Actuator fault-tolerant control based on set separation

C. Ocampo-Martinez[1,*,†], J. A. De Doná[2] and M. M. Seron[2]

[1]*Institut de Robòtica i Informàtica Industrial* (*IRI*), *Spanish National Research Council* (*CSIC*), *Technical University of Catalonia* (*UPC*), *Barcelona*, *Spain*
[2]*ARC Centre for Complex Dynamic Systems and Control* (*CDSC*), *The University of Newcastle*, *Callaghan*, *NSW 2308*, *Australia*

SUMMARY

In this paper, an actuator fault-tolerant control (FTC) strategy based on set separation is presented. The proposed scheme employs a standard configuration consisting of a bank of observers which match the different fault situations that can occur in the plant. Each of these observers has an associated estimation error with a distinctive behaviour when a estimator matches the current fault situation of the plant. With this information from each observer, a fault diagnosis and isolation (FDI) module is able to reconfigure the control loop by selecting the appropriate stabilising controller from a bank of precomputed control laws, each of them related to one of the considered fault models. The control law consists of a reference feedforward term and a feedback gain multiplying the state estimate provided by the matching observer. A novel feature of the proposed scheme resides in the decision criteria of the FDI, which is based on the computation of sets towards which the output estimation errors related to each fault scenario and for each control configuration converge. Conditions for the design of the FDI module and for fault tolerant closed-loop stability are given, and the effectiveness of the approach is illustrated by means of a numerical example.

KEY WORDS: fault-tolerant control; actuator faults; fault diagnosis and isolation; invariant sets

1. INTRODUCTION

Modern automatic control industrial systems can have their reliability degraded due to the huge number of components and their increasing number of possible faults (understood as a deviation from a specified mode of behaviour). It is known that those abnormal situations due to instrument or component failure can prevent or endanger continuous operation. It is, thus, of utmost importance to endow control systems with fault-tolerance capabilities. A comprehensive treatment of fault-tolerant control (FTC) systems can be found in [1]. In this study, attention is focused on

*Correspondence to: C. Ocampo-Martinez, Institut de Robòtica i Informàtica Industrial (IRI), Parc Tecnològic de Barcelona, Llorens i Artigas, 4-6, 2nd floor, 08028 Barcelona, Spain.
†E-mail: cocampo@iri.upc.edu

Contract/grant sponsor: Juan de la Cierva Research Programme; contract/grant number: JCI-2008-2438
Contract/grant sponsor: Spanish Science and Technology Ministry CICYT; contract/grant number: DPI2009-13744

severe actuator faults (i.e. total loss of some actuators). Therefore, the presence of a fault diagnosis and isolation (FDI) module is required to detect and identify the fault. In addition, an active FTC strategy is necessary to ensure, in presence of a fault, the highest possible performance of the controlled system. As soon as the FTC unit receives the signal from the FDI module identifying the type of the fault, an appropriate decision must be made in order to maintain the system properties, namely stability, and performance.

The actuator FTC strategy proposed in this paper is based on an invariant set computation (see e.g. [2]). The proposed scheme consists of a bank of observers (see e.g. [3]), which match different fault situations that can occur in the plant. Each of these observers has an associated estimation error with a distinctive behaviour when the observer matches the current fault situation in the plant. With this information from each observer, an FDI module is able to reconfigure the control loop by selecting the appropriate stabilising controller from a bank of precomputed control laws, each of them consisting of a state feedback gain and an exogenous reference signal related to the considered fault models. The FDI module also selects the appropriate state estimate in order to build a feedback signal consisting of the selected feedback gain multiplying the difference between the state estimate provided by the matching observer and the selected exogenous reference signal. The decision criteria of the FDI is based on the computation of sets towards which the estimation errors converge. These sets are computed for each considered fault scenario, for each observer, and for each control configuration.

A key property for the correct fault diagnosis in the proposed scheme is the separation of the sets that characterise healthy operation from the ones that characterise faulty operation. The inherent component redundancy that is required for an actuator FTC scheme provides, in many applications, enough flexibility to achieve the aforementioned set separation. In addition, the proposed technique is particularly well suited for reference tracking problems when the reference signal contains an offset component. In those cases, the reference signal provides an additional mechanism to achieve the desired set separation. Conditions for the design of the FDI module, and for achieving the required set separation are discussed in this paper. Under those conditions, fault-tolerant closed-loop stability of the proposed scheme can be guaranteed.

The main contributions of this paper are, first, that stability of the proposed scheme can be guaranteed under an easily checkable set of conditions. Moreover, design choices so as to achieve the proper set of conditions for closed-loop stability are discussed in detail. Second, a remarkable feature is the simplicity of the FDI mechanism. In effect, once the required set of conditions is satisfied by design (this set of conditions—set separation—can be checked *off-line*), then the design of the FDI is simple since its complexity depends linearly on the number of fault situations that are taken into account. In contrast with other schemes (see e.g. [4, 5]), which use stochastic arguments for fault detection and control reconfiguration, the approach followed here is purely deterministic and does not require any statistical description neither for noises, disturbances nor fault occurrences. Finally, our approach considers a generalisation of the observers proposed in [3], relaxing the condition of the full state measurement, situation that is not always possible. This relaxation allows us to consider a more realistic problem under some assumptions related to disturbances that affect the system.

The work presented in this paper was inspired by previous results by the authors on fault-tolerant multisensor switching control, see [6]. However, the *actuator* fault-tolerant problem poses a different set of challenges with respect to its *sensor* fault-tolerant counterpart, since the plant *mixes* the effects of actuator malfunctions as observed from the system output. For a preliminary version of this paper, where full state measurement was required, see [7]. See also [8] for a related discrete-time implementaton of the proposed scheme.

The remainder of this paper is organised as follows: In Section 2, the actuator fault-tolerant detection and reconfiguration scheme is presented and its main parts are explained. In Section 3, the dynamic equations of the closed-loop system are derived. Section 4 contains the main results of this paper; namely, the computation of the sets, the conditions needed for their adequate separation, and the proof of closed-loop stability of the scheme when set separation is achieved. In Section 5, the effectiveness of the proposed approach is illustrated using an application example. Finally, conclusions are provided in Section 6.

Notation

In the sequel, let $\mathbb{R}$ and $\mathbb{R}_+$ denote the set of real numbers and the set of non-negative real numbers, respectively. A given system variable $v(t)$ is expressed as $v^k_{i,j}(t)$, where the subindex i denotes its dependence on the fault mode of the plant (fault scenario), the subindex j is related to the control configuration, and the superindex k is related to the observer. $|M|$ and $\mathbf{Re}(M)$ denote the elementwise magnitude and real part, respectively, of a (possibly complex) matrix M and $x \leqslant y$ ($x < y$) denotes the set of elementwise (strict) inequalities between the components of the real vectors x and y. The set $\mathscr{B}_r \subset \mathbb{R}^p$ is a closed ball of radius r centred at the origin of $\mathbb{R}^p$, that is, $\mathscr{B}_r \triangleq \{x \in \mathbb{R}^p : \|x\|_2 \leqslant r\}$, where $\|x\|_2$ denotes the Euclidean 2-norm of the vector x.

2. ACTUATOR FAULT DETECTION AND RECONFIGURATION SCHEME

In this section, the proposed actuator fault detection and reconfiguration scheme is described. The schematic of the whole system is depicted in Figure 1 and its constitutive parts are explained in the following subsections.

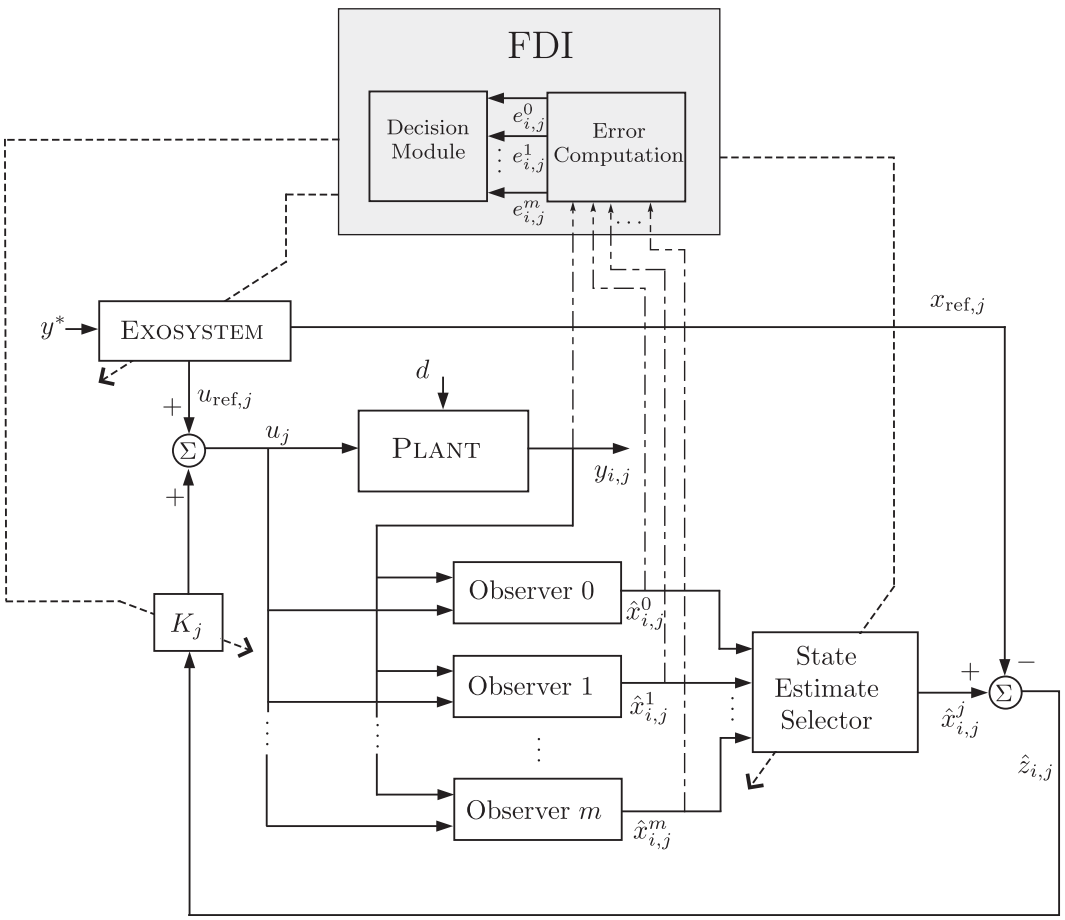

Figure 1. Proposed fault detection and reconfiguration scheme.t

2.1. Nominal plant and fault models

We consider an LTI perturbed system described by

$$\dot{x}(t) = Ax(t) + B'u(t) + Ed(t), \tag{1a}$$

$$y(t) = Cx(t), \tag{1b}$$

with $B' \triangleq BL$, where $x(t) \in \mathbb{R}^n$ is the system state, $u(t) \in \mathbb{R}^m$ is the control input, $d(t) \in \mathbb{R}^p$ is an unknown disturbance assumed to be bounded according to the following assumption.

Assumption 2.1
$|d(t)| \leqslant d^{\max}$, where $d^{\max} \in \mathbb{R}^p$ is a known vector with non-negative components.

Remark 2.1
Note that the system disturbances can be considered as random variables but we do not assume knowledge of their statistical properties; all we require is knowledge of their bounds. Hence, disturbances with uniform distribution or any truncated distribution, for example, are within the scope of our analysis.

Vector $y(t) \in \mathbb{R}^q$ is the system output and A, B, C, and E are constant matrices of suitable dimensions. Matrix L is used to model the occurrence of actuator faults. It is defined as

$$L \triangleq \text{diag}[l_1 \quad l_2 \quad \dots \quad l_m], \quad l_h \in \{0, 1\} \quad \text{for } h = 1, \dots, m. \tag{2}$$

As mentioned in the introduction, this paper is focused on severe (outage) actuator faults. Accordingly, the case $l_h = 1$ represents no fault in the h-th actuator; whereas, $l_h = 0$ models an outage in the h-th actuator. In the nominal case, i.e. no faults, L is the identity matrix. In this paper, it is considered, for simplicity of exposition, that only one actuator can fail at the time. That is, the matrix L in (2) can take $m+1$ different values $L = L_i$, where

$$\begin{aligned} L_0 &= I, \\ L_i &= \text{diag}[1 \dots \overset{i}{\underset{\downarrow}{0}} \dots 1], \quad i = 1, \dots, m. \end{aligned} \tag{3}$$

Next, an *actuator redundancy* assumption is imposed, which is inherent to the actuator FTC scheme.

Assumption 2.2
The system (1)–(2) is stabilizable for all possible values of $L = L_i$, with $i = 0, \dots, m$, as defined in (3).

We remark that, provided the system continues to be stabilizable, outage of more than one actuator at the same time can also be contemplated within the framework of this paper.

In the proposed scheme, the control $u(t)$ can take $m+1$ possible forms $u(t) = u_j(t)$, for $j = 0, \dots, m$, each form designed for a particular value of the matrix $L = L_i$ given in (3), as explained in Section 2.5 below. The FDI module decides which control to use at each time according to its evaluation of the current fault situation of the system. In order to emphasise the current system fault situation (determined by matrix $L = L_i$) and the current control in use ($u(t) = u_j(t)$), in the sequel we will add subindexes i and j to the state variable x and output variable y in (1) and we will employ the following notation for the system dynamics:

$$\dot{x}_{i,j}(t) = Ax_{i,j}(t) + BL_i u_j(t) + Ed(t), \tag{4a}$$

$$y_{i,j}(t) = Cx_{i,j}(t). \tag{4b}$$

2.2. Exogenous system for reference tracking

The exogenous system for reference tracking module (called in the sequel *exosystem*) generates input and state reference trajectories, $u_{\mathrm{ref},j}(t)$, and $x_{\mathrm{ref},j}(t)$, to be used under each possible fault situation, that is, for each possible value of the matrix L_i in (3). These reference trajectories satisfy

$$\dot{x}_{\mathrm{ref},j}(t) = Ax_{\mathrm{ref},j}(t) + BL_j u_{\mathrm{ref},j}(t), \tag{5a}$$

$$y_{\mathrm{ref},j}(t) = Cx_{\mathrm{ref},j}(t), \tag{5b}$$

with $j=0,\ldots,m$, where $x_{\mathrm{ref},j}(t)$, and $u_{\mathrm{ref},j}(t)$ are bounded signals. Notice that this is always possible by using an auxiliary control loop inside the exosystem, since the exosystem model (5) *mimics* the plant model and, hence, also satisfies Assumption 2.2. Moreover, it is assumed that $u_{\mathrm{ref},j}(t)$, for $j=0,\ldots,m$, satisfy the following assumption.

Assumption 2.3
The reference inputs $u_{\mathrm{ref},j}(t)$, for $j=0,\ldots,m$, are assumed to be bounded and expressible as $u_{\mathrm{ref},j}(t)=\bar{u}_{\mathrm{ref},j}+\tilde{u}_{\mathrm{ref},j}(t)$, where $\bar{u}_{\mathrm{ref},j}\in\mathbb{R}^m$ are constant offset levels and $\tilde{u}_{\mathrm{ref},j}(t)$ are variations around the respective offsets, whose amplitudes are bounded as $|\tilde{u}_{\mathrm{ref},j}(t)|\leqslant\tilde{u}^{\max}_{\mathrm{ref},j}$, for all t, where $\tilde{u}^{\max}_{\mathrm{ref},j}\in\mathbb{R}^m$ are known vectors containing non-negative components.

The exosystem (5) is designed such that its output $y_{\mathrm{ref},j}(t)$ exponentially tracks an external signal $y^*(t)$, that is

$$\lim_{t\to\infty}[\,y_{\mathrm{ref},j}(t)-y^*(t)\,]=0. \tag{6}$$

The signal $y^*(t)$ is an output reference trajectory that we ultimately wish the plant output $y_{i,j}(t)$ in (4b) to track under all possible fault situations. To guarantee the latter objective, stabilizing state feedback gains are designed (see Section 2.5 below) which ensure that, in the absence of disturbances, the system state $x_{i,j}(t)$ in (4a) asymptotically tracks the exosystem reference states $x_{\mathrm{ref},j}(t)$ in (5a) for each possible fault situation.

Note that the exosystem, as a module containing the reference model, can be obtained using any control design method which might be as complex as we decide. This fact adds extra flexibility to the overall system design that complements the computation of suitable feedback gains K (see Section 2.5 below) in fulfilling the desired control objective (6).

2.3. Plant state observers

We propose to perform actuator fault detection using a bank of observers inspired in the unknown input observer (UIO) proposed in [3]. The difference lies in that we allow for the output matrix C in (4b) to have rank $q<n$, that is, we do not require full state measurement, as was the case in [3].

We require the following assumption.

Assumption 2.4
System (4) is detectable.

The equations that characterise the proposed observers are

$$\dot{w}^k_{i,j}(t) = Fw^k_{i,j}(t) + GBL_k u_j(t) + My_{i,j}(t), \tag{7a}$$

$$\hat{x}^k_{i,j}(t) = w^k_{i,j}(t) + Hy_{i,j}(t), \tag{7b}$$

with $k=0,\ldots,m$, where $\hat{x}^k_{i,j}(t)\in\mathbb{R}^n$ is the state estimate, $w^k_{i,j}(t)\in\mathbb{R}^n$ is the observer state, $u_j(t)$ is the control input applied to the plant (see (4a)), $y_{i,j}(t)$ is the plant output (see (4b)), and L_k are as defined in (3). Note that

there is a total of $m+1$ observers, indexed by the superscript k; the subindexes i and j simply reflect the current fault situation, and the current control in use (see (4) and its preceding paragraph). Following [3], the matrices F, G, H, and M are chosen, such that

$$G = I - HC, \tag{8a}$$

$$F = GA - M_1 C, \tag{8b}$$

$$M_2 = FH, \tag{8c}$$

$$M = M_1 + M_2, \tag{8d}$$

with F, a Hurwitz matrix. Note that the choice $H = 0$ corresponds to the standard Luenberger-type observer. Thus, Assumption 2.4 guarantees that (8) always have a solution such that F is Hurwitz.

2.4. State estimate selector

The state estimate selector (SES) module selects a certain state estimate from the set of all state estimates provided by the bank of observers. The selection is done according to the decision made by the FDI module. This FDI module (described below in Section 2.6) decides the index $j \in \{0, \ldots, m\}$ that corresponds to the *evaluated fault situation* and passes the corresponding state estimate (7b) to implement the feedback control law $u_j(t)$ (see (10) below). The selected state estimate corresponds to the output of the observer $k = j$, i.e. $\hat{x}^j_{i,j}(t)$.

2.5. Feedback control laws

This part of the scheme consists of a set of state feedback gains which are computed off-line for the nominal case (no faults), and for each possible fault scenario. These gains are represented by the block K_j in Figure 1.

In combination with the exosystem module described in Section 2.2 and the SES module described in Section 2.4, these gains guarantee the desired tracking objective that the system output $y(t)$ in (1b) asymptotically tracks the output reference trajectory $y^*(t)$ in the absence of disturbances and when the control law corresponds to the model that matches the current fault situation of the system. In order to achieve this objective for the nominal and each possible fault scenario, let us define the tracking error for the selected state estimate as

$$\hat{z}_{i,j}(t) \triangleq \hat{x}^j_{i,j}(t) - x_{\mathrm{ref},j}(t), \tag{9}$$

for $i = 0, \ldots, m$ and $j = 0, \ldots, m$. The control input for each scenario takes the form

$$u_j(t) \triangleq K_j \hat{z}_{i,j}(t) + u_{\mathrm{ref},j}(t). \tag{10}$$

Notice that the state estimate used to implement the control law corresponds to the one obtained from the observer $k = j$ according to the selection done by the FDI module at the SES (as explained in Section 2.4). In this way, the FDI module (described in Section 2.6 below) decides the index $j \in \{0, \ldots, m\}$ that corresponds to the *evaluated* fault situation and passes the corresponding control input (10) to the plant (4).

2.6. Fault diagnosis and isolation module

The FDI module receives the plant output (4b) and the state estimates (7b), obtained from the observers described in Section 2.3. As shown in Figure 1, this module is formed by two subsystems. The first subsystem is the *error computation module*, which computes the output estimation errors $e^k_{i,j}(t)$, defined as

$$e^k_{i,j}(t) \triangleq y_{i,j}(t) - \hat{y}^k_{i,j}(t), \tag{11}$$

for $k=0,\ldots,m$, where

$$\hat{y}^k_{i,j}(t)\triangleq C\hat{x}^k_{i,j}(t). \tag{12}$$

The second subsystem is the *decision module*, which implements the FDI algorithm described in Section 4 below. Once the fault is detected and isolated using the computed output estimation errors, the FDI module selects the appropriate index $j\in\{1,\ldots,m\}$ for the feedback control law, the exosystem and the SES, and this index is used to implement the control input (10).

3. CLOSED-LOOP DYNAMICS

In this section, we derive closed-loop dynamic equations for the scheme of Figure 1 that are valid for fixed values of i and j, that is, while the fault situation of the plant (which defines i according to (3)) and the decision of the FDI module (which defines j and the associated control input (10)) remain unchanged. In particular, let us define the state tracking and estimation errors

$$z_{i,j}(t)\triangleq x_{i,j}(t)-x_{\mathrm{ref},j}(t) \quad \text{(state tracking error)} \tag{13}$$

$$\tilde{x}^k_{i,j}(t)\triangleq x_{i,j}(t)-\hat{x}^k_{i,j}(t) \quad \text{(state estimation error)} \tag{14}$$

and study their dynamics when the control input (10) is applied.

Using (13) and (14), and after some manipulations, the control input (10) can be rewritten as

$$u_j(t)=K_j z_{i,j}(t)-K_j\zeta_{i,j}(t)+u_{\mathrm{ref},j}(t), \tag{15}$$

where

$$\zeta_{i,j}(t)\triangleq\tilde{x}^j_{i,j}(t) \tag{16}$$

is the state estimation error corresponding to the state estimate selected by the SES (i.e. the state estimate from the observer $k=j$).

Considering the closed-loop system with (15), and using (4a) and (5a), the dynamics of the state tracking error $z_{i,j}(t)$, for $i=0,\ldots,m,\ j=0,\ldots,m$, can be written as

$$\begin{aligned}\dot{z}_{i,j}(t)&=\dot{x}_{i,j}(t)-\dot{x}_{\mathrm{ref},j}(t)\\&=Ax_{i,j}(t)+BL_i[K_j z_{i,j}(t)-K_j\zeta_{i,j}(t)+u_{\mathrm{ref},j}(t)]+Ed(t)-Ax_{\mathrm{ref},j}(t)-BL_j u_{\mathrm{ref},j}(t)\\&=(A+BL_iK_j)z_{i,j}(t)-BL_iK_j\zeta_{i,j}(t)+B(L_i-L_j)u_{\mathrm{ref},j}(t)+Ed(t).\end{aligned} \tag{17}$$

Similarly, using (4), (7), (8), and (15), the dynamics of the state estimation error in (14) for the case $k=j$, i.e. $\zeta_{i,j}(t)$, $i=0,\ldots,m,\ j=0,\ldots,m$ (see (16)), can be written as

$$\begin{aligned}\dot{\zeta}_{i,j}(t)&=\dot{x}_{i,j}(t)-\dot{\hat{x}}^j_{i,j}(t)\\&=\dot{x}_{i,j}(t)-\dot{w}^j_{i,j}(t)-HC\dot{x}_{i,j}(t)\\&=G\dot{x}_{i,j}(t)-\dot{w}^j_{i,j}(t)\end{aligned}$$

$$
\begin{aligned}
&= GAx_{i,j}(t) + GBL_i u_j(t) + GEd(t) - Fw_{i,j}^{j}(t) - GBL_j u_j(t) - MCx_{i,j}(t) \\
&= [GA - M_1C - M_2C + FHC]x_{i,j}(t) + GB(L_i - L_j)u_j(t) + GEd(t) - F\hat{x}_{i,j}^{j}(t) \\
&= F\zeta_{i,j}(t) + GB(L_i - L_j)[K_j z_{i,j}(t) - K_j\zeta_{i,j}(t) + u_{\mathrm{ref},j}(t)] + GEd(t) \\
&= [F - GB(L_i - L_j)K_j]\zeta_{i,j}(t) + GB(L_i - L_j)K_j z_{i,j}(t) + GB(L_i - L_j)u_{\mathrm{ref},j}(t) + GEd(t). \qquad (18)
\end{aligned}
$$

Hence, combining (17), and (18), and using the definitions

$$
A_{i,j} \triangleq \begin{bmatrix} A + BL_iK_j & -BL_iK_j \\ GB(L_i - L_j)K_j & F - GB(L_i - L_j)K_j \end{bmatrix}, \qquad (19a)
$$

$$
B_{i,j} \triangleq \begin{bmatrix} B(L_i - L_j) & E \\ GB(L_i - L_j) & GE \end{bmatrix}, \qquad (19b)
$$

$$
\varphi_j(t) \triangleq \begin{bmatrix} u_{\mathrm{ref},j}(t) \\ d(t) \end{bmatrix}, \qquad (19c)
$$

the following subsystems are obtained:

$$
\begin{bmatrix} \dot{z}_{i,j}(t) \\ \dot{\zeta}_{i,j}(t) \end{bmatrix} = A_{i,j} \begin{bmatrix} z_{i,j}(t) \\ \zeta_{i,j}(t) \end{bmatrix} + B_{i,j}\varphi_j(t), \quad i = 0, \ldots, m, \quad j = 0, \ldots, m. \qquad (20)
$$

In order to ensure internal closed-loop stability of the proposed scheme, we make the following assumption.

Assumption 3.1
The feedback control gains K_j and matrices H and M_1 (and hence G and F) in (8) are such that the closed-loop matrices $A_{i,j}$ in (19a), for $i = 0, \ldots, m$, and $j = 0, \ldots, m$, are Hurwitz.

Remark 3.1
In practise, one would typically design the estimator matrices (8) using some standard procedure (e.g. Kalman filter design) and, independantly, the feedback gain K_j, for $j = 0, \ldots, m$ such that the closed-loop system associated with the matrix $A + BL_jK_j$ is asymptotically stable and, in addition, satisfies some desirable performance criteria (e.g. is optimal in some sense). Then, one would verify that Assumption 3.1 is satisfied by testing the stability of matrices $A_{i,j}$ in (19a), for $i = 0, \ldots, m$ and $j = 0, \ldots, m$. This is the approach taken in the example of Section 5.

Alternatively, using fixed values of K_j (obtained, for instance, by some optimal design procedure, as discussed above), one recognises, using Lyapunov arguments, that Assumption 3.1 is equivalent to the existence of matrices H and M_1 (and hence G and F) in (8) and symmetric matrices $P_{i,j} \in \mathbb{R}^{2n \times 2n}$ satisfying

$$
\begin{bmatrix} A_{i,j}^{\mathrm{T}}P_{i,j} + P_{i,j}A_{i,j} & 0 \\ 0 & -P_{i,j} \end{bmatrix} < 0 \quad \text{for } i = 0, \ldots, m, \quad j = 0, \ldots, m. \qquad (21)
$$

It can be checked using (8) and (19a) that, for fixed values of $i \in \{0, \ldots, m\}$, and $j \in \{0, \ldots, m\}$, the expression in (21) is a bilinear matrix inequality (BMI) [9] due to the products of $P_{i,j}$ and the design matrices H and M_1, which appear in the expressions for matrices F and G (see (8)). Therefore, BMI solvers (e.g. PENBMI over Tomlab® [10]) may be used to find values of the design matrices H and M_1 (and hence F and G) that satisfy the BMI (21).

We next consider the state estimation errors, defined in (14), for the case $k \neq j$. Using (4), (7), (8), and (15), the dynamics of the state estimation error $\tilde{x}^k_{i,j}(t)$, for $i=0,\ldots,m$, $j=0,\ldots,m$, $k=0,\ldots,m$, and $k\neq j$, can be written as

$$\begin{aligned}
\dot{\tilde{x}}^k_{i,j}(t) &= \dot{x}_{i,j}(t) - \dot{\hat{x}}^k_{i,j}(t) \\
&= \dot{x}_{i,j}(t) - \dot{w}^k_{i,j}(t) - HC\dot{x}_{i,j}(t) \\
&= G\dot{x}_{i,j}(t) - \dot{w}^k_{i,j}(t) \\
&= GAx_{i,j}(t) + GBL_i u_j(t) + GEd(t) - Fw^k_{i,j}(t) - GBL_k u_j(t) - MCx_{i,j}(t) \\
&= F\tilde{x}^k_{i,j}(t) + GB(L_i - L_k)[K_j z_{i,j}(t) - K_j\zeta_{i,j}(t) + u_{\mathrm{ref},j}(t)] + GEd(t) \\
&= F\tilde{x}^k_{i,j}(t) + GB(L_i - L_k)K_j z_{i,j}(t) - GB(L_i - L_k)K_j\zeta_{i,j}(t) + GB(L_i - L_k)u_{\mathrm{ref},j}(t) + GEd(t).
\end{aligned} \tag{22}$$

Defining

$$\begin{aligned}
N^k_{i,j} &\triangleq [GB(L_i - L_k)K_j \;\; -GB(L_i - L_k)K_j \;\; GB(L_i - L_k) \;\; GE], \\
v_{i,j}(t) &\triangleq [z_{i,j}(t)^{\mathrm{T}} \;\; \zeta_{i,j}(t)^{\mathrm{T}} \;\; u_{\mathrm{ref},j}(t)^{\mathrm{T}} \;\; d(t)^{\mathrm{T}}]^{\mathrm{T}},
\end{aligned} \tag{23}$$

the dynamics of $\tilde{x}^k_{i,j}(t)$ can now be rewritten as

$$\dot{\tilde{x}}^k_{i,j}(t) = F\tilde{x}^k_{i,j}(t) + N^k_{i,j}v_{i,j}(t), \quad i=0,\ldots,m, \;\; j=0,\ldots,m, \;\; k=0,\ldots,m, \;\; k\neq j. \tag{24}$$

Notice the difference between state estimation errors $\zeta_{i,j}(t) \triangleq \tilde{x}^j_{i,j}(t)$ and $\tilde{x}^k_{i,j}(t)$ for $k \neq j$, with dynamics given by (18) and (24), respectively. $\zeta_{i,j}(t)$ corresponds to the selection done by the FDI module at the SES, whereas $\tilde{x}^k_{i,j}(t)$ for $k \neq j$ is related to each one of the remaining m observers. Then, due to the feedback loop, $\zeta_{i,j}(t)$ will appear in the control signal (see (15)) and thus it will be part of the input driving the dynamics of $\tilde{x}^k_{i,j}(t)$ in (23)–(24).

Also notice that, under Assumption 3.1 for fixed i and j and since F is a Hurwitz matrix (see Section 2.3), (20) and (24) define stable systems excited by bounded inputs, and hence their state trajectories will converge to invariant sets that will be computed in Section 4.1 below.

Remark 3.2

Notice that the plant model (1) only considers the disturbance $d(t)$ affecting the state equation (1a). However, we can also consider within the same framework the inclusion of measurement noise in the output equation of the plant, i.e.,

$$y(t) = Cx(t) + \eta(t), \tag{25}$$

where $\eta(t) \in \mathbb{R}^q$ denotes a vector whose components correspond to bounded measurement noise for each output. In this case, and due to the particular structure of the considered observers (see Section 2.3), it is convenient to select $H=0$ in order to avoid terms including the noise time derivative, $\dot{\eta}(t)$, that would appear in the dynamics of the state estimation errors (see (18) and (22)). Alternatively, one can assume the knowledge of bounds for both the measurement disturbance and its derivative, in which case the analysis of this paper applies with minor modifications to account for the terms added by these bounded signals.

4. DETERMINISTIC ACTUATOR FAULT DIAGNOSIS

4.1. Set computation

The computation of ultimate bound sets for the state trajectories of the closed-loop system described in Section 3 is explained in this section.

First, ultimate bounds for $z_{i,j}(t)$ and $\zeta_{i,j}(t)$ are computed, whose dynamics obey (20) with inputs $u_{\mathrm{ref},j}(t) = \bar{u}_{\mathrm{ref},j} + \tilde{u}_{\mathrm{ref},j}(t)$, and $d(t)$ (which are bounded signals, see Assumptions 2.1 and 2.3). These variables can be expressed, respectively, as $z_{i,j}(t) = \bar{z}_{i,j} + \tilde{z}_{i,j}(t)$, and $\zeta_{i,j}(t) = \bar{\zeta}_{i,j} + \tilde{\zeta}_{i,j}(t)$, where $\bar{z}_{i,j}$ and $\bar{\zeta}_{i,j}$ are constant offset levels while $\tilde{z}_{i,j}(t)$ and $\tilde{\zeta}_{i,j}(t)$ are variations around their respective offsets. The offset levels can be computed from (20) in steady state with constant input $\bar{\varphi}_j = \begin{bmatrix} \bar{u}_{\mathrm{ref},j} \\ 0 \end{bmatrix}$, and are given by

$$\begin{bmatrix} \bar{z}_{i,j} \\ \bar{\zeta}_{i,j} \end{bmatrix} = -{A_{i,j}}^{-1} B_{i,j} \bar{\varphi}_j. \tag{26}$$

Performing the change of coordinates

$$\tilde{u}_{\mathrm{ref},j}(t) = u_{\mathrm{ref},j}(t) - \bar{u}_{\mathrm{ref},j}, \quad \tilde{z}_{i,j}(t) = z_{i,j}(t) - \bar{z}_{i,j} \quad \text{and} \quad \tilde{\zeta}_{i,j}(t) = \zeta_{i,j}(t) - \bar{\zeta}_{i,j},$$

Equation (20) can be expressed as

$$\begin{bmatrix} \dot{\tilde{z}}_{i,j}(t) \\ \dot{\tilde{\zeta}}_{i,j}(t) \end{bmatrix} = A_{i,j} \begin{bmatrix} \tilde{z}_{i,j}(t) \\ \tilde{\zeta}_{i,j}(t) \end{bmatrix} + B_{i,j} \tilde{\varphi}_j(t), \tag{27}$$

where $\tilde{\varphi}_j(t) = \begin{bmatrix} \tilde{u}_{\mathrm{ref},j}(t) \\ d(t) \end{bmatrix}$.

According to Assumption 3.1, matrix $A_{i,j}$ in (27) is the Hurwitz for all $i = 0, \ldots, m$ and for all $j = 0, \ldots, m$. Moreover, by Assumptions 2.1 and 2.3, the inputs in (27) are bounded as $|\tilde{u}_{\mathrm{ref},j}(t)| \leqslant \tilde{u}^{\max}_{\mathrm{ref},j}$, and $|d(t)| \leqslant d^{\max}$. Therefore, (a minor modification of) Theorem 1 in [2] can be used in order to compute ultimate bounds on the elements of $\begin{bmatrix} \tilde{z}_{i,j}(t) \\ \tilde{\zeta}_{i,j}(t) \end{bmatrix}$ as

$$\left| \begin{bmatrix} \tilde{z}_{i,j}(t) \\ \tilde{\zeta}_{i,j}(t) \end{bmatrix} \right| \leqslant \begin{bmatrix} \tilde{z}^{\max}_{i,j} \\ \tilde{\zeta}^{\max}_{i,j} \end{bmatrix}, \tag{28}$$

where

$$\begin{bmatrix} \tilde{z}^{\max}_{i,j} \\ \tilde{\zeta}^{\max}_{i,j} \end{bmatrix} = |V_{i,j}| |(\mathbf{Re}(\Lambda_{i,j}))^{-1}| |V_{i,j}^{-1} B_{i,j}| \begin{bmatrix} \tilde{u}^{\max}_{\mathrm{ref},j} \\ d^{\max} \end{bmatrix}, \tag{29}$$

and $(\Lambda_{i,j}, V_{i,j})$ are the matrices of the Jordan decomposition $A_{i,j} = V_{i,j} \Lambda_{i,j} V_{i,j}^{-1}$. Thus, if the closed-loop dynamics (27) were to hold indefinitely (that is, without changes in the fault situation i and in the FDI decision j), the state estimation error $\zeta_{i,j}(t) \triangleq \tilde{x}^j_{i,j}(t)$, corresponding to the observer selected by the FDI (i.e. $k = j$), would ultimately

converge to the set

$$\mathscr{S}^{j}_{i,j} \triangleq \{\zeta_{i,j} \in \mathbb{R}^n : |\zeta_{i,j} - \bar{\zeta}_{i,j}| \leqslant \tilde{\zeta}^{\max}_{i,j}\}, \quad i=0,\ldots,m, \quad j=0,\ldots,m, \tag{30}$$

where $\bar{\zeta}_{i,j}$ and $\tilde{\zeta}^{\max}_{i,j}$ are defined in (26) and (29), respectively.

Following similar steps, we compute invariant sets for the state estimation errors $\tilde{x}^k_{i,j}(t)$ in (24), for $i=0,\ldots,m$, $j=0,\ldots,m$, $k=0,\ldots,m$, $k\neq j$. The latter errors can be expressed as $\tilde{x}^k_{i,j}(t)=\bar{\chi}^k_{i,j}+\tilde{\chi}^k_{i,j}(t)$, where the offset levels are computed from (24) as

$$\bar{\chi}^k_{i,j} = -F^{-1}N^k_{i,j}\bar{v}_{i,j}, \tag{31}$$

with $N^k_{i,j}$ as in (23) and

$$\bar{v}_{i,j} = [\bar{z}^{\mathrm{T}}_{i,j} \;\; \bar{\zeta}^{T}_{i,j} \;\; \bar{u}^{\mathrm{T}}_{\mathrm{ref},j} \;\; 0]^{\mathrm{T}}. \tag{32}$$

In addition, the dynamics for the variations of the state estimation error around its offset level are given by

$$\dot{\tilde{\chi}}^k_{i,j}(t) = F\tilde{\chi}^k_{i,j}(t) + N^k_{i,j}\tilde{v}_{i,j}(t), \tag{33}$$

with $\tilde{v}_{i,j}(t)=[\tilde{z}_{i,j}(t)^{\mathrm{T}} \;\; \tilde{\zeta}_{i,j}(t)^{\mathrm{T}} \;\; \tilde{u}_{\mathrm{ref},j}(t)^{\mathrm{T}} \;\; d(t)^{\mathrm{T}}]^{\mathrm{T}}$. Using again Theorem 1 in [2], with $F=V\Lambda V^{-1}$, invariant sets for the variations of the state estimation errors around the offset levels (31) can be computed as

$$\tilde{\mathscr{S}}^k_{i,j} = \left\{ \tilde{\chi}^k_{i,j} \in \mathbb{R}^n : |V^{-1}\tilde{\chi}^k_{i,j}| \leqslant |(\mathbf{Re}(\Lambda))^{-1}||V^{-1}N^k_{i,j}| \begin{bmatrix} \tilde{z}^{\max}_{i,j} \\ \tilde{\zeta}^{\max}_{i,j} \\ \tilde{u}^{\max}_{\mathrm{ref},j} \\ d^{\max} \end{bmatrix} \right\}, \tag{34}$$

where $\tilde{z}^{\max}_{i,j}$ and $\tilde{\zeta}^{\max}_{i,j}$ were previously computed in (29). Noting that $\tilde{x}^k_{i,j}(t)=\bar{\chi}^k_{i,j}+\tilde{\chi}^k_{i,j}(t)$, then an invariant set for the state estimation error, $\mathscr{S}^k_{i,j}$, when $k\neq j$, can be computed as the Minkowski sum of the set $\tilde{\mathscr{S}}^k_{i,j}$ in (34) and the singleton $\{\bar{\chi}^k_{i,j}\}$ whose value is given in (31). Thus, we have

$$\mathscr{S}^k_{i,j} = \tilde{\mathscr{S}}^k_{i,j} \oplus \{\bar{\chi}^k_{i,j}\}, \quad i=0,\ldots,m, \quad j=0,\ldots,m, \quad k=0,\ldots,m, \quad k\neq j. \tag{35}$$

It should be noted that the sets in (35) are invariant and attractive for the state estimation error trajectories, see [2]. That is, trajectories starting inside the set will remain inside the set, whereas trajectories starting outside will converge towards the set.‡

Substituting (4b) and (12) in (11), and using (14), the output estimation error $e^k_{i,j}(t)$ can be written as

$$\begin{aligned} e^k_{i,j}(t) &= Cx_{i,j}(t) - C\hat{x}^k_{i,j}(t), \\ &= C\tilde{x}^k_{i,j}(t). \end{aligned} \tag{36}$$

‡To be rigorous, the right-hand side of the inequalities defining the sets in (29) and (34) have to be expanded by a vector of arbitrarily small positive components in order to guarantee convergence to the sets in finite time.

Thus, sets where the output estimation errors $e^k_{i,j}(t)$ will lie whenever $\tilde{x}^k_{i,j}(t)$ belong to $\mathscr{S}^k_{i,j}$, can be computed using (30), (35), and (36) as

$$\begin{aligned}\mathscr{E}^k_{i,j} &\triangleq C\mathscr{S}^k_{i,j} \\ &= \left\{ e^k_{i,j} \in \mathbb{R}^n : e^k_{i,j} = C\tilde{x}^k_{i,j}, \tilde{x}^k_{i,j} \in \mathscr{S}^k_{i,j} \right\}, \end{aligned} \tag{37}$$

for $i=0,\ldots,m$, $j=0,\ldots,m$, $k=0,\ldots,m$.

Remark 4.1
The sets defined when $i=j=k$ in (30) and $i=k\neq j$ in (35) deserve special attention. In the case $k=i=j$, the dynamics of the state estimation error $\zeta_{i,j}(t)\triangleq\tilde{x}^j_{i,j}(t)$ in (19)–(20), for $j=0,\ldots,m$, are given by

$$\dot{\zeta}_{j,j}(t) = F\zeta_{j,j}(t) + GEd(t). \tag{38}$$

Similarly, when $k=i\neq j$, the dynamics of the state estimation errors $\tilde{x}^k_{i,j}(t)$ in (23)–(24), for $j=0,\ldots,m$, $k=0,\ldots,m$, $k\neq j$, becomes

$$\dot{\tilde{x}}^k_{k,j}(t) = F\tilde{x}^k_{k,j}(t) + GEd(t). \tag{39}$$

Thus, for all observers $k=0,\ldots,m$ (including the one selected by the FDI to implement the control law, $k=j$), an invariant set for the state estimation error dynamics when $L_k=L_i$ (see (3)) is given by

$$\mathscr{S}^k_{k,j} = \{\tilde{\chi}^k_{k,j} \in \mathbb{R}^n : |V^{-1}\tilde{\chi}^k_{k,j}| \leqslant |(\mathbf{Re}(\Lambda))^{-1}||V^{-1}GE|d^{\max}\}. \tag{40}$$

That is, when the kth observer (7a) has matrix L_k that *matches* the current fault situation of the plant, represented by L_i in (4), the state estimation error dynamics converge to the set $\mathscr{S}^k_{k,j}$ defined in (40), independantly of the control law in use, and therefore the corresponding output estimation error dynamics tends to $\mathscr{E}^k_{k,j}\triangleq C\mathscr{S}^k_{k,j}$. Notice that $d(t)$ is assumed to have no offset level and then these sets $\mathscr{E}^k_{k,j}$ will be centred at the origin of the output estimation error space. Also note from (40) that these sets are independant of the index j selected by the FDI module, and will be hence denoted as

$$\mathscr{E}^k_{k,*}\triangleq C\mathscr{S}^k_{k,j}, \tag{41}$$

with $\mathscr{S}^k_{k,j}$ defined in (40).

4.2. Fault detection criterion

A key property that the proposed fault-tolerant scheme requires is that the sets $\mathscr{E}^k_{i,j}$ in (37), for all $i=0,\ldots,m$, $j=0,\ldots,m$, $i\neq k$ (i.e. when the kth observer does not match the current fault situation of the plant), do not intersect the sets $\mathscr{E}^k_{k,*}$ in (41) for the output estimation error corresponding to each observer with index $k=0,\ldots,m$. That is

$$\mathscr{E}^k_{i,j} \cap \mathscr{E}^k_{k,*} = \emptyset, \quad \text{for } i=0,\ldots,m,\ \ j=0,\ldots,m,\ \ k=0,\ldots,m,\ \ i\neq k. \tag{42}$$

To simplify the FDI mechanism, we will assume that the sets in (42) can be separated by balls centred around the origin, so that the following condition is satisfied:

$$\min\left\{ \|e^k_{i,j}\|_2 : e^k_{i,j} \in \bigcup_{i=0, i\neq k}^{m} \bigcup_{j=0}^{m} \mathscr{E}^k_{i,j} \right\} > \max\{\|e^k_{i,j}\|_2 : e^k_{i,j} \in \mathscr{E}^k_{k,*}\}, \tag{43}$$

for each $k=0,\ldots,m$. In Section 4.3 below, mechanisms to achieve this set separation will be discussed, but for the moment, it will be assumed that condition (43) holds. Recall also that when $i=k$ (i.e. when the kth observer matches the current fault situation) the output estimation error trajectories converge to $\mathscr{E}^k_{k,*}$ as explained in Remark 4.1.

The FDI approach proposed in this paper considers balls $\mathscr{B}_{r_k}$ centred around the origin of the output estimation error space for each observer. The radii of these balls, denoted by r_k, are determined in such a way that the kth ball contains the set $\mathscr{E}^k_{k,*}$, and it does not overlap with any of the sets $\mathscr{E}^k_{i,j}$ computed from (37), when $i\neq k$. Then, the condition for selecting a control configuration depends on whether the output estimation error trajectory remains inside the ball corresponding to one and only one of the observers at a given time. However, this condition is related to the time of convergence of the state estimation error trajectories. We will denote by t_c an upper bound for the convergence time of trajectories starting in any set $\mathscr{S}^k_{i,j}$ and ending up in any other set $\mathscr{S}^k_{l,h}$ (when driven by the dynamics related to the latter set), for all $i,j,l,h\in\{0,\ldots,m\}$ and each $k=0,\ldots,m$, including $i=k$. Note that the time t_c should be computed based on the sets $\mathscr{S}^k_{i,j}$ instead of sets $\mathscr{E}^k_{i,j}$, since the latter sets are not invariant and therefore an output estimation error trajectory which enters to a set $\mathscr{E}^k_{i,j}$ does not necessarily remain inside that set.

The FDI decision module is constantly checking for trajectories which are inside the corresponding ball $\mathscr{B}_{r_k}$ for each output estimation error space. If a fault occurs, the trajectories will either change between sets or stay in them. In particular, the fault will be detected when the (only) output estimation error trajectory that was inside its associated ball leaves the ball. In order to avoid abrupt changes in situations when, due to transient behaviour, there are two or more trajectories inside their corresponding balls $\mathscr{B}_{r_k}$, or when a different trajectory from the one that should converge to the set $\mathscr{E}^k_{k,*}$ for the current fault scenario crosses its ball $\mathscr{B}_{r_k}$ during a transient, the algorithm waits a time t_c in order to ensure that all trajectories have converged to the new sets. After this time t_c, the whole system is again checked and only one of the trajectories of $e^k_{i,j}(t)$—the one related to the observer which *matches* the plant behaviour—will be inside the corresponding ball $\mathscr{B}_{r_k}$. This determines the new FDI decision index $j\in\{0,\ldots,m\}$. Note that, the feature of waiting a time t_c before changing the FDI decision prevents from undesired oscillations in the FDI decisions and in the closed-loop behaviour. Summarizing, the fault detection criterion implemented by the FDI can be outlined as follows:

Algorithm 4.1 (**FDI criterion**)

1. *While* $e^k_{i,j}(t)$, *for some* $k\in\{0,\ldots,m\}$, *is inside the corresponding ball* $\mathscr{B}_{r_k}$, *keep control law* K_j *in place*, *with* $j=k$;
2. *If* $e^k_{i,j}(t)$ *leaves the corresponding ball* $\mathscr{B}_{r_k}$, *wait for* t_c *units of time*;
3. *Check all trajectories* $e^k_{i,j}(t), t\geqslant t_c$, *for* $k=0,\ldots,m$. *Choose the control law* $K_{\tilde{j}}$, *with* $\tilde{j}=\tilde{k}$, *corresponding to the trajectory* $e^{\tilde{k}}_{i,\tilde{j}}(t)$ *that is inside the corresponding ball* $\mathscr{B}_{r_{\tilde{k}}}$.

As a result of the implementation of Algorithm 4.1, the index j is obtained by the FDI module, which will fix the corresponding feedback control gain K_j, the signals from the exosystem, $x_{\mathrm{ref},j}(t)$ and $u_{\mathrm{ref},j}(t)$, and the corresponding state estimate $\hat{x}^j_{i,j}(t)$ at the SES.

Remark 4.2
The convergence time t_c can be estimated in a number of ways, for example, using a slight modification of Theorem 7.3 in [11].

The operation of the fault detection scheme is illustrated in Figure 2. In the figure, the output estimation error spaces of three observers ($k=0,1,2$) have been conceptually depicted.[§] Consider two fault modes in the plant, for

[§] With some abuse of notation, the vector components in the estimation error spaces are denoted by e_1 and e_2.

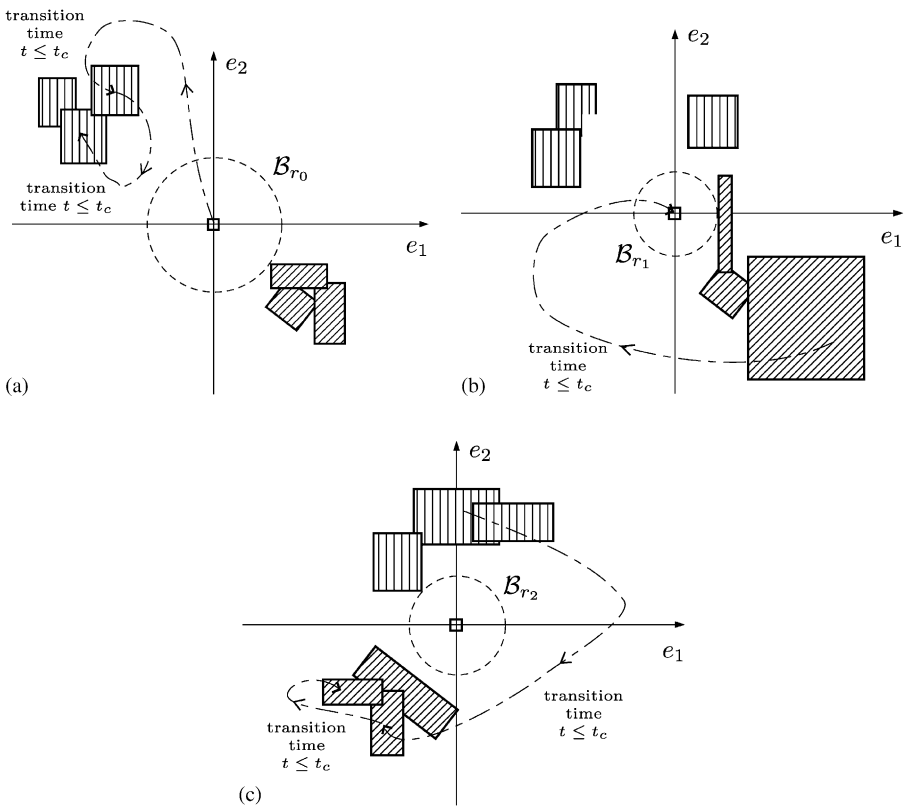

Figure 2. Conceptual scheme of the set approach: (a) sets for observer 0; (b) sets for observer 1; and (c) sets for observer 2.

$i=0$, and $i=1$. The initial fault situation of the plant, $i=0$, is such that L_i in (4) is matched by the observer $k=0$. Consequently, the trajectories of observer 0 are in the set $\mathscr{E}^0_{0,*}$, depicted in Figure 2(a) as the little square centred at the origin ($L_k=L_i$, for $k=i=0$), whereas the trajectories of observers 1 and 2 lie in their corresponding sets $\mathscr{E}^1_{0,j}$ and $\mathscr{E}^2_{0,j}$, depicted in Figure 2(a) as the two groups of three sets away from the origin (since $L_k \neq L_i$ for $k=1,2$ and $i=0$). At some point in time, a new fault situation in the plant (fault mode $i=1$) changes L_i in (3) so that now it is matched by observer 1 ($L_k=L_i$, for $k=1$ and $i=1$). Therefore, according to Remark 4.1, the trajectories of observer 1 will converge to the set $\mathscr{E}^1_{1,*}$, centred at the origin, and the trajectories of observers 0 and 2 will converge to the corresponding sets $\mathscr{E}^0_{1,j}$ and $\mathscr{E}^2_{1,j}$, respectively, outside the balls $\mathscr{B}_{r_k}$, $k=0,2$ (since $L_k \neq L_i$ for $k=0,2$, and $i=1$). All the transitions between sets illustrated in Figure 2 will take a time less than the upper bound t_c, hence by the time the FDI makes a new decision (new index j), all trajectories will have converged to their respective sets, reflecting the new fault situation in the plant. When the FDI switches to the configuration that corresponds to the new fault situation that has been correctly identified, all the trajectories away from the corresponding set centred at the origin will experience a new transient towards the sets related to the new control configuration. This situation is illustrated in Figure 2(a) for the case of observer 0 and Figure 2(c) for the case of observer 2. However, the trajectory of observer 1 in Figure 2(b) will remain in the set $\mathscr{E}^1_{1,*}$, centred at the origin, according to Remark 4.1 (since $L_k=L_i$ for $k=1$, and $i=1$).

4.3. Conditions for correct fault diagnosis

As mentioned above, and illustrated in Figure 2, the separation condition condition (43) is a key feature that is required for correct fault diagnosis based on the FDI criterion presented in Section 4.2. Some design mechanisms for the overall reference tracking control system will be discussed in this section, which can be used in order to achieve the required set separation.

Three aspects play an important role in the separation of the sets. First of all, an offset value for the reference signal $y^*(t)$, to be followed by the exosystem (and in turn by the plant), will imply an offset value, $\bar{u}_{\mathrm{ref},j}$, for the reference input. The latter offset also implies an offset in the corresponding sets $\mathscr{E}^k_{i,j}$ (see (26), (30), (31), and (35)). In order to achieve the desired set separation, the reference offset value $\bar{u}_{\mathrm{ref},j}$ should be 'large enough' with respect to the disturbance bound $d^{\max}$.

Second, the condition given in Assumption 2.2 implies that, in the presence of a fault—as evaluated by the FDI—in a particular actuator $j\in\{1,\ldots,m\}$, according to (3), the jth component of the input vector $u_j(t)\in\mathbb{R}^m$ related to the faulty actuator constitutes a *degree of freedom*, which can be varied conveniently so as to achieve the desired set separation. Notice that this jth component of the input vector will not be seen by the plant when the FDI decision matches the fault situation due to the type of fault model considered in this paper (total outage). Therefore, an offset term can be introduced by redefining the control reference from the exosystem corresponding to a fault in the jth component as

$$u'_{\mathrm{ref},j}(t)\triangleq u_{\mathrm{ref},j}(t)+u_{\mathrm{df},j}, \tag{44}$$

where

$$u_{\mathrm{df},j}=\begin{cases}\Upsilon[0\cdots\overset{j}{\underset{\downarrow}{1}}\cdots 0]^{\mathrm{T}} & \text{for fault situation,}\\ [0\cdots 0]^{\mathrm{T}} & \text{for nominal situation}\end{cases} \tag{45}$$

denotes the degree of freedom added to the jth element of the input vector. Diagonal matrix Υ contains the values of the added offset levels for each component of the input vector according to the actuator. Notice that, in the nominal case, i.e. no faults, there is no degree of freedom and then $u_{\mathrm{df},j}$ is a column vector of m zeros. Thus, the control signal (15) can be now written as

$$u_j(t)\triangleq K_j z_{i,j}(t)-K_j\zeta_{i,j}(t)+u'_{\mathrm{ref},j}(t). \tag{46}$$

Several signals within the scheme of Figure 1 would be affected by the addition of this offset levels. The main influence of $u_{\mathrm{df},j}$ can be seen in the offset levels of the state tracking and estimation errors. For instance, matrices $B_{i,j}$ and $\bar{\varphi}_j$ in (26) (from (19)) are now redefined as

$$B_{i,j}\triangleq\begin{bmatrix}B(L_i-L_j) & E & B(L_i-L_j)\\ GB(L_i-L_j) & GE & GB(L_i-L_j)\end{bmatrix},\quad \bar{\varphi}_j\triangleq\begin{bmatrix}\bar{u}_{\mathrm{ref},j}\\ 0\\ u_{\mathrm{df},j}\end{bmatrix},$$

the right-hand side bound in (29) is now written as

$$\begin{bmatrix}\tilde{u}^{\max}_{\mathrm{ref},j}\\ d^{\max}\\ 0\end{bmatrix},$$

and matrices $N_{i,j}^k$ and $\bar{v}_{i,j}$ in (31) (from (23)) are redefined as

$$N_{i,j}^k = [GB(L_i - L_k)K_j \;\; -GB(L_i - L_k)K_j \;\; GB(L_i - L_k) \;\; GE \;\; GB(L_i - L_k)], \tag{47a}$$

$$\bar{v}_{i,j} = [\bar{z}_{i,j}^{\mathrm{T}} \;\; \bar{\zeta}_{i,j}^{\mathrm{T}} \;\; \bar{u}_{\mathrm{ref},j}^{\mathrm{T}} \;\; 0 \;\; u_{\mathrm{df},j}^{\mathrm{T}}]^{\mathrm{T}}. \tag{47b}$$

Notice that the offset level of the output estimation error trajectories can be computed from (31) and (36) as

$$\begin{aligned} \bar{e}_{i,j}^k &\triangleq C\bar{\chi}_{i,j}^k, \\ &= -CF^{-1}N_{i,j}^k\bar{v}_{i,j}, \end{aligned} \tag{48}$$

where $N_{i,j}^k$ and $\bar{v}_{i,j}$ are given in (47).

Finally, and related to the previous situation, since the jth input channel is not seen by the plant, there is flexibility in the design of the jth row of the feedback control gain K_j which, again, will influence the offset levels of the output estimation error trajectories according to (47) and (48). However, the use of this mechanism to achieve set separation is subject to the satisfaction of Assumption 3.1. Note that, when a row of K_j is conveniently changed in order to achieve the set separation, the resulting K_j does not necessarily stabilize the closed-loop. Therefore, Assumption 3.1 must be verified when modifying K_j.

4.4. Closed-loop stability

The proof of stability is based on the following assumptions related to the fault scenario that the scheme can handle and the set separation condition.

Assumption 4.1
Condition (43) holds.

Assumption 4.2
The minimum time interval between any change in fault scenario is greater than $2t_c$, where t_c is an upper bound for the convergence time of the trajectories of $\tilde{x}_{i,j}^k(t)$ starting in any set $\mathscr{S}_{i,j}^k$ and ending up in any other set $\mathscr{S}_{l,h}^k$, for all $i, j, l, h \in \{0, \ldots, m\}$, and each $k = 0, \ldots, m$.

We then have the following result.

Theorem 4.1
Under the conditions stated in Assumptions 2.1–2.4, 3.1, and 4.1. the system (4), in closed loop with control law (10) reconfigured by the FDI criterion of Algorithm 4.1, is closed-loop stable and, in the absence of disturbances, the output $y_{i,j}(t)$ follows the reference trajectory $y^*(t)$ for any fault scenario that satisfies Assumption 4.2.

Proof
From Assumption 4.2, if L_{i_1} has been the matrix associated with the system condition for a sufficiently long time (greater than $2t_c$), then it follows that before the occurrence of a new fault scenario, all the output estimation error trajectories for the observers for which $L_{k_1} \neq L_{i_1}$ are inside their corresponding sets and outside the ball $\mathscr{B}_{r_{k_1}}$ (Assumption 4.1). Moreover, the trajectory corresponding to the observer for which $i_1 = k_1$ remains within the set $\mathscr{E}_{k_1,*}^{k_1}$ centred at the origin (Remark 4.1) and inside the ball $\mathscr{B}_{r_{k_1}}$. When the next fault scenario i_2 occurs, there will be only one new observer that matches the new fault mode ($L_{k_2} = L_{i_2}$, $k_2 \neq k_1$) whose trajectory will converge towards the set $\mathscr{E}_{k_2,*}^{k_2}$ (see Remark 4.1). All the output estimation error trajectories will migrate to their new

corresponding sets, in particular the trajectory previously confined to the set $\mathscr{E}_{k_1,*}^{k_1}$ corresponding to the observer that no longer matches the current fault situation. When the trajectory of the latter observer leaves the corresponding ball $\mathscr{B}_{r_{k_1}}$ centred at the origin, the FDI detects the presence of the new fault situation in the plant. By design, the FDI will not make a new decision until a time t_c has elapsed (Algorithm 4.1). This implies, since t_c is an upper bound for all convergence times between sets, that all output estimation error trajectories will have settled down in their new sets by the time the FDI makes the decision $j_2 = i_2$, guaranteeing the correctness of the decision. The reconfiguration of the whole fault-tolerant scheme caused by the FDI decision will imply that all trajectories will once more move towards new sets, attractive for the new control configuration according to (20) and (24). However, the output estimation error trajectories of the matched observer ($L_{k_2} = L_{i_2}$) will continue to remain inside the set $\mathscr{E}_{k_2,*}^{k_2}$. Assumption 4.2 guarantees that all the previously described transients occur before the appearance of a new fault scenario, which ensures the correct operation of the fault detection and reconfiguration scheme and, hence, the boundedness of all closed-loop trajectories at all times.

Moreover, from Assumption 3.1, $A_{i,j}$ with $i = j = i_2$ is Hurwitz. It then follows from (20) and the previous discussion that, since the FDI effectively identifies the fault, the closed-loop tracking error in (13) will converge towards zero in steady state (before the occurrence of the new fault situation) in the absence of disturbances. Finally, (5b) and (6) imply that, in the absence of disturbances, the plant output $y_{i,j}(t) = Cx_{i,j}(t)$ follows the reference trajectory $y^*(t)$. □

5. NUMERICAL EXAMPLE

This section presents an example based on an electric circuit, where the fault-tolerant approach proposed in this paper is used when a set of preestablished fault scenarios are considered. The sets computed for each case were plotted using the multi-parametric toolbox (MPT) for Matlab® [12].

Consider the electric circuit shown in Figure 3, whose equations in state-space representation can be written as in (4), with the following system matrices:

$$A = \begin{bmatrix} -\dfrac{1}{R_{eq}C_p} & \dfrac{R_1}{R_{eq}C_p} \\ \dfrac{1}{L}\left(\dfrac{R_2}{R_{eq}} - 1\right) & -\dfrac{1}{L}\left(\dfrac{R_1 R_2}{R_{eq}} - R_3\right) \end{bmatrix},$$

$$B = \begin{bmatrix} \dfrac{1}{R_{eq}C_p} & 0 \\ -\dfrac{R_2}{L R_{eq}} & \dfrac{1}{L} \end{bmatrix} \quad \text{and} \quad E = \begin{bmatrix} \dfrac{\alpha_1}{R_{eq}C_p} \\ \dfrac{1}{L}\left(\alpha_2 - \dfrac{R_2}{R_{eq}}\alpha_1\right) \end{bmatrix},$$

where $R_1 = R_3 = 20\,\Omega$, $R_2 = 1\,\mathrm{K}\Omega$, $L = 80\,\mathrm{mH}$, $C_p = 50\,\mu\mathrm{F}$, and $R_{eq} = R_1 + R_2$. The state variables correspond to the capacitor voltage, $v_C(t)$, and the inductor current, $i_L(t)$. In Figure 3, the signal $d(t)$ represents a disturbance introduced to the circuit by inductive coupling with an external circuit (not represented in the figure). This effect has been modelled using dependant linear voltage sources with proportionality constants α_1 and α_2, whose values are $\alpha_1 = \alpha_2 = 1$. This external disturbance signal is bounded as $|d(t)| \leqslant d^{\max}$, with $d^{\max} = 1.5$.

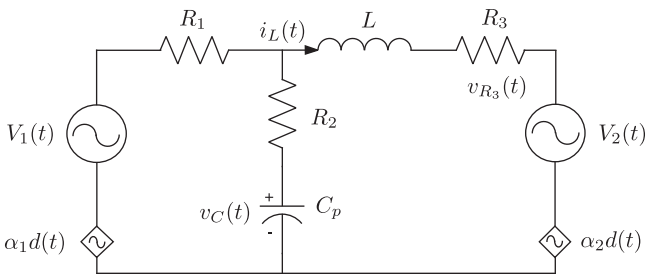

Figure 3. Electrical circuit used as a case study for FTC.

The capacitor voltage is required to track a reference signal of the form

$$y^*(t) = a + b\sin\omega t,$$

where $\omega = 20\pi$, $a = 50\,\mathrm{V}$, and $b = 1.5\,\mathrm{V}$.

The fault scenarios considered are:

- SCENARIO 0: Both voltage sources, V_1 and V_2, are operational. This scenario is modelled by $L_i = L_0$, where

$$L_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

- SCENARIO 1: Voltage source V_1 is short-circuited, that is $V_1(t) = 0$, and V_2 is operational. This fault scenario is modelled by $L_i = L_1$, where

$$L_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

- SCENARIO 2: Voltage source V_2 is short-circuited, that is $V_2(t) = 0$, and V_1 is operational. This fault scenario is modelled by $L_i = L_2$, where

$$L_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

We assume that the capacitor voltage, $v_C(t)$, and the voltage in resistor R_3, i.e. $v_{R_3}(t) = R_3 i_L(t)$, are measured (this is assumed only for better visualisation of the different sets in the output estimation error space but similar analyses can be carried out if only one of the state variables is measured). Therefore, the output matrix in (4b) is written as:

$$C = \begin{bmatrix} 1 & 0 \\ 0 & R_3 \end{bmatrix}.$$

The state observers are designed as described in Section 2.3, with $H = \mathrm{diag}[-2 \;\; -0.2]$, and $M_1 = \mathrm{diag}[250 \;\; -1]$. The feedback control gains K_j used for the control signal in (46) are designed using the LQR methodology. They are computed from the algebraic Riccati equation

$$P = A^{\mathrm{T}}PA + Q - K_j^{\mathrm{T}}(R + (BL_j)^{\mathrm{T}}PBL_j)K_j, \tag{49a}$$

$$K_j = (R + (BL_j)^{\mathrm{T}}PBL_j)^{-1}(BL_j)^{\mathrm{T}}PA, \tag{49b}$$

with L_j as in (3), for $i=0,1,2$, according to the corresponding fault scenarios described above. The weighting matrices used in (49) are $R=0.1I$ and $Q=I$, where I corresponds to the identity matrix of suitable dimensions. It was verified by direct calculation that Assumption 3.1 holds for this example. The reference signals used for the simulations satisfy $u_{\mathrm{ref},j}(t)=\bar{u}_{\mathrm{ref},j}+\tilde{u}_{\mathrm{ref},j}(t)$, where $\bar{u}_{\mathrm{ref},0}=[55,45]^{\mathrm{T}}$, $\bar{u}_{\mathrm{ref},1}=[0,100]^{\mathrm{T}}$, $\bar{u}_{\mathrm{ref},2}=[100,0]^{\mathrm{T}}$, and $|\tilde{u}_{\mathrm{ref},0}(t)|\leqslant[35,25]^{\mathrm{T}}$, $|\tilde{u}_{\mathrm{ref},1}(t)|\leqslant[0,11]^{\mathrm{T}}$, $|\tilde{u}_{\mathrm{ref},2}(t)|\leqslant[11,0]^{\mathrm{T}}$. The values used for the degree of freedom in the control signal were set as $u_{\mathrm{df},0}=[0,0]^{\mathrm{T}}$, $u_{\mathrm{df},1}=[100,0]^{\mathrm{T}}$, and $u_{\mathrm{df},2}=[0,100]^{\mathrm{T}}$.

Figure 4 shows the sequence of fault scenarios considered (top graph), and the FDI decision output, according to Algorithm 4.1 with $t_c=0.004\,\mathrm{s}$. In this figure, values 0, 1 and 2 are related to SCENARIO 0, SCENARIO 1, and SCENARIO 2, respectively, as described above. Although the *simultaneous* commutation between two faulty scenarios is unlikely, this situation has been contemplated in this simulations at times $t=0.3\,\mathrm{s}$, and $t=2.1\,\mathrm{s}$, in order to test the operation of the FDI scheme. Note from the simulations that the FDI module makes, in all cases, the right decision after a time t_c.

Figure 5 shows the system performance under the proposed scheme when the sequence of fault scenarios in Figure 4 (top graph) is considered. Notice that both the measured and estimated capacitor voltage tend to follow

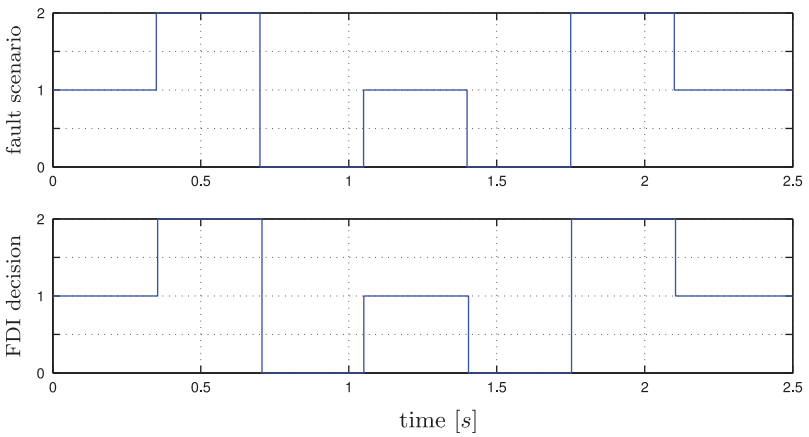

Figure 4. Sequence of simulated fault scenarios (top graphic) and the corresponding FDI decision (bottom graphic).

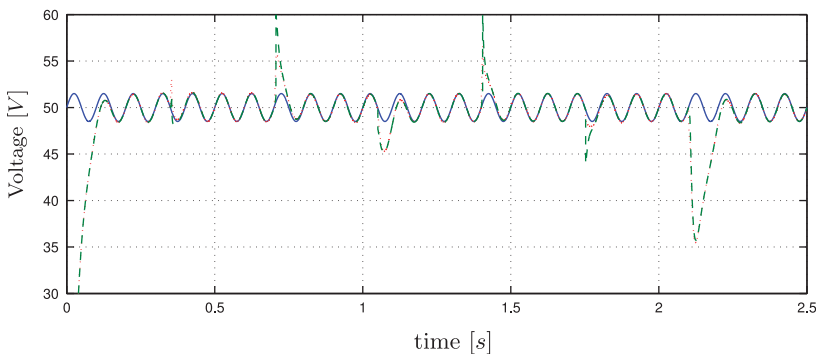

Figure 5. Voltage signals. Continuous line: reference $y^*(t)$, dashed line: estimated capacitor voltage $\hat{v}_C(t)$ (at the output of the SES), dotted line: measured capacitor voltage $v_C(t)$.

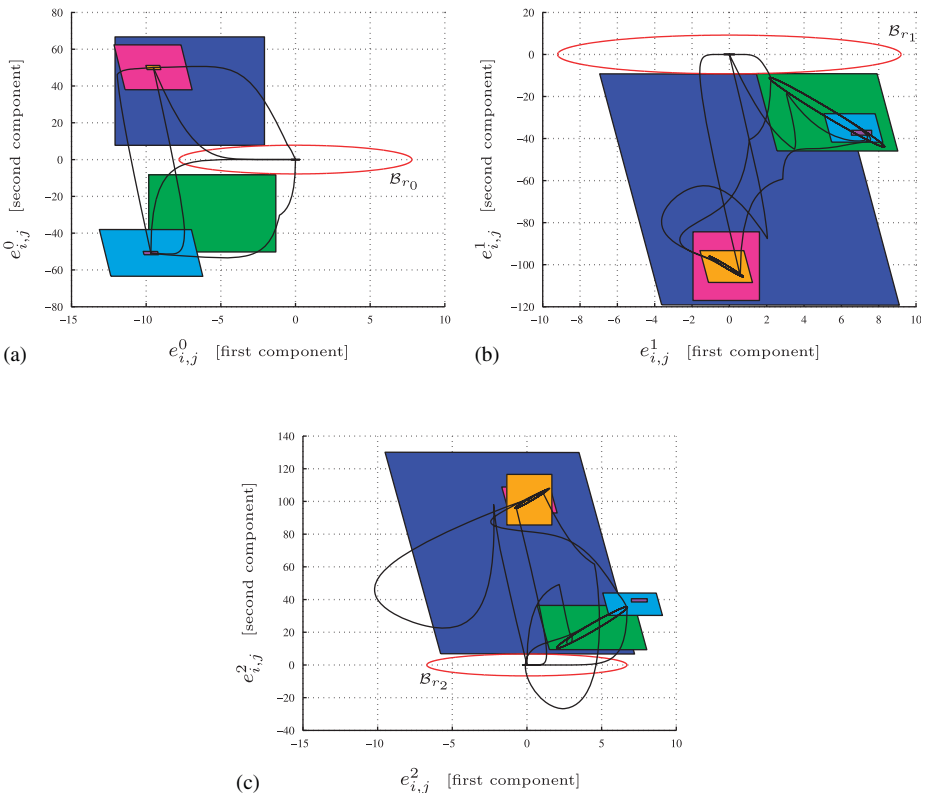

Figure 6. Sets for the observers of the electric circuit example. Also shown are the balls $\mathscr{B}_{r_k}$ around the origin upon which the FDI decisions are based: (a) sets related to the observer $k=0$; (b) sets related to the observer $k=1$; and (c) sets related to the observer $k=2$.

the system reference after the fault occurrence showing that the closed-loop performance is recovered after the corresponding transient by the fault-tolerant strategy, and the control objective is achieved.

The sets $\mathscr{E}^k_{i,j}$ for the output estimation errors corresponding to each of the k observers, $k=0,1,2$, each of the possible fault scenarios, $i=0,1,2$, and each of the feedback control gains K_j, $j=0,1,2$, are computed using (30), (31), (35), and (37). These sets are depicted in Figure 6, together with the balls $\mathscr{B}_{r_k}$, around the origin for $k=0,1,2$, upon which the FDI decisions are based[¶] (see Algorithm 4.1). Notice that the output estimation error trajectories in Figure 6(c) cross the corresponding ball $\mathscr{B}_{r_2}$ when the commutation between SCENARIO 0 and SCENARIO 1 occurs. In this case, without the inclusion of a waiting time t_c in the FDI criterion, the FDI module could diagnose, erroneously, SCENARIO 2 because the output estimation error trajectories related to observer $k=2$ could be the only trajectories inside a ball at some time instant. However, the FDI criterion avoids these transients by means of the waiting time t_c and the fault diagnosis is done properly. Finally, we remark that the overall operation of the fault-tolerant scheme satisfies the desired control objectives; namely, it maintains closed-loop stability and achieves reference tracking under all fault scenarios contemplated.

[¶]Note that the balls $\mathscr{B}_{r_k}$ appear as ellipses in Figure 6 due to the scales used.

6. CONCLUSIONS

This paper has proposed an actuator FTC scheme based on the computation of estimation errors from a bank of observers. Each observer is designed to match, with a distinctive behaviour, the different fault situations that can occur in the plant. The main novelty of the scheme resides in the computation of invariant sets where the output estimation errors corresponding to each fault situation lie, and the appropriate use of information concerning the separation of these sets by a fault diagnosis and isolation (FDI) module in the selection of a matching controller from a bank of precomputed stabilising controllers. More importantly, conditions for guaranteeing the correct decision of the FDI, and hence stability and fault tolerance of the scheme, are given under a set of assumptions. The effectiveness of the approach has been illustrated by using an example based on an electric circuit. Future work is focused on relaxing the set of assumptions this approach is based on, in order to generalise the family of systems to which the FDI strategy is suitable. Also, further research includes the use of different feedback stabilising control laws within the proposed scheme and the consideration of disturbances whose values are not centred around zero, which modifies the position of sets $\mathscr{E}_{k,*}^{k}$ in the output estimation error space.

REFERENCES

1. Blanke M, Kinnaert M, Lunze J, Staroswiecki M. *Diagnosis and Fault-tolerant Control* (2nd edn). Springer: Berlin, 2006.
2. Kofman E, Haimovich H, Seron MM. A systematic method to obtain ultimate bounds for perturbed systems. *International Journal of Control* 2007; **80**(2):167–178.
3. Wang D, Lum KY. Adaptive unknown input observer approach for aircraft actuator fault detection and isolation. *International Journal of Adaptive Control and Signal Processing* 2007; **21**:31–48.
4. Hajiyev C, Caliskan F. Sensor/actuator fault diagnosis based on statistical analysis of innovation sequence and robust Kalman filtering. *Aerospace Science and Technology* 2000; **4**:415–422.
5. Larson Jr EBP, Clark B. Model-based sensor and actuator fault detection and isolation. *Proceedings of the American Control Conference*, Anchorange, AK, 2002.
6. Seron MM, Zhuo X, De Doná J, Martinez J. Multisensor switching control strategy with fault tolerance guarantees. *Automatica* 2008; **44**(1):88–97.
7. Ocampo-Martinez C, De Doná JA, Seron MM. Actuator fault-tolerant control based on invariant set separation. *Proceedings of the IFAC World Conference*, Seoul, Korea, 2008.
8. Seron MM, De Doná JA, Martinez J. Invariant set approach to actuator fault-tolerant control. *7th IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes* (*Safeprocess*), Barcelona, Spain, 2009; 1605–1610.
9. VanAntwerp J, Braatz R. A tutorial on linear and bilinear matrix inequalities. *Journal of Process Control* 2000; **10**:363–385.
10. Holmström K, Edvall MM, Göran AO. Tomlab—for large-scale robust optimization. *Proceedings of the Nordic MATLAB Conference*, Copenhagen, Denmark, 2003.
11. Haimovich H. Quantisation issues in feedback control. *Ph.D. Thesis*, School of Electrical Engineering and Computer Science, The University of Newcastle, Australia March 2006. Available from: http://usuarios.fceia.unr.edu.ar/~haimo.
12. Kvasnica M, Grieder P, Baotić M. Multi-parametric toolbox (MPT), 2004. Available from: http://control.ee.ethz.ch/~mpt/.