Bank of Virtual Actuators for Fault Tolerant Control

María M. Seron [*,1] **José A. De Doná** [*] **Jan H. Richter** [**]

[*] *Centre for Complex Dynamic Systems and Control (CDSC), School of Electrical Engineering and Computer Science, The University of Newcastle, Callaghan, NSW 2308, Australia*
[**] *Siemens AG, Industry Sector, Gleiwitzer Str. 555 90475 Nuremberg, Germany*

Abstract: We propose an actuator fault tolerant control scheme based on a bank of *virtual actuators* (VA), with the novel feature that the virtual actuators implicitly integrate both fault detection and isolation (FDI) and controller reconfiguration (CR) tasks. The bank of VAs operates in closed-loop with an observer-based tracking controller designed for a nominal (fault free) model of the plant. We consider abrupt actuator faults ranging over a finite cover. Each VA is designed to operate appropriately in combination with the nominal controller to achieve correct CR for a particular fault situation in the considered range. A switching rule that engages the suitable VA from the bank is based on sets defined for measurable residual signals constructed directly from the virtual actuators signals. The overall scheme is shown to guarantee closed-loop boundedness and setpoint tracking under all considered fault situations. The method is applied to an example of aircraft lateral control.

Keywords: Fault tolerant control, fault detection and isolation, controller reconfiguration, virtual actuators, actuator faults, invariant sets.

1. INTRODUCTION

Active fault tolerant control (FTC) systems are concerned with the integration of an FDI system together with a reconfigurable mechanism which decides the best configuration of the system to achieve fault tolerance. An interesting approach to controller reconfiguration based on the concept of *virtual actuators* (VA) has been developed in Steffen (2005); Blanke et al. (2006); Lunze and Steffen (2006); Richter and Lunze (2009); Richter et al. (2011). This approach is highly advantageous since it aims at applying a minimal change in the control loop when faults occur. Thus, the method uses a single nominal controller, designed for the nominal or "fault-free" system, which is always present in the closed-loop system, and a virtual actuator, which takes different actions, according to the evaluated fault situation of the plant, in order to cancel or mitigate the effect of the fault in the closed-loop system. The advantage of this approach is that any existing nominal controller which has been designed, and possibly fine-tuned and tested, 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 VA is independent of the controller and is aimed at preserving specific closed-loop properties under fault, for example, stability and setpoint tracking (Steffen, 2005).

In Seron et al. (2011) we presented an integrated FTC scheme that adapts and combines the above VA approach to controller reconfiguration with a recently proposed set-separation approach to FDI (Seron et al., 2008; Seron and De Doná, 2010; Olaru et al., 2010). The FDI approach is based on the separation of sets that characterise the system operation under different actuator fault situations that can occur in the plant. Analytic conditions in terms of closed-loop system parameters and bounds on external signals can be deduced from the required set separation which, in turn, guarantees closed-loop stability of the scheme under all considered fault situations. The scheme proposed in Seron et al. (2011) utilises *a single VA*, whose mode of operation is adapted to the evaluated fault situation via a supervisory logic guided by the FDI decision. In addition, a *separate bank of observers*, each matching a considered fault situation, is employed by the FDI unit for residual generation.

In the present paper, we continue the line of work that combines the set-separation approach to FDI with the VA approach to controller reconfiguration. We depart from previous approaches, however, by the novel feature of utilising a *bank of virtual actuators* that embody both the FDI and CR tasks, without the need of resorting to additional FDI observers. The resulting scheme is simpler since one less dynamic object is required; that is, if N different fault situations are considered, the current scheme requires N VAs, as opposed to one VA *and* N FDI observers as in our previous approach. A schematic of the proposed FTC scheme is shown in Figure 1. The bank of VAs operates in closed-loop with an observer-based tracking controller designed for a nominal (fault free) model of the plant. Each VA is designed to operate appropriately in combination with the nominal controller to achieve correct CR for a particular fault situation in a finite range of considered

[1] Corresponding author. Email: maria.seron@newcastle.edu.au

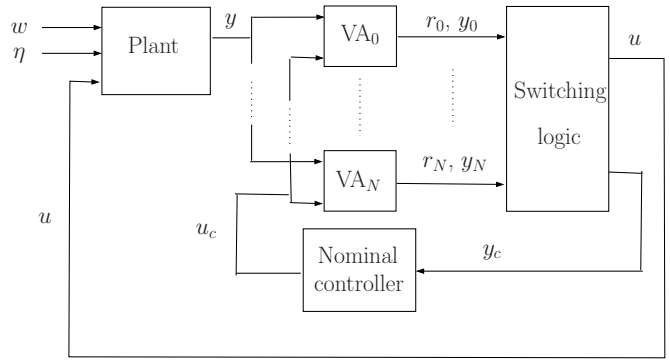

Fig. 1. Proposed FTC scheme.

scenarios. In addition, to each VA we associate a suitable residual signal with distinctive dynamic behaviours both when its model "matches" the actual plant fault situation and when changes to a "non-matching" fault situation occur. A switching logic monitors these residual signals to determine which VA matches the current fault situation and should be engaged in the loop. The analysis of the residual dynamics yields conditions, expressed as the separation of sets that characterise matching and non-matching operation, which ensure correct FDI and appropriate CR within the considered fault range. The derived conditions thus guarantee the preservation of closed-loop boundedness and setpoint tracking under all considered fault situations. The scheme is applied to an example of lateral lateral control of a Boeing 747 aircraft.

2. PLANT AND NOMINAL CONTROLLER

In this section we describe the models used for the plant and actuator faults and further analyse the closed-loop system properties under nominal conditions.

The plant is given by the linear discrete-time model [2]

$$x^+ = Ax + BFu + Ew, \tag{1a}$$
$$y = Cx + \eta, \tag{1b}$$
$$v = C_v x, \tag{1c}$$

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, $v \in \mathbb{R}^q$ is a performance output and $\eta \in \mathbb{R}^p$ is a bounded measurement disturbance. Actuator faults are modelled by changes of the matrix $F \in \mathbb{R}^{m\times m}$ in (1a). Indeed, we consider that F can take values over the finite cover:

$$F \in \{F_0, F_1, \ldots, F_N\}. \tag{2}$$

In particular, $F_0 = I$ (the identity matrix) represents the "nominal" case, that is, no actuator fault. Typically, one would include in (2) those fault situations that are considered more critical for the process performance such as, for example, total outage of actuators. We will say that an (abrupt) change in the actuator fault situation occurs if F changes from $F = F_i$ to $F = F_j$, $i, j \in \{0, \ldots, N\}$, $j \neq i$, at some time $k_F \geq 0$.

[2] The dependence of variables on discrete time k will be omitted when clear from the context.

We assume that the pair (A, C) is detectable and the pairs (A, BF_i), for $i = 0, 1, \ldots, N$ are stabilisable. In addition, the pairs $\left(\begin{bmatrix} A & 0 \\ C_v & I \end{bmatrix}, \begin{bmatrix} BF_i \\ 0 \end{bmatrix}\right)$ are stabilisable, for $i = 0, 1, \ldots, N$. (This is required to achieve constant setpoint tracking under all considered fault situations.)

We will further assume that the process disturbance and the measurement noise satisfy $w(k) \in \mathcal{W}$ and $\eta(k) \in \mathcal{N}$ for all time instants $k \geq 0$, where the bounding sets are defined as [3] $\mathcal{W} \triangleq \{w \in \mathbb{R}^r : |w| \leq \overline{w}\}$ and $\mathcal{N} \triangleq \{\eta \in \mathbb{R}^p : |\eta| \leq \overline{\eta}\}$ for some nonnegative vectors $\overline{w} \in \mathbb{R}^r$ and $\overline{\eta} \in \mathbb{R}^p$.

We consider the following, observer-based, reference tracking controller:

$$u_c = -K(\hat{x} - x_{\rm ref}) + u_{\rm ref}, \tag{3}$$
$$\hat{x}^+ = A\hat{x} + Bu_c + L(y_c - C\hat{x}), \tag{4}$$
$$x^+_{\rm ref} = A\, x_{\rm ref} + Bu_{\rm ref}, \tag{5}$$

where, under nominal conditions, $u_c = u$, $y_c = y$ (u, y are the signals in the plant (1)). More generally, u, u_c, y and y_c are related through the virtual actuator selected by the switching logic (cf. (6)–(8)).

The observer gain L and the feedback gain K in the nominal observer-based controller (3)–(5) are designed such that $A - LC$ and $A - BK$ are Schur matrices. (This can readily be satisfied by the detectability and stabilisability assumptions made above.)

Remark 2.1. (Reference System). The reference system (5) generates a trajectory $(u_{\rm ref}, x_{\rm ref})$ that is solution of the nominal model. These trajectories are designed such that they are bounded and the output $C_v x_{\rm ref}$, where C_v is the plant performance output matrix in (1c), asymptotically tracks a bounded external signal v^*, that is, such that $\lim_{k\to\infty}[\, C_v x_{\rm ref}(k) - v^*(k)\,] = 0$. 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. Note that this imposes the condition that v cannot have more independent elements than the number of available independent inputs under all possible fault situations (given by the minimum of $\mathrm{rank}(BF_i)$, $i = 0, \ldots, N$). Given the designed reference system, it is straightforward to obtain constant vectors $u^0_{\rm ref} \in \mathbb{R}^m$ and $\overline{u_{\rm ref}} \in \mathbb{R}^m$ such that $u_{\rm ref}(k) \in \mathcal{U}_{\rm ref} = \{u \in \mathbb{R}^m : |u - u^0_{\rm ref}| \leq \overline{u_{\rm ref}}\}$ for all $k \geq 0$. The offset $u^0_{\rm ref}$, in particular, is related to the offset (or DC component) of the reference signal v^*. ∘

3. BANK OF VIRTUAL ACTUATORS

We will consider virtual actuators with integral action (see Steffen (2005), Section 9.4, for the continuous-time version). Each VA in the bank is described by the following equations associated with each actuator fault matrix F_i, for $i = 0, \ldots, N$, considered in (2) (with $F_0 = I$):

$$\begin{bmatrix} \theta_i^+ \\ \sigma_i^+ \end{bmatrix} = \begin{bmatrix} A & 0 \\ t_s C_v & I \end{bmatrix} \begin{bmatrix} \theta_i \\ \sigma_i \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} u_c - \begin{bmatrix} B \\ 0 \end{bmatrix} F_i u_i, \tag{6}$$
$$u_i = -M_i \begin{bmatrix} \theta_i \\ \sigma_i \end{bmatrix} + N_i u_c + d_i, \tag{7}$$
$$y_i = y + C\theta_i, \tag{8}$$

[3] Inequalities and absolute values are taken elementwise.

where $\theta_i \in \mathbb{R}^n$ is the VA state; $\sigma_i \in \mathbb{R}^q$ is the integral action state; t_s is a positive scalar; the matrices M_0 and N_0 in (7) satisfy (in order to recover the nominal control action for $i = 0$)

$$M_0 = 0, \qquad N_0 = I; \tag{9}$$

the matrices $M_i = [M_{i,\theta}\ M_{i,\sigma}]$ in (7) are such that the closed-loop matrices

$$A_i \triangleq \begin{bmatrix} A & 0 \\ t_s C_v & I \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} F_i M_i = \begin{bmatrix} A + BF_iM_{i,\theta} & BF_iM_{i,\sigma} \\ t_sC_v & I \end{bmatrix} \tag{10}$$

are Schur, for $i \in \{1, \ldots, N\}$ (this is always possible due to the stabilisability condition assumed in Section 2); the matrices N_i in (7), for $i = 1, \ldots, N$, are arbitrary matrices, which can be used to satisfy some desired design specifications; the signals d_i in (7) are constant vectors that represent degrees of freedom in the design and satisfy

$$d_i \in \ker(BF_i) \quad \text{for } i \in \{0, 1, \ldots, N\}, \tag{11}$$

where 'ker' denotes null space; and the remaining signals and matrices are as in the plant and nominal controller equations (1)–(5). Note for future use that, from (6), (7), and using (10)–(11), the dynamics of each VA satisfy

$$\begin{bmatrix} \theta_i^+ \\ \sigma_i^+ \end{bmatrix} = A_i \begin{bmatrix} \theta_i \\ \sigma_i \end{bmatrix} + \begin{bmatrix} B \\ 0 \end{bmatrix} (I - F_iN_i)u_c. \tag{12}$$

The signals u_i and y_i in (7)–(8) are fed back into the closed-loop system whenever the switching logic's decision is to engage the ith VA according to the evaluated fault situation; in particular $u = u_i$ is fed to the plant and $y_c = y_i$ is fed to the nominal controller (see Figure 1). In addition, whenever the switching logic selects the VA with index $i = 0$, denoted as VA_0, the following "initial-condition resetting" takes place in the VA_0 dynamics:

$$\begin{bmatrix} \theta_0(k_0) \\ \sigma_0(k_0) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ at each time } k_0 \text{ when } \text{VA}_0 \text{ is selected.} \tag{13}$$

Note that (13) ensures the deactivation of the VA associated with the nominal condition $F = F_0$ when the switching logic selects this VA; indeed, together with $M_0 = 0$ and $N_0 = I$, the resetting implies that $u = u_0 = u_c + d_0$ (with $BF_0d_0 = Bd_0 = 0$) and thus the nominal control law is engaged for the plant (1a) under nominal conditions.

Fault hiding goal. An important property of the VA is to "hide" faults from the nominal controller, that is, to restore the controller signals u_c and y_c to their nominal trajectories (Steffen, 2005). To see this, we define the combined state variables

$$\xi_i \triangleq x + \theta_i, \quad i = 0, \ldots, N. \tag{14}$$

Using (1) and (6) we have

$$\xi_i^+ = A\xi_i + B(Fu - F_iu_i) + Bu_c + Ew. \tag{15}$$

When $F_i = F$ (that is, the ith VA "matches" the plant fault situation) and $u = u_i$, $y_c = y_i$ (that is, the ith VA is selected by the switching logic and its associated signals fed back in the closed-loop system, see Figure 1), and using (1b), (7), (8) and (11), we have that (14) satisfies

$$\xi_i^+ = A\xi_i + Bu_c + Ew. \tag{16}$$

$$y_c = C\xi_i + \eta. \tag{17}$$

Note that the above system coincides with the nominal plant dynamics ($F = I$) with input u_c and output y_c (see (1)). 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, the fault hiding objective is achieved.

In Section 5, we will show that engaging the ith VA in the closed-loop system when the plant's fault matrix F in (1a) is $F = F_i$, correctly reconfigures the controller achieving closed-loop stability and setpoint tracking (see Lemma 5.1). In the following section we explain the additional use of the bank of virtual actuators for residual generation and fault diagnosis.

4. RESIDUAL GENERATION AND FDI PRINCIPLE

We propose to use as residual associated with the ith VA the measurable quantity

$$r_i \triangleq y_i - C\hat{x}, \tag{18}$$

where y_i is the output (8) provided by VA_i and $\hat{x}$ is the state of the nominal observer (4).

To analyse the behaviour of the above residual signals we will introduce the following error variables, for $i = 0, \ldots, N$:

$$\tilde{\xi}_i \triangleq \xi_i - \hat{x}, \tag{19}$$

$$\zeta_i \triangleq \xi_i - x_{\text{ref}}, \tag{20}$$

where ξ_i is as defined in (14). Using (8), (1b), (14) and (19) it follows that the residual (18) can be expressed as

$$r_i = C\tilde{\xi}_i + \eta. \tag{21}$$

Using (15), (17) and (3)–(5), and further noting from (19)–(20) that the nominal control law (3) can be equivalently expressed as

$$u_c = -K\zeta_i + K\tilde{\xi}_i + u_{\text{ref}}, \tag{22}$$

for any $i \in \{0, \ldots, N\}$, we obtain

$$\tilde{\xi}_i^+ = A\tilde{\xi}_i + B(Fu - F_iu_i) + Ew - L(y_c - C\hat{x}), \tag{23}$$

$$\zeta_i^+ = (A - BK)\zeta_i + B(Fu - F_iu_i) + BK\tilde{\xi}_i + Ew. \tag{24}$$

Working hypothesis and matching sets. We will next consider that $F_i = F$ (that is, the ith VA "matches" the plant fault situation) and make the *working hypothesis* that the FDI logic makes the correct decision and sets $u = u_i$, $y_c = y_i$; that is, the ith VA is selected by the switching logic and its associated signals fed back in the closed-loop system, see Figure 1 (in Section 5 we will provide the required elements which ensure that the working hypothesis is in fact satisfied, see Theorem 5.3). We then have, using (17), (19), that (23)–(24) become

$$\tilde{\xi}_i^+ = (A - LC)\tilde{\xi}_i + Ew - L\eta, \tag{25}$$

$$\zeta_i^+ = (A - BK)\zeta_i + BK\tilde{\xi}_i + Ew. \tag{26}$$

Since $A - LC$ and $A - BK$ are Schur matrices by design and the external disturbance signals w and η are bounded, then the trajectories of the above system are bounded. Moreover, using the bounding sets $\mathcal{W}$ and $\mathcal{N}$ for the disturbances introduced in Section 2, we can compute attractive invariant sets [4] $\tilde{\Xi}$ and $\mathcal{Z}$ associated with system (25)–

[4] These sets are such that their associated dynamics are attracted to the set if started outside and remain in the set if started inside. Several methods can be used for their computation; in this paper we use the procedures of Kofman et al. (2007); Olaru et al. (2010).

(26). We compute these sets so that they are "centred" at zero (which is possible since the same is true for the disturbance bounding sets). Note also from (22), and using $\tilde{\Xi}$ and $\mathcal{Z}$, that the nominal controller output satisfies the set membership ($\oplus$ denotes Minkowski sum)

$$u_c \in \mathcal{U}_c \triangleq -K\mathcal{Z} \oplus K\tilde{\Xi} \oplus \mathcal{U}_{\text{ref}}, \tag{27}$$

(where $\mathcal{U}_{\text{ref}}$ is defined in Remark 2.1) whenever $\tilde{\xi}_i \in \tilde{\Xi}$ and $\zeta_i \in \mathcal{Z}$. The set $\mathcal{U}_c$ is centred at the reference offset u^0_{ref}, which is the centre of $\mathcal{U}_{\text{ref}}$ (see Remark 2.1).

For each VA, in particular the matching VA, we can use its associated dynamics (12) and the fact that A_i is Schur and u_c is bounded as in (27) to compute an attractive invariant set which will retain its states (θ_i, σ_i) whenever u_c remains in $\mathcal{U}_c$. Let us denote this set $\mathcal{S}_i$ and observe that it is centred at

$$c_i \triangleq (I - A_i)^{-1} \begin{bmatrix} B \\ 0 \end{bmatrix} (I - F_i N_i) u^0_{\text{ref}}. \tag{28}$$

Note then that, whenever $(\theta_i, \sigma_i) \in \mathcal{S}_i$ and $u_c \in \mathcal{U}_c$, the control output (7) associated with VA_i satisfies

$$u_i \in \mathcal{U}_i \triangleq -M_i\mathcal{S}_i \oplus N_i\mathcal{U}_c \oplus \{d_i\}. \tag{29}$$

In view of (21) we then have that, under the working hypothesis that the matching VA ($F_i = F$) is selected by the switching logic and its associated signals fed back in the closed-loop system ($u = u_i$, $y_c = y_i$), and whenever $\xi_i \in \tilde{\Xi}$, the residual signal associated with the matching VA satisfies

$$r_i \in \mathcal{R}, \quad \text{where } \mathcal{R} \triangleq C\tilde{\Xi} \oplus \mathcal{N}. \tag{30}$$

We observe that the set $\mathcal{R}$ is centred at zero since $\tilde{\Xi}$ and $\mathcal{N}$ are centred at zero.

After-change sets and FDI logic. Suppose next that a change in the plant fault situation occurs so that the system matrix F in (1a) changes from $F = F_i$ to $F = F_j$, for some $j \in \{0, 1, \ldots, N\}$, $j \neq i$. Using (23) and noting that u is still equal to u_i and y_c is still equal to y_i since no reconfiguration has been made yet, we have that the "after-change" residual signal of the previously matching VA_i satisfies

$$r^+_{ij} \in \mathcal{R}^+_{ij}, \quad \text{where } \mathcal{R}^+_{ij} \triangleq C[(A - LC)\tilde{\Xi} \oplus B(F_j - F_i)\mathcal{U}_i \oplus E\mathcal{W} \oplus (-L)\mathcal{N}] \oplus \mathcal{N}, \tag{31}$$

whenever $\xi_i \in \tilde{\Xi}$ and $u_i \in \mathcal{U}_i$. Notice that the second summand in the definition of the set $\mathcal{R}^+_{ij}$ in (31), $CB(F_j - F_i)\mathcal{U}_i$, determines a shift of this set away from zero enabled by the difference $F_j - F_i$. Indeed, if follows from (27)–(29) that this shift depends on both the reference offset u^0_{ref} and the degree of freedom signals d_i. Thus, both u^0_{ref} and d_i are mechanisms that can be utilised to "separate" the matching and after-change sets to achieve fault detection and discernibility. In view of this observation, we will impose the following condition.

Assumption 4.1. (Set Separation). For each $i \in \{0, ..., N\}$, the matching set $\mathcal{R}$ and the after-change sets $\mathcal{R}^+_{ij}$, for $j = 0, \ldots, N$, $j \neq i$, are all disjoint. ∘

We also specify the fault scenario for which correct FDI can be achieved.

Assumption 4.2. (Fault Scenario). Between the occurrence of any two consecutive changes in the fault matrix F, sufficient time [5] elapses such that the after-fault system states converge to their respective invariant sets. ∘

Under the above assumptions, a simple FDI mechanism can be devised by monitoring the matching VA and testing whether its associated residual r_i satisfies (30) (in which case no change has occurred) or satisfies (31) for some $j \in \{0, \ldots, N\}$, $j \neq \ell$ (in which case a change with fault matrix F_j has occurred). In the case of detecting a change, the algorithm needs to wait enough time before making another test so that the after-change system states converge to their respective invariant sets. Let us denote this time T and observe that it can be estimated as mentioned in footnote 5. We thus propose the following algorithm.

Algorithm 4.3. (FDI and CR logic).

(1) For the matching VA_i evaluate its associated residual signal r_i as in (18).
(2) If $r_i \in \mathcal{R}$ [c.f. (30)] go to step 1; if $r_i \in \mathcal{R}^+_{ij}$ for some $j \in \{0, 1, \ldots, N\}$, $j \neq i$ [c.f. (31)], then engage VA_j in the loop by setting $u = u_j$ and $y_c = y_j$.
(3) Wait T time steps before performing any action.
(4) Go to step 1.

In the following section we establish the closed-loop properties of the overall FTC scheme based on Algorithm 4.3.

5. CLOSED-LOOP PROPERTIES

We begin by showing the stability and tracking properties of the closed-loop system under matching conditions.

Lemma 5.1. (Matching Properties). Suppose that $F = F_i$ in (1a) and let $u = u_i$, $y_c = y_i$, that is, the matching ith VA is engaged in the closed-loop system of Figure 1, thus consisting of the plant (1), nominal controller (3)–(5) and VA_i (6)–(8). Then: (i) All closed-loop system variables are bounded; (ii) If the external disturbance signals w and η are zero and the reference input signal u_{ref} is constant and designed as explained in Remark 2.1, the performance variable v defined in (1c) asymptotically converges to the desired setpoint v^*, for constant v^*.

Proof. (i) If $F = F_i$ in (1a) and $u = u_i$, $y_c = y_i$, we have that the VA error variables (19), (20) satisfy (25)–(26) and are therefore bounded as discussed in Section 4. Thus, we have from (20) that, since x_{ref} is bounded, then ξ_i is bounded. Since ξ_i is bounded, it follows from (19) that $\hat{x}$ is bounded. Finally, since θ_i is bounded (in fact, all VAs have bounded states, see (12), (22) and recall that A_i in (10) are Schur matrices), we have from (14) that x is bounded. That is, all internal variables in the closed-loop system remain bounded, thus proving the first part.

(ii) When the external signals w and η are zero, it follows from (25)–(26) and the fact that $A - LC$ and $A - BK$ are Schur matrices by design, that $u_c = u_{\text{ref}}$ in steady state. Thus, if u_{ref} is constant, and since the matrix A_i defined in (10) is Schur, then the virtual actuator (6)–(7) [equivalently, (12)] reaches a constant

[5] This "convergence time" can be estimated using standard set theoretic techniques, see, e.g., Seron and De Doná (2010).

equilibrium point. In particular, the integral action state in steady state satisfies $\sigma_i^+ = \sigma_i$, which yields $C_v\theta_i = 0$. Combining this information with (1c) and (14) we obtain $v = C_v x = C_v(\xi_i - \theta_i) = C_v\xi_i$. Moreover, since in the absence of disturbances, we have from (20), (26) that ξ_i converges to $x_{\rm ref}$ in steady state, then v converges to $C_v x_{\rm ref}$ in steady state. Finally, together with the property $\lim_{k\to\infty}[\,C_v x_{\rm ref}(k) - v^*\,] = 0$ of Remark 2.1, we have that v converges to v^* in steady state, as claimed. □

Next, we establish the fault tolerant properties of the overall scheme. We require an initialisation assumption. [6]

Assumption 5.2. (Initial Conditions). Before the first change in the plant fault situation, the matching VA$_i$ (that is, $F_i = F$ in (1a) and (6), $u = u_i$ and $y_c = y_i$) is engaged in the closed-loop system, and the error variables of all VAs $\tilde{\xi}_j$ and ζ_j, for $j = 0, \ldots, N$, defined in (19) and (20) are in their attractive invariant sets $\tilde{\Xi}$ and $\mathcal{Z}$, respectively. In addition, the VA states (θ_j, σ_j), for $j = 0, \ldots, N$, are in the attractive invariant sets $\mathcal{S}_j$. ∘

Theorem 5.3. (Fault Tolerance). Suppose that Assumption 5.2 holds. Then, under the set separation condition of Assumption 4.1 and the fault scenario of Assumption 4.2, the states of the closed-loop system represented in Figure 1, encompassing the plant (1)–(2), the nominal tracking controller (3)–(5) and the bank of virtual actuators (6)–(8), reconfigured by Algorithm 4.3, are bounded. Moreover, in the absence of disturbances and for constant reference $u_{\rm ref}$, the variable v defined in (1c) converges, in steady state, to a neighbourhood of the reference signal v^* defined in Remark 2.1, when v^* is constant.

Proof. By Assumption 5.2, before any change in the plant fault situation the matching VA$_i$ (that is, $F_i = F$, $u = u_i$ and $y_c = y_i$) is engaged in the closed-loop system and thus all closed-loop system states are bounded, as shown in Lemma 5.1-(i). Moreover, also by Assumption 5.2 all relevant variables are in their respective invariant sets and hence the analysis of Section 4 following the *working hypothesis* is validated. In particular, the residual r_i associated with the matching VA satisfies (30) and it is thus sensitive to any subsequent change in the plant fault situation, which will cause r_i to satisfy (31) one time step after the change occurs. Hence, Assumption 4.1 ensures that Algorithm 4.3 makes the correct decision and controller reconfiguration and, due to the waiting timer of its third step and the fault scenario of Assumption 4.2, the initialisation conditions of Assumption 5.2 are recovered after at most T time steps. The same arguments can then be applied for any subsequent change in the fault situation, concluding that the closed-loop system states remain bounded at all times. To prove the setpoint tracking result, note that in the absence of disturbances and for constant $u_{\rm ref}$, the result of Lemma 5.1-(ii) holds in the intervals when the plant fault situation and Algorithm 4.3's decision remain unchanged. However, since the stated convergence is asymptotic, and each change in the fault situation causes a transient that perturbs this convergence, only "practical" convergence of the variable v to a neighbourhood of the reference signal v^* can be guaranteed in the presence of persistent fault changes. The result then follows. □

[6] This assumption will hold if the system has evolved with the matching VA engaged in the loop for sufficiently long time before any change of the fault situation occurs. This is a reasonable assumption since the system will typically start operating under perfectly known actuator conditions.

6. EXAMPLE

We consider the linearised lateral dynamic model of a Boeing 747 airplane with three additional rudder actuation vectors, as proposed in Chen et al. (2002) for the study of actuator fault diagnosis and compensation. Using data from Franklin et al. (2002), in horizontal flight at 40000 ft and nominal forward speed 774 ft/s (Mach 0.8), the aircraft lateral perturbation dynamics, discretised with a sampling period $t_s = 0.1$s, can be represented by a model of the form (1a) with matrices

$$A = \begin{bmatrix} 0.9902 & -0.0985 & 0.0082 & 0.0041 \\ 0.0597 & 0.9855 & -0.0028 & 0.0001 \\ -0.2956 & 0.0525 & 0.9533 & -0.0006 \\ -0.0147 & 0.0104 & 0.0977 & 1.0000 \end{bmatrix},$$

$$B = \begin{bmatrix} 0.0031 & 0.0061 & 0.0051 & 0.0035 \\ -0.0470 & -0.0794 & -0.0695 & -0.0497 \\ 0.0137 & 0.0290 & 0.0235 & 0.0162 \\ 0.0005 & 0.0012 & 0.0009 & 0.0006 \end{bmatrix}.$$

We further take $E^T = -\,[0.0021\ 0\ -0.0002\ 1] \cdot 10^{-3}$ as the input matrix of an additive disturbance w, assumed bounded as $|w| \le 10^{-3}$. The state vector is given by $x = [\beta\ \rho\ \pi\ \psi]^T$, where β is the side-slip angle in radians, ρ is the yaw rate in rad/s, π is the roll rate in rad/s, ψ is the roll angle in radians, and $u = [u_1\ u_2\ u_3\ u_4]^T$ contains four control signals representing four rudder servos (Chen et al., 2002). We consider the fault matrix $F \in \{F_0, \ldots, F_4\}$ with

$$F_0 = I, \quad F_i = \mathrm{diag}(1, \ldots, \overset{i}{\underset{\downarrow}{0}}, \ldots, 1), \quad i = 1, \ldots, 4, \quad (32)$$

that is, total outage of each actuator.

As in Franklin et al. (2002) we consider yaw rate ρ as the measured output (note that Chen et al. (2002) assumes full state measurement); thus the output matrix in (1b) is $C = [0\ 1\ 0\ 0]$ and we further assume that the measurement noise satisfies $|\eta| \le 10^{-5}$. We take $C_v = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$ in (1c), that is, we are interested in both yaw rate (ρ) and side-slip angle (β) as performance variables.

The tracking controller (3)–(5) employs the feedback and observer gains

$$K = \begin{bmatrix} -0.0071 & -0.3211 & 0.0020 & -0.0010 \\ -0.0092 & -0.5432 & 0.0041 & -0.0013 \\ -0.0090 & -0.4753 & 0.0033 & -0.0013 \\ -0.0067 & -0.3395 & 0.0023 & -0.0010 \end{bmatrix},\ L = \begin{bmatrix} -0.1141 \\ 0.0691 \\ -0.0786 \\ -0.3811 \end{bmatrix}.$$

The reference signal (5) is computed for the constant setpoint $v^* = [\rho^*\ \ \beta^*]' = [0.005\ \ 0]'$, and is bounded as stated in Remark 2.1 with

$$u_{\rm ref}^0 = [0.0435\ -0.0375\ 0.0035\ 0.0129]', \qquad \overline{u_{\rm ref}} = 0.$$

The virtual actuator matrices M_i, for $i = 0, \ldots, 4$, in (7) are computed via LQR with weighting matrices $Q = [C_v\ \ 10I]'\,[C_v\ \ 10I]$, $R = I$. We further take $N_i = 0$, for $i = 0, \ldots, 4$, in (7). The "degree of freedom" signals $d_0, \ldots, d_4$ in (7), are selected such that (11) holds.

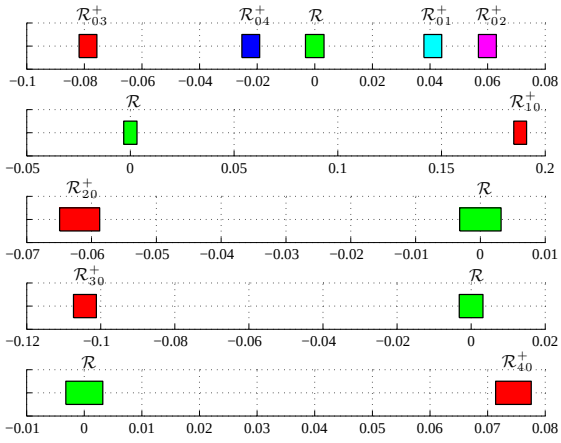

Fig. 2. Matching and after-change sets for the residuals r_0, ..., r_4, from top to bottom. (All sets are line segments, the vertical width was added for illustration purposes.)

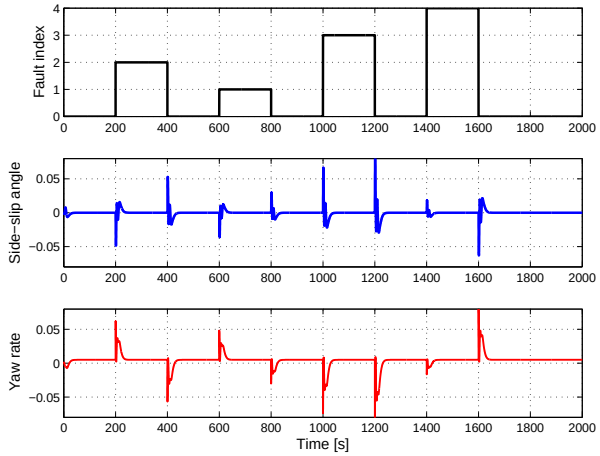

Fig. 3. Fault index and performance variables.

For illustration purposes and to simplify the exposition we will only consider the following changes in the actuator fault situation (although the scheme functions satisfactority in more general situations): from the "healthy" condition $F_0 = I$, any of the faulty situations F_1 to F_4 can occur; on the other hand, from a faulty situation, only recovery of the healthy situation can occur, that is, no change from one faulty situation to another can occur without first recovering the healthy situation. The top plot of Figure 2 shows the matching set $\mathcal{R}$ and the after-change sets $\mathcal{R}^+_{0j}$ associated with VA_0, where $j = 1, \ldots, 4$ corresponds to a change from $F = F_0$ to $F = F_1, \ldots, F_4$. The second to fifth plots of Figure 2 show the matching set $\mathcal{R}$ and the after-change set $\mathcal{R}^+_{i0}$ associated with VA_i, for $i = 1, \ldots, 4$, corresponding, respectively, to the matching situation for this VA and to a change in the plant fault situation from $F = F_i$ to $F = F_0$. Note that all sets are separated for each VA and thus Assumption 4.1 holds for the changes in fault situation analysed.

We simulated the FTC scheme under the fault scenario given in the top plot of Figure 3, where the plotted value corresponds to the subindex j of the actual value of the matrix $F = F_j$ at each time. The FDI Algorithm 4.3 correctly diagnosed the fault situation one step after each change and reconfigured the controller accordingly. The second and third plots of Figure 3 show the resulting evolution of the performance variables (side-slip angle and yaw rate). Note that each change in fault situation causes a transient that rapidly decays towards the desired setpoint values of 0 and 0.005, respectively.

7. CONCLUSIONS

We have proposed an actuator fault tolerant control scheme based on a bank of virtual actuators, with the novel feature that the virtual actuators implicitly integrate both fault detection and isolation and controller reconfiguration tasks. We consider abrupt actuator faults ranging over a finite cover. Each VA is designed to operate appropriately in combination with a nominal controller to achieve correct reconfiguration for a particular fault situation of the cover. We have proposed a switching rule that engages the suitable VA from the bank and is based on sets defined for residual signals constructed *directly* from the virtual actuators signals. We have shown that the overall scheme guarantees closed-loop boundedness and setpoint tracking under all considered fault situations. The method was applied to an example of aircraft lateral control.

REFERENCES

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2006). *Diagnosis and Fault-Tolerant Control*. Springer, 2nd edition.

Chen, S., Tao, G., and Joshi, S.M. (2002). On matching conditions for adaptive state tracking control of systems with actuator failures. *IEEE Trans. on Automatic Control*, 47(3), 473–478.

Franklin, G., Powell, J.D., and Emami-Naeini, A. (2002). *Feedback Control of Dynamic Systems*. Prentice Hall, Upper Saddle River, New Jersey, fourth edition.

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

Lunze, J. and Steffen, T. (2006). Control reconfiguration after actuator failures using disturbance decoupling methods. *IEEE Trans. on Automatic Control*, 51(10), 1590–1601.

Olaru, S., De Doná, J.A., Seron, M.M., and Stoican, F. (2010). Positive invariant sets for fault tolerant multisensor control schemes. *International Journal of Control*, 83(12), 2622–2640.

Richter, J.H., Heemels, W.P.M.H., van de Wouw, N., and Lunze, J. (2011). Reconfigurable control of piecewise affine systems with actuator and sensor faults: stability and tracking. *Automatica*, 47(4), 678–691.

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. and De Doná, J. (2010). Actuator fault tolerant multi-controller scheme using set separation based diagnosis. *International Journal of Control*, 83(11), 2328–2339.

Seron, M.M., De Doná, J.A., and Richter, J.H. (2011). Fault tolerant control using virtual actuators and set-separation detection principles. *International Journal of Robust and Nonlinear Control*. To appear.

Seron, M.M., Zhuo, X.W., De Doná, J.A., and Martínez, J.J. (2008). Multisensor switching control strategy with fault tolerance guarantees. *Automatica*, 44(1), 88–97.

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