International Journal of Control

ISSN: 0020-7179 (Print) 1366-5820 (Online) Journal homepage: https://www.tandfonline.com/loi/tcon20

Actuator fault tolerant multi-controller scheme using set separation based diagnosis

María M. Seron & José A. De Doná

To cite this article: María M. Seron & José A. De Doná (2010) Actuator fault tolerant multi-controller scheme using set separation based diagnosis, International Journal of Control, 83:11, 2328-2339, DOI: 10.1080/00207179.2010.520032

To link to this article: https://doi.org/10.1080/00207179.2010.520032

International Journal of Control
Vol. 83, No. 11, November 2010, 2328–2339

Taylor & Francis
Taylor & Francis Group

Actuator fault tolerant multi-controller scheme using set separation based diagnosis

María M. Seron* and José A. De Doná

Centre for Complex Dynamic Systems and Control, School of Electrical Engineering and Computer Science, The University of Newcastle, Callaghan 2308, NSW, Australia

(*Received 25 October 2009; final version received 12 August 2010*)

We present a fault tolerant control strategy based on a new principle for actuator fault diagnosis. The scheme employs a standard 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 distinctive dynamics when an estimator matches the current fault situation of the plant. Based on the information from each observer, a fault detection and isolation (FDI) module is able to reconfigure the control loop by selecting the appropriate control law from a bank of controllers, each of them designed to stabilise and achieve reference tracking for one of the given fault models. The main contribution of this article is to propose a new FDI principle which exploits the separation of sets that characterise healthy system operation from sets that characterise transitions from healthy to faulty behaviour. The new principle allows to provide pre-checkable conditions for guaranteed fault tolerance of the overall multi-controller scheme.

Keywords: fault tolerant systems; fault diagnosis; controller reconfiguration; actuators; observers; sets

1. Introduction

Fault tolerant control (FTC) systems combine fault detection and isolation (FDI) and controller reconfiguration principles in an integrated manner that automatically avoids, or minimises, performance degradation when faults occur. Numerous methodologies for FDI have been proposed in the literature since the introduction of the early techniques in the 1970s; see, for example, the monographs and surveys: Frank (1990), Basseville and Nikiforov (1993), Leonhardt and Ayoubi (1997), Frank, Ding, and Marcu (2000), Patton, Frank, and Clark (2000), Venkatasubramanian, Rengaswamy, Yin, and Kavuri (2003), Isermann (2006) and Ding (2008), as well as the earlier reviews: Willsky (1976), Chow and Willsky (1984) and Isermann (1984). A well-established technique for model-based FDI relies on analytical redundancy in the form of dedicated observers. These observers generate *residual variables* that act as fault indicators. Publications on control reconfiguration are relatively more recent, see, for example, Mahmoud, Jiang, and Zhang (2003), Zhang and Jiang (2003) and Steffen (2005). A thorough compilation of a large diversity of techniques and methods for FDI and FTC can be found in the monograph Blanke, Kinnaert, Lunze, and Staroswiecki (2006). Despite this diversity, the approaches described in Blanke et al. (2006) for FTC – integrating both FDI and controller reconfiguration – do not specifically focus on providing *guaranteed* fault tolerance properties which ensure that closed-loop stability is preserved in the presence of faulty system components.

Towards the aim of devising schemes with guaranteed fault tolerance properties, we have recently presented in Ocampo-Martínez, De Doná, and Seron (2008) a new control scheme that tackles the problem of actuator FTC within a new framework. The architecture of the scheme, which we preserve in this article, 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 (or residuals) with a distinctive ('matching') behaviour when an estimator matches the current fault situation of the plant.
- An FDI algorithm which, based on the residual 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 multiple control laws, each consisting of a reference feedforward term and a feedback

*Corresponding author. Email: maria.seron@newcastle.edu.au

ISSN 0020–7179 print/ISSN 1366–5820 online

DOI: 10.1080/00207179.2010.520032
http://www.informaworld.com

gain multiplying the state estimate provided by the matching observer.

The novelty of the approach recently proposed by the authors in Ocampo-Martínez et al. (2008) lay in a new decision criterion for FDI. This new criterion was based on the computation of attractive invariant sets towards which the estimation errors related to each fault scenario and associated control configuration are guaranteed to converge. A key property for correct fault diagnosis was then the separation of the sets that characterise healthy operation from the ones that characterise faulty operation. A related 'set-based' approach was proposed in Wolff, Krutina, and Krebs (2008), where the real system behaviour given by measurements and the modelled system behaviour are checked for consistency through the use of set-valued observers. In Ocampo-Martínez et al. (2008), both FDI and controller reconfiguration were achieved *in steady state*, since, after the occurrence of an actuator fault, the algorithm was required to wait a suitable time until the estimation errors had converged to the sets associated with the new fault situation. Thus, although all system states were shown to remain bounded at all times, potentially large transient behaviour could still occur and compromise performance. Also, only actuator total outage was considered.

In this article, 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*. Moreover, we consider a larger class of faults by treating not only actuator outage but also loss of effectiveness by an *uncertain* amount. In addition, we extend the multi-controller to incorporate integral action. This latter feature allows us to successfully apply the method and achieve offset-free setpoint tracking for a nonlinear simulation model consisting of two interconnected tanks, often utilised in the FTC literature (see e.g. Richter and Lunze 2009).

Other approaches have focused on providing guaranteed fault tolerance properties which ensure that closed-loop stability is preserved in the presence of faulty system components, see for example, the papers Boskovic and Mehra (1999), Zhang, Parisini, and Polycarpou (2004), Mhaskar et al. (2006), Tang, Tao, and Joshi (2007), and references therein. In particular, the papers Zhang et al. (2004), Mhaskar et al. (2006) and Tang et al. (2007) present FTC methodologies based on the use of nonlinear models. These methodologies are very powerful but, naturally, require fairly involved design procedures and specialised tools, such as nonlinear transformations (Tang et al. 2007), control Lyapunov functions and invariant sets for constrained nonlinear dynamics (Mhaskar et al. 2006), or sophisticated fault detection filters based on learning algorithms and neural networks. In addition, Zhang et al. (2004) and Tang et al. (2007) assume full state measurements, and Mhaskar et al. (2006) only consider *single-input* configurations, thus fault isolation is not treated in general (although it is discussed in an example). In contrast, our approach is simple, yet treats multiple input linear systems under output feedback (i.e. full state measurement is not required) in the presence of process and measurement disturbances, and it is based on an adequate orchestration of standard linear observer and tracking controller designs with appropriate switching rules based on set-separation fault detection and isolation. A related approach for linear systems, but assuming full state measurement and minimum phase dynamics was proposed in Boskovic and Mehra (1999) using a multiple model adaptive reconfigurable control approach.

The remainder of this article proceeds as follows. Section 2 describes the plant and actuator fault models, the bank of state observers and the tracking multi-controller. In Section 3, we analyse the closed-loop system properties and compute invariant and 'after-fault' sets for the relevant system variables. Section 4 presents the proposed set-based FDI approach and establishes fault tolerant closed-loop stability and setpoint tracking. Section 5 shows the results of the application of the proposed FTC scheme to a simulation model of the two interconnected tank system of Richter and Lunze (2009). Finally, Section 6 concludes this article.

A preliminary conference version of this article was presented in Seron, De Doná, and Martínez (2009).

2. Plant, observers and multi-controller

2.1 *Plant and actuator fault models*

The plant is given by the linear discrete-time model

$$x^+ = Ax + BFu + Ew, \tag{1a}$$

$$y = Cx + \eta, \tag{1b}$$

$$v = Hy \triangleq C_v x + \eta_v, \tag{1c}$$

选择需要跟踪的y

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 measured output, $\eta \in \mathbb{R}^p$ is a bounded measurement disturbance and $v \in \mathbb{R}^q$ is a measured performance output (typically, one or more components of the measured output y). 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 $N = m+1$ different families of values

$$F \in \{F_1^*, F_2^*, \ldots, F_N^*\}, \tag{2}$$

where F_i^* is associated with faults in the ith actuator, that is each F_i^* has the form

$$F_i^* = \operatorname{diag}(1, \ldots, \overset{i}{\underset{\downarrow}{f_i}}, \ldots, 1), \quad f_i \in [0, 1), \qquad \text{for } i = 1, \ldots, m, \quad F_N^* = I_m. \tag{3}$$

部分失效

The parameter f_i in (3) represents the unknown 'fault intensity'. For example, $f_i = 0$ models the loss of the ith actuator. More generally, $f_i \in (0,1)$ corresponds to loss of effectiveness of the ith actuator. Also, note that $F_N^* = I_m$ (the $m \times m$ identity matrix) represents the 'nominal' case, that is no actuator fault.

In Section 4, we will develop an FDI approach that will detect actuator faults having intensity parameters f_i in (3) ranging over a certain interval. Once a fault has been detected, we will force the control signal corresponding to the faulty actuator to zero in order to have a correct model matching for the subsequent controller reconfiguration step. To this end, we define the following actuator 'nullifying' matrices:

$$F_i = \operatorname{diag}(1, \ldots, \overset{i}{\underset{\downarrow}{0}}, \ldots, 1), \quad \text{for } i = 1, \ldots, m, \qquad F_N = F_N^* = I_m, \tag{4}$$

检测到故障后置0

which are used after a fault in the ith actuator has been detected so that the control input u in (1) can be effectively assumed to have the form $F_i u$ (this follows from the property $F_i^* F_i = F_i$ for $i = 1, \ldots, N$ that results from (3)–(4)).

We will say that an (abrupt) change in the actuator fault situation occurs if F changes from $F = F_i^*$ to $F = F_j^*$, $i, j \in \{1, \ldots, N\}$, $j \neq i$, at some discrete-time instant $k_F \geq 0$.

We assume the following properties of system (1), (4).

Assumption 2.1 (Detectability)**:** *The pair (A, C) is detectable.*

Assumption 2.2 (Stabilisability)**:** *The pairs $\left(\left[\begin{smallmatrix} A & 0 \\ C_v & I_q \end{smallmatrix}\right], \left[\begin{smallmatrix} BF_i \\ 0 \end{smallmatrix}\right]\right)$ are stabilisable, for $i = 1, \ldots, N$.*

Assumption 2.2 ensures the possibility to achieve constant setpoint tracking, as shown in Section 2.3. Note that this assumption is stated in terms of the matrices F_i defined in (4) since the ith actuator signal will be forced to zero after a fault in this actuator is detected. While this signal remains zero the 'after-fault' value of the matrix F in (1) can be effectively considered to be $F = F_i^* F_i = F_i$.

Assumption 2.3 (Disturbance bounds)**:** *Bounding sets*[1] *$\mathcal{W} \triangleq \{w \in \mathbb{R}^r : |w| \leq \overline{w}\}$ and $\mathcal{N} \triangleq \{\eta \in \mathbb{R}^p : |\eta| \leq \overline{\eta}\}$ for some constant non-negative vectors $\overline{w} \in \mathbb{R}^r$ and $\overline{\eta} \in \mathbb{R}^p$ 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 $k \geq 0$.*

Remark 2.4: The boundedness requirement of Assumption 2.3 is key to the current invariant-set approach. It has the advantage, with respect to probabilistic approaches, that no stochastic model of the noises is needed; that is, noises and disturbances can obey any arbitrary probabilistic distribution, provided they remain bounded. The assumption that they remain bounded, on the other hand, is realistic in many applications.

2.2 *Bank of state observers*

The scheme employs a bank of N state observers given by

$$\hat{x}_i^+ = A\hat{x}_i + BF_i u + L_i(y - C\hat{x}_i), \quad i = 1, \ldots, N, \tag{5}$$

观测器增益是置0后的Fi

where $\hat{x}_i \in \mathbb{R}^n$ is the state estimate associated with the ith fault situation, u and y are the plant input and output and F_i has the form (4). Notice that each observer for $i = 1, \ldots, N-1$ (where $N - 1 = m$) 'matches' the case of outage in one actuator whereas the Nth observer 'matches' the fault-free case.

Assumption 2.5 (Observer gains)**:** *The gains L_i, for $i = 1, \ldots, N$, are such that $A - L_i C$ are Schur matrices.*[2]

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

$$\tilde{x}_i \triangleq x - \hat{x}_i, \tag{6}$$

and the output estimation error

$$e_i \triangleq y - C\hat{x}_i = C\tilde{x}_i + \eta, \tag{7}$$

for $i = 1, \ldots, N$. From (1a), (1b) and (5), the estimation errors satisfy

$$\tilde{x}_i^+ = (A - L_i C)\tilde{x}_i + B(F - F_i)u + Ew - L_i\eta. \tag{8}$$

CvX的追踪目标为v

2.3 *Reference tracking multi-controller*

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

$$u = F_\ell\,[-K_{\ell,1}(\hat{x}_\ell - x_{\mathrm{ref}}) - K_{\ell,2}\sigma + u_{\mathrm{ref},\ell}], \tag{9}$$

$$x_{\mathrm{ref}}^{+} = A\,x_{\mathrm{ref}} + BF_\ell\,u_{\mathrm{ref}}, \quad u_{\mathrm{ref}} = u_{\mathrm{ref},\ell}, \tag{10}$$

$$\sigma^{+} = \sigma + \kappa(v - C_v x_{\mathrm{ref}}), \tag{11}$$

σ为积分器，表示的是输出的跟踪误差

where $x_{\mathrm{ref}} \in \mathbb{R}^n$ and $u_{\mathrm{ref}} \in \mathbb{R}^m$ are state and input reference signals, respectively, A, B are the system matrices in (1a), F_ℓ is as defined in (4), v is the performance output defined in (1c), $\sigma \in \mathbb{R}^q$ is the state of the discrete-time integrator (11) and $\kappa \neq 0$ is a scalar gain.[3]

The tracking multi-controller (9)–(11) satisfies, by design, the following properties:

(1) The multiple state-feedback gains $K_{i,1}$, $K_{i,2}$, for $i = 1, \ldots, N$, used in (9) are computed off-line for each possible fault situation so that the following condition is satisfied.

Assumption 2.6 (Controller gains)**:** *The gains* $K_i \triangleq [K_{i,1}\ K_{i,2}]$, *for* $i = 1, \ldots, N$, *are such that the closed-loop matrices* A_{F_i,K_i}; *that is, when* $F = F_i$ *and* $K = K_i$ *in the definition*

$$A_{F,K} \triangleq \begin{bmatrix} A & 0 \\ \kappa C_v & I_q \end{bmatrix} - \begin{bmatrix} BF \\ 0 \end{bmatrix} K, \tag{12}$$

are Schur matrices.

Note that the above can always be satisfied by the stabilisability requirement of Assumption 2.2.

(2) The input reference $u_{\mathrm{ref},i}$ and the resulting state reference x_{ref} in (10) are bounded signals by design. In particular, the following assumption holds.

Assumption 2.7 (Reference bounds)**:** *Constant vectors* $u^0_{\mathrm{ref},i} \in R^m$ *and* $0 \leq \overline{u_{\mathrm{ref},i}} \in \mathbb{R}^m$, *for* $i = 1, \ldots, N$, *are known such that* $u_{\mathrm{ref},i}(k) \in \mathcal{U}_{\mathrm{ref},i} = \{u \in \mathbb{R}^m : |u - u^0_{\mathrm{ref},i}| \leq \overline{u_{\mathrm{ref},i}}\}$ *for all* $k \geq 0$.

(3) The reference system (10) is designed such that the output $C_v x_{\mathrm{ref}}$, where C_v is the plant's performance output matrix in (1c), asymptotically tracks an external bounded signal v^*, that is, $\lim_{k\to\infty}[C_v x_{\mathrm{ref}}(k) - v^*(k)] = 0$. The signal v^* is a reference trajectory that we ultimately want the plant's performance output v in (1c) to track under all possible fault situations.

Remark 2.8 (Actuator redundancy)**:** In applications where the input matrix B in (1) has a non-trivial right null space, which is typical whenever there is actuator redundancy, then extra offset terms $d_{\mathrm{ref},i}$, where $d_{\mathrm{ref},i}$ are such that $BF_i d_{\mathrm{ref},i} = 0$, can be added to the offsets $u^0_{\mathrm{ref},i}$ of the input reference signal (see Assumption 2.7), without affecting the reference tracking properties of the controller. These additional offsets provide extra degrees of freedom that can be exploited to achieve the desired set separation in the proposed FTC scheme.

We show in Section 3 that when the FDI algorithm makes the 'correct' decision (this will be ensured by the conditions imposed in later sections), that is, when it correctly identifies the index ℓ associated with the current actuator fault situation, then Assumptions 2.3 and 2.5 together with the above properties of the tracking multi-controller (9)–(11) guarantee that the closed-loop system evolves with bounded dynamics. Moreover, if the changes in the actuator fault situation are 'sufficiently slow', the plant's performance output v in (1c) asymptotically tracks the desired signal v^*.

3. Closed-loop system, attractive invariant sets and after-fault 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 'integrator-augmented' plant tracking error

$$\xi = \begin{bmatrix} z \\ \sigma \end{bmatrix} \triangleq \begin{bmatrix} x - x_{\mathrm{ref}} \\ \sigma \end{bmatrix}, \tag{13}$$

and the estimation errors, $\tilde{x}_i$, $i = 1, \ldots, N$, evolves as (see (1a), (7), (8) and (9)–(12))

$$\mathbf{X}^{+} = \mathbf{A}_{F,\ell}\mathbf{X} + \mathbf{B}_{F,\ell}\,\mathbf{v}_\ell, \tag{14}$$

where

$$\mathbf{A}_{F,\ell} \triangleq \begin{bmatrix} A_{F,F_\ell K_\ell} & 0 & \cdots & \begin{bmatrix} BFF_\ell K_{\ell,1} \\ 0 \end{bmatrix} & \cdots & 0 \\ B(F_1 - F)F_\ell K_\ell & A - L_1 C & \cdots & B(F - F_1)F_\ell K_{\ell,1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ B(F_\ell - F)F_\ell K_\ell & 0 & \cdots & A - L_\ell C + B(F - F_\ell)F_\ell K_{\ell,1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ B(F_N - F)F_\ell K_\ell & 0 & \cdots & B(F - F_N)F_\ell K_{\ell,1} & \cdots & A - L_N C \end{bmatrix} \tag{15}$$

$$\mathbf{X} \triangleq \begin{bmatrix} \xi \\ \tilde{x}_1 \\ \vdots \\ \tilde{x}_\ell \\ \vdots \\ \tilde{x}_N \end{bmatrix}, \quad \mathbf{B}_{F,\ell} \triangleq \begin{bmatrix} \begin{bmatrix} B(FF_\ell - F_\ell) & E & 0 \\ 0 & 0 & \kappa H \end{bmatrix} \\ B(F-F_1)F_\ell \quad E \quad -L_1 \\ \vdots \\ B(F-F_\ell)F_\ell \quad E \quad -L_\ell \\ \vdots \\ B(F-F_N)F_\ell \quad E \quad -L_N \end{bmatrix},$$

$$\mathbf{v}_\ell \triangleq \begin{bmatrix} u_{\mathrm{ref},\ell} \\ w \\ \eta \end{bmatrix}, \tag{16}$$

where we have used $\eta_v = H\eta$, which follows from (1c).

We can make the following remark and definitions regarding the closed-loop system behaviour.

Remark 3.1 (Boundedness)**:** For each fixed value of the index ℓ, $\ell \in \{1,\dots,N\}$, selected by the FDI algorithm, Assumptions 2.3–2.7 ensure that the closed-loop system (14) has bounded states whenever either of the following two actuator fault situations hold:

- $F = F_\ell^*$ (i.e. the index ℓ selected by the FDI algorithm matches the correct actuator fault situation),
- $F = F_N^* = I_m$ (i.e. the actuator fault situation corresponds to the nominal case where all m actuators are healthy).

To see the above property, we first note that the controller closed-loop matrix defined in (12) satisfies $A_{F,F_\ell K_\ell} = A_{F_\ell,K_\ell}$ in any of the above two cases of F, and further use the equalities $F_\ell^* F_\ell = F_\ell$, $F_N^* F_\ell = F_\ell$ and $F_\ell F_\ell = F_\ell$ in (14)–(16) to obtain the following sets of equations for the estimation error of the selected estimate, $\tilde{x}_\ell$, the (integrator augmented) plant tracking error, ξ, and the ('non-selected') estimation errors, $\tilde{x}_i$, for $i = 1,\dots,N$, $i \neq \ell$:

(17 18)式是在对应模式下，(19）式不对应

$$\tilde{x}_\ell^+ = (A - L_\ell C)\tilde{x}_\ell + \begin{bmatrix} E & -L_\ell \end{bmatrix} \begin{bmatrix} w \\ \eta \end{bmatrix}, \tag{17}$$

$$\xi^+ = A_{F_\ell,K_\ell}\xi + \begin{bmatrix} BF_\ell K_{\ell,1} & E & 0 \\ 0 & 0 & \kappa H \end{bmatrix} \begin{bmatrix} \tilde{x}_\ell \\ w \\ \eta \end{bmatrix}, \tag{18}$$

$$\tilde{x}_i^+ = (A - L_i C)\tilde{x}_i + B(F_\ell - F_i F_\ell)[-K_\ell \xi + K_{\ell,1}\tilde{x}_\ell] + \begin{bmatrix} B(F_\ell - F_i F_\ell) & E & -L_i \end{bmatrix} \mathbf{v}_\ell, \tag{19}$$

式8代入u的表达式即可

where $\mathbf{v}_\ell$ is defined in (16). We then note that Assumptions 2.3 and 2.5 guarantee that the state $\tilde{x}_\ell$ of (17) is bounded. From the latter fact and Assumptions 2.3 and 2.5, we have that the state ξ of (18) is bounded. Finally, Assumptions 2.3, 2.5 and 2.7, and the fact that $\tilde{x}_\ell$ and ξ are bounded guarantee that the state $\tilde{x}_i$ of (19) is also bounded.

Notice that, as shown above (and due to the use of the matrix F_ℓ in the controller (9)), the closed-loop system (17)–(19) is insensitive to changes in the actuator fault situation between $F = F_\ell^*$ and $F = F_N^* = I_m$. Thus, a structural characteristic of the presented approach is the inability to automatically detect the recovery of the nominal situation and reconfigure the controller accordingly. Note, however, that the closed-loop boundedness property is still preserved since the controller remains reconfigured to match the previous fault situation, forced to be correct by effect of the matrix F_ℓ. On the other hand, the nominal situation can be recovered manually by re-initialisation.

Definition 3.2 (Attractive invariant sets)**:** Using the results of Appendix A, we can construct attractive invariant sets $\tilde{\mathcal{X}}_{\ell,\ell}$, $\mathcal{Z}_\ell$, for $\ell = 1,\dots,N$, and $\tilde{\mathcal{X}}_{i,\ell}$, for i, $\ell \in \{1,\dots,N\}$, $i \neq \ell$, associated with systems (17), (18) and (19), 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 2.3). On the other hand, the sets $\tilde{\mathcal{X}}_{i,\ell}$, for i, $\ell = 1,\dots,N$, $i \neq \ell$, are centred around

根据式（8）求集合中心，ω和η中心都在0

$$\tilde{x}_{i,\ell}^0 \triangleq (I_n - A + L_i C)^{-1} B(F_\ell - F_i F_\ell) u_{\mathrm{ref},\ell}^0 \tag{20}$$

(see (28) in Appendix A), where $u_{\mathrm{ref},\ell}^0$ is defined in Assumption 2.7. We also define the sets

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

($\times$ denotes Cartesian product), which are attractive and invariant for system (14) for $F = F_\ell^*$ or $F = F_N^*$.

Definition 3.3 (Output Sets)**:** We define the output sets

$$\mathcal{E}_{i,\ell} \triangleq C\tilde{\mathcal{X}}_{i,\ell} \oplus \mathcal{N}, \quad \text{for } i,\ell = 1,\dots,N, \tag{22}$$

(the symbol $\oplus$ denotes Minkowski sum of sets) which are sets where the output estimation errors e_i, defined in (7), live whenever the corresponding estimation error $\tilde{x}_i$ lives in $\tilde{\mathcal{X}}_{i,\ell}$. Note that $\mathcal{E}_{i,i}$ is centred around 0, whereas $\mathcal{E}_{i,\ell}$, $\ell \neq i$, is centred around $e_{i,\ell}^0 \triangleq C\tilde{x}_{i,\ell}^0$, where $\tilde{x}_{i,\ell}^0$ is given by (20).

The output sets are illustrated for $N = 3$ in Figure 1 (the bigger green sets) in the $\mathbb{R}^2$ output estimation error space corresponding to the observer with index 3 (the other two observers are indexed as 1 and 2).

Suppose next that the states of system (14) for some $\ell \in \{1,\dots,N\}$ and $F = F_\ell^*$ or $F = F_N^* = I_m$

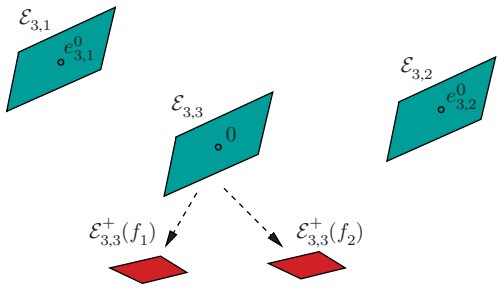

Figure 1. Sets associated with the observer with index 3. The illustration corresponds to $N=3$; the other two observers are indexed as 1 and 2. Note that the observer with index 3 corresponds to the nominal case according to the notation introduced in (3). Available in colour online.

(see Remark 3.1) are in the set $\mathcal{S}_\ell$ defined in (21). Let a change in the actuator fault situation occur so that F in the plant equation (1a) changes at some time k_F to $F=F_j^*=\mathrm{diag}(1,\ldots,f_j,\ldots,1)$, for some $j\in\{1,\ldots,m\}$, $j\neq\ell$ (see (3)). Using the dynamic equation (14) and Assumptions 2.3 and 2.7 we have that the 'after-fault' state $\mathbf{X}^+$ of (14)–(16) (i.e. the state at time k_F+1) satisfies

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

式（14）的集合形式 (23)

and where $\mathcal{V}_\ell\triangleq\mathcal{U}_{\mathrm{ref},\ell}\times\mathcal{W}\times\mathcal{N}$. (Note, in particular, that the subindex ℓ in $\mathbf{A}_{F_j^*,\ell}$ and $\mathbf{B}_{F_j^*,\ell}$ is not changed since the controller (9)–(11) has not yet been reconfigured to correspond to the new fault situation.)

Definition 3.4 ('After-fault' sets)**:** Associated with the previously selected ℓth observer, when a change from $F=F_\ell^*$ or $F=F_N^*=I_m$ to $F=F_j^*=\mathrm{diag}(1,\ldots,f_j,\ldots,1)$, for some $j\in\{1,\ldots,m\}$, $j\neq\ell$ occurs, we define the 'after-fault' set

$$\mathcal{E}^+_{\ell,\ell}(f_j)\triangleq\big[0_{p\times(n+q)}\quad\underset{\downarrow}{\overset{1}{0_{p\times n}}}\quad\cdots\quad\underset{\downarrow}{\overset{\ell}{C}}\quad\cdots\quad\underset{\downarrow}{\overset{N}{0_{p\times n}}}\big]\mathcal{S}_\ell^+(f_j)\oplus\mathcal{N},$$

where $0_{p\times n}$ denotes a $p\times n$ matrix with zero entries. Using (21), (23) and the structure of the matrices in (15)–(16), yields

$$\begin{aligned}\mathcal{E}^+_{\ell,\ell}(f_j)=&\,CB(F_\ell-F_j^*F_\ell)K_\ell\mathcal{Z}_\ell\\&\oplus C[A-L_\ell C+B(F_j^*F_\ell-F_\ell)K_{\ell,1}]\tilde{\mathcal{X}}_{\ell,\ell}\\&\oplus CB(F_j^*F_\ell-F_\ell)\mathcal{U}_{\mathrm{ref},\ell}\oplus CE\mathcal{W}\oplus(-CL_\ell)\mathcal{N}\oplus\mathcal{N}.\end{aligned}\tag{24}$$

Note that the set $\mathcal{E}^+_{\ell,\ell}(f_j)$ will contain the 'after-fault' output estimation error associated with the previously selected ℓth observer, denoted by e_ℓ^+, if before the fault the estimation error $\tilde{x}_\ell$ belonged to the set $\tilde{\mathcal{X}}_{\ell,\ell}$ and the tracking error ξ belonged to the set $\mathcal{Z}_\ell$. The first of those conditions, in turn, implies that the output estimation error e_ℓ belonged to the set $\mathcal{E}_{\ell,\ell}$ defined in (22). Hence, the 'after-fault' sets (24) represent the collection of all possible 'after-fault' values of the output estimation error e_ℓ at time k_F+1 starting from the set $\mathcal{E}_{\ell,\ell}$ at time k_F.

Figure 1 illustrates the 'after-fault' sets (24) (the smaller red sets) for $N=3$ in the $\mathbb{R}^2$ output estimation error space corresponding to the observer with index 3 (the other two observers are indexed as 1 and 2).

4. Fault detection and isolation approach

4.1 *Basic principle*

We will motivate our FDI approach via an informal discussion based on the illustration of Figure 1, corresponding to a scheme having three observers with indices 1, 2 and 3. We will assume that, as illustrated in the figure, the sets $\mathcal{E}_{3,3}$ and $\mathcal{E}^+_{3,3}(f_j)$ for $j=1,2$ are separated from each other.[4]

Suppose that the closed-loop system has been operating for sufficiently long time under a particular fault situation, $F=F_3^*$, say, accompanied by the right selection $\ell=3$ 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 $\mathcal{S}_3$ given in (21) and the output estimation errors of all three observers belong to the respective sets in (22). In particular, the output estimation error e_3 of the selected observer 3 belongs to the set $\mathcal{E}_{3,3}$, which is centred around 0 in the corresponding output estimation space associated to observer 3, as shown in Figure 1.

Suppose next that the plant fault situation changes at time k_F from $F=F_3^*$ to $F=F_1^*=\mathrm{diag}(f_1,1,1)$ or to $F=F_2^*=\mathrm{diag}(1,f_2,1)$, with $f_1,\ f_2\in[0,1)$. Hence, the output estimation error e_3 corresponding to the previous selected observer 3 will either move into the set $\mathcal{E}^+_{3,3}(f_1)$, or to the set $\mathcal{E}^+_{3,3}(f_2)$. Thus, by monitoring the output estimation error of the currently selected observer (in this example, monitoring e_3 at times $k\leq k_F+1$) to determine which set it belongs to, we can correctly detect and isolate the fault one sampling instant after its occurrence (i.e. at $k=k_F+1$), and reconfigure the controller accordingly. Once a reconfiguration has been made (in our example, the FDI algorithm selects the index $\ell=j$), in order to avoid false alarms, the algorithm does not make another output estimation error check or decision until enough time has elapsed so that all estimation errors have converged to the sets (21) corresponding to the new decision $\ell=j$. We will call this convergence time the

'set-transition time', and we point out that this time can be estimated using, for example, standard set-theoretic techniques as explained in Appendix B. After that time, the algorithm proceeds to monitor the sets associated to the newly selected observer j. In our allowed fault scenario we will assume that no other fault can occur within such set-transition 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* $i = 1, \ldots, N$, *the set* $\mathcal{E}_{i,i}$ *and the* $m-1$ *collections of sets* $\cup_{f_j \in \mathcal{I}_j} \mathcal{E}^+_{i,i}(f_j)$, *for* $j = 1, \ldots, m$, $j \neq i$, *and some non-empty intervals* $\mathcal{I}_j \subset [0, 1)$, *are all disjoint*.

There are two main mechanisms to achieve the set separation of Assumption 4.1. One is to adjust the offset of the reference signal v^* (see Property 3 in Section 2.3), which changes the offsets $u^0_{\mathrm{ref},\ell}$; and the other is to exploit the degree-of-freedom signals $d_{\mathrm{ref},\ell}$ (see Remark 2.8) afforded by the system's actuator redundancy. Both mechanisms change the 'centres' of the after-fault sets (24). More specifically, since $F^*_j \neq I_m$ the third summand in (24), associated with the reference set $\mathcal{U}_{\mathrm{ref},\ell}$, will cause a 'shift' of the after-fault set $\mathcal{E}^+_{\ell,\ell}(f_j)$ away from the origin (the remaining summands in (24), associated with the sets $\mathcal{Z}_\ell$, $\tilde{\mathcal{X}}_{\ell,\ell}$, $\mathcal{W}$ and $\mathcal{N}$, do not contribute to this shift since they are all centred at zero).

Notice also that the observer gains L_ℓ influence the size of the sets in Assumption 4.1. In particular, choosing L_ℓ so as to minimise some measure of the size of the set $\tilde{\mathcal{X}}_{\ell,\ell}$ (associated with the selected estimation error dynamics (17)), subject to the constraint that $A - L_\ell C$ is a Schur matrix (see Assumption 2.5), has the potential to reduce the size of the sets $\mathcal{E}_{\ell,\ell}$ (see (22)) and $\mathcal{E}^+_{\ell,\ell}(f_j)$ (see (24)), thus facilitating the required separation.

We also require the following definition.[5]

Definition 4.2 (Set-transition time)**:** Let T be an upper bound on the number of time steps it takes for the trajectories of system (14) for all $\ell = 1, \ldots, m$ and $F = F_\ell$ to converge to the attractive invariant set $\mathcal{S}_\ell$ (see (21)), from initial conditions in the collection of 'after-fault' sets $\cup_{f_\ell \in \mathcal{I}_\ell} \mathcal{S}^+_i(f_\ell)$ (see (23)), for $i = 1, \ldots, N$, $i \neq \ell$.

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 (FDI and controller reconfiguration)**:**
***Initialisation*:** At time $k = k_0$ the index of the initial fault situation, $F = F_i$, for some $i \in \{1, \ldots, N\}$, is known, the controller is using the index $\ell = i$ in (9)–(11) and the states of system (14) belong to the attractive invariant set $\mathcal{S}_i$ (see (21)). We initialise the 'decision' and 'checking' variables $\mathbf{d}(k_0) = i$, $\ell = \mathbf{d}(k_0)$ and $\mathbf{Check}(k_0) = \mathbf{yes}$.

***Subsequent steps*:** For $k > k_0$, while $\mathbf{Check}(k-1) = \mathbf{yes}$:

(1) (Decision) Get the current value $e_i(k)$ of the output estimation error associated with the observer that matches the previous decision $\mathbf{d}(k-1) = i$.
   (a) if $e_i(k) \in \mathcal{E}_{i,i}$ then set $\mathbf{d}(k) = i$ and $\mathbf{Check}(k) = \mathbf{yes}$;
   (b) if $e_i(k) \in \cup_{f_j \in \mathcal{I}_j} \mathcal{E}^+_{i,i}(f_j)$, for some $j \in \{1, \ldots, m\}$, $j \neq i$, then set $\mathbf{d}(\tau) = j$ for $\tau = k, \ldots, k+T$ and $\mathbf{Check}(\tau) = \mathbf{no}$ for $\tau = k, \ldots, k+T-1$, $\mathbf{Check}(k+T) = \mathbf{yes}$ (waiting timer).

(2) (Reconfiguration) Set $\ell = \mathbf{d}(k)$ in the multi-controller equations (9)–(11).

4.3 *Closed-loop stability and setpoint tracking*

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.

We then have the following results.

Theorem 4.5 (Closed-loop stability)**:** *Under Assumptions* 2.1–4.4, *the states of the closed-loop system* (14) – *encompassing the plant* (1), *the observers* (5) *and the tracking controller* (9)–(11) *reconfigured by Algorithm* 4.3 – *are bounded. Moreover*, *they converge to the attractive invariant set* $\mathcal{S}_j$ *of the form* (21) *after the occurrence of any fault characterised by the matrix* $F = F^*_j = \mathrm{diag}(1, \ldots, f_j, \ldots, 1)$, *for some* $j \in \{1, \ldots, m\}$ *and* $f_j \in \mathcal{I}_j$ (*see Assumption* 4.1). *In particular*, *the tracking error* (13) *converges to the set* $\mathcal{Z}_j$ *constructed as in Definition* 3.2, *and to zero in the absence of disturbances*.

Proof: Consider without loss of generality the occurrence of a change in the actuator fault situation characterised by the matrix $F = F^*_j = \mathrm{diag}(1, \ldots, f_j, \ldots, 1)$, for some $j \in \{1, \ldots, m\}$ and $f_j \in \mathcal{I}_j$.

By Assumption 4.4 and Definition 4.2, before the change the states of the closed-loop system (14) belong to a set $\mathcal{S}_i$ of the form (21), for some $i \in \{1, \ldots, N\}$, $i \neq j$, and hence are bounded. Also, the output estimation error (7) of the selected ith observer belongs to the set $\mathcal{E}_{i,i}$ defined in (22) (see Definition 3.3). The first time instant after the change in the actuator fault situation, the states of system (14) move to the set $\mathcal{S}_i^+(f_j)$ of the form (23) and the output estimation error e_i of the, now, 'previously selected' ith observer moves to the set (24), that is, $e_i^+ \in \mathcal{E}_{i,i}^+(f_j)$ (see Definition 3.4). Since the sets $\mathcal{E}_{i,i}$ and $\mathcal{E}_{i,i}^+(f_j)$ are disjoint (Assumption 4.1), then step 1b of Algorithm 4.3 makes the right decision, and, hence the controller (9)–(11) is correctly reconfigured by setting $\ell = j$ (step 2 of Algorithm 4.3). Note also from step 1b of Algorithm 4.3 that no other check, decision or reconfiguration takes place for the following $T+1$ time steps and, in addition, no other change in the actuator fault situation occurs within that lapse (Assumption 4.4). Using the results of Appendix A (see also Definition 3.2), we conclude that the states of the closed-loop system (14) converge to the set $\mathcal{S}_j$ of the form (21) and the tracking error (13) converges to the set $\mathcal{Z}_j$ constructed as in Definition 3.2. Moreover, it is evident from (17) and (18) that the latter set collapses to zero in the absence of disturbances. The result then follows. □

Corollary 4.6 (Setpoint tracking)**:** *Under the conditions of Theorem* 4.5, *for a constant reference signal* v^* (*see Property 3 in Section* 2.3), *the performance output* v *in* (1c) *converges to the setpoint* v^* *even in the presence of* (*nonzero*) *constant disturbances*.

Proof: Theorem 4.5 has shown that the states of the closed-loop system are bounded. Then, if the reference signal v^* and all disturbances are constant, the integrator state σ in (11) must converge to a constant value, that is $\sigma^+ = \sigma$. Hence, Equation (11) and the exosystem property, $\lim_{k\to\infty}[C_v x_{\text{ref}}(k) - v^*] = 0$, ensure the satisfaction of the claimed setpoint tracking objective. The result then follows. □

Remark 4.7: 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 (Definition 3.4) 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.

5. Example

We consider the model of interconnected tanks presented in Richter and Lunze (2009), where two tanks with levels h_1 and h_2 are interconnected through lower and upper valves, whose effect is described by the variables u_{L} and u_{U}, and the first tank is filled via a pump, described by the variable u_{P}. Taking as state vector $x = [h_1\ h_2]'$, input vector $u = [u_{\text{P}}\ u_{\text{L}}\ u_{\text{U}}]'$ and the operating point $x_o = [0.4\ \ 0.06]'$, $u_o = [0.48\ \ 0.75\ \ 0.2]'$, the linearised incremental model of the system around the operating point, discretised with sampling period $t_s = 1$ s, can be described by the model (1a) with matrices

$$A = \begin{bmatrix} 0.9931 & 0.0035 \\ 0.0068 & 0.9823 \end{bmatrix},$$
$$B = \begin{bmatrix} 0.0081 & -0.0032 & -0.0034 \\ 0.0000 & 0.0032 & 0.0034 \end{bmatrix},$$
$$E = -\begin{bmatrix} 0.9966 \\ 0.0034 \end{bmatrix} \times 10^{-3},$$

and where w represents a leak in the first tank, assumed bounded as $|w| \leq 10^{-3}$.

We consider the fault matrix $F \in \{F_2^*, F_3^*, F_4^*\}$ with

$$F_2^* = \text{diag}(1, f_2, 1), \quad F_3^* = \text{diag}(1, 1, f_3), \quad F_4^* = I_3, \tag{25}$$

and $f_2 \in \mathcal{I}_2 = [0,\ 0.6]$, $f_3 \in \mathcal{I}_3 = [0,\ 0.6]$.

The output matrix in (1b) is $C = I$ and the measurement noise satisfies $|\eta| \leq [1\ \ 1]' \cdot 10^{-5}$. The performance variable matrix in (1c) is $C_v = [0\ \ 1]$, that is, the level of the second tank.

The scheme employs three observers of the form (5), each one associated with a fault matrix in (25), whose gains $L_2 = L_3 = L_4 = L$ are computed by pole placement (to place the eigenvalues of $A - LC$ at $(0.1, 0.05)$) as

$$L = \begin{bmatrix} 0.8931 & 0.0035 \\ 0.0068 & 0.9323 \end{bmatrix}.$$

The tracking controller (9)–(11) employs the feedback gains $K_i \triangleq [K_{i,1}\ K_{i,2}]$, where

$$K_2 = \begin{bmatrix} 74.0487 & 144.0117 & 41.4957 \\ 0 & 0 & 0 \\ 1.3575 & 350.8722 & 103.8830 \end{bmatrix},$$
$$K_3 = \begin{bmatrix} 49.4359 & 102.8133 & 20.8364 \\ 1.8759 & 246.6231 & 47.2899 \\ 0 & 0 & 0 \end{bmatrix},$$

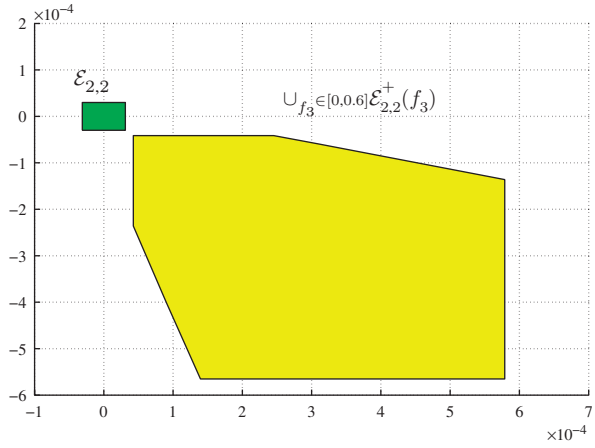

Figure 2. 'Matching' set $\mathcal{E}_{2,2}$ and collection of 'after-fault' sets $\cup_{f_3\in[0,0.6]}\mathcal{E}^+_{2,2}(f_3)$ associated with observer 2.

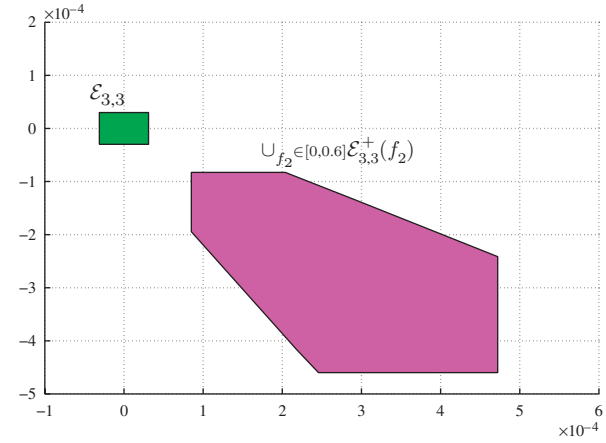

Figure 3. 'Matching' set $\mathcal{E}_{3,3}$ and collection of 'after-fault' sets $\cup_{f_2\in[0,0.6]}\mathcal{E}^+_{3,3}(f_2)$ associated with observer 3.

$$K_4 = \begin{bmatrix} 74.0487 & 144.0117 & 41.4957 \\ 0.6775 & 175.1142 & 51.8462 \\ 0.7199 & 186.0589 & 55.0866 \end{bmatrix}.$$

The reference signal (10) is computed for v^* equal to a step of 0.02 m for the level h_2 (see Property 3 in Section 2.3), that is, from 0.06 m to 0.08 m, and satisfies Assumption 2.7 with

$$u^0_{\text{ref},2} = \begin{bmatrix} 0.0356 \\ 0 \\ 0.1053 \end{bmatrix}, \quad u^0_{\text{ref},3} = \begin{bmatrix} 0.0356 \\ 0.1119 \\ 0 \end{bmatrix},$$

$$u^0_{\text{ref},4} = \begin{bmatrix} 0.0356 \\ 0.0526 \\ 0.0558 \end{bmatrix},$$

and $\overline{u_{\text{ref},2}} = \overline{u_{\text{ref},3}} = \overline{u_{\text{ref},4}} = [0\ 0\ 0]'$. The value $\kappa = 1$ is used for the integrator constant in Equation (11). The degree-of-freedom signal $d_{\text{ref},4}$ (see Remark 2.8) is taken as $d_{\text{ref},4} = [0\ \ -0.2185\ \ 0.2056]'$ and satisfies $Bd_{\text{ref}} = 0$.

Figures 2–4 show the 'matching' sets (22) (with $\ell = i$) and the 'after-fault' sets (24), for observers 2, 3 and 4, respectively. We can see from these figures that Assumption 4.1 holds.

We simulated the FTC scheme described above *applied to the nonlinear model of the system*[6] under the following fault scenario. The plant starts with the nominal condition $F = F_4^*$ at time $t = 0$ s. Then the following changes in the plant fault matrix F occur: $F_4^* \to F_2^*$ at $t = 230$ s; $F_2^* \to F_4^*$ at $t = 446$ s; F_4^* to F_3^* at $t = 714$ s; $F_3^* \to F_2^*$ at $t = 980$ s; $F_2^* \to F_3^*$ at $t = 1245$ s; $F_3^* \to F_4^*$ at $t = 1480$ s; $F_4^* \to F_3^*$ at $t = 1750$ s. In all cases, F_2^*, F_3^* and F_4^* are as in (25) with $f_2 = 0.5$ and $f_3 = 0.3$.

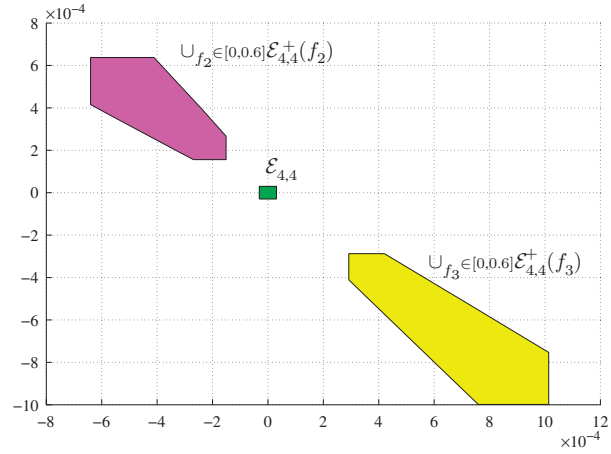

Figure 4. 'Matching' set $\mathcal{E}_{4,4}$ and collection of 'after-fault' sets $\cup_{f_2\in[0,0.6]}\mathcal{E}^+_{4,4}(f_2)$ and $\cup_{f_3\in[0,0.6]}\mathcal{E}^+_{4,4}(f_3)$ associated with observer 4.

The value $T = 100$ was used in the timers of Algorithm 4.3. Also, the set membership tests used in the algorithm were simplified to checking the location of the tested points with respect to lines separating the sets of Figures 2–4.

The top subplot of Figure 5 shows the fault index (i.e. the subindex j of the actual value of the matrix $F = F_j^*$) and the index ℓ selected by the FDI algorithm, which makes the right decision for all tested faults.[7] Note that the FDI does not detect the recovery of the nominal situation $F = F_4^*$, as discussed in Remark 3.1, but this does not impact on performance as seen from

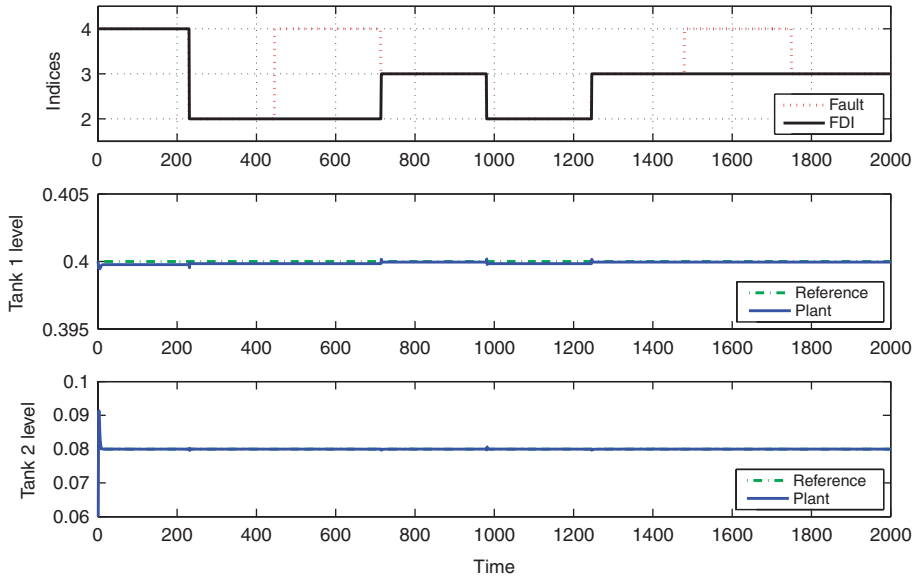

Figure 5. Top plot: fault index (i.e. the subindex j of the actual value of the matrix $F = F_j^*$) and index ℓ selected by the FDI algorithm. Second and third plots: tank levels (blue solid line), and reference model state, x_{ref} in (10) (green dashed-dotted line). Available in colour online.

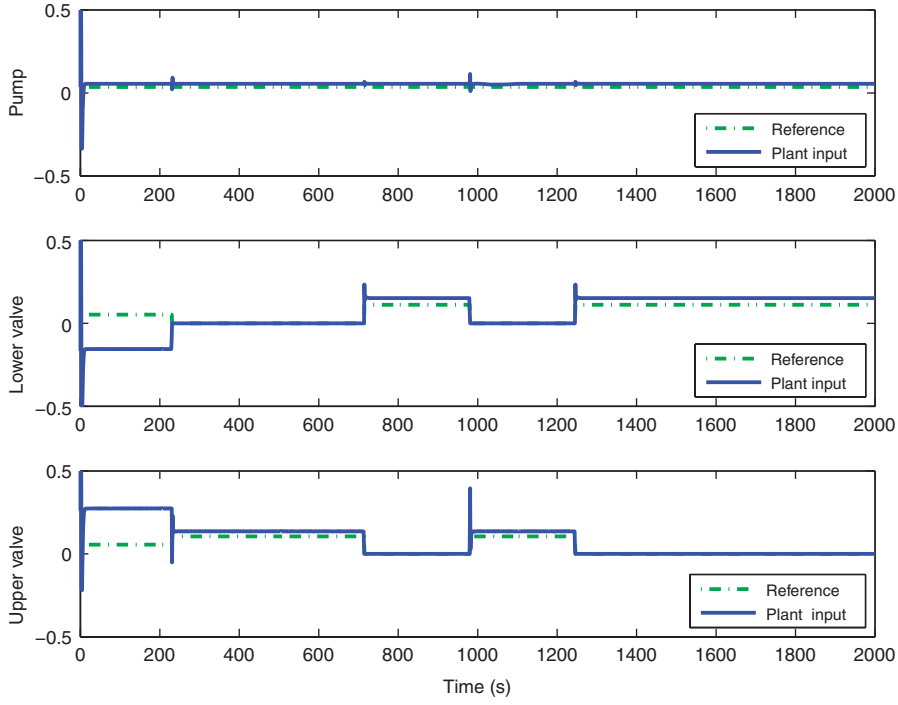

Figure 6. Components of the actual plant input, Fu in (1a) (blue solid line), and reference control signal u_{ref} in (10) (green dashed-dotted line). All plotted values are incremental with respect to the input operating point $u_o = [0.48\ 0.75\ 0.2]'$. Available in colour online.

the second and third plots of Figure 5, which show the resulting levels of each tank. Notice that the faults have only little impact on these levels, especially on the level of the second tank (the performance output), which satisfactorily tracks the desired reference of 0.08 m.

Figure 6 shows the effective incremental plant input Fu in (1a) (solid blue curves) with respect to the input operating point $u_o = [0.48\ 0.75\ 0.2]'$, together with the incremental value of the reference control signal u_{ref} in (10) (dashed-dotted green curves). The differences

between the two signals Fu and u_{ref} in the initial period when all three actuators are healthy (corresponding to the actuator situation $F_4^* = I_3$), is due to the effect of the degree-of-freedom signal $d_{\text{ref},4}$, which is a key element to achieve correct fault detection and identification based on set separation. Note that, this component of the input does not affect the system when Fu is applied to (1a).

6. Conclusions

We have presented an FTC strategy based on a new principle for actuator fault diagnosis. The scheme employs a standard 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 distinctive dynamics when an estimator matches the current fault situation of the plant. Based on the information from each observer, a fault diagnosis and isolation module is able to reconfigure the control loop by selecting the appropriate control law from a bank of controllers, each of them designed to stabilise and achieve reference tracking for one of the given fault models. We have proposed a new detection and diagnosis principle which exploits the separation of sets that characterise healthy system operation from sets that characterise transitions from healthy to faulty behaviour. The new principle allows to provide pre-checkable conditions for guaranteed fault tolerance of the overall multi-controller scheme. The results were illustrated on a nonlinear simulation model consisting of two interconnected tanks, which is frequently utilised in the FTC literature. Future work includes the investigation of fault tolerance under a continuous range of faults by combining concepts of controller reconfiguration and robust control.

Acknowledgement

The authors thank John Jairo Martínez and Jan Richter for helpful discussions.

Notes

1. Inequalities and absolute-value/magnitude of vectors and matrices are taken elementwise.
2. A Schur matrix has all its eigenvalues strictly inside the unit circle.
3. The integrator gain κ is typically taken equal to the sampling period when (1) represents the discretisation of a continuous-time system.
4. Since the fault intensity parameter f_j is unknown, this separation requirement will be later assumed to hold of all f_j in some interval $\mathcal{I}_j \subset [0,1)$.
5. The time T of Definition 4.2 can be estimated, for example, using set-theoretic tools as explained in Appendix B.
6. A realistic nonlinear simulation model of the two-tank system used in Richter and Lunze 2009) was kindly provided by Jan Richter.
7. To avoid wrong controller reconfigurations during the initial transient, the FDI was not fed the initial values of the output estimation errors; instead, the FDI's decision was fixed to be equal to 4 for the first 50 time instants.

References

Basseville, M., and Nikiforov, I.V. (1993), *Detection of Abrupt Changes – Theory and Application*, Englewood Cliffs, NJ: Prentice-Hall.

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2006), *Diagnosis and Fault-tolerant Control* (2nd ed.), Secaucus, NJ: Springer.

Boskovic, J.D., and Mehra, R.K. (1999), 'Stable Multiple Model Adaptive Flight Control for Accommodation of a Large Class of Control Effector Failures', in *Proceedings of the 1999 American Control Conference*, San Diego, CA, June 1999, Vol. 6, pp. 1920–1924.

Chow, E.Y., and Willsky, A.S. (1984), 'Analytical Redundancy and the Design of Robust Failure Detection Systems', *IEEE Transactions on Automatic Control*, 29, 603–614.

Ding, S. (2008), *Model-based Fault Diagnosis Techniques*, Berlin, Heidelberg: Springer.

Frank, P.M. (1990), 'Fault Diagnosis in Dynamic Systems using Analytical and Knowledge-based Redundancy. A Survey and Some New Results', *Automatica*, 26, 459–474.

Frank, P.M., Ding, S.X., and Marcu, T. (2000), 'Model-based Fault Diagnosis in Technical Processes', *Transactions of the Institute of Measurement and Control*, 22, 57–101.

Isermann, R. (1984), 'Process Fault Detection Based on Modeling and Estimation Methods – A Survey', *Automatica*, 20, 387–404.

Isermann, R. (2006), 'Fault-dIagnosis Systems', *An Introduction from Fault Detection to Fault Tolerance*, Berlin: Springer.

Kofman, E.J., Haimovich, H., and Seron, M.M. (2007), 'A Systematic Method to Obtain Ultimate Bounds for Perturbed Systems', *International Journal of Control*, 80, 167–178.

Leonhardt, S., and Ayoubi, M. (1997), 'Methods of Fault Diagnosis', *Control Engineering Practice*, 5, 683–692.

Mahmoud, M., Jiang, J., and Zhang, Y. (2003), *Active Fault Tolerant Control Systems: Stochastic Analysis and Synthesis*, Lecture Notes in Control and Information Sciences, Vol. 287, Berlin: Springer.

Mhaskar, P., Gani, A., El-Farra, N.H., McFall, C., Christofides, P.D., and Davis, J.F. (2006), 'Integrated Fault-detection and Fault-tolerant Control of Process Systems', *AIChE Journal*, 52, 2129–2148.

Ocampo-Martínez, C., De Doná, J.A., and Seron, M.M. (2008), 'Actuator Fault Tolerant Control Based on Set Separation', in *Proceedings of the 17th IFAC World Congress*, Seoul, Korea, July 2008, 7276–7281.

Olaru, S., De Doná, J.A., and Seron, M.M. (2008), 'Positive Invariant Sets for Fault Tolerant Multisensor Control Schemes', in *Proceedings 17 IFAC World Congress*, Seoul, Korea, July, 1224–1229.

Patton, R., Frank, P.M., and Clark, R. (2000), *Issues of Fault Diagnosis for Dynamic Systems*, London: Springer.

Richter, J.H., and Lunze, J. (2009), 'H_∞-based Virtual Actuator Synthesis for Optimal Trajectory Recovery', in *Preprints of the 7TH IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SafeProcess'09)*, Barcelona, Spain.

Seron, M.M., De Doná, J.A., and Martínez, J.J. (2009), 'Invariant Set Approach to Actuator Fault Tolerant Control', in *7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS'09*, Barcelona, Spain, 30 June to 3 July 2009.

Steffen, T. (2005), *Control Reconfiguration of Dynamical Systems*, Berlin, Heidelberg: Springer.

Tang, X., Tao, G., and Joshi, S.M. (2007), 'Adaptive Actuator Failure Compensation for Nonlinear MIMO Systems with an Aircraft Control Application', *Automatica*, 43, 1869–1883.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., and Kavuri, S.N. (2003), 'A Review of Process Fault Detection and Diagnosis: Part I. Quantitative Model-based Methods', *Computers and Chemical Engineering*, 27, 293–311.

Willsky, A.S. (1976), 'A Survey of Design Methods for Failure Detection in Dynamic Systems', *Automatica*, 12, 601–611, November.

Wolff, F., Krutina, P., and Krebs, V. (2008), 'Robust Consistency-based Diagnosis of Nonlinear Systems by Set Observation', in *Proceedings of the 17th IFAC World Congress*, Seoul, Korea, pp. 10124–10129.

Zhang, Y., and Jiang, J. (2003), 'Bibliographical Review on Reconfigurable Fault-tolerant Control Systems', in *Proceedings of the 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS'03)*, Washington, D.C., USA, pp. 265–276.

Zhang, X., Parisini, T., and Polycarpou, M.M. (2004), 'Adaptive Fault-tolerant Control of Nonlinear Uncertain Systems: an Information-based Diagnostic Approach', *IEEE Transactions on Automatic Control*, 49, 1259–1274.

Appendix A

Attractive invariant sets

Consider a discrete-time dynamical system

$$\zeta^+ = \bar{A}\zeta + \bar{B}v, \tag{26}$$

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

$$v \in \mathcal{V} \quad \text{where } \mathcal{V} \triangleq \{v \in \mathbb{R}^t : |v - v^0| \le \bar{v}\}, \tag{27}$$

for some constant vectors v^0 and $\bar{v} \ge 0$ 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

$$\zeta^0 \triangleq (I_q - \bar{A})^{-1}\bar{B}\,v^0, \tag{28}$$

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

$$\Phi_0 \triangleq \{\zeta \in \mathbb{R}^q : |\bar{V}^{-1}\zeta| \le (I_q - |\bar{\Lambda}|)^{-1}|\bar{V}^{-1}\bar{B}|\bar{v} + \epsilon\} \oplus \{\zeta^0\}$$

($\oplus$ denotes Minkowski sum of sets) has the properties that the trajectories of (26)–(27) remain in Φ_0 if started inside and converge to Φ_0 (in finite time) if started outside (Kofman, Haimovich, and Seron 2007). Moreover, starting from 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 (26)–27) (Olaru, De Doná, and Seron 2008), that is, $\zeta^+ \in \Phi_k$ for all $\zeta \in \Phi_k$ and all $v \in \mathcal{V}$. Note that all sets Φ_k, $k \ge 0$, are 'centred' around ζ^0.

Appendix B

Computation of the set-transition time

For each $\ell = 1, \ldots, m$ and $i = 1, \ldots, N$, $i \ne \ell$, let the set $\mathcal{P}^*_{i\ell}$ be a polytopic set that contains the collection of 'after-fault' sets $\cup_{f_\ell \in \mathcal{I}_\ell}\mathcal{S}^+_i(f_\ell)$ (see (23)), that is $\mathcal{P}^*_{i\ell} \supseteq \cup_{f_\ell \in \mathcal{I}_\ell}\mathcal{S}^+_i(f_\ell)$. Next, compute the set recursion (see (14) and (23) and notice that $\mathbf{A}_{F^*_\ell,\ell} = \mathbf{A}_{F_\ell,\ell}$ and $\mathbf{B}_{F^*_\ell,\ell} = \mathbf{B}_{F_\ell,\ell}$)

$$\mathcal{P}_{i\ell}(t+1) = \mathbf{A}_{F_\ell,\ell}\,\mathcal{P}_{i\ell}(t) \oplus \mathbf{B}_{F_\ell,\ell}\,\mathcal{V}_\ell, \quad \mathcal{P}_{i\ell}(0) = \mathcal{P}^*_{i\ell}.$$

Let $\tau_{i\ell}$ be the minimum iteration index such that the inclusion $\mathcal{P}_{i\ell}(\tau_{i\ell}) \subseteq \mathcal{S}_\ell$ holds (this index is finite since $\mathcal{P}^*_{i\ell}$ is bounded and convergence from a bounded initial state to the attractive invariant set $\mathcal{S}_\ell$ in finite time is guaranteed for system (14) with $F = F_\ell$, see Definition 3.2 and Appendix A). Then the set-transition time of Definition 4.2 can be computed as

$$T = \max_{i,\ell}\{\tau_{i,\ell} : i \in \{1, \ldots, N\}, \ell \in \{1, \ldots, m\}, i \ne \ell\}.$$