Fault tolerant control using virtual actuators and invariant-set based fault detection and identification

María M. Seron and José A. De Doná

Abstract—In this paper we combine an invariant-set approach to fault detection and identification (FDI), recently proposed by the authors, with the virtual actuator approach to controller reconfiguration of Steffen, Lunze and co-authors. The FDI approach is based on the separation of invariant sets that characterise healthy system operation from invariant sets that characterise faulty operation. The derivation of these sets takes into account the closed-loop system reconfigured by means of the virtual actuator under all considered fault situations. We provide analytic conditions, in terms of closed-loop system parameters and bounds on external signals, which guarantee the aforementioned set separation and, thus, closed-loop stability of the scheme under all considered fault situations.

I. INTRODUCTION

We have recently presented in [1] and [2] a novel fault tolerant control (FTC) scheme that utilises a new decision criterion for fault detection and identification (FDI). This new criterion is based on the computation of invariant 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 invariant sets that characterise healthy operation from the ones that characterise faulty operation.

In [1] and [2], controller reconfiguration was achieved by utilising a standard approach where a bank of control laws was designed to achieve reference tracking for each of the considered fault situations that can occur in the plant (see, for example, [3]). In the present paper, we employ a different type of controller reconfiguration based on the concept of *virtual actuators* [3], [4], [5], [6]. This approach is illustrated in Fig. 1. In this figure, the *nominal* feedback control loop is shown in solid lines. It consists of a plant with input u , measured output y and performance output v , and a *nominal* controller with input y_c and output u_c . (The remaining signals in the figure are a process disturbance w , a measurement disturbance η , and a reference signal u_{ref} .) Plant and nominal controller are normally (in healthy operation) interconnected by setting $y_c = y$ and $u = u_c$, as indicated by the solid lines in Fig. 1. When actuators (or other system components) fail and disrupt the control loop, it is usually necessary to reconfigure the control system by changing its structure (for example, by creating new interconnections, using different sets of input and output signals, activating/desactivating system components, etc.). One solution to the reconfiguration problem, which tries to apply a minimal change to the control

Fig. 1. Feedback control loop with virtual actuator

loop, is based on the use of a *virtual actuator*. The latter is a dynamic system with inputs y and u_c and outputs y_c and u (see Fig. 1), which only interferes with the nominal loop when an actuator fault is detected. In this case, the role of the virtual actuator is to generate new interconnections (as indicated by the dashed crosses in Fig. 1) that produce, together with the faulty plant, for a given input u_c , the same (or approximately the same) output y_c as the nominal plant. Hence, the nominal controller, which remains an unchanged block of the loop, “sees” the same plant and reacts in the same way as before the fault [3]. The plant, on the other hand, receives the input u “reconfigured” by the virtual actuator. The advantage of this approach is that any existing nominal controller, which has been designed to satisfy the desired specifications for the plant, can be used and kept in the loop at all times. In addition, the design of the virtual actuator is aimed at preserving specific closed-loop properties under fault, for example, stability and setpoint tracking [4]. In this paper we combine the virtual actuator approach to controller reconfiguration with the invariant-set approach to FDI. The combined FTC scheme has pre-checkable analytic conditions that guarantee closed-loop stability and setpoint tracking under all considered fault situations.

II. PLANT AND ACTUATOR FAULT MODELS

The plant is given by the linear discrete-time model¹

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

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

$$v = C_v x, \quad (1c)$$

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

¹The dependence on time k will be omitted when clear from the context.

The authors are with the Centre for Complex Dynamic Systems and Control, School of Elec. Eng. and Comp. Sci., The University of Newcastle, Callaghan 2308, NSW, Australia. J.A. De Doná is currently on study leave with a visiting position at CAS, Ecole des Mines de Paris, France.

disturbance and $v \in \mathbb{R}^q$ is a performance output. Matrix $F \in \mathbb{R}^{m \times m}$ in (1a) models actuator faults; we consider that F can take $N + 1$ different (a priori known) values

$$F \in \{F_0, F_1, \dots, F_N\}, \quad (2)$$

In particular, $F_0 = I$ (the identity matrix) represents the “nominal” case, that is, no actuator fault, and, for example,

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

models the loss of the i th actuator. We will say that an (abrupt) change in the actuator fault situation occurs if F changes from $F = F_i$ to $F = F_j$, $i, j \in \{0, \dots, N\}$, $j \neq i$, at some time $k_F \geq 0$.

We assume the following properties of system (1).

Assumption 2.1: The pair (A, C) is detectable and the pairs (A, BF_i) , for $i = 0, 1, \dots, N$ are stabilisable. In addition, to ensure the possibility to achieve constant setpoint tracking, we assume that the matrix $\begin{bmatrix} A-I & BF_i \\ C_v & 0 \end{bmatrix}$ has rank $n + q$, for $i = 0, 1, \dots, N$. $\circ$

Assumption 2.2 (Disturbance Bounds): Bounding sets² $\mathcal{W} \triangleq \{w \in \mathbb{R}^r : |w| \leq \bar{w}\}$ 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 disturbances satisfy $w(k) \in \mathcal{W}$ and $\eta(k) \in \mathcal{N}$ for all time instants $k \geq 0$. $\circ$

III. NOMINAL CONTROLLER

Consider the observer-based, reference tracking controller

$$u_c = -K(\hat{x} - x_{\text{ref}}) + u_{\text{ref}}, \quad (3)$$

$$\hat{x}^+ = A\hat{x} + Bu_c + L(y_c - C\hat{x}), \quad (4)$$

$$x_{\text{ref}}^+ = Ax_{\text{ref}} + Bu_{\text{ref}}. \quad (5)$$

The controller (3)–(5) satisfies the following assumptions.

Assumption 3.1 (Nominal Observer Gain): The gain L in (4) is such that $A - LC$ is a Schur matrix.³ (This can always be satisfied by Assumption 2.1). $\circ$

Assumption 3.2 (Controller Gain): The gain K in (3) is such that $A - BK$ is a Schur matrix. (This can always be satisfied by Assumption 2.1.) $\circ$

Assumption 3.3 (Reference Bounds): Constant vectors $u_{\text{ref}}^0 \in \mathbb{R}^m$ and $\bar{u}_{\text{ref}} \in \mathbb{R}^m$ are known such that, for all $k \geq 0$, $u_{\text{ref}}(k) \in \mathcal{U}_{\text{ref}} = \{u \in \mathbb{R}^m : |u - u_{\text{ref}}^0| \leq \bar{u}_{\text{ref}}\}$. $\circ$

Remark 3.4 (Reference Exosystem): The reference system (5) is designed such that the output $C_v x_{\text{ref}}$, where C_v is as in (1c), asymptotically tracks an external signal v^* , that is, $\lim_{k \rightarrow \infty} [C_v x_{\text{ref}}(k) - v^*(k)] = 0$. The signal v^* is a reference trajectory that we ultimately wish the plant output v in (1c) to track, in the absence of disturbances, under all possible fault situations. Under the stated assumptions, it is straightforward to design an “exosystem” that achieves the above property. It is also straightforward, given the exosystem, to obtain the bounds and offsets, $\bar{u}_{\text{ref}}$ and u_{ref}^0 , respectively, of Assumption 3.3. The offset u_{ref}^0 , in particular, is related to the offset of the reference signal v^* . $\circ$

²Inequalities and absolute values are taken elementwise.

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

A. Nominal Closed-Loop System

It is convenient to define the nominal observer estimation error, $\tilde{x}$, and the tracking error, z , as

$$\tilde{x} \triangleq x - \hat{x}, \quad z \triangleq x - x_{\text{ref}}. \quad (6)$$

From (1) and (3)–(5), setting $y_c = y$, $u = u_c$ and $F = F_0 = I$ (nominal conditions) we have

$$\tilde{x}^+ = (A - LC)\tilde{x} + Ew - L\eta, \quad (7)$$

$$z^+ = (A - BK)z + BK\tilde{x} + Ew. \quad (8)$$

Note from Assumptions 3.1 and 3.2, that, in the absence of disturbances ($w \equiv 0$, $\eta \equiv 0$), both estimation and tracking errors converge to zero. The tracking objective explained in Remark 3.4 will then be achieved for the nominal closed-loop system. Moreover, using Theorem 3.2 of [7] and the bounds on the disturbances described in Assumption 2.2, we can compute the following attractive invariant set:⁴

$$\tilde{\mathcal{X}} \triangleq \left\{ \tilde{x} \in \mathbb{R}^n : |\tilde{V}^{-1}\tilde{x}| \leq \tilde{r} + \tilde{\epsilon} \right\}, \quad (9)$$

where $\tilde{r} \triangleq (I - |\tilde{\Lambda}|)^{-1} |\tilde{V}^{-1} [E \ -L]| [\bar{w}' \ \bar{\eta}']'$, $\tilde{V}\tilde{\Lambda}\tilde{V}^{-1}$ is the Jordan decomposition of $A - LC$ and $\tilde{\epsilon} > 0$ is any (arbitrarily small) vector. From (9), we can compute the following ultimate bound⁵ on $\tilde{x}$:

$$|\tilde{x}| \leq \bar{\tilde{x}} + |\tilde{V}|\tilde{\epsilon}, \quad \text{where } \bar{\tilde{x}} \triangleq |\tilde{V}|\tilde{r}. \quad (10)$$

Similarly, we can compute the following attractive invariant set for the tracking error system (8):

$$\mathcal{Z} \triangleq \{z \in \mathbb{R}^n : |V^{-1}z| \leq r_z + \epsilon_z\}, \quad (11)$$

where $r_z \triangleq (I - |\Lambda|)^{-1} |V^{-1} [E \ BK]| [\bar{w}' \ (\bar{\tilde{x}} + |\tilde{V}|\tilde{\epsilon})']'$, $V\Lambda V^{-1}$ is the Jordan decomposition of $A - BK$, $\epsilon_z > 0$ is any (arbitrarily small) vector and $\bar{\tilde{x}}$ was defined in (10). From (11), we can compute the ultimate bound on z :

$$|z| \leq \bar{z} + |V|\epsilon_z \quad \text{where } \bar{z} \triangleq |V|r_z. \quad (12)$$

Remark 3.5 (Invariant set refinement): The attractive invariant sets of the form (9) and (11) are constructed using techniques developed in [8]. These sets can be tightened using the results of [9], where a contractive procedure was developed to obtain arbitrarily close approximations of the minimal robust positively invariant set for a stable system driven by bounded disturbances. $\circ$

IV. VIRTUAL ACTUATOR WITH SETPOINT TRACKING

We consider the following virtual actuator with integral action proposed by [4] (Section 9.4):

$$\begin{bmatrix} \theta^+ \\ \sigma^+ \end{bmatrix} = \begin{bmatrix} A & 0 \\ C_v & I \end{bmatrix} \begin{bmatrix} \theta \\ \sigma \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} u_c - \begin{bmatrix} B \\ 0 \end{bmatrix} F_\ell u_\ell, \quad (13)$$

⁴For our purposes, an attractive invariant set for a dynamic system is a set in which the trajectories of the system will remain if started inside or towards which the trajectories will converge in finite time if started outside.

⁵If $\nu(k) \in \mathbb{R}^m$ is a discrete-time signal and $\bar{\nu} \geq 0$ is a vector in $\mathbb{R}^m$, the notation $|\nu| \leq \bar{\nu}$ denotes the elementwise ultimate bound $|\nu(k)| \leq \bar{\nu}$ for all times $k \geq k^*$, for some $k^* \geq 0$.

$$u_\ell = \begin{cases} u_c - M_0 \begin{bmatrix} \theta' & \sigma' \end{bmatrix}' & \text{if } \ell = 0, \\ -M_\ell \begin{bmatrix} \theta' & \sigma' \end{bmatrix}' & \text{if } \ell \in \{1, \dots, N\}, \end{cases} \quad (14)$$

$$u = u_\ell + d_\ell, \quad (15)$$

$$y_c = y + C\theta, \quad (16)$$

where $\theta \in \mathbb{R}^n$ is the virtual actuator state; $\sigma \in \mathbb{R}^q$ is the integral action state; F_ℓ , for $\ell = 0, \dots, N$ is as in (2) (with $F_0 = I$); the matrices M_ℓ , for $\ell = 0, \dots, N$, are such that

$$A_\ell \triangleq \begin{bmatrix} A & 0 \\ C_v & I \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} F_\ell M_\ell \quad (17)$$

are Schur (this is always possible due to the stabilisability and rank conditions of Assumption 2.1);

$$d_\ell = \begin{cases} M_0 \begin{bmatrix} \theta' & \sigma' \end{bmatrix}' & \text{if } \ell = 0, \\ \text{constant and } F_\ell d_\ell = 0 & \text{if } \ell \in \{1, \dots, N\}, \end{cases} \quad (18)$$

is a degree of freedom in the design; and the remaining signals and matrices are as in equations (1)–(5).

The following theorem, which extends the results of [4] to the discrete-time case, establishes the properties of the above virtual actuator.

Theorem 4.1: Assume that the virtual actuator *matches the plant fault situation*, i.e., in (1a) and (13), $F_\ell = F$. Then the virtual actuator given by equations (13)–(16) achieves the following goals for the closed-loop system (1)–(5): (i) fault hiding, i.e., the controller signals u_c and y_c are restored to their nominal trajectory; (ii) stabilisation i.e., all poles of the reconfigured closed-loop system are strictly inside the unit circle and (iii) equilibrium restoration, i.e., the performance signal v in (1c) is restored to its nominal constant value when the external signals w and η are zero and u_{ref} is constant.

Proof: We analyse the cases $\ell = 0$ and $\ell \in \{1, \dots, N\}$ separately. The case $\ell = 0$ corresponds to the nominal case, that is, no actuator fault. In this case, $u = u_c$ and, if the virtual actuator has zero initial condition, then (13)–(16), (18) yield $y_c = y$, thus leaving the nominal control loop of Fig. 1 unchanged. If the virtual actuator has initial state different from zero, then the condition $y_c = y$ is attained asymptotically, since the controller dynamics reduces in this case to $[(\theta^+)' \ (\sigma^+)']' = A_0 [\theta' \ \sigma']'$ with A_0 Schur.

The cases $\ell \in \{1, \dots, N\}$ correspond to each of the considered actuator fault modes, as described by the matrix F in (2). For these cases, consider the variable

$$\xi \triangleq x + \theta. \quad (19)$$

From (1a) and (13), when $F_\ell = F$ (that is, the virtual actuator “matches” the plant fault situation), and using (15), (16), (1b) and (18), we have that ξ in (19) satisfies

$$\xi^+ = A\xi + Bu_c + Ew, \quad y_c = C\xi + \eta, \quad (20)$$

which coincides with the nominal plant dynamics ($F = I$) with input u_c and output y_c (see (1a)–(1b) and Fig. 1). Now, even though controller (3)–(5) is designed for the nominal system ($F = I$), so as to achieve nominal stability (see (7) and (8)), this would not be the case, in general,

when the plant is faulty ($F = F_1, F_2$, etc.). However, by virtue of (16) (and the rest of the construct), the controller can also be thought of as controlling system (20), which, despite having been derived for a faulty case has the same form as the nominal system (1a)–(1b), that is, the matrix F does not appear in the model. Hence, the virtual actuator effectively “hides” the fault from the nominal controller (3)–(5), which continues to receive its nominal input y_c and generate its nominal output u_c , thus achieving the fault hiding objective (i).

In relation with (19), we will also introduce the variables

$$\tilde{\xi} \triangleq \xi - \hat{x}, \quad \zeta \triangleq \xi - x_{\text{ref}}. \quad (21)$$

From (21), and using (3)–(5) and (20), we obtain

$$\tilde{\xi}^+ = (A - LC)\tilde{\xi} + Ew - L\eta, \quad (22)$$

$$\zeta^+ = (A - BK)\zeta + BK\tilde{\xi} + Ew. \quad (23)$$

Comparing the above two equations with (7) and (8), we see that the variables $\tilde{\xi}$ and ζ have exactly the same dynamic behaviour as the variables $\tilde{x}$ and z , respectively, of the nominal closed-loop system. Since the latter is stable by design, then the stabilisation objective (ii) is achieved.

Next, note from (21) that the nominal control law (3) can be equivalently expressed as

$$u_c = -K\zeta + K\tilde{\xi} + u_{\text{ref}}, \quad (24)$$

and, hence, when the external signals w and η are zero, it follows from (22)–(23) and Assumptions 3.1 and 3.2, that $u_c = u_{\text{ref}}$ in steady state. Thus, if u_{ref} is constant, and since the matrix A_ℓ defined in (17) is Schur, then the virtual actuator (13)–(14) reaches a constant equilibrium point. In particular, the integral action state in steady state satisfies $\sigma^+ = \sigma$, which yields $C_v\theta = 0$. Combining this information with (1c) and (19) we obtain $v = C_v x = C_v(\xi - \theta) = C_v\xi$. Moreover, since in the absence of disturbances, we have from (21)–(23) that ξ converges to x_{ref} in steady state, then v converges to $C_v x_{\text{ref}}$ in steady state. Finally, together with the property $\lim_{k \rightarrow \infty} [C_v x_{\text{ref}}(k) - v^*] = 0$ of Remark 3.4, we have that v converges to v^* in steady state, for constant v^* . Thus, the nominal equilibrium of v is restored and objective (iii) is also achieved. ■

We will next derive attractive invariant sets for the trajectories of the virtual actuator dynamics (13)–(14). From (24) together with (13)–(14), (17), we have

$$\phi^+ = A_\ell \phi + \underbrace{\begin{bmatrix} B \\ 0 \end{bmatrix} \begin{bmatrix} -K & K & I \end{bmatrix}}_{B_\phi} \begin{bmatrix} \zeta \\ \tilde{\xi} \\ u_{\text{ref}} \end{bmatrix}, \quad \phi \triangleq \begin{bmatrix} \theta \\ \sigma \end{bmatrix}. \quad (25)$$

From (22)–(23) we note that the variables $\tilde{\xi}$ and ζ converge to the sets $\tilde{X}$ of the form (9) and Z of the form (11), respectively, under the conditions of Assumption 2.2. Thus, the variables $\tilde{\xi}$ and ζ can be ultimately bounded as in (10) and (12), respectively, that is, $|\tilde{\xi}| \leq \tilde{x} + |\tilde{V}|\tilde{\epsilon}$, $|\zeta| \leq \bar{z} + |\bar{V}|\epsilon_z$. Using these bounds and a minor modification of Theorem 3.2 of [7] (see also [8] and [9]) applied to system (25), together

with the bounds on the reference trajectory given in Assumption 3.3, we can compute the following ultimate-bound attractive invariant sets, for $\ell = 1, \dots, N$:

$$\Phi_\ell \triangleq \{\phi \in \mathbb{R}^{n+q} : |V_\ell^{-1}(\phi - \phi_\ell^0)| \leq r_\ell + \epsilon_\phi\}, \quad (26)$$

$$\text{where } \phi_\ell^0 \triangleq (I - A_\ell)^{-1} \begin{bmatrix} B \\ 0 \end{bmatrix} u_{\text{ref}}^0, \quad (27)$$

$r_\ell \triangleq (I - |\Lambda_\ell|)^{-1} |V_\ell^{-1} B_\phi| \left[(\bar{z} + |V| \epsilon_z)' (\bar{x} + |\tilde{V}| \bar{\epsilon})' \overline{u_{\text{ref}}} \right]',$ $V_\ell \Lambda_\ell V_\ell^{-1}$ is the Jordan decomposition of A_ℓ and $\epsilon_\phi > 0$ is any (arbitrarily small) vector. From (26), we can compute an ultimate bound on ϕ :

$$|\phi - \phi_\ell^0| \leq \bar{\phi}_\ell + |V_\ell| \epsilon_\phi, \quad \text{where } \bar{\phi}_\ell \triangleq |V_\ell| r_\ell. \quad (28)$$

The above analysis assumed that the virtual actuator matches the plant fault situation, that is, in (1a) and (13), $F_\ell = F$. In the following sections we will propose a mechanism to identify the current plant fault situation in order to communicate it to the virtual actuator for correct controller reconfiguration.

V. FAULT DETECTION AND IDENTIFICATION APPROACH

In this section we describe the proposed FDI approach.

A. Bank of State Observers for FDI

The scheme employs the bank of N state observers

$$\dot{\hat{x}}_i^+ = A \hat{x}_i + B F_i u + L_i (y - C \hat{x}_i), \quad i = 1, \dots, N, \quad (29)$$

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 5.1 (Observer Gains): The gains L_i , for $i = 1, \dots, N$, are such that $A - L_i C$ are Schur matrices. (This can always be satisfied by Assumption 2.1.) $\circ$

To each observer we associate the state and output estimation errors

$$\tilde{x}_i \triangleq x - \hat{x}_i, \quad \tilde{y}_i \triangleq y - C \hat{x}_i = C \tilde{x}_i + \eta, \quad (30)$$

for $i = 1, \dots, N$. From (1a), (1b) and (29), we have

$$\tilde{x}_i^+ = (A - L_i C) \tilde{x}_i + B(F - F_i)u + Ew - L_i \eta. \quad (31)$$

B. Attractive Invariant Sets for the FDI Estimation Errors

We will next derive attractive invariant sets for the estimation error dynamics (31) assuming, once again, that the virtual actuator matches the plant fault situation, that is, $F_\ell = F$ in (1a) and (13). Consider first the nominal case $\ell = 0$ and $F = F_0 (= I)$. As discussed in the proof of Theorem 4.1, $u = u_c$ in this case. Note from (3) and (6) that

$$u = u_c = -Kz + K\tilde{x} + u_{\text{ref}}. \quad (32)$$

Substituting (32) in (31) yields, for $i = 1, \dots, N$,

$$\tilde{x}_i^+ = A_{L_i} \tilde{x}_i + \underbrace{\begin{bmatrix} B(F_0 - F_i) \end{bmatrix} \begin{bmatrix} -K & K & I \end{bmatrix} \begin{bmatrix} E & -L_i \end{bmatrix}}_{B_{i0}} \begin{bmatrix} \tilde{z} \\ \tilde{x} \\ u_{\text{ref}} \\ w \\ \eta \end{bmatrix}, \quad (33)$$

where $A_{L_i} \triangleq (A - L_i C)$ and the second subindex of the matrix B_{i0} corresponds to the current plant matrix $F = F_0$.

Using (10), (12), and the bounds in Assumptions 2.2 and 3.3, attractive invariant sets for (33) can be computed as

$$\tilde{X}_{i0} \triangleq \left\{ \tilde{x}_i \in \mathbb{R}^n : \left| \tilde{V}_i^{-1}(\tilde{x}_i - \tilde{x}_{i0}^0) \right| \leq \tilde{r}_{i0} + \tilde{\epsilon}_{i0} \right\}, \quad (34)$$

for $i = 1, \dots, N$, where $\tilde{V}_i \tilde{\Lambda}_i \tilde{V}_i^{-1}$ is the Jordan decomposition of A_{L_i} , $\tilde{r}_{i0} \triangleq (I - |\tilde{\Lambda}_i|)^{-1} \left| \tilde{V}_i^{-1} B_{i0} \right| \left[(\bar{z} + |V| \epsilon_z)' (\bar{x} + |\tilde{V}| \bar{\epsilon})' \overline{u_{\text{ref}}} \overline{w}' \overline{\eta}' \right]',$ $\tilde{\epsilon}_{i0} > 0$ and the “centres” $\tilde{x}_{i0}^0$ are defined as

$$\tilde{x}_{i0}^0 \triangleq (I - A_{L_i})^{-1} B(F_0 - F_i) u_{\text{ref}}^0. \quad (35)$$

Next consider the case $\ell \in \{1, \dots, N\}$ and $F = F_\ell$. From (15), (14) and (25) we have that

$$u = -M_\ell \phi + d_\ell, \quad (36)$$

and further substituting in (31) yields, for $i, \ell \in \{1, \dots, N\}$,

$$\tilde{x}_i^+ = A_{L_i} \tilde{x}_i + \underbrace{\begin{bmatrix} B(F_\ell - F_i) \end{bmatrix} \begin{bmatrix} -M_\ell & I \end{bmatrix} \begin{bmatrix} E & -L_i \end{bmatrix}}_{\tilde{B}_{i\ell}} \begin{bmatrix} \phi \\ d_\ell \\ w \\ \eta \end{bmatrix}, \quad (37)$$

where the second subindex of the matrix $\tilde{B}_{i\ell}$ corresponds to the current plant matrix $F = F_\ell$. Using (28), (18), and the bounds in Assumptions 2.2 and 3.3, attractive invariant sets for (37) can be computed, for $i, \ell \in \{1, \dots, N\}$, as

$$\tilde{X}_{i\ell} \triangleq \left\{ \tilde{x}_i \in \mathbb{R}^n : \left| \tilde{V}_i^{-1}(\tilde{x}_i - \tilde{x}_{i\ell}^0) \right| \leq \tilde{r}_{i\ell} + \tilde{\epsilon}_{i\ell} \right\}, \quad (38)$$

where $\tilde{r}_{i\ell} \triangleq (I - |\tilde{\Lambda}_i|)^{-1} \left| \tilde{V}_i^{-1} \tilde{B}_{i\ell} \right| \left[(\bar{\phi}_\ell + |V| \epsilon_\phi)' \overline{0} \overline{w}' \overline{\eta}' \right]'$ and $\tilde{\epsilon}_{i\ell} > 0$. The sets (38) are “centred” at

$$\tilde{x}_{i\ell}^0 \triangleq (I - A_{L_i})^{-1} [-B(F_\ell - F_i) M_\ell \phi_\ell^0 - B F_i d_\ell]. \quad (39)$$

Both for (34) and (38), the corresponding output estimation error in (30) has the associated sets for $i = 1, \dots, N$, $\ell = 0, 1, \dots, N$ ($\oplus$ denotes the Minkowski sum)

$$\tilde{Y}_{i\ell} \triangleq C \tilde{X}_{i\ell} \oplus \mathcal{N}, \quad (40)$$

where $\mathcal{N}$ is as in Assumption 2.2.

C. After-fault Sets

The analysis that follows assumes that the system has evolved with the virtual actuator matching the plant fault situation for sufficiently long time such that, if $\ell = 0$, the estimation errors (33) are in the corresponding sets $\tilde{X}_{i0}$, for $i = 1, \dots, N$, defined in (34) (with associated output estimation errors in the sets $\tilde{Y}_{i0}$ defined in (40)), or, if $\ell \in \{1, \dots, N\}$, they are in the corresponding sets $\tilde{X}_{i\ell}$, for $i = 1, \dots, N$ defined in (38) (with associated output estimation error in the set $\tilde{Y}_{i\ell}$ defined in (40)).

Then, at some time k_F , a change in the plant fault situation occurs and the system matrix F in (1a) changes from $F = F_\ell$ to $F = F_j$, for some $j \in \{0, 1, \dots, N\}$, $j \neq \ell$.

Definition 5.2 (After-fault Sets): We define the “after-fault” sets $\tilde{X}_{ij\ell}^+$ as the sets where the state estimation error $\tilde{x}_i$ lives at the time instant $(k_F + 1)$ after the change in the plant fault situation. The subindices of $\tilde{X}_{ij\ell}^+$ indicate: i , the index of the observer to which the set is associated; j , the new fault situation; ℓ , the previous fault situation. $\circ$

We then have:

- if $\ell = 0$, using the dynamic equation (33) (noting that u in (32) at time k_F is not affected by the fault since the virtual actuator has not been reconfigured yet), the sets (11), (9), and Assumptions 2.2 and 3.3, the “after-fault” state estimation error $\tilde{x}_i^+$ (that is, at time $k_F + 1$) satisfies

$$\tilde{x}_i^+ \in \tilde{X}_{ij0}^+, \tilde{X}_{ij0}^+ \triangleq A_{L_i} \tilde{X}_{i0} \oplus B_{ij}(Z \times \tilde{X} \times \mathcal{U}_{\text{ref}} \times \mathcal{W} \times \mathcal{N}) \quad (41)$$

where the matrix B_{ij} , of the form of B_{i0} in (33) with F_0 replaced by F_j , reflects the new fault situation in the plant.

- if $\ell \in \{1, \dots, N\}$, using the dynamic equation (37) (noting that u in (36) at time k_F is not affected by the fault), the set (26) and Assumption 2.2, the “after-fault” state estimation error $\tilde{x}_i^+$ (that is, at time $k_F + 1$) satisfies

$$\tilde{x}_i^+ \in \tilde{X}_{ij\ell}^+, \tilde{X}_{ij\ell}^+ \triangleq A_{L_i} \tilde{X}_{i\ell} \oplus \bar{B}_{ij\ell}(\Phi_\ell \times \{d_\ell\} \times \mathcal{W} \times \mathcal{N}), \quad (42)$$

where the matrix $\bar{B}_{ij\ell}$, of the form of $\bar{B}_{i\ell}$ in (37) with F_ℓ replaced by F_j , reflects the new fault situation in the plant.

Define, for $i = 1, \dots, N$, $j, \ell = 0, 1, \dots, N$, $j \neq \ell$, the sets

$$\tilde{Y}_{ij\ell}^+ \triangleq C \tilde{X}_{ij\ell}^+ \oplus \mathcal{N}, \quad (43)$$

where $\tilde{X}_{ij\ell}^+$ is as defined in (41), for $\ell = 0$, and in (42), for $\ell \neq 0$. Note that the “after-fault” output estimation error associated with the i th observer will belong to the set $\tilde{Y}_{ij\ell}^+$ if before the fault the estimation error $\tilde{x}_i$ belonged to the set $\tilde{X}_{i\ell}$ defined in (34), for $\ell = 0$, and in (38), for $\ell \neq 0$.

VI. FDI ALGORITHM AND CLOSED-LOOP STABILITY

In this section we describe the proposed FDI algorithm and establish the stability properties of the resulting FTC scheme. We begin with the following assumption.

Assumption 6.1 (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

$$\max \{ \tilde{y}_i' P_i \tilde{y}_i : \tilde{y}_i \in S_i \} < r_i < \min \{ \tilde{y}_i' P_i \tilde{y}_i : \tilde{y}_i \in S_i^F \},$$

$$\text{where } S_i \triangleq \tilde{Y}_{ii} \cup \bigcup_{\substack{j=0 \\ j \neq i}}^N \tilde{Y}_{ij}^+, S_i^F \triangleq \left[\bigcup_{\substack{j=0 \\ j \neq i}}^N \tilde{Y}_{ij} \right] \cup \left[\bigcup_{\substack{j=0 \\ j \neq i}}^N \bigcup_{\substack{k=0 \\ k \neq j}}^N \tilde{Y}_{ijk}^+ \right].$$

There are two main mechanisms to achieve the above set separation. One is to adjust the offset of the reference signal v^* , which changes the offset u_{ref}^0 (see Remark 3.4) and, in consequence, the centres in (35) and (39) and the offsets of the sets $\mathcal{U}_{\text{ref}}$ and Φ_ℓ in (41) and (42) that correspond, respectively, to the dynamics (33) and (37). The other is to exploit the degrees of freedom d_ℓ defined in (18), which change the centres in (39) and the offset in (42).

We also require the following definition.

Definition 6.2 (Convergence Time): Let T be an upper bound on the time it takes for the trajectories of the estimation errors $\tilde{x}_i$, for all state observers, $i = 1, \dots, N$ and all plant fault situations $F = F_j$, $j = 0, 1, \dots, N$, to converge from the set $\tilde{X}_{ijk}^+$, for all $k = 0, 1, \dots, N$, $k \neq j$, to the attractive invariant set $\tilde{X}_{ij}$ according to the dynamics (33) for $j = 0$ and (37) for $j \neq 0$. $\circ$

Based on the above assumption and definition, the fault detection criterion and controller reconfiguration implemented by the FDI algorithm can be outlined as follows:

Algorithm 6.3 (FDI and Reconfiguration):

Off-line initialisation: The initial fault situation, $F = F_j$ say, for some $j \in \{0, 1, \dots, N\}$, is known and we set $\ell = j$ in the virtual actuator equations (13)–(16).

On-line algorithm:

- 1) While one of the following two situations holds:
    - $\tilde{y}_j' P_j \tilde{y}_j \leq r_j$, for $j \in \{1, \dots, N\}$, use (13)–(16) with $\ell = j$;
    - $\tilde{y}_i' P_i \tilde{y}_i > r_i$, for **all** $i = 1, \dots, N$, use (13)–(16) with $\ell = 0$.
  - 2) If, at some time instant,
    - $\tilde{y}_j' P_j \tilde{y}_j > r_j$ and $\tilde{y}_i' P_i \tilde{y}_i \leq r_i$, for some $i \in \{1, \dots, N\}$, $i \neq j$, reconfigure (13)–(16) by changing $\ell = j$ to $\ell = i$;
    - $\tilde{y}_i' P_i \tilde{y}_i > r_i$, for **all** $i = 1, \dots, N$, reconfigure (13)–(16) by changing $\ell = j$ to $\ell = 0$.
  - 3) Wait for T time steps before going back to step 1). $\circ$
- We also impose an assumption on the allowed fault scenario.

Assumption 6.4 (Fault Scenario): The time between any two consecutive changes in the fault matrix F is, at least, $T+1$ time instants, with T as in Definition 6.2. $\circ$

We then have the following result.

Theorem 6.5: Under Assumptions 2.1 to 6.4, the states of the closed-loop system represented in Fig. 1, encompassing the plant (1)–(2), the nominal tracking controller (3)–(5) and the virtual actuator (13)–(16) reconfigured by Algorithm 6.3, are bounded. Moreover, in the absence of disturbances, the variable v defined in (1c) converges, in steady state, to the reference signal v^* defined in Remark 3.4, when v^* is constant.

Proof: (Outline) Assumptions 2.1 to 5.1 on the plant properties and bounds on the external signals allow us to compute invariant sets for the different variables in the resulting closed-loop system. In particular, we can compute invariant sets for the FDI output estimation errors and associated “after-fault” sets which are used in Assumption 6.1. Then, Assumptions 6.1 and 6.4, guarantee that the FDI Algorithm 6.3 detects the correct new plant fault situation within one sample from the occurrence of a change and hence the analysis of Section IV (which assumes that the virtual actuator matches the plant fault situation) follows. In particular, all states of the closed-loop system are bounded and, in the absence of disturbances, v in (1c) converges to $C_v x_{\text{ref}}$ in steady state. Finally, together with the property $\lim_{k \rightarrow \infty} [C_v x_{\text{ref}}(k) - v^*] = 0$ of Remark 3.4, we have that v converges to v^* in steady state, for constant v^* . ■

VII. EXAMPLE

Consider the plant model (1a) where

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

w satisfies $|w| \leq 0.001$ and $F \in \{F_0, F_1, F_2\}$ with $F_0 = I$, $F_1 = \text{diag}(0, 1)$, and $F_2 = \text{diag}(1, 0)$. The output matrix in (1b) is $C = I$ and η satisfies $|\eta| \leq [0.005 \ 0.005]'$. The performance matrix in (1c) is $C_v = [1 \ 0]$. The tracking controller (3)–(5) employs the feedback gain $K = \begin{bmatrix} 7.2662 & 3.7147 \\ 10.8993 & 5.5721 \end{bmatrix}$, computed

Fig. 2. Sets for observers $i = 1, 2$.

to place the eigenvalues of $A - BK$ at $[0.6 \ 0.7]$. The reference signal (5) satisfies Assumption 3.3 with $u_{\text{ref}}^0 = [6.1538 \ 9.2308]'$, $\bar{u}_{\text{ref}} = [0.6154 \ 0.9231]'$. The virtual actuator matrices M_1 and M_2 in (14) are chosen as $M_1 = \begin{bmatrix} 0 & 0 \\ -75.9706 & -16.5197 \\ 0 & -5.2895 \end{bmatrix}$, $M_2 = \begin{bmatrix} 0 & 0 \\ -113.9558 & -24.7795 \\ 0 & -7.9342 \end{bmatrix}$. The “degree of freedom” signals d_1 and d_2 in (18) are selected as $d_1 = [-70 \ 0]'$ and $d_2 = [0 \ -35]'$. The FDI mechanism employs two observers of the form (29) whose gains $L_2 = L_3 = L$ are computed by pole placement (to place the eigenvalues of $A - LC$ at $[0.0273 \ 0.0318]$) as $L = \begin{bmatrix} 0.9703 & 0.0975 \\ -0.0487 & 0.9170 \end{bmatrix}$. Fig. 2 shows the sets (40) and (43) (with $i = j$) for observers $i = 1$ and $i = 2$, inside circles of radii $r_1 = 0.2$ and $r_2 = 0.22$, respectively. The remaining sets of the form (40) and (43) (with $i \neq j$) lie outside the circle (some of the sets are not shown for clarity of the figure). Thus, Assumption 6.1 holds with $P_i = I$, for $i = 1, 2$, and $r_1 = (0.2)^2$, $r_2 = (0.22)^2$.

We simulated the FTC scheme described above under the following fault scenario. The plant starts with the nominal condition $F = F_0$ at time $k = 0$. Then the following changes in the plant fault matrix F occur: $F_0 \rightarrow F_2$ at $k = 110$; $F_2 \rightarrow F_1$ at $k = 220$; $F_1 \rightarrow F_0$ at $k = 330$; $F_0 \rightarrow F_1$ at $k = 440$. The top subplot of Fig. 3 shows the index ℓ selected by the FDI algorithm, which makes the right decision for all tested faults. The last two subplots of Fig. 3 show the 2-norms of the output estimation errors $\tilde{y}_1$ and $\tilde{y}_2$, defined in (30). Also shown in these subplots (red line) are the values $r_1 = 0.2$ (second subplot) and $r_2 = 0.22$ (third subplot) of the radii of the circles that separate the sets around zero from those away from zero (the blue dotted circle in Fig. 2). Notice that the 2-norms of the estimation errors stay below the value r_i when the corresponding observer matches the plant fault situation (which is, thus, correctly identified by the FDI algorithm) and stay above r_i when the corresponding observer does not match the plant fault situation. This behaviour was correctly predicted by the set separation of Fig. 2. Fig. 4 shows the resulting plant and reference states, actual plant input, Fu in (1a) (blue dotted), and nominal control, u_c in (3) (red solid). Notice that the faults have negligible effect on the plant states, which track the desired reference almost perfectly.

VIII. CONCLUSIONS

In this paper we have proposed a new FTC scheme which combines an invariant-set approach to FDI with a virtual actuator approach to controller reconfiguration. The FDI approach is based on the separation of sets that characterise healthy system operation from sets that characterise faulty

Fig. 3. FDI index ℓ and output estimation error norms.

Fig. 4. States and inputs resulting from the simulation.

operation. The derivation of these sets takes into account the reconfiguration of the closed-loop system by means of the virtual actuator under all considered actuator faults. We have provided analytic conditions, in terms of closed-loop system parameters and external signals, which guarantee the aforementioned set separation and, thus, closed-loop stability of the FTC scheme under all considered fault situations.

REFERENCES

- [1] C. Ocampo-Martínez, J. De Doná, and M. Seron, “Actuator fault tolerant control based on set separation,” in *Proceedings 17 IFAC World Congress*, Seoul, Korea, July 2008.
- [2] M. Seron, J. De Doná, and J. Martínez, “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.
- [3] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*, 2nd ed. Springer, 2006.
- [4] T. Steffen, *Control Reconfiguration of Dynamical Systems*. Springer, 2005.
- [5] J. Lunze and T. Steffen, “Control reconfiguration after actuator failures using disturbance decoupling methods,” *IEEE Transactions on Automatic Control*, vol. 51, no. 10, pp. 1590–1601, 2006.
- [6] J. Richter, W. Heemels, N. van de Wouw, and J. Lunze, “Reconfigurable control of piecewise affine systems with actuator and sensor faults,” in *Proceedings of the 47th IEEE Conference on Decision and Control*, Cancun, Mexico, December 2008.
- [7] M. Seron, X. Zhuo, J. De Doná, and J. Martínez, “Multisensor switching control strategy with fault tolerance guarantees,” *Automatica*, vol. 44, no. 1, pp. 88–97, 2008.
- [8] E. Kofman, H. Haimovich, and M. Seron, “A systematic method to obtain ultimate bounds for perturbed systems,” *International Journal of Control*, vol. 80, no. 2, pp. 167–178, 2007.
- [9] S. Olaru, J. De Doná, and M. Seron, “Positive invariant sets for fault tolerant multisensor control schemes,” in *Proceedings 17 IFAC World Congress*, Seoul, Korea, July 2008.