SUPERVISORY FAULT-TOLERANT CONTROL WITH APPLICATION TO THE IFATIS TWO-TANKS BENCHMARK [1]

Joseph J. Yamé, Michel Kinnaert

Service d'Automatique et d'Analyse des Systèmes, CP 165
Fac. des sciences appliquées, Université libre de Bruxelles,
50 av. F.D. Roosevelt, Brussels-1050, Belgium
Fax:32-2-650.26.77, email: joseph.yame@ulb.ac.be

Abstract: This paper reports the main ideas of a new technique for real-time fault-tolerant control (FTC) and demonstrates the effectiveness of this technique on a two-tanks process benchmark. The proposed technique relies on the operating data produced by the plant and on the control objective expressed quantitatively by a performance functional. The resulting control system architecture is of a supervisory type with the main feature that it achieves real-time fault tolerant control without on-line model-based fault detection and isolation (FDI) algorithms. The research activity has been performed within the framework of the research project Intelligent Fault Tolerant Control in Integrated Systems-IFATIS- funded by the European Union.

Keywords: Fault tolerant control, performance monitoring, supervisory switching

1. INTRODUCTION

A Fault-tolerant control (FTC) system is a control system that is able to accommodate system component faults automatically (Patton, 1997; Blanke et al., 2003). Here, a fault is meant to designate a deviation or a change in the characteristics of a component of that system such that it does no longer satisfy its objective. Common examples of faults are the blocking or the loss of effectiveness of actuactors, the drift or loss of sensors, changes in the plant dynamics due to component damage, wear or leakage, etc...When such faults occur, the nominal controller designed for the fault-free system might be unable to maintain the control objective of the overall system. If no action is taken promptly, the faults might develop into a total failure which can be catastrophic and cause danger to humans and to the system and its environments. In order to avoid or mitigate such consequences, a fault-tolerant control system will try whenever possible to recover the original system performance/functionality completely or partially after the detection of a fault. Typically, the operation of a fault-tolerant control system breaks down into the following tasks: fault detection and isolation (FDI) and control reconfiguration. The control reconfiguration is based on the information provided by the FDI system which uses a model of the plant to detect any discrepancy between the fault-free plant and any of its faulty behavior. The inevitable inaccuracies of the model used for FDI system design are sources of difficulties which corrupt the FDI system performance and can lead to undesirable behaviors of the overall FTC system. Furthermore, when a fault has been detected and the reconfiguration has been enabled, not only a new control law should be triggered but the running FDI algorithm should also be adapted to the new system configuration. This typical FTC procedure gives rise to computational burden and system complexity which may decrease the overall FTC system reliability.

In this paper, we introduce a novel real-time fault-tolerant control procedure which has a supervisory structure (Morse, 2003) and which is able to maintain acceptable level of performance subsequently to the occurrence of a class of faults. The key feature of this real-time FTC procedure is that it makes no use of an online plant model and therefore it does not experience the drawbacks of fault-tolerant control systems made up of on-line model-based detection algorithm. A byproduct of the proposed model-free procedure is that the fault-tolerant control algorithm is fast and reliable. The logic of the reconfiguration mechanism is derived from the theory of unfalsified control (Safonov and Tsao, 1997) and the adaptation

[1] This work is supported by the European project IFATIS under the Information Society Technology Research programme IST2001

of the control laws to a faulty situation is based on a real-time closed-loop performance measure and on the experimental data. The theory is applied to a two-tanks pilot plant and issues of implementation are considered. For more details on the theory, we refer to Yamé and Kinnaert (2003).

2. SYSTEM BEHAVIOR MODELING AND PROBLEM FORMULATION

As a paradigm for describing the operation of a plant, including its nominal and faulty states, we introduce a general model structure referred as the behavioral approach (J.C. Willems, 1986; J.C. Willems, 1991). From this general model structure perspective, a dynamical plant is simply a subset of time-trajectories, that is, a family of time signals taking on values in an appropriate signal space. The following gives a precise definition of the concept of dynamical system.

Definition 1. A dynamical system Σ is a triple $\Sigma = (\mathbb{T}, \mathbb{S}, \mathcal{B})$ where $\mathbb{T}$ is a subset of $\mathbb{R}$, called the time axis, $\mathbb{S}$ a set called the signal space, and $\mathcal{B}$ a subset of $\mathbb{S}^{\mathbb{T}}$ called the *behavior*. ($\mathbb{S}^{\mathbb{T}}$ is the set of *all* $\mathbb{S}$-valued time trajectories)

The set $\mathbb{S}$ is the space in which the system time-signals take on their values and the behavior $\mathcal{B} \subseteq \mathbb{S}^{\mathbb{T}}$ is a *family* of $\mathbb{S}$-valued time trajectories.The elements of $\mathcal{B}$ are precisely the signals $s : \mathbb{T} \to \mathbb{S}$ which can occur and which are *compatible* with the laws governing the dynamical system Σ whilst those outside $\mathcal{B}$ cannot occur. A controller C for the plant $\mathcal{G}$ is a dynamical system $\Sigma_C = (\mathbb{T}, \mathbb{S}, \mathcal{B}_C)$ acting on the same time axis $\mathbb{T}$ and the same signal space $\mathbb{S}$ as $\mathcal{G}$. When the plant and the controller are connected, we denote the interconnected system by $\Sigma_{\mathcal{G}} \wedge \Sigma_C$. In that case, the plant signals are constrained to obey the laws of *both* the plant and the controller. The behavior of the interconnection $\Sigma_{\mathcal{G}} \wedge \Sigma_C$ consists of those trajectories $s : \mathbb{T} \to \mathbb{S}$ that are compatible with the laws of $\Sigma_{\mathcal{G}}$ and those of Σ_C, i.e.,

$$\Sigma_{\mathcal{G}} \wedge \Sigma_C = (\mathbb{T}, \mathbb{S}, \mathcal{B}_{\mathcal{G}} \cap \mathcal{B}_C) \tag{1}$$

The problem of controlling the plant $\mathcal{G}$ can be described as that of choosing a controller Σ_C so as to impose that $\Sigma_{\mathcal{G}} \wedge \Sigma_C$ behaves like a *desired* dynamical system $\Sigma_J = (\mathbb{T}, \mathbb{S}, \mathcal{B}_J)$ where $\mathcal{B}_J \subseteq \mathbb{S}^{\mathbb{T}}$ is the set of signals constrained by the requirement on a performance functional J. The set $\mathcal{B}_J$ is explicitly and usually given by $\mathcal{B}_J = \{s \in \mathbb{S} : J(s) < \gamma\}$ where γ is a real bound. The performance functional J is assumed to capture the control objective and examples of such functionals are the integrated absolute control error (IAE), plant output variance, peak value of plant output, etc... Note that in this framework, the control performance specification is simply viewed as a behavior, i.e., a set of constrained signals. From the behavior of the interconnected system (1), the following obvious proposition gives a simple condition for a controller to meet the control performance specification.

Proposition 2. A necessary and sufficient condition for the controller Σ_C to implement a controlled system $\Sigma_{\mathcal{G}} \wedge \Sigma_C$ which behaves as the desired dynamical system Σ_J is

$$\mathcal{B}_J \supseteq \mathcal{B}_{\mathcal{G}} \cap \mathcal{B}_C \neq \varnothing \tag{2}$$

Now, consider the fault-tolerant control problem. If the plant is subject to faults, then the effect of a fault acting on that plant is that the behavior changes since new constraints should be satisfied by the signals in order to represent the faulty plant. For a fault f acting on the plant, the behavior becomes $\mathcal{B}_{\mathcal{G}_f}$ and the control objective requirement (2) may no longer be satisfied by the current controller. To achieve fault tolerance, the control law should be changed in order to constrain the behavior of the faulty plant to the set $\mathcal{B}_J$, that is,

$$\mathcal{B}_J \supseteq \mathcal{B}_{\mathcal{G}_f} \cap \mathcal{B}_{C_f} \neq \varnothing \tag{3}$$

where C_f is the new corrective control law. In order to be able to automatically tolerate and accommodate for faults in a given plant, a necessary preliminary step should provide a systematic examination of potential faults/failures, analyze the effects of each fault/failure on the plant operation and identify appropriate corrective actions. We will assume that, at the outset, such an analysis has been performed and for the corrective actions, a finite set of control laws

$$\mathcal{C} = \{C_1, ..., C_N\} \tag{4}$$

has been designed to accommodate the faults that might occur in the plant. Throughout, we will assume that for the class of faults considered, the control solution does not modify the physical channels of the input/output signals of the plant. The problem we aim to solve is how to effectively implement the fault-tolerant control system in *real time* without an *online* plant-model based FDI algorithm. Note that the preliminary systematic analysis reduces to determining, for the whole operation of the plant, an appropriate plant-model set for the faults on which a (off-line) design of a set of controllers is performed to satisfy the control objective as imposed by equation (2). With such a pre-designed set of corrective controllers (4), it is clear that a satisfactory performance will be obtained for some controller in that set when a fault occurs during plant operation.

3. STRUCTURE OF THE FTC SYSTEM

From the considerations of section 2, a natural structure of the fault-tolerant control system is that of a supervisory system in which a high-level controller, called the "supervisor", orchestrates the switching of the controllers from the set (4), into feedback with the plant, so as to maintain the control objective despite the occurrence of faults. The structure of the FTC system is shown in figure 1. The supervisor task

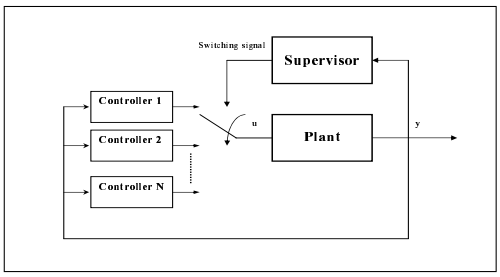

Fig. 1. Supervisory FTC system

is to decide *when* to change the control law and *which* controller should be switched into feedback with the evolving unknown plant. The task of deciding when to change an active controller is easily performed from the observed data by computing the real-time performance functional of the closed-loop system. However, when a change of controller is initiated, the task of selecting a new controller is less evident since no online model of the plant is used to determine the actual faulty mode. From the hypothesis of the existence of at least one corrective controller in the pre-designed set (4) for any fault occurring in the plant, a naive solution to the controller selection would be to experimentally evaluate each potential controller's performance by applying it to the plant. Unfortunately, the N potential controllers cannot be simultaneously tested in the feedback loop. To bypass this difficulty, we should be able to directly identify the right corrective controller to be switched into feedback using only the experimental information up to the current time. Therefore, the problem amounts to inferring the behavior of the feedback loop consisting of the unknown plant and a given controller from the observed data produced by the plant driven by a different controller. Using the notion of behavior introduced in section 2 and the concept of unfalsified control (Safonov and Tsao, 1997), we show how such inference can be made. At this stage, it is worth noting that the set $\mathcal{B}_{\mathcal{G}}$ considers all signals which can occur as outcomes of the plant $\mathcal{G}$, however only measurements from the experimental setting are available for actual running systems. These measurements give a partial knowledge about the system and might be thought as representing a somewhat small set of the behavior of the dynamical system. Let $\mathcal{B}_{\mathcal{G}_{data}}$ be the subset of the plant behavior $\mathcal{B}_{\mathcal{G}}$ corresponding to the experimental observed data up to the current time. Clearly $\mathcal{B}_{\mathcal{G}_{data}}(\subseteq \mathcal{B}_{\mathcal{G}})$ constitutes a partial knowledge through our observation of the running unknown plant up to the current time. With this known subset $\mathcal{B}_{\mathcal{G}_{data}}$, it is possible to verify if a potential controller C would have implemented a closed-loop system $\Sigma_{\mathcal{G}} \wedge \Sigma_C$ satisfying the performance goal through the test

$$\mathcal{B}_J \supseteq \mathcal{B}_{\mathcal{G}_{data}} \cap \mathcal{B}_C \neq \varnothing \tag{5}$$

If the test is affirmative at the current time, then controller C is said to be unfalsified by the experimental data $\mathcal{B}_{\mathcal{G}_{data}}$. This means that controller C met the performance objective if it had been connected to the plant up to the current time and therefore it should be provisionally retained in the loop until it is superseded (or falsified) by a better controller. Note that since $\mathcal{B}_{\mathcal{G}_{data}}$ is not related to any particular experimental setting , the above test turns out to be a powerful tool to assess the performance of a potential controller even if this controller is not actually operating in the loop. To perform the controller falsification test, consider the standard two-degree-of-freedom controller structure of figure 2. The available data produced by the plant

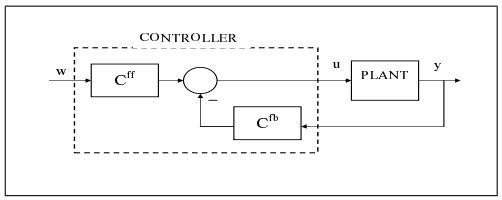

Fig. 2. Basic feedback loop

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 (4) based on the measured data $(u^{(m)}, y^{(m)})$ proceeds as follows. The behavior of controller C_k is given by the set

$$\mathcal{B}_{C_k} = \{s = (w, u, y) \in \mathbb{S}^T : u = C_k^{ff} w - C_k^{fb} y\} \tag{6}$$

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

$$w_k = (C_k^{ff})^{-1} \left\{ u^{(m)} + C_k^{fb} y^{(m)} \right\} \tag{7}$$

where we have assumed that the feed-forward component of the controller's transfer function has a causal inverse. Note that this assumption is not so restrictive since the controllers can be designed to be bi-proper. The triple $s_k = (w_k, u^{(m)}, y^{(m)})$ is therefore the signal in $\mathbb{S}^T$ which is compatible with the behavior obtained by interconnecting controller C_k to the unknown plant. Controller C_k is unfalsified by the experimental data $\mathcal{B}_{\mathcal{G}_{data}}$ produced by the unknown plant whenever $s_k \in \mathcal{B}_J$, that is when the value of the performance functional J at $s_k \in \mathbb{S}^{\mathbb{T}}$ satisfies $J(s_k) \leq \gamma$. Equation (7) defines a filter F_k which reconstructs the reference signal w_k from the measurements of (u, y). The above procedure can be applied to any controller in the set (4) of the N potential controllers, thus yielding N performance indexes $\{J(s_i), i = 1, 2, ...N\}$. The unfalsified controllers are those controllers with index i such that $J(s_i) < \gamma$. It remains to select the right unfalsified controller to be switched in the loop. The control selection algorithm has input $\{J(s_i)\}_{i=1}^N$ and output σ where σ is the switching signal, that is, a function from the time axis $\mathbb{T}$ to the controllers index set: $\sigma = \mathbb{T} \to \{1, 2, ...N\}$. To avoid arbitrary small switching times which can destabilize the overall system, it is necessary to impose a lower bound on the lenght of intervals between successive switches. This minimum lenght of time in which a controller is active in the

loop, called the *dwell time*, can be fixed by collecting the measured data on time intervals $[t_n, t_n + \tau_D]$ of lenght $\tau_D > 0$. The logic is then realized through

$$\sigma(t) = \sigma(t_n) \quad \text{for } t_n \leq t < t_{n+1} \tag{8}$$

with the updating rule

$$\sigma(t_{n+1}) = \begin{cases} \sigma(t_n) \text{ if } C_{\sigma(t_n)} \text{ is not invalidated} \\ \widehat{k} = \arg\min \{ J(s_k) | \, J(s_k) \leq \gamma \}_{k \neq \sigma(t_n)} \end{cases} \tag{9}$$

The switching logic enforces 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 occurence of a fault to the invalidation of the active controller. Note that a short detection delay requirement will need a short dwell-time τ_D which clearly conflicts with the stability of the closed-loop switched system. The dwell-time should result from a trade-off between the requirements on stability and the detection delay depending on the faults scenarios and their severity. The time for reconfiguration, i.e. the time needed after a controller invalidation to the selection of the next controller is however quasi-instantaneous needing only the computation time.

4. CASE STUDY: A TWO-TANKS PLANT

In the framework of the IFATIS project, a simple pilot plant has been devised for testing and integrating the FTC softwares developed by the project partners. This plant is a two-tanks system depicted in figure 3 and full details on its characteristics are reported in (Hamelin et al., 2004). The technique developed in the previous section has been applied to the plant.

4.1 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 figure 3). The control inputs to the plant are the voltages V_{pump_1}, V_{pump_2} 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^*.

4.2 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

$$\begin{aligned} S_1 \dot{Q}_1 &= Q_1 - Q_{12} - Q_{F1} \\ S_2 \dot{Q}_2 &= Q_2 + Q_{12} - Q_{F2} \end{aligned} \tag{10}$$

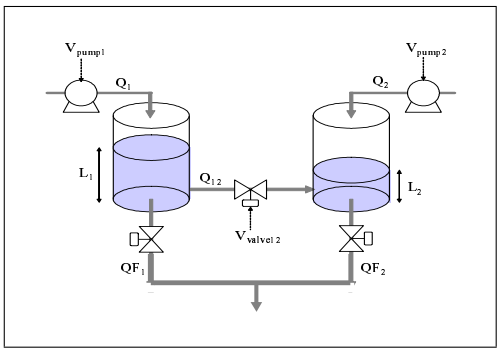

Fig. 3. The IFATIS two-tanks plant

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

$$\begin{aligned} &Q_1 = \pi_1(V_{pump_1}), \; Q_2 = \pi_2(V_{pump_2}) \\ &Q_{F1} = R_1\sqrt{L_1}, \quad Q_{F2} = R_2\sqrt{L_2} \end{aligned} \tag{11}$$

and

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

where π_1, π_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 throtlling 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 Hamelin et al. (2004). 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

$$L_1^0 = \left(\frac{y_1^* y_2^*}{R_1 (1 + y_2^*)} \right)^2, \quad L_2^0 = \left(\frac{y_1^*}{R_2 (1 + y_2^*)} \right)^2 \tag{13}$$

4.3 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 in the IFATIS project take care of such faults.

4.4 Design of the feedback controllers

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 (10) at the nominal operating point yields

$$\dot{x} = Ax + B_v v,\ y = Cx \tag{14}$$

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

$$A = \begin{pmatrix} -0.0037 & -0.0017 \\ -0.0018 & -0.0035 \end{pmatrix} \tag{15}$$

$$B_v = \begin{pmatrix} 64.9351 & 0 & -0.0001 \\ 0 & 65.7895 & 0.0002 \end{pmatrix},\ C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{16}$$

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 (14). Two multivariable digital controllers, with sampling period $h = 1s$, 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 controller's 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 (Balasubramanian, 1989) 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 w, the tracking error signal $e = w - y$ has the dynamics

$$\dot{e} = -C\xi \tag{17}$$

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

$$\dot{z} = \mathcal{A}z + \mathcal{B}\mu \tag{18}$$

with $z = \begin{pmatrix} e \\ \xi \end{pmatrix}$, $\mathcal{A} = \begin{pmatrix} 0 & -C \\ 0 & A \end{pmatrix}$, $\mathcal{B} = \begin{pmatrix} 0 \\ B \end{pmatrix}$ where B is the 2×2 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 (18) is also controllable (Balasubramanian, 1989). Hence, this system can be stabilized by a state feedback law

$$\mu = -Kz = -\begin{bmatrix} K_1 & K_0 \end{bmatrix} \begin{pmatrix} e \\ \xi \end{pmatrix} \tag{19}$$

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

$$u(t) = -K_1 \int_0^t e(\tau)\, d\tau - K_0 x(t) + u_0 \tag{20}$$

where $u_0 = u(0)$. Note that controller (20) has the structure of an integral (on the error) and state-feedback controller. In order to meet the requirement for constructing the filters (7), the feed-forward part of the controllers should be causally invertible. Therefore, we modify the structure (20) to a "Proportional+Integral" (on the error) structure by explicitly introducing a feed-forward matrix gain G_{ff}.

$$u(t) = G_{ff}.w - K_1 \int_0^t e(\tau)\, d\tau - K_0 x(t) + u_0 \tag{21}$$

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

$$u(t) = K_0 e(t) - K_1 \int_0^t e(\tau)\, d\tau + u_0 \tag{22}$$

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 (18). The design parameters are the weighting matrices Q and R of the performance index $\mathcal{J} = \int_0^\infty (z^T Q z + u^T R u) dt$. 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

$$Q_0 = 10^{-3}.\begin{pmatrix} 0.1 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 \\ 0 & 0 & 0.4 & 0 \\ 0 & 0 & 0 & 0.4 \end{pmatrix} \tag{23}$$

$$Q_{fault} = \begin{pmatrix} 0.1 & 0 & 0 & 0 \\ 0 & 0.1024 & 0 & 0 \\ 0 & 0 & 0.0004 & 0 \\ 0 & 0 & 0 & 6.5536 \end{pmatrix} \tag{24}$$

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

$$K_0 = \begin{pmatrix} 0.0153 & 0 \\ 0 & 0.0151 \end{pmatrix},\ K_1 = \begin{pmatrix} -0.0047 & 0 \\ 0 & -0.0047 \end{pmatrix} \tag{25}$$

and those of the faulty mode digital controller are

$$K_0 = \begin{pmatrix} 0.0153 & 0.0069 \\ 0 & 0.0398 \end{pmatrix},\ K_1 = \begin{pmatrix} -0.0047 & -0.0009 \\ 0 & -0.0045 \end{pmatrix} \tag{26}$$

Having the set of controllers for the different modes, the supervisor can now be designed to select in real time the right controller based on the actual process input/output data. From section 3, the explicit structure of the supervisor consists in a system of filters (7), a performance indices generator, and a control selection algorithm as depicted in figure 4. Note

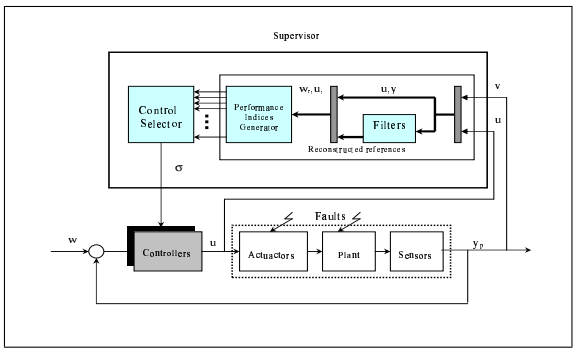

Fig. 4. Block Diagram of the FTC system

that the system of filters (7) is uniquely determined from the set of controllers. These filters reconstructs "virtual" reference signals as if the controller were in the loop. Then, using these virtual references and the plant input/output data, the performance generator computes the values of the inferred performance functional of each potential controller. Finally, the control selector implements controller switching into feedback through the algorithm (8),(9). The performance functional chosen here is the ISE (Integral of Squared Error).

$$J = \int_{t_n}^{t_{n+1}} \|e(\varsigma)\|_2^2 \, d\varsigma \qquad (27)$$

where $\|e(\varsigma)\|_2$ is the Euclidian norm of 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 dwell time given by $\tau_D = \ell h$ for an integer ℓ, with t_n the instants of possible switchings and h the sampling period of the feedback loop.
- The performance threshold γ. This threshold should be set in a way such that the two modes can be discriminated.

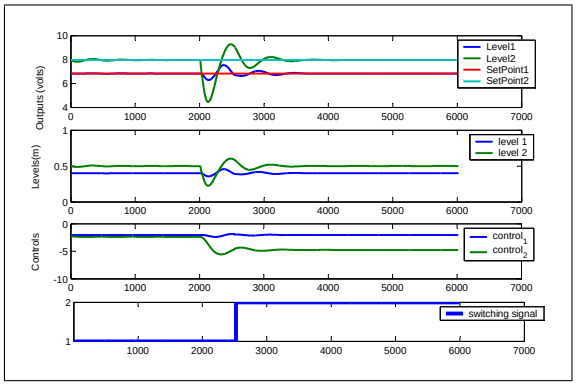

Fig. 5. Closed-loop signals with supervisory FTC of the two-tanks plant

These parameters are set to $\gamma = 1$, $\tau_D = 180s$. An experiment is run with the power loss of pump 2 appearing at time $2000s$. The closed-loop signals of figure 5 show that the real-time FTC system successfully reacts at time $2500s$ by switching to controller 2 (faulty mode controller). 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.

5. CONCLUDING REMARKS

In this paper, we have presented a new real-time fault-tolerant control scheme which is based on the data produced by an operating plant with *no* online plant-model for fault detection. The threshold on the performance functional values plays the role of a detector of unexpected changes or faults in the *closed-loop* system. However, the system has not the ability to diagnose or isolate a fault in real time. Hence, the proposed FTC scheme is limited to cases where the hardware components in the loop remain invariant with respect to fault scenarios. The important benefit of the proposed supervisory scheme is that it rules out the use of unsatisfactory controllers in the feedback loop and therefore enhances the reliability of the overall FTC system. A computational property of the algorithm is that it is fast because no convergence process takes place in the supervisor as in FDI-based scheme using observers or parameter estimation techniques. A simple case study applying the proposed FTC technique on a pilot plant has shown that the method is effective for a class of faults.

REFERENCES

Balasubramanian, R.(1989), *Continuous-time Controller Design*. Peter Peregrinus Ltd., London

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

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

Morse A.S. (1996), Supervisory Control of Families of Linear Set-Point Controllers. Part 1: Exact Matching. *IEEE Transactions on Automatic Control*, Vol. 41, N°10, pp. 1413-1431

Patton, R.J.(1997), Fault-tolerant Control Systems: The 1997 Situation. *Proceedings of the IFAC SAFEPROCESS'97*

Safonov M.G., Tsao T-C.(1997), The Unfalsified Control Concept and Learning. *IEEE Transactions on Automatic Control*, Vol. 42, N°6, pp. 843-847

Willems, J.C.(1986), From Time Series to Linear Systems. Part II. Exact Modelling. *Automatica*, Vol. 22,N°6, pp. 675-694

Willems, J.C.(1991), Paradigms and Puzzles in the Theory of Dynamical Systems. *IEEE Transactions on Automatic Control*, Vol. 36, N°3, pp. 259-294

Yamé, J., Kinnaert M.(2003), Performance-Based Switching for Fault-Tolerant Control. *Proceedings of the 5th IFAC SAFEPROCESS*, Washington D.C., USA, pp. 555-560