49th IEEE Conference on Decision and Control
December 15-17, 2010
Hilton Atlanta Hotel, Atlanta, GA, USA

# A Fault Tolerant Control Scheme Based on Sensor-Actuation Channel Switching and Dwell Time

F. Stoican†, S. Olaru†, María M. Seron‡ and José A. De Doná‡

***Abstract*— The present paper deals with a switching control scheme for a plant with multiple *estimator-controller-actuator* pairs. The scheme has to deal with specific problems originated by the switching between the different feedback loops and accommodate to faults in the observation channels (sensors outputs). The main contribution is a fault tolerant switching scheme with stability guarantees assured by a pre-imposed dwell-time. The detection and the fault tolerance capabilities are assured through set separation for the residual signals corresponding to healthy and faulty functioning. Another contribution of the paper resides in a recovery technique for faulty sensors which makes use of a virtual sensor whose estimation, based on an optimization procedure, minimizes recovery time.**

## I. INTRODUCTION

In [1] a comprehensive result for fault tolerant stability of multisensor switching feedback control systems was presented upon the use of a common feedback gain matrix for all the *sensor-estimator* pairs. The main contribution of the present paper resides in the use of a switch feedback with different gains, thus making the assessment of global stability a nontrivial task, even in the absence of faults. It is noteworthy to mention that within this line of research, in [2], different feedback gains are used and stability is guaranteed under normal (fault free) operation conditions by imposing a switching rule based on the decrease of each individual Lyapunov function for the tracking error subsystems. In the present paper, a different switching condition, based on the calculation of a dwell time, will not only guarantee stability in the fault free case but also will offer concrete fault tolerant guarantees based on set separation. For determining robust positive invariant (RPI) sets used through the paper, we employ a construction based on outer approximations similar to the ones in [3]. In addition, an explicit separation method and a novel recovery mechanism that acknowledges healthy sensors through the use of a so-called *virtual sensor* are presented. The following notation will be used: $\mathbb{N}$ denotes the set of non negative integers; $\mathbb{N}^+$ denotes the set $\mathbb{N} \setminus \{0\}$. Whenever time is unspecified, a variable $x$ stands for $x(k)$ for some (unspecified) $k \in \mathbb{N}$, and $x^+$ stands for the *successor* variable, i.e. $x(k+1)$. The Minkowski sum of two sets is defined as $A \oplus B = \{a + b : \ a \in A \text{ and } b \in B\}$.

† SUPELEC Systems Sciences (E3S) - Automatic Control Department, Gif sur Yvette, France {florin.stoican,sorin.olaru}@supelec.fr
‡ CDSC, The University of Newcastle, NSW 2308, Australia {maria.seron,jose.dedona}@newcastle.edu.au

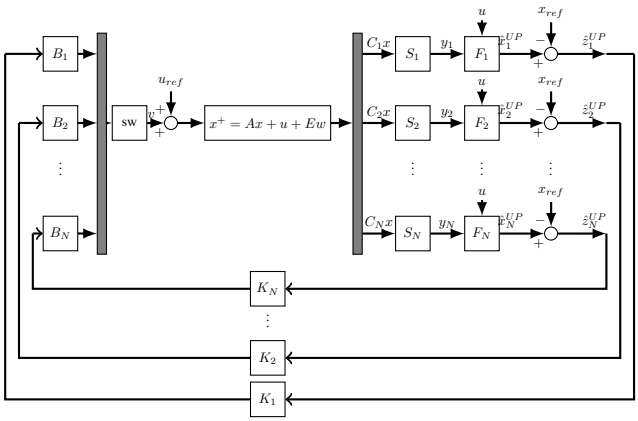


Fig. 1: Switching control scheme

## II. PLANT DYNAMICS AND FAULT SCENARIO

The present paper considers a linear discrete-time state space model of the plant:

$$x^+ = Ax + u + Ew \tag{1}$$

where $x \in \mathbb{R}^n$ and $x^+ \in \mathbb{R}^n$ are, respectively, the current and successor system states, $u \in \mathbb{R}^n$ is the input, and $w \in W \subset \mathbb{R}^r$ is a bounded process disturbance. The input consists of a switching between $N$ different actuator combinations, each of them characterized by a matrix $B_l$, such that each of the pairs $(A, B_l)$ is controllable for $l = 1, \ldots, N$. The information provided by each sensor can be used for estimation and control purposes, but it closes the feedback loop individually, with a particular actuation matrix gain $K_l$. This makes, in fact, the multisensor scheme to function as a switching mechanism between different feedback loops.

The control objective is for the state of the plant (1) to track a reference signal $x_{ref}$ that satisfies

$$x_{ref}^+ = Ax_{ref} + u_{ref} \tag{2}$$

The state reference is considered to be bounded by a closed polyhedral set $X_{ref}$ defined as:

$$x_{ref} \in X_{ref} = \left\{x_{ref}^0\right\} \oplus \Delta_{ref} \tag{3}$$

with $x_{ref}^0$ the analytic centre of the set.

Figure 1 depicts the switching scheme with plant (1), sensors $S_i$, estimators $F_i$, feedback gains $K_i$, actuator matrices $B_i$, $i = 1, \ldots, N$ and switching law $SW$.

### A. Sensor and estimator dynamics

The state vector $x$ is not directly measurable, but linear combinations of it, $C_i x, \quad i = 1, \ldots, N$ can be measured via $N$ sensors (under the assumption that each pair $(A, C_i)$ is detectable). The sensors have output signal:

$$y_i = C_i x + \eta_i \tag{4}$$

The sensor faults considered in this paper are of the type of total sensor outage. The failure is then represented by the following switching on the observation equation:

$$\begin{aligned} y_i = C_i x + \eta_i \quad &\xrightarrow{FAULT} \quad y_i = 0 \cdot x + \eta_i^F \\ y_i = C_i x + \eta_i \quad &\xleftarrow{RECOVERY} \quad y_i = 0 \cdot x + \eta_i^F \end{aligned} \tag{5}$$

The noise occurring during the fault, $\eta_i^F$, may be different from the one during healthy functioning, $\eta_i$.

In general, all the noises presented are considered to be bounded. As such, $w \in W$, $\eta_i \in N_i$ and $\eta_i^F \in N_i^F$ for $i = 1, \ldots, N$ where the polyhedral sets $W \subseteq \mathbb{R}^r, N_i \subseteq \mathbb{R}^{n_i}, N_i^F \subseteq \mathbb{R}^{n_i}$ are considered to be bounding boxes.

The estimators are designed such that they will have an adequate dynamic behavior for the plant state estimate:

$$\begin{aligned} \hat{x}_i^+ &= A\hat{x}_i + u + L_i\left(y_i - C_i\hat{x}_i\right) \\ &= \underbrace{\left(A - L_i C_i\right)}_{A_{L_i}}\hat{x}_i + u + L_i\left(C_i x + \eta_i\right) \end{aligned} \tag{6}$$

with the gains $L_i$ chosen such that matrices $A_{L_i}$ are strictly stable (always possible by the detectability assumption).

Using (1) and (6) one can define the estimation error affecting the sensor:

$$\tilde{x}_i^+ = x^+ - \hat{x}_i^+ = A_{L_i}\underbrace{\left(x - \hat{x}_i\right)}_{\tilde{x}_i} + \begin{bmatrix} E & -L_i \end{bmatrix}\begin{bmatrix} w \\ \eta_i \end{bmatrix} \tag{7}$$

The plant tracking error is given by the difference between the state (1) and its respective reference signal (2):

$$z^+ = x^+ - x_{ref}^+ = A\underbrace{\left(x - x_{ref}\right)}_{z} + \underbrace{\left(u - u_{ref}\right)}_{v} + Ew \tag{8}$$

Update estimations, intended to enhance the dynamic performance of the system and the fault detection process are also provided:

$$\begin{aligned} \hat{x}_i^{UP} &= \hat{x}_i + M_i\left(y_i - C_i\hat{x}_i\right) \\ \hat{z}_i^{UP} &= \hat{x}_i^{UP} - x_{ref} \end{aligned} \tag{9}$$

with matrices $M_i$ determined from $AM_i = L_i$ and where $\hat{z}_i^{UP}$ are the update tracking estimation errors.

### B. Closed loop dynamics

The fault tolerant scheme works under the condition that only healthy sensors will be used in the control law design. This condition is guaranteed by a fault detection and isolation (FDI) algorithm, which is fully developed in Section V below.

As such, let there be a partition of the sensors $i \in \mathcal{I} = \{1, \ldots, N\}$ into the sets:

- $\mathcal{I}_{\mathcal{H}}$, all the sensors acknowledged healthy
- $\mathcal{I}_{\mathcal{F}}$, all the sensors acknowledged faulty

so that $\mathcal{I}_{\mathcal{H}} \cup \mathcal{I}_{\mathcal{F}} = \mathcal{I}$ and $\mathcal{I}_{\mathcal{H}}$ is assumed to never be empty along the closed loop functioning. The partition is updated through an FDI mechanism, detailed in Subsection V-A. This means that we are able to identify and select only the healthy, $i \in \mathcal{I}_{\mathcal{H}}$ sensors (understood as a sensor with a healthy functioning in the sense of (4) and for which the estimation error (7) is confined to a safety region developed in Section III) and from them, the minimizer of a given cost function is obtained[1]:

$$\hat{z}^* = \underset{\hat{z} \in \mathcal{Z}_i}{argmin}\, J\left(\hat{z}\right) \tag{10}$$

with $\mathcal{Z}_i = \left\{\hat{z}_i^{UP} : \quad i \in \mathcal{I}_{\mathcal{H}}\right\}$. Using the minimizer $\hat{z}^* = \hat{z}_l^{UP}$, for some $l \in \mathcal{I}_{\mathcal{H}}$, the control action has the form:

$$u = u_{ref} + v^* = u_{ref} - B_l K_l \hat{z}^* \tag{11}$$

We remark here that each *sensor-estimator-actuator* loop will have a different feedback matrix gain $K_l$. The gains can be, for example, computed as independent solutions to Riccati equations for the pairs $(A, B_l)$ and weighting matrices $(Q_l, R_l)$. Henceforth it will be assumed that all matrices $(A - B_l K_l)$ have all their eigenvalues inside the unit circle.

As a consequence of the selection of a healthy sensor, that is, a sensor with the update estimated tracking error $\hat{z}^* = \hat{z}_l^{UP}$, for some $l \in \mathcal{I}_{\mathcal{H}}$, by using (4), (7), (8) and (9), we have

$$\hat{z}^* = z - \left(I - M_l C_l\right)\tilde{x}_l + M_l \eta_l \tag{12}$$

and, the control action (11) can be expressed as

$$u = u_{ref} - B_l K_l\left(z - \left(I - M_l C_l\right)\tilde{x}_l + M_l \eta_l\right) \tag{13}$$

## III. Stability of switched systems and invariant set construction

### A. Switched systems with dwell time

Consider a discrete-time switched system

$$x^+ = A_{\sigma(k)} x \tag{14}$$

where $\sigma(k) : k \geq 0 \rightarrow \mathcal{M} = \{1, \ldots, M\}$ is the switching index between the linear systems $A_i$, $i \in \mathcal{M}$.

We denote the set of all switching policies with dwell time[2] equal to a given positive integer constant $\tau \in \mathbb{N}^+$:

$$\mathcal{T}_\tau = \left\{\sigma(\cdot) : \; t_{j+1} - t_j \geq \tau\right\} \tag{15}$$

where $t_{j+1}$ and $t_j$ are successive switching times, for all $j \in \mathbb{N}$. The following theorem is useful in this context [4]:

[1]Within the scope of this paper, no particular choice of the cost function is prescribed but we point to [1] for the use of a quadratic index weighting the reference tracking performance and the control energy.

[2]The notion of dwell time, understood as the minimal time interval between consecutive switches in a system that can switch between a finite set of linear dynamics, is employed in order to guarantee global stability (details can be found in [4]).

*Theorem 1:* Assume that, for a given $\tau \geq 0$ and $\forall i \in \mathcal{M}$ there exist $P_i$ such that

$$P_i > 0,\ A_i' P_i A_i < P_i,\ A_i'^{\tau} P_j A_i^{\tau} < P_i \quad \forall j \neq i \tag{16}$$

Then, the system (14) with a switching policy in $\mathcal{T}_\tau$ is globally stable with an associated Lyapunov function

$$v(x,k) = x' P_{\sigma(k)} x \tag{17}$$

■

An upper bound for the minimal stabilizing dwell time can be computed by taking the minimum value of $\tau$ satisfying the conditions of Theorem 1. This can be calculated through a linear search with the optimization problem

$$\underset{\text{s.t. (16) are feasible}}{min} \quad \tau > 0 \tag{18}$$

The previous results consider a nominal switching system (14) in the disturbance free case. In the following subsection we will use these results to derive invariant sets when the system is affected by bounded disturbances.

### B. Invariant sets

*1) Basic definitions for set invariance [3]:* We consider a discrete-time switched system with linear dynamics subject to bounded disturbances:

$$\begin{aligned} x^+ &\in \mathcal{D}(x, \mathbb{A}, \mathbb{W}) \\ \mathcal{D}(x, \mathbb{A}, \mathbb{W}) &= \{Ax + w :\ A \in \mathbb{A},\ w \in \mathbb{W}\} \\ \mathbb{A} &= \left\{A_i \in \mathbb{R}^{n \times n}, \quad i = 1 \dots M\right\} \\ \mathbb{W} &\subset \mathbb{R}^n \end{aligned} \tag{19}$$

We assume that the autonomous system $x^+ \in \mathcal{D}(x, \mathbb{A}, \{0\})$ is absolutely asymptotically stable, that is, there exists a Lyapunov function $V(x)$ such that

$$V(x^+) - V(x) < 0 \tag{20}$$

The one step forward set for the switched system (19)

$$\mathcal{D}(X, \mathbb{A}, \mathbb{W}) = \{Ax + w :\ x \in X,\ A \in \mathbb{A},\ w \in \mathbb{W}\} \tag{21}$$

can be used to define the set sequence $\{D_k\}$:

$$D_{k+1} = \mathcal{D}(D_k, \mathbb{A}, \mathbb{W}),\ k \in \mathbb{N}^+,\ D_0 = \{0\} \tag{22}$$

*Definition 1:* RPI set. The set $\Omega \subset \mathbb{R}^n$ is a *robust positively invariant (RPI) set* of (19) if $\mathcal{D}(x, \mathbb{A}, \mathbb{W}) \subseteq \Omega$ for all $x \in \Omega$, i.e. if and only if $\mathcal{D}(\Omega, \mathbb{A}, \mathbb{W}) \subseteq \Omega$. ■

*2) Construction of RPI approximations:*

*Theorem 2 (Theorem 2 of [3]):* For a system (19) that satisfies (20) there exists a finite integer $s \in \mathbb{N}^+$ and a scalar $\alpha \in [0, 1)$ such that

$$R_s \subseteq \alpha \mathbb{W} \tag{23}$$

where $R_s$ is defined by the following set recursion

$$R_k = \mathcal{D}(R_{k-1}, \mathbb{A}, \{0\}),\ k \in \mathbb{N}^+,\ R_0 = \mathbb{W} \tag{24}$$

Moreover, given any pair $(\alpha, s) \in [0, 1) \times \mathbb{N}^+$ such that (23) is true, the set $D(\alpha, s)$ defined by

$$D(\alpha, s) = (1 - \alpha)^{-1} D_s \tag{25}$$

is a compact RPI set for system (19) such that $D_\infty \subseteq D(\alpha, s)$, with $D_s$ and $D_\infty$ obtained from the recursion (22). ■

*3) Invariant sets for a switched system with dwell time:* Let $\tau$ be the value computed from (18) for system (14), then the system is asymptotically stable under any switching law in (15). We denote:

$$\mathcal{D}_\tau(x, \mathbb{A}, \mathbb{W}) = \left\{ \underbrace{\mathcal{D}(\mathcal{D}(\mathcal{D} \dots}_{\tau \text{iterations}} \mathcal{D}(x, A, \mathbb{W}), A, \mathbb{W}),\ A \in \mathbb{A} \right\} \tag{26}$$

Using (26) we can define the dynamic system

$$x^+ \in \mathcal{D}_\tau(x, \mathbb{A}, \mathbb{W}) \tag{27}$$

The above system considers a switch every $\tau$ time instants and represents a particular case of switching strategy which is asymptotically stable with associated piecewise quadratic Lyapunov function (17) for the disturbance free case ($\mathbb{W} = \{0\}$). It follows then that condition (20) is verified for the disturbance free case and we can proceed with the set constructions detailed in Theorem 2 for the dynamics (27), leading to an invariant set $D^\tau(\alpha, s)$.

This construction will guarantee that any trajectory of a system switching every $\tau$ steps, starting inside the set will remain inside it at the switching instants. However, it tells nothing about the trajectory's behavior in between the switching instants. The set $\bar{D}(\alpha, s)$, which adds to $D^\tau(\alpha, s)$ the sets corresponding to transitions from moment $t_j + 1$ to $t_j + \tau - 1$ will be considered:

$$\bar{D}(\alpha, s) = D^\tau(\alpha, s) \bigcup_{\substack{l=1,\dots,M \\ k=1,\dots,\tau-1}} \Theta_k^l \tag{28}$$

where $\Theta_k^l$ is defined by the following set recursion

$$\Theta_k^l = \mathcal{D}(\Theta_{k-1}^l, A_l, \mathbb{W}),\ k \in \mathbb{N}^+,\ \Theta_0^l = D^\tau(\alpha, s) \tag{29}$$

*Proposition 1:* By construction, the set $\bar{D}(\alpha, s)$ is cyclic invariant for the set $D^\tau(\alpha, s)$ and the switching dynamics

$$x^+ \in \mathcal{D}\left(x, A_{\sigma(k)}, \mathbb{W}\right)$$

with switching policy $\sigma(\cdot)$ such that $t_{j+1} - t_j = \tau$, where $t_j, t_{j+1}$ are successive switching times (in particular, $\sigma(\cdot) \in \mathcal{T}_\tau$ in (15)). This means that $\forall x(0) \in D^\tau(\alpha, s)$ we have that $x(k) \in \bar{D}(\alpha, s), \forall k \geq 0$, and $x(t_j) \in D^\tau(\alpha, s)$ for all switching instants $t_j$. ■

## IV. Invariant sets for the multisensor scheme

The fault tolerant approach for the system described in Section II requires the construction of an invariant set associated to the plant tracking error (8).

Using (1), (2), (8) and (13) we have:

$$z^+ = A_{z,l} z + B_{z,l} \delta_{z,l} \tag{30}$$

with $A_{z,l} = A - B_l K_l$, $B_{z,l} = \begin{bmatrix} E & B_l K_l & -B_l K_l \end{bmatrix}$ and

$$\delta_{z,l} = \begin{bmatrix} w' & (I - M_l C_l)\, \tilde{x}_l' & M_l \eta_l' \end{bmatrix}' \tag{31}$$

Note that term $\tilde{x}_l$ is not a priori known but an invariant set containing it may be computed as described in Subsection III-B.2. For further use we will denote such a set[3]

$$\tilde{S}_l \triangleq \text{RPI set under dynamics (7)} \tag{32}$$

Let the $\tau$-step successor system dynamics associated with (30), assuming no switching has occurred, be defined as:

$$z_\tau^+ = A_{z,l}^\tau z_\tau + A_{z,l}^{\tau-1} B_{z,l} \delta_{z,l}^{-\tau+1} + \cdots + B_{z,l}\delta_{z,l}^0 \tag{33}$$

where $\delta_{z,l}^{-k}$ denotes the noise affecting system (30) $k$ instants prior to the current time. These dynamics describe the evolution of system (30) observed every $\tau$ samples as introduced in (26) and constitute a first step for the construction of the invariant sets $S_z^\tau$ of Theorem 2 and cyclic invariant sets for the switched system as described in Proposition 1. The set $\bar{S}_z$ (constructed as a special case of (28)), which adds the intermediate sets from the instant after the switch $t_j + 1$ to $t_j + \tau - 1$ is computed as:

$$\bar{S}_z = S_z^\tau \bigcup_{\substack{l=1,\ldots,N \\ k=1,\ldots,\tau-1}} A_{z,l}^k S_z^\tau \oplus A_{z,l}^{k-1} B_{z,l}\Delta \oplus \cdots \oplus B_{z,l}\Delta \tag{34}$$

where $\Delta_{z,l} = W \times (I - M_l C_l)\tilde{S}_l \times M_l N_l$ are bounding sets for $\delta_{z,l}$ in (31) and $\Delta = ConvexHull\{\Delta_{z,l},\ l \in \mathcal{I}\}$ covers all the possible realisations of estimation errors from healthy sensors and corresponding measurements noises.

## V. Fault tolerant scheme

In the following subsections we will discuss a fault tolerant scheme implementation for system (1). Before entering into the details of the FDI and recovery mechanisms we introduce the partition into *healthy* and *faulty* indices for the set $\mathcal{I} = \mathcal{I}_\mathcal{H} \cup \mathcal{I}_\mathcal{F} = \{1, \ldots, N\}$:

$$\begin{aligned} \mathcal{I}_\mathcal{H} &= \left\{ i :\ y_i = Cx + \eta_i \text{ and } \tilde{x}_i \in \tilde{S}_i \right\} \\ \mathcal{I}_\mathcal{F} &= \mathcal{I} \setminus \mathcal{I}_\mathcal{H} \end{aligned} \tag{35}$$

### A. FDI based on set separation

An FDI (fault detection and isolation) mechanism analyzes the transition $\mathcal{I}_\mathcal{H} \to \mathcal{I}_\mathcal{F}$. A signal called a *residual*, sensitive to fault occurrences and presenting a manageable dependence on the disturbances, has to be defined for the detection of faults. Indeed, the presence of faults implies, through the structural changes (5), a modification in the inputs affecting the corresponding estimator which thus carries information on the fault signature.

As such, for the multisensor scheme considered in the present paper we propose the residual signal $r_i$

$$r_i = \hat{z}_i^{UP} - (I - M_i C_i)\,\hat{z}_i \tag{36}$$

where $\hat{z}_i = \hat{x}_i - x_{ref}$. Note that the residual, $r_i$, is a linear combination of measurable quantities associated to the $i^{th}$ sensor. From (4), (5) and (9) one can distinguish between the healthy and the faulty cases

$$\begin{aligned} \text{healthy functioning: } r_i &= M_i C_i z + M_i \eta_i && (37) \\ \text{faulty functioning: } r_i &= -M_i C_i x_{ref} + M_i \eta_i^F && (38) \end{aligned}$$

These residuals can be used to identify the faults if the sets containing (37) and (38) are separated. The separation reduces then to the study of the sets $S_i^H$ and $S_i^F$ of all the possible values in the healthy, respectively faulty, case of the residual signal:

$$\begin{aligned} S_i^H &= M_i C_i \bar{S}_z \oplus M_i N_i \\ S_i^F &= (-M_i C_i)\, X_{ref} \oplus M_i N_i^F \end{aligned} \tag{39}$$

*Remark 1:* The membership of residual (36) to either set in (39) is an indicator of the current condition of the sensor in question. Note also that the change (5) is detected at the actual instant of occurrence due to the updated term (9) that takes into account the current output of the sensor. ■

*Remark 2:* The separation between the sets (39) is achieved by means of the reference signal offset $x_{ref}^0$ in (3). Indeed, for a given $\Delta_{ref}$, one can find a minimal value of $x_{ref}^0$ for which the separation (in the sense (40), see below) is valid. ■

Depending on the trade-off sought between computational load and accuracy of the FDI mechanism, various methods to check set separation can be employed. In the present work we concentrate on the explicit separation based on the assumption that:

$$S_i^H \cap S_i^F = \emptyset, \quad \forall i \in \mathcal{I} \tag{40}$$

The online FDI test then reduces to the verification of the inclusion of the residual (36) in one of the sets (39).

### B. Recovery

The recovery procedure of the FDI has to validate the transition $\mathcal{I}_\mathcal{F} \to \mathcal{I}_\mathcal{H}$. It decides if a previously faulty sensor respects the conditions defining it as healthy:

$$r_i \in S_i^H, \quad \tilde{x}_i \in \tilde{S}_i \tag{41}$$

In [5], [6] a set membership test of the estimation errors for the sensor in question was employed, but the duration of the recovery was dependent on the convergence of the trajectories to their invariant sets and the recovery process itself was not guaranteed to succeed for all combinations of faulty/healthy sensors.

By definition, the estimation error (7) is not directly measurable and as such only an indirect information can be manipulated. The solution proposed here is to verify for each sensor under recovery if healthy functioning has been verified for a predefined number of steps (recall that healthy sensor functioning can be directly acknowledged by checking the residual signal (36) against the sets (39)). After a number of iterations with output equation (4) the estimation error (7) will converge to its invariant set (32) thus satisfying the second condition in (41). An upper bound on the number of steps can be obtained with any suitable algorithm that

[3]The invariant set $\tilde{S}_l$ will actually have the form $(1+\epsilon)D(\alpha, s)$, with $\epsilon > 0$ arbitrarily small, to facilitate the computation of convergence times to this set (see Proposition 2 in Section V below).

computes in how many iterations all trajectories starting from an initial set will converge inside the associated invariant set. Using the notation from Section III we define, for a given initial set $\Omega_0$ and destination set $\Omega$, the convergence time as:

$$\theta^* = \underset{k}{argmin} \{X_k \subseteq \Omega,\ X_i = \mathcal{D}(X_{i-1}, \mathbb{A}, \mathbb{W}), X_0 = \Omega_0\} \tag{42}$$

As an additional element, as long as the sensor has a faulty functioning, an *artificial* estimation (based on the information provided by the rest of the healthy sensors) will be provided, thus creating a so called *virtual sensor*. If the sensor starts to exhibit a healthy functioning the estimation is again provided by the dynamics (6). This is useful in increasing the speed of the eventual recovery by "keeping" the updated tracking estimation error (9) near its healthy functioning region.

*Remark 3:* Note the distinction between the notions of healthy/faulty functioning and the acknowledgment of a sensor as being healthy. The first refers to the actual behavior of the sensor at a given time instant according to (5) (and leading to the residual values (37) or (38)), whereas the second notion refers to both conditions in (41) being satisfied. As such, it is entirely possible for a sensor to be considered faulty even with a healthy functioning (4) if the signals of interest are not (yet) inside their invariants sets (that is, $\tilde{x}_i \notin \tilde{S}_i$). ■

We are able to analyze the plant tracking error as a combination of measured values from healthy sensors, and uncertain but bounded variables, as follows (see (12)):

$$z(k) = \underbrace{\hat{z}_l^{UP}(k)}_{measured\,value} + \underbrace{(I - M_l C_l)\tilde{x}_l(k) - M_l \eta_l(k)}_{uncertainties} \tag{43}$$

Each healthy sensor proposes a set of possible values for the plant tracking error. Thus, the tracking error estimation can be enhanced by considering the values (43) proposed by all the healthy sensors:

$$z(k) \in \underbrace{\bigcap_{l \in \mathcal{I}_H(k)} \left[ \left\{ \hat{z}_l^{UP}(k) \right\} \oplus (I - M_l C_l)\tilde{S}_l \oplus (-M_l) N_l \right]}_{I_{\mathcal{I}_H}} \tag{44}$$

The sensor under recovery is replaced by a virtual sensor in the sense that its state estimation is discarded and an artificial one, $\hat{x}_j^*$, will be provided. To this artificial estimate we associate an update tracking estimation error $\hat{z}_j^{UP,*}$. Using (43) and (44) (i.e., "giving" to the under recovery sensor the characteristics of the healthy sensors) the set of all possible values of the associated estimation error $\tilde{x}_j^*$ is reduced to:

$$\tilde{S}^j_{\mathcal{I}_H(k)} \left( \hat{z}_j^{UP,*} \right) = (I - M_j C_j)^{-1} \left[ \left\{ -\hat{z}_j^{UP,*}(k) \right\} \oplus M_j N_j \oplus I_{\mathcal{I}_H} \right] \tag{45}$$

The set (45) is parameterized by the values $\hat{z}_l^{UP}$, $l \in \mathcal{I}_H$ (see (44)) and $\hat{z}_j^{UP,*}$. Since $\hat{z}_j^{UP,*}$ can be arbitrarily chosen, a suitable value, that minimizes the convergence time (42) (with destination set $\tilde{S}_j$ in place of $\Omega$ and with initial conditions in the set (45)) will be computed when the sensor $j$ changes from faulty to healthy functioning, thus resetting its estimation dynamics. In order to provide a constructive procedure for the choice of $\hat{z}_j^{UP,*}$, the following proposition is presented.

*Proposition 2:* Consider the invariant set $D(\alpha, s)$ of the form (25) with respect to the dynamics $x^+ = Ax + w, w \in \mathbb{W}$. Given a polytope $P \subset \mathbb{R}^n$ and a scalar $\epsilon > 0$ there exists a minimum integer $\theta(P, \epsilon) \in \mathbb{N}^+$ and an associated $\delta \in \mathbb{R}^n$ such that $\forall x(0) \in P \oplus \{\delta\}$ we have $x(k) \in (1 + \epsilon)D(\alpha, s), \forall k \geq \theta(P, \epsilon)$. An upper approximation $\bar{\theta}(P, \epsilon)$ can be obtained from the minimization

$$\{\delta^*, \bar{\theta}(P, \epsilon)\} = \underset{\substack{(\delta, \theta) \\ \text{subject to:}}}{arg\,min} \quad \theta \quad P \oplus \{\delta\} \subseteq D_s \oplus A^{-\theta} \cdot \epsilon D(\alpha, s) \tag{46}$$

where $D_s$ is obtained from the recursion (22).

*Proof:* The proof is based on standard manipulations with (minimal) RPI sets (see, e.g., [3]) and it is omitted for space reasons. ■

Let $\tilde{S}_j$ in (32) be constructed as $\tilde{S}_j = (1+\epsilon)D(\alpha, s)$, with $\epsilon > 0$ and $D(\alpha, s)$ as in Theorem 2. Let $D_s$ be the associated set obtained by the recursion (22). Then Proposition 2 can be applied to estimate the convergence time to $\tilde{S}_j$ from the set (45) (where $(I - M_j C_j)^{-1})(-\hat{z}_j^{UP,*}(k))$ takes the role of the variable $\delta$ being optimized) as follows:

$$\left\{ \hat{z}_j^{UP,*}, \bar{\theta}_j \right\} = \underset{\substack{(\hat{z}_j^{UP,*}, \theta) \\ \text{subject to:}}}{arg\,min} \quad \theta \quad \tilde{S}^j_{\mathcal{I}_H}\left(\hat{z}_j^{UP,*}\right) \subseteq D_s \oplus A_{L_j}^{-\theta} \epsilon D(\alpha, s) \tag{47}$$

Resetting the parameter $\hat{z}_j^{UP,*}$ to the optimal value found in (47) we assure an optimal convergence time $\bar{\theta}_j$ in the sense of (42).

The final step of the reconfiguration is the construction of the estimation for the virtual sensor coherent with (47). Rewriting (43) one obtains that any $\hat{x}_j^*$ verifying

$$\hat{x}_j^*(k) \in (I - M_j C_j)^{-1} \left[ \left\{ \hat{z}_j^{UP,*}(k) + (I - M_j C_j) x_{ref}(k) \right\} \oplus (-M_j C_j) I_{\mathcal{I}_H}(k) \oplus (-M_j) N_j \right] \tag{48}$$

is a valid choice.

Finally, if the recovery mechanism acknowledges the healthy functioning (4) of the sensor and the convergence time $\bar{\theta}_j$ computed with (47) has elapsed, the next value of its estimation is no longer discarded. Indeed the estimator is allowed again to use the information provided by the sensor.

Algorithm 1 implements a reconfiguration procedure that diagnoses the healthy and faulty sensors (steps 11 and 17). Each sensor under recovery has an associated convergence time $\bar{\theta}_i$ computed from (47) that will be decreased (step 9) if the subsequent dynamic is healthy and is reinitialized when the sensor first recovers (step 6). Finally, a counter associated to the dwell time $\tau$ computed in (18) (step 20) will signal if switches can be performed ($k = t_j + \tau$).

**Algorithm 1:** Fault tolerance scheme

**Input**: $\mathcal{I} = \mathcal{I}_{\mathcal{H}}(0) \cup \mathcal{I}_{\mathcal{F}}(0); \quad \mathcal{I}_{\mathcal{H}}(0) \neq \emptyset$

1 $k \leftarrow$ the current sampling time;
2 $t_j \leftarrow$ time of the last switch ($t_j < k$);
3 $l_j \leftarrow$ index of last estimator selected by the switching;
4 **foreach** *sensor* $i \in \mathcal{I}_{\mathcal{F}}(k-1)$ **do**
5  **if** $r_i(k-1) \in S_i^F$ *and* $r_i(k) \in S_i^H$ **then**
6  compute (45), (47) and (48);
7  **end**
8  **if** $r_i(k-1) \in S_i^H$ *and* $r_i(k) \in S_i^H$ **then**
9  $\bar{\theta}_i = \bar{\theta}_i - 1$;
10  **if** $\bar{\theta}_i = 0$ **then**
11  label sensor as healthy;
12  **end**
13  **end**
14 **end**
15 **foreach** *sensor* $i \in \mathcal{I}_{\mathcal{H}}(k-1)$ **do**
16  **if** $r_i(k) \in S_i^F$ **then**
17  label sensor as faulty;
18  **end**
19 **end**
20 **if** $k = t_j + \tau$ **then**
21  select a sensor $l \in \mathcal{I}_{\mathcal{H}}(k)$ that minimizes (10);
22  $t_j = k$; $l_j = l$;
23 **else**
24  **if** $l_j \in \mathcal{I}_{\mathcal{H}}(k)$ **then**
25  $\hat{z}^* = \hat{z}_{l_j}^{UP}$;
26  **else**
27  choose $\hat{z}^* \in ConvexHull\left\{\hat{z}_l^{UP},\, l \in \mathcal{I}_H(k)\right\}$ ;
28  **end**
29 **end**
30 construct control law $u$ as in (11);

*Remark 4:* Once an actuator-control pair has been selected by the switching criterion (10) to implement the control law (11), Algorithm 1 does not allow to discard it before the required dwell time $\tau$ has elapsed. If the imposed $\tau$ period of selection for the given actuator-control pair has not elapsed and the associated sensor is acknowledged faulty during this period, an artificial updated tracking error estimate taken as a convex sum of the updated tracking estimation errors of the remaining healthy sensors will be provided to the control loop (step 27). The cyclic invariance is ensured since the construction of the set $\bar{S}_z$ uses the convex hull of the disturbances from all possible combinations of healthy sensors affecting (30). ■

## VI. Example

A plant, with dynamics given by the model:

$$x^+ = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix} x + u + \begin{bmatrix} 0 \\ 0.1 \end{bmatrix} w \tag{49}$$

with $|w| \leq 0.02$ and a set of actuators $B_i = \begin{bmatrix} 1.5 & 0 \\ 0 & 0.1 \end{bmatrix}, \begin{bmatrix} 0.5 & 0.5 \\ 0 & 0.2 \end{bmatrix}$ and $\begin{bmatrix} 2 & 0 \\ 1 & 0.2 \end{bmatrix}$ will be used as an example in this section.

We use three sensors described by:

$$\begin{aligned} C_1 &= \begin{bmatrix} 0.30 & 0.25 \end{bmatrix} \text{ and } |\eta_1| \leq 0.1, \quad |\eta_1^F| \leq 1 \\ C_2 &= \begin{bmatrix} 0.25 & 0.10 \end{bmatrix} \text{ and } |\eta_2| \leq 0.1, \quad |\eta_2^F| \leq 0.25 \\ C_3 &= \begin{bmatrix} 0.25 & 0.25 \end{bmatrix} \text{ and } |\eta_3| \leq 0.1, \quad |\eta_3^F| \leq 1 \end{aligned} \tag{50}$$

The estimators for each sensor are constructed as in (6) using the gains: $L_i = \begin{bmatrix} 0.83 \\ 3 \end{bmatrix}, \begin{bmatrix} 3.25 \\ 2 \end{bmatrix}$ and $\begin{bmatrix} 1.20 \\ 1 \end{bmatrix}$.

The feedback gains are determined as solutions of Riccatti equations for common tuning parameters ($Q = diag(\begin{bmatrix} 0.1 & 5 \end{bmatrix})$ and $R = diag(\begin{bmatrix} 1 & 0.1 \end{bmatrix})$):

$$K_i = \begin{bmatrix} 0.25 & 0.04 \\ 0.01 & 5.00 \end{bmatrix}, \begin{bmatrix} 0.27 & -0.61 \\ 0.17 & 3.35 \end{bmatrix}, \begin{bmatrix} 0.15 & 0.44 \\ -0.67 & 2.12 \end{bmatrix} \tag{51}$$

For $\Delta_{ref} = \left\{ x : \quad |x| \leq \begin{bmatrix} 12 \\ 5.04 \end{bmatrix} \right\}$ fixed, a minimal offset $x_{ref}^0 = \begin{bmatrix} 50 & -4.96 \end{bmatrix}'$ assures condition (40).

Using the procedure described in Subsection III-B.3 the invariant sets (34) that satisty condition (40) were determined for a computed dwell time of $\tau = 2$ with $s = 4$ iterations, for an $\alpha = 0.23$.

To verify the significance of the choice of the artificial estimation we propose two modalities of implementing the recovery: using the set (48) as a provider for the artificial estimation, on the one hand, and using the estimation provided by some healthy sensor, $l$ say, on the other hand. In the first case we obtain (45) as a starting set for the estimation error convergence when the sensor switches to healthy functioning while in the latter case, the set will be $\tilde{S}_l$ of the form (32). We obtained that the use of set (45) averaged a recovery time of 27.5s and set (32) a recovery time of 57s, thus justifying the use of an artificial estimate satisfying (48).

## VII. Conclusions

This paper has proposed an effective method for fault tolerant switching with a dwell-time mechanism for a plant with multiple sensor-estimator-actuator loops. The selected sensor-estimator-actuator triplet provides the control action for a pre-determined period of time (larger than the dwell-time) thus ensuring nominal stability. Additionally, a novel recovery acknowledgment mechanism that uses a virtual sensor has been proposed.

## References


[1] M. M. Seron, X. W. Zhuo, J. A. De Doná, and J. J. Martínez, "Multisensor switching control strategy with fault tolerance guarantees," *Automatica*, vol. 44, no. 1, pp. 88–97, 2008.

[2] J. J. Martínez, M. M. Seron, and J. A. De Doná, "Fault-tolerant switching scheme with multiple sensor-controller pairs," in *Proc. of the 17th IFAC World Congress*, (Seoul, South Korea), pp. 1212–1217, 6-11 July 2008.

[3] K. I. Kouramas, S. V. Rakovic, E. C. Kerrigan, J. Allwright, and D. Q. Mayne, "On the minimal robust positively invariant set for linear difference inclusions," in *Proceedings of the 44th IEEE Conference on Decision and Control and European Control Conference*, (Seville, Spain), pp. 2296–2301, 12-15 December 2005.

[4] J. Geromel and P. Colaneri, "Stability and stabilization of discrete time switched systems," *Int. J. of Control*, vol. 79, no. 7, pp. 719–728, 2006.

[5] S. Olaru, F. Stoican, J. A. De Doná, and M. M. Seron, "Necessary and sufficient conditions for sensor recovery in a multisensor control scheme," in *Proc. of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, (Barcelona, Spain), pp. 977–982, 30 June-3 July 2009.

[6] F. Stoican, S. Olaru, J. A. De Doná, and M. M. Seron, "Enhanced fault tolerant multisensor control scheme with fast sensor recovery," in *Proc. of the 29th American Control Conference*, (Baltimore, Maryland, USA), 30 June-2 July 2010.