Actuator Fault Tolerant Control Based on Probabilistic Ultimate Bounds

Noelia Pizzi[a], Ernesto Kofman[a], José A. De Doná[b], Maria M. Seron[b]

[a] *CIFASIS - CONICET, FCEIA - UNR, Argentina.*
(emails: kofman, pizzi@cifasis-conicet.gov.ar)
[b] *School of Electrical Engineering and Computer Science and CDSC, The University of Newcastle, Australia.*
(emails: Jose.Dedona, Maria.Seron@newcastle.edu.au)

Abstract

In this work we introduce a novel set-based fault tolerant control scheme for linear systems under Gaussian disturbances. In the proposed strategy, actuator faults are detected and diagnosed when residual trajectories enter and remain in certain sets that are computed as probabilistic ultimate bounds. After a fault is diagnosed, the control scheme is reconfigured to take into account the corresponding actuator failure and preserve certain closed loop features. We show that our strategy can detect and diagnose the different faults considered with an arbitrarily small probability of misdetection.

Keywords: Fault diagnosis; Gaussian noise; probabilistic ultimate bounds.

1. Introduction

The safe and efficient operation of automatic control systems in modern industries is essential in view of the growing economic, environmental and safety demands. When faults occur in any component of the system, its performance usually deteriorates and may even have catastrophic consequences. Early detection of faults in the system and correct diagnosis of their origin, are critical to make decisions to accommodate, or reconfigure, the system in order to adapt to the new situation.

Since the introduction of the first techniques of diagnosis in the 1970s, many methods have been proposed for detection and identification of faults. These can be found in books and survey papers such as [6, 16, 2, 10, 4, 8, 7]. Most of these techniques are based on the use of observers that provide "analytical redundancy". These observers generate signals (commonly called "residuals") which act as indicators of the presence of faults. In healthy operation, residuals usually have small values caused by disturbances and other uncertainties. When a fault occurs, their values grow and the fault is detected provided that the residuals exceed certain "thresholds" chosen a priori according to some assumptions about the system and external signals.

Some alternative approaches to the one of the current paper, which deal with different aspects of the problem of actuator faults, can be found in [22, 19, 15, 23, 21]. In [22], a 'virtual sensor' and a 'virtual actuator' are designed for the reconfiguration of linear parameter varying systems after faults, and stability of the reconfigured system is established using input to state stability theory. The faulty system is assumed to be known, that is, no fault detection nor fault estimation

capabilities are included. The work in [19] considers the use of a virtual sensor and a virtual actuator for linear parameter varying systems with fault estimation formulated as a parameter estimation problem. The authors of [15] provide a scheme that deals with actuator fault tolerant control of systems with polytopic uncertainties, by using set-based diagnosis and virtual-actuator-based reconfiguration. In addition, the manuscripts [23] and [21] present an active fault tolerant control scheme for systems with dissimilar redundant actuation."

A methodology related to the principle of diagnosis by residual and thresholds is based on verifying that the residuals belong to certain sets representing state values that are consistent with healthy or faulty situations [18, 9].

In this set-based fault diagnosis area, the last two authors of this paper have proposed in recent years a new method based on the concepts of *invariant sets* and *ultimate bounds* [14, 20, 13, 5]. The main feature of this method is that it guarantees fault detection and diagnosis exploiting the fact that the residuals converge to these sets and remain inside them indefinitely provided that there are no changes in the fault situation. This methodology treats disturbances and other sources of uncertainty in a *deterministic* way, assuming only that the disturbances are bounded, without taking into account that they may follow some probabilistic distribution.

On the other hand, in many applications of control systems theory it is more appropriate to represent disturbances by unbounded signals, such as Gaussian white noise. In these cases, ultimate bounds and invariant sets cannot be obtained using traditional deterministic definitions [3]. Motivated by this limitation, we have proposed in [11, 12] the novel concepts of *probabilistic ultimate bound* and *probabilistic invariant sets*. These definitions extend the deterministic concepts of invariance and ultimate boundedness to the stochastic case by considering that the state "belongs in probability" to certain sets; thus they allow the treatment of stochastic disturbances with more general distributions, including the ubiquitous Gaussian white noise.

A first approach for the usage of probabilistic sets for fault diagnosis was presented in [17]. However, that preliminary work did not consider a reconfiguration scheme.

In this paper, following the fault diagnosis and reconfiguration strategy based on deterministic sets developed in [5], we extend the fault diagnosis mechanism presented in [17] and propose a control reconfiguration scheme. In consequence, we propose an actuator fault tolerant control strategy based on probabilistic ultimate bounds so that it is possible to consider the presence of unbounded Gaussian white noise.

In the proposed scheme, faults are detected and diagnosed when the residuals remain for some time in certain probabilistic sets. After a fault is diagnosed, the control scheme is reconfigured to take into account the corresponding actuator failure and preserve certain closed loop features. We show that our strategy can detect and diagnose the different faults in the different control configurations with an arbitrarily small probability of misdetection.

The paper is organized as follows: Section 2 describes the deterministic scheme proposed in [5] and it recalls the concepts of continuous time probabilistic ultimate bounds presented in [11, 12]. Then, Section 3 presents the proposed scheme and it explains its components. In Section 4, we compute the probabilistic ultimate bounds obtained for each fault occurrence under each fault configuration and then we develop a diagnosis technique and a reconfiguration scheme based on these sets. Finally, Section 5 illustrates the results with a numerical example.

2. Background

In this section we first revisit a deterministic fault tolerant control strategy on which our work is based. Then, we recall the definition and some properties of Probabilistic Ultimate Bounds.

2.1. Fault Tolerant Control Based on Set Separation

The fault tolerant control strategy proposed in this work is inspired in the deterministic scheme introduced in [5] which is depicted in Figure 1.

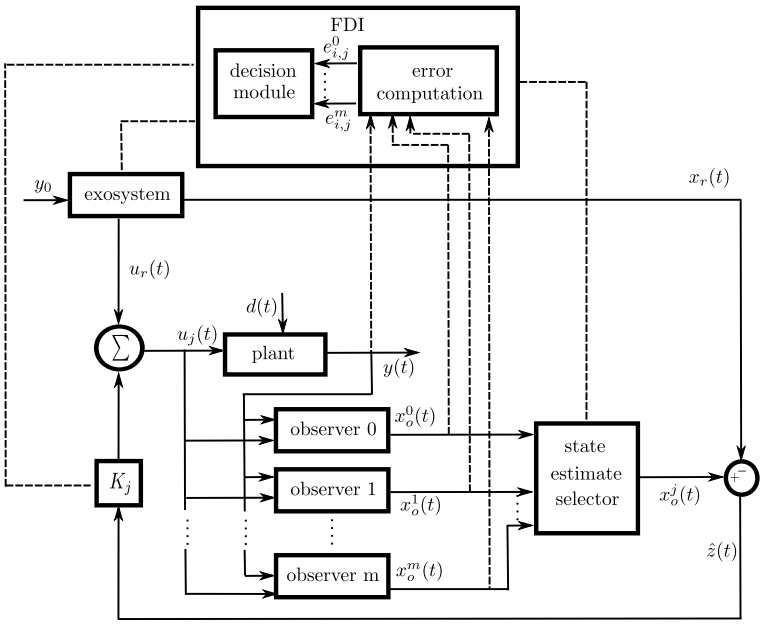

Figure 1: Scheme proposed in [5].

The scheme is formed by the plant (where the actuator faults can occur), a bank of observers, a state–feedback controller, an *exosystem* or reference system and a fault detection and isolation (FDI) module. This FDI module diagnoses the actuator faults and reconfigures the reference system, the controller and the observer bank, accordingly. The reconfiguration process consists in selecting the appropriate stabilizing controller from a bank of control laws.

The bank of observers provides a state estimation for the different fault situations. The controller uses the state estimation from the observer that matches the diagnosed fault situation, and a reference signal, generated by the exosystem, to be tracked by the plant trajectories.

The FDI module detects and isolates the current fault based on pre-computed invariant sets towards which certain estimation errors, which are used as residuals, converge. These sets are computed for each considered fault situation, and for each possible fault configuration.

A key property for the correct fault diagnosis in this scheme is the separation of the sets that characterize the healthy operation from those that characterize each faulty situation.

The main limitation of the scheme as initially conceived in [5] is that the invariant sets depend on the boundedness of the disturbances. In the case of unbounded noise, these sets do not exist.

2.2. Probabilistic Ultimate Bounds

We consider a continuous-time LTI system given by the following stochastic differential equation

$$\mathrm{d}x(t) = Ax(t)\mathrm{d}t + \mathrm{d}w(t) \tag{1}$$

with $x(t), w(t) \in \mathbb{R}^n$. We assume that A is a Hurwitz matrix, i.e., all its eigenvalues have strictly negative real part, and that the disturbance vector $w(t)$ is a stochastic process whose increments are uncorrelated with zero mean values. In particular, we will assume a Gaussian distribution, in which case the disturbance is a Wiener process.

In the remainder of this section we recall some of the concepts introduced and developed in our previous work [11, 12].

Definition 1 (Probabilistic Ultimate Bounds [11, 12])**.** *Let $0 < p \leq 1$ and let $S \subset \mathbb{R}^n$. We say that S is a probabilistic ultimate bound (PUB) with probability p for system* (1) *if for every initial state $x(t_0) = x_0 \in \mathbb{R}^n$ there exists $T = T(x_0) \in \mathbb{R}$ such that the probability $\Pr[x(t) \in S] \geq p$ for each $t \geq t_0 + T$.*

When the disturbance $w(t)$ is generated by a Gaussian process, a PUB with probability p for system (1) can be computed as follows

- First, given the probability p, such that $0 < p < 1$, we define n parameters $\tilde{p}_i \in (0, 1)$ such that
$$\sum_{i=1}^{n} \tilde{p}_i = 1 - p.$$
- Then, we compute
$$b_i \triangleq \sqrt{2[\Sigma_x]_{i,i}}\mathrm{erf}^{-1}(1 - \tilde{p}_i); \;\; i = 1, \ldots, n, \tag{2}$$
where Σ_x is the solution of the Lyapunov equation
$$A\Sigma_x + \Sigma_x A^T = -\Sigma_w, \tag{3}$$
with $\Sigma_w dt$ the incremental covariance matrix of $w(t)$, and erf is the *error function*: $\mathrm{erf}(z) \triangleq \frac{2}{\sqrt{\pi}} \int_0^z e^{-\zeta^2} d\zeta$.

Then, according to Theorem 16 in [12], any set of the form

$$S = \{x : |x_i| \leq b_i + \varepsilon; \; i = 1, \ldots, n\}$$

for any $\varepsilon > 0$, is a probabilistic ultimate bound for system (1) with probability p.

We observe that for the non Gaussian case, Eq.(2) is replaced by a different expression derived from Chebyshev's inequality (see details in [12]).

3. Proposed Scheme

In this section, we describe the fault tolerant control scheme. Following the idea of [5], Figure 2 shows our proposed scheme and its constitutive parts are explained in the following subsections.

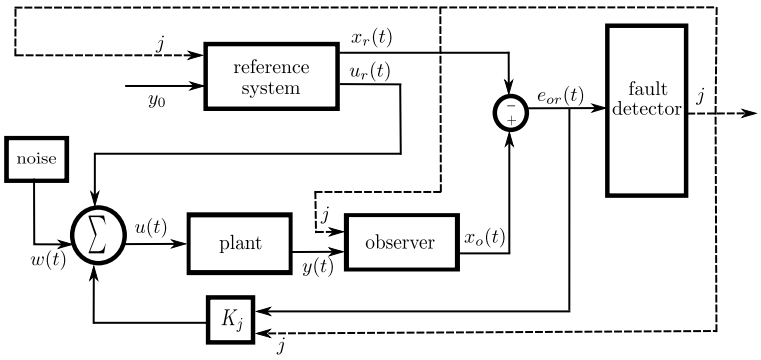

Figure 2: Proposed scheme.

In this scheme, a control strategy is designed to ensure that the plant tracks the dynamics of a reference system under all considered actuator fault scenarios. This control uses a single observer that provides state estimates to implement a state feedback law. Indeed, the main structural difference from the scheme of [5] is that the bank of (fixed-parameter) observers is replaced by a single observer, adaptable to the diagnosed fault situation. The state of the observer and the state of the reference system are compared by the FDI module to determine the possible presence of faults. The FDI principle, to be described later, uses probabilistic ultimate bounds and their properties to diagnose faults. Once a fault has been detected and isolated, a reconfiguration is made by adjusting the reference system, the controller feedback gain, and the observer parameters, to match the diagnosed fault situation. Then, the diagnosis process is restarted after certain time.

3.1. Plant Model

The plant is modeled by an LTI perturbed system described by

$$\begin{aligned} \mathrm{d}x_p(t) &= Ax_p(t)\mathrm{d}t + BPu(t)\mathrm{d}t + F\mathrm{d}w(t), \\ y_p(t) &= Cx_p(t). \end{aligned} \tag{4}$$

where $x_p(t) \in \mathbb{R}^n$ is the system state, $u(t) \in \mathbb{R}^m$ is the control input, $w(t)$ is a Wiener process with incremental covariance matrix $\Sigma_w dt$, $y_p(t) \in \mathbb{R}^s$ is the system output, and A, B, C and F are constant matrices of suitable dimensions. Matrix P is used to model the occurrence of actuator faults.

$$P \triangleq \mathrm{diag}\{P_1, P_2, \cdots, P_m\}, \;\; 0 \leq P_k \leq 1,$$

Here, $P_k = 1$ represents the absence of fault in the k-th actuator, whereas $P_k = 0$ models the k-th actuator outage. Any value $0 < P_k < 1$ represents a partial fault in the k–th actuator.

Thus, in the absence of faults, P is the identity matrix. We consider a finite number of possible fault situations represented by $P = P^i$ for $i = 0, \ldots, q$, with P^i defined as follows:

$$\begin{aligned} P^0 &= I, \\ P^i &= \mathrm{diag}\{P_1^i, P_2^i, \cdots, P_m^i\}. \end{aligned} \tag{5}$$

In the sequel we will assume that system (4) is stabilizable for all possible values of $P = P^i$, with $i = 0, \cdots, q$, as defined in (5).

In order to emphasize the current system fault situation (determined by matrix $P = P^i$) we will employ the following notation for the system dynamics:

$$\begin{aligned} \mathrm{d}x_p(t) &= Ax_p(t)\mathrm{d}t + BP^i u(t)\mathrm{d}t + F\mathrm{d}w(t), \\ y_p(t) &= Cx_p(t). \end{aligned} \tag{6}$$

3.2. Exosystem for Reference Tracking

The reference system computes the input and state reference trajectories, $u_r(t)$ and $x_r(t)$. Under the j–th fault situation (for $j = 0, \ldots, q$), these reference trajectories satisfy the disturbance-free model equations

$$\begin{aligned} \mathrm{d}x_r(t) &= Ax_r(t)\mathrm{d}t + BP^j u_r(t)\mathrm{d}t, \\ y_r(t) &= Cx_r(t). \end{aligned} \tag{7}$$

where the input

$$u_r(t) = \bar{u}_r^j + \Delta u_r(t) \tag{8}$$

is computed by some control laws that ensure that $y_r(t)$ exponentially tracks the constant output reference y_0. The signal y_0 is a reference value that we ultimately wish the plant output $y_p(t)$ in (6) to track under every possible fault situation.

The input reference $u_r(t)$ is composed of a constant part $\bar{u}_r^j$ and a varying part $\Delta u_r(t)$. We will assume that $\lim_{t\to\infty} u_r(t)$ exists and hence take $\bar{u}_r^j \doteq \lim_{t\to\infty} u_r(t)$; this then implies $\lim_{t\to\infty} \Delta u_r(t) = 0$.

3.3. Plant State Observer

In order to obtain an estimation of the plant state, which will be used to implement the control and to detect and isolate actuator faults, we propose an observer that is adapted to the diagnosed fault situation. Namely, under the diagnosis of the j–th fault the observer dynamics is characterized by

$$\mathrm{d}x_o(t) = Ax_o(t)\mathrm{d}t + BP^j u(t)\mathrm{d}t + L(y_p(t) - Cx_o(t))\mathrm{d}t, \tag{9}$$

for $j = 0, \ldots, q$.

3.4. Feedback Control Laws

The proposed control input in (6) is based on the observer state (9) and the reference signals (7), (8), and takes the form

$$u(t) = K_j(x_o(t) - x_r(t)) + u_r(t), \tag{10}$$

where K_j represents the state feedback gain designed for the j–th fault scenario ($j = 0, \ldots, q$).

4. Main Result

In this section, the proposed actuator FDI and reconfiguration scheme is presented. Towards that goal, we first derive the closed-loop dynamics of the scheme described in the previous section and then we compute the probabilistic ultimate bounds obtained for each fault occurrence under each fault configuration. The FDI mechanism, based on filtering some indicator functions of the probabilistic ultimate bound sets, is then presented.

4.1. Closed-loop Dynamics

In the sequel, we shall consider that the system is configured for the j–th fault situation but the plant is under the occurrence of the i–th fault (i and j might be different from each other).

Defining the state estimate tracking error, which will be used as residual, as

$$e_{or}(t) \triangleq x_o(t) - x_r(t), \tag{11}$$

the control law (10) can be written as

$$u(t) = K_j e_{or}(t) + u_r(t). \tag{12}$$

Also, we define the state estimation error as

$$e_{po}(t) \triangleq x_p(t) - x_o(t). \tag{13}$$

Considering the closed-loop system with Eq.(12), and using Eqs., (4), (7) and (9), the state estimate tracking error dynamics $e_{or}(t)$ can be written as

$$\begin{aligned} \mathrm{d}e_{or}(t) &= \mathrm{d}x_o - \mathrm{d}x_r = \\ &= (A + BP^j K_j)e_{or}(t)\mathrm{d}t + LCe_{po}(t)\mathrm{d}t. \end{aligned} \tag{14}$$

Similarly, using Eqs.(4) and (9), the state estimation error $e_{po}(t)$ dynamics can be written as

$$\begin{aligned} \mathrm{d}e_{po}(t) &= \mathrm{d}x_p - \mathrm{d}x_o = \\ &= (A - LC)e_{po}(t)\mathrm{d}t + B(P^i - P^j)K_j e_{or}(t)\mathrm{d}t + \\ &+ B(P^i - P^j)u_r(t)\mathrm{d}t + F\mathrm{d}w. \end{aligned} \tag{15}$$

Then, combining Eqs.(14) and (15), and defining

$$e(t) \triangleq \begin{bmatrix} e_{or}(t) \\ e_{po}(t) \end{bmatrix}, \tag{16}$$

the following system is obtained:

$$\begin{aligned} de(t) = &\begin{bmatrix} A + BP^j K_j & LC \\ B(P^i - P^j)K_j & A - LC \end{bmatrix} e(t)\mathrm{d}t + \\ &+ \begin{bmatrix} 0 \\ B(P^i - P^j) \end{bmatrix} u_r(t)\mathrm{d}t + \begin{bmatrix} 0 \\ F \end{bmatrix} \mathrm{d}w(t). \end{aligned} \tag{17}$$

Remark 1. *In order to ensure the stability of the closed-loop system* (17) *under every considered fault situation and control configuration, the feedback control gains K_j and the observer matrix L in* (9) *should be such that the closed-loop matrices*

$$A_\ell^{i,j} = \begin{bmatrix} A + BP^j K_j & LC \\ B(P^i - P^j)K_j & A - LC \end{bmatrix} \tag{18}$$

for $i = 0, \ldots, q$ and $j = 0, \ldots, q$, are Hurwitz.

4.2. PUB Computation

Assuming that the system is under the i–th fault situation ($i \in \{0, \ldots, q\}$), and configured assuming the j–th fault situation, Eq. (17) can be rewritten as

$$\mathrm{d}e(t) = \left[A_\ell^{i,j} e(t) + B_\ell^{i,j} u_r(t)\right] \mathrm{d}t + G\mathrm{d}w(t), \tag{19}$$

with $A_\ell^{i,j}$ defined in Eq. (18) and with

$$B_\ell^{i,j} \triangleq \begin{bmatrix} 0 \\ B(P^i - P^j) \end{bmatrix}, \; G \triangleq \begin{bmatrix} 0 \\ F \end{bmatrix}. \tag{20}$$

Then, using the constant input reference term in (8) to define

$$\bar{e}^{i,j} = \begin{bmatrix} \bar{e}_{or}^{i,j} \\ \bar{e}_{po}^{i,j} \end{bmatrix} \triangleq -(A_\ell^{i,j})^{-1} B_\ell^{i,j} \bar{u}_r^j, \tag{21}$$

and considering the change of coordinates

$$\tilde{e}^{i,j}(t) = e(t) - \bar{e}^{i,j},$$

the system in (19), recalling that $u_r(t) = \bar{u}_r^j + \Delta u_r(t)$, can be expressed as

$$\mathrm{d}\tilde{e}^{i,j}(t) = A_\ell^{i,j} \tilde{e}^{i,j}(t)\mathrm{d}t + G\mathrm{d}w(t) + B_\ell^{i,j} \Delta u_r(t)\mathrm{d}t. \tag{22}$$

Notice that the last term goes to zero since $\lim_{t\to\infty} \Delta u_r(t) = 0$. Thus, it can be ignored for the PUB computation.

According to Remark 1, matrix $A_\ell^{i,j}$ in (22) is Hurwitz and given that $w(t)$ is a Wiener process with incremental covariance $\Sigma_w dt$, we can use Theorem 16 in [12] to compute the ultimate bound, for $0 < p < 1$, as (see Section 2.2)

$$\tilde{S}^{i,j} = \{\tilde{e}^{i,j} \in \mathbb{R}^{2n} : |\tilde{e}_k^{i,j}| \leq b_k^{i,j} + \varepsilon; \; k = 1, \ldots, 2n\} \tag{23}$$

where

$$b_k^{i,j} \triangleq \sqrt{2[\Sigma_x^{i,j}]_{k,k}} \mathrm{erf}^{-1}(1 - \tilde{p}_k); \quad k = 1, \ldots, 2n \tag{24}$$

with $\tilde{p}_k \in (0, 1)$ such that

$$\sum_{k=1}^{2n} \tilde{p}_k = 1 - p, \tag{25}$$

and where $\Sigma_x^{i,j}$ is the solution of Lyapunov's equation.

$$A_\ell^{i,j} \Sigma_x^{i,j} + \Sigma_x^{i,j} (A_\ell^{i,j})^T = -G\Sigma_w G^T.$$

In the original coordinates, $e(t)$, the set $\tilde{S}^{i,j}$ becomes

$$S^{i,j} = \{e \in \mathbb{R}^{2n} : |e_k - \bar{e}_k^{i,j}| \leq b_k^{i,j} + \varepsilon; \; k = 1, \ldots, 2n\}, \tag{26}$$

which represents the PUB for system (17) under the i–th fault situation considering the j–th configuration.

4.3. Fault Diagnosis

The basic idea to detect the occurrence of a fault is to check if the error $e(t)$ evolves inside a PUB set $S^{i,j}$. However, only the component $e_{or}(t)$ (i.e., the state estimate tracking error) can be measured. Thus, we will be interested in the following PUB sets:

$$S^{i,j}_{or} = \{e_{or} \in \mathbb{R}^n : |e_{or} - \bar{e}^{i,j}_{or}| \preceq b^{i,j}_{or} + \bar{\varepsilon}\}, \tag{27}$$

where $\bar{\varepsilon} \triangleq [\varepsilon, \ldots, \varepsilon]^T$, and the symbol "$\preceq$" denotes the elementwise inequality, and according to Eq.(24),

$$b^{i,j}_{or} \triangleq \left[b^{i,j}_1, \ldots, b^{i,j}_n\right]^T \tag{28}$$

Then, the fault diagnosis strategy is based on verifying the convergence of the residual $e_{or}(t)$ to the PUB sets $S^{i,j}_{or}$. The following lemma establishes a basic property of these sets.

Lemma 1. *Given a configuration $j \in \{0, \ldots, q\}$, we assume that the system is in the i–th fault situation from time t^i_f. Then, given $p \in (0, 1)$, there exists $T > 0$ such that the probability* $\Pr[e_{or}(t) \in S^{i,j}_{or}] \geq p$, $\forall t \geq t^i_f + T$.

Proof. $S^{i,j}$ is a PUB with probability p, then for every initial state $e(t^i_f) = e_0 \in \mathbb{R}^{2n}$, there exists $T = T(e_0)$ such that the probability

$$\Pr[e(t) \in S^{i,j}] \geq p, \;\; \forall t \geq t^i_f + T.$$

On the other hand, if $e(t) \in S^{i,j}$ then $e_{or}(t) \in S^{i,j}_{or}$, and hence

$$\Pr[e_{or}(t) \in S^{i,j}_{or}] \geq \Pr[e(t) \in S^{i,j}] \geq p, \;\; \forall t \geq t^i_f + T.$$

□

In a deterministic context, assuming that the ultimate bound sets are disjoint, the fact that $e_{or}(t)$ converges to $S^{i,j}_{or}$ implies that the i–th fault has occurred. This is in fact the idea used in [5] to perform the fault diagnosis.

However, in the probabilistic case, $e_{or}(t)$ may reach a set without the occurrence of the corresponding fault. Also, $e_{or}(t)$ may leave the corresponding PUB set with certain probability. Thus, to decide that a fault has occurred we need to check that the residual belongs to the corresponding set most of the time (i.e., in an 'average' sense, according to the probability p of the PUB set).

In order to take into account this remark, the fault diagnosis strategy relies on filtering the indicator functions of each set. The following theorem shows that this idea can reduce the probability of errors in the fault detection to an arbitrary small value.

Theorem 1. *Suppose the closed-loop system is under a configuration $j \in \{0, \ldots, q\}$, and the plant is under the i–th fault situation from time t^i_f. Assume the PUB sets are disjoint, that is, $S^{i,j}_{or} \cap S^{k,j}_{or} = \emptyset$, for $i \neq k$, and we define*

$$d^{k,j}(t) \triangleq \mathbf{1}_{S^{k,j}_{or}}(e_{or}(t)); \;\; k = 0, \ldots, q, \tag{29}$$

where $\mathbf{1}_S$ is the indicator function of set S. In addition, we consider the low–pass filters defined by the differential equations

$$\dot{d}^{k,j}_f(t) = -\lambda \left[d^{k,j}_f(t) - d^{k,j}(t)\right]; \;\; k = 0, \ldots, q. \tag{30}$$

with initial states $d_f^{k,j}(t_f^i) \in [0,1]$.

Then, if the PUB probability $p > p^*$ *and the filter parameter* $\lambda > 0$ *is sufficiently small, given* $\hat{\delta} > 0$*, there exists* $\hat{T}^{i,j} > 0$ *such that*

$$\Pr[d_f^{i,j}(t) < d_f^{k,j}(t)] < \hat{\delta} \quad \forall t > \hat{T}^{i,j},$$

where $p^* \approx 0.8133$ *is the solution of*

$$\sup_{\gamma>0} \left[1 - 2\mathrm{e}^{-\gamma} - 2\gamma(1-p)\right] = 0. \tag{31}$$

Proof. Given [1] $t_0 >> t_f^i$, for every $\tau \geq t_0$, $e_{or}(\tau)$ is a uniformly ergodic stationary Gaussian process. Let $C^{i,j} \triangleq \mathbb{R}^n \backslash S_{or}^{i,j}$ be the complement of $S_{or}^{i,j}$ and take $t_1 \geq t_0$. Then, it results that

$$\frac{1}{t}\int_{t_1}^{t_1+t} \mathbf{1}_{C^{i,j}}(e_{or}(\tau))\mathrm{d}\tau \underset{t\to\infty}{\overset{p}{\to}} \mathrm{E}[\mathbf{1}_{C^{i,j}}(e_{or}(t_1))]$$

uniformly in t_1. In particular, given $\delta > 0$, and $\epsilon > 0$, there exists $T > 0$ independent of t_1 such that $\forall\, t > T$,

$$\Pr\left[\frac{1}{t}\int_{t_1}^{t_1+t} \left[1 - d^{i,j}(\tau)\right]\mathrm{d}\tau \geq \mathrm{E}[\mathbf{1}_{C^{i,j}}(e_{or}(t_1))] + \epsilon\right] < \delta,$$

where we used the fact that $\mathbf{1}_{C^{i,j}}(e_{or}(\tau)) = 1 - d^{i,j}(\tau)$.

Since $\mathrm{E}[\mathbf{1}_{C^{i,j}}(e_{or}(t_1))] = \Pr[e_{or}(t_1) \notin S_{or}^{i,j}] = 1 - \Pr[e_{or}(t_1) \in S_{or}^{i,j}] \leq 1 - p$ (Lemma 1 and footnote 1), then, for every $t > T$,

$$\Pr\left[\frac{1}{t}\int_{t_1}^{t_1+t} \left[1 - d^{i,j}(\tau)\right]\mathrm{d}\tau \geq 1 - p + \epsilon\right] < \delta,$$

Then, given $\lambda > 0$,

$$\Pr\left[\lambda\int_{t_1}^{t_1+t} \left[1 - d^{i,j}(\tau)\right]\mathrm{d}\tau \geq \lambda t(1 - p + \epsilon)\right] < \delta. \tag{32}$$

Notice that, provided that $\tau < t + t_1$, it results that $0 < \mathrm{e}^{-\lambda(t+t_1-\tau)} < 1$. Also, since $d^{i,j} \in \{0,1\}$ it results that $[1 - d^{i,j}(\tau)] \geq 0$, $\forall\tau$. Thus, from Eq.(32) we obtain

$$\Pr\left[\lambda\int_{t_1}^{t_1+t} \left[1 - d^{i,j}(\tau)\right]\mathrm{e}^{-\lambda(t+t_1-\tau)}\mathrm{d}\tau > \lambda t(1 - p + \epsilon)\right] < \delta \tag{33}$$

On the other hand, solving Eq.(30) with $k = i$, we obtain

$$\begin{aligned} d_f^{i,j}(t_1 + t) &= \mathrm{e}^{-\lambda t} d_f^{i,j}(t_1) + \lambda\int_{t_1}^{t_1+t} \mathrm{e}^{-\lambda(t+t_1-\tau)} d^{i,j}(\tau)\mathrm{d}\tau = \\ &= \mathrm{e}^{-\lambda t} d_f^{i,j}(t_1) + (1 - \mathrm{e}^{-\lambda t}) - \lambda\int_{t_1}^{t_1+t} \mathrm{e}^{-\lambda(t+t_1-\tau)}[1 - d^{i,j}(\tau)]\mathrm{d}\tau. \end{aligned}$$

[1] In particular t_0 has to be such that $t_0 - t_f^i$ is greater than the time such that $e_{or}(t)$ is in the set $S_{or}^{i,j}$ with probability greater than or equal to p, according to Lemma 1 (such a time is a function of the initial state $e_{or}(t_f^i)$—cf. Definition 1).

Using the above in Eq.(33) and the fact that $d_f^{i,j}(t_f^i) \geq 0 \Rightarrow d_f^{i,j}(t_1) \geq 0$, it results that

$$\Pr\left[d_f^{i,j}(t_1+t) < 1 - \mathrm{e}^{-\lambda t} - \lambda t(1-p+\epsilon)\right] < \delta \tag{34}$$

for every $t > T$. Now, solving Eq.(30) with $k \neq i$, and taking into account that $d_f^{k,j}(t_f^i) \leq 1 \Rightarrow d_f^{k,j}(t_1) \leq 1$ and $S_{or}^{i,j} \cap S_{or}^{k,j} = \emptyset \Rightarrow d^{k,j}(\tau) \leq 1 - d^{i,j}(\tau)$, it follows that

$$\begin{aligned} d_f^{k,j}(t_1+t) &= \mathrm{e}^{-\lambda t} d_f^{k,j}(t_1) + \lambda \int_{t_1}^{t_1+t} \mathrm{e}^{-\lambda(t+t_1-\tau)} d^{k,j}(\tau)\mathrm{d}\tau \\ &\leq \mathrm{e}^{-\lambda t} + \lambda \int_{t_1}^{t_1+t} \mathrm{e}^{-\lambda(t+t_1-\tau)}[1 - d^{i,j}(\tau)]\mathrm{d}\tau \\ &\leq \mathrm{e}^{-\lambda t} + \lambda \int_{t_1}^{t_1+t} [1 - d^{i,j}(\tau)]\mathrm{d}\tau \end{aligned}$$

Taking into account the last inequality and Eq.(32), it results that

$$\Pr\left[d_f^{k,j}(t_1+t) > \mathrm{e}^{-\lambda t} + \lambda t(1-p+\epsilon)\right] < \delta. \tag{35}$$

From Eqs.(34)–(35) and simple probabilistic properties [2] we obtain

$$\Pr\left[d_f^{i,j}(t_1+t) - d_f^{k,j}(t_1+t) < 1 - 2\mathrm{e}^{-\lambda t} - 2\lambda t(1-p+\epsilon)\right] < 2\delta,$$

for any $t_1 \geq t_0$ and for every $t > T$.

Notice that a condition $\alpha(t_1+t) > \beta(t)$ for every $t_1 \geq t_0$ and for every $t > T$ implies that $\alpha(t_0+t) > \sup_{\tau>T}\beta(\tau)$ for every $t \geq T_s \triangleq \arg\sup_{\tau>T}\beta(\tau)$, and, hence $\Pr[\alpha(t_1+t) < \beta(t)] \geq \Pr[\alpha(t_0+t) < \sup_{\tau>T}\beta(\tau)]$. Using this reasoning on the last inequality, it follows that

$$\Pr\left[d_f^{i,j}(t_0+t) - d_f^{k,j}(t_0+t) < \sup_{\tau>T}[1 - 2\mathrm{e}^{-\lambda\tau} - 2\lambda\tau(1-p+\epsilon)]\right] < 2\delta,$$

for every $t \geq T_s^{i,j}$. Let $\gamma \triangleq \lambda\tau$,

$$\Pr\left[d_f^{i,j}(t_0+t) - d_f^{k,j}(t_0+t) < \sup_{\gamma>\lambda T}[1 - 2\mathrm{e}^{-\gamma} - 2\gamma(1-p+\epsilon)]\right] < 2\delta. \tag{36}$$

Let p^* be the solution of (31) and compute $\gamma^* \approx 1.6783$ such that $1 - 2\mathrm{e}^{-\gamma^*} - 2\gamma^*(1-p^*) = 0$. Thus, assuming that p and λ were chosen such that $p > p^* + \epsilon$ and $\lambda < \frac{\gamma^*}{T}$, the supremum in Eq.(36) results greater than zero and then

$$\Pr\left[d_f^{i,j}(t_0+t) < d_f^{k,j}(t_0+t)\right] < 2\delta, \ \ \forall t > T_s^{i,j}.$$

and the proof concludes taking $\hat{T}^{i,j} = t_0 + T_s^{i,j}$ and $\hat{\delta} = 2\delta$. □

[2] Given two random variables $x \in \mathbb{R}$, $y \in \mathbb{R}$, and two real numbers a, b, the events $\{(x,y) : x < a\}$, $\{(x,y) : y > b\}$ and $\{(x,y) : x + b < y + a\}$ satisfy $\{x + b < y + a\} \subset \{x < a\} \cup \{y > b\}$. Then $\Pr[x + b < y + a] \leq \Pr[x < a] + \Pr[y > b]$.

Theorem 1 shows that if the system is configured to match the j-th fault situation and at time t_f^i the i–th fault occurs, then, by applying first order filters on the indicator functions of the different sets, after some time $\hat{T}^{i,j}$, the filtered signal corresponding to the i–th fault situation has an arbitrarily small probability of becoming smaller than any other filtered signal.

Then, we can detect the i–th fault according to $i = \arg\max_k d_f^{k,j}(t)$, with an arbitrary small probability of misdetection.

According to this idea, the proposed detection scheme is depicted in Fig. 3.

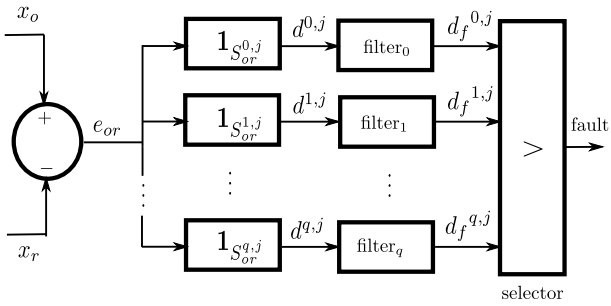

Figure 3: Proposed detection scheme.

Once the fault is detected, we must reconfigure the control as it is explained below.

4.4. Reconfiguration Scheme

In the normal operation mode (healthy or faulty) we should have $j = \arg\max_k d_f^{k,j}(t)$, i.e., the detected fault situation is equal to the current fault situation.

When this situation changes, i.e., when $j \neq i = \arg\max_k d_f^{k,j}(t)$, we shall reconfigure the scheme by taking $j = i$. After this reconfiguration step, we know that for certain time we cannot rely on the diagnosis module (Theorem 1 only ensures the correct fault detection with arbitrarily small probability of misdetection after some time $\hat{T}^{i,j}$). Thus, under the detection of the i–th fault situation at time t_d^i we proceed as follows:

- We reconfigure the control, observer and reference system according to the new fault situation by setting $j = i$.
- We wait for some time until the residual $e_{or}(t)$ arrives to the set $S_{or}^{i,i}$, where it should remain (with probability p) provided the fault situation does not change again.
- We restart the filter states according to $d_f^{i,i}(t) = 1$ and $d_f^{k,i}(t) = 0$ for $k \neq i$ so they start filtering from a state consistent with the detected current fault situation.
- We restart the diagnosis module comparing again the filter states.

Remark 2. *Notice that we only ask that the different configurations under the different fault situations are stable, i.e., that the closed loop matrices $A_\ell^{i,j}$ in* (18) *are Hurwitz. This condition alone does not ensure the stability of the switched system that results after the occurrence of arbitrary sequences of faults and reconfigurations. However, if we assume that a new change in the fault*

situation can only occur after the state arrives to the corresponding ultimate bound set, and that the subsequent reconfiguration only takes place after the state arrives to the new ultimate bound set, then a switching sequence that makes the system unstable cannot occur. This is, the state will always move (with probability) between the computed ultimate bound sets for the different fault situations and configurations.

While the last remark tells that, in practice, the configuration remains stable, the following theorem provides a formal proof that the trajectory converges (in probability) to a bounded region.

Theorem 2. *Consider the system* (19)*. Assume that matrices* $A_\ell^{i,j}$ *are Hurwitz and that the input reference signal* $u_r(t)$ *is bounded. Assume also that the switching intervals are bounded from below by a* $T > 0$ *large enough such that* $\|\mathrm{e}^{A_\ell^{i,j}t}\| < 1$ *for all* $t \geq T$ *and for all* i, j*. Then, given an arbitrary probability* $0 < p < 1$*, a bounded PUB* S *with probability* p *can be found for system* (19)*.*

Proof. Let $\tau_1, \tau_2, \cdots, \tau_j, \tau_{j+1}, \cdots$ be an arbitrary switching sequence with $\tau_1 \geq t_0 + T$, from which we build the following sequence

$$t_{k+1} = \begin{cases} \tau_j & \text{if } \tau_j \text{ is such that } t_k + T \leq \tau_j < t_k + 2T \\ t_k + T & \text{otherwise} \end{cases}$$

Notice that the sequence t_k contains the switching sequence τ_j, but it also can have more points so that

$$T \leq t_{k+1} - t_k < 2T \tag{37}$$

Let $t \in (t_k, t_{k+1}]$. Since there are no switching occurrences in that interval, the solution of Eq.(19) can be written as

$$e(t) = \mathrm{e}^{A_\ell^{i,j}(t-t_k)}e(t_k) + \int_{t_k}^{t} \mathrm{e}^{A_\ell^{i,j}(t-\tau)}B_\ell^{i,j}u_r(\tau)\mathrm{d}\tau + \int_{t_k}^{t} \mathrm{e}^{A_\ell^{i,j}(t-\tau)}G\mathrm{d}w(\tau) \tag{38}$$

Taken expectations at both sides of the solution, we get

$$\begin{aligned} E[e(t)] &= E\left[\mathrm{e}^{A_\ell^{i,j}(t-t_k)}e(t_k) + \int_{t_k}^{t} \mathrm{e}^{A_\ell^{i,j}(t-\tau)}B_\ell^{i,j}u_r(\tau)\mathrm{d}\tau + \int_{t_k}^{t} \mathrm{e}^{A_\ell^{i,j}(t-\tau)}G\mathrm{d}w(\tau)\right] \\ &= \mathrm{e}^{A_\ell^{i,j}(t-t_k)}E[e(t_k)] + \int_{t_k}^{t} \mathrm{e}^{A_\ell^{i,j}(t-\tau)}B_\ell^{i,j}u_r(\tau)\mathrm{d}\tau \end{aligned}$$

where the third term is null since the process $w(t)$ has zero mean.

Taking norm 2 on both sides of the last equation, we obtain,

$$\begin{aligned} \|E[e(t)]\| &= \left\|\mathrm{e}^{A_\ell^{i,j}(t-t_k)}E[e(t_k)] + \int_{t_k}^{t} \mathrm{e}^{A_\ell^{i,j}(t-\tau)}B_\ell^{i,j}u_r(\tau)\mathrm{d}\tau\right\| \\ &\leq \left\|\mathrm{e}^{A_\ell^{i,j}(t-t_k)}\right\| \|E[e(t_k)]\| + \int_{t_k}^{t} \left\|\mathrm{e}^{A_\ell^{i,j}(t-\tau)}B_\ell^{i,j}\right\| \|u_r(\tau)\| \,\mathrm{d}\tau \end{aligned} \tag{39}$$

Let us define

$$\gamma \triangleq \max_{i,j} \sup_{\tau \geq T} \|\mathrm{e}^{A_\ell^{i,j}\tau}\|; \quad \upsilon \triangleq \max_{i,j} \sup_{\tau \geq 0} \|\mathrm{e}^{A_\ell^{i,j}\tau}\| \tag{40}$$

and notice that, by assumption, the fact that $\tau \geq T$ implies $\|\mathrm{e}^{A_\ell^{i,j}\tau}\| < 1$ and then $\gamma < 1$. Also, since $A_\ell^{i,j}$ are Hurwitz matrices, υ is bounded by some constant.

Define also

$$\eta \triangleq \max_{i,j} \sup_{t\geq 0} \int_0^t \left\| \mathrm{e}^{A_\ell^{i,j}\tau} B_\ell^{i,j} \right\| \bar{u}_r \mathrm{d}\tau \tag{41}$$

where $\bar{u}_r$ is an upper bound for the bounded signal $\|u_r(\tau)\|$ for all $\tau \geq t_0$. Notice that η is bounded due to the fact that $A_\ell^{i,j}$ are Hurwitz matrices.

Using Eqs.(40)–(41) in inequality (39) for $t = t_{k+1}$ we obtain,

$$\|E[e(t_{k+1})]\| \leq \gamma \|E[e(t_k)]\| + \eta \tag{42}$$

Then the sequence $\|E[e(t_k)]\|$ is bounded from above by a monotonic sequence that converges to $\frac{\eta}{1-\gamma}$. Hence, we have

$$\lim_{k\to\infty} \|E[e(t_{k+1})]\| \leq \frac{\eta}{1-\gamma} \tag{43}$$

and then, given $\varepsilon > 0$ there exists K_ε such that

$$\|E[e(t_k)]\| \leq \frac{\eta}{1-\gamma} + \varepsilon, \quad \forall k \geq K_\varepsilon. \tag{44}$$

Using now Eqs.(41) and (44) in inequality (39), we obtain

$$\|E[e(t)]\| \leq \left\| \mathrm{e}^{A_\ell^{i,j}(t-t_k)} \right\| \left(\frac{\eta}{1-\gamma} + \varepsilon \right) + \eta \leq \upsilon \left(\frac{\eta}{1-\gamma} + \varepsilon \right) + \eta \triangleq \mu_\varepsilon \tag{45}$$

for all $t > t_k$ with $k \geq K_\varepsilon$, where we used the fact that $\left\| \mathrm{e}^{A_\ell^{i,j}t} \right\| \leq \upsilon$ for $t \geq 0$ according to Eq.(40).

Notice that $t_{k+1} - t_k < 2T$ in Eq.(37) implies that $t_k < t_0 + 2kT$. Then, defining

$$T_\varepsilon \triangleq t_0 + 2K_\varepsilon T \tag{46}$$

the condition $t \geq T_\varepsilon$ implies that $t > t_k$ with $k = K_\varepsilon$, and

$$\|E[e(t)]\| \leq \mu_\varepsilon \tag{47}$$

for all $t \geq T_\varepsilon$.

The covariance of $e(t)$ in Eq.(38) is defined as $\Sigma_e(t) = E[(e(t) - E[e(t)])(e(t) - E[e(t)])^T]$.

Notice that the term $\int_{t_k}^t \mathrm{e}^{A_\ell^{i,j}(t-\tau)} B_\ell^{i,j} u_r(\tau)\mathrm{d}\tau$ of Eq.(38) is deterministic, so it does not contribute to the covariance, which can be then computed as $\Sigma_e(t) = \Sigma_z(t) = E[(z(t) - E[z(t)])(z(t) - E[z(t)])^T]$ with

$$z(t) = \mathrm{e}^{A_\ell^{i,j}(t-t_k)} z(t_k) + \int_{t_k}^t \mathrm{e}^{A_\ell^{i,j}(t-\tau)} G \mathrm{d}w(\tau)$$

and $z(t_k) = e(t_k)$. This last expression is the solution of a linear stochastic differential equation whose variance, following Eq.(6.9) of [1], is given by

$$\Sigma_z(t) = \mathrm{e}^{A_\ell^{i,j}(t-t_k)} \Sigma_z(t_k) \mathrm{e}^{A_\ell^{i,j\,T}(t-t_k)} + \int_{t_k}^t \mathrm{e}^{A_\ell^{i,j}(t-\tau)} G \Sigma_w G^T \mathrm{e}^{A_\ell^{i,j\,T}(t-\tau)} \mathrm{d}\tau$$

and then,

$$\Sigma_e(t) = \mathrm{e}^{A_\ell^{i,j}(t-t_k)}\Sigma_e(t_k)\mathrm{e}^{A_\ell^{i,j\,T}(t-t_k)} + \int_{t_k}^{t} \mathrm{e}^{A_\ell^{i,j}(t-\tau)}G\Sigma_w G^T \mathrm{e}^{A_\ell^{i,j\,T}(t-\tau)}\mathrm{d}\tau$$

Taking norm 2 on both sides, it results

$$\begin{aligned}
\|\Sigma_e(t)\| &\leq \left\|\mathrm{e}^{A_\ell^{i,j}(t-t_k)}\Sigma_e(t_k)\mathrm{e}^{A_\ell^{i,j\,T}(t-t_k)}\right\| + \left\|\int_{t_k}^{t} \mathrm{e}^{A_\ell^{i,j}(t-\tau)}G\Sigma_w G^T \mathrm{e}^{A_\ell^{i,j\,T}(t-\tau)}\mathrm{d}\tau\right\| \\
&\leq \left\|\mathrm{e}^{A_\ell^{i,j}(t-t_k)}\right\|^2 \|\Sigma_e(t_k)\| + \int_{t_k}^{t} \left\|\mathrm{e}^{A_\ell^{i,j}(t-\tau)}G\Sigma_w G^T \mathrm{e}^{A_\ell^{i,j\,T}(t-\tau)}\right\| \mathrm{d}\tau \\
&\leq \left\|\mathrm{e}^{A_\ell^{i,j}(t-t_k)}\right\|^2 \|\Sigma_e(t_k)\| + \delta \qquad (48)
\end{aligned}$$

where

$$\delta \triangleq \max_{i,j}\sup_{t\geq 0}\int_0^t \left\|\mathrm{e}^{A_\ell^{i,j}\tau}G\Sigma_w G^T \mathrm{e}^{A_\ell^{i,j\,T}\tau}\right\| \mathrm{d}\tau \qquad (49)$$

Using Ineq.(48) for $t = t_{k+1}$ we obtain

$$\|\Sigma_e(t_{k+1})\| \leq \left\|\mathrm{e}^{A_\ell^{i,j}(t_{k+1}-t_k)}\right\|^2 \|\Sigma_e(t_k)\| + \delta \leq \gamma^2 \|\Sigma_e(t_k)\| + \delta \qquad (50)$$

If we consider that the initial state $e(t_0)$ is deterministic (i.e. $\Sigma_e(t_0) = 0$), the last equation says that the sequence $\|\Sigma_e(t_k)\|$ is bounded from above by a monotonically growing sequence that converges to the value $\frac{\delta}{1-\gamma^2}$. Thus,

$$\|\Sigma_e(t_k)\| \leq \frac{\delta}{1-\gamma^2} \qquad (51)$$

for all $k \geq 0$, and then, using Eq.(48) again we obtain

$$\|\Sigma_e(t)\| \leq \left\|\mathrm{e}^{A_\ell^{i,j}(t-t_k)}\right\|^2 \|\Sigma_e(t_k)\| + \delta \leq \upsilon^2 \frac{\delta}{1-\gamma^2} + \delta \triangleq \sigma^2 \qquad (52)$$

showing that the covariance of $e(t)$ is bounded by σ^2 for all $t \geq t_0$.

Let $e_i(t)$ be the i–th component of $e(t)$. Recalling that $\|E[e(t)]\| \leq \mu_\varepsilon$ for $t \geq T_\varepsilon$ and $\|\Sigma_e(t)\| \leq \sigma^2$, and that $e(t)$ is $2n$ dimensional (cf.(16)), we have

$$|E[e_i(t)]| \leq \mu_\varepsilon, \quad \forall t \geq T_\varepsilon$$

and

$$[\Sigma_e(t)]_{i,i} \leq \|\Sigma_e(t)\|_\infty \leq \|\Sigma_e(t)\|\sqrt{2n} \leq \sigma^2\sqrt{2n}$$

Then, for $t \geq T_\varepsilon$, given $\tilde{p}_i$ such that $0 < \tilde{p}_i < 1$, we obtain

$$\begin{aligned}
\Pr\left[|e_i(t)| \geq \mu_\varepsilon + \sigma\sqrt[4]{\frac{2n}{\tilde{p}_i^2}}\right] &\leq \Pr\left[|e_i(t)| \geq |E[e_i(t)]| + \sqrt{[\Sigma_e(t)]_{i,i}}\sqrt{\frac{1}{\tilde{p}_i}}\right] \\
&\leq \Pr\left[|e_i(t) - E[e_i(t)]| \geq \sqrt{\frac{[\Sigma_e(t)]_{i,i}}{\tilde{p}_i}}\right] \\
&\leq \tilde{p}_i
\end{aligned}$$

where we used Chebyshev inequality in the last step.

Taking $0 < \tilde{p}_i < 1$ for $i = 1, \cdots, 2n$ such that $\sum_{i=1}^{2n} \tilde{p}_i = 1 - p$, we define the region

$$S = \left\{ e : |e_i| \leq \mu_\varepsilon + \sigma \sqrt[4]{\frac{2n}{\tilde{p}_i^2}}; \quad i = 1, \cdots, 2n \right\} \tag{53}$$

and we notice that

$$\Pr[e(t) \in S] = 1 - \Pr[e(t) \notin S] \geq 1 - \sum_{i=1}^{2n} \Pr\left[|e_i(t)| \geq \mu_\varepsilon + \sigma \sqrt[4]{\frac{2n}{\tilde{p}_i^2}} \right] \geq 1 - \sum_{i=1}^{2n} \tilde{p}_i = p$$

for $t \geq T_\varepsilon$, showing that the bounded set S is a PUB with probability p for system (19). □

The last theorem proves that the trajectories converge in probability to a bounded region provided that the minimum interval T between successive switching times, as computed in the theorem, is satisfied.

5. Examples

5.1. Aircraft Control

The following example, taken from [24], represents a bank-angle control system for a jet transport aircraft flying at the speed of 0.8 Mach, and the attitude of 40,000 ft. There are two manipulated variables: the aileron position and the rudder position.

The state-space representation for this model can be written as in Eq.(4) with the following system matrices:

$$A = \begin{bmatrix} -0.6358 & 1 & 0 & 0 \\ -0.9389 & 0 & 1 & 0 \\ -0.5116 & 0 & 0 & 1 \\ -0.0037 & 0 & 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 1.1476 & 10.7290 \\ -2.0036 & 2.3169 \\ 13.7264 & 10.2370 \end{bmatrix}, C = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}^T \text{ and } F = \begin{bmatrix} 2 \\ 1.1476 \\ -2.0036 \\ -13.7264 \end{bmatrix}.$$

The fault scenarios are represented by the following matrices:

$$P^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, P^1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \text{and } P^2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

where P^0 models that both actuators are operational, and P^1 and P^2 model faults in the aileron and the rudder, respectively.

The state observer is designed according to Eq.(9) with

$$L = \begin{bmatrix} 13.3642 & 70.0611 & 153.4884 & 119.9963 \end{bmatrix}^T.$$

The feedback control gains K_j for each fault scenario (Eq.(10) are designed using the LQR methodology, resulting:

$$K_1 = \begin{bmatrix} -0.0833 & 0.0021 & 0.1427 & 0.1531 \\ 0.0105 & -0.0208 & -0.0212 & -0.0126 \end{bmatrix},$$

$$K_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0.0223 & -0.0085 & -0.0400 & -0.0579 \end{bmatrix}, \text{ and}$$

$$K_3 = \begin{bmatrix} -0.1075 & 0.0249 & 0.1745 & 0.1704 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

It can be verified by direct calculation that Remark 1 holds with these control and observer matrices.

For the reference system we designed a linear quadratic integral (LQI) control law so that the output tracks a constant reference $y_0(t) = 1$. The usage of this LQI controller on the system of Eq.(7) provides the input reference signals:

$$\bar{u}_{r,0} = [0.0648,\ 0.0873]^T,\ \bar{u}_{r,1} = [0.0885,\ 0.0004]^T,\ \text{and}\ \bar{u}_{r,2} = [-0.0003,\ 0.1260]^T,$$

for each fault configuration scenario.

Then, the PUB sets $S_{or}^{i,j} = \{e_{or} \in \mathbb{R}^4 : |e_{or} - \bar{e}_{or}^{i,j}| \preceq b_{or}^{i,j} + \bar{\varepsilon}\}$, where $\bar{\varepsilon} \triangleq [\varepsilon, \ldots, \varepsilon]^T$, were computed for a probability $p = 0.813$ and a noise incremental covariance $\Sigma_w \mathrm{d}t = 10^{-5}\mathrm{d}t$. We take $\tilde{p}_k = (1-p-\delta)/4$ for $k = 1, \ldots, 4$, and $\tilde{p}_k = \delta/4$, for $k = 5, \ldots, 8$, with a very small value for δ (we chose $\delta = 10^{-4}$). Hence, Eq.(25) is satisfied and we obtain a small size for $S_{or}^{i,j}$ in the directions of the measured variables (the first $n = 4$ components of the $2n$ combined state vector (16)).

Thus, using Eq.(21), Eq.(24), and (28) the following values for $\bar{e}_{or}^{i,j}$ and $b_{or}^{i,j}$ were obtained:

$$\bar{e}_{or}^{0,0} = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T, \qquad \bar{b}_{or}^{0,0} = \begin{bmatrix} 0.1003 & 0.0995 & 0.1010 & 0.0610 \end{bmatrix}^T,$$
$$\bar{e}_{or}^{1,0} = \begin{bmatrix} 0.4349 & 0.2517 & 0.3492 & -0.0244 \end{bmatrix}^T, \qquad \bar{b}_{or}^{1,0} = \begin{bmatrix} 0.2875 & 0.2772 & 0.1979 & 0.0967 \end{bmatrix}^T,$$
$$\bar{e}_{or}^{2,0} = \begin{bmatrix} -0.2557 & -0.1480 & -0.2053 & 0.0144 \end{bmatrix}^T, \quad \bar{b}_{or}^{2,0} = \begin{bmatrix} 0.1320 & 0.1263 & 0.1272 & 0.0723 \end{bmatrix}^T,$$

for the healthy configuration,

$$\bar{e}_{or}^{0,1} = \begin{bmatrix} -0.3564 & -0.2124 & -0.3923 & -0.0480 \end{bmatrix}^T, \quad \bar{b}_{or}^{0,1} = \begin{bmatrix} 0.1705 & 0.1655 & 0.1805 & 0.0738 \end{bmatrix}^T,$$
$$\bar{e}_{or}^{1,1} = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T, \qquad \bar{b}_{or}^{1,1} = \begin{bmatrix} 0.1705 & 0.1655 & 0.1805 & 0.0738 \end{bmatrix}^T,$$
$$\bar{e}_{or}^{2,1} = \begin{bmatrix} -35.306 & -21.043 & -38.866 & -4.7549 \end{bmatrix}^T, \quad \bar{b}_{or}^{2,1} = \begin{bmatrix} 1.4400 & 0.9002 & 1.5828 & 0.2394 \end{bmatrix}^T,$$

for the first actuator fault, and

$$\bar{e}_{or}^{0,2} = \begin{bmatrix} 0.3113 & 0.1836 & 0.2063 & 0.0129 \end{bmatrix}^T, \qquad \bar{b}_{or}^{0,2} = \begin{bmatrix} 0.1274 & 0.1280 & 0.0996 & 0.0719 \end{bmatrix}^T,$$
$$\bar{e}_{or}^{1,2} = \begin{bmatrix} 33.7494 & 19.9005 & 22.3642 & 1.4026 \end{bmatrix}^T, \quad \bar{b}_{or}^{1,2} = \begin{bmatrix} 1.4393 & 0.8875 & 0.9417 & 0.1342 \end{bmatrix}^T,$$
$$\bar{e}_{or}^{2,2} = \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}^T, \qquad \bar{b}_{or}^{2,2} = \begin{bmatrix} 0.1274 & 0.1280 & 0.0996 & 0.0719 \end{bmatrix}^T,$$

for the fault in the second actuator configuration. It can be verified that the resulting PUB sets for the different configurations are disjoint, thus satisfying the assumption of Theorem 1.

In order to implement the diagnosis scheme of Fig.3, we designed the filters (30) using the parameter $\lambda = 0.1$.

In order to test our scheme, the system was simulated for 1000 seconds, varying the fault situation between the 3 fault scenarios, as shown with the dashed line in Fig. 4. In the same figure,

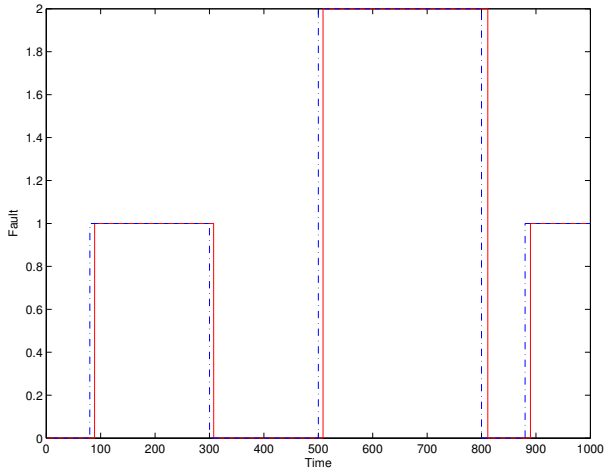

Figure 4: Actual fault situation (dashed line) and the corresponding detection (solid line).

the solid line shows the output of the diagnosis block, which correctly detects the fault after a lapse of time that is of the order of the filter response time.

For the same fault sequence, Figure 5 shows the plant output when the reconfiguration scheme is applied. It can be seen that the reference signal is correctly tracked in all the situations (except for some short transients due to the time required for correct fault diagnosis). The effectiveness of the proposed methodology becomes evident when this signal is compared with that of Figure 6, which shows the plant output under the same fault sequence when no reconfiguration is made.

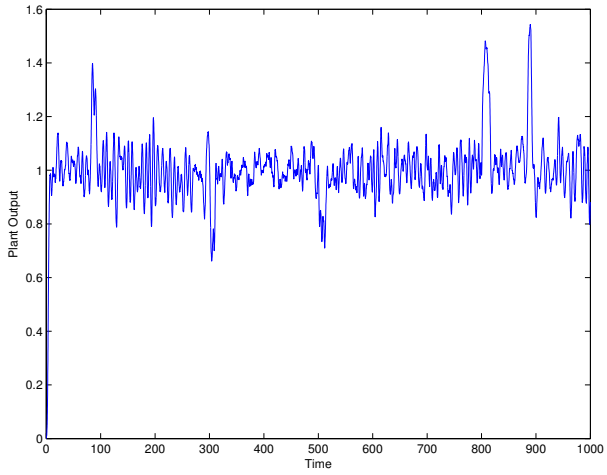

Figure 5: Plant output with reconfiguration.

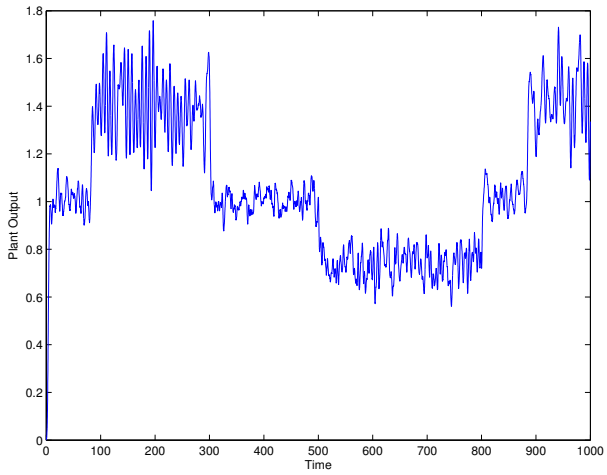

Figure 6: Plant output without reconfiguration.

5.2. Autonomous Vehicle Control

We consider a nonlinear model of a car moving in a plane. The car is impulsed by four independent motors, whose torque can be controlled. The car has also a steering wheel that can be manipulated in the range $\psi \in (-\pi/4, \pi/4)$. The model considers that the wheels can slip (with a large friction coefficient).

The overall model has 7 degrees of freedom: the displacement in x and y coordinates, the vehicle angle θ with respect to the x axis, and the angular position of the four wheels. The total order is then 14 (considering positions and velocities). The measured variables are the wheel angular speeds, and the deviation and the angle with respect to the x axis: $y(t)$, and $\theta(t)$.

The control goal is that the car moves at a constant speed $v_x = 1\text{m/s}$ following a straight line representing the x axis (i.e., $y(t) = 0$). Thus, the total order of the model was reduced to 9, since nor the angle of the wheels neither the position $x(t)$ play any role in the controlled system. Thus, the reduced order plant state, input and output dimensions are $n = 9$, $m = 5$, and $s = 6$, respectively.

A Matlab function containing the nonlinear state equations of the car can be downloaded from `http://www.fceia.unr.edu.ar/~kofman/files/car/carStateEqs.m`. This function is used inside a Simulink model containing the car model that can be downloaded from `http://www.fceia.unr.edu.ar/~kofman/files/car/car.mdl`.

In the model, the input noise is a scalar Wiener process with incremental covariance $\Sigma_w \mathrm{d}t = 1\mathrm{d}t$, that enters the plant through the input affected by a matrix G, so the plant model has the form

$$\mathrm{d}x(t) = f(x(t))\mathrm{d}t + g(x)(u(t)\mathrm{d}t + G\mathrm{d}w(t))$$

with $G = [0.1, 0.1, 0.1, 0.1, 0.05]^T$.

We consider that only two motors can fail at the same time, so we have a total of 11 fault situations (4 corresponding to individual actuator faults, 6 corresponding to all the possible combinations of two actuators with simultaneous faults, and the healthy situation).

In order to build the exosystem, and to design the observer, the controllers and to compute the PUBs, the plant model was linearized (using Matlab's command `linmod`), obtaining the following system matrices:

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0.15 & 0.15 & 0.15 & 0.15 \\ 0 & 1.2 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -10.88 & -0.36 & 0.36 & -0.36 & 0.36 \\ 0 & 0 & 20 & 0 & -12 & -6.34 & 0 & 0 & 0 \\ 0 & 0 & 20 & 0 & 12 & 0 & -6.34 & 0 & 0 \\ 0 & 0 & 20 & 0 & -12 & 0 & 0 & -6.34 & 0 \\ 0 & 0 & 20 & 0 & 12 & 0 & 0 & 0 & -6.34 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.6 \\ 0 & 0 & 0 & 0 & 2.4 \\ 0.2 & 0 & 0 & 0 & 0 \\ 0 & 0.2 & 0 & 0 & 0 \\ 0 & 0 & 0.2 & 0 & 0 \\ 0 & 0 & 0 & 0.2 & 0 \end{bmatrix} \quad C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The model of Eq.(4) is completed with $F = BG$.

The different components of the control reconfiguration scheme were designed as follows:

- The exosystem is the linearized version of the nonlinear plant with different controllers for each fault situation designed using an LQI technique. The design ensures stability under the 11 possible configurations. In addition, it ensures that the output $y_r(t)$ converges to the reference constant output y_0 corresponding to $y(t) = 0$ mts and $v_x(t) = 1$ m/s.
- The state observer was designed with a Luenberger structure using pole placement.
- The feedback control gains K_j were designed using LQR on the linearized model for the 11 possible configurations. For the LQR design, in all cases, we chose $Q = 100 I_{9\times 9}$ and $R = I_{5\times 5}$. The resulting feedback gains ensure that the closed–loop system is stable under the occurrence of any fault situation while the scheme is in any of the 11 possible configurations.

The calculation of the PUBs for the 11 possible configurations under the 11 possible fault occurrences for a probability $p = 0.99$, satisfies the set separation assumption of Theorem 1. For the filters in Eq.(30), we used the parameter $\lambda = 1$.

A Matlab script performing the design of the exosystem, controllers, observer, and the computation of the different PUBs can be downloaded from `http://www.fceia.unr.edu.ar/~kofman/files/car/car_script.m`.

In order to evaluate the proposed fault tolerant strategy we simulated the complete scheme using the nonlinear model for the plant with the sequence of faults depicted in Figure 7. This sequence corresponds to an initial healthy situation, then there is a fault (at $t = 50$ secs) in the

third actuator (forward left motor) that is recovered at time $t = 300$ secs. At time $t = 500$ secs there is a fault in the second actuator (rear right motor) and at time $t = 700$ the first actuator (rear left motor) also fails (the fault situation $i = 5$ denotes the simultaneous fault of the first and the second actuator). At time $t = 900$ the second actuator recovers so there is only a fault in the first actuator.

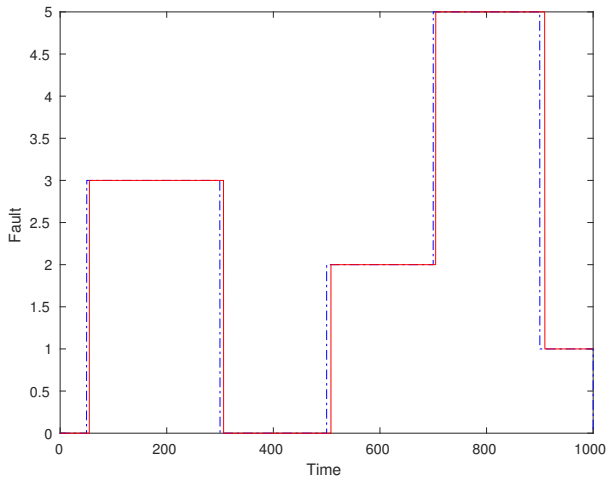

Figure 7: Fault sequence (dashed line) and the corresponding detection (solid line).

Figure 7 also shows that all the faults are correctly detected. In all cases, the detection takes from 5 to 8 seconds. In summary, the whole scheme works as predicted and the output is correctly tracked as shown in Figure 8.

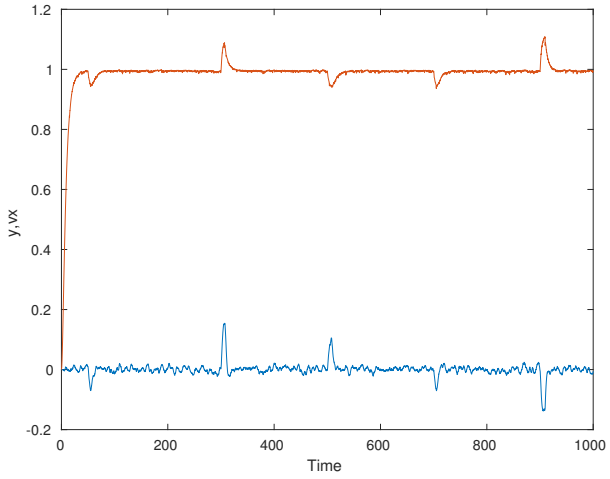

Figure 8: Output trajectories with reconfiguration: y position (blue line) and v_x speed (red line).

In order to demonstrate the advantages of the proposed scheme, we simulated the system again under the same sequence of faults but without reconfiguration. The corresponding trajectories are shown in Figure 9, where a significant tracking error can be noticed.

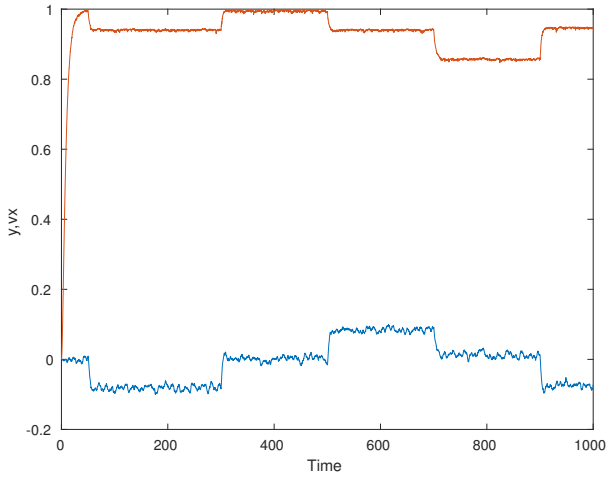

Figure 9: Output trajectories without reconfiguration: y position (blue line) and v_x speed (red line).

This example shows that the methodology is robust and it can work even when the model of the plant does not coincide with the model used to design and implement the exosystem, observer and controllers. The mismatch between the plant and its model can have two effects: the closed loop system may result unstable or, if it is stable, the PUBs computed may not coincide with the actual ones, which can affect the diagnosis strategy. The first problem can be avoided by using a robust controller. The second problem can be mitigated by using a large probability $p \approx 1$ so that the computed PUB sets are large and they can contain the real but unknown PUB sets corresponding to the real plant (using a smaller probability).

6. Conclusions

We have presented a fault diagnosis strategy with reconfiguration of the control law based on the computation of probabilistic ultimate bound sets. The use of these sets allows for unbounded disturbances such as Gaussian white noise to be considered, a fact that is not possible under deterministic set-based schemes.

We showed that the proposed strategy guarantees the correct diagnosis of actuator faults with arbitrarily small probability of error.

To the best of our knowledge, this novel scheme constitutes the first link between deterministic set-based fault diagnosis approaches and probabilistic strategies.

Future work is aimed at extending the results to discrete-time control schemes.

The results can be also extended to consider the presence of other component faults; for example, sensor faults. In this case, the faults can typically be modeled as $y_p = Q^j C x_p$, instead of the second equation in (4), where the matrix Q^j models the sensor fault (in an analogous manner

as P^i modeling an actuator fault in Eq.(6)). In that case, the corresponding observer (9) is built using Q^jC instead of C in the last term. Assuming that the resulting PUB sets are disjoint (as in Theorem 1), in particular that the PUB sets characterizing actuator faults are separated from those characterizing sensor faults, then the same results of the paper can be applied.

7. References

[1] Karl J Åström. *Introduction to stochastic control theory*. Academic Press, 1970.

[2] M. Basseville and I.V. Nikiforov. *Detection of Abrupt Changes – Theory and Application*. Prentice-Hall, Inc., 1993.

[3] F. Blanchini and S. Miani. *Set-theoretic methods in control*. Birkhauser, 2007.

[4] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer, 2nd edition, 2006.

[5] C. Ocampo-Martínez, J. De Doná and M. Seron. Actuator fault-tolerant control based on set separation. *International Journal of Adaptive Control and Signal Processing*, 24(12):1070–1090, 2010.

[6] S.X. Ding. *Model-based Fault Diagnosis Techniques*. Springer, 2008.

[7] P. M. Frank and X. Ding. Survey of robust residual generation and evaluation methods in observer-based fault detection systems. *Journal of Process Control*, 7(6):403–424, 1997.

[8] J.J. Gertler. Survey of model-based failure detection and isolation in complex plants. *IEEE Control Systems Magazine*, 8(6):3–11, 1988.

[9] A. Ingimundarson, V. Puig, T. Alamo, J. Bravo, and P. Guerra. Robust fault detection using zonotope-based set-membership consistency test. *International Journal of Adaptive Control and Signal Processing*, 23(4):311–330, 2008.

[10] R. Isermann. *Fault-Diagnosis Systems. An Introduction from Fault Detection to Fault Tolerance*. Springer, 2006.

[11] E. Kofman, J. De Doná, and M. Seron. Probabilistic set invariance and ultimate boundedness. *Automatica*, 48(10):2670–2676, 2012.

[12] E. Kofman, J. De Doná, M. Seron, and N. Pizzi. Computation of Continuous-Time Probabilistic Invariant Sets and Ultimate Bounds. In *Proceedings of 19th IFAC World Congress*, Cape Town, South Africa. August 24-29, 2014.

[13] M. Seron, J. De Doná and S. Olaru. Fault tolerant control allowing sensor healthy-to-faulty and faulty-to-healthy transitions. *IEEE Transactions on Automatic Control*, 77(7):1657–1669, 2012.

[14] M. Seron, X. Zhuo, J. De Doná and J. Martínez. Multisensor switching control strategy with fault tolerance guarantees. *Automatica*, 44(1):88–97, 2008.

[15] Raheleh Nazari, Maria M Seron, and José A De Doná. Actuator fault tolerant control of systems with polytopic uncertainties using set-based diagnosis and virtual-actuator-based reconfiguration. *Automatica*, 75:182–190, 2017.

[16] R.J. Patton, P.M. Frank, and R. Clark. *Issues of Fault Diagnosis for Dynamic Systems*. Springer, 2000.

[17] N. Pizzi, E. Kofman, M. Seron, and J. De Doná. Actuator Fault Diagnosis Using Probabilistic Ultimate Bounds. *IEEE Latin America Transactions*, 14(6):2548–2543, 2016.

[18] V. Puig. Fault diagnosis and fault tolerant control using set-membership approaches: application to real case studies. *International Journal of Applied Mathematics and Computer Science*, 20(4):619–635, 2010.

[19] Damiano Rotondo, Fatiha Nejjari, and Vicenç Puig. A virtual actuator and sensor approach for fault tolerant control of lpv systems. *Journal of Process Control*, 24(3):203–222, 2014.

[20] S. Olaru, J.A. De Doná, M. Seron and F. Stoican. Positive invariant sets for fault tolerant multisensor control schemes. *International Journal of Control*, 83(12):2622–2640, December 2010.

[21] Cun Shi, Shaoping Wang, Xingjian Wang, Jun Wang, and Mileta M Tomovic. Active fault-tolerant control of dissimilar redundant actuation system based on performance degradation reference models. *Journal of the Franklin Institute*, 354(2):1087–1108, 2017.

[22] S Mojtaba Tabatabaeipour, Jakob Stoustrup, and Thomas Bak. Fault-tolerant control of discrete-time lpv systems using virtual actuators and sensors. *International journal of Robust and nonlinear Control*, 25(5):707–734, 2015.

[23] Jun Wang, Shaoping Wang, Xingjian Wang, Cun Shi, and Mileta M Tomovic. Active fault tolerant control for vertical tail damaged aircraft with dissimilar redundant actuation system. *Chinese Journal of Aeronautics*, 29(5):1313–1325, 2016.

[24] Q Zhao and J Jiang. Reliable state feedback control system design against actuator failures. *Automatica*, 34(10):1267–1272, 1998.