal{D}, \forall e_{i',seq\_stuck(i')} \in \tilde{\mathcal{E}}^{i',seq\_stuck(i')}, \forall i' : \mathcal{T}_{k-1}^{i',seq\_stuck(i')} \cap \mathcal{T}_{k-1}^{i,seq\_stuck(i)} \neq \emptyset\},$$
$$i = 1,\ldots,l. \tag{19}$$

Moreover, at each level k the predecessor set

$$\Omega_k := \left\{(x_{(\cdot),seq\_stuck}^{aug}, u, d, e_{(\cdot),seq\_stuck}) \,|\, g^{seq\_stuck}(x_{(\cdot),seq\_stuck}^{aug}, u, d, e_{(\cdot),seq\_stuck}) \in \Omega_{k-1}\right\}$$
$$= \bigcup_{i \in \mathcal{R}^{\Omega_k^{seq\_stuck}}} \{(x_{i,seq\_stuck(i)}^{aug}, u, d, e_{i,seq\_stuck(i)}) \in \mathcal{P}_i^{\Omega_k^{seq\_stuck}} \,|\, A_i^{aug}x_{i,seq\_stuck(i)}^{aug} + B_i^{aug}u + B_{d_i}^{aug}d \tag{20}$$
$$+ E_{i,seq\_stuck(i)}^{aug}e_{i,seq\_stuck(i)} + F_i^{aug}\bar{u}_F^{i,seq\_stuck(i)} \in \mathcal{P}_i^{\Omega_{k-1}^{seq\_stuck}}\}$$

is a polygon.

Proof - The proof follows similar lines as in [8]. □

Note that the running cost $J_{k(t)}(\hat{x}_{\hat{\sigma}(t)}(t), u)$ is:

$$J_{k(t)}(\hat{x}_{\hat{\sigma}(t)}(t), u) := \|A\hat{x}_{\hat{\sigma}(t)}(t) + B^{i(t)}u + F^{i(t)}\bar{u}_F^{i(t),j(t)}\|_2^2 \tag{21}$$

Proposition 2: Let the sequences of sets $\mathcal{T}_k^{ij}$ be non-empty. Then, the **SAFTC** algorithm guarantees the correctness of healthy-to-faulty and faulty-to-healthy transitions and ensures closed-loop asymptotic stability under constraints satisfaction.

Proof - By means of reachability and set-invariance arguments the proof follows, see e.g. [8]. □

IV. ILLUSTRATIVE EXAMPLE

In this section an application of the proposed control architecture is presented. Specifically, the aim is to deal with the flight control problem of a Cessna 182 aircraft subject to asset and command constraints.

The 3-DOF longitudinal model of the aircraft motion dynamics is described by the following equations

$$\dot{v} = -\frac{\rho v^2 S_w}{2m}(C_{D_0} + C_{D_\alpha}\alpha + C_{D_q}\frac{q\bar{c}}{2v} + C_{D_{\delta_e}}\delta_e) + \frac{T}{m}\cos\alpha - g\sin(\theta-\alpha) \tag{22}$$

$$\dot{\alpha} = q - \frac{\rho v^2 S_w}{2mv}(C_{L_0} + C_{L_\alpha}\alpha + C_{L_q}\frac{q\bar{c}}{2v} + C_{L_{\delta_e}}\delta_e) - \frac{T}{mv}\sin\alpha + \frac{g}{v}\cos(\theta-\alpha) \tag{23}$$

$$\dot{q} = \frac{\rho v^2 S_w \bar{c}}{2I_{yy}}(C_{m_0} + C_{m_\alpha}\alpha + C_{m_q}\frac{q\bar{c}}{2v} + C_{m_{\delta_e}}\delta_e) \tag{24}$$

$$\dot{\theta} = q \tag{25}$$

where $x_p = [v,\ \alpha,\ q,\ \theta]^T$ and $u = [T,\ \delta_e]^T$. The meaning of the involved variables and parameters can be found in [12]. The plant (22)-(25) has been discretized via forward Euler differences with the sampling time $T_c = 0.05\,s$, and the following physical constraints have been considered:

$$\mathcal{C} \in \mathbb{R}^6 : \left\{\begin{array}{rcl} 45.263 \leq & v & \leq 73.263\ \ [m/sec] \\ -0.296 \leq & \alpha & \leq 0.304\ \ [rad] \\ -1.6 \leq & q & \leq 1.6\ \ [rad/sec] \\ -0.457 \leq & \theta & \leq 0.415\ \ [rad] \\ 210 \leq & T & \leq 1110\ \ [N] \\ -0.4670 \leq & \delta_e & \leq 0.533\ \ [rad] \end{array}\right. \tag{26}$$

The nonlinear plant dynamics has been evaluated by resorting to gridding and linearization arguments, see [8] for details. Hence by hypothesising stuck phenomena on the deflector, the plant operates by switching amongst two modes: healthy $(mode-0)$ and faulty on δ_e $(mode-1)$. Hence, by resorting to the notation of (5) δ_e can assume the following three stuck drifts with respect to the nominal flight condition defined by (x_{eq}, u_{eq}) :

$$\bar{u}_F^{11} = -0.155,\ \bar{u}_F^{12} = 0.0889,\ \bar{u}_F^{13} = 0.1412. \tag{27}$$

For each PWA configuration, families of 200 one-step controllable regions have been computed by following the prescriptions of Proposition 1 and Theorem 2.

Starting from the initial healthy condition $x(0) = \left[\begin{array}{cccc} 72.792 & -0.295 & 1.600 & -0.445 \end{array}\right]^T \in \mathcal{T}_{119}^{0,0}$, the aim of the simulation is to maintain the trajectory *as close as possible* to the the nominal flight condition regardless of the stuck actuator fault scenario depicted in the upper graph of Fig. 2 (continuous red line). All the numerical result are summarized in Figs. 2-4. At $t = 10\,sec$ the deflector gets stuck at a -9^o drift w.r.t. the nominal flight condition, see the grey zone of Fig. 3. Initially, the **SAFTC** algorithm is not capable to correctly recognize such an event: in fact within the time interval $[10\ 11.5]\,sec$ the $\hat{\sigma}$ assumes the following values $(0,0)$ and $(1,3)$. The reason of this uncorrected behaviour has to be mainly ascribed to the estimator transients, see Fig. 4 where a significant discrepancy between real and estimated states results. On the other, it is important to remark that by construction both $(0,0)$ and $(1,3)$ can be used in place of the correct $(1,1)$ because $\hat{x}(10) \in \mathcal{T}_0^{0,0} \bigcap \mathcal{T}_0^{1,1}$ whereas $\hat{x}(11.3) \in \mathcal{T}_0^{1,1} \bigcap \mathcal{T}_0^{1,3}$, see the bottom graph of Fig. 2. Finally, at $t = 11.5\,sec$ the transition *healthy-to-faulty* is accomplished because $\hat{x}(11.4) \in \mathcal{T}_{181}^{1,1}$. Similar arguments apply for the other *stuck-to-stuck* transitions from $t = 24\,sec$ until $52\,sec$ when a recovery from the fault occurs. Again, the correct system mode cannot be identified because $\hat{x}(52) \notin \{\mathcal{T}_k^{0,0}\}$ while we have that $\hat{x}(52) \in \mathcal{T}_{176}^{1,2}$. Though incorrect, this choice is admissible thanks to the set inclusion $\mathcal{T}_k^{00} \subset \mathcal{T}_k^{i,seq\_stuck(i)}, \forall i = 1,\ldots,3, \forall k = 0,\ldots,200$, which guarantees that in a finite number of steps the state estimate will belong to $\{\mathcal{T}_k^{0,0}\}$, i.e. $\hat{x}(70) \in \mathcal{T}_{168}^{0,0}$.

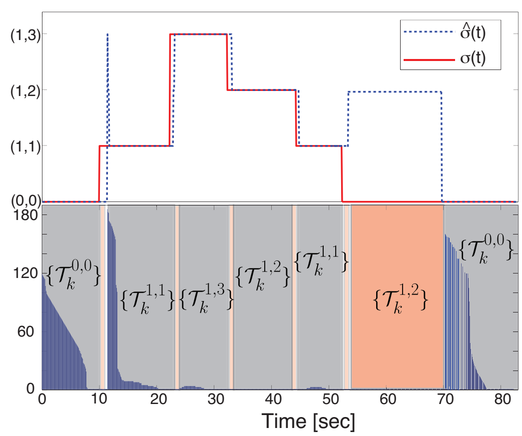

Fig. 2. Switching signals

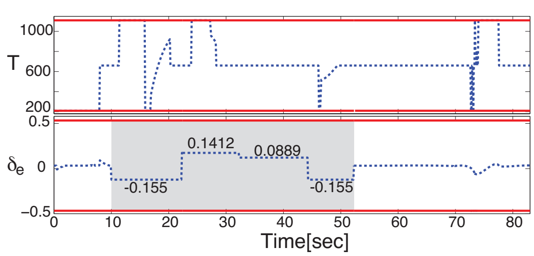

Fig. 3. Command inputs

V. Conclusions

In this paper we have presented a fault tolerant scheme for constrained linear discrete-time systems subject to multiple positions stuck actuator faults. Key features of the proposed

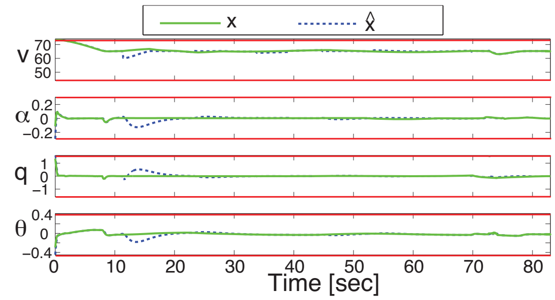

Fig. 4. State evolution

method, that combines piecewise affine systems with set-theoretic ideas in a unique framework, can be summarized as: a formal description of the plant dynamics in response to stuck events, correctness of healthy-to-faulty and *vicercersa* mode transitions and large domain of attractions.

References

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

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

[3] J. D. Boskovic and R. K. Mehra, "Stable multiple model adaptive flight control for accommodation of a large class of control effector failures", *ACC 1999*, pp. 1920-1924, 1999.

[4] J. Daafouz, P. Riedinger and C. Iung, "Stability analysis and control synthesis for switched systems: a switched Lyapunov function approach", *IEEE Trans. on Auto. 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.*, Vol. 27, No. 4, pp. 251-279, 2013.

[6] D. Famularo and G. Franzè, "Output Feedback Model Predictive Control of Uncertain Norm-Bounded Linear Systems", *Int. J. of Rob. and Non. Contr.*, Vol. 21, No. 8, pp. 838-862, 2011.

[7] D. Famularo, G. Franzè, A. Furfaro and M. Mattei. "An hybrid real-time command governor supervisory scheme for constrained control systems", *IEEE Trans. on Contr. Sys. Tech.*, Vol. 23, No. 3, pp. 924-936, 2015.

[8] G. Franzè, F. Tedesco and D. Famularo, "Actuator Fault Tolerant Control: A Receding Horizon Set-Theoretic Approach", *IEEE Trans. on Auto. Contr.*, Vol. 60, No. 8, pp. 2225-2230, 2015.

[9] D. Moerder, N. Halyo, J. Broussard, and A. Caglayan, " Application of precomputed control laws in a reconfigurable aircraft flight control system", *J. of Guid., Contr., Dyn.*, Vol. 12, pp. 325-333, 1989.

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

[11] S. V. Raković, E. C. Kerrigan, D. Q. Mayne and J. Lygeros, "Reachability analysis of discrete-time systems with disturbances", *IEEE Trans. on Auto. Contr.*, Vol. 51, No. 4, pp. 546-561, 2006.

[12] A. Roskam, "Airplane Flight Dynamics and Automatic Flight Control Part I", 1985.

[13] 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. on Auto. Contr.*, Vol. 59, No. 1, pp. 1657-1669, 2012.

[14] M. Staroswiecki, "On reconfiguration-based Fault Tolerance", *18th MED*, pp. 1681 - 1691, Marrakech, 2010.

[15] G. Tao, S. M. Joshi, and X. L. Ma, " Adaptive state feedback and tracking control of systems with actuator failures", *IEEE Trans. on Auto. Contr.*, Vol. 46, No. 1, pp. 78-95, 2001.

[16] B. Xiao, Q. Hu and Y. Zhang, "Adaptive Sliding Mode Fault Tolerant Attitude Tracking Control for Flexible Spacecraft Under Actuator Saturation", *IEEE Trans. on Contr. Sys. Tech.*, Vol. 20, No. 6, pp. 1605-1612, 2012.