Int. J. Appl. Math. Comput. Sci., 2012, Vol. 22, No. 1, 125–137
DOI: 10.2478/v10006-012-0009-6

amcs

MODEL–FREE RECONFIGURATION MECHANISM FOR FAULT TOLERANCE

TUSHAR JAIN, JOSEPH J. YAMÉ, DOMINIQUE SAUTER

Research Centre for Automatic Control, CNRS UMR 7039, Faculty of Science and Technology
University of Lorraine, BP 239, 54506 Vandoeuvre-lés-Nancy Cedex, France
e-mail: {tushar.jain,joseph.yame,dominique.sauter}@cran.uhp-nancy.fr

The problem of fault tolerant control is studied from the behavioral point of view. In this mathematical framework, the concept of interconnection among the variables describing the system is a key point. The problem is that the behavior we intend to control is not known. Therefore, we are interested in designing a fault accommodation scheme for an unknown behavior through an appropriate behavioral interconnection. Here we deal simply with the trajectories that are generated by the system in real time. These trajectories determine the behavior of a system in various (faulty/healthy) modes. Based on the desired interconnected behavior, only the trajectories that obey certain laws are selected. These laws, representing the desired behavior, can indeed be achieved by a regular interconnection. Thus, when the trajectories do not belong to a certain desired behavior, it is considered to be due to the occurrence of a fault in the system. The vantage point is that the fault tolerant control problem now becomes completely a model-free scheme. Moreover, no explicit fault diagnosis module is required in our approach. The proposed fault tolerance mechanism is illustrated on an aircraft during the landing phase.

Keywords: fault tolerant control, control performance, behavioral theory, switching control.

1. Introduction

A *fault* represents an unexpected change in the system dynamics that tends to degrade the overall system performance and can lead to system instability as well. Generally, a *Fault Tolerant Control* (FTC) system includes two modules: the Fault Diagnosis (FD) module and the Fault Accommodation (FA) module (see Fig. 1). The former is a monitoring module that is used to detect faults and diagnose their location and significance in a system. The module with a fault estimation sub-module is very often regarded as Fault Detection and Isolation (FDI). The latter is a Fault-recovery module that controls the faulty system in a specific way, such that the system still achieves the objectives which were met by the healthy system before the occurrence of fault.

The general block diagram of a fault tolerant control is shown in Fig. 1. The main controller activities occur on the execution level. In the faultless case, the nominal controller attenuates the disturbance d and ensures set-point following and other requirements on the closed loop system on the execution level. On the supervision level, the diagnosis block simply recognizes that the closed-loop system is faultless and no change of the control law is necessary. If a fault occurs, the supervision level makes the control loop fault-tolerant. The diagnostic block identifies the fault and gives this information as D to the fault accommodation block. The FA module adjusts the controller to the new situation, such that the closed loop satisfies the performance specifications (Jain *et al*., 2010; Zhang and Jiang, 1999).

The problem of fault tolerant control is often handled in two ways, namely, using a model-based approach and a model-free approach. In the former the full information of the actual plant is known *a priori*. Accordingly, a subsystem (state observer, output observer, Kalman's filter, etc.) is built, which reconstructs the plant output and diagnoses the fault. The fault is then accommodated using the FA module. On the other hand, generally, in the so-called model-free approaches in the existing literature, the model of the plant is estimated. Nevertheless, the plant knowledge is required during estimation in real-time as well. Hence, the *knowledge of a plant model* is mandatory at any time to achieve fault tolerance either by assuming the plant model to be known or to be estimated. This entails the model mismatching issue that can generate *false alarms*, even in the faultless situation.

Consider the case of *disgraceful performance degradation* where control objectives are modified to achieve partial tolerance to a fault. This implies that after the accommodation of the fault, the current state of the plant still

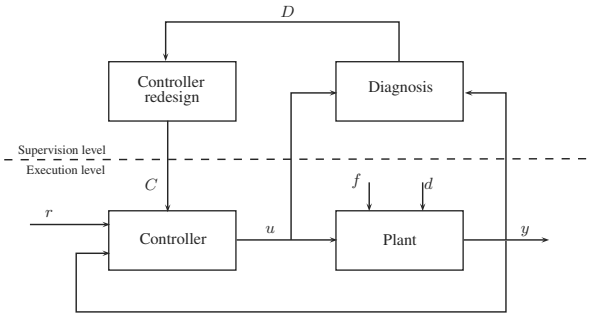

Fig. 1. Fault tolerant control architecture: r is a reference signal, u is the control signal, y is the output signal, f is a fault signal, d is a disturbance, D is the diagnosis information and C is the controller redesign information.

involves some dynamics of the fault in the faulty mode that have not been accommodated entirely. Therefore, the fault diagnosis module must be *adaptive* with respect to the fault accommodation module so that the further modeling issue can be averted. Otherwise, it will again result in a false alarm.

As we have seen, FTC requires two distinctive modules that operate sequentially to accommodate the fault. These two modules involve their respective time delays, particularly, known as *fault detection delay* and *fault accommodation delay*. Significant attention has to be paid while handling these time delays. In the time interval between the occurrence of a fault and its accommodation, the *stability aspects* of any FTC scheme become a concern. In addition, due to historical reasons and the complexity of the problem, most of the research on FD and FA was carried out in two directions. Specifically, most of the FDI techniques are developed as a diagnostic or monitoring tool, rather than an integral part of FTC systems. As a result, some existing FD methods may not satisfy the need of controller reconfiguration in the FA module. On the other hand, most of the research on reconfigurable controls is carried out assuming the availability of a perfect FD. Little attention has been paid to the analysis and design with the overall system structure and interaction between FD and FA modules (Zhang and Jiang, 2008).

Seeing these shortcomings, the objective of this work is to develop a generic method for fault tolerant control based on real trajectories from the system subjected to faults. The main aim of the paper is to formulate a model-free approach to FTC that does not require any information about the plant in *real-time*. Unlike in the so-called subspace approach for FTC by Ding *et al*. (2009), we do not focus on designing an FDI module that implicitly requires the knowledge of the plant parameters. On the contrary, our approach does not include any explicit FD module. The idea here is to choose an appropriate control law such that the system in any (faulty/healthy) mode

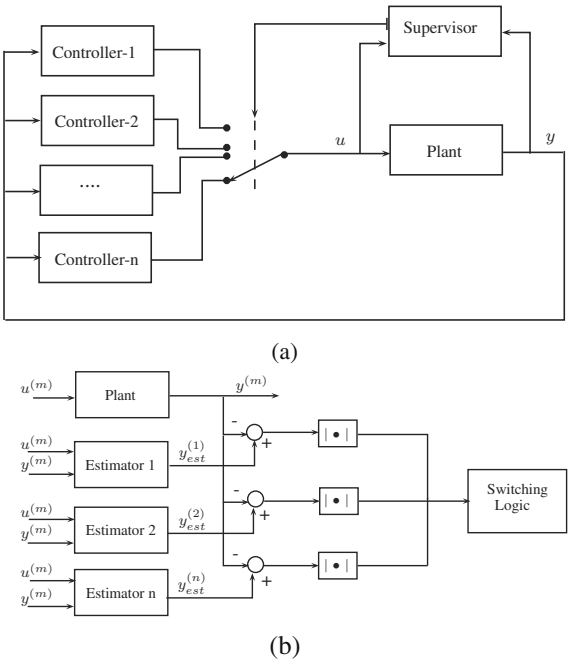

Fig. 2. Structure of a logic-based switching controller (a), structure of the supervisor (b).

achieves the performance specifications without the need for a plant model. We employed the mathematical framework of behavioral systems for the proposed approach. In the last decade, the behavioral point of view has received increasingly broader acceptance as an approach for modeling dynamic systems, and now it is generally viewed as a cogent framework for system analysis (Zerz, 2008). The proposed FTC mechanism is illustrated on an aircraft during the landing phase.

2. Active fault tolerant control strategy

In a model based fault tolerant control, it is generally that the primary aim is to estimate the constraints $\mathfrak{C}_{\mathfrak{f}}(\theta_{\mathfrak{f}})$ of the faulty system for the FD module. Based on this information, a new control law is applied in the fault accommodation phase such that the system satisfies the performance specifications. The scheme is termed *active fault tolerance*. On the contrary, in passive fault tolerance the control law is not redesigned subject to the occurrence of a fault. This implies that the system objectives can be obtained when the system is healthy, as well as when the system is faulty with the same control law. Hence, in the literature, passive FTC systems are also known as *reliable* control systems (Zhao and Jiang, 1998) or control systems with *integrity*.

Fault tolerant control is concerned with the control of a faulty system. This implies that we can regard any FTC problem as a control problem subject to the state of the system (healthy/faulty). The problem is completely

defined by the triple (Blanke *et al*., 2003)

$$\langle \mathfrak{O}, \mathfrak{C}(\theta), \mathfrak{U} \rangle, \tag{1}$$

where the objective $\mathfrak{O}$ defines what the system is expected to achieve. This implies that the system should satisfy certain performance specifications. The constraints $\mathfrak{C}$ are functional relations that depend on some parameter vector θ. The controlled system satisfies these constraints over time. This represents the state and measurement equations of an actual plant model in state space representation. The set $\mathfrak{U}$ represents admissible control laws. These control laws are designed so as to achieve the desired objective.

Now, let us analyze the impact of faults on the control problem. The occurrence of a fault on the system transforms the control problem from $\langle \mathfrak{O}, \mathfrak{C}_{\mathfrak{n}}(\theta_{\mathfrak{n}}), \mathfrak{U} \rangle$ into $\langle \mathfrak{O}, \mathfrak{C}_{\mathfrak{f}}(\theta_{\mathfrak{f}}), \mathfrak{U}_{\mathfrak{f}} \rangle, \mathfrak{f} \in \mathfrak{F}$, where $\mathfrak{F}$ indexes the set of all faults considered, $\mathfrak{C}_{\mathfrak{n}}(\theta_{\mathfrak{n}})$ is the set of nominal constraints with nominal system parameters, and $\mathfrak{C}_{\mathfrak{f}}(\theta_{\mathfrak{f}})$ is a set of faulty constraints with faulty system parameters. Generally, the occurrence of a fault does not result in a change of system objectives because the main idea of fault tolerant control is to try to reach them even in the presence of a fault. However, this may sometimes be impossible. In the case when current specified objectives cannot to be achieved, the problem is transformed into finding new objectives which are less restrictive such that the system still manages to satisfy the fault-tolerance property. This is known as *disgraceful degraded performance* in the FTC literature.

One of the active approaches to FTC is to employ switching theory that is based on constructing a bank of controllers, each controller being associated with a healthy or a faulty plant mode. The selection of a controller to be used for the present working mode is assumed to be achieved with some delay. The critical issue in any model-based Active FTC System (AFTCS) is the limited amount of time available for FD and for control system reconfiguration. The theory of logic based switching control provides a unique direction for AFTCS without using an explicit diagnosis module, which relies on a bank of controllers (Fig. 2 (a)).

The supervisor block shown in Fig. 2(b) is composed of a set of estimators, followed by the so-called performance evaluation block and a switching logic scheme. Each estimator reconstructs the actual plant output in either healthy or faulty working modes. Its performance is evaluated by computing a norm of the output estimation error, and the estimator that yields the smallest error corresponds to the present working mode. Consequently, the controller corresponding to the smallest value of the performance index is applied to the process by the switching logic. Here the notion of performance evaluation does not correspond to the closed loop system performance.

This approach has some shortcomings from a practical point of view. In the present configuration, the scheme presupposes that for each fault a reasonable controller has been designed before the plant is put into operation. However, the presence condition of a right controller is assumed in the controller bank. To build a set of estimators, partial or complete knowledge of the plant is required and, therefore, introducing model mismatch issues. In other words, the above scheme requires the knowledge of the plant model in real-time as well. Nevertheless, one cannot ignore the *role of gradual convergence* in the latter approach, required to estimate the current working mode. A notable feature of our proposed scheme is that it does not require an explicit fault diagnosis module in real-time.

3. FTC in the behavioral context

A mathematical model in the behavioral setting is viewed as any dynamical relation among system variables classified as *manifest variables* and *latent variables*. Indeed, the resulting dynamical relations are constrained by the time-evolution of these variables. Hence, the collection of all time trajectories satisfying these equations is called the *behavior*. When the trajectories do not belong to a specified desired behavior, the cause is the occurrence of a fault. The following gives a precise definition of the concept of a dynamical system.

Definition 1. A dynamical system Σ is represented by a triple $\Sigma = (\mathbb{T}, \mathbb{W}, \mathcal{B})$ where $\mathbb{T} \subseteq \mathbb{R}$ is called the time axis, $\mathbb{W} \subseteq \mathbb{R}^{\mathbf{w}}$ is called the signal space and $\mathcal{B} \subseteq \mathbb{W}^{\mathbb{T}}$ is called the behavior. A trajectory is a function

$$\mathbf{w} : \begin{cases} \mathbb{T} \to \mathbb{W}, \\ t \mapsto \mathbf{w}(t). \end{cases}$$

The set $\mathbb{W}$ is the space in which the system time-signals take on their values and the behavior $\mathcal{B} \subseteq \mathbb{W}^{\mathbb{T}}$ is a *family* of $\mathbb{W}$-valued time trajectories. Any behavior of a dynamical system is also represented by its kernel representation, $\mathcal{B} :\equiv P(\frac{\mathrm{d}}{\mathrm{d}t})\mathbf{w} = 0$, where $P \in \mathbb{R}^{\bullet \times \mathbf{w}}[\xi]$ and ξ is an indeterminate operator. By assuming this point of view, important aspects of the classical system theory have been translated and solved in the behavioral framework.

3.1. Control via system interconnection. In the behavioral setting, a control problem is viewed as an interconnection of two dynamical subsystems. These subsystems are the plant and the controller. Here we will consider the case of partial interconnection, which is different from the notion of full interconnection. The difference lies in the fact that in the latter all the variables are accessible for interconnection while in the former only few are available. Therefore, it is natural to separate the variable $\mathbf{w}$ as $\mathbf{w} := \begin{bmatrix} w & c \end{bmatrix}^T$, where w is the *manifest variable* and c is the *latent variable* (see Fig. 3(a)).

If $\Sigma_1 = (\mathbb{T}, \mathbb{W}, \mathcal{B}_1)$ and $\Sigma_2 = (\mathbb{T}, \mathbb{W}, \mathcal{B}_2)$ are two dynamical subsystems with the same time axis and same

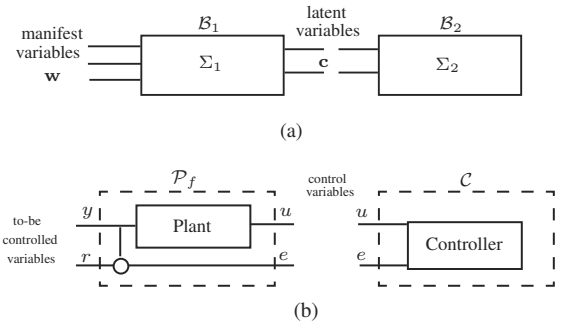

Fig. 3. Interconnection of subsystems (a), feedback control in the behavioral context (b).

signal space, then the interconnection of Σ_1 and Σ_2 shared by variable c, denoted as $\Sigma_1 \wedge_c \Sigma_2$, is defined as $\Sigma_1 \wedge_c \Sigma_2 := (\mathbb{T}, \mathbb{W}, \mathcal{B}_1 \wedge_c \mathcal{B}_2)$. Thus, the behavior of $\Sigma_1 \wedge_c \Sigma_2$ consists simply of those trajectories $w : \mathbb{T} \to \mathbb{W}$ which are compatible with both the laws of Σ_1 and of Σ_2. In a closed-loop feedback control, w and c are also termed *to-be controlled variables* and *control variables* (see Fig. 3(b)).

In the case of a Linear Time Invariant (LTI) system, there exist co-prime polynomials R_y and R_u such that $G = R_y^{-1} R_u$, where $G(\xi)$ is the rational representation of plant. In the behavioral context, a control problem is now formulated as follows. Assume that the plant, a dynamical subsystem $\Sigma_p = (\mathbb{T}, \mathbb{W}, \mathcal{P}_f)$ whose behavior is given by

$$\mathcal{P}_f = \{(w, c) \in \mathbb{R}^{q+p} \mid R(\xi)w = M(\xi)c\} \qquad (2)$$

with appropriate $R \in \mathbb{R}^{\bullet \times q}[\xi]$ and $M \in \mathbb{R}^{\bullet \times p}[\xi]$, where

$$\begin{bmatrix} R(\xi) & -M(\xi) \end{bmatrix} \begin{bmatrix} w(t) \\ c(t) \end{bmatrix} = 0,$$

is the kernel representation of the plant's behavior, $w := (r^T, y^T)^T, c := (e^T, u^T)^T$ and

$$R = \begin{bmatrix} 0 & R_y \\ 1 & -1 \end{bmatrix}, \quad M = \begin{bmatrix} 0 & R_u \\ 1 & 0 \end{bmatrix}.$$

Here $\mathcal{P}_f$ represents the full behavior of the plant, and the manifest behavior in to-be-controlled variables is given by

$$\mathcal{P} = \{w \in \mathbb{R}^q \mid \exists c \in \mathbb{R}^p \text{ such that } (w, c) \in \mathcal{P}_f\}. \qquad (3)$$

Similarly, for the controller, there exist co-prime polynomials C_e and C_u such that $C = C_e^{-1} C_u$, where $C(\xi)$ is the rational representation of the controller and its behavior is described as

$$\mathcal{C} = \{c \in \mathbb{R}^p \mid H(\xi)c = 0\}, \qquad (4)$$

with $H \in \mathbb{R}^{\bullet \times p}[\xi]$, where $H(\xi)c(t) = 0$ is the kernel representation. The interconnection between $\mathcal{P}_f$ and $\mathcal{C}$ results in a manifest controlled behavior, $\mathcal{K} = (\mathcal{P}_f \wedge_c \mathcal{C})_w$, defined as

$$\mathcal{K} = \{w \in \mathbb{R}^q \mid \exists c \in \mathcal{C} \text{ such that } (w, c) \in \mathcal{P}_f\}. \qquad (5)$$

Therefore, we say that $\mathcal{K}$ is implemented by $\mathcal{C}$, which (in connection with the hidden behavior $\mathcal{N}$) gives the implementability condition (Belur and Trentelman, 2002),

$$\mathcal{N} \subset \mathcal{K} \subset \mathcal{P}, \qquad (6)$$

where the hidden behavior is defined as the behavior consisting of plant trajectories with the interconnection variables put equal to zero. It is described as

$$\mathcal{N} = \{w \in \mathbb{R}^q \mid (w, 0) \in \mathcal{P}_f\}.$$

Let us present an example of a control problem in the behavioral framework.

Example 1. Given a plant

$$G(\xi) = \frac{\xi - 1}{\xi(\xi + 1)}$$

and the controller

$$C(\xi) = -\frac{\xi + 1}{\xi + 2.6},$$

find the controlled behavior $\mathcal{K}$.

We get

$$\frac{y}{u} = \frac{\xi - 1}{\xi(\xi + 1)} = \frac{R_u(\xi)}{R_y(\xi)},$$

$$[\xi(\xi + 1)]y + (-\xi + 1)u = 0,$$

$$e = r - y,$$

$$\mathcal{P}_f := \begin{bmatrix} 1 & -1 & -1 & 0 \\ 0 & \xi^2 + \xi & 0 & -\xi + 1 \end{bmatrix} \begin{bmatrix} r \\ y \\ e \\ u \end{bmatrix} = 0.$$

For the controller $C(\xi)$, we obtain

$$\frac{u}{e} = -\frac{\xi + 1}{\xi + 2.6} = \frac{C_u}{C_e},$$

$$(\xi + 1)e + (\xi + 2.6)u = 0,$$

$$\mathcal{C} := \begin{bmatrix} 0 & 0 & \xi + 1 & \xi + 2.6 \end{bmatrix} \begin{bmatrix} r \\ y \\ e \\ u \end{bmatrix} = 0,$$

$(\mathcal{P}_f \wedge_c \mathcal{C})_w$:

$$= \begin{bmatrix} 1 & -1 & -1 & 0 \\ 0 & \xi^2+\xi & 0 & -\xi+1 \\ 0 & 0 & \xi+1 & \xi+2.6 \end{bmatrix} \begin{bmatrix} r \\ y \\ e \\ u \end{bmatrix} = 0.$$

From (6) $\mathcal{K}$ is a restricted behavior in $\mathcal{P}$ and $\mathcal{K} = (\mathcal{P}_f \wedge_c \mathcal{C})_w$ (Polderman and Willems, 1997, Sec. 6.2.3), and hence there must exist an unimodular matrix. The greatest common divisor of $R_u(\xi)$ and $C_e(\xi)$ is 1. Using the Bezout identity, there exist polynomials $a(\xi)$ and $b(\xi)$ such that $a(\xi) \cdot R_u(\xi) + b(\xi) \cdot C_e(\xi) = 1$. Define unimodular matrices $U_1(\xi)$, $U_2(\xi)$ as follows:

$$U_1(\xi) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \xi+1 & 0 & 1 \end{bmatrix},$$

$$U_2(\xi) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a(\xi) & b(\xi) \\ 0 & \xi+2.6 & \xi-1 \end{bmatrix}$$

Here

$$a(\xi) = -\frac{1}{3.6}, \quad b(\xi) = \frac{1}{3.6}.$$

We easily check that

$$U_2(\xi)U_1(\xi) \begin{bmatrix} 1 & -1 & -1 & 0 \\ 0 & \xi^2+\xi & 0 & -\xi+1 \\ 0 & 0 & \xi+1 & \xi+2.6 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -1 & -1 & 0 \\ \frac{\xi+1}{3.6} & -\frac{(\xi+1)^2}{3.6} & 0 & \frac{\xi+0.8}{1.8} \\ \xi^2-1 & (\xi+1)(\xi^2+1.6\xi+1) & 0 & 0 \end{bmatrix},$$

$$\mathcal{K} := \begin{bmatrix} 1 & -1 & -1 & 0 \\ \frac{\xi+1}{3.6} & -\frac{(\xi+1)^2}{3.6} & 0 & \frac{\xi+0.8}{1.8} \\ \xi^2-1 & (\xi+1)(\xi^2+1.6\xi+1) & 0 & 0 \end{bmatrix} \times \begin{bmatrix} r \\ y \\ e \\ u \end{bmatrix} = 0. \tag{7}$$

Here we see that the relation between r and y is given by the third row in the above equation. ♦

In this framework, the control problem is also formulated as finding a controller $\mathcal{C}$ that yields a *desired controlled behavior* $\mathcal{D}$. Hence the controller $\mathcal{C}$ should yield a *controlled behavior* $\mathcal{K}$ such that $\mathcal{K} \subseteq \mathcal{D}$. If it is possible to find a controller $\mathcal{C}$ that yields $\mathcal{K} \subseteq \mathcal{D}$, then $\mathcal{D}$ is said to be *implementable* or *implemented* by $\mathcal{C}$. Further, if a given desired behavior $\mathcal{D}$ is implementable, we say that 'the control problem is solvable'. Polderman (2000) proposed that, for a given control objective, we must *select* a desired behavior to design a controller such that the control objectives are satisfied, while Weiland *et al*. (1997) proposed that, for a given control objective, there *exists an equivalent* desired behavior to design a controller such that the control objectives are satisfied. These two investigations were generally formalized as a single entity by van der Schaft (2003) to design a controller based upon the desired behavior. This controller is termed the *canonical controller*, irrespective of the control objective. Therefore, we can regard the desired behavior $\mathcal{D}$ as equivalent to the control objective $\mathfrak{O}$.

3.2. Switching control in the behavioral context. The theory of switching control relies on constructing a bank of controllers. Adopting a well-defined switching algorithm, one of the controllers in the bank is selected such that the control objectives are satisfied. In the analysis and development phase, it has been assumed that a finite set of controllers

$$\mathbf{C} = \{C_1, C_2, \ldots, C_N\} \tag{8}$$

is constructed in such a way that in every situation, either a healthy or faulty mode of the plant, there is at least one controller in that set which has the appropriate control action and is able to satisfy the control objectives. The notion of directability in the behavioral framework precisely describes the existence of a controller bank. A definition of *weak directability* is given below (Polderman and Willems, 1997).

Definition 2. Let $w_1, w_2 \in \mathcal{B}$ and $t \in \mathbb{T}$. We say that w_1 *is weakly directable to* w_2 at time t'' if there exists a trajectory $w_3 \in \mathcal{B}$ and a $t' \leq t''$ such that

$$w_3(t) = \begin{cases} w_1(t), & t \leq t', \\ w_2(t), & t > t''. \end{cases}$$

In the above definition, the trajectories before t' belong to an undesired behavior. Therefore, satisfying the weak directability on the plant ensures that it is possible to switch the trajectory at any time t' such that it achieves the desired behavior after time t'', introducing some time delay.

Remark 1. The notion of directability is stronger than Definition 2. Unlike weak directability, the interconnected system satisfying directability does not allow any time-delay while switching to the desired trajectory. If the interconnected system is weakly directable, then it is equivalent to say that there must exist a controller such that $\mathcal{K} \subseteq \mathcal{D}$.

Interestingly, the behavior we intend to control is of the form given by (2). The matrices of polynomials $R(\xi)$ and $M(\xi)$ are unknown. Once a fault occurs, the behavior of the closed loop becomes inconsistent with respect to the

desired behavior, and it must be compensated by making an interconnection with another controller (compensator).

A compensator is a set of laws that restrict the interconnection variable c and therefore w. Beyond any doubt, the measurements provide information about a dynamical system. These measurements give partial knowledge about the systems and might be thought of as representing a small set of the behavior of a dynamical system. This can be formalized by viewing these measurements, collected over time τ, as a nonempty subset $\mathcal{M}$ of $\mathbb{W}^{\mathbb{T}}$. Polderman (2000) uses a somewhat similar explanation relying only on the measurements taken from a dynamical system. In that explanation, each time a measurement is completed, a model from that measurements is derived using an iterative algorithm. A controller is then *generated* so that the interconnection satisfies the control objective for that particular derived model. This model is known as the *Most Powerful Unfalsified Model* (MPUM). A formal definition of measurements illustrating the plant behavior (Willems, 1986) is given as follows.

Definition 3. Given a vector space of time signals $\mathbb{W}^{\mathbb{T}}$, a model or dynamical system $\Sigma_p = (\mathbb{T}, \mathbb{W}, \mathcal{P}_f)$, a mapping $\mathsf{O}_\tau : \mathbb{W}^{\mathbb{T}} \to \mathbb{W}^{\mathbb{T}}$ and a measurement set $\mathcal{M}_\tau \subset \mathsf{O}_\tau(\mathbb{W}^{\mathbb{T}})$, we say that the behavior $\mathcal{P}_f$ is said to be *unfalsified* by the measurement set $\mathcal{M}_\tau$ if

$$\mathcal{M}_\tau \subset \mathsf{O}_\tau(\mathcal{P}_f),$$

where $\mathsf{O}_\tau(x)$ is the experimental observation time sampling operator defined by

$$[\mathsf{O}_\tau(x)](t) = \begin{cases} x(t), & t_a - \tau \le t < t_a\,, \\ 0, & \text{otherwise,} \end{cases}$$

where t_a is arbitrary current time. Thus $\mathsf{O}_\tau(x)$ returns values of $x(t)$ only for past time intervals over which experimental observations of $x(t)$ have been recorded. The measurement set $\mathcal{M}_\tau$ is the set of actual experimental observations of the plant behavior as observed through the time sampler O_τ. Thus, $\mathsf{O}_\tau^{-1}(\mathcal{M}_\tau)$ is a behavior that interpolates the observed data during the time interval τ.

Definition 4. Given a vector space of time signals $(\mathbb{T} \times \mathbb{W})$, a controller $\Sigma_c = (\mathbb{T}, \mathbb{W}, \mathcal{C})$, a desired behavior $\mathcal{D}$, a mapping $\mathsf{O}_\tau : \mathbb{W}^{\mathbb{T}} \to \mathbb{W}^{\mathbb{T}}$ and a measurement set $\mathcal{M}_\tau \subset \mathsf{O}_\tau(\mathbb{W}^{\mathbb{T}})$, we say that a controller Σ_c is unfalsified by the measurement set $\mathcal{M}_\tau$ if

$$\mathsf{O}_\tau(\mathsf{O}_\tau^{-1}(\mathcal{M}_\tau)) \wedge_c \mathcal{C}) \subset \mathsf{O}_\tau(\mathcal{D}),$$

where $\mathsf{O}_\tau^{-1}(\mathcal{M}_\tau)) \wedge_c \mathcal{C} = \mathcal{K}$. Definition 4 supposes roughly that a controller, whose behavior is denoted by $\mathcal{C}$, is said to be unfalsified if the set of trajectories that are consistent with the data and the controller, at the past observation times, is a subset of the desired set $\mathsf{O}_\tau(\mathcal{D})$. As we are working in real time, introducing the time sampling operator is justified.

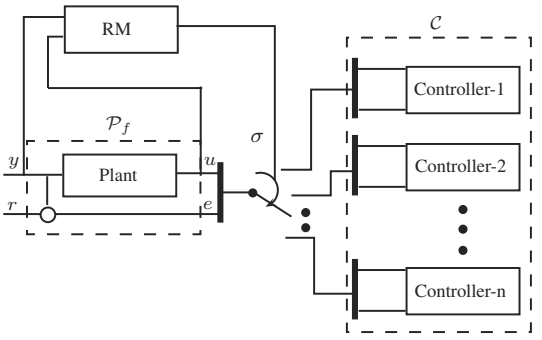

Fig. 4. Switching control scheme for FTC in the behavioral setting.

Remark 2. The underlying idea of utilizing the behavioral approach is that it captures the behavior of the plant without any explicit modeling. In Definition 4, the trajectories collected over an interval τ determine the behavior of the plant. Later, we shall show that the performance of the closed loop is analyzed as well during this interval only.

Consider the architecture of switching control for FTC in the behavioral setting as shown in Fig. 4, the supervisor or Reconfiguration Mechanism (RM) manages the switching of controllers from the set given in (8) into feedback with the plant such that the closed loop satisfies the control objective despite the occurrence of a fault. From the FTC problem (1), when a fault occurs, it converts the control problem from $\langle \mathfrak{O}, \mathfrak{C}_{\mathfrak{n}}(\theta_{\mathfrak{n}}), \mathfrak{U} \rangle$ into $\langle \mathfrak{O}, \mathfrak{C}_{\mathfrak{f}}(\theta_{\mathfrak{f}}), \mathfrak{U}_{\mathfrak{f}} \rangle, \mathfrak{f} \in \mathfrak{F}$ where $\mathfrak{F}$ indexes the set of all faults considered. Constraints $\mathfrak{C}(\theta)$ in any mode (healthy/faulty) are unknown.

The RM performs a *when-which* task that implies when to change the control law and which controller should be switched into feedback with the evolving plant. From the hypothesis of the existence of at least one corrective controller in the pre-designed set (8) for the faults occurring in the plant and taking Definition 4 into account, a simple conceptual solution to the controller selection would be to evaluate experimentally each candidate controller's performance by applying it to the plant. Unfortunately, not all the potential controllers can be tested simultaneously in the feedback loop. To overcome this situation, the idea of identifying directly the right corrective controller to be switched into the feedback loop using only the experimental information up to the current time would be appealing. The problem amounts to inferring the closed loop behavior from the observed data produced by the plant driven by a different controller.

Moreover, without further modeling assumptions on the plant Σ_p, it is logically impossible to verify that a controller Σ_c will implement an interconnected system $\mathcal{K}$ that achieves the desired behavior $\mathcal{D}$. Thus we provide a bound

on the time of a controller to be present in the closed loop so that its performance can be analyzed during that time interval. The controller will be provisionally retained as the best available controller until it is falsified (or rejected) or possibly outmoded by a better controller present in the bank. As in real time operation, it is impossible to foresee the realization of the desired behavior by a closed loop system, unless we know the model of the plant. Whenever the controller is not rejected by the experimental data, it is said to be *unfalsified*. This formulation is based on an approach which is popularly known as the unfalsified control concept (Safonov and Tsao, 1997).

Notice that the observed data $\mathcal{M}_\tau$ are not related to any particular experimental setting. Hence a deep consequence of Definition 4 is that the controller Σ_c can be tested, even if it is not actually interconnected to the plant. This fact is a powerful tool for evaluating the ability of an off-the-shelf controller to perform corrective actions and satisfy the performance objective following an unexpected change in a feedback loop. Weiland *et al*. (1997) formalize the desired or acceptable behavior with the notion of control objective as follows.

Definition 5. A control objective is a quadruple $\mathfrak{O} = (\mathcal{R}_{\min}, \mathcal{S}_{\min}, \mathcal{R}_{\max}, \mathcal{S}_{\max})$ of subsets of $\mathbb{W}^{\mathbb{T}}$. A controller Σ_c is said to achieve the control objective $\mathfrak{O}$ for the interpolated plant behavior $\mathsf{O}_\tau^{-1}(\mathcal{M}_\tau)$ if the behavior $\mathsf{O}_\tau(\mathcal{K})$ satisfies the inclusions

$$\mathsf{O}_\tau(\mathcal{S}_{\min}) \subseteq \mathsf{O}_\tau(\mathcal{K}) + \mathsf{O}_\tau(\mathcal{R}_{\min}), \tag{9}$$

$$\mathsf{O}_\tau(\mathcal{K}) \cap \mathsf{O}_\tau(\mathcal{R}_{\max}) \subseteq \mathsf{O}_\tau(\mathcal{S}_{\max}). \tag{10}$$

The control objective $\mathfrak{O}$ from (1) specifies the desired behavior. It is specified in terms of a *minimal* and a *maximal* requirement on the behavior of the controlled system. Thus we call (9) a minimal and (10) a maximal requirement for $\mathsf{O}_\tau(\mathcal{K})$. Roughly speaking, the minimal requirement formalizes the idea that $\mathsf{O}_\tau(\mathcal{K})$ should be "sufficiently rich" so that a suitable extension of this system contains at least a specified set of trajectories (such as disturbances, reference trajectories or norm-bounded signals). The maximal requirement articulates the performance of the system.

Definition 6. Given $\mathcal{L}_2^+$, the space of square integrable trajectories which vanish for $t < 0$, the truncated $\mathcal{L}_2$ inner-product $\langle \mathbf{w}_1, \mathbf{w}_2 \rangle_\tau$ and norm $\|\mathbf{w}\|_\tau$ are denoted by

$$\langle \mathbf{w}_1, \mathbf{w}_2 \rangle_\tau \triangleq \int_t^{t+\tau} \mathbf{w}_1^T(t)\mathbf{w}_2(t)\,\mathrm{d}t,$$

$$\|\mathbf{w}\|_\tau \triangleq \sqrt{\langle \mathbf{w}, \mathbf{w} \rangle_\tau},$$

where $\mathbf{w} : \mathbb{R} \to \mathbb{R}^q$.

Let $Q = Q^T$ be a real symmetric full rank indefinite $q \times q$ matrix and suppose that

$$Q = Q_+ - Q_-,$$

where $Q_+ \geq 0$ and $Q_- \geq 0$ are such that $q_+ := \text{ rank } Q_+$ and $q_- := \text{ rank } Q_-$ satisfy $q_+ + q_- = q$. Given such a Q, the control objective is defined by the quadruple

$$\mathcal{R}_{\min} := Q_- \mathcal{L}_2^+, \tag{11}$$

$$\mathcal{S}_{\min} := \mathcal{L}_2^+, \tag{12}$$

$$\mathcal{R}_{\max} := \mathcal{L}_2^+, \tag{13}$$

$$\mathcal{S}_{\max} := \{\mathbf{w} \in \mathcal{L}_2^+ \mid J(\mathbf{w}) \equiv \langle \mathbf{w}, Q\mathbf{w} \rangle \geq 0\}, \tag{14}$$

where $J(\mathbf{w})$ is the performance index.

Let $\mathbf{w}$ be partitioned as

$$\mathbf{w} := \begin{bmatrix} r & u & y \end{bmatrix}^T \in \mathbb{W}^{\mathbb{T}},$$

where r has dimension $n_r > 0$, u has dimension $n_u > 0$, y has dimension $n_y > 0$ and $n_{\mathbf{w}} = n_r + n_u + n_y$. The $\mathcal{H}_\infty$ control problem amounts then to finding a controller which, when connect in the closed-loop, makes the system stable and satisfying

$$\lambda^2\|r\|_\tau^2 - \|u\|_\tau^2 - \|y\|_\tau^2 = \left\langle \begin{bmatrix} r \\ u \\ y \end{bmatrix}, \begin{bmatrix} \lambda^2 I_{n_r} & 0 & 0 \\ 0 & -I_{n_u} & 0 \\ 0 & 0 & -I_{n_y} \end{bmatrix} \begin{bmatrix} r \\ u \\ y \end{bmatrix} \right\rangle_\tau \geq 0, \quad \forall \mathbf{w} \in \mathcal{L}_2^+, \tag{15}$$

where the constant $\lambda > 0$ is an upper bound of the $\mathcal{H}_\infty$ norm of the closed loop transfer function (see Grimble, 1993, Chapter 3).

Now we proceed with the controller falsification test. For an unknown dynamical system $\Sigma_p = (\mathbb{T}, \mathbb{W}, \mathcal{P}_f)$, named the plant, we have a set of measurements $\mathcal{M}_\tau$ during the time interval τ composed of trajectories u and y such that $\mathsf{O}_\tau^{-1}(\mathcal{M}_\tau) \subseteq \mathcal{P}_f$, where

$$\mathcal{M}_\tau = \{(r, u, y) \in \mathsf{O}_\tau(\mathbb{W}^{\mathbb{T}}) \mid u = u^{(m)}, y = y^{(m)}\}, \tag{16}$$

with $\mathbb{W}^{\mathbb{T}} = \mathcal{R} \times \mathcal{U} \times \mathcal{Y}$, for some

$$(u^{(m)}, y^{(m)}) \in \mathsf{O}_\tau(\mathcal{U} \times \mathcal{Y}).$$

In other words, $(u^{(m)}, y^{(m)})$ is the data measured during τ. The performance evaluation of a controller C_k based on the measurement set $(u^{(m)}, y^{(m)})$ proceeds as follows. The behavior of the controller C_k is given by

$$\mathcal{C}_k = \{\mathbf{w} := (r, u, y) \in \mathbb{W}^{\mathbb{T}} \mid u(t) = C_k(r(t) - y(t))\}, \tag{17}$$

so that, based on the measurements, the signal r should have been

$$r_k(t) = C_k^{-1}u^{(m)}(t) + y^{(m)}(t) \tag{18}$$

for $t_a - \tau \leq t \leq t_a$, where we have assumed that all the controllers in the set are Stable Causally Left Invertible (SCLI) controllers. Note that this assumption is not

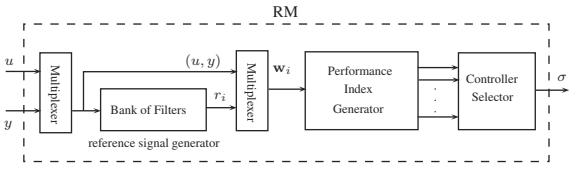

Fig. 5. Structure of the reconfiguration mechanism.

restrictive since the controllers can be designed to be biproper. Alternatively, in order to avoid the restriction to the minimum phase (SCLI) controllers, we can use the Matrix Fraction Description (MFD) form (Stefanovic and Safonov, 2008) for the controllers.

The signal $\mathbf{w}_k = (r_k, u^{(m)}, y^{(m)}) \in \mathbb{W}^{\mathbb{T}}$ on the time interval $[t_a - \tau, t_a]$ clearly belongs to the controller behavior $\mathcal{C}_k$ as well as to $\mathsf{O}_\tau^{-1}(\mathcal{M}_\tau)$, i.e., $\mathbf{w}_k \in \mathsf{O}_\tau(\mathcal{C}_k \wedge_c \mathsf{O}_\tau^{-1}(\mathcal{M}_\tau))$. From Definition 4, a controller C_k is unfalsified by the experimental measurements $\mathcal{M}_\tau$ generated by an unknown plant whenever $\mathbf{w}_k \in \mathsf{O}_\tau(\mathcal{D})$, i.e., the feedback loop with the current controller satisfies the control objective $\mathfrak{O}$ at $\mathbf{w}_k \in \mathbb{W}^{\mathbb{T}}$ for a certain value of λ. We denote by $\mathfrak{O}^{\mathbf{w}_i}$ the control objective $\mathfrak{O}$ at $\mathbf{w}_i$. Equation (18) defines a filter F_k that reconstructs the reference signal r_k from the measurements of (u, y) (Yamé and Sauter, 2008). The above procedure can also be applied to any off-the-shelf controller in the set (8) of N potential candidate controllers, thus yielding N performance indexes,

$$\{J(\mathbf{w}_i), i = 1, 2, \ldots, N\}. \tag{19}$$

The unfalsified controllers are those controllers with index i that satisfy the control objective $\mathfrak{O}^{\mathbf{w}_i}$ for a certain value of λ. These performance indexes facilitate the selection of right unfalsified controller that can switch into the loop. The explicit structure of the reconfiguration mechanism consists of a bank of filters (18), a performance index generator producing the indexes (19), and a controller selector block as shown in Fig. 5. The controller selector block is a system that produces a piecewise constant signal (the switching signal) σ based on $\{J(\mathbf{w}_i)\}_{i=1}^N$ whose task is to select the corrective controller from the bank. The switching signal is a map from the time axis $\mathbb{T}$ to the controllers index set $\{1, 2, \ldots, N\}$, i.e., $\sigma : \mathbb{T} \to \{1, 2, \ldots, N\}$.

As we have mentioned earlier, we take the measurements and scrutinize the performance index on the time interval $[t_a - \tau, t_a]$. This implies that, if it requires switching of the controller, the switch will occur after time τ exclusively. Therefore, it imposes a lower bound on the length of intervals between successive switches. This minimum length of time in which a controller is active in the loop is known as the *dwell time*. The logic is then realized through

$$\sigma(t) = \sigma(t_a) \quad \text{for } t_a \le t < t_{a+1} \tag{20}$$

with an updating rule (21), where $\hat{k}$ is the index of a to-be-switched controller. The controller selector block contains the control selection algorithm given in (20) and (21). The switching logic implements the following: It lets the stable dynamics of the closed-loop switched system have enough time to decay before a next possible switching occurs, and it bounds the detection delay, i.e., the time elapsed from the occurrence of a fault to the invalidation of the active controller. Note that a short detection delay requirement will need a short dwell-time that clearly conflicts with the stability of the closed-loop switched system. Moreover, Wang and Safonov (2005) prove and Baldi *et al*. (2010) experimentally illustrate that the unfalsified control concept cannot prevent the destabilizing controller to be switched in the feedback loop. This implies that the switching signal $\sigma \in \{1, 2, \ldots, N\}$ follows a certain switching order before selecting the right controller. Hence, the corrective controller will not be switched directly in the loop. Therefore, any destabilizing controller is expected to remain in the loop during the time interval τ. This also infringes the stability of the switching system. Thus here we see that the stability of the closed loop conflicts for two reasons: (a) due to the short dwell time that may lead to multiple switching, (b) due to the impact of a destabilizing controller operating in the closed loop during the time interval τ.

For (b), we can assume that the controllers installed in the bank are stabilizing for at least one working mode of the plant. For the latter case, we do not consider the multiple switching any more. Since it is well known that the large dwell time itself ensures the global exponential stability (Morse, 2008), these stabilizing controllers correspond to the modes, i.e., there always exist at least one plant/controller stable interconnection. Reacting to these issues, a lower bound to τ should be imposed to ensure the exponential stability of the overall switched system (Morse, 2008, Lemma 1.1). As a result, a lower bound on the dwell time is also determined in the analysis and development phase.

As we have mentioned, for a fixed short dwell time, there will be multiple switchings in the system. On the other hand, a fixed large dwell time can lead to the second stability issue. Therefore, in much the same way as in the work of Stefanovic and Safonov (2008), the dwell time must be adaptive with the evolving time. Stefanovic and Safonov (2008) discuss the finiteness of the overall number of switches in the case of multiple switchings and develop a bound on it that depends on the data. Since it is also proven that the final controller will be the corrective one, which implies that the number of switches would be some finite value and hence there could be a set of data for which the number of switches can be arbitrarily large (though finite). Nevertheless, this situation depends on the switching algorithm and the evaluation of the performance functional. Adopting a more precise view

$$\sigma(t_{a+1}) = \begin{cases} \sigma(t_a), & \text{if } C_{\sigma(t_a)} \text{ is not falsified,} \\ \hat{k} = \arg \min\limits_{k \neq \sigma(t_a)} \{J(\mathbf{w}_k)\}, & \text{if } \mathfrak{O}^{\mathbf{w}_k} \text{ is not satisfied for some value of } \lambda. \end{cases} \tag{21}$$

of Stefanovic and Safonov (2008), the performance of all the controllers is evaluated on the whole time axis, starting from the origin to the current time. In the switching algorithm the performance functional is evaluated for all the controllers, even if it has already been falsified. However, in our switching algorithm, the correct controller is selected in one shot.

As mentioned before, we evaluate the performance in a fixed time window, and thus the evaluation of the dwell time of Morse (2008, Lemma 1.1) considers the fact that the right controller is identified. Moreover, for the stability of the overall system, the performance index should reflect any instability taking place in the closed loop. This feature is termed *cost-detectability* (Stefanovic and Safonov, 2008), which is different from plant detectability. At the same time, cost-detectability is determined from the knowledge of the performance index and the candidate controllers, based upon the trajectories generated by the system in real time. The formal definition is as follows.

Definition 7. Let $\mathbf{w}_i^m = (r, u^m, y^m)$ denote the measured trajectories and $J(\mathbf{w}_i)$ denote the performance index with the i-th controller C_i as the current controller. The set $\{J(\mathbf{w}_i)\}_{i=1}^N$ is said to be cost-detectable if, without any assumption on the plant and for every $i \in \{1, 2, \ldots, N\}$, the following statements are equivalent:

1. $J(\mathbf{w}_f^m)$, where $f \in \{1, 2, \ldots, N\}$ is bounded as t increases to infinity, where the index f corresponds to the final corrective controller;

2. the control objective $\mathfrak{O}$ of the system $\mathsf{O}_\tau^{-1}(\mathcal{M}_\tau))\wedge_c\mathcal{C}$ is satisfied by the trajectory $\mathbf{w}_i^m$ for some value of λ.

From Definition 7, it is now clear that any *unpermitted* behavior in the closed loop will be reflected by the performance index evaluation. The proposed algorithm to achieve real-time fault tolerant control is illustrated in Fig. 6. The following theorem provides the main result.

Theorem 1. *Let $\mathcal{D}$ be the desired behavior that captures the control objective $\mathfrak{O}$ (Definition 5) using a cost-detectable performance functional $J(\mathbf{w})$ (Definition 7), τ be the interval during which the behavior of plant is determined, and the interconnection between the plant and the controller assumed to be weakly directable (Definition 2). For any system with $\sigma(t)$ selected in accordance with (20) and (21), the following statements are equivalent:*

- *with any occurrence of unpermitted behavior, the system is fault-tolerant;*

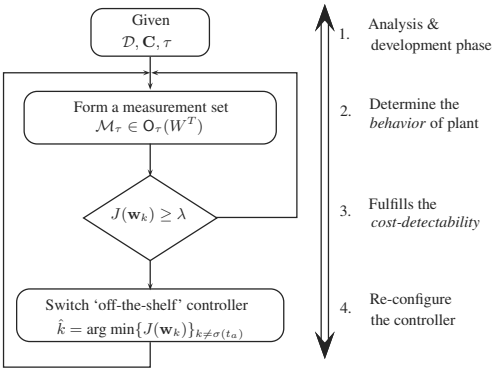

Fig. 6. Proposed algorithm.

- *global stability of the final interconnected system is assured by the experimental measurement set $\mathcal{M}_\tau$.*

Proof. See Appendix. ■

Note that here we provided the 'logic-based switching' mechanism contrary to the switching criterion dealt with by Yang *et al*. (2009), who used the so-called continuous arbitrary switching criterion. Certainly, with a periodic switching law the stability issue during the switching becomes a concern. It is studied by Hespanha *et al*. (2003) that the limitations often seen in an arbitrary switching are successfully overcome in a logic-based switching.

4. Simulation example

In this section, we show an application of the proposed approach to constructing the autopilot mechanism for an aircraft during the landing phase (Oishi *et al*., 2002). The auto-landing system of the modern aircraft is supposed to follow a certain trajectory called glide-slope. The landing of a civil transport aircraft is divided into three parts, namely, approaching a trajectory, flare, and touchdown and ground run. Figure 7 shows the aircraft in a certain trajectory-approaching phase, which constitutes the final phase of the descent (i.e., the glide-slope). The Instrument Landing System (ILS) on ground determines the difference between the actual trajectory of the aircraft and the reference trajectory imposed for the descent. Here the purpose is to design a fault tolerant autopilot that fully supports the conduct of the flight in the vertical plane along the glide scope. In these simulations, we ignored the lateral movement and rolling movements of the aircraft assuming that these aspects are handled by another automated system.

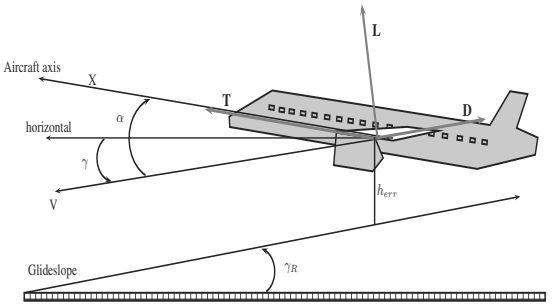

Fig. 7. Aircraft during the landing phase.

For the problem considered (longitudinal flight), the aircraft is seen as a system with three outputs that are measured in real-time: the speed V, the angle γ of the flight path, and the distance from the center of mass of the aircraft relative to the glide-slope h_{err}. The control inputs of the system are the aircraft thrust T and the elevator command δ (Oishi *et al.*, 2002). The elevator is a movable aerodynamic surface located in the empennage that controls the pitch of the aircraft. We assume there are no dynamics between the elevator command and the angle of attack α of the wing. Thus, we view α as equivalent to δ, and consequently, for the sake of simplicity, we treat α as a control input. The thrust controls the speed V of the aircraft. The objective is that the aircraft follows along the glide–slope, making a desired flight path angle at 3 degrees clockwise (i.e., $\gamma_r = -3\,\text{deg}$). Thus, it makes h_{err} zero. The non-linear model of the longitudinal dynamics of a large jet aircraft is given as

$$\begin{bmatrix} m\dfrac{\mathrm{d}V}{\mathrm{d}t} \\ mV\dfrac{\mathrm{d}\gamma}{\mathrm{d}t} \\ \dfrac{\mathrm{d}h_{err}}{\mathrm{d}t} \end{bmatrix} = \begin{bmatrix} -D(\alpha,V) + T\cos\alpha - mg\sin\gamma \\ L(\alpha,V) + T\sin\alpha - mg\cos\gamma \\ V(\sin\gamma + \cos\gamma\tan\gamma_R) \end{bmatrix}, \quad (22)$$

cf. the work of Yamé (2005) for the data and the parameters of the aircraft.

4.1. Fault scenario. For illustrating the FTC mechanism, we consider a complete loss of one of the control surfaces, i.e., a fault in the elevator. Two modes of the aircraft system are considered: the nominal mode (no fault) and a complete stuck in the angle of attack (faulty mode).

4.2. Constructing a controller bank. We use the following linearized model for designing a controller bank around the trim points, $\alpha = 2.686\,\text{deg}$ and $T = 4.23 \times 10^4 N$:

$$\dot{x} = Ax + Bu, \quad z = Cx, \quad (23)$$

where

$$x = \begin{bmatrix} V & \gamma & h_{err} \end{bmatrix}^T, u = \begin{bmatrix} \alpha & T \end{bmatrix}^T,$$

$$A = \begin{bmatrix} -0.0180 & -9.7966 & 0 \\ 0.0029 & -0.0063 & 0 \\ 0 & 81.9123 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} -4.8374 & 5.2574 \times 10^{-6} \\ 0.5786 & 3.0149 \times 10^{-9} \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

As mentioned before, the control objective is to maintain h_{err} equal to zero. However, the references to be tracked are V and h_{err}. Thus, the output is now given as $y = C_o x$, where

$$C_o = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

We design two corresponding controllers for the two different modes based on (23). The control law is given as

$$u(t) = -K \cdot z(t) + K_p \cdot e(t) + K_i \cdot \int_0^t e(\vartheta)\,\mathrm{d}\vartheta \quad (24)$$

with $e(t) = w - y$, where w is the reference trajectory. The matrix gain corresponding to the measurement (or state) feedback is designed using the pole-placement technique. The poles for both modes are placed at $(-2.8782, -2.3026 \pm 1.7269i)$ which makes the system internally stable. The matrix gains corresponding to the "Proportional + Integral" (PI) structure allow following the desired trajectory. The gains for healthy and faulty modes are then chosen as

$$K_h = \begin{bmatrix} 2.328 \times 10^{-3} & 7.919 & 0.174 \\ 5.461 \times 10^5 & 5.409 \times 10^{-3} & 1.598 \times 10^5 \end{bmatrix},$$

$$K_{ph} = \begin{bmatrix} 2.2 \times 10^{-3} & 5.21 \times 10^{-2} \\ 9.2755 \times 10^5 & 5.9528 \times 10^6 \end{bmatrix},$$

$$K_{ih} = \begin{bmatrix} 2.2 \times 10^{-2} & 1.563 \times 10^{-1} \\ 9.2755 \times 10^6 & 1.7858 \times 10^7 \end{bmatrix},$$

$$K_f = \begin{bmatrix} 0 & 0 & 0 \\ 7.926 \times 10^5 & 1.091 \times 10^9 & 1.886 \times 10^7 \end{bmatrix},$$

$$K_{pf} = \begin{bmatrix} 1 & 131.63 \\ -1.9018 \times 10^4 & 9.5928 \times 10^4 \end{bmatrix},$$

$$K_{if} = \begin{bmatrix} 0.6339 & 2.7853 \times 10^3 \\ -1.2057 \times 10^4 & 2.0298 \times 10^6 \end{bmatrix}.$$

The subscripts h and f represent the gains for healthy and faulty modes, respectively.

4.3. Parameters of the supervisor. The time interval during which the measurements are taken is τ and the performance is evaluated with t_a, the instants of possible

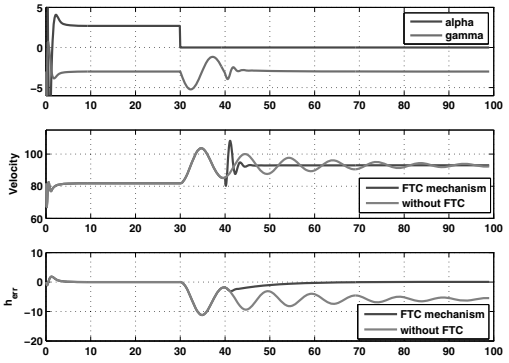

Fig. 8. Closed-loop signals aircraft autopilot landing system.

switchings. The performance threshold λ distinguishes various modes of the system. These parameters are set to $\lambda = 5, \tau = 5$ s.

An experiment is run with a complete stuck in the angle of attack appearing at 30 s. The closed-loop signals of Fig. 8 show that the real-time FTC system successfully reacts at 40 s by switching to Controller 2 (faulty mode controller). After an acceptable transient, the control objective is recovered as seen from the distance from the center of mass of the aircraft relative to the glide-scope approaching to zero. Note that since the FTC scheme is based on the control performance, when the active controller is invalidated by the operating plant data, the supervisor puts into feedback the best controller from the set of potential controllers that is, the controller yielding optimal closed-loop performance in *real-time*.

5. Conclusion

In this paper, the fault tolerant control problem has been formalized in the behavioral setting using the concept of system interconnection. This results in a model-free reconfiguration scheme in *real-time* that is solely based upon the input-output trajectories. In fact, the concept of interconnection among the variables describing the system is regulated by the closed-loop performance evaluation. A cost-detectable "performance functional" captures the control objectives effectively and plays the role of a detector for any abnormal situation or faults in the closed-loop system. On detecting this undesired behavior of the closed loop, an appropriate interconnection is made in real-time without using an explicit model of the plant so that the control objective is satisfied at any time. A novel feature of this scheme is that it does not require any FDI unit. This clearly rules out the issues of generating false or missed alarms associated with standard FDI units, and thus increases the reliability of the FTC system.

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful comments and fruitful suggestions that clearly improved the quality of the paper.

References

Baldi, S., Battistelli, G., Mosca, E. and Tesi, P. (2010). Multi-model unfalsified adaptive switching supervisory control, *Automatica* **46**(2): 249–259.

Belur, M.N. and Trentelman, H.L. (2002). Stabilization, pole placement and regular implementability, *IEEE Transactions on Automatic Control* **47**(5): 735–744.

Blanke, M., Kinnaert, M., Staroswiecki, M. and Lunze, J. (2003). *Diagnosis and Fault Tolerant Control*, Springer-Verlag, Berlin.

Ding, S., Zhang, P., Naik, A., Ding, E. and Huang, B. (2009). Subspace method aided data-driven design of fault detection and isolation systems, *Journal of Process Control* **19**(9): 1496–1510.

Grimble, M. (1993). *Robust Industrial Control: Optimal Design Approach for Polynomial Systems*, Prentice Hall, Upper Saddle River, NJ.

Hespanha, J., Liberzon, D. and Morse, A. (2003). Overcoming the limitations of adaptive control by means of logic-based switching, *Systems & Control Letters* **49**(1): 49–65.

Jain, T., Yamé, J. J. and Sauter, D. (2010). A model based 2-DOF fault tolerant control strategy, *18th IEEE Mediterranean Conference on Control and Automation, Marrakech, Morocco*, pp. 1073–1078.

Morse, A. (2008). Lectures notes on logically switched dynamical systems, *in* P. Nistri and G. Stefani (Eds.) *Nonlinear and Optimal Control Theory*, Lectures Notes in Mathematics, Vol. 1932, Springer-Verlag, Berlin/Heidelberg, pp. 61–161.

Oishi, M., Mitchell, I., Bayen, A., Tomlin, C. and Degani, A. (2002). Hybrid verification of an interface for an automatic landing, *41st IEEE Conference on Decision and Control, Las Vegas, NV, USA,* Vol. 2, pp. 1607–1613.

Polderman, J.W. (2000). Sequential continuous time adaptive control: A behavioral approach, *Proceedings of the 39th IEEE Conference on Decision and Control, Sydney, Australia*, Vol. 3, pp. 2484–2487.

Polderman, J.W. and Willems, J.C. (1997). *Introduction to Mathematical Systems Theory: A Behavioral Approach*, Springer-Verlag, New York, NY.

Safonov, M. and Tsao, T.-C. (1997). The unfalsified control concept and learning, *IEEE Transactions on Automatic Control* **42**(6): 843–847.

Stefanovic, M. and Safonov, M. (2008). Safe adaptive switching control: Stability and convergence, *IEEE Transactions on Automatic Control* **53**(9): 2012–2021.

van der Schaft, A.J. (2003). Achievable behavior of general systems, *Systems & Control Letters* **49**(2): 141–149.

Wang, R. and Safonov, M. (2005). Stability of unfalsified adaptive control using multiple controllers, *Proceedings of the American Control Conference, Portland, OR, USA*, Vol. 5, pp. 3161–3167.

Weiland, S., Stoorvogel, A.A. and Jager, B. (1997). A behavioral approach to the $\mathcal{H}_\infty$ optimal control problem, *Systems & Control Letters* **32**(5): 323–334.

Willems, J. C. (1986). From time series to linear systems, Part II: Exact modeling, *Automatica* **22**(6): 675–694.

Yamé, J.J. (2005). Modeling and simulation of an aircraft in landing approach, *Technical report*, Research Centre for Automatic Control, Nancy.

Yamé, J.J. and Sauter, D. (2008). A real-time model-free reconfiguration mechanism for fault-tolerance: Application to a hydraulic process, *Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision, ICARCV 2008, Hanoi, Vietnam*, pp. 91–96.

Yang, H., Jiang, B. and Staroswiecki, M. (2009). Supervisory fault tolerant control for a class of uncertain nonlinear systems, *Automatica* **45**(10): 2319–2324.

Zerz, E. (2008). Behavioral systems theory: A survey, *International Journal of Applied Mathematics and Computer Science* **18**(3): 265–270, DOI: 10.2478/v10006-008-0024-9.

Zhang, Y. and Jiang, J. (1999). Design of integrated fault detection, diagnosis and reconfigurable control systems, *38th IEEE Conference on Decision and Control, Phoenix, AZ, USA*, pp. 3587–3592.

Zhang, Y. and Jiang, J. (2008). Bibliographical review on reconfigurable fault-tolerant control systems, *Annual Reviews in Control* **32**(2): 229–252.

Zhao, Q. and Jiang, J. (1998). Reliable state feedback control systems design against actuator failures, *Automatica* **34**(10): 1267–1272.

Tushar Jain was born in Meerut, India, in 1985. Currently, he is a Ph.D. student at CRAN, Nancy University (now the University of Lorraine), in the SURFDIAG group. He received his M.Sc. degree in control and guidance from the Indian Institute of Technology (IIT), Roorkee, in 2009, and a B.Sc. (Hons.) in electronics and telecommunication in 2007. His general research interests include data-drive fault tolerant control, behavioral theory, supervisory control, and biologically inspired optimization algorithms.

Joseph J. Yamé received the Doctor in Applied Science degree with the highest distinction from the Free University of Brussels (ULB), Brussels, Belgium, in 2001. He previously graduated from the Polytechnic School of the ULB in electrical and mechanical engineering with the civil engineer title and also received the post-graduate engineering degree in automatic control. From 2000 to 2005, he was a research associate in the Control Engineering and Systems Analysis Department of the ULB. In September 2005, he joined Henri Poincaré University, Nancy (now the University of Lorraine), France, as an associate professor of control engineering and computer science. Over the past several years his educational and research activities have focused on various subjects in systems theory and advanced control engineering with special interests in dual adaptive control of stochastic systems, mathematical control theory with an emphasis on sampled-data control and infinite-dimensional discrete-time systems, and the analytical aspects of fuzzy control. During these last years, his research interest has been mainly concentrated on fault tolerant control and networked control systems. He is a member of the IEEE, AMS, ASEE, and a senior member of the AIAA.

Dominique Sauter received the D.Sc. degree (1991) from Henri Poincaré University, Nancy 1 (now the University Lorraine), France. Since 1993 he has been a full professor at this university, where he teaches automatic control. He was the head of the Electrical Engineering Department for four years, and now he is a vice-dean of the Faculty of Science and Technology. He is a member of the Research Center in Automatic Control of Nancy (CRAN) associated with the French National Center for Scientific Research (CNRS). He is also a member of the French-German Institute for Automatic Control and Robotics (IAR), where he has chaired a working group on intelligent control and fault diagnosis. His current research interests are focused on model-based fault diagnosis and fault tolerant control with emphasis on networked control systems. The results of his research works are published in over 50 articles in journals and book contributions as well as 150 conference papers.

Appendix

The proof of Theorem 1 is somewhat similar to the stability proof of Stefanovic and Safonov (2008). First, it is convenient to provide the following lemma.

Lemma 1. *Consider a fault tolerant system with $\sigma(t)$ selected in accordance with (20) and (21). For any controller C_k in the loop, the corresponding virtual reference $\tilde{r}_k$ converges exponentially to the true reference r.*

Proof. For any controller C_k, (18) yields

$$C_{k_u}(\xi)\tilde{r}(t) = C_{k_e}(\xi)u(t) + C_{k_u}(\xi)y(t).$$

The corresponding controller in the loop gives the control signal by

$$C_{k_e}(\xi)u(t) = C_{k_u}(\xi)r(t) - C_{k_u}(\xi)y(t).$$

From the above two equations, we get

$$C_{k_u}(\xi)(\tilde{r}(t) - r(t)) = 0.$$

Hence, $\tilde{r}(t) - r(t)$ converges exponentially to zero with $C_{k_u}(\xi)$ being a co-prime factor. ■

We show our results corresponding to an $\mathcal{H}_\infty$-stable (15) interconnected system by the measurement set $\mathcal{M}_\tau$.

Proof of Theorem 1. Recall that, by construction, $\tilde{r}_i$ can be viewed as the virtual reference that, if injected into the interconnected system $(\mathcal{P} \wedge \mathcal{C})_i$, would reproduce $(u^{(m)}, y^{(m)})$. Then, for any index i corresponding to an

$\mathcal{H}_\infty$-stable interconnected system, there exist positive reals $\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\delta}_1, \tilde{\delta}_2$ such that

$$\|u^{(m)}\| \leq \tilde{\alpha}_1 \|\tilde{r}_i\| + \tilde{\delta}_1, \quad \|y^{(m)}\| \leq \tilde{\alpha}_2 \|\tilde{r}_i\| + \tilde{\delta}_2.$$

In other words, for every right controller connected to the corresponding plant working mode, the interconnected system $\mathcal{P} \wedge \mathcal{C}$ is $\mathcal{H}_\infty$-stable by the set of trajectories $\mathbf{w} := (\tilde{r}_i, u^{(m)}, y^{(m)})$, regardless of the switching sequence $\sigma(t), t \in \mathbb{T}$. Consequently, from Definition 7, we conclude that $J(\mathbf{w})$ is bounded by λ. Since the measurement set $\mathcal{M}_\tau$ determines the behavior of the plant, after the occurrence of a fault the unfalsification inequality will not be satisfied.

By Remark 1, there exists a controller C_f such that the performance functional corresponding to C_f is minimal relative to the connected controller C_i in the loop. Thus, on directing C_f in the loop, the system $(\mathcal{P} \wedge \mathcal{C})_f$ is $\mathcal{H}_\infty$-stable by the set of trajectories $\mathbf{w} := (\tilde{r}_f, u^{(m)}, y^{(m)})$. Then, there exist finite nonnegative constants $\alpha_1, \alpha_2, \delta_1$, and δ_2 such that

$$\|u^{(m)}\| \leq \alpha_1 \|\tilde{r}_f\| + \delta_1, \quad \|y^{(m)}\| \leq \alpha_2 \|\tilde{r}_f\| + \delta_2.$$

As the virtual reference $\tilde{r}_f$ converges exponentially to the true reference r, there exists a finite nonnegative constant δ such that

$$\|\tilde{r}_f^\tau\| \leq \|r^\tau\| + \|\tilde{r}_f^\tau - r^\tau\| \leq \|r^\tau\| + \delta.$$

Consequently, we conclude that

$$\|u^{(m)}\| \leq \alpha_1 \|r\| + \beta_1, \quad \|y^{(m)}\| \leq \alpha_2 \|r\| + \beta_2,$$

where $\beta_1 := \alpha_1 \delta + \delta_1 \approx 0, \beta_2 := \alpha_2 \delta + \delta_2 \approx 0$ and $\alpha_1 + \alpha_2 = \lambda$, viz. the system $\mathcal{P} \wedge \mathcal{C}$ is $\mathcal{H}_\infty$-stable by $\mathcal{M}_\tau$. Here we see, after the occurrence of a fault, following (20) and (21), that the interconnected system is $\mathcal{H}_\infty$-stable. Hence, it is a fault tolerant system.

Received: 27 December 2010
Revised: 25 May 2011
Re-revised: 24 June 2011