NOVA

University of Newcastle Research Online

nova.newcastle.edu.au

Seron, María M., De Doná, José A., Martínez-Molina, John J., "Invariant set approach to actuator fault tolerant control". Originally published in Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (Barcelona, Spain 30 June - 3 July, 2009) p. 1605-1610, (2010).

Available from: <http://dx.doi.org/10.3182/20090630-4-ES-2003.00117>

Accessed from: <http://hdl.handle.net/1959.13/933955>

Invariant set approach to actuator fault tolerant control

María M. Seron* José A. De Doná*,¹ John J. Martínez**

* Centre for Complex Dynamic Systems and Control (CDSC), School of EE&CS, The University of Newcastle, Callaghan, NSW 2308, Australia, (email: {Maria.Seron, Jose.Dedona}@newcastle.edu.au)

** Gipsa-lab UMR 5216, Département Automatique. BP.46, St. Martin D'Hères 38440, France, (email: Jairo.Martinez@inpg.fr)

Abstract: We present a new actuator fault-tolerant control strategy based on the separation of sets that characterise healthy system operation from sets that characterise faulty operation. The new scheme is an extension of a similar strategy recently proposed by the authors. In the present paper we propose a new criterion for fault detection and isolation that leads to less conservative conditions for fault tolerant closed-loop stability. These new conditions employ discrete-time models for the plant, reference system and observers and allow for quicker fault detection and consequent reconfiguration of the controller.

Keywords: Fault tolerant systems, Actuators, Observers, Sets

1. INTRODUCTION

We have recently presented in Ocampo-Martínez et al. [2008] a new control scheme that tackles the problem of actuator fault tolerant control (FTC) within a new framework. The architecture of the scheme, which we preserve in the present paper, is similar to other FTC strategies previously proposed in the literature, see, for example, Chapter 7 in Blanke et al. [2006]. It consists 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 an estimator matches the current fault situation of the plant.
- A fault diagnosis and isolation (FDI) algorithm which, based on the information from each observer, 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 given fault models.
- A bank of control laws, each consisting of a reference feedforward term and a feedback gain multiplying the state estimate provided by the matching observer.

The novelty of the approach of Ocampo-Martínez et al. [2008] lies in a new decision criterion for FDI. This new criterion is based on the computation of sets towards which the estimation errors related to each fault scenario and associated control configuration converge. A key property for correct fault diagnosis is then the separation of the sets that characterise healthy operation from the ones that characterise faulty operation. In contrast with other schemes (see, e.g., Hajiyev and Caliskan [2000], Larson et al. [2002]), which use stochastic arguments for fault detection and control reconfiguration, the approach of Ocampo-Martínez et al. [2008] followed here is purely deterministic and does not require any statistical description neither for noises, disturbances nor fault occurrences.

In the present paper, we give improved, less conservative, conditions for the FDI algorithm and for fault tolerant closed-loop stability. These new conditions employ discrete-time models for the plant, reference system and observers and allow for quicker fault detection and consequent reconfiguration of the controller. The main reason for the quicker fault detection property is that we compute “after fault” sets which characterise the “one step ahead” transient faulty behaviour, thus allowing to detect the fault, and reconfigure the controller, *in one sampling instant* (as opposed to *in steady state*, as was the case in the approach of Ocampo-Martínez et al. [2008]). In addition, we relax the assumption in Ocampo-Martínez et al. [2008] of complete measurability of the state.

2. PLANT, OBSERVERS AND CONTROLLER

2.1 Plant and Actuator Fault Models

The plant is given by the linear discrete-time model

$$x^+ = Ax + BFu + Ew, \quad (1a)$$

$$y = Cx + \eta, \quad (1b)$$

where $x \in \mathbb{R}^n$ and $x^+ \in \mathbb{R}^n$ are, respectively, the current and successor system states, $u \in \mathbb{R}^m$ is the control input, $w \in \mathbb{R}^r$ is a bounded process disturbance, $y \in \mathbb{R}^p$ is the plant output and $\eta \in \mathbb{R}^p$ is a bounded measurement disturbance. Matrix $F \in \mathbb{R}^{m \times m}$ in (1a) is used to model actuator faults. To this end, we consider that F can take N different (a priori known) values $F \in \{F_1, F_2, \dots, F_N\}$, where, for $i = 1, \dots, N$,

$$F_i = \text{diag}(f_1, \dots, f_m), \quad f_j \in [0, 1]. \quad (2)$$

For example, $F = I_m$ (the $m \times m$ identity matrix) represents the “nominal” case, that is, no actuator fault, and

$$F = \text{diag}(1, \dots, \underset{i}{0}, \dots, 1)$$

models the loss of the i th actuator. We will say that an (abrupt) change in the actuator fault situation occurs if F

¹ On study leave at CAS, Mathématiques et Systèmes, Mines-ParisTech, France.

changes from $F = F_i$ to $F = F_j$, $i, j \in \{1, \dots, N\}$, $j \neq i$, at some discrete-time instant $k_F \geq 0$.

We assume the following properties of system (1).

Assumption 2.1. (Detectability and Stabilisability). The pair (A, C) is detectable and the pairs (A, BF_i) , for $i = 1, \dots, N$ are stabilisable. $\circ$

Assumption 2.2. (Disturbance Bounds). Bounding sets $\mathcal{W} \triangleq \{w \in \mathbb{R}^r : |w| \leq \bar{w}\}$ and $\mathcal{N} \triangleq \{\eta \in \mathbb{R}^p : |\eta| \leq \bar{\eta}\}$ for some constant nonnegative vectors $\bar{w} \in \mathbb{R}^r$ and $\bar{\eta} \in \mathbb{R}^p$ are known such that the process and measurement disturbances satisfy $w(k) \in \mathcal{W}$ and $\eta(k) \in \mathcal{N}$ for all discrete-time instants $k \geq 0$. $\circ$

2.2 Bank of State Observers

The scheme employs a bank of N state observers given by

$$\hat{x}_i^+ = A\hat{x}_i + BF_i u + L_i(y - C\hat{x}_i), \quad i = 1, \dots, N, \quad (3)$$

where $\hat{x}_i \in \mathbb{R}^n$ is the state estimate associated with the i th fault situation, u and y are the plant input and output and F_i is as defined in (2).

Assumption 2.3. (Observer Gains). The gains L_i , for $i = 1, \dots, N$, are such that $A - L_i C$ are Schur matrices. $\circ$

Note that the above assumption can always be satisfied by detectability of the pair (A, C) (see Assumption 2.1).

To each observer we associate the state estimation error

$$\tilde{x}_i \triangleq x - \hat{x}_i, \quad (4)$$

and the output estimation error

$$e_i \triangleq y - C\hat{x}_i = C\tilde{x}_i + \eta, \quad (5)$$

for $i = 1, \dots, N$. From (1a) and (3), the estimation errors satisfy

$$\tilde{x}_i^+ = (A - L_i C)\tilde{x}_i + B(F - F_i)u + Ew - L_i \eta. \quad (6)$$

Note that the estimation error of the observer that matches the actual plant situation ($F_i = F$) evolves with dynamics

$$\tilde{x}_i^+ = (A - L_i C)\tilde{x}_i + Ew - L_i \eta, \quad (7)$$

independent from the control input u . This property will be key to the FDI principle explained in Section 4 below.

2.3 Reference Tracking Controller

The FDI algorithm (described below in Section 4) decides the index ℓ , $\ell \in \{1, \dots, N\}$, that corresponds to the “evaluated” fault situation and passes the corresponding state estimate $\hat{x}_\ell$ to implement the following controller:⁴

$$u = -K_\ell(\hat{x}_\ell - x_{\text{ref}}) + u_{\text{ref},\ell}, \quad (8)$$

$$x_{\text{ref}}^+ = A x_{\text{ref}} + BF_\ell u_{\text{ref}}, \quad u_{\text{ref}} = u_{\text{ref},\ell}. \quad (9)$$

The properties of the tracking controller (8)–(9) are:

(i) The state feedback gains K_i , for $i = 1, \dots, N$, used in (8) are computed off-line for each possible fault situation so that the following condition is satisfied.

Assumption 2.4. (Controller Gains). The gains K_i , for $i = 1, \dots, N$, are such that $A - BF_i K_i$ are Schur matrices. $\circ$

² Inequalities and absolute-value/magnitude bars on vectors and matrices are taken elementwise.

³ A Schur matrix has all its eigenvalues strictly inside the unit circle.

⁴ Note that the control law (8)–(9) does not assume complete measurability of the state, but utilises an estimate. Thus, in this sense, the present method is less conservative than the previous approach in Ocampo-Martínez et al. [2008].

Note that the above can always be satisfied by the stabilisability requirement (see Assumption 2.1).

(ii) The input reference $u_{\text{ref},i}$ and the resulting state reference x_{ref} in (9) are bounded signals. In particular, the following assumptions holds.

Assumption 2.5. (Reference Bounds). Constant vectors $u_{\text{ref},i}^0 \in \mathbb{R}^m$ and $\bar{u}_{\text{ref},i} \in \mathbb{R}^m$, for $i = 1, \dots, N$, are known such that $u_{\text{ref},i}(k) \in \mathcal{U}_{\text{ref},i} = \{u \in \mathbb{R}^m : |u - u_{\text{ref},i}^0| \leq \bar{u}_{\text{ref},i}\}$ for all $k \geq 0$. $\circ$

(iii) The reference system (9) is designed such that the output Cx_{ref} , where C is the plant output matrix in (1b), asymptotically tracks an external signal y^* , that is, $\lim_{k \rightarrow \infty} [Cx_{\text{ref}}(k) - y^*(k)] = 0$. The signal y^* is a reference trajectory that we ultimately wish the plant output y in (1b) to track, in the absence of disturbances, under all possible fault situations.

Remark 2.6. (Exosystem). Under the stated assumptions, an “exosystem” that achieves Property (iii) can be readily designed. It is also immediate, given the exosystem, to obtain the bounds and offsets, $\bar{u}_{\text{ref},i}$ and $u_{\text{ref},i}^0$, respectively, of Assumption 2.5. The offsets $u_{\text{ref},i}^0$, in particular, are related to the offset of the reference signal y^* . $\circ$

We will show in Section 3 that when the FDI algorithm makes the “correct” decision, that is, when the selected index ℓ matches the plant fault situation ($F_\ell = F$), then Assumptions 2.2 and 2.3 together with the above properties of the tracking controller (8)–(9) guarantee that the closed-loop system evolves with bounded dynamics. Moreover, if the faults are “sufficiently infrequent” (according to a fault scenario to be defined later, see Assumption 4.4), the plant output y in (1b) asymptotically tracks the desired signal y^* in the absence of disturbances.

3. CLOSED-LOOP SYSTEM AND INVARIANT SETS

For a particular value of F in (2) and while the selection ℓ of the FDI algorithm does not change, the closed-loop system consisting of the plant tracking error

$$z \triangleq x - x_{\text{ref}}, \quad (10)$$

and the estimation errors, $\tilde{x}_i$, $i = 1, \dots, N$, evolves as (see (1a), (9), (5), (6) and (8))

$$\mathbf{X}^+ = \mathbf{A}_{F,\ell} \mathbf{X} + \mathbf{B}_{F,\ell} \mathbf{v}_\ell, \quad (11)$$

where

$$\mathbf{A}_{F,\ell} \triangleq \begin{bmatrix} A - BF_\ell K_\ell & 0 & \dots & BF_\ell K_\ell & \dots & 0 \\ B(F_1 - F)K_\ell & A - L_1 C & \dots & B(F - F_1)K_\ell & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ B(F_\ell - F)K_\ell & 0 & \dots & A - L_\ell C + B(F - F_\ell)K_\ell & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ B(F_N - F)K_\ell & 0 & \dots & B(F - F_N)K_\ell & \dots & A - L_N C \end{bmatrix} \quad (12)$$

$$\mathbf{X} \triangleq \begin{bmatrix} z \\ \tilde{x}_1 \\ \vdots \\ \tilde{x}_\ell \\ \vdots \\ \tilde{x}_N \end{bmatrix}, \quad \mathbf{B}_{F,\ell} \triangleq \begin{bmatrix} B(F - F_\ell) & E & 0 \\ B(F - F_1) & E & -L_1 \\ \vdots & \vdots & \vdots \\ B(F - F_\ell) & E & -L_\ell \\ \vdots & \vdots & \vdots \\ B(F - F_N) & E & -L_N \end{bmatrix}, \quad \mathbf{v}_\ell \triangleq \begin{bmatrix} u_{\text{ref},\ell} \\ w \\ \eta \end{bmatrix}. \quad (13)$$

We can make the following remarks about the closed-loop system behaviour.

Remark 3.1. (Boundedness). For each fixed value of ℓ , $\ell \in \{1, \dots, N\}$, and for $F = F_\ell$ (note that this condition means that the index ℓ selected by the FDI algorithm matches the plant fault situation), Assumptions 2.2 to 2.5 ensure that the closed-loop system (11) has bounded states. To see this, set $F = F_\ell$ in (11)–(13) to obtain the following sets of equations for the estimation error of the selected estimate, $\tilde{x}_\ell$, the plant tracking error, z , and the (“non-selected”) estimation errors, $\tilde{x}_i$, for $i = 1, \dots, N$, $i \neq \ell$:

$$\tilde{x}_\ell^+ = (A - L_\ell C)\tilde{x}_\ell + [E \quad -L_\ell] \begin{bmatrix} w \\ \eta \end{bmatrix}, \quad (14)$$

$$z^+ = (A - BF_\ell K_\ell)z + [BF_\ell K_\ell \quad E] \begin{bmatrix} \tilde{x}_\ell \\ w \end{bmatrix}, \quad (15)$$

$$\begin{aligned} \tilde{x}_i^+ &= (A - L_i C)\tilde{x}_i \\ &+ [-B(F_\ell - F_i)K_\ell \quad B(F_\ell - F_i)K_\ell] \begin{bmatrix} z \\ \tilde{x}_\ell \end{bmatrix} \\ &+ [B(F_\ell - F_i) \quad E \quad -L_i] \mathbf{v}_\ell, \end{aligned} \quad (16)$$

where $\mathbf{v}_\ell$ is defined in (13). We then note that Assumptions 2.2 and 2.3 guarantee that the state $\tilde{x}_\ell$ of (14) is bounded. From the latter fact and Assumptions 2.2 and 2.4, we have that the state z of (15) is bounded. Finally, Assumptions 2.2, 2.3 and 2.5, and the fact that $\tilde{x}_\ell$ and z are bounded guarantee that the state $\tilde{x}_i$ of (16) is also bounded. $\circ$

Remark 3.2. (Invariant Sets). Using the results of Appendix A, we can construct invariant sets $\tilde{\mathcal{X}}_{\ell,\ell}$, $\mathcal{Z}_\ell$, for $\ell = 1, \dots, N$, and $\tilde{\mathcal{X}}_{i,\ell}$, for $i, \ell = 1, \dots, N$, $i \neq \ell$, associated with systems (14), (15) and (16), respectively. Note that $\tilde{\mathcal{X}}_{\ell,\ell}$ and $\mathcal{Z}_\ell$, for $\ell = 1, \dots, N$, are “centred” around 0, since the disturbance sets $\mathcal{W}$ and $\mathcal{N}$ are centred around 0 (see Assumption 2.2). On the other hand, the sets $\tilde{\mathcal{X}}_{i,\ell}$, for $i, \ell = 1, \dots, N$, $i \neq \ell$, are centred around

$$\tilde{x}_{i,\ell}^0 \triangleq (I_n - A + L_i C)^{-1} B(F_\ell - F_i) u_{\text{ref},\ell}^0, \quad (17)$$

(see (A.3) in the Appendix) where $u_{\text{ref},\ell}^0$ is defined in Assumption 2.5. We also define the sets

$$\mathcal{E}_{i,\ell} \triangleq C\tilde{\mathcal{X}}_{i,\ell} \oplus \mathcal{N}, \quad \text{for } i, \ell = 1, \dots, N, \quad (18)$$

(the symbol $\oplus$ denotes Minkowski sum of sets) which are sets where the output estimation errors e_i defined in (5) live whenever the corresponding estimation error $\tilde{x}_i$ lives in $\tilde{\mathcal{X}}_{i,\ell}$. The N^2 sets defined in (18) satisfy:

$$\mathcal{E}_{i,i} \text{ is centred around } 0, \quad (19)$$

$$\mathcal{E}_{i,\ell} \text{ is centred around } e_{i,\ell}^0 \triangleq C\tilde{x}_{i,\ell}^0, \quad (20)$$

for $i, \ell = 1, \dots, N$, $i \neq \ell$, where $\tilde{x}_{i,\ell}^0$ is defined in (17). These sets are illustrated for $N = 3$ in Fig. 1 (the bigger green parallelograms) in the $\mathbb{R}^2$ output estimation error space corresponding to an observer with index i (the other two observers are indexed as j and k).

We will also require the sets

$$\mathcal{S}_\ell \triangleq \mathcal{Z}_\ell \times \tilde{\mathcal{X}}_{1,\ell} \times \dots \times \tilde{\mathcal{X}}_{N,\ell}, \quad \ell = 1, \dots, N, \quad (21)$$

(where $\times$ denotes Cartesian product), which are invariant sets for system (11) for all $\ell = 1, \dots, N$ and $F = F_\ell$. $\circ$

Remark 3.3. (“After-fault” Sets). Suppose that the states of system (11) for some $\ell \in \{1, \dots, N\}$ and $F = F_\ell$ (that is, the FDI algorithm matches the plant fault situation) are in the set $\mathcal{S}_\ell$ defined in (21). Let an actuator fault occur so

Fig. 1. Sets associated to an observer with index i . The illustration corresponds to $N = 3$; the other two observers are indexed as j and k .

that F in the plant equation (1a) changes at some time k_F from $F = F_\ell$ to $F = F_j$, for some $j \in \{1, \dots, N\}$, $j \neq \ell$. Using the dynamic equation (11) and Assumptions 2.2 and 2.5 we have that the “after-fault” state $\mathbf{X}^+$ of (11)–(13) (that is, the state at time $k_F + 1$) satisfies

$$\mathbf{X}^+ \in \mathcal{S}_{j,\ell}^+ \quad \text{where} \quad \mathcal{S}_{j,\ell}^+ \triangleq \mathbf{A}_{F_j,\ell} \mathcal{S}_\ell + \mathbf{B}_{F_j,\ell} \mathcal{V}_\ell, \quad (22)$$

and where $\mathcal{V}_\ell \triangleq \mathcal{U}_{\text{ref},\ell} \times \mathcal{W} \times \mathcal{N}$. Define⁵

$$\mathcal{E}_{i,j,\ell}^+ \triangleq [0_{p \times n} \quad 0_{p \times n} \quad \dots \quad \overset{1}{\downarrow} C \quad \dots \quad \overset{i}{\downarrow} C \quad \dots \quad \overset{N}{\downarrow} C] \mathcal{S}_{j,\ell}^+ \oplus \mathcal{N}, \quad (23)$$

where $0_{p \times n}$ denotes a $p \times n$ matrix with zero entries. Note that the “after-fault” output estimation error associated with the i th observer, denoted by e_i^+ , will belong to the set $\mathcal{E}_{i,j,\ell}^+$ if before the fault the estimation error e_i belonged to the set $\mathcal{E}_{i,\ell}$ defined in (18). Also note that the observer with index $i = j$ that matches the new plant fault situation $F = F_j$ will evolve with dynamics given by (7), and hence the centres of the sets $\mathcal{E}_{j,j,\ell}^+$, for $\ell = 1, \dots, N$, $\ell \neq j$, will tend towards zero, whereas the remaining sets $\mathcal{E}_{i,j,\ell}^+$, for $\ell = 1, \dots, N$, $\ell \neq j$, $i = 1, \dots, N$, $i \neq j$, will tend towards other “centres” away from zero (due to the offset in the centre of the set $\mathcal{U}_{\text{ref},\ell}$, which forms part of $\mathcal{V}_\ell$ in (22)). Fig. 1 illustrates the “after-fault” sets (23) (the smaller red parallelograms) for $N = 3$ in the $\mathbb{R}^2$ output estimation error space corresponding to an observer with index i (the other two observers are indexed as j and k). $\circ$

4. FAULT DETECTION AND ISOLATION APPROACH

4.1 Basic Principle

We will introduce our FDI approach via an informal discussion based on the illustration of Fig. 1, corresponding to three observers with indices i , j and k . We will assume that, for each observer, we can “separate” (by, for example,

⁵ Note that the subindices of the set $\mathcal{E}_{i,j,\ell}^+$ indicate: i , the index of the observer to which the set is associated; j , the new fault situation in the plant; ℓ , the previous fault situation in the plant.

a circle, as illustrated in the figure) the sets that are “close” to zero from the remaining sets “away” from zero.

Suppose that the closed-loop system has been operating for sufficiently long time under a particular fault situation $F = F_j$ accompanied by the right selection $\ell = j$ of the FDI. We assume that the elapsed time is long enough so that the closed-loop system states belong to the (attractive and invariant) set (21) and the estimation errors of all three observers belong to the respective set in (18). In particular, the estimation error e_i corresponding to observer i belongs to the set $\mathcal{E}_{i,j}$ depicted on the top right corner of Fig. 1. Also, the estimation error e_j of the fault-matching observer j belongs to the set $\mathcal{E}_{j,j}$, which is centred around 0 in the corresponding output estimation space associated to observer j (not shown in the figure).

Suppose next that the plant fault situation changes from $F = F_j$ to $F = F_i$. Hence, the estimation error e_i corresponding to the new fault-matching observer i will move into the set $\mathcal{E}_{i,i,j}^+$, inside the “separating circle”, whereas the estimation error e_j of the previous fault-matching observer j will move outside the corresponding circle. In addition, the estimation error e_k , corresponding to observer k that does not play a role in this simple example, will continue to be outside the corresponding circle. Thus, by monitoring the estimation errors to determine which one is inside the corresponding separating circle we can correctly detect and isolate the fault, and reconfigure the controller accordingly, in exactly one sampling instant. Once a reconfiguration has been made (in our example, the FDI algorithm selects the index $\ell = i$), in order to avoid false alarms, the algorithm does not make another decision until enough time has elapsed so that the estimation errors have converged to the sets (21) corresponding to the new decision $\ell = i$. In our allowed fault scenario we will assume that no other fault can occur within such time.

4.2 FDI Algorithm and Controller Reconfiguration

We next describe the proposed FDI approach and controller reconfiguration more formally. We begin with an assumption on the separation of the sets presented in Section 3.

Assumption 4.1. (Set Separation). For each $i = 1, \dots, N$, there exist a positive semidefinite matrix $P_i = P_i' \in \mathbb{R}^{p \times p}$ and a positive number $r_i \in \mathbb{R}$ such that

$$\begin{aligned} & \max \left\{ e_i' P_i e_i : e_i \in \mathcal{E}_{i,i} \cup \bigcup_{\substack{j=1 \\ j \neq i}}^N \mathcal{E}_{i,i,j}^+ \right\} < r_i < \\ & \min \left\{ e_i' P_i e_i : e_i \in \bigcup_{\substack{j=1 \\ j \neq i}}^N \mathcal{E}_{i,j} \cup \bigcup_{\substack{j=1 \\ j \neq i}}^N \bigcup_{\substack{k=1 \\ k \neq j}}^N \mathcal{E}_{i,j,k}^+ \right\}. \end{aligned} \quad (24)$$

There are two main mechanisms to achieve the above set separation. One is to adjust the offset of the reference signal y^* , which changes the offsets $u_{\text{ref},\ell}^0$ and, in consequence, the centres in (17) and (20). The other is to exploit the degrees of freedom afforded by the system’s actuator

redundancy (see, e.g., the free design parameters α_2 , α_3 , β_2 , and β_3 , utilised in the example of Section 5).

We also require the following definition.

Definition 4.2. (Convergence Time). Let T be an upper bound on the number of time steps it takes for the trajectories of system (11) for all $\ell = 1, \dots, N$ and $F = F_\ell$ to converge to the attractive, invariant set $\mathcal{S}_\ell$ [see (21)], from initial conditions in the sets $\mathcal{S}_{\ell,i}^+$ [see (22)], for $i = 1, \dots, N$, $i \neq \ell$. $\circ$

Based on the above assumption and definition, the FDI criterion and controller reconfiguration implemented by the proposed FTC scheme can be outlined as follows:

Algorithm 4.3. (Fault Tolerant Control).

Initialisation: The initial fault situation, $F = F_j$ say, for some $j \in \{1, \dots, N\}$, is known and we set $\ell = j$.

FDI and controller reconfiguration:

- (1) While $e_j' P_j e_j \leq r_j$, for some $j \in \{1, \dots, N\}$, use the tracking controller (8)–(9) with index $\ell = j$.
- (2) If, at some time instant, $e_j' P_j e_j > r_j$ and $e_i' P_i e_i \leq r_i$, for some $i \in \{1, \dots, N\}$, $i \neq j$, reconfigure the tracking controller (8)–(9) by changing $\ell = j$ to $\ell = i$.
- (3) Wait for T time steps before going back to (1) (that is, before making another FDI decision and controller reconfiguration). $\circ$

4.3 Closed-loop Stability

In this section we establish the stability properties of the proposed FTC scheme. We impose the following assumption on the allowed fault scenario.

Assumption 4.4. (Fault Scenario). Between the occurrence of any two consecutive changes in the fault matrix F , the system has been operating under a particular condition (fixed F and ℓ) for at least $T + 1$ time instants, where T is as in Definition 4.2. $\circ$

We then have the following result.

Theorem 4.5. Under Assumptions 2.1 to 4.4, the states of the closed-loop system (11)—encompassing the plant (1), the observers (3) and the tracking controller (8), (9) reconfigured by Algorithm 4.3—are bounded. Moreover, they converge to the set $\mathcal{S}_i$ of the form (21) after the occurrence of any fault characterised by the matrix $F = F_i$, for some $i \in \{1, \dots, N\}$. In particular, the tracking error (10) converges to the set $\mathcal{Z}_i$ constructed as in Remark 3.2, and to zero in the absence of disturbances.

Proof. We will consider without loss of generality the occurrence of a fault characterised by the matrix $F = F_i$, for some $i \in \{1, \dots, N\}$. By Assumption 4.4 and Definition 4.2, before the fault the states of the closed-loop system (11) belong to a set $\mathcal{S}_j$ of the form (21), for some $j \in \{1, \dots, N\}$, $j \neq i$, and hence are bounded. Also, the estimation errors (5) belong to the sets (18) (see Remark 3.2). The first time instant after the fault, the states of system (11) move to the set $\mathcal{S}_{i,j}^+$ of the form (22) and the output estimation errors move to the sets (23) (see Remark 3.3). In particular, (recall footnote 5 for the meaning of the subindices) $e_i^+ \in \mathcal{E}_{i,i,j}^+$, whereas $e_k^+ \in \mathcal{E}_{k,i,j}^+$, for $k = 1, \dots, N$, $k \neq i$, including $k = j$, the previous FDI selection. It follows from condition (24) that e_j^+ satisfies

$(e_j^+)'P_j e_j^+ > r_j$ and e_i^+ is the only estimation error satisfying $(e_i^+)'P_i e_i^+ < r_i$. Thus, step (2) of Algorithm 4.3 makes the right decision, the controller (8)–(9) is correctly reconfigured by setting $\ell = i$, and no other decision or reconfiguration takes place for the following T time steps (step (3)). Using the results of Appendix A (see also Remark 3.2), we conclude that the states of the closed-loop system (11) converge to the set $\mathcal{S}_i$ of the form (21) and the tracking error (10) converges to the set $\mathcal{Z}_i$ constructed as in Remark 3.2. Moreover, it is evident from (14) and (15) that the latter set collapses to zero in the absence of disturbances. The result then follows. $\square$

Remark 4.6. Note, in particular, from the proof of Theorem 4.5 that, under the assumptions of the theorem, correct fault detection and controller reconfiguration are achieved in one sampling time after the occurrence of a fault. Thus, the characterisation of the “under fault” sets (Remark 3.3) allows for a less conservative approach than that previously presented in Ocampo-Martínez et al. [2008] where fault detection and controller reconfiguration were achieved after the transient behaviour had elapsed. $\circ$

5. EXAMPLE

Consider the plant model (1a) with matrices

$$A = \begin{bmatrix} 0.9975 & 0.0975 \\ -0.0487 & 0.9488 \end{bmatrix}, \quad B = \begin{bmatrix} 0.0025 & 0.0037 \\ 0.0487 & 0.0731 \end{bmatrix}, \quad E = 0,$$

and the fault matrix $F \in \{F_1, F_2, F_3\}$ with

$$F_1 = I_2, \quad F_2 = \text{diag}(0, 1), \quad F_3 = \text{diag}(1, 0). \quad (25)$$

The output matrix in (1b) is $C = I_2$ and the measurement disturbance satisfies $|\eta| \leq [0.005 \ 0.005]'$. The scheme employs three observers of the form (3), each one associated with a fault matrix in (25), whose gains $L_1 = L_2 = L_3 = L$ are computed by pole placement [to place the eigenvalues of $A - LC$ at $(0.1333, 0.0667)$] as $L = \begin{bmatrix} 0.8642 & 0.0975 \\ -0.0487 & 0.8821 \end{bmatrix}$. The tracking controller (8)–(9) employs the feedback gains $K_1 = \begin{bmatrix} 45.1359 & 8.1189 \\ 67.7038 & 12.1784 \end{bmatrix}$, $K_2 = \begin{bmatrix} 0 & 0 \\ 97.7943 & 17.5910 \end{bmatrix}$, $K_3 = \begin{bmatrix} 146.6915 & 26.3865 \\ 0 & 0 \end{bmatrix}$, computed to place the eigenvalues of $A - BF_i K_i$, for each F_i in (25), at $(0.1, 0.2)$. The reference signal (9) satisfies Assumption 2.5 with

$$u_{\text{ref},1}^0 = \begin{bmatrix} 7.6923 \\ 11.5385 \end{bmatrix}, \quad u_{\text{ref},2}^0 = \begin{bmatrix} \alpha_2 \\ 16.6667 \end{bmatrix}, \quad u_{\text{ref},3}^0 = \begin{bmatrix} 25 \\ \alpha_3 \end{bmatrix},$$

$$\overline{u}_{\text{ref},1} = \begin{bmatrix} 0.6154 \\ 0.9231 \end{bmatrix}, \quad \overline{u}_{\text{ref},2} = \begin{bmatrix} \beta_2 \\ 1.3333 \end{bmatrix}, \quad \overline{u}_{\text{ref},3} = \begin{bmatrix} 2 \\ \beta_3 \end{bmatrix},$$

where $\alpha_2 = \alpha_3 = -10$ and $\beta_2 = \beta_3 = 2$ are design parameters which can be freely chosen (since they will not affect the plant due to the loss of the respective actuator) to aid to the desired set separation of Assumption 4.1. Fig. 2–4 show the sets (18) and (23) for observers $i = 1$, $i = 2$ and $i = 3$, respectively. The black sets centred at 0 are the sets (19), the yellow sets centred away from 0 are the sets (20), the blue sets inside the dotted circle are sets of the form (23) with $i = j$, $j \neq \ell$, whereas the red and light blue sets outside the dotted circle are of the form (23) with $i \neq j$, $j \neq \ell$. Note that for all three observers we can separate, by a circle of radius 0.21, the sets that are “close” to zero from the remaining sets “away” from zero. Thus, Assumption 4.1 holds with $P_i = I_2$ and $r_i = (0.21)^2$, for $i = 1, 2, 3$. We simulated the FTC scheme described above under the following fault scenario. The plant starts

Fig. 2. Sets for observer $i = 1$. Black set (centred at 0): $\mathcal{E}_{11}$; yellow sets: $\mathcal{E}_{12}$ and $\mathcal{E}_{13}$, as defined in (18); blue sets (inside the dotted circle): $\mathcal{E}_{112}^+$ and $\mathcal{E}_{113}^+$, of the form (23); red sets: $\mathcal{E}_{121}^+$ and $\mathcal{E}_{131}^+$; light blue sets: $\mathcal{E}_{123}^+$ and $\mathcal{E}_{132}^+$, of the form (23).

Fig. 3. Sets for observer $i=2$. All sets are as described in the caption of Fig. 2, interchanging subindices 1 and 2.

Fig. 4. Sets for observer $i=3$. All sets are as described in the caption of Fig. 2, interchanging subindices 1 and 3.

with the nominal condition $F = F_1$ at time $k = 0$. At time $k = 150$ a fault occurs such that F changes from F_1 to F_2 . At $k = 300$, F changes from F_2 to F_3 and then returns to the initial value F_1 at $k = 450$. The top plot of Fig. 5 shows the index ℓ selected by the FDI algorithm, which, except for an initial transient period, makes the

6. CONCLUSIONS

We have presented a new actuator fault-tolerant control strategy based on the separation of sets that characterise healthy system operation from sets that characterise faulty operation. This set separation property allows us to construct an FDI algorithm that ensures fault tolerant closed-loop stability. We provide conditions, in terms of bounds on reference signals, disturbance signals and closed-loop system parameters, which guarantee the aforementioned set separation.

Appendix A. POSITIVELY INVARIANT SETS

Consider the linear, discrete-time system

$$\xi^+ = \bar{A}\xi + \bar{B}v, \quad (\text{A.1})$$

where $\xi \in \mathbb{R}^q$ and $\xi^+ \in \mathbb{R}^q$ are, respectively, the current and successor system states and where $v \in \mathbb{R}^t$ satisfies

$$v \in \mathcal{V} \quad \text{where} \quad \mathcal{V} \triangleq \{v \in \mathbb{R}^t : |v - v^0| \leq \bar{v}\}, \quad (\text{A.2})$$

for some constant vectors v^0 and $\bar{v}$ in $\mathbb{R}^t$. Suppose that $\bar{A}$ is a Schur matrix and let $\bar{A} = \bar{V}\bar{\Lambda}\bar{V}^{-1}$ be its Jordan decomposition. Define the vector

$$\xi^0 \triangleq (I_q - \bar{A})^{-1}\bar{B}v^0, \quad (\text{A.3})$$

where I_q denotes the $q \times q$ identity matrix and let $\epsilon \in \mathbb{R}^q$ be a vector with positive components. Then the set

$\Phi_0 \triangleq \{\xi \in \mathbb{R}^q : |\bar{V}^{-1}\xi| \leq (I_q - |\bar{\Lambda}|)^{-1}|\bar{V}^{-1}\bar{B}|\bar{v} + \epsilon\} \oplus \{\xi^0\}$ ($\oplus$ denotes Minkowski sum of sets) has the properties that the trajectories of (A.1)–(A.2) remain in Φ_0 if started inside and converge to Φ_0 (in finite time) if started outside [Kofman et al., 2007]. Moreover, starting with Φ_0 , the set recursion $\Phi_{k+1} = \bar{A}\Phi_k \oplus \bar{B}\mathcal{V}$, has the property that $\Phi_{k+1} \subset \Phi_k$ and Φ_k is convex, compact, and a positively invariant set for system (A.1)–(A.2) [Olaru et al., 2008], that is, $\xi^+ \in \Phi_k$ for all $\xi \in \Phi_k$ and all $v \in \mathcal{V}$. Note that all sets Φ_k , $k \geq 0$, are “centred” around ξ^0 .

REFERENCES

- M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer, 2nd edition, 2006.
- C. Hajiyeve 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.J. 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, February 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 American Control Conference*, Anchorage, AK, May 2002.
- C. Ocampo-Martínez, J.A. De Doná, and M.M. Seron. Actuator fault tolerant control based on set separation. In *Proceedings 17 IFAC World Congress*, Seoul, Korea, July 2008.
- S. Olaru, J.A. De Doná, and M.M. Seron. Positive invariant sets for fault tolerant multisensor control schemes. In *Proceedings 17 IFAC World Congress*, Seoul, Korea, July 2008.

Fig. 5. Index ℓ selected by the FDI algorithm (top plot) and norms of the output estimation errors (5) (second to fourth plot). Also shown (in red) is the value 0.21 of the radius of the circle that separates the sets around zero from those away from zero.

Fig. 6. Plots 1 and 2: components of plant state, x in (1a) (blue dotted), and reference model state, x_{ref} in (9) (green solid). Plots 3 and 4: components of actual plant input, Fu in (1a) (blue dotted), and reference model input, u_{ref} in (9) (green solid).

right decision for all tested faults.⁶ The last three plots of Fig. 5 show the norms of the output estimation errors e_1 , e_2 and e_3 , defined in (5). Also shown in these plots (red line) is the value 0.21 of the radius of the circle that separates the sets around zero from those away from zero (the blue dotted circle in Fig. 2–4). Notice that the norms of the estimation errors stay below the value 0.21 when the corresponding observer matches the plant fault situation (correctly identified by the FDI algorithm) and stay above 0.21 when the corresponding observer does not match the plant fault situation. This behaviour was correctly predicted by the set separation of Fig. 2–4. Fig. 6 shows the resulting plant and reference model states and inputs. Notice that the faults have negligible effect on the plant states, which track the desired reference states almost perfectly.

⁶ To avoid wrong controller selections during this initial transient, the index $\ell = 1$, which matches the initial fault situation of the plant, was fixed and used in the tracking controller (8)–(9) until $k = 100$.