Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Actuator Fault-Tolerant Control based on Invariant Set Separation

Carlos Ocampo-Martínez José De Doná María M. Seron

ARC Centre of Excellence for Complex Dynamic Systems and Control (CDSC)
The *University* of *Newcastle, Callaghan, NSW, 2308, Australia*
e-mail: {Carlos.Ocampo-Martinez, Jose.Dedona, Maria.Seron}@ newcastle.edu.au

Abstract: In this paper an actuator fault-tolerant control (FTC) strategy based on invariant set computation is presented. The proposed scheme is based on a bank of observers which match different fault situations that can occur in the plant. Each of these observers produces an estimation error with a distinctive behavior when the observer matches the current fault situation in the plant. With the information of the estimation errors from each of the considered observers, 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 decision criteria of the FDI is based on the computation of invariant sets of the estimation errors for each fault scenario and for each control configuration. 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 with an example.

Keywords: 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 behavior). It is known that those abnormal situations due to instrument or component failure can prevent or endanger continuous operation. A classic treatment of fault-tolerant control (FTC) systems is given in Blanke et al. (2003). In the present study, attention is focused on 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 fault-tolerant control (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 invariant set computation (see, e.g., Kofman et al. (2007)). The proposed scheme consists of a bank of *unknown input observers* (UIO), see Wang and Lum (2007), which match different fault situations that could occur in the plant. Each one of these observers produces an estimation error with a distinctive behavior when the estimator matches the current fault situation in the plant. With the information of the estimation errors, the 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 decision criteria of the FDI is based on the computation of invariant sets of the estimation errors of each observer for each fault scenario and for each control configuration.

A key property for the correct fault diagnosis in the proposed scheme is the separation of the invariant sets that characterise healthy operation from the ones that characterise faulty operation. The inherent component redundancy that is required for an actuator fault-tolerant 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, especially when the reference signal contains an offset component. In those cases, the reference signal provides an additional mechanism to achieve 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, firstly, 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. Secondly, a remarkable feature is the simplicity of the fault diagnosis and isolation 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 very simple, its complexity depending linearly on the number of actuators that can possibly fail. In contrast with other schemes, (see, e.g., Larson et al.

(2002); Hajiyev and Caliskan (2000)), 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. The work presented in this paper was inspired by previous results on fault-tolerant multisensor switching control, see Seron et al. (2008). However, the *actuator* fault-tolerant problem has posed 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.

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.

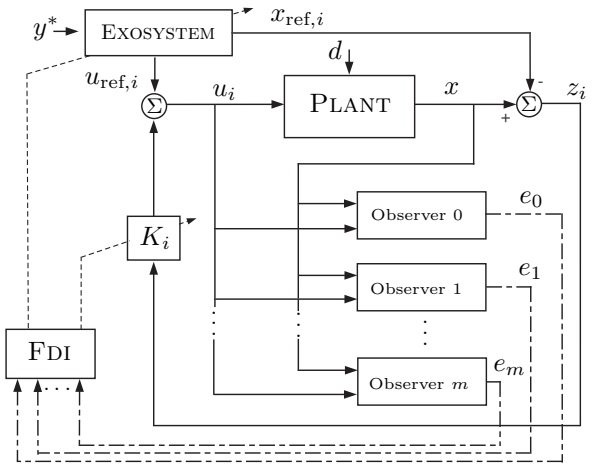


Fig. 1. Proposed fault detection and reconfiguration scheme.

2.1 Nominal Plant and Fault Models

We consider a linear perturbed system described by

$$\dot{x}(t) = Ax(t) + BLu_i(t) + Ed(t), \tag{1a}$$

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

where $x(t) \in \mathbb{R}^n$ is the system state, $u_i(t) \in \mathbb{R}^m$ is the control input (where the subindex i will be explained in the following sections), $d(t) \in \mathbb{R}^p$ is an unknown disturbance assumed to be bounded, i.e., $|d(t)| \leq d^{\max}$, where $d^{\max} \in \mathbb{R}^p$ is a vector with positive components. $y(t) \in \mathbb{R}^q$ is the 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

$$L \triangleq \mathrm{diag}[l_1 \quad l_2 \quad \dots \quad l_m], \quad l_i \in \{0, 1\}. \tag{2}$$

As mentioned in the introduction, this paper is focused on severe (outage) actuator faults. Accordingly, the case $l_i = 1$ represents no fault in the i-th actuator; whereas, $l_i = 0$ models an outage in the i-th actuator. In the nominal case, i.e., no faults, L is the identity matrix ($L_0 = I$). 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 $L = L_k$, where

$$L_0 = I, \quad L_k = \mathrm{diag}[1 \ \dots \ \overset{k}{\underset{\downarrow}{0}} \ \dots \ 1], \quad k = 1, \dots, m. \tag{3}$$

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

Assumption 2.1. The system (1)–(2) is controllable for all possible values of $L = L_k$, with $k = 0, \dots, m$, as defined in (3). ∘

We remark that, provided the system continues to be controllable, simultaneous outage of more than one actuator can also be contemplated within the present framework.

2.2 Exosystem for Reference Tracking

The exosystem module generates input and state reference trajectories, $u_{\mathrm{ref},i}(t)$ and $x_{\mathrm{ref},i}(t)$, for each possible fault situation, that is, for each possible value of the matrix L in (3). These reference trajectories satisfy

$$\dot{x}_{\mathrm{ref},i}(t) = Ax_{\mathrm{ref},i}(t) + BL_iu_{\mathrm{ref},i}(t), \tag{4}$$

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

with $i = 0, \dots, m$, where $x_{\mathrm{ref},i}$ and $u_{\mathrm{ref},i}$ are bounded signals. Notice that this is always possible by using an auxiliary control loop inside the exosystem, since the exosystem model (4)–(5) *mimics* the plant model and, hence, also satisfies Assumption 2.1. The exosystem (4)–(5) is designed such that its output tracks exponentially a signal $y^*(t)$, that is

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

where $y^*(t)$ is an output reference trajectory that we ultimately wish the plant output $y(t)$ to follow under all possible fault situations. To guarantee the latter objective, stabilising state feedback gains are designed (see Section 2.3 below) which ensure that, in the absence of disturbances, the system state $x(t)$ in (1) asymptotically tracks the exosystem reference states $x_{\mathrm{ref},i}(t)$ for each possible fault situation.

2.3 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_i in Figure 1 and satisfy the following assumption.

Assumption 2.2. The feedback control gains K_i are such that the closed-loop matrices $A + BL_kK_i$, for $i = 0, \dots, m$ and $k = 0, \dots, m$, are Hurwitz. ∘

In combination with the exosystem described in Section 2.2, these gains guarantee the desired tracking objective that the system output $y(t)$ in (1) asymptotically track the output reference trajectory $y^*(t)$ in the absence of disturbances. In order to achieve this objective for the nominal and each possible fault scenarios, the state tracking error is defined as

$$z_i(t) \triangleq x(t) - x_{\mathrm{ref},i}(t), \tag{7}$$

for $i = 0, \ldots, m$, and the control law assumes the form

$$u_i(t) \triangleq K_i z_i(t) + u_{\text{ref},i}(t). \tag{8}$$

The FDI module (described below in Section 2.5) decides the index $i \in \{0, \ldots, m\}$ that corresponds to the evaluated scenario and passes the corresponding control input (8) to the plant (1). Hence, from (1), (4), (7), and (8), the dynamics of the state tracking error $z_i(t)$ are written as

$$\dot{z}_i(t) = (A + BLK_i)z_i(t) + B(L - L_i)u_{\text{ref},i} + Ed(t). \tag{9}$$

2.4 Plant State Observers

The actuator fault detection is done using a bank of unknown input observers (UIO) of the form proposed in Wang and Lum (2007), namely,

$$\dot{w}_j^i(t) = Fw_j^i(t) + GBL_j u_i(t) + Mx(t), \tag{10a}$$

$$\hat{x}_j^i(t) = w_j^i(t) + Hx(t), \tag{10b}$$

with $j = 1, \ldots, m$, where $\hat{x}_j^i(t) \in \mathbb{R}^n$ is the state estimate, $w_j^i(t) \in \mathbb{R}^n$ is the observer state, $u_i(t)$ is the control input (8) applied to the plant, $x(t)$ is the plant state assumed to be available for measurement, and L_j are as defined in (3). F, G, M, and H are matrices to be designed below. The estimation error for each observer is defined as

$$e_j^i(t) \triangleq x(t) - \hat{x}_j^i(t). \tag{11}$$

Substituting (1) and (10) in the time derivative of (11), the dynamics of the estimation error can be written as

$$\begin{aligned}\dot{e}_j^i(t) = {} & [A - HA - M_1]\, e_j^i(t) + [(I - H)BL - GBL_j]\, u_i(t) \\ & + (I - H)Ed(t) + [(A - HA - M_1) - F]\, w_j^i(t) \\ & + [(A - HA - M_1)H - M_2]\, x(t),\end{aligned}$$

where $M = M_1 + M_2$, M_1 and M_2 being design matrices to be determined. Following Wang and Lum (2007), we choose the matrices F, G, H, M_1, and M_2 such that

$$G = I - H, \quad GE = 0, \tag{12a}$$

$$F = GA - M_1, \quad M_2 = FH, \tag{12b}$$

with F a Hurwitz matrix. The estimation error dynamics then satisfy

$$\dot{e}_j^i(t) = Fe_j^i(t) + GB(L - L_j)u_i(t). \tag{13}$$

Finally, substituting $u_i(t)$ from (8) in (13) yields

$$\dot{e}_j^i(t) = Fe_j^i(t) + GB(L - L_j)K_i z_i(t) + GB(L - L_j)u_{\text{ref},i}. \tag{14}$$

Notice that (9)–(13) define, for fixed i and j, a stable system excited by bounded inputs, hence the error trajectories will converge to the invariant sets that will be computed in Section 3.1 below.

2.5 Fault Diagnosis and Isolation (FDI) Module

This module receives the estimation errors obtained from the observers described in Section 2.4. The approach for diagnosis and isolation by the FDI, with guaranteed fault tolerance, is the main contribution of this paper. This approach is described in Section 3 below. Once the fault is detected and isolated, the FDI module selects the appropriate index i for both the feedback control law and the exosystem, and this index is used to implement the control input (8). Thus, in the absence of disturbances, the tracking error $z_i(t)$ defined in (7) asymptotically tends to zero and, in consequence, $y(t)$ asymptotically tends to $y^*(t)$, as desired.

3. DETERMINISTIC ACTUATOR FAULT DIAGNOSIS

3.1 Invariant Sets Computation

The computation of the invariant sets for each estimation error $e_j^i(t)$ in (14) is explained in this section. From (14) we note that the dynamics of the estimation errors are stable with inputs $u_{\text{ref},i}(t)$ and $z_i(t)$. The reference input $u_{\text{ref},i}(t)$ is assumed to be bounded (see Section 2.2) and can be expressed as $u_{\text{ref},i}(t) = \bar{u}_{\text{ref},i} + \tilde{u}_{\text{ref},i}(t)$, where $\bar{u}_{\text{ref},i}$ is a constant offset level and $\tilde{u}_{\text{ref},i}(t)$ is a variation around the offset, with amplitude bounded as $|\tilde{u}_{\text{ref},i}(t)| \leq \tilde{u}_{\text{ref},i}^{\max}$, for all t.

Next, we compute ultimate bounds for the state tracking error $z_i(t)$, whose dynamics obey (9) with inputs $u_{\text{ref},i}(t) = \bar{u}_{\text{ref},i} + \tilde{u}_{\text{ref},i}(t)$ (as explained above) and $d(t)$. The latter is the unknown disturbance, whose values are assumed to be centered around zero and bounded by $|d(t)| \leq d^{\max}$. We can then express the state tracking error as $z_i(t) = \bar{z}_i + \tilde{z}_i(t)$, where $\bar{z}_i$ is a constant offset level and $\tilde{z}_i(t)$ is a variation around that offset. The offset level can be computed from (9) in steady state with constant input $\bar{u}_{\text{ref},i}$, and is given by:

$$\bar{z}_i = -(A + BLK_i)^{-1} B(L - L_i)\bar{u}_{\text{ref},i}. \tag{15}$$

Performing the change of coordinates $\tilde{u}_{\text{ref},i}(t) = u_{\text{ref},i}(t) - \overline{u}_{\text{ref},i}$ and $\tilde{z}_i(t) = z_i(t) - \bar{z}_i$, we can express equation (9) as

$$\dot{\tilde{z}}_i(t) = (A + BLK_i)\tilde{z}_i(t) + B(L - L_i)\tilde{u}_{\text{ref},i}(t) + Ed(t). \tag{16}$$

According to Assumption 2.2 and the fact that the inputs are bounded as $|\tilde{u}_{\text{ref},i}(t)| \leq \tilde{u}_{\text{ref},i}^{\max}$ and $|d(t)| \leq d^{\max}$, we can then use (a minor modification of) Theorem 1 in Kofman et al. (2007) to compute ultimate bounds on the elements of $\tilde{z}_i(t)$ as $|\tilde{z}_i(t)| \leq \tilde{z}_i^{\max}$, where the bounds are given by

$$\tilde{z}_i^{\max} = |V_i|\, \left|(\mathbf{Re}(\Lambda_i))^{-1}\right|\, \left|V_i^{-1}[E \;\; B(L - L_i)]\right| \begin{bmatrix} d^{\max} \\ \tilde{u}_{\text{ref},i}^{\max} \end{bmatrix}, \tag{17}$$

and where (Λ_i, V_i) correspond to the Jordan decomposition $A + BLK_i = V_i \Lambda_i V_i^{-1}$.

Finally, following similar steps, invariant sets for the estimation errors $e_j^i(t)$ in (14) are computed. We call $\Upsilon_j = GB(L - L_j)$, and express the estimation errors as $e_j^i(t) = \overline{e}_j^i + \tilde{e}_j^i(t)$, where the offset level is computed from

$$\overline{e}_j^i = -F^{-1}\Upsilon_j(K_i \bar{z}_i + \overline{u}_{\text{ref},i}). \tag{18}$$

Hence, the dynamics for the variations of the estimation error around the offset level are given by:

$$\dot{\tilde{e}}_j^i(t) = F\tilde{e}_j^i(t) + \Upsilon_j K_i \tilde{z}_i(t) + \Upsilon_j \tilde{u}_{\text{ref},i}(t). \tag{19}$$

Using again Theorem 1 in Kofman et al. (2007), with $F = V\Lambda V^{-1}$, invariant sets for the variations of the estimation errors around the offset level are computed as

$$\begin{aligned}\tilde{\mathcal{S}}_j^i = \Big\{ \tilde{e}_j^i \in \mathbb{R}^n \,:\, & \left|V^{-1}\tilde{e}_i\right| \leq \left|(\mathbf{Re}(\Lambda))^{-1}\right| \\ & \left|V^{-1}[\Upsilon_j K_i \quad \Upsilon_j]\right| \begin{bmatrix} \tilde{z}_i^{\max} \\ \tilde{u}_{\text{ref},i}^{\max} \end{bmatrix} \Big\},\end{aligned} \tag{20}$$

where $\tilde{z}_i^{\max}$ was previously obtained in (17). Noting that $e_j^i(t) = \overline{e}_j^i + \tilde{e}_j^i(t)$, then an invariant set for the estimation error, $\mathcal{S}_j^i$, can be computed as the Minkowski sum of the set $\tilde{\mathcal{S}}_j^i$ in (20) and the singleton $\{\overline{e}_j^i\}$ whose value is computed from (18). Thus we have:

$$\mathcal{S}_j^i = \tilde{\mathcal{S}}_j^i \oplus \{\overline{e}_j^i\}. \tag{21}$$

Remark 3.1. It should be noted that the sets in (21) are invariant and attractive for the estimation error trajectories, see Kofman et al. (2007). That is, trajectories starting inside the set will remain inside the set, whereas trajectories starting outside will converge towards the set. [1] ∘

Remark 3.2. Notice from (18), (20), and (21) that, when $L_j = L$, we have $\Upsilon_j = 0$ and hence $\mathcal{S}_j^i = \{0\}$. That is, when the j-th observer has matrix L_j (cf. (14)) that *matches* the current fault situation of the plant, represented by L in (1), the estimation error dynamics converge to zero. ∘

3.2 Fault Detection Criterion

A key property that the proposed scheme requires is that the invariant sets $\mathcal{S}_j^i$ computed using (18), (20), and (21), are separated from the origin when $L_j \neq L$ (i.e., when the j-th observer does not match the current fault situation of the plant). In Section 3.3 below, we will discuss mechanisms to achieve this set separation, but for the moment, it will be assumed that this is the case. Recall also, that when $L_j = L$ the estimation error trajectories converge to zero with dynamics $\dot{e}_j^i(t) = Fe_j^i(t)$ [see (13)].

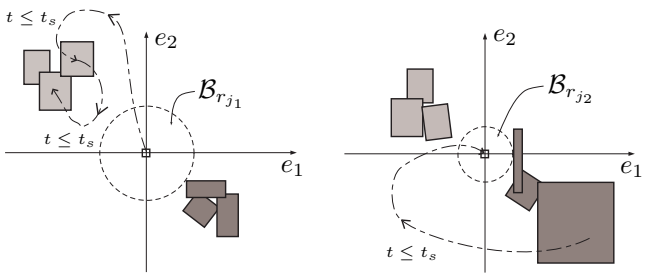
The FDI approach proposed in this paper considers balls $\mathcal{B}_{r_j}$ centered around the origin of the error space for each observer. The radii of these balls, r_j, are determined in such a way that they do not overlap with any of the invariant sets $\mathcal{S}_j^i$ computed beforehand from (21), when $L_j \neq L$. Then, the condition for selecting a control configuration depends on whether the error trajectory remains inside of this ball for one and only one of the observers at a given time. However, this condition is related to the time of convergence of the estimation error trajectories. We will denote by t_s an upper bound for the convergence time of trajectories starting in any set $\mathcal{S}_j^i$ and ending up in any other set $\mathcal{S}_l^r$, for all $i, j, l, r \in \{0, \ldots, m\}$. (This upper bound time t_s can be adjusted by the design of the matrix F—see (12b)—that governs the dynamics of the estimation error trajectories according to (14).)

The criterion implemented by the FDI is as follows:

Algorithm 3.1. (FDI Criterion).

(1) While $e_j^i(t)$, for some $j \in \{0, \ldots, m\}$, is inside the corresponding ball $\mathcal{B}_{r_j}$ around the origin, keep control law K_i in place, with $i = j$;
(2) If $e_j^i(t)$ leaves the corresponding ball $\mathcal{B}_{r_j}$ around the origin, wait for t_s units of time;
(3) Check all trajectories $e_j^i(t)$, $t \geq t_s$, for $j = 0, \ldots, m$. Choose the control law K_i, with $i = \tilde{\jmath}$, corresponding to the trajectory $e_{\tilde{\jmath}}^i(t)$ inside the corresponding ball $\mathcal{B}_{r_{\tilde{\jmath}}}$ around the origin.

[1] To be rigorous, the right hand side of the inequalities defining the invariant sets in (20) should be expanded by a vector of arbitrarily small positive components in order to guarantee convergence to the invariant sets in finite time. However, this technicality will be avoided for simplicity of exposition.



(a) Invariant sets for observer j_1. (b) Invariant sets for observer j_2.

Fig. 2. Conceptual scheme of the invariant set approach.

Note that, in order to avoid abrupt changes in situations when, due to transient behavior, there are two or more trajectories inside of their corresponding balls or when, a trajectory different from the one that should converge to the origin for the current fault scenario crosses its ball during a transient, the FDI decision according to the criterion above remains the same for a time t_s necessary for the transient behavior to settle down. This feature (hysteresis) prevents from undesired oscillations in the FDI decisions and on the closed-loop behavior.

The operation of the fault detection scheme is illustrated in Figure 2. In the figure, the estimation error spaces of two observers have been conceptually depicted. [2] The initial fault situation in the plant is such that L in (1) is matched by the observer matrix L_{j_1}. Consequently, the trajectories of observer j_1 are at the origin ($L_{j_1} = L$), whereas the trajectories of observers j_2 lie on their corresponding invariant sets $S_{j_2}^i$, away from the origin (since $L_{j_2} \neq L$). At some point in time, the fault situation in the plant changes L so that it is now matched by observer j_2 ($L_{j_2} = L$). Therefore, according to Remark 3.2, the trajectories of observer j_2 will converge to the origin and the trajectories of the observer j_1 will converge to the corresponding invariant set $S_{j_1}^i$, away from the origin (since $L_{j_1} \neq L$). All the transitions between sets illustrated in Figure 2 will take a time less than the upper bound t_s, hence by the time the FDI makes a new decision, all trajectories will have converged to their respective invariant sets, reflecting the new fault situation in the plant. Once the FDI switches to the controller that corresponds to the new fault situation, all the trajectories away from the origin will experience a new transient to the invariant sets related to the new controller. This situation is illustrated, for observer j_1, in Figure 2(a). However, the trajectory of observer j_2 will remain at the origin according to Remark 3.2 (since $L_{j_2} = L$).

3.3 Conditions for Correct Fault Diagnosis

As mentioned above, and illustrated in Figure 2, a key feature that is required for correct fault diagnosis based on the FDI criterion presented in Section 3.2, is for the sets $\mathcal{S}_j^i$ to be separated from the origin whenever $L_j \neq L$. Depending of the problem setup, some of these

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

sets could overlap with the origin. We will discuss below some design mechanisms for the overall reference tracking control system, that can be used in order to achieve the required set separation.

Three aspects play an important role in the separation of the invariant sets. Firstly, 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, $\bar{u}_{\mathrm{ref},i}$, for the reference input. This offset implies in turn an offset in the corresponding invariant sets $\mathcal{S}_j^i$. Secondly, according to Assumption 2.1, in the presence of a fault in a particular actuator $k \in \{1, \ldots, m\}$, the k-th component of the input vector $u_i \in \mathbb{R}^m$ related to the faulty actuator constitutes a *degree of freedom* which can be varied conveniently so as to achieve set separation. Notice that this k-th component of the input vector will not be seen by the plant due to the type of fault model considered (total outage). This component can be introduced by the new control signal

$$u_i(t) \triangleq K_i z_i(t) + u_{\mathrm{ref},i}(t) + u_{\mathrm{df},i}, \tag{22}$$

where $u_{\mathrm{df},i}$ denotes the aforementioned degree of freedom. The offset level of $e_j^i(t)$in (18) is now given by

$$\overline{e}_j^i = -F^{-1}\Upsilon_j \left(K_i \bar{z}_i + \bar{u}_{\mathrm{ref},i} + u_{\mathrm{df},i}\right). \tag{23}$$

Finally, and related to the previous situation, since the k-th input channel is not seen by the plant, there is flexibility in the design of the k-th row of the feedback control gain K_i which, again, will influence the offset level of the estimation error trajectories according to (23).

3.4 Closed Loop Stability

Our stability proof is based on the following assumptions related to the fault scenario and set separation.

Assumption 3.1. When $L_j \neq L$, $0 \notin \mathcal{S}_j^i$, where the sets $\mathcal{S}_j^i$ are computed as in (21). ∘

Assumption 3.2. Before the occurrence of the first change in fault scenario, the system has been operating under a particular condition for a sufficiently long time such that all estimation error trajectories are inside the corresponding invariant sets. ∘

Assumption 3.3. The minimum time interval between faults, denoted by t_f, satisfies

$$t_f \geq 2t_s \tag{24}$$

where t_s is an upper bound for the convergence time of trajectories starting in any set $\mathcal{S}_j^i$ and ending up in any other set $\mathcal{S}_l^r$, for all $i, j, l, r \in \{0, \ldots, m\}$. ∘

We then have the following result.

Theorem 1. Under the conditions stated in Assumptions 2.2, 3.1 and 3.2, the system (1), in closed loop with control law (8) reconfigured by the FDI criterion of Algorithm 3.1, is closed-loop stable and, in the absence of disturbances, its output $y(t)$ follows asymptotically the reference trajectory $y^*(t)$ for any fault scenario that satisfies Assumption 3.3.

Proof. (Outline) From Assumption 3.2, the system has been operating under a particular condition, say $L = L_{\hat{\jmath}}$, $\hat{\jmath} \in \{0, \ldots, m\}$, for a sufficiently long time. Then, it follows that before the occurrence of a new fault scenario, all the trajectories $e_j^i(t)$ for the observers for which $L_j \neq L$ are inside their corresponding invariant sets away from the origin (Assumption 3.1), and the trajectory corresponding to the observer for which $L_{\hat{\jmath}} = L$ remains at the origin (Remark 3.2). When the next fault scenario occurs, there will be only one new observer that matches the current fault scenario ($L_{\tilde{\jmath}} = L$, $\tilde{\jmath} \neq \hat{\jmath}$) whose trajectory will converge towards the origin. All the trajectories $e_j^i(t)$, for $j \neq \tilde{\jmath}$, will migrate to their new corresponding invariant sets (away from the origin by Assumption 3.1), in particular the previous trajectory at the origin corresponding to an observer that no longer matches the fault situation ($L_{\hat{\jmath}} \neq L$). When the trajectory of the latter observer leaves the corresponding ball $\mathcal{B}_{r_{\hat{\jmath}}}$ around the origin, the FDI detects the presence of the new fault situation. By design, the FDI will not make a new decision until a time t_s has elapsed (Algorithm 3.1). This implies, since t_s is an upper bound for all settling times, that all $e_j^i(t)$ trajectories will have settled down in their new invariant sets by the time the FDI makes the decision, guaranteeing the correctness of the decision. The reconfiguration of the control law induced by the FDI decision will imply that all trajectories will once again move towards new invariant sets, attractive for the new control configuration according to (14). However, the estimation error trajectories of the matched observer ($L_{\tilde{\jmath}} = L$) will continue to remain at the origin. Assumption 3.3 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. Note that the system will now be back in an operating condition that satisfies Assumption 3.2 and, hence, it is closed-loop stable since all trajectories will remain bounded. Moreover, from Assumption 2.2, $A + BLK_i$ with $i = \tilde{\jmath}$ is Hurwitz. It then follows from (9) that, since (see previous discussion) the FDI effectively identifies the fault ($L_i = L$, with $i = \tilde{\jmath}$), the state tracking error defined in (7) will, in the absence of disturbances, converges to zero in steady state (unless a new fault scenario occurs, in which case the analysis above has to be repeated). Finally, (6) implies that the plant output $y(t) = Cx(t)$ follows the reference trajectory $y^*(t)$. □

4. EXAMPLE

Consider the electric circuit shown in Figure 3, whose equations in state-space representation can be written as in (1), with the following system matrices:

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

$$B = \begin{bmatrix} \frac{1}{R_{eq}C} & 0 \\ -\frac{R_2}{LR_{eq}} & \frac{1}{L} \end{bmatrix}, \qquad E = \begin{bmatrix} \frac{\alpha_1}{R_{eq}C} \\ \frac{1}{L}\left(\alpha_2 - \frac{R_2}{R_{eq}}\alpha_1\right) \end{bmatrix},$$

where $R_1 = R_3 = 20\Omega$, $R_2 = 1K\Omega$, $L = 80mH$, $C = 50\mu F$, and $R_{eq} = R_1 + R_2$. The states (capacitor voltage, $v_C(t)$, and inductor current, $i_L(t)$) are available for measurement. 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 modeled using dependent linear voltage sources with proportionality constants α_1 and α_2, with values $\alpha_1 = \alpha_2 = 1$. This external disturbance signal is

bounded as $|d(t)| \leq d^{\max}$, with $d^{\max} = 1$. The capacitor voltage is required to track a reference signal of the form $y^*(t) = a + b \sin \omega t$, where $\omega = 20\pi$, $a = 50V$ and $b = 1.5V$. The fault scenarios considered are:

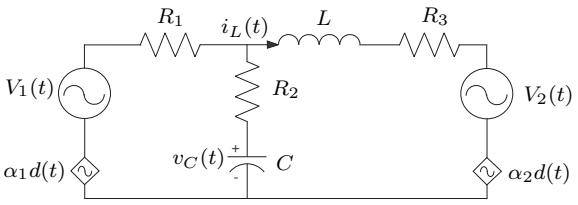


Fig. 3. Electrical circuit used as a case study for FTC.

- SCENARIO 0: Both voltage sources, V_1 and V_2, are operational. This scenario is modeled by $L = L_0$, where $L_0 = \text{diag}\,[1, 1]$.
- SCENARIO 1: Voltage source V_1 is short-circuited, that is $u_1(t) = 0$, and V_2 is operational. This fault scenario is modeled by $L = L_1$, where $L_1 = \text{diag}\,[0, 1]$.
- SCENARIO 2: Voltage source V_2 is short-circuited, that is $u_2(t) = 0$, and V_1 is operational. This fault scenario is modeled by $L = L_2$, where $L_2 = \text{diag}\,[1, 0]$.

The observers are designed as described in Section 2.4, with $H = EE^+$ (where E^+ denotes the pseudoinverse matrix of E), and $M_1 = \text{diag}\,[80, -1]$. The feedback control gains K_i used in (8), corresponding to the different fault scenarios with $i = 0, 1, 2$, are designed using the LQR methodology with $R = 0.1I$ and $Q = I$, where $I = \text{diag}\,[1, 1]$.

Figure 4 shows the sequence of fault scenarios considered and the FDI decision output, according to Algorithm 3.1 with $t_s = 0.004s$. In this figure, values 0, 1 and 2 are related to SCENARIO 0, SCENARIO 1, and SCENARIO 2, respectively, as described above. Although the instantaneous commutation between two faulty scenarios is unlikely, this situation has been contemplated in this simulation at $t = 0.9s$ to test the operation of the FDI scheme. Note from the simulation that the FDI makes, in all cases, the right decision after a time t_s. Figure 5 shows (due to space limitations) only the invariant sets $\mathcal{S}_j^i$ of observers related to SCENARIO 0 and SCENARIO 1, considering all feedback control gains. Also shown in the figures are the balls $\mathcal{B}_{r_0}$ and $\mathcal{B}_{r_1}$ around the origin, upon which the FDI decisions are based. (Note that the balls are distorted because of the scales employed in the representation.) Notice that the error trajectories in Figure 5(a) cross the corresponding balls when the commutation between SCENARIO 2 and SCENARIO 1, at time $t = 0.9$, occurs. In this case, the FDI diagnoses correctly due to the inclusion of a waiting time t_s in the FDI criterion. 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.

5. CONCLUSION

This paper has proposed a new actuator fault-tolerant control (FTC) scheme based on the computation of invariant sets where the estimation errors corresponding to each fault situation lie, and the appropriate use of

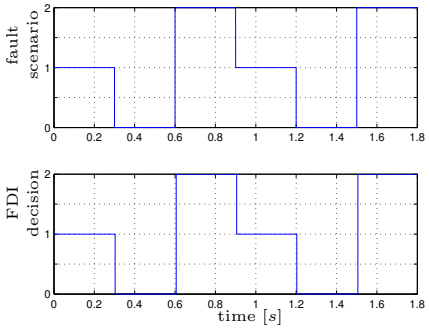
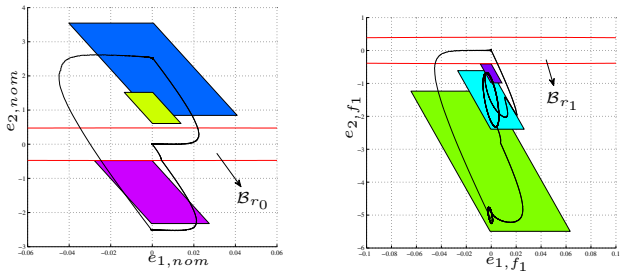


Fig. 4. Sequence of simulated fault scenarios (top graph) and the corresponding FDI decision (bottom graph).



(a) Invariant sets of observer related to SCENARIO 0.

(b) Invariant sets of observer related to SCENARIO 1.

Fig. 5. Invariant sets for the observers of the example. (Although not appreciated in Figure 5(a), there is a very small invariant set near the point (0,-2.6) towards which some trajectories transitorily converge.)

this information by a fault diagnosis and isolation (FDI) module in the selection of a matching controller from a bank of precomputed stabilising controllers. Conditions for guaranteeing the correct decision of the FDI, and hence stability and fault tolerance of the scheme, are given.

REFERENCES

M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag Berlin Heidelberg, 2003. ISBN 3-540-01056-4.

C. Hajiyev and F. Caliskan. Sensor/actuator fault diagnosis based on statistical analysis of innovation sequence and robust Kalman filtering. *Aerosp. Sci. Technol.*, 4: 415 – 422, 2000.

E. Kofman, H. Haimovich, and M. M. Seron. A systematic method to obtain ultimate bounds for perturbed systems. *International Journal of Control*, 80(2):167 – 178, 2007.

E.C. Larson, B.E. Parker Jr, and B.R. Clark. Model-based sensor and actuator fault detection and isolation. In *Proceedings of the Americal Control Conference*, Anchorange, AK, May 2002.

Maria M. Seron, Xiang W. Zhuo, José A. De Dona, and John J. Martínez. Multisensor switching control strategy with fault tolerance guarantees. *Automatica*, 44(1):88 – 97, January 2008.

Dan Wang and Kai-Yew Lum. Adaptive unknown input observer approach for aircraft actuator fault detection and isolation. *International Journal of Adaptive Control and Signal Processing*, 21:31 – 48, 2007.