INTERNATIONAL JOURNAL OF ADAPTIVE CONTROL AND SIGNAL PROCESSING
Int. J. Adapt. Control Signal Process. 0000; **00**:1–18
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/acs

Integration of invariant-set-based FDI with varying sampling rate virtual actuator and controller*

Esteban N. Osella[1], Hernan Haimovich[1], and María M. Seron[2]

[1]*CIFASIS-CONICET and Departamento de Control, Esc. de Ing. Electrónica, FCEIA, Universidad Nacional de Rosario, Argentina.* {osella.esteban,h.haimovich}@gmail.com
[2] *Centre for Complex Dynamic Systems and Control, The University of Newcastle, Australia.* maria.seron@newcastle.edu.au
**This work was partially supported by grant PICT 2010-0783, FONCYT-ANPCYT, Argentina.*

SUMMARY

We present a new output feedback fault tolerant control strategy for continuous-time linear systems with bounded disturbances. The strategy combines a digital nominal controller under controller-driven (varying) sampling with virtual-actuator (VA)-based controller reconfiguration to compensate for abupt actuator faults, and invariant-set-based fault detection and isolation (FDI). Two independent objectives are considered: (a) closed-loop stability with setpoint tracking and (b) controller reconfiguration under faults. Our main contribution is to extend an existing FDI and VA-based controller reconfiguration strategy to systems under controller-driven sampling in such a way that if objective (a) is possible under controller-driven sampling (without VA) and objective (b) is possible under uniform sampling (without controller-driven sampling), then closed-loop stability and setpoint tracking will be preserved under both healthy and faulty operation for any possible sampling rate evolution that may be selected by the controller. Copyright © 0000 John Wiley & Sons, Ltd.

Received ...

KEY WORDS: Fault-tolerant control, invariant sets, controller-driven sampling, switched systems, networked control.

1. INTRODUCTION

Active Fault-Tolerant Control (FTC) systems aim to maintain control performance levels under a number of fault scenarios by means of a controller reconfiguration mechanism. The main advantage of the virtual actuator (VA) approach to controller reconfiguration for FTC [31, 18, 25], is that it allows the engineer to design the controller for the nominal (*"healthy"*) plant, ignoring the possible faults. In healthy operation, the incidence of the VA on the control signal provided to the plant is null, and the whole control action is provided by the nominal controller. In faulty operation, the VA generates additional signals that combine with the existing signals in specific ways in order to cancel or mitigate the effect of the fault in the closed-loop system. Any existing nominal controller, designed to satisfy the desired specifications for the fault-free plant, can be kept in the loop at all times. In addition, the VA design is independent of the nominal controller and is aimed at preserving specific closed-loop properties, such as stability and setpoint tracking, in the presence of faults.

A specific configuration of VA-based FTC technique was proposed in [27], where the use of a bank of VAs that implicitly integrate both fault detection and isolation (FDI) and controller reconfiguration tasks was proposed. Each VA is designed to operate appropriately in combination with the nominal controller to achieve correct reconfiguration for a particular fault situation in a considered range. In addition, a residual signal is constructed for each VA directly from its available measurable signals. A switching rule engages the suitable VA from the bank according to an FDI decision based on sets defined for the residual signals. This set-based approach for FDI (see, e.g., [28, 29]) relies on the principle that each residual signal will belong to an invariant "correct-matching" set when the associated VA model "matches" the actual actuator fault situation and will shift to a "fault-transition-matching" set when a change to a "non-matching" fault situation occurs. An important advantage of this invariant-set approach to FDI is that fault tolerance and closed-loop stability can be guaranteed when the relevant sets have no intersection.

In the present paper we extend the approach of [27] to continuous-time linear systems operating under a controller-driven (varying) sampling setting, where both the nominal controller and the bank of VAs operate under a varying sampling rate administered by the controller. The motivation for considering this class of systems stems from the increasing popularity of Networked Control Systems (NCS) [1, 2], which broadly refers to control systems that include some kind of shared communications network. In this setting, acceptable control performance and communication bandwidth preservation may be conflicting objectives: increasing control performance by sampling at a higher rate may require too much bandwidth and prevent other processes from accessing the network. Thus, research effort has been directed at control strategies able to modify the sampling rate on-line, according to time-dependent performance and bandwidth requirements (see [11] for further details). As opposed to the general NCS setting where the different component elements (sensors, actuators, controllers) may operate asynchronously, we consider a setting with a centralised controller, with synchronous operation, and where the centralised controller is in charge of not only computing control actions but also deciding on the appropriate sampling rate by selecting, at each sampling instant, when it will take the next sample and control action. This controller-driven sampling setting is akin to that presented in [4].

When a continuous-time system is controlled by means of controller-driven sampling as described above, it can be regarded as a Discrete-Time Switched System (DTSS). Such DTSS is a kind of hybrid system composed by a set of discrete-time subsystems and a switching logic that orchestrates the switching between such subsystems. Indeed, viewed from the controller, the continuous-time system can be interpreted as a DTSS under arbitrary switching, where each discrete-time equivalent of the continuous-time system sampled at some of the possible sampling periods represents a subsystem, and the sampling period sequence represents the switching law. For a general DTSS under arbitrary switching, stability is ensured provided there exists a common Lyapunov function (see [16]). This common Lyapunov function may be of a more complex form than quadratic. However, the search for a common quadratic Lyapunov function can be approached via different techniques, involving in most of the cases the use of Linear Matrix Inequalities (LMIs) [6, 15]. Alternatively, the existence of such a Lyapunov function can be ensured using some matrix-structure-related conditions, associated with the solvability of the Lie algebra generated by the DTSS matrices [7, 32, 20, 16]. An advantage of using the latter conditions is that invariant sets for the DTSS can be computed using a simple formula, as shown in [13, 14].

In this context, the main contribution of the present paper is to adapt and extend the VA-based FTC technique of [27] to the aforementioned controller-driven sampling setting, using a DTSS approach. This extension is non trivial and requires a new design method for the VA parameters to achieve the desired goals in this DTSS framework. Two independent objectives are considered: (a) closed-loop stability with setpoint tracking and (b) controller reconfiguration under faults. Our proposed design is such that if objective (a) is possible under controller-driven sampling (without VA) and objective (b) is possible under uniform sampling (without controller-driven sampling), then closed-loop stability and setpoint tracking will be preserved under both healthy and faulty operation for any possible sampling rate evolution that may be selected by the controller.

The proposed FTC scheme with controller-driven sampling is illustrated in Figure 1. This FTC scheme involves three main parts: a controller-driven sampling system, which computes the control action and decides the next sampling instant (which will be used for sampling and hold and informed to the FDI mechanism); a bank of VAs, each of which is designed for a specific fault situation; and an FDI unit, which is in charge of diagnosing the current fault situation and engaging the corresponding VA in the loop between the plant and the controller. The bank of VAs and the FDI unit constitute the Fault Tolerance Mechanism illustrated in Figure 1. Some preliminary results related to this scheme

DOI: 10.1002/acs

have been recently presented in [24] and [23], for those cases where the system evolution matrix is invertible; the results in the present paper, on the other hand, hold for invertible and non-invertible evolution matrices. The remainder of the paper is organised as follows. In Section 2 we define the equations of the plant to be controlled, the FTC strategy, and the bank of VAs. In Section 3 we present the main conditions related to the controller, the control objectives, the VA and FDI design. Section 4 establishes the results associated to the closed-loop properties of the considered scheme, namely, input convergence, VA state convergence, and setpoint tracking. In Section 5 we describe the proposed FDI principle, based on an invariant set approach. In Section 6 we present an illustrative example, while in Section 7 we provide some concluding remarks.

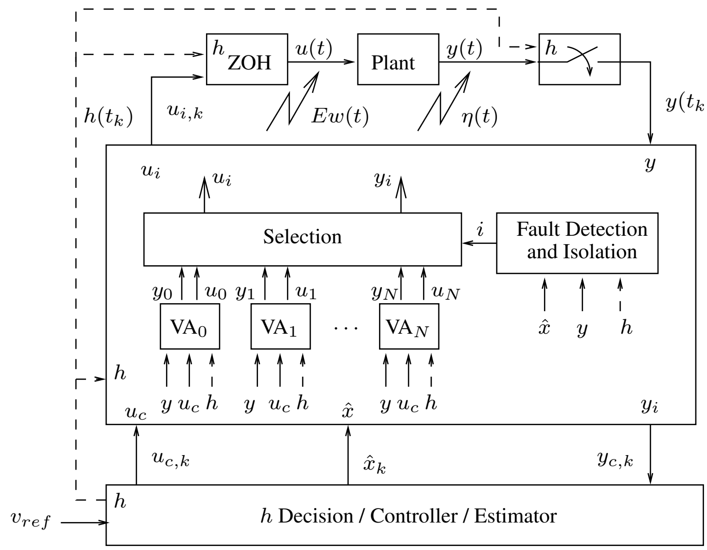


Figure 1. Considered scheme: a central controller is in charge of commanding both the process and the next sampling instant. The fault tolerance mechanism involves an FDI unit and a bank of VAs. The selection of the active sampling period is communicated to the fault tolerance mechanism.

2. PROBLEM FORMULATION

We consider actuator-fault-tolerant output-feedback control of a continuous-time plant by means of a discrete-time controller, bank of virtual actuators, and FDI unit. The discrete-time controller is designed for the fault-free (healthy) situation and hence knowledge of the fault scenario is not necessary at the controller design stage. In addition to computing the control action assuming fault-free operation, this “fault-ignorant” controller is in charge of performing on-line variations of the sampling rate. In the sequel, we explain the different components of the feedback control system considered.

2.1. *Continuous-time plant*

The plant model that we employ is the following:

$$\dot{x} = Ax + BFu + Ew, \quad y = Cx + \eta, \tag{1}$$

$$v = C_v x, \tag{2}$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$ is the control input, $w \in \mathbb{R}^{n_w}$ is a bounded state disturbance, E its incidence matrix, $y \in \mathbb{R}^p$ is the plant measured output, $\eta \in \mathcal{N} \subset \mathbb{R}^p$ its bounded disturbance, and $v \in \mathbb{R}^q$ is a performance output. The matrix $F \in \mathbb{R}^{m\times m}$ takes values from a finite set

$$F \in \mathcal{F} := \{F_0, F_1, \cdots, F_N\}, \quad F_0 = I, \tag{3}$$

Prepared using acsauth.cls
DOI: 10.1002/acs

and represents the plant's actuator fault situation. Under healthy operation, the matrix F in (1) takes the value $F = F_0 = I$, so that B in (1) represents the "healthy" plant input matrix. Under fault, $F = F_j$ for some $j = 1, \ldots, N$. For example, total loss of actuator 2 is modelled by zeroing the $2nd$ column of F_0. Additionally, the occurence of faults over multiple actuators can be modeled by a matrix $F_j \in \mathcal{F}$, zeroing their corresponding columns of F_0. We assume that the pairs (A, BF_i) are stabilisable for $i = 0, 1, \cdots, N$, and that (C, A) is detectable.

The performance output v in (2) and the different fault situations in (3) must be such that for every desired constant value v_{ref} of the performance output and every fault i, there exist equilibrium input $\bar{u}_i$ and state $\bar{x}_i$ such that $C_v \bar{x}_i = v_{ref}$, i.e. for every v_{ref} there exist $\bar{x}_i$, $\bar{u}_i$ such that

$$\begin{bmatrix} A & BF_i \\ C_v & 0 \end{bmatrix} \begin{bmatrix} \bar{x}_i \\ \bar{u}_i \end{bmatrix} = \begin{bmatrix} 0 \\ v_{ref} \end{bmatrix} \tag{4}$$

for all $i \in \{0, 1, \ldots, N\}$. Condition (4) means that the plant has sufficient levels of redundancy to admit setpoint tracking in each fault scenario. Note that if, for a given v_{ref} and specific fault i, no $\bar{x}_i, \bar{u}_i$ exist satisfying (4), then the performance output will not converge to v_{ref} under fault i, no matter how sophisticated the fault tolerance mechanism may be. On the other hand, the VA fault tolerance mechanism has to be designed so that the required equilibrium values satisfying (4) are achieved under all possible fault situations; this will be addressed in detail in Section 3.2.

2.2. *Fault-ignorant varying-sampling-rate controller*

As previously explained, knowledge of the fault scenario is not needed at the controller design stage. Consequently, controller design is independent of virtual actuator design. We consider a healthy-plant-model-based reference-tracking sampled-data controller given by

$$u_c = -K^h(\hat{x} - x_{ref}) + u_{ref}, \tag{5}$$
$$\hat{x}^+ = A^h\hat{x} + B^h u_c + L^h(y_c - C\hat{x}), \tag{6}$$

where u_c represents the controller-computed plant input signal (recall Figure 1), y_c is the plant output signal supplied to the controller, x_{ref}, u_{ref} are state and input constant reference signals, respectively, and $\hat{x}$, $\hat{x}^+$ are the current and successor states of the observer (6). The matrices A^h and B^h are the discrete-time equivalents of A and B in (1), corresponding to a sampling period h,

$$A^h := e^{Ah}, \quad B^h := \int_0^h e^{At} B dt, \tag{7}$$

and the reference signals satisfy

$$Ax_{ref} + Bu_{ref} = 0, \qquad C_v x_{ref} = v_{ref}. \tag{8}$$

Observe that the above equation is a particular solution of (4), for the case when $i = 0$. The controller may perform on-line variations of the sampling period h, under the constraint that all possible sampling periods are taken from a finite set:

$$h \in \mathcal{H} := \{h_1, \cdots, h_{n_s}\}, \tag{9}$$

where every $h \in \mathcal{H}$ should be non-pathological (see [5] for further details on pathological sampling). The feedback and observer gains K^h and L^h employed by the controller may depend on the sampling period selected. The computation of these gains will be explained in Section 3.1. If no fault tolerance mechanism were present, the plant input u would equal the controller-computed plant input u_c and the plant output supplied to the controller, y_c, would equal the true plant output, y, at all sampling instants. In the presence of the fault tolerance mechanism discussed in the current paper, the equalities $y = y_c$ and $u = u_c$ will be true only under nominal (healthy) conditions and provided the fault tolerance mechanism accurately detects that the plant is under healthy operation.

2.3. Nominal plant-controller feedback loop

Under nominal conditions, at instant t_k the controller receives the sample y_c and processes it in order to compute the required feedback action. To do so, it also determines the instant $t_{k+1} = t_k + h(k)$, with $h(k) \in \mathcal{H}$, at which it will take the next sample and control action. The plant dynamics at the sampling instants can be written as

$$x^+ = A^h x + B^h F u + w^h \tag{10}$$

where $x = x(t_k)$, $u = u(t_k)$, $x^+ = x(t_{k+1})$, A^h and B^h are as in (7) with $h = h(k)$, $w^h = \int_{t_k}^{t_{k+1}} e^{A(t_{k+1}-t)} E w(t) dt$. Note that a bound on w^h can be computed when a bound on $w(t)$ is known, and hence, we write $w^h \in \mathcal{W}$, where $\mathcal{W} \subset \mathbb{R}^n$ is a bounded set.

The nominal controller signal given in (5) uses the reference values satisfying (8), which define an equilibrium point for the continuous-time (CT) system $\dot{x} = Ax + Bu$. These values also define an equilibrium point for the discrete-time (DT) system $x^+ = A^h x + B^h u$ for all values of the sampling period h. To see this, first, from (7), we can obtain the identity $\int_0^h e^{At} dt A = A^h - I$. Next, compute

$$B^h u_{ref} = \int_0^h e^{At} dt B u_{ref} = -\int_0^h e^{At} dt A x_{ref}, \tag{11}$$

where we have used (8). On the right-hand-side, replace the integral using the above identity to obtain $B^h u_{ref} = (I - A^h) x_{ref}$. Thus,

$$x_{ref} = A^h x_{ref} + B^h u_{ref} \quad \forall h \in \mathcal{H}. \tag{12}$$

Since the controller may perform arbitrary on-line variations of h, the DT system (10) (obtained by looking at the CT plant only at the sampling instants) can be regarded as a *Discrete-Time Switched System* (DTSS). Since we are interested in establishing closed-loop properties (such as stability and setpoint tracking) that hold irrespective of the way in which the controller may vary h, we consider a DTSS under *arbitrary switching* [16, 30].

2.4. Bank of virtual actuators

As in [27], we consider a bank of VAs where each of the VAs in the bank is designed to compensate for a specific actuator fault. The VA corresponding to the i-th fault situation F_i is given by

$$\theta_i^+ = A^h \theta_i + B^h u_c - B^h F_i u_i, \tag{13}$$

$$u_i = -M_i^h \theta_i + N_i^h u_c + d_i, \tag{14}$$

$$y_i = y + C\theta_i \tag{15}$$

where d_i are constant vectors that represent degrees of freedom in the design and must satisfy

$$BF_i d_i = 0 \quad \text{for} \quad i \in \{0, 1, \cdots, N\}. \tag{16}$$

This condition is imposed in order that d_i have effect on the system only under *wrong matching* situation (*i.e.*when $F_j \neq F_i$), but to have no effect under *correct matching* ($F = F_i$). Appropriate selection of d_i enables the fault detection unit to distinguish between correct and wrong matching situations, as will be illustrated in Section 6.

The variable θ_i represents the i-th VA internal state, u_i is the i-th VA plant input signal, and y_i the i-th VA output to be supplied to the controller. How u_i and y_i relate to the true plant input u and the true output supplied to the controller y_c is explained in Section 2.5. The 0-th VA corresponds to nominal operating conditions (healthy or fault-free) and has

$$M_0^h = 0, \quad N_0^h = I, \quad \text{and} \quad d_0 = 0, \tag{17}$$

for all sampling periods h. For $i = 1, \ldots, N$, the VAs' internal matrices M_i^h and N_i^h may depend on the sampling period h selected by the controller. The design of M_i^h and N_i^h is explained in

DOI: 10.1002/acs

Section 3.2. For future reference, note that substitution of (14) into (13) yields

$$\theta_i^+ = A_i^h \theta_i + B^h(I - F_i N_i^h)u_c, \quad \text{with} \tag{18}$$
$$A_i^h := A^h + B^h F_i M_i^h. \tag{19}$$

that is, the dynamics of each VA is driven by the controller-computed plant input signal, u_c. To obtain (18), we have used the fact that, because of (16), $B^h F_i d_i = \int_0^h e^{At} dt B F_i d_i = 0$.

2.5. FDI and controller reconfiguration mechanism

Controller reconfiguration is achieved through a selector that, in response to the diagnosed fault situation, interconnects the appropriate virtual actuator from the bank of virtual actuators with the controller and the plant.

When the FDI mechanism detects that a transition from a fault status i to the j-th status has occurred, the j-th virtual actuator is interconnected with the controller and plant by making $u = u_j$ and $y_c = y_j$. In particular, whenever the FDI diagnoses that the plant is under healthy operation, the selector will set $u = u_0$ and $y_c = y_0$. The reconfiguration also resets the 0-th virtual actuator state θ_0 to zero whenever healthy operation is detected.

Under the above considerations, we next show that if the plant is under healthy operation and if the FDI mechanism successfully assesses the plant's healthy condition, then the plant and controller feedback loop will operate as if the bank of virtual actuators and reconfiguration mechanism were not present. From (14) and (17), then $u_0 = u_c$. Therefore, if at time k_0 the FDI mechanism detects that healthy operation is restored, then $\theta_0 = 0$ according to the virtual actuator state reset condition, $y_0 = y$ from (15), and it follows that $y_c = y_0 = y$ and $u = u_0 = u_c$ at time k_0. According to (13) it follows that $\theta_0 = 0$ and $y_c = y_0 = y$ and $u = u_0 = u_c$ will continue to hold for time instants $k \geq k_0$ until the FDI mechanism diagnoses a change in the plant fault condition. The design of the controller and VA matrices, as well as the FDI mechanism is explained in Section 3.

3. CONTROLLER, VIRTUAL ACTUATOR AND FDI DESIGN

The controller and bank of virtual actuators must be designed so that the performance output v [see (2)] is able to track a constant reference in closed loop, even if faults occur, and so that all closed-loop variables remain bounded. To do so, the FDI system must ensure the correct fault identification and engagement of the correct VA.

3.1. Controller design

Controller design involves the appropriate selection of the matrices K^h and L^h in (5)–(6). In order for the desired closed-loop properties to hold irrespective of the sampling period sequence selected by the varying-sampling-rate controller, the matrices K^h and L^h should be selected so that the closed-loop matrices

$$A^{h,\text{CL}} := A^h - B^h K^h, \tag{20}$$
$$A^{h,\text{O}} := A^h - L^h C, \tag{21}$$

make the sets $\{A^{h,\text{CL}} : h \in \mathcal{H}\}$ and $\{A^{h,\text{O}} : h \in \mathcal{H}\}$ stable under arbitrary switching. Stability under arbitrary switching is equivalent to the existence of a Lyapunov function common to every matrix in the corresponding sets (see, e.g. [30, 17]). In general, this common Lyapunov function may be not quadratic.

If K^h and L^h exist so that the closed-loop matrices (20) on the one hand, and (21) on the other, share a common *quadratic* Lyapunov function (CQLF) for all $h \in \mathcal{H}$, then K^h and L^h can be computed via linear matrix inequalities (LMIs) (see, e.g. [6, 26]).

In some cases, K^h and L^h can be found so that not only CQLFs exist, but also additional properties hold for the closed-loop matrices (20) and (21). One such case is when invertible T_{CL}

DOI: 10.1002/acs

and T_{O} exist so that $T_{\mathrm{CL}}^{-1}A^{h,\mathrm{CL}}T_{\mathrm{CL}}$ and $T_{\mathrm{O}}^{-1}A^{h,\mathrm{O}}T_{\mathrm{O}}$ are upper triangular for all $h \in \mathcal{H}$ (solvable Lie algebra case). Such common transformations T_{CL} and T_{O} are also useful for computing invariant sets and ultimate bounds in DTSS, as shown in [13, 14]. In addition, several works address the computation of K^h (and L^h) so that this simultaneous triangularization is achieved for $A^{h,\mathrm{CL}}$ (and $A^{h,\mathrm{O}}$) for general switched linear systems [10, 8], and specifically for cases as the current one, where A^h and B^h arise from sampling a single continuous-time system at different rates [12, 21, 11, 22]. While for general DTSS this design criterion may be restrictive, a reduction on such restrictiveness can be observed in this specific context, considering the following facts:

- the DTSS arises from sampling a single continuous-time system at different rates [12, 21, 11, 22],
- the system has input redundancy, in order to achieve successful trajectory tracking in the presence of total actuator loss, as explained in Section 2.1 [9].

3.2. *Virtual actuator features and design*

The bank of VAs, as defined in (13)–(15), jointly with the controller reconfiguration mechanism endow the feedback loop with specific features when the plant's fault situation is correctly diagnosed. One of these features is known as "fault hiding" because the controller variables u_c and y_c are related in such a way as if a plant under nominal conditions were connected to the controller. In order to see this feature, define

$$\xi_i := x + \theta_i, \quad i = 1, \cdots, N, \tag{22}$$

and write, using (13) and (10),

$$\xi_i^+ = A^h\xi_i + B^h(Fu - F_iu_i) + B^hu_c + w^h. \tag{23}$$

When the plant fault situation is correctly diagnosed, we have $F_i = F$, $u_i = u$ and $y_c = y_i$. From the latter equalities, (1), (15) and (23), it follows that

$$\xi_i^+ = A^h\xi_i + B^hu_c + w^h, \tag{24}$$

$$y_c = C\xi_i + \eta. \tag{25}$$

Eqs. (24)–(25) show that under the correct fault diagnosis and reconfiguration, the controller effectively sees a nominal plant, whose state is ξ_i instead of x.

A second feature of the bank of VAs and switching mechanism is that the desired setpoint v_{ref} for the performance output v defined in (2) should be preserved for all fault situations and sampling period variations, provided the plant fault situation is correctly diagnosed. In closed loop and under absence of disturbances and noise, the boundedness of all variables and the tracking of the desired setpoint v_{ref} are achieved by ensuring the following:

a) the controller-computed plant input u_c converges to the steady state value $\bar{u}_c = u_{ref}$,

b) the VA state vector θ_i converges to a constant steady-state value $\bar{\theta}_i$,

c) Under fault i, the plant state x and input u both converge to steady-state values $\bar{x}_i$ and $\bar{u}_i$ (independent of h) and satisfy (4).

In Section 4 we will show that items a)–c) above will be true (for noise- and disturbance-free plant) if we select the matrices M_i^h and N_i^h as explained next.

The matrices M_i^h should be selected so that for every $i \in \{0, 1, \ldots, N\}$, the matrices in the set $\{A_i^h : h \in \mathcal{H}\}$, with A_i^h as in (19), are stable under arbitrary switching. The latter can be achieved using, for example, LMI- or Lie-algebraic-solvability-based methods, as mentioned in Section 3.1, and implies that every eigenvalue of A_i^h has magnitude less than 1, and hence that $(I - A_i^h)$ is invertible.

Once the M_i^h are designed, select one sampling period $h' \in \mathcal{H}$ and compute

$$N_i^{h'} = \left[X_i^{h'}\right]^{\dagger} C_v (I - A_i^{h'})^{-1} B^{h'}, \tag{26}$$
$$X_i^h := C_v (I - A_i^h)^{-1} B^h F_i \quad \text{for all } h \in \mathcal{H}, \tag{27}$$

where † denotes the Moore-Penrose generalised inverse. For every other sampling period $h \in \mathcal{H}$, select the corresponding N_i^h as follows:

$$N_i^h = N_i^{h'} - (M_i^{h'} - M_i^h) P_i^{h'}, \quad \text{where} \tag{28}$$
$$P_i^h := (I - A_i^h)^{-1} B^h (I - F_i N_i^h) \quad \text{for all } h \in \mathcal{H}. \tag{29}$$

The following result concerning the expression for P_i^h above will be required in Section 4.

Lemma 1
Let $h \in \mathcal{H}$ and $i \in \{0, \ldots, N\}$. Then,

$$(I - A_i^h)^{-1} B^h = -(A + BF_i M_i^h)^{-1} B. \tag{30}$$

Proof
Define $\Phi(h)$ as

$$\Phi(h) := \int_0^h e^{A\tau} d\tau. \tag{31}$$

Since $h > 0$ and $e^{A\tau}$ is invertible, so is $\Phi(h)$. Also, from (7) consider the identity

$$I - A^h = -\Phi(h) A. \tag{32}$$

Expand the left hand side of (30) and use (7), (31) and (19),

$$\begin{aligned}
(I - A_i^h)^{-1} B^h &= (I - A_i^h)^{-1} \Phi(h) B & (33)\\
&= \left(\Phi(h)^{-1} (I - (A^h + B^h F_i M_i^h)\right)^{-1} B & (34)\\
&= \left[\left(\Phi(h)^{-1} - \Phi(h)^{-1} A^h\right) - \Phi(h)^{-1} B^h F_i M_i^h\right]^{-1} B & (35)
\end{aligned}$$

From (32), observe that $\Phi(h)^{-1} - \Phi(h)^{-1} A^h = -A$ and using (7) and (31) we get that $\Phi(h)^{-1} B^h = B$. Thus,

$$(I - A_i^h)^{-1} B^h = (-A - BF_i M_i^h)^{-1} B \tag{36}$$

whence, (30) follows. □

Observe that the above result also states that $(A + BF_i M_i^h)$ is invertible for every possible sampling period h.

In the next two sections we will present the main results of this paper. First, in Section 4 we show that if the matrices M_i^h and N_i^h are selected as previously explained, then items a)–c) above will be ensured and the closed-loop system will successfully track the desired setpoint v_{ref} under both nominal and faulty conditions, even when the varying-sampling-rate controller performs on-line variations of the sampling period. Secondly, in Section 5 we explain the residual generation and describe the operation of the FDI unit via an algorithm based on (invariant) set membership tests.

4. CLOSED-LOOP PROPERTIES UNDER VARYING SAMPLING RATE

In this section, we present the closed-loop properties results obtained under the considered scheme. These results are given below as Theorems 1, 2 and 3. Each theorem establishes the validity of one of the items a)–c) detailed in Section 3.2, under the design conditions and assumptions explained in Sections 2 and 3. These results ensure the appropriate operation of the VA for the considered varying-sampling-rate case, by ensuring the boundedness of all closed-loop variables and the convergence of the performance output to the desired reference value under persistent faults.

DOI: 10.1002/acs

4.1. *Control-computed plant input convergence*

To proceed, let us first define the following observer and tracking errors

$$\tilde{\xi}_i := \xi_i - \hat{x}, \tag{37}$$
$$\zeta_i := \xi_i - x_{ref}, \tag{38}$$

with ξ_i as in (22), and express the controller-computed plant input u_c in (5) as

$$u_c = -K^h\zeta_i + K^h\tilde{\xi}_i + u_{ref}. \tag{39}$$

Using (5)–(6), (12), (22), and (24)–(25), the observer and tracking error dynamics is given by

$$\tilde{\xi}_i^+ = A^h\tilde{\xi}_i + B^h(Fu - F_iu_i) + w^h - L^h(C\tilde{\xi}_i + \eta), \tag{40}$$
$$\zeta_i^+ = (A^h - B^hK^h)\zeta_i + B^h(Fu - F_iu_i) + B^hK^h\tilde{\xi}_i + w^h. \tag{41}$$

Observe that if the FDI unit correctly identifies the fault situation and engages its associated VA, (the *"matching hypothesis"*), then $\tilde{\xi}^+$ and ζ^+ take the form

$$\tilde{\xi}_i^+ = (A^h - L^hC)\tilde{\xi}_i + w^h - L^h\eta, \tag{42}$$
$$\zeta_i^+ = (A^h - B^hK^h)\zeta_i + B^hK^h\tilde{\xi}_i + w^h. \tag{43}$$

We are now ready to present our first Theorem, proving item a) of Section 3.2.

Theorem 1
Consider the continuous-time plant (1)–(2) without disturbances ($w \equiv 0$, $\eta \equiv 0$), in closed-loop with the varying-sampling-rate controller (5)–(8) and bank of VAs (13)–(17). Suppose that there exist feedback matrices K^h and observer-gain matrices L^h such that the sets $\{A^{h,\mathrm{CL}} : h \in \mathcal{H}\}$ and $\{A^{h,\mathrm{O}} : h \in \mathcal{H}\}$, with $A^{h,\mathrm{CL}}$ and $A^{h,\mathrm{O}}$ as in (20) and (21), are stable under arbitrary switching. If the plant's fault condition is persistent and successfully diagnosed by the FDI unit, then

i) the combined plant-VA state ξ_i in (22), where i identifies the plant's fault condition, converges to the steady-state value $\bar{\xi}_i = x_{ref}$, and so does the observer state $\hat{x}$.

ii) the controller-computed plant input u_c converges to the steady-state value $\bar{u}_c = u_{ref}$.

Proof
The equality (39) is valid for all $i \in \{0, \cdots, N\}$, and the equations for $\tilde{\xi}_i$ and ζ_i without disturbances are obtained from (40)–(41), setting $w^h = 0$ and $\eta = 0$. By hypothesis, the FDI unit correctly diagnoses the plant's fault condition and hence interconnects the i-th VA with the controller and plant ($u = u_i$, $F = F_i$, $y_c = y_i$). Under this matching hypothesis, the error dynamics (40)–(41) become as in (42)–(43), with $w^h = 0$ and $\eta = 0$. Since both $A^h - L^hC$ and $A^h - B^hK^h$ are stable under arbitrary switching, then

$$\lim_{k\to\infty} \tilde{\xi}_i = 0 \quad \text{and} \quad \lim_{k\to\infty} \zeta_i = 0, \tag{44}$$

which establishes i) by recalling (37)–(38). From (39), then

$$\bar{u}_c = \lim_{k\to\infty} u_c = u_{ref}, \tag{45}$$

which establishes ii). Note that both (44) and (45) are true for every possible evolution of the sampling periods $h \in \mathcal{H}$ (even when varied on-line). □

4.2. *VA state convergence*

The convergence of the VA state, as per item b) of Section 3.2, is established in Theorem 2 below. We first require the following auxiliary result.

DOI: 10.1002/acs

Lemma 2
Consider the matrices X_i^h as defined in (27). Suppose that the continuous-time system matrices A, B are such that (A, BF_i) are stabilisable for $i = 0, 1, \cdots, N$, and for each fault matrix F_i there exist constant values $\bar{x}_i$ and $\bar{u}_i$ satisfying (4). Then, $X_i^h \left[X_i^h\right]^\dagger = I$.

Proof
The existence of constant values $\bar{x}_i$ and $\bar{u}_i$ satisfying (4) is equivalent to the condition that the matrix $\begin{bmatrix} -A & BF_i \\ -C_v & 0 \end{bmatrix}$ has rank $n+q$. Under non-pathological sampling $h \in \mathcal{H}$ the latter rank condition implies (see, e.g., the proof of Lemma IV.3 in [3])*

$$\operatorname{rank} \begin{bmatrix} I_n - A^h & B^h F_i \\ -C_v & 0 \end{bmatrix} = n + q. \tag{46}$$

Correct design of M_i^h (recall Section 3.2) implies that A_i^h defined in (19) has all eigenvalues with magnitude less than one; then $(I_n - A_i^h)$ is invertible and we can write

$$\begin{bmatrix} I_n & 0 \\ C_v(I_n - A_i^h)^{-1} & I_q \end{bmatrix} \begin{bmatrix} I_n - A^h & B^h F_i \\ -C_v & 0 \end{bmatrix} \begin{bmatrix} I_n & 0 \\ -M_i^h & I_m \end{bmatrix} = \begin{bmatrix} I_n - A_i^h & B^h F_i \\ 0 & X_i^h \end{bmatrix}, \tag{47}$$

where $X_i^h \in \mathbb{R}^{q \times m}$ is defined in (27). Since the first and third matrices on the left-hand side (LHS) of (47) are invertible, it follows (using Sylvester's inequality and properties of the matrix rank) that the rank of the second matrix on the LHS is equal to the rank of the matrix on the right-hand side of (47). Using (46) we then have $\operatorname{rank} X_i^h = q$, that is, X_i^h has full row rank. Thus, its Moore-Penrose generalised inverse can be written as $[X_i^h]^\dagger = [X_i^h]^T \left[X_i^h [X_i^h]^T\right]^{-1}$ and satisfies $X_i^h \left[X_i^h\right]^\dagger = I_q$. The result then follows. □

We are now ready to establish item b) of Section 3.2.

Theorem 2
Under the hypotheses of Theorem 1, suppose also that for each fault matrix F_i, $i = 0, 1, \ldots, N$, there exist constant values $\bar{x}_i$ and $\bar{u}_i$ satisfying (4), and matrices M_i^h so that the set of matrices $\{A_i^h : h \in \mathcal{H}\}$, with A_i^h as in (19), is stable under arbitrary switching. Suppose that N_i^h are selected as explained in Section 3.2. If the plant's fault condition is persistent and successfully diagnosed by the FDI unit, then the VA state satisfies

$$\lim_{k \to \infty} \theta_i = \bar{\theta}_i \quad \text{and} \quad C_v \bar{\theta}_i = 0, \tag{48}$$

where $\bar{\theta}_i$ is constant and independent of the sampling period h, and the limit in (48) is valid for every possible evolution (*i.e.*, on-line variations) of the sampling period.

Proof
From Theorem 1-ii), we know that $\bar{u}_c = u_{ref}$. Let $\bar{\theta}_i^h$ denote the equilibrium value of the VA state θ_i if a constant sampling period h were kept by the controller. Solving from (18) and using (29), we can write

$$\bar{\theta}_i^h = P_i^h u_{ref}. \tag{49}$$

We next show that P_i^h is independent of h. Let $h' \in \mathcal{H}$ be the sampling period selected for the computation of $N_i^{h'}$ as in (26). Using (29) and Lemma 1, we can write

$$P_i^h = -(A + BF_i M_i^h)^{-1} B (I - F_i N_i^h) \tag{50}$$

*For clarity, in this proof we use a sub-index to indicate the dimensions of the identity matrices, that is, I_n denotes the $n \times n$ identity matrix.

for all $h \in \mathcal{H}$. Replacing N_i^h by the expression (28), adding $-AP_i^{h'} + AP_i^{h'}$ inside the square brackets, and operating, yields

$$P_i^h = -(A + BF_iM_i^h)^{-1}\big[B(I - F_iN_i^{h'}) - (A + BF_iM_i^h)P_i^{h'} + (A + BF_iM_i^{h'})P_i^{h'}\big]. \tag{51}$$

Using (50), then $(A + BF_iM_i^{h'})P_i^{h'} = -B(I - F_iN_i^{h'})$. Using the latter expression in (51) yields

$$P_i^h = -(A + BF_iM_i^h)^{-1}[-(A + BF_iM_i^h)P_i^{h'}] = P_i^{h'},$$

which establishes that P_i^h is independent of h. We can thus write $P_i^h = P_i$ for all $h \in \mathcal{H}$. Therefore, the steady-state value $\bar{\theta}_i^h$ also is independent of h, as follows from (49), and we can write $\bar{\theta}_i^h = \bar{\theta}_i$ for all $h \in \mathcal{H}$. Define the incremental variables

$$\Delta\theta_i := \theta_i - \bar{\theta}_i, \quad \text{and} \quad \Delta u_c := u_c - \bar{u}_c = u_c - u_{ref}. \tag{52}$$

Use (18) to write the VA dynamics in the incremental variables as

$$\Delta\theta_i^+ = A_i^h \Delta\theta_i + B^h(I - F_iN_i^h)\Delta u_c,$$

where $\Delta u_c \to 0$ by Theorem 1, and $\{A_i^h : h \in \mathcal{H}\}$ are stable under arbitrary switching for every $i = 0, \ldots, N$. It follows that $\Delta\theta_i \to 0$ and hence $\lim_{k\to\infty} \theta_i = \bar{\theta}_i$. Using (26)–(27) and (29), yields

$$C_vP_i = C_vP_i^{h'} = \left(I - X_i^{h'}\left[X_i^{h'}\right]^{\dagger}\right) C_v(I - A_i^{h'})^{-1}B^{h'}.$$

Using Lemma 2, then $C_vP_i = C_vP_i^h = 0$ for all $h \in \mathcal{H}$. Recalling (49), then $C_v\bar{\theta}_i = C_v\bar{\theta}_i^h = C_vP_iu_{ref} = 0$. □

Theorem 2 shows that the virtual actuator state converges to a constant steady-state value that is independent of the sampling periods $h \in \mathcal{H}$ and, in addition, is in the null space of the performance output matrix C_v [see (2)]. This property is key to achieving the correct setpoint v_{ref} for the performance output v, a property that is established in the following section.

4.3. *Setpoint tracking*

We next present our last result on closed-loop properties, which establishes item c) of Section 3.2, related to the setpoint tracking property of the controller-driven sampling VA introduced.

Theorem 3
Under the same hypotheses as for Theorem 2, the plant state x and the performance output v satisfy

$$\lim_{k\to\infty} x = \bar{x}_i := x_{ref} - \bar{\theta}_i \quad \text{and} \quad \lim_{k\to\infty} v = v_{ref}.$$

Proof
From Theorem 1-i), the combined plant and VA state ξ_i converges to the steady-state value x_{ref} and From Theorem 2, the VA state θ_i converges to $\bar{\theta}_i$. Recalling (22), then the plant state x must converge to the steady-state value $\bar{x}_i = x_{ref} - \bar{\theta}_i$. The performance output thus satisfies

$$\lim_{k\to\infty} v = C_v\bar{x}_i = C_vx_{ref} - C_v\bar{\theta}_i = v_{ref},$$

where we have used (8) and (48). □

The above result shows that, if the correct fault situation has been diagnosed and the matching VA has been engaged in the closed-loop system, then the VA-reconfigured system will achieve the desired constant setpoint tracking, irrespective of the on-line variations of the sampling periods $h \in \mathcal{H}$.

While the above convergence results have been established for the system without disturbances, boundedness of the closed-loop trajectories holds for the system with bounded disturbances. Additionally, ultimate bounds for the system and VAs states can be computed using, for example, the ultimate bound computation method for switched systems presented in [13].

DOI: 10.1002/acs

5. FDI PRINCIPLE AND RESIDUAL GENERATION

The FDI unit is responsible for correctly identifying the fault situation, and engaging the correct VA in the loop. In this paper, we extend the FDI and residual generation strategy of [27] to the controller-driven sampling case considered here. In [27], the FDI unit uses available quantities to compute a *residual* signal, which is a signal whose behaviour under fault distinctively deviates from its behaviour under healthy operation, and verifies membership of the residual to some previously computed sets. A change in the membership from a set to another means an abrupt change in the fault situation. Recalling the definition of the observer error in (37), we will use as residual the quantity

$$r_i := y_i - C\hat{x} = C\tilde{\xi}_i + \eta, \tag{53}$$

(as in [27]) where y_i is the output provided by the i-th VA (15), and $\hat{x}$ is the state of the observer (6). We will next analyse the behaviour of the residual (53) under healthy and faulty operation through the computation of sets where it evolves in each case.

Consider the observer and tracking error dynamics under the matching hypothesis, given by (42)–(43). Since $\{A^{h,\text{CL}} : h \in \mathcal{H}\}$ and $\{A^{h,\text{O}} : h \in \mathcal{H}\}$ are both stable under arbitrary switching (recall Section 3.1), and since the process disturbance w^h and measurement noise η are both bounded (*i.e.*, $w^h \in \mathcal{W}$ and $\eta \in \mathcal{N}$), then attractive invariant sets $\mathcal{Z}$ and $\tilde{\Xi}$ can be computed for the error variables ζ_i and $\tilde{\xi}_i$. These sets are such that the errors converge to them in finite time (attractiveness) and remain inside (invariance) if the fault situation is maintained for a sufficiently long time (persistent fault). Invariant sets for stable DTSSs under arbitrary switching can be computed using their common Lyapunov function. Alternatively, if the required closed-loop matrices have some additional structure, such as being simultaneously triangularizable, some structure-based invariant-set computation methods can be directly applied [13, 14]. This computation strategy is illustrated in Section 6. Note that due to the form of (42)–(43), the sets $\mathcal{Z}$ and $\tilde{\Xi}$ are independent of which fault occurs (independent of i). In other words, if a persistent fault i occurs and is correctly detected, then the variables ζ_i and $\tilde{\xi}_i$ will converge to sets that are independent of which fault has occurred (and also independent of the evolution of the sampling rate). Then, under persistent fault i and if the FDI correctly detects the fault status change and engages the appropriate VA, the residual (53) will satisfy (after some initial finite-time transient):

$$r_i \in \mathcal{R}, \quad \text{where} \quad \mathcal{R} := C\tilde{\Xi} \oplus \mathcal{N} \tag{54}$$

is the "correct-matching" set and $\oplus$ denotes the Minkowski sum of sets.

Since the proposed fault diagnosis will rely on set membership, when a change in the fault situation occurs the residual signal must have converged to its corresponding correct-matching set for correct diagnosis of the new fault situation. This leads to the following fault scenario.

Assumption 1 (Fault Scenario)
Between the occurrence of any two consecutive changes in the fault situation, sufficient time elapses such that the after-fault system variables converge to their respective invariant sets.

We next derive a set where the residual will belong when the fault situation suddenly changes from i to j, assuming that fault situation i has been maintained for a sufficiently long time so that $\zeta_i \in \mathcal{Z}$, $\tilde{\xi}_i \in \tilde{\Xi}$ and (54) hold right up to the time when the change occurs. From (39), whenever $\zeta_i \in \mathcal{Z}$ and $\tilde{\xi}_i \in \tilde{\Xi}$, the controller-computed signal u_c satisfies

$$u_c \in \mathcal{U}_c^h := -K^h\mathcal{Z} \oplus K^h\tilde{\Xi} \oplus \{u_{ref}\}. \tag{55}$$

Recalling features a) to c) in Section 3.2, we may define the incremental variables $\Delta\theta_i := \theta_i - \bar{\theta}_i$ and $\Delta u_c := u_c - u_{ref}$ and obtain, using (18), $\Delta\theta_i^+ = A_i^h\Delta\theta_i + H_i^h\Delta u_c$, where $H_i^h := B^h(I - F_iN_i^h)$. Since Δu_c converges to the bounded set $\Delta\mathcal{U}_c := \cup_{h\in\mathcal{H}}\{-K^h\mathcal{Z} \oplus K^h\tilde{\Xi}\}$ and $\{A_i^h : h \in \mathcal{H}\}$ is stable under arbitrary switching, then under persistent fault i the increment $\Delta\theta_i$ will converge to an attractive invariant set $\Delta\mathcal{S}_i$ and hence, θ_i will converge to $\mathcal{S}_i := \Delta\mathcal{S}_i + \bar{\theta}_i$. Note that whenever

DOI: 10.1002/acs

$\theta_i \in \mathcal{S}_i$ and $u_c \in \mathcal{U}_c^h$, the i-th VA variable u_i in (14) satisfies

$$u_i \in \mathcal{U}_i^h := -M_i^h \mathcal{S}_i \oplus N_i^h \mathcal{U}_c^h \oplus \{d_i\} \tag{56}$$

at time instant t_k, with $h = t_{k+1} - t_k$. Suppose that the plant fault situation changes from i at instant t_k to j at t_{k+1}. The fault matrix F in (1) thus changes from F_i to F_j. At t_{k+1}, the residual r_i of the previously-matching i-th VA will satisfy, using (53), (40) and (21),

$$r_i \in \mathcal{R}_{ij,h}^{+} := C\big[A^{h,\mathrm{o}}\tilde{\Xi} \oplus B^h(F_j - F_i)\mathcal{U}_i^h \oplus \mathcal{W} \oplus (-L^h)\mathcal{N}\big] \oplus \mathcal{N}. \tag{57}$$

The second addend within the square brackets in the above definition forces the set $\mathcal{R}_{ij,h}^{+}$ to shift away from zero. If this set has empty intersection with $\mathcal{R}$, then the change in the fault situation can be successfully detected.

Assumption 2 (Set separation)

$$\begin{aligned} \mathcal{R} \cap \mathcal{R}_{ij,h}^{+} &= \emptyset && \forall\, i \neq j,\ \forall h \in \mathcal{H} \\ \text{and } \mathcal{R}_{ij,h}^{+} \cap \mathcal{R}_{ik,h}^{+} &= \emptyset && \forall k \neq j,\ \forall h \in \mathcal{H}, \forall i \neq j, \forall i \neq k \end{aligned}$$

The scheme is guaranteed to work correctly for abrupt faults that are such that the set separation of Assumption 2 holds. Notice that since $BF_i d_i = 0$ and the sets $\mathcal{R}_{ij,h}^{+}$ depend on d_i [recall (56)–(57)], then d_i can be used as a design parameter in order to achieve the correct set separation. Observe that knowledge of the sampling period h is necessary for testing whether the residual r_i satisfies (57). Following [27], the FDI mechanism can be devised by monitoring the matching VA and testing whether its associated residual r_i satisfies (54) or (57). If a change is detected, the correct VA is immediately engaged but the algorithm waits enough time before making another test so that the after-change system states converge to their respective invariant sets. The following is the analogue of Algorithm 4.3 of [27] for the case of controller-driven sampling.

Algorithm 1 (FDI and controller reconfiguration logic)
Compute the sets $\mathcal{R}$ and $\mathcal{R}_{ij,h}^{+}$, for all $i, j \in \{0, 1 \ldots, N\}, i \neq j$, and all $h \in \mathcal{H}$.

1. Initialisation. Suppose that the initial fault situation i is known (e.g. healthy, $i = 0$) and allow sufficient time for the system variables to converge to their respective invariant sets.
2. Evaluate the residual r_i from y_i and $\hat{x}$ as in (53):
   (a) If $r_i \in \mathcal{R}$, go to Step 2; else
   (b) If $r_i \in \mathcal{R}_{ij,h}^{+}$ for some $j \neq i$, then engage the j-th VA by setting $u = u_j$ and $y = y_j$ (reconfiguration). Set $i \leftarrow j$ and go to Step 3; else
   (c) If $r_i \notin \mathcal{R}$ and $r_i \notin \mathcal{R}_{ij,h}^{+}$ for any $j \neq i$, require intervention.
3. Wait sufficient time to allow convergence to invariant sets[†].
4. Go to Step 2

The required waiting time (at initialization and Step 3) can be obtained, in general, by means of the common Lyapunov function that is admitted by the stable closed-loop discrete-time switched system. This would give an estimate of the required time as a number of discrete steps (number of sampling events to wait for before performing any action). In the case where feedback design achieves closed-loop Lie-algebraic solvability (simultaneous triangularization), an estimate of the required waiting time can be obtained by following the ideas in [13, 14]. Condition 2(c) may occur, for example, if the system experiences a new fault status change before reaching the invariant set.

[†]The details over the estimation of this convergence time is out of the scope of this paper, but a discussion on algorithms to estimate this convergence time can be consulted in [19]

DOI: 10.1002/acs

In such a case, due to the misconfiguration, the state variables may not reach their invariant sets and thus, convergence to $\mathcal{R}$ cannot be ensured. Additionally, observe that controller reconfiguration after a change in the fault situation is performed in only one sampling period, and hence takes at most $\max\{\mathcal{H}\}$ seconds. The implementation of the proposed FDI mechanism does not introduce much processing overhead, since it only requires residual computation and set membership verification, which are simple algebraic operations when the required sets are convex. We will next illustrate the overall FTC scheme with an example.

6. EXAMPLE

We revisit the two tanks example presented in [31]. The considered plant is composed of two interconnected tanks as shown in Figure 2, where the objective is to keep a constant level on the second tank. In this plant, the redundant input is given by the inflow to the first tank control and the connecting valve opening, which is located at a height l_v.

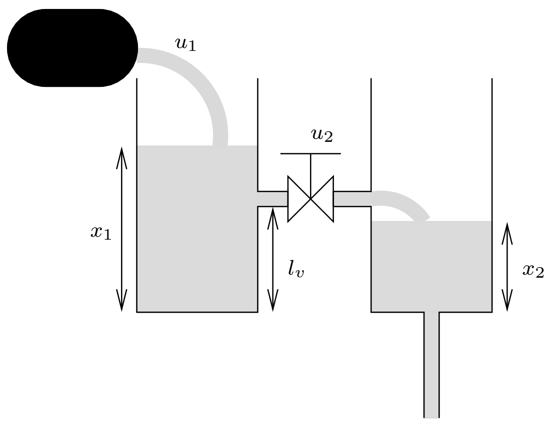


Figure 2. Two interconnected tanks. Tank 1 (left) is fed by a pump (flow u_1). Flow from Tank 1 into Tank 2 passes through the interconnecting valve (valve opening u_2). The objective is to maintain a constant level on Tank 2 (right).

Being x_1 and x_2 the incremental levels of the first and the second tank respectively, about equilibrium levels $\bar{x}_1$ and $\bar{x}_2$, under the condition that $\bar{x}_2 < l_v < \bar{x}_1$, the linearised plant equations are given by (1)–(2), where

$$A := \begin{bmatrix} -0.25 & 0 \\ 0.25 & -0.25 \end{bmatrix}, \; B := \begin{bmatrix} 1 & -0.5 \\ 0 & 0.5 \end{bmatrix}, \; C = I, \; C_v := \begin{bmatrix} 0 & 1 \end{bmatrix}$$

and each component of the measurement disturbance η is bounded within the interval $[-10^{-4}, 10^{-4}]$. In this example, we will consider only the loss of actuator u_2 (connecting valve blocked in nominal position), referred as Fault type 2 in [31], producing

$$F \in \mathcal{F} := \{F_0, F_1\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \right\}.$$

When actuator u_2 fails, the level in Tank 2 can only be modified by controlling the level in Tank 1 through the pump.

The considered sampling period set is given by $\mathcal{H} := \{h_1 = 0.1, \; h_2 = 0.05, \; h_3 = 0.025\}$. Note that, while each of the considered sampling periods is a multiple of h_3, this is not a requirement of the proposed strategy. We assume that each component of the perturbation w^h in the plant dynamics at the sampling instants (10) is bounded within the interval $[-10^{-4}, 10^{-4}]$ for every possible sampling period.

Since ensuring acceptable performance under total actuator outage requires that the plant have sufficient input redundancy, some structure-based feedback design methods, such as those based on simultaneous triangularization (*i.e.*, solvable Lie algebra), become increasingly appealing [9, 11] and facilitate the computation of the invariant sets required [13]. In this example we compute feedback matrices for both controller (K^h) and VA (M_1^h), using the Lie-algebraic-solvability-based method presented as Algorithm 1 in [10]. For such algorithm, we selected the parameter $\epsilon_c = 0.01$, which is associated with the stability limits. We first applied such algorithm to the matrix pairs $\{(A^h, B^h), h \in \mathcal{H}\}$ and obtained the feedback matrices:

$$K^{h_1} = 0.01 \begin{bmatrix} 999 & 975 \\ -6.14 & -5.99 \end{bmatrix}, \; K^{h_2} = 0.01 \begin{bmatrix} 1999 & 1975 \\ -6.19 & -6.12 \end{bmatrix}, \quad K^{h_3} = 0.01 \begin{bmatrix} 3999 & 3975 \\ -6.21 & -6.18 \end{bmatrix},$$

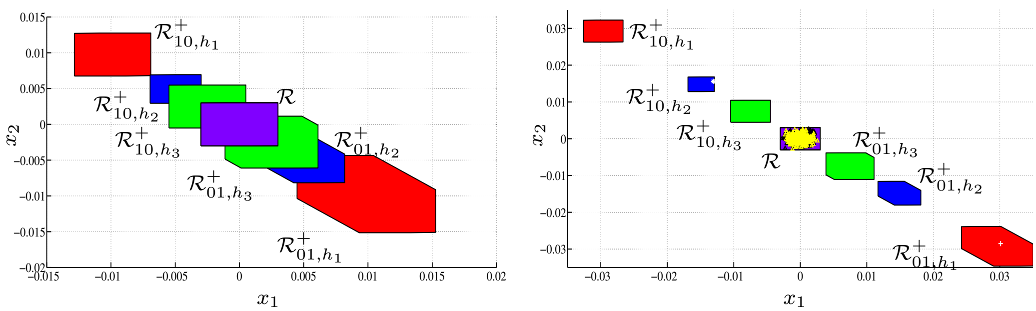
and then to the pairs $\{(A^h, B^h F_1), h \in \mathcal{H}\}$, in order to obtain the VA feedback matrices:

$$M_1^{h_1} = -\begin{bmatrix} 11.23 & 107.99 \\ 0 & 0 \end{bmatrix}, M_1^{h_2} = -\begin{bmatrix} 21.34 & 233.18 \\ 0 & 0 \end{bmatrix}, M_1^{h_3} = -\begin{bmatrix} 41.39 & 485.57 \\ 0 & 0 \end{bmatrix}.$$

Using h_1, we can compute $N_1^{h_1}$ from (26) and then $N_1^{h_2}$ and $N_1^{h_3}$ using (28)–(29). The computed values are

$$N_1^{h_1} = \begin{bmatrix} 1 & 22.46 \\ 0 & 0 \end{bmatrix}, \; N_1^{h_2} = \begin{bmatrix} 1 & 2.25 \\ 0 & 0 \end{bmatrix}, \; N_1^{h_3} = \begin{bmatrix} 1 & -37.86 \\ 0 & 0 \end{bmatrix}.$$

Since $C = I$ we can choose $L^h = A^h$ for all $h \in \mathcal{H}$ (dead-beat observer). The last step to finalize the design usign the presented strategy is to select proper values of d_i in (14). As mentioned in Section 2.4, $d_0 = [0\,0]^T$ and d_1 is a design parameter that facilitates correct set separation, as required by the FDI unit. The correct-matching and fault-transition FDI sets (54) and (57) are computed based on invariant sets $\tilde{\Xi}$ and $\mathcal{Z}$ obtained through the method in [13]. To illustrate how the selection of d_1 affects set separation, we experimented with two values: $d_1 = [0,\ 0.2]^T$ and $d_1 = [0,\ 0.6]^T$. The sets corresponding to each value of d_1 are displayed in Figure 3. Observe that $d_1 = [0,\ 0.6]^T$ achieves the desired set separation. Hence, $d_1 = [0,\ 0.6]^T$ is selected for the simulation.



(a) FDI sets for $d_1 = [0,\ 0.2]^T$.

(b) FDI sets for $d_1 = [0,\ 0.6]^T$ and residual signal values.

Figure 3. FDI sets $\mathcal{R}$, $\mathcal{R}^+_{01,h}$ and $\mathcal{R}^+_{10,h}$ for $d_1 = [0,\ 0.2]^T$ (left) and $d_1 = [0,\ 0.6]^T$ (right). Computed residuals falling into $\mathcal{R}$, $\mathcal{R}^+_{01,h_1}$ and $\mathcal{R}^+_{10,h_2}$ are shown for $d_1 = [0,\ 0.6]^T$.

In order to test the strategy, we simulated the two-tank system from the initial conditions $x_1 = 0, x_2 = 0$, with $v_{ref} = 0.05$ and with arbitrary choices for the sampling periods $h \in \mathcal{H}$, including actuator fault and restitution at time instants that ensure that the required variables have already converged to their corresponding invariant sets.

The level in the first tank is displayed in Fig. 4(a), and the level and reference for the second tank are shown in Fig. 4(b); the evolution of the first component of both the controller-computed input and the input effectively sent to the actuator are displayed in Fig. 4(c), while that of their second

Int. J. Adapt. Control Signal Process. (0000)
DOI: 10.1002/acs

component in Fig. 4(d); Figures 4(e) and 4(f) display the evolutions of these control signals over the time interval 18 to 18.5, which contains the time instant when the fault occurs; the sampling period and fault indices are shown in Fig. 4(g). The fault occurs at 18.05 sec, and restitution at 35.025 sec. During healthy periods the controller-computed input coincides with the input effectively sent to the actuator, except for one sampling period immediately after restitution. Fault detection and controller reconfiguration behaviour can be observed in Figs. 4(e) and 4(f). At 18.05 sec, when the fault occurs, and up to the next sampling instant (18.15 sec), the controller-computed input still coincides with the input effectively sent to the actuator; one sampling period after the fault occurs (18.15 sec), the fault is diagnosed, the reconfiguration is performed, and hence a difference between the controller-computed input and the input effectively sent to the actuator can be observed beginning at the latter time instant and up to the next reconfiguration instant.

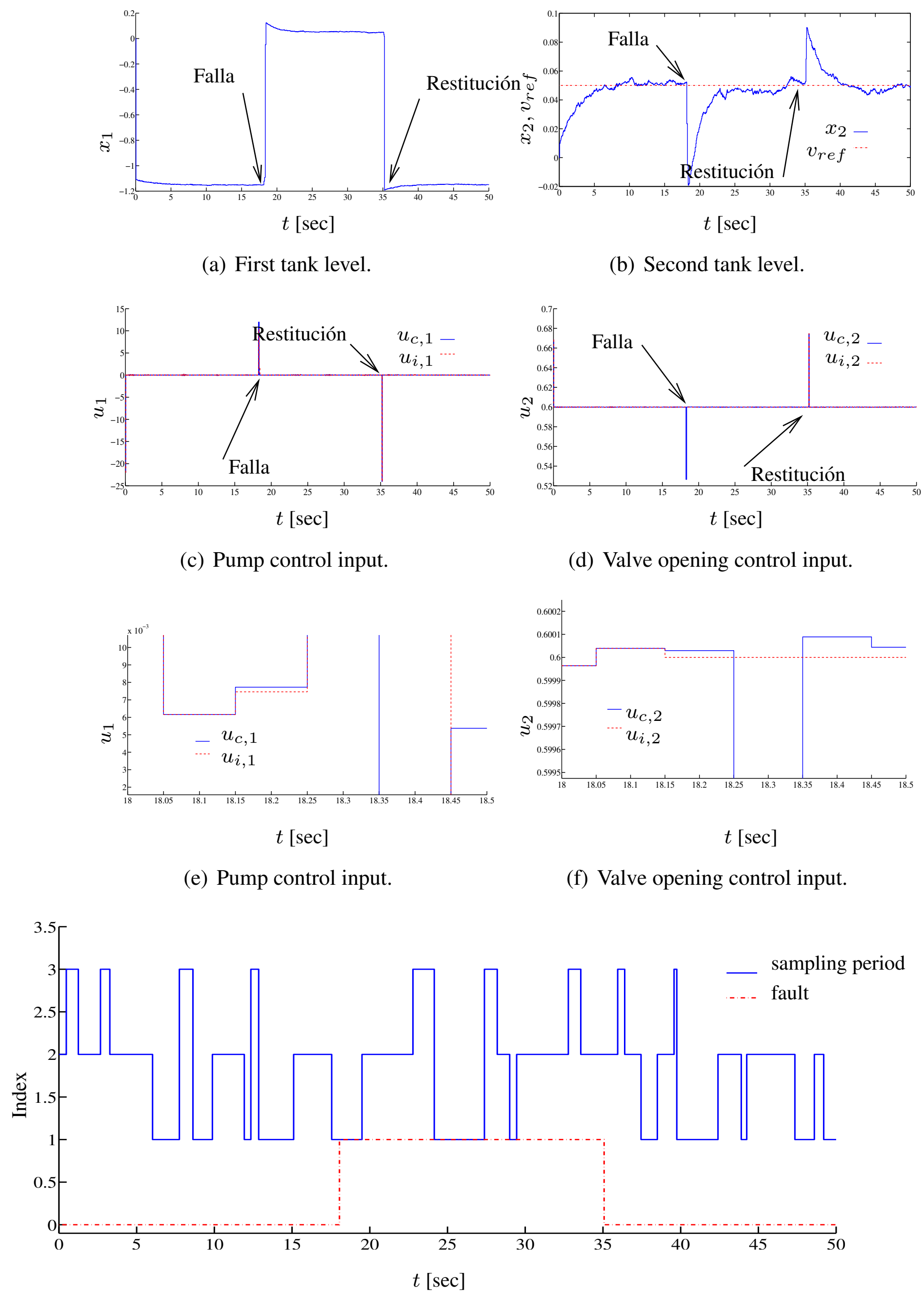
The computed residual signal values are shown in Fig. 3 (right). The residuals fall into $\mathcal{R}$ when the FDI matches the fault and after the corresponding variables have converged to their respective invariant sets (marked with triangles); at a fault instant the residual falls into one of the $\mathcal{R}^+_{01,h}$ sets (marked with a white $+$); and at the restitution instant, the residual falls into one of the $\mathcal{R}^+_{10,h}$ sets (marked with a white $*$).

7. CONCLUSIONS

In this paper we have presented a new approach for the virtual actuator technique under varying-sampling-rate control systems. In this approach, the controller (designed for the fault-free plant) is in charge of both providing the control action and determining the sampling instants to the continuous-time process. Such sampling period is informed to the FDI unit, and is selected from a finite set. The FDI mechanism computes a residual signal and checks membership of such signal to “correct-matching” or “fault-transition-matching” sets. The considered faults consist of abrupt actuator faults. The main results of this paper show that in the considered scheme and under persistent faults, the system will track the reference values, the control input will achieve its desired constant reference, the VA states will converge to a constant value (irrespective of the sampling period used, and the variations on it), and the desired constant setpoint tracking objective is ensured for the performance variable. In addition, reconfiguration is performed in at most 1 sampling period. The proposed approach is of particular interest for plants with input redundancy.

REFERENCES

1. P. Antsaklis and J. Baillieul. Guest Eds. Special issue on networked control systems. *IEEE Trans. on Aut. Control*, 49(9), 2004.
2. P. Antsaklis and J. Baillieul. Guest Eds. Special issue on technology of networked control systems. *Proc. of the IEEE*, 95(1), 2007.
3. L. Ben Jemaa and E.J. Davison. Performance limitations in the robust servomechanism problem for discrete-time LTI systems. *IEEE Transactions on Automatic Control*, 48(8):1299–1311, 2003.
4. A. Cervin, J. Eker, B. Bernhardsson, and K.-E. Arzen. Feedback-feedforward scheduling of control tasks. *Real-Time Systems*, 23:25–53, 2002.
5. T. Chen and B.A. Francis. *Optimal sampled-data control systems*. Springer-Verlag, 1995.
6. J. Daafouz, P. Riedinger, and C. Iung. Stability analysis and control synthesis for switched systems: A switched Lyapunov function approach. *IEEE Trans. on Aut. Control*, 47 No. 11:1883–1887, 2002.
7. L. Gurvits. Stability of discrete linear inclusion. *Linear Algebra and its Applications*, 231:47–85, 1995.
8. H. Haimovich and J.H. Braslavsky. Feedback stabilization of switched systems via iterative approximate eigenvector assignment. In *49th IEEE Conf. on Dec. and Control, Atlanta, GA, USA*, pages 1269–1274, 2010. Available at `arxiv.org`, doi arXiv:1009.2032.
9. H. Haimovich and J.H. Braslavsky. Sufficient conditions for generic feedback stabilizability of switching systems via Lie-algebraic solvability. *IEEE Trans. on Aut. Control*, 58(3):814–820, 2013.
10. H. Haimovich, J.H. Braslavsky, and F. Felicioni. Feedback stabilisation of switching discrete-time systems via Lie-algebraic techniques. *IEEE Trans. on Aut. Control*, 56(5):1129–1135, 2011.
11. H. Haimovich and E. Osella. On controller-driven varying-sampling-rate stabilization via Lie-algebraic solvability. *Nonlinear Analysis: Hybrid Systems*, 7(1):28–38, 2012.
12. H. Haimovich, E. N. Osella, and J. H. Braslavsky. On Lie-algebraic-solvability-based feedback stabilization of systems with controller-driven sampling. In *IFAC World Congress, Milano*, pages 8731–8736, 2011.



(a) First tank level.

(b) Second tank level.

(c) Pump control input.

(d) Valve opening control input.

(e) Pump control input.

(f) Valve opening control input.

(g) Sampling time index selection and failure status.

Figure 4. A difference between the computed control u_c and the effectively introduced to the plant u_i can be observed at the reconfiguration instant

13. H. Haimovich and M.M. Seron. Componentwise ultimate bound computation for switched linear systems. In *48th IEEE Conf. on Dec. and Control, Shanghai, China*, pages 2150 – 2155, 2009.
14. H. Haimovich and M.M. Seron. Componentwise ultimate bound and invariant set computation for switched linear systems. *Automatica*, 46:1897–1901, 2010.
15. Z. Ji, L. Wang, G. Xie, and F. Hao. Linear matrix inequality approach to quadratic stabilisation of switched systems. *IEE Proceedings: Control Theory and Applications*, 151(3):289–294, 2004.
16. D. Liberzon. *Switching in systems and control*. Boston, MA: Birkhauser, 2003.

17. H. Lin and P. J. Antsaklis. Stability and stabilisability of switched linear systems: a survey of recent results. *IEEE Trans. on Aut. Control*, 54(2):308–322, February 2009.
18. J. Lunze and T Steffen. Control reconfiguration after actuator failures using disturbance decoupling methods. *IEEE Trans. on Aut. Control*, 51(10):1590–1601, 2006.
19. R. J. McCloy, J.A. De Doná, and M.M. Seron. On the estimation of convergence times to invariant sets in convex polytopic uncertain systems. In *Australasian Conference on Artificial Life and Computational Intelligence, ACALCI, Newcastle, Australia*, Febraury, 2015.
20. A. P. Molchanov and Ye. S. Pyatnitskiy. Criteria of asymptotic stability of differential and difference inclusions encountered in control theory. *Systems and Control Letters*, 13(1):59–64, 1989.
21. E. Osella and H. Haimovich. Sufficient Lie-algebraic-solvability-based conditions for stabilization of VSR-DTSSs with two unstable eigenvalues. In *XIV RPIC*, pages 863–868, 2011.
22. E. Osella and H. Haimovich. An output feedback stabilization method for systems with controller-driven sampling. In *23 Congreso Argentino de Control Automático (AADECA), Buenos Aires, Argentina*, 2012.
23. E. Osella, H. Haimovich, and M. M. Seron. Virtual-actuator-based fault-tolerant control for systems with controller-driven sampling. In *XV RPIC*, 2013.
24. E. N. Osella, H. Haimovich, and M. M. Seron. Fault-tolerant control under controller-driven sampling using virtual actuator strategy. In *Australian Control Conference*, 2013.
25. J.H. Richter, W.P.M.H. Heemels, N. van De Wouw, and J. Lunze. Reconfigurable control of piecewise affine systems with actuator and sensor faults: Stability and tracking. *Automatica*, 47(4):678–691, 2011.
26. A. Sala. Computer control under time-varying sampling period: an LMI gridding approach. *Automatica*, 41(12)(12):2077–2082, 2005.
27. M. M. Seron, J. De Doná, and Jan H. Richter. Bank of virtual actuators for fault tolerant control. In *18th IFAC World Congress Milano (Italy) August 28 - September 2*, pages 5436–5441, 2011.
28. M.M. Seron and J.A. De Doná. Actuator fault tolerant multi-controller scheme using set separation based diagnosis. *International Journal of Control*, 83(10)(11):2328–2339, 2010.
29. M.M. Seron, J.A. De Doná, and S. Olaru. Fault tolerant control allowing sensor healthy-to-faulty and faulty-to-healthy transitions. *IEEE Transactions on Automatic Control*, 77(7):1657–1669, 2012.
30. R. Shorten, F. Wirth, O. Mason, K. Wulff, and C. King. Stability criteria for switched and hybrid systems. *SIAM Review*, 49(4):545–592, 2007.
31. Thomas Steffen. *Control Reconfiguration of Dynamical Systems*. Springer Berlin Heidelberg, 2005.
32. J. Theys. *Joint spectral radius: theory and approximations*. PhD thesis, Center for Systems Engineering and Applied Mechanics, Université catholique de Louvain, 2005.

DOI: 10.1002/acs