# A novel supervisory-based fault tolerant control: application to hydraulic process

Tushar Jain, Joseph Julien Yamé, Dominique Sauter

# A Novel Supervisory-based Fault Tolerant Control: Application to Hydraulic Process

Tushar Jain, Joseph J. Yamé and Dominique Sauter

***Abstract*— In this paper, we demonstrate a performance-based supervisory approach to achieve fault tolerance that does not require any explicit fault-diagnosis module. Moreover, in our real-time approach the information about the plant is unavailable. The time-valued trajectories generated by the system determine the behavior of the plant-working mode. These trajectories are supposed to follow a certain desired behavior. Therefore, the trajectories when does not belong to that desired behavior assumes the occurrence of fault. A performance functional that formulate these trajectories ruled this desired behavior. Furthermore, we proposed a novel switching logic that effectively determines a suitable control law for the current plant-working mode. Since our approach comprises switching mechanism, we also addressed the stability issues for the overall FTC scheme. Lastly, we demonstrate the proposed approach by applying it to a Hydraulic Process.**

## I. INTRODUCTION

Fault, in general, is defined as an unpermitted behavior that changes the behavior of the system in such a way it no longer satisfies the desired behavior [1]. Thus, the aim of fault tolerant control (FTC) is to counteract that behavior by applying a suitable control law such that the system *encore* achieves the desired behavior. Mostly, the overall process to re-establish the desired behavior undergoes two stages: Fault Detection and Diagnoses (FDD), and Fault Accommodation (FA) (or controller reconfiguration (CR)). In former stage, the information about the fault, i.e. location, size, and severity (LSS), is extracted from the faulty plant. This information is fed to second stage that makes necessary changes to control law to achieve fault tolerance. Usually, the fault behavior is available to FA stage either by estimating the current process parameters or by assuming nominal multiple-models that robustly identifies the behavior of plant. In fact, this introduces uncertainty issues while utilizing the estimated or nominal models, in *real-time*. Moreover, each sub-stage (determining LSS) introduces their respective time delays before feeding to FA. This serves our one of the motivations to decimate the need of first stage in FTC.

Recently, supervisor or logic-based approach to FTC has drawn a significant attention. It is true that this approach can handle a particular class of faults, but the interest lies to handle that class efficiently keeping in mind the real-time aspects. Note, this particular class defines the pre-assumed faults, not some certain types of fault (e.g. step, ramp etc.). In fact, a model-based approach to FTC requires a fault to be estimated, thus, a faulty model has to be assumed that incarnates certain set of faults for which the system is designed. Otherwise, a continuous mechanism is required that tunes the observer or fault estimator such that the system achieves the desired behavior. As we have seen many times [16], an observer effectively estimates a certain class of pre-modeled fault but to other types of faults, it loses its performance. Therefore, a proper tuning is required not only to identify a fault but after the controller reconfiguration as well [17].

The FTC approach taken here is based on a pre-designed set of dynamic (possibly robust) control laws for the nominal and the likely faulty modes. In real-time classical approach to FTC problem, a suitable controller is selected from the set through the monitoring of plant with a certain logic that takes the role of an indicator of the current plant-working mode. Usually, in model-based FTC, an adaptive-FDD scheme regulates this logic, which in turn induces the above-mentioned problem. Therefore, the main idea behind the proposed approach is to directly identify the correct pair "controller/faulty plant mode" with a real-time mechanism in such a way it makes no use of an online plant model, thus FDD stage. Consequently, this results in model-free approach to FTC with fast and reliable controller reconfiguration. Since this approach does not involve any prior plant knowledge in *real-time* and depends solely on trajectories generated by the system, it is also termed as data-driven fault tolerant control. The main goal of this paper is to discuss the novel switching logic introduced in [6] from stability point of view. We employ the mathematical framework of behavioral systems [13] to support our approach. In addition, we utilize virtual reference tool [10] and norm-based trajectories [2] to carry out the stability analysis and other aspects in this performance-based supervisory logic mechanism to FTC. The approach is successfully demonstrated with a two-tank hydraulic process [4].

## II. PRELIMINARIES

In this section, we briefly introduce the behavioral approach to control and system interconnection, and other mathematical tools.

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

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

The authors are with Centre de Recherche en Automatique de Nancy (CRAN), UMR 7039, Faculté des Sciences et Techniques, Université Henri Poincare Nancy 1, 54506 Vandoeuvre-les-Nancy, France {tushar.jain, joseph.yame, dominique.sauter}@cran.uhp-nancy.fr

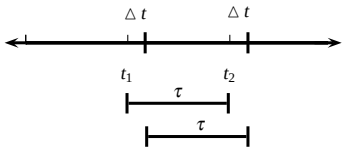


Fig. 1. Sliding time-window

The set $\mathbb{W}$ is the space in which the system time-signals take on their values and the behavior $\mathscr{B} \subseteq \mathbb{W}^{\mathbb{T}}$ is a *family* of $\mathbb{W}$-valued time trajectories.

*Remark 1:* Any behavior of dynamical system is represented by its kernel representation, $\mathscr{B} :\equiv P(\frac{d}{dt})\mathbf{w} = 0$, where $P \in \mathbb{R}^{\bullet \times \mathbf{w}}[\xi]$ and $\xi \equiv \frac{d}{dt}$ is an indeterminate operator.

*Definition 2:* $\mathfrak{L}_e^\infty$ denotes the space of trajectories which are bounded for finite time, i.e.

$$\mathfrak{L}_e^\infty = \{ f : \mathbb{R}^+ \to \mathbb{R} / \sup_{t>\tau} |f(\tau)| < \infty, \forall t \in \mathbb{R}^+ \}$$

$|\cdot|$ denotes any norm on a finite dimensional linear space. $\mathfrak{L}_e^\infty$ is equivalent to $\mathbb{W}^{\mathbb{T}}$ in behavioral definition of dynamical systems. Now we introduce the concept of control in behavioral context.

*Definition 3:* Given a plant, dynamical system $\Sigma_p = (\mathbb{T}, \mathbb{W}, \mathscr{P})$ with behavior $\mathscr{P}$. Let $\mathbf{C}$ be a family of dynamical systems, all with $\mathbb{T}$ as common axis and $\mathbb{W}$ as common signal space. Let $\mathbf{C}$ the set of admissible controllers. An element $\Sigma_c \in \mathbf{C}, \Sigma_c = (\mathbb{T}, \mathbb{W}, \mathscr{C})$ is called an admissible controller. The interconnected system $\Sigma_p \wedge \Sigma_c = (\mathbb{T}, \mathbb{W}, \mathscr{P} \cap \mathscr{C})$ represents the controlled system $\Sigma_k$ with behavior $\mathscr{K} \equiv \mathscr{P} \cap \mathscr{C}$.

*Remark 2:* The controller is a dynamical system that impose restrictions, in some sense, on the behavior of plant by a *regular feedback interconnection* such that it results into a controlled system. Two types of trajectories, viz., to-be-controlled and controlled trajectories are involved in this interconnection.

The controller $\Sigma_c$ should be chosen such that $\mathscr{K} \subseteq \mathscr{D}$, where $\mathscr{D}$ is the desired behavior given as

$$\mathscr{D} = \{ \mathbf{w} \in \mathfrak{L}_e^\infty \mid \mathbf{w} \in \mathscr{P} \cap \mathscr{C}, J(\mathbf{w}) \leq \gamma \} \tag{1}$$

Here $J(\mathbf{w}) : \mathbb{T} \to \mathbb{W}$ is the performance functional that captures the control objective and $\gamma$ is a real bound.

*Remark 3:* All trajectories in this paper can grow at most exponentially by Definition 2, and the performance functional as well, therefore, belong to $\mathfrak{L}_e^\infty$ space.

In [12], Willems deals with the data and measurements that define the behavior of system. It is assumed that the measurement consists of observed realizations of the phenomena itself. Thus, we form a measurement set $\mathscr{M}$, which is a nonempty subset of $\mathbb{W}^{\mathbb{T}}$. Following Remark 1, since the polynomial in kernel representation of plant is unknown we work only with the measured information evolving with time. Note the trajectories are collected until the present time only (the future being unknown), for a certain time-window $\tau$ (See Fig. 1).

*Definition 4:* Given a vector space of time signals $\mathbb{W}^{\mathbb{T}}$, a model or dynamical system $\Sigma_p = (\mathbb{T}, \mathbb{W}, \mathscr{P})$, a mapping $\mathsf{O}_\tau : \mathbb{W}^{\mathbb{T}} \to \mathbb{W}^{\mathbb{T}}$ and a measurement set $\mathscr{M}_\tau \subset \mathsf{O}_\tau(\mathbb{W}^{\mathbb{T}})$, we say that the behavior $\mathscr{P}$ is said to be unfalsified by the measurement set $\mathscr{M}_\tau$ if

$$\mathscr{M}_\tau \subset \mathsf{O}_\tau(\mathscr{P})$$

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

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

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 $\mathscr{M}_\tau$ is the set of actual experimental observations of the plant behavior as observed through the time sampler $\mathsf{O}_\tau$. Thus, $\mathsf{O}_\tau^{-1}(\mathscr{M}_\tau)$ is a behavior that interpolate the observed data during the time interval $\tau$.

$$\mathsf{O}_\tau^{-1}(\mathscr{M}_\tau) = \{ \mathbf{w} \in \mathfrak{L}_e^\infty \mid \mathbf{w} \in \mathscr{P}, (\mathsf{O}_\tau \mathbf{w}) \in \mathscr{M}_\tau \} \tag{2}$$

**Problem Formulation** For a given measurement set $\mathscr{M}$, the fault tolerant control problem is now given as:

- describe the set of admissible controllers
- describe what desirable properties the controlled system should have
- to find an admissible controller $\Sigma_c$ such that $\Sigma_p \wedge \Sigma_c$ has these desired behavior at *anytime*

*Definition 5:* Given a vector space of time signals $(\mathbb{T} \times \mathbb{W})$, a controller $\Sigma_c = (\mathbb{T}, \mathbb{W}, \mathscr{C})$, a desired behavior $\mathscr{D}$, a mapping $\mathsf{O}_\tau : \mathbb{W}^{\mathbb{T}} \to \mathbb{W}^{\mathbb{T}}$ and a measurement set $\mathscr{M}_\tau \subset \mathsf{O}_\tau(\mathbb{W}^{\mathbb{T}})$, we say that a controller $\Sigma_c$ is unfalsified by the measurement set $\mathscr{M}_\tau$ if

$$\mathsf{O}_\tau(\mathsf{O}_\tau^{-1}(\mathscr{M}_\tau)) \cap \mathscr{C}) \subset \mathsf{O}_\tau(\mathscr{D}); \text{ where } \mathsf{O}_\tau^{-1}(\mathscr{M}_\tau)) \cap \mathscr{C} = \mathscr{K}$$

Definition 5 supposes roughly that a controller, whose behavior is denoted by $\mathscr{C}$, is said to be unfalsified if the set of trajectories that are consistent with the measurement and the controller, at the past observation times, is a subset of the desired set $\mathsf{O}_\tau(\mathscr{D})$.

*Remark 4:* Definition 4 articulates the concept of Most Powerful Unfalsified Model (MPUM) [12] while Definition 5 extrapolates the Unfalsified Control Concept (UCC) [10].

Visiting to our problem, in the analysis and development phase we assumed that a finite set of controllers

$$\mathbf{C} = \{ C_1, C_2, ..., C_K \} \tag{3}$$

is constructed in such a way so that in every situation either healthy or any faulty mode of the plant, there is at least one controller in that set which has the appropriate control action and is able to achieve the desired behavior *anytime*. This assumption generalizes an important concept of controllability that is often seen in the analysis and synthesis of dynamical system. It is generally defined as the possibility of transferring the state of system from one mode to another. This reflects the ability of controlling the plant we have at hand. Unfortunately, this property was originally introduced in the context of state-space systems [3]. Since we do not have any physical representation for our plant,

we will employ behavioral approach [13] to deal with this property. Suppose initially our system works well with any of the controller belong to (3). After an occurrence of fault the current mode of operation becomes undesired, i.e. does not belongs to desired behavior anymore. Therefore, now we have to transfer our system from that mode to another mode, referred to as a desired mode. Nevertheless, this transfer should be automatic.

*Definition 6:* Let $\Sigma = (\mathbb{T}, \mathbb{W}, \mathscr{B})$ be a linear differential system, $\Sigma$ is said to be controllable if for all $\mathbf{w}_1, \mathbf{w}_2 \in \mathscr{B}$ there exists $T \in \mathbb{R}, T \geq 0$ and $\mathbf{w} \in \mathscr{B}$ such that $\mathbf{w}(t) = \mathbf{w}_1(t)$ for $t < 0$ and $\mathbf{w}(t) = \mathbf{w}_2(t-T)$ for $t \geq T$.

*Remark 5:* Controllability refers to the ability to switch from any one trajectory in the behavior to any other one, allowing some time delay. Interestingly, this is an underlying idea to *feasibility* assumption referred in [11].

We now bring in the notion of stabilizability in behavioral context. This notion is concerned with the situation that we are on a given trajectory of the given behavior $\mathscr{B}$ and we want to switch to a trajectory that asymptotically tends to zero, while remaining on a trajectory within the behavior. Following Remark 3, cost functional is also a trajectory in $\mathfrak{L}_e^\infty$.

**Proposition** Let $\Sigma = (\mathbb{T}, \mathbb{W}, \mathscr{B}), \mathscr{B} \in \mathfrak{L}_e^\infty$. Let for every trajectory $\mathbf{w} \in \mathscr{B}$, there exists a trajectory $J(\mathbf{w}(t)) \in \mathfrak{L}_e^\infty$. The following statements are equivalent:

a. The system $\Sigma$ is stabilizable.
b. The cost functional has the property that $\lim_{t\to\infty} J(\mathbf{w}(t)) = 0$.
c. The cost functional has the property that $J(\mathbf{w}(t)) \leq \gamma, \forall t \in \mathbb{T}$, where $\gamma$ is the stability margin.
d. The cost functional has the property in time that $\frac{J(w(t)) - J(w(t-\tau_{ds}))}{\tau_{ds}} \leq 0$, where $\tau_{ds}$ is the dynamics settling time such that the non-increasing behavior of $J$-trajectory in $\tau_{ds}$ is visible.

Proceeding with our problem, the desired properties represents what the system is expected to deliver. This is given by a performance functional in (1). This functional plays two important role in real-time:

- it *renders* the information about the operating behavior of system,
- it *prognosticates* that which controller from the bank can satisfy Definition 6 in case the fault occurs, thus, maintains the *anytime* property.

We will see in the following section that how the performance functional prognosticate the behavior of "off-the-shelf" controllers. At this point, we consider that a functional $J(\mathbf{w}_k), \forall k \in K$ is associated with each controller in the bank and which properties are required to determine the current behavior.

*Definition 7:* Let $\mathscr{M}$ denotes the resulting plant data collected with $C_k$ as the current operating controller. The pair $(J(\mathbf{w}_k), \mathbf{C}), \forall k \in K$ is said to be *cost-detectable* if, without any assumptions on the plant and for every $C_k \in \mathbf{C}$, stability of the closed-loop system is falsified/unfalsified by $\mathscr{M}_\tau$.

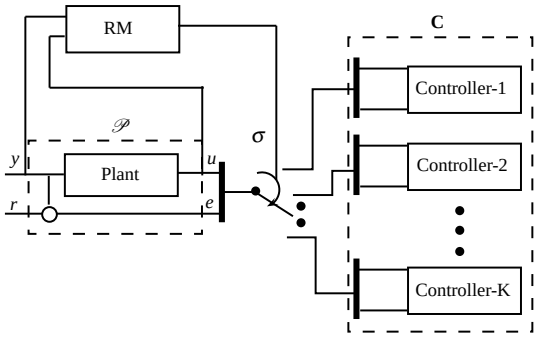


Fig. 2. Switching control scheme for FTC in behavioral setting

Therefore, $J_k, \forall k \in K$ must satisfy cost-detectability such that it can reliably detect any stability/instability in the closed-loop. Cost-detectability is completely determined from the knowledge of cost function and candidate controllers, without reference to plant.

To deal with the last and most important part of our problem, we consider the architecture of switching control for FTC in behavioral setting as shown in Fig.2 (signals have their usual meanings). The supervisor or reconfiguration mechanism (RM) manages the switching of controllers from the set of admissible controllers into feedback with the plant such that the closed loop satisfies the control objective despite the occurrence of fault. The only remaining task is to design an appropriate switching logic that can select the right controller for the operating mode.

## III. Switching Logic and More about Stability

In this section, we will briefly discuss about the different types of switching logic and the stability issues related with the proposed switching mechanism. Three types of supervision or reconfiguration mechanism as follows exists in the literature [7]:

- Pre-routed supervision (PRS)
- Estimator-based supervision (EBS)
- Performance-based Supervision (PBS)

The merits and demerits of these supervision mechanisms are discussed in [6]. Since we do not have any access to plant in real-time, performance-based supervision, based on the comparison, is considered a potential mechanism in the present context. Two types of switching logic as follows can achieve PBS mechanism:

- Fixed dwell time
- Adaptive dwell time (Hysteresis based switching)

While "hysteresis switching logic" provides a number of attractive properties [8], adaptive dwell-time switching was known to have some significant shortcomings, notably an inability to function correctly in the face of un-modeled dynamics and exogenous disturbances [11]. Moreover, it cannot prevent the switching to wrong controller while the right corrective controller is operating in the loop [6]. Recognition of this led to the introduction of an alternative logic called "dwell-time switching" which circumvented hysteresis

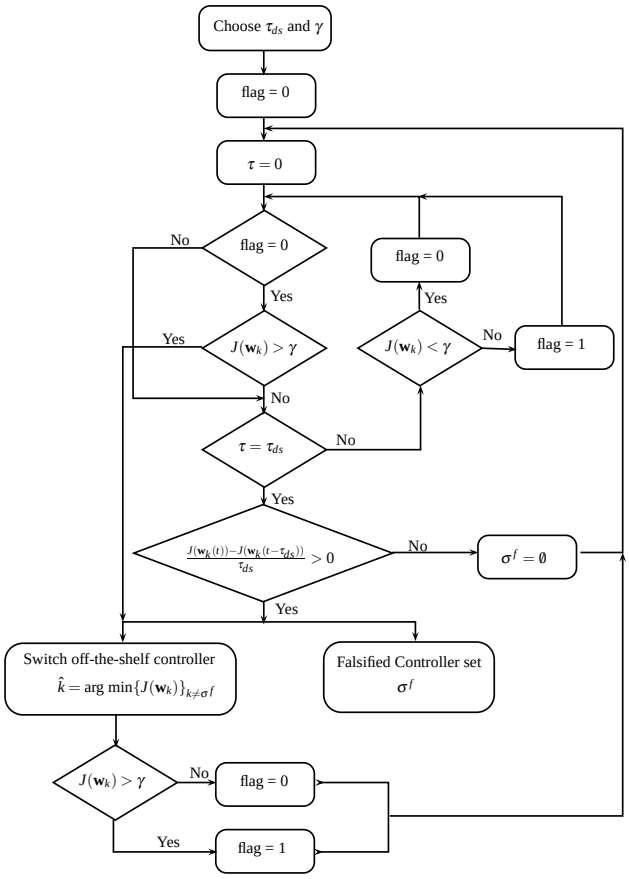


Fig. 3. Proposed switching logic

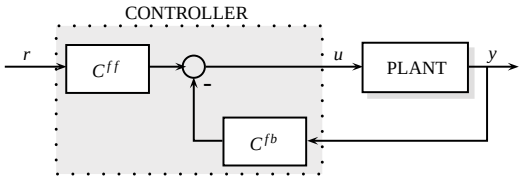


Fig. 4. Two-degree-of-freedom feedback structure

switching's deficiencies (See [7]). However, utilizing fixed-dwell time logic in real-time FTC, wrong controller can stay in loop for a considerable time such that the system becomes uncontrollable. Consequently, we proposed a switching logic that circumvents the deficiencies seen in the above classical switching logic. Fig. 3 illustrates the computer program for that logic. Here we will talk more about the practical issues.

### A. Performance Evaluation

To evaluate the performance of "off-the-shelf" controllers, consider the standard two-degree-of-freedom controller structure of Fig. 4. The available data produced by the plant is its measured input/output signals $(u^{(m)}, y^{(m)})$ up to the current time. The performance evaluation of a controller $C_k$ in the set (3) based on the measured data $(u^{(m)}, y^{(m)})$ proceeds as follows. The full behavior of controller $C_k$ is given by the set

$$\mathscr{C}_k = \{\mathbf{w} = (r,u,y) \in \mathfrak{L}_e^\infty \mid u = C_k^{ff} r - C_k^{fb} y\} \tag{4}$$

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

$$r_k = (C_k^{ff})^{-1}\{u^{(m)} + C_k^{fb} y^{(m)}\} \tag{5}$$

where the feed-forward component of the controllers transfer function is stable-causally-left-invertible (SCLI). Note that this assumption is not restrictive since the controllers can be designed to be bi-proper. The triple $\mathbf{w}_k = (r_k, u^{(m)}, y^{(m)})$ is therefore the signal in $\mathbb{W}^{\mathbb{T}}$ which is compatible with the behavior obtained by interconnecting controller $C_k$ to the unknown plant. The above procedure can be applied to any controller in the set (3) of the $K$ potential controllers, thus yielding $K$ performance indexes

$$\{J(w_k), k = 1,2,...,K\} \tag{6}$$

### B. Features of Switching Logic

Here we list out few important features of the novel switching logic [6].

- Choose performance threshold or stability margin $\gamma$, and dynamics settle down time $\tau_{ds}$. This can also be considered as dwell-time in some respect, though $\tau_{ds} \neq \tau$ and $\tau_{ds} < \tau_D$ (in fixed dwell-time). Selection of $\tau_{ds}$ [7, A.1] considers the fact that if the right controller is in the loop then corresponding cost-function should have non-increasing behavior.
- Once a controller is falsified, then that controller will not be test for unfalsification until the fault is accommodated. Here we consider the case of only one fault at a time.
- Controller is falsified if one of them is true.
  - $J(\mathbf{w}_k) \leq \gamma$ before the occurrence of fault, controller is falsified if $J(\mathbf{w}_k) > \gamma$.
  - $J(\mathbf{w}_k) \leq \gamma$ just after the switching (i.e.$t_\uparrow$), controller is falsified if $J(\mathbf{w}_k) > \gamma$.
  - $J(\mathbf{w}_k) > \gamma$ just after the switching (i.e. $t_\uparrow$), controller is falsified if $J(\mathbf{w}_k)$ has increasing behavior at the end of $\tau_{ds}$.
- Suppose at $t_\uparrow$, right controller is selected. Before its selection (i.e. $t_\downarrow$), it might be possible that $J(\mathbf{w}_{\hat{k}}) > \gamma$ because its behavior was being inferred by another destabilizing controller in the loop. Third point in above falsification conditions guarantees that the supervisor will not reject it.

*Remark 6:* In fixed dwell-time switching one has to guarantee $\lim_{t\to\tau_D} J(\mathbf{w}_k) \leq \gamma$. However, here $\tau_{ds} < \tau_D$, thus, $\lim_{t\to\tau_{ds}} J(\mathbf{w}_k) < \gamma$ is not assured as it depends on the severity of fault. Therefore, we introduce the notion of unfalsification based on non-increasing behavior of cost functional in $\tau_{ds}$. This implies that if after switching to right controller, $J(\mathbf{w}_k)$ -trajectory is non-increasing in $\tau_{ds}$, then it is guaranteed that $\lim_{t\to\infty} J(\mathbf{w}_k) = 0 < \gamma$.

### C. Stability Issues

Here we will discuss about the notion of stability in the present context that clearly distinguish from the notion dealt in classical arbitrary switching control.

*1) Stability while Switching:* It is true that if the controller bank consists only destabilizing controllers then it is difficult to ensure the stability of the system. Hespanha et. al. [5] shows that the arbitrary switching between all stabilizing controllers can also cause the instability. The solution suggested to this problem is that for a given strictly proper transfer matrix of the process and a finite family of transfer matrices of stabilizing controllers, there exist realizations of the process and the controllers such that the corresponding closed-loop systems share a quadratic common Lyapunov function. Interestingly, the underlying idea of this realization is to provide a bound on impulse response due to bumps generated while switching. Niemann et. al. [9] as well works on the realization of controllers using Youla-Jabr-Bongiorno-Kucera (YJBK) parametrization in such a way so that the bumps occurring at the time of switching are bounded. Therefore, if we impose an inherent bound on the impulses via a suitable *bumpless technique* then it automatically ensures the stability at least between the stabilizing controllers.

As a result, we utilize a self-conditioned architecture of controllers discussed in [14] such that it makes an inherent bound on the impulses experienced during switching. The advantage of this architecture is that it is completely model-free, i.e. it does not require any plant knowledge. However, the above two realizations depends on the state-space parameters of plant. The above examination can also be justified by Willems definition of *regular feedback interconnection* [13] in behavioral setting. The notion is equivalent to what is usually called well-posedness, i.e. if the controller is regular feedback implementable and stabilizable then the control action can start acting at any time, the system will be stable.

*2) Overall Closed-loop Stability:* Liberzon [7] investigated that the switched system is stable if

- the switching stops in finite time,
- there exist common-Lyapunov function or multiple-Lyapunov function for each mode, which is always non-increasing

Following the switching logic in Fig. 3, it is guaranteed that the final selected controller for the current operating mode will be a corrective controller. Since the controller set (3) is finite, switching will definitely stop in finite time and in worst case, the maximum number of switches will be $K-1$ in infinite time-horizon.

With Lyapunov function based stability, the first issue is to give utmost attention for its selection that requires the knowledge of plant parameters. Secondly, this type of stability is mainly concerned with those types of system where one controller is unable to achieve the system objectives, thus, multiple periodic switching is required between two or more controllers. This is commonly known as *arbitrary switching*. Therefore, the search is for a suitable switching order of

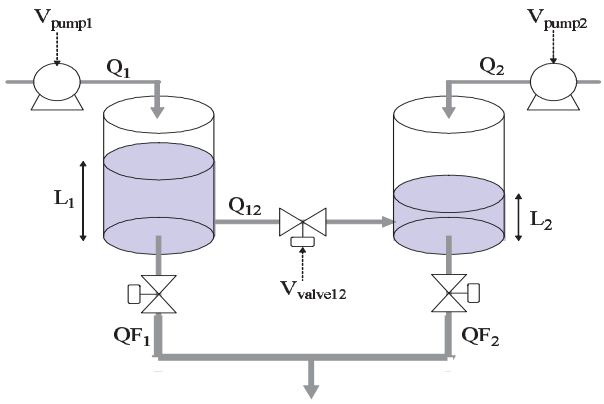


Fig. 5. The two-tanks plant

controller indices that can stabilize the system. However, in our approach the switching logic does not search for a *stabilizing switching order* instead it searches for a *single stabilizing controller*.

*3) Stability affected by the insertion of destabilizing controller:* Since the supervisor based on virtual reference tool (5) cannot guarantee switching to wrong controller after the occurrence of fault, this conflicts the stability of switched system. However, it is true that the trajectories will not reach to infinity in finite time. After an initial learning process, the final selected controller would be the right corrective controller [11]. Therefore, longer the destabilizing controller stays in the loop greater the impact it has on the stability. As a result, our objective is to ensure the falsification of wrong controller as soon as it switched into the loop. We discussed this particular case in detail using a time map in [6]. Thus, utilizing the switching logic (Fig. 3) we can assure that the wrong controller will be removed as soon as possible. However, this falsification procedure is highly influenced by the *cost-detectability* (Definition 7) property of cost functional.

## IV. Application to a Hydraulic Plant

The plant is a two-tanks system depicted in Fig. 5 and full details on its characteristics can be found in [4]. We used the same procedure to design the controllers as discussed in [15], however, the difference lies only in the switching logic. The technique developed in the previous section has been applied to the plant.

### A. Description of the plant

The plant is composed of two interconnected tanks, two pumps that provide the flow rates $Q_1$ and $Q_2$, two level sensors $L_1, L_2$, five flow-rate sensors for the measurements of $Q_1, Q_2, Q_{F1}, Q_{F2}$ and $Q_{12}$ and three valves (see Fig. 5). The control inputs to the plant are the voltages $V_{pump1}, V_{pump2}$ applied to the pumps and the voltage $V_{12}$ for the throttling of the interconnection valve. The flows $Q_{F1}$ and $Q_{F2}$ are mixed through the valves located at the output of the tanks.

The main objective of the system is to keep the sum $y_1 = Q_{F1} + Q_{F2}$ and the ratio $y_2 = Q_{F1}/Q_{F2}$ of the output flow-rates to desired set-points $y_1^*$ and $y_2^*$.

*B. Model of the plant*

The system has two state variables which are the liquid levels $L_1$ and $L_2$ of the tanks. The equations describing the evolution of the states are

$$\begin{aligned} S_1\dot{Q}_1 &= Q_1 - Q_{12} - Q_{F1} \\ S_2\dot{Q}_2 &= Q_2 - Q_{12} - Q_{F2} \end{aligned} \tag{7}$$

The variables in the right-hand side of these state equations are given by the known nonlinear maps

$$\begin{aligned} Q_1 = \pi_1(V_{pump1}), \quad Q_2 = \pi_2(V_{pump2}) \\ Q_{F1} = R_1\sqrt{L_1}, \quad Q_{F2} = R_2\sqrt{L_2} \end{aligned} \tag{8}$$

and

$$Q_{12} = R_{12}(V_{12}).\sqrt{|L_1 - L_2|}.sign(|L_1 - L_2|) \tag{9}$$

where $\pi_1, \pi_2$ and $R_{12}$ are nonlinear transformations which describe the characteristics of the pumps and the interconnection valve as a function of the corresponding input voltages. The parameters $R_1, R_2$ are the throttling of valves 1 and 2, and $S_1, S_2$ are the section of tank 1 and tank 2 respectively (details on the model identification can be found in [4]. With the explicit expression of $Q_{F1}$ and $Q_{F2}$, the controlled outputs of the system are given by $y_1 = R_1\sqrt{L_1} + R_2\sqrt{L_2}$ and $y_2 = \frac{R_1\sqrt{L_1}}{R_2\sqrt{L_2}}$. Since these controlled outputs are required to follow the desired set-points $y_1^*$ and $y_2^*$, these set-points can be rewritten as desired set-points $L_1^0, L_2^0$ for the measured levels $L_1, L_2$ with

$$L_1^0 = \left(\frac{y_1^* y_2^*}{R_1(1+y_2^*)}\right)^2, \quad L_2^0 = \left(\frac{y_1^*}{R_2(1+y_2^*)}\right)^2 \tag{10}$$

*C. Faults*

The main hardware devices used for controlling and sensing the pilot plant, i.e. the two pumps, the interconnection valve and the two level sensors, can be affected by a fault. Different types of faults, such as bias, drift, power loss and stuck can be realized on these devices. For the purpose of illustrating the FTC technique of the previous section, we consider pump 2 subject to a power loss fault. Two faulty modes of the plant are considered: the nominal mode (no fault) and the "power loss of pump 2" mode with an effectiveness factor of 0.5. Note that stuck in actuators or faults on sensors, which require a detection and isolation of the faulty components and a change in the input/output channels of the plant, fall outside the scope of the supervisory FTC technique presented in this paper. Other methods developed elsewhere take care of such faults.

*D. Controllers design*

The nominal fault-free system operating point is fixed at $(L_1^0, L_2^0) = (0.4, 0.5)$ meters, $V_{12} = 2$ Volts. The linearization of the nonlinear equations (7) at the nominal operating point yields

$$\dot{x} = Ax + B_v v, \quad y = Cx \tag{11}$$

with $y = x = \begin{pmatrix} l_1 & l_2 \end{pmatrix}^T$ and $v = \begin{pmatrix} u_1 & u_2 & u_3 \end{pmatrix}^T$

$$A = \begin{pmatrix} -0.0037 & -0.0017 \\ -0.0018 & -0.0035 \end{pmatrix} \tag{12}$$

$$B_v = \begin{pmatrix} 64.9351 & 0 & -0.0001 \\ 0 & 65.7895 & 0.0002 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{13}$$

where $l_i = L_i - L_i^0, u_i = V_{pump_i} - V_{pump_i}^0$ for $i = 1, 2$ and $u_3 = V_{12} - V_{12}^0$; the variables with superscript 0 denotes values at the nominal point. The interconnection valve will be maintained open at the constant nominal value $V_{12}^0 = 2$ Volts in all modes. With the above consideration, the plant can be viewed as a multivariable system with two controlled inputs, and two sensed outputs. Since the control objective reduces to maintaining the levels of the two tanks at their set-point values for the two modes (fault-free mode and "pump 2 power loss" mode), the design of the corresponding controllers will be based on the linearization (11). Two multivariable digital controllers, with sampling period $\triangle t = 1s$, are designed for the corresponding linearized plant models using the Linear Quadratic Regulator (LQR) synthesis method. Note that since the LQR method results in pure state-feedback, integral action will be added to the controllers structure in order to force the steady-state errors (to step inputs) tend to zero. The structure of the multivariable controllers is derived through the robust servomechanism approach [3] and proceeds as follows. The dynamics of the plant is augmented with the dynamics of the reference signals which are constant set-points here. Denoting the reference signals vector by $r$, the tracking error signal $e = r - y$ has the dynamics

$$\dot{e} = -C\zeta \tag{14}$$

where $\zeta = \dot{x}$. Setting $\mu = \dot{u}$, where $u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$, the augmented state equation of the system is

$$\dot{z} = \mathbf{A}z + \mathbf{B}\mu \tag{15}$$

with $z = \begin{pmatrix} e \\ \zeta \end{pmatrix}, \mathbf{A} = \begin{pmatrix} 0 & -C \\ 0 & A \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 0 \\ B \end{pmatrix}$ where $B$ is the $2 \times 2$ submatrix of $B_v$ obtained from its first and second columns. It is easily verified that system $(A, B)$ is controllable which implies that the composite system (15) is also controllable [3]. Hence, this system can be stabilized by a state feedback law

$$\mu = -Kz = -\begin{pmatrix} K_1 & K_0 \end{pmatrix}\begin{pmatrix} e \\ \zeta \end{pmatrix} \tag{16}$$

which, in terms of the original plant signals, is given by

$$u(t) = -K_1\int_0^t e(\delta)d\delta - K_0 x(t) + u_0 \tag{17}$$

where $u_0 = u(0)$. Note that controller (17) has the structure of an integral (on the error) and state-feedback controller. In order to meet the requirement for constructing the filters (5), the feed-forward part of the controllers should be causally invertible. Therefore, we modify the structure (17) to a

"Proportional+Integral" (on the error) structure by explicitly introducing a feed-forward matrix gain $G_{ff}$.

$$u(t) = G_{ff}.r - K_1 \int_0^t e(\delta)d\delta - K_0 x(t) + u_0 \qquad (18)$$

Taking advantage of the fact that $x = y$, we set $G_{ff} = K_0$ and end up with a multivariable PI control structure

$$u(t) = K_0 e(t) - K_1 \int_0^t e(\delta)d\delta + u_0 \qquad (19)$$

We make use of this PI control structure for the two plant modes and compute the corresponding gains via the LQR method applied to the composite system (15). The design parameters are the weighting matrices $Q$ and $R$ of the performance index $\mathbf{J} = \int_0^\infty (z^T Qz + u^T Ru)dt$. These weighting matrices are obtained after subsequent iterations to achieve an acceptable tradeoff between performance and control effort. Setting $R$ equal to the 2-dimensional identity matrix for the two plant modes, satisfactory behaviors for the nominal operating point and for the "pump 2 power loss" mode are respectively obtained with

$$Q_0 = 10^{-3} \begin{pmatrix} 0.1 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 \\ 0 & 0 & 0.4 & 0 \\ 0 & 0 & 0 & 0.4 \end{pmatrix} \qquad (20)$$

$$Q_{fault} = \begin{pmatrix} 0.1 & 0 & 0 & 0 \\ 0 & 0.1024 & 0 & 0 \\ 0 & 0 & 0.0004 & 0 \\ 0 & 0 & 0 & 6.5536 \end{pmatrix} \qquad (21)$$

With the above Q parameters, the computed gains of the digital controller for the nominal point are

$$K_0 = \begin{pmatrix} 0.0153 & 0 \\ 0 & 0.0151 \end{pmatrix}, K_1 = \begin{pmatrix} -0.0047 & 0 \\ 0 & -0.0047 \end{pmatrix} \qquad (22)$$

and those of the faulty mode digital controller are

$$K_0 = \begin{pmatrix} 0.0153 & 0.0069 \\ 0 & 0.0398 \end{pmatrix}, K_1 = \begin{pmatrix} -0.0047 & 0.0009 \\ 0 & -0.0045 \end{pmatrix} \qquad (23)$$

Having the set of controllers for the different modes, the reconfiguration mechanism can now be designed to select in real time the right controller based on the actual process input/output data. The performance functional (1) chosen here is the ISE (Integral of Squared Error).

$$J|_{t=t_n} = \int_{\tau+n\triangle t}^{2\tau+n\triangle t} \|e(\delta)\|_2^2 d\delta \qquad (24)$$

where $e(\delta) \in \mathfrak{L}_e^\infty$ is the control error vector. Note that this functional might not be necessary the same as the performance index used for the off-line design of the controllers. The tuning parameters of the supervisor are:

- the dynamics settling time given by $\tau_{ds} = \ell_1 \triangle t$ for an integer $\ell_1$ and $\triangle t$ the sampling period of the feedback loop
- the sliding window given by $\tau = \ell_2 \triangle t$ for an integer $\ell_2$.

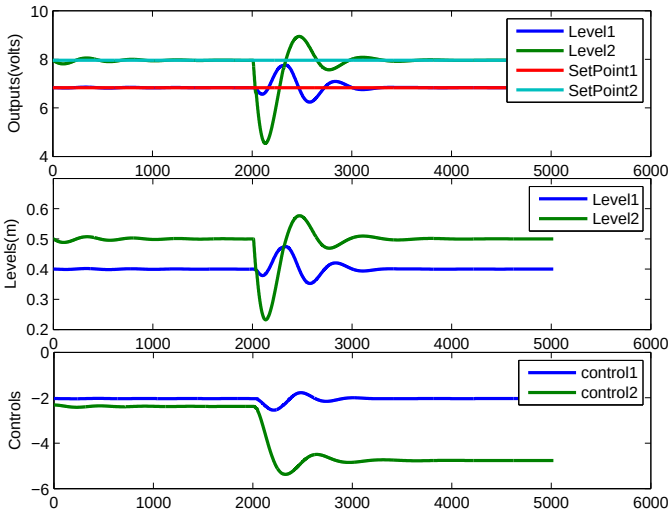


Fig. 6. Closed-loop signals with supervisory FTC of two-tanks plant

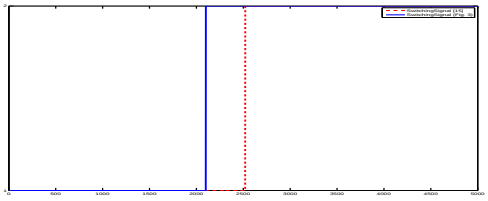

Fig. 7. Comparison of switching signal

- the performance threshold $\gamma$. This threshold should be set in a way such that the two modes can be discriminated.
- the performance functional $J(\mathbf{w}(t))$ given by (24) such that it satisfies Definition 7.

These parameters are set to $\gamma = 1, \tau_{ds} = 120s, \tau = 10s$. We run two experiments with the power loss of pump 2 appearing at time 2000s. In first experiment, we consider fixed dwell-time switching logic with suitable tuning parameters as given in [15]. While for second experiment, we utilize the novel switching logic. The first two types of stability discussed in section III-C are guaranteed, as first type of stability is concerned with controller's realizations. Second type of stability considers providing a limit on the number of switches, which is also assured utilizing both the switching logic. As discussed earlier, third type of stability issue arises due to the prolong stay of destabilizing controller in feedback loop. Therefore, the main objective is to abridge this stay as much as possible. Since it depends on the switching algorithm, utilizing the algorithm discussed in section III we are able to accomplish this task. The closed-loop signals in Fig. 6 show that the real-time FTC system successfully reacts at time 2030s by switching to controller 2 (faulty mode controller). The significance of novel switching logic is illustrated in Fig. 7. After an acceptable transient, the

control objective is recovered as seen from the levels of the two tanks being equal to the set-points. Note that since the FTC scheme is based on *control performance*, when the active controller is invalidated by the operating plant data, the supervisor puts into feedback the best controller from the potential controllers set, that is the controller yielding optimal closed-loop performance in real-time.

## V. Conclusion

In this paper, we have presented a real-time fault-tolerant control scheme, which is based on the data produced by an operating plant with no online fault diagnosis unit. The novel supervisory logic, proposed in [6] is successfully demonstrated on a hydraulic process followed by other practical issues. Cost-detectability plays a vital role of a *detector* to determine any unexpected changes or faults in the closed-loop system. Following only cost-detectability property, configuring directly to right corrective controller is not guaranteed, however, on occurrence of fault the final selective controller is the right controller. Therefore, cost-detectability is only a necessary condition, not a sufficient condition for our data-driven approach to FTC. The sufficient condition can only be promised by *cost-selectability* property such that the supervisor is able to select the right controller in one shot. The notion of cost-selectability subsumes cost-detectability. Our future work will deal with this issue only.

## References


[1] M. Blanke, M. Kinnaert, M. Staroswiecki, and J. Lunze. *Diagnosis and Fault tolerant control*. Springer-Verlag, 2003.

[2] S. P. Boyd and C. H. Barratt. *Linear Controller Design: Limits of Performance*. Prentice Hall, New Jersey, 1991.

[3] C-T Chen. *Linear System Theory and Design*. Oxford University Press, New York, 1999.

[4] F. Hamelin, H. Jamouli, and D. Sauter. The two tanks pilot plant. IFATIS report IFAN014R01, Centre de Recherche en Automatique de Nancy (CRAN), Nancy, France, 2004.

[5] J.P. Hespanha and A. Morse. Switching between stabilizing controllers. *Automatica*, 38:1905–1917, 2002.

[6] T. Jain, J. Yamé, and D. Sauter. A novel implementation of supervisory based fault tolerant control. In *IEEE Multi-Conference on Systems and Control (submitted)*, 2011.

[7] D. Liberzon. *Switching in systems and control*. Boston: Birkauser, 2003.

[8] A.S. Morse, D.Q. Mayne, and G.C. Goodwin. Applications of hysteresis switching in parameter adaptive control. *IEEE Transactions On Automatic Control*, 37:1343–1354, 1992.

[9] H. Niemann, J. Stoustrup, and R. B. Abrahamsen. Switching between multivariable controllers. *Optim. Control Appl. Meth.*, 25:51–66, 2004.

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

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

[12] J. C. Willems. Paradigms and puzzles in the theory of dynamic systems. *IEEE Transactions on Automatic Control*, 36:259–294, 1991.

[13] J. C. Willems. On interconnections, control, and feedback. *IEEE Transactions on Automatic Control*, 42:326–339, 1997.

[14] J. J. Yamé, H. Qiao, and M. Kinnaert. A self-conditioned implementation of switching controllers for smooth transition in multimode systems. In *IEEE Conference on Control and Fault-Tolerant Systems, Systol'10*, 2010.

[15] J.J. Yamé and D. Sauter. A real-time model-free reconfiguration mechanism for fault-tolerance: Application to a hydraulic process. In *Proc. 10th International Conference on Control, Automation, Robotics and Vision( ICARCV)*, pages 91–96, 2008.

[16] K. Zhang, B. Jiang, and V. Cocquempot. Adaptive observer-based fast fault estimation. *International Journal of Control, Automation, and Systems*, 6:320–326, 2008.

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