*Int. J. Appl. Math. Comput. Sci.*, 2011, Vol. 21, No. 3, 457–466
DOI: 10.2478/v10006-011-0034-x

# PERFORMANCE EVALUATION BASED FAULT TOLERANT CONTROL WITH ACTUATOR SATURATION AVOIDANCE

BOUMEDYEN BOUSSAID [*,**], CHRISTOPHE AUBRUN [*], MOHAMED NACEUR ABDELKRIM [**],
MOHAMED KONI BEN GAYED [**]

[*] Research Centre in Automation of Nancy (CRAN)
Nancy University, CNRS, BP 239, 54506 Vandoeuvre Cedex, France
e-mail: {boussaid.boumedyen,christophe.aubrun}@cran.uhp-nancy.fr

[**]Modelling Analysis and Control of Systems (MACS)
Gabès University, Omar Ibn Khattab Road, 6029 Gabès, Tunisia
e-mail: naceur.abdelkrim@enig.rnu.tn,mbengayed@yahoo.fr

In this paper, a new approach regarding a reconfigured system is proposed to improve the performance of an active fault tolerant control system. The system performance is evaluated with an intelligent index of performance. The reconfiguration mechanism is based on a model predictive controller and reference trajectory management techniques. When an actuator fault occurs in the system, a new degraded reference trajectory is generated and the controller calculates new admissible controls. A constraint set and cost function are established to avoid actuator saturation and reduce the control energy spent in closed loop dynamics. The effectiveness of the proposed method is illustrated using a hydrothermal system subject to actuator faults and constraints on actuator dynamic ranges.

**Keywords:** fault tolerant control systems, performance degradation, reference management, model predictive control, performance index.

## 1. Introduction

Industrial systems have become more sophisticated and complex. This complexity leads to an increased request for reliability, reconfigurability and safety of the systems. In order to guarantee the properties quoted above, it is essential to develop methods of supervision such as diagnosis and Fault Tolerant Control (FTC). Recently, the importance of FTC systems becomes increasingly apparent, and significant amount of research has already been done in this area (Patton, 1997; Korbicz *et al*., 2004; Guerra *et al*., 2006; Lunze and Richter, 2008; Zhang and Jiang, 2008; Noura *et al*., 2009; Puig, 2010).

According to a variety and severity of faults that may affect the system, different levels of performance have to be considered in different fault scenarios. From safety region to danger region, degraded performances are often acceptable. In addition, to ensure that the closed-loop system be able to track a command input or a reference model/trajectory even in the event of faults, a reconfigurable feed-forward controller has to be synthesized to achieve command tracking (Zhang and Jiang, 2003). In the case of performance degradation and actuator saturation avoidance being required, reference management may need to be used to adjust the command input or reference trajectory automatically or provide advisory information to human operators in the event of faults.

To the best of our knowledge, few works have published on the topic of reference management for fault tolerant systems. However, there are still many open issues which have to be addressed. Jiang and Zhang (2002; 2006) have proposed a reference management approach based on graceful performance degradation and explicit model-following techniques. When a fault is detected by the Fault Detection and Diagnosis (FDD) algorithm, a reconfigurable controller is automatically designed so that the dynamics of the closed-loop system match those of the reference model known as the performance reduced reference model. Another case of multiple actuator failures is studied by Zhang *et al*. (2008). The approach proposed by Theilliol *et al*. (2008) is based on a modified recovery control system in which the reconfigurable reference input, applied when an actuator fault occurs in the system, is determined by considering the error between the reference and the output as an impulse signal. In the work of Theilliol *et al.* (2009), the modified reference trajectory is computed by minimizing the output-tracking error by a cost function based on the control energy concept.

Other approaches using set-point optimization based on Model Predictive Control (MPC) algorithms are discussed by Marusak and Tatjewski (2008) as well as Tatjewski (2010), who propose a predictive constrained set-point optimizer in order to deal with system faults. The capabilities of MPC algorithms to perform a reconfiguration action after a fault occurrence are quite limited by the accuracy of the FDD stage (Maciejowski, 2002; Ding *et al.*, 2004; Boussaid *et al.*, 2009). To deal with model uncertainty after a fault occurrence induced by the fault detection mechanism error, robust approaches have been proposed by Bemporad and Morari (1999) as well as Cannon and Kouvaritakis (2005).

This paper proposes a method to reconfigure the reference trajectory based on performance evaluation with different levels of achievable performance in the presence of various faults under given potential system performance limitations. In the present work, the capabilities of MPC to handle on-line system constraints and reference trajectory management are exploited to design a fault tolerant controller.

The main contribution of this paper is to introduce a new methodology to generate an explicit degraded reference trajectory and an admissible control set after an actuator fault has occurred. A hydrothermal example is used to illustrate the concepts and the design procedures, and some simulation results are shown. The paper is organized as follows. Some performance backgrounds are considered in Section 2. Problem formulation is detailed in Section 3. Section 4 is dedicated to the design of the fault tolerant controller based on reference trajectory management and model predictive control. Numerical examples with simulation results are presented in Section 5 to illustrate the proposed scheme, followed by conclusions in Section 6.

## 2. Performance analysis principle

**2.1. System operating modes.** A fault tolerant system has three distinct operating modes (Blanke *et al.*, 2006):

- *Nominal mode:* this mode corresponding to normal operating characteristics. In this mode, all objectives are assumed to be attainable. That means that, if nominal control signals are sent to the actuators, nominal performances will be provided.

- *Faulty mode:* after a fault occurrence, the system switches to an abnormal operating mode which is called the “Faulty mode”. In this condition, the system provides faulty performances for nominal controls. The faulty mode may induce different system behavior depending on fault severity.

- *Degraded mode:* this mode is a temporary operating mode. In this mode, the system continues to work with acceptable objectives/performances. These performances are considered to be degraded and the control signals are supposed to be admissible.

The objective of fault tolerant control is to establish a strategy of control which has the property to limit or even cancel the effects of a fault on the performances of the plant. This strategy must modify the control structure according to the fault severity. In certain situations, particularly when the degradation of the performances is critical, fault tolerance should be achieved by modifying both the set point of the process and the control parameters in a way that releases constraints on the actuators. Then, the new operating points allow the system to recover performances as close as possible to the nominal ones (Aubrun *et al.*, 2003; Zerz, 2008).

**2.2. Performance consideration.** Usually, the controller is designed for the faultless plant in order to meet given performance specifications in a closed loop. FTC has the ability to react on the existence of the fault in order to satisfy the declared performances. Production systems have some various objectives to reach. These objectives are usually expressed in terms of quality, energy cost, time constraints, etc. On the other hand, objectives should be reached under certain constraints related to

- systems stability,

- the error between the reference signal and the output signal which impacts, e.g., on the product quality,

- robustness against disturbances or parameter variations,

- fault tolerance.

Hence, a fault tolerant system works in a closed loop to maintain the performance specifications expected by the operator (Fig. 1).

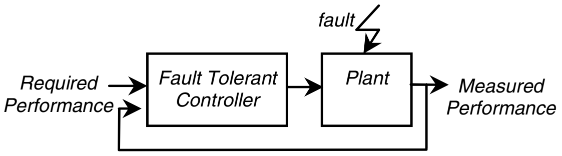

Fig. 1. Fault tolerant system closed loop.

The system operations can be decomposed into three functioning modes: nominal, faulty and degraded. The principle of performance degradation is illustrated in Fig. 2. Due to the occurrence of a fault, the system deviates from its nominal functioning mode, defined by a pair ($\pi_{\rm nom}$,$\upsilon_{\rm nom}$), to a faulty operating point ($\pi_f$,$\upsilon_f$).

The goal of the accommodation procedure is to determine a new control law that takes the degraded system parameters into account and drives the system to a new operating point ($\pi_{\rm deg}$,$\upsilon_{\rm deg}$), with respect to the control constraints.

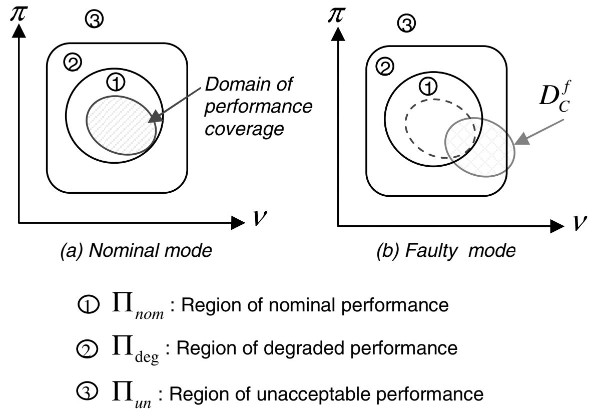
π
③
②
①
Domain of performance coverage
v
(a) Nominal mode
π
③
②
①
$D_C^f$
v
(b) Faulty mode
① $\Pi_{nom}$ : Region of nominal performance
② $\Pi_{\rm deg}$ : Region of degraded performance
③ $\Pi_{un}$ : Region of unacceptable performance

Fig. 2. Domain of performance coverage in nominal and faulty mode functioning.

Let us consider $\Pi$ as the set of all possible performances $\pi$ and $\upsilon$ as the pair ($u$,$o$),

$$\Pi \triangleq \{\pi : \upsilon = (u, o) \in \mathbb{R}^m \times \mathbb{R}^n\}, \tag{1}$$

where $\pi$, $u$ and $o$ are respectively the performance, control and objective vectors. It is easy to see that

$$\Pi = \Pi_{\rm nom} \cup \Pi_{\rm deg} \cup \Pi_{\rm un}, \tag{2}$$

where $\Pi_{\rm nom}$, $\Pi_{\rm deg}$ and $\Pi_{\rm un}$ are depicted in Fig. 2.

In order to explain the difference between each operating mode, we introduce the domain of performance coverage, $D_C$, for a controlled and stable system, which is defined as

$$D_C := \{\pi \in \Pi : (u, o) \in (U, O)\}, \tag{3}$$

where $U$ and $O$ are respectively the control and objective sets. Figure 2(a) shows that this domain is entirely included in the required performance region, $\Pi_{\rm nom}$. In a faulty case (Fig. 2(b)), this domain is moved in space, which leads to cross the degraded and/or the unacceptable performance region depending to the severity of the fault.

Let us consider the following sets for nominal and faulty cases:

$$D_C^{\rm nom} \triangleq \{\pi \in \Pi_{\rm nom} : (u, o) \in (U_{\rm nom}, O_{\rm nom})\}, \tag{4}$$

$$D_C^f \triangleq \{\pi \in \Pi : (u, o) \in (U_f, O_f)\}. \tag{5}$$

For a perfect design of the nominal controller, the domain of performance coverage should be completely included in the nominal performance region, $D_C^{\rm nom} \cap \Pi_{\rm nom} = D_C^{\rm nom}$. In the faulty case, it can be decomposed into three partial domains, $D_C^{\rm nom}$, $D_C^{\rm deg}$ and $D_C^{\rm un}$, which represent the nominal, degraded and unacceptable performance coverage domains, respectively:

$$D_C^f = D_C^{\rm nom} \cup D_C^{\rm deg} \cup D_C^{\rm un} \tag{6}$$

with

$$\begin{cases} D_C^{\rm nom} = D_C^f \cap \Pi_{\rm nom}, \\ D_C^{\rm deg} = D_C^f \cap \Pi_{\rm deg}, \\ D_C^{\rm un} = D_C^f \cap \Pi_{\rm un}. \end{cases}$$

The following different cases arise:

*Case 1:* $D_C^{\rm nom} \neq \varnothing$.
In this case, the system is completely reconfigurable and the nominal objectives are achieved.

*Case 2:* $D_C^{\rm nom} = \varnothing$ and $D_C^{\rm deg} \neq \varnothing$.
This means that the nominal objectives are not achievable. Only the degraded objectives are met if they are accepted by the supervision instructions.

*Case 3:* $D_C^{\rm nom} = \varnothing$, $D_C^{\rm deg} = \varnothing$ and $D_C^{\rm un} \neq \varnothing$.
In this case, the fault is severe and the system should be stopped. Then, maintenance operations could be performed.

### 2.3. Performance evaluation.

The performance is evaluated by means of the following performance index:

$$\varepsilon_\pi = \frac{\|o - \pi\|_2}{\|o\|_2}, \tag{7}$$

where $o$ and $\pi$ represent the objective and the measured performance, respectively.

In practice, the performance of a system is measured at each sampling time $k$ which induces the computation of the performance index at each sampling time. It can be noticed that, for an abrupt variation in the output, it is meaningful to comment this index. To solve this problem, we propose here to use a moving average of the measured performance $\bar{\pi}$ through a receding horizon $h$:

- simple moving average:

$$\bar{\pi}(k) = \frac{1}{h}\sum_{i=0}^{h-1} \pi(k - i), \tag{8}$$

- weighted moving average:

$$\bar{\pi}(k) = \sum_{i=0}^{h-1} \alpha_i \pi(k - i), \tag{9}$$

with

$$\sum_{i=0}^{h-1} \alpha_i = 1, \quad \alpha_i > \alpha_{i-1}.$$

Here $\alpha_i$ can be chosen as a geometric progression:

$$\alpha_i = q_0 \cdot q^i$$

with $0 < q < 1$ and

$$q_0 = \frac{1-q}{1-q^h}.$$

The sampled performance index becomes

$$\varepsilon_\pi(k) = \frac{\|o(k) - \bar{\pi}(k)\|_2}{\|o(k)\|_2}. \tag{10}$$

Using the following thresholds: $\varepsilon_\pi^{\mathrm{nom}}$, $\varepsilon_\pi^{\mathrm{deg}}$ and $\varepsilon_\pi^{d}$, the performance sets for each region could be defined as

- $\Pi_{\mathrm{nom}} \triangleq \{\pi : 0 \le \varepsilon_\pi \le \varepsilon_\pi^{\mathrm{nom}}\}$,
- $\Pi_{\mathrm{deg}} \triangleq \{\pi : \varepsilon_\pi^{\mathrm{nom}} < \varepsilon_\pi \le \varepsilon_\pi^{\mathrm{deg}}\}$,
- $\Pi_{\mathrm{un}} \triangleq \{\pi : \varepsilon_\pi^{\mathrm{deg}} < \varepsilon_\pi\}$.

These thresholds are fixed by the operator according to the plant requirements such as safety, production quality, energy spent, etc.

## 3. Problem statement

Let us consider a nominal and faulty system described by the following state space representations:

$$S_{\mathrm{nom}} : \begin{cases} x(k+1) = A_n x(k) + B_n u(k), \\ \quad y(k) = C_n x(k), \end{cases} \tag{11}$$

$$S_f : \begin{cases} x(k+1) = A_f x(k) + B_f u(k), \\ \quad y(k) = C_f x(k), \end{cases} \tag{12}$$

where $x(k) \in \mathbb{R}^n$ is the state vector, $u(k) \in \mathbb{R}^m$ is the input vector, $y(k) \in \mathbb{R}^p$ is the output vector, and $(A_n,B_n,C_n)$ represents the system in the nominal behavior and $(A_f,B_f,C_f)$ represents the system in the faulty case.

First of all, it is supposed that the system is stable and controlled in three operating modes, and the structures ($S_{\mathrm{nom}}$ and $S_f$ ) are known in nominal and faulty cases. It is also assumed that the state matrices $(A_n,B_n,C_n)$ and $(A_f,B_f,C_f)$ are detectable in both cases. Thus, we can define the following sets: the set of the nominal controls, $U_{\mathrm{nom}}$, which correspond to the normal operating mode, and the set of the faulty controls, $U_f$, which lead to abnormal functioning. The two sets can be written as

$$\begin{aligned} U_{\mathrm{nom}} \triangleq \{u^{\mathrm{nom}} : u_{j,\min}^{\mathrm{nom}} \le u_j^{\mathrm{nom}} \le u_{j,\max}^{\mathrm{nom}}, \\ 1 \le j \le m, o \in O_{\mathrm{nom}}\}, \end{aligned} \tag{13}$$

$$\begin{aligned} U_f \triangleq \Big\{u^f \in U_{\mathrm{nom}} : u_{j,\min}^{f} \le u_j^{f} \le u_{j,\max}^{f}, \\ 1 \le j \le m, o \in O_f\Big\}, \end{aligned} \tag{14}$$

where $m$ is the number of actuators, $(u_{j,\min}^{\mathrm{nom}}, u_{j,\max}^{\mathrm{nom}})$ stand for the pair of upper and lower control bounds for each actuator $j$ in the nominal mode, $(u_{j,\min}^{f}, u_{j,\max}^{f})$ stand for the pair of upper and lower control bounds for each actuator $j$ in the faulty mode, $o$ is the objective, $O_{\mathrm{nom}}$ denotes the objective set in the nominal mode, $O_f$ means the objective set in the faulty mode.

For the sake of simplicity, only the static operating condition is considered. Without loss of generality, when this condition is established, it is assumed that $y \backsimeq y_{\mathrm{ref}}$ where $y$ represents the output trajectory and $y_{\mathrm{ref}}$ the reference trajectory that the system is supposed to be able to track. In the following, the output trajectory expresses explicitly a performance level and the reference trajectory reflects the objective that the system has to reach.

According to the previous set definitions, the following sets of nominal (respectively faulty) trajectories are defined:

$$\begin{aligned} Y_{\mathrm{nom}} \triangleq \{y^{\mathrm{nom}} : u \in U_{\mathrm{nom}}, y_j^{\min} \le y \le y_j^{\max}, \\ 1 \le j \le m\}, \end{aligned} \tag{15}$$

$$Y_f \triangleq \{y^f : u \in U_f, y_j^{\min} \le y \le y_j^{\max}, 1 \le j \le m\}. \tag{16}$$

In order to define the reference trajectories, the following sets are constructed:

$$Y_{\mathrm{ref}}^{\mathrm{nom}} \triangleq \{y_{\mathrm{ref}}^{\mathrm{nom}} : y_{\mathrm{ref}} \in D_C^{\mathrm{nom}}\}, \tag{17}$$

$$Y_{\mathrm{ref}}^{f} \triangleq \Big\{y_{\mathrm{ref}}^{f} : y_{\mathrm{ref}} \in D_C^{f}\Big\}, \tag{18}$$

where $y_{\mathrm{ref}}^{\mathrm{nom}}$ and $y_{\mathrm{ref}}^{f}$ denote the reference trajectory in nominal and faulty cases, respectively.

In the following study and for clearance, we suppose that the faults induce a slight shift of the performance coverage disc, which means that either $D_C^{\mathrm{nom}}$ or $D_C^{\mathrm{deg}}$ is nonempty. In addition, it is supposed that the degraded objectives are accepted and the corresponding controls are called admissible controls. The corresponding measured performances are also called degraded performances or degraded outputs. Hence, the set of these admissible controls, $U_{\mathrm{adm}}$, which satisfies the degraded objectives/outputs, $Y_{\mathrm{deg}}$, can be written as

$$U_{\mathrm{adm}} \triangleq \{u^{\mathrm{adm}} \in U_{\mathrm{nom}} : u^{\mathrm{adm}}_{j,\min} \leq u^{\mathrm{adm}}_{j} \leq u^{\mathrm{adm}}_{j,\max}, \\ 1 \leq j \leq m, o \in O_{\mathrm{deg}}, \} \tag{19}$$

$$Y_{\mathrm{deg}} \triangleq \{y^{\mathrm{deg}} : u \in U_{\mathrm{adm}}, y^{\min}_{j} \leq y \leq y^{\max}_{j}, \\ 1 \leq j \leq p\}, \tag{20}$$

where $(u^{\mathrm{adm}}_{j,\min}, u^{\mathrm{adm}}_{j,\max})$ is the pair of upper and lower admissible control bounds for each actuator $j$, and $O_{\mathrm{deg}}$ is the degraded objective set.

Hence, the main idea is to determine a set of reference trajectories that allow the system under faulty conditions to operate with limited/degraded performances. Basically, the reference trajectories should be included in the degraded performance coverage domain in order to ensure the attainability of the objectives/performances. Thus, the degraded reference trajectory set, $Y^{\mathrm{deg}}_{\mathrm{ref}}$ can be defined as

$$Y^{\mathrm{deg}}_{\mathrm{ref}} \triangleq \left\{ y^{\mathrm{deg}}_{\mathrm{ref}} : y_{\mathrm{ref}} \in D^{\mathrm{deg}}_{C} \right\}. \tag{21}$$

## 4. Fault tolerant controller design

**4.1. FTC mechanism.** The reconfiguration strategy of the proposed fault tolerant controller is described in Fig. 3, which includes modules of reference management, the MPC controller, FDD and the reconfiguration mechanism.

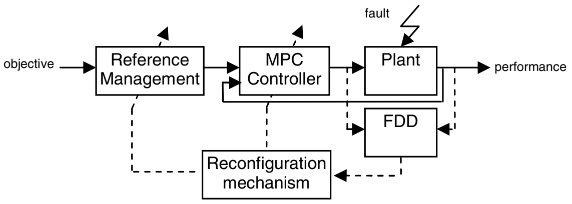

Fig. 3. Proposed FTC reconfiguration mechanism.

**4.2. Fault model.** In this study only actuator faults with the reduction of effectiveness are considered. In fact, such a fault can be considered a parametric fault modulated by a static or variable coefficient $\gamma$ comprised between 0 and 1,

$$u^{f}_{j}(k) = (1 - \gamma^{k}_{j}) u_{j}(k), \tag{22}$$

where $\gamma^{k}_{j} \in [0,1]$ and $j$ is the actuator, $j \in \{1, \dots, m\}$. In (22), the additive fault component which denotes a constant offset, occurs after actuator jamming is ignored. We only consider the loss of actuator effectiveness after fault occurrence.

Let $\Gamma^{k} \in \mathbb{R}^{m} \times \mathbb{R}^{m}$ be the distribution matrix of actuator faults:

$$\Gamma^{k} = \begin{bmatrix} \gamma^{k}_{1} & 0 & 0 \\ 0 & \gamma^{k}_{j} & 0 \\ 0 & 0 & \gamma^{k}_{m} \end{bmatrix}.$$

Equation (22) can be written as $u^{f}(k) = (I_m - \Gamma^{k})u(k)$. We set $B_f = B_n(I_m - \Gamma^{k}) = B_n - B_n\Gamma^{k}$ and get

$$\begin{aligned} x(k+1) =& A_f x(k) + B_f u(k) \\ =& A_n x(k) + B_n u(k) - B_n \Gamma^{k} u(k) \\ =& A_n x(k) + B_n u(k) + f^{\gamma}_{k}, \end{aligned}$$

where $f^{\gamma}_{k} \in \mathbb{R}^{m}$ is the vector of faults.

The FDD module should estimate the fault magnitude $\hat{f}^{\gamma}_{k}$, and then we deduce $\hat{\gamma}^{k}_{j}$ for each actuator $j$. Notice that the FDD module is beyond the scope of our study.

**4.3. Reconfiguration mechanism.** The reconfiguration module should find the pair ($u$,$o$) that makes the system operate in the nominal performance region or in the degraded performance region if the nominal ones are unachievable. Let us consider the worst case, where only the degraded performances could be met, and there exists a pair ($u_{\mathrm{adm}}$,$o_{\mathrm{deg}}$) such that $\Pi_{\mathrm{deg}}$ is nonempty. In fact, $u_{\mathrm{adm}} \in U_{\mathrm{adm}}$ and $o_{\mathrm{deg}} \in O_{\mathrm{deg}}$. Thus, the reconfiguration problem is reduced to determine the two sets $U_{\mathrm{adm}}$ and $O_{\mathrm{deg}}$.

**4.3.1. Admissible control set.** Let us start from the nominal control for an actuator $j$ in the fault-free case:

$$u^{\mathrm{nom}}_{j,\min} \leq u^{\mathrm{nom}}_{j} \leq u^{\mathrm{nom}}_{j,\max}, \tag{23}$$

where the upper and lower nominal control limits are completely known after the design of the nominal controller. Assuming that the fault occurs at the time $k_f$, and is detected at the time $k_d$ with the estimated fault magnitude $\hat{\gamma}^{k_d}$, for $k > k_d$, we have

$$(1 - \hat{\gamma}^{k_d}_{j}) u^{\mathrm{nom}}_{j,\min} \leq (1 - \hat{\gamma}^{k_d}_{j}) u^{\mathrm{nom}}_{j} \leq (1 - \hat{\gamma}^{k_d}_{j}) u^{\mathrm{nom}}_{j,\max}, \tag{24}$$

where $\hat{\gamma}^{k_d}_{j}$ is a positive real number and $\hat{\gamma}^{k_d}_{j} \in [0,1]$ so that $(1 - \hat{\gamma}^{k_d}_{j}) \in [0,1]$. Due to (23) and (24), we get

$$(1 - \hat{\gamma}^{k_d}_{j}) u^{\mathrm{nom}}_{j,\min} \leq u_{j} \leq (1 - \hat{\gamma}^{k_d}_{j}) u^{\mathrm{nom}}_{j,\max}. \tag{25}$$

We use the following notation

$$\begin{cases} u^{\mathrm{adm}}_{j,\min} = (1 - \hat{\gamma}^{k_d}_{j}) u^{\mathrm{nom}}_{j,\min}, \\ u^{\mathrm{adm}}_{j,\max} = (1 - \hat{\gamma}^{k_d}_{j}) u^{\mathrm{nom}}_{j,\max}. \end{cases}$$

Thus (25) can be re-written as

$$u_{j,\min}^{\mathrm{adm}} \le u_j \le u_{j,\max}^{\mathrm{adm}}. \tag{26}$$

Besides, the admissible control should avoid any actuator saturation. Hence

$$u_j^{\mathrm{adm}} = \sigma_j(u_j)$$

such as

$$\sigma_j(u_j) = \begin{cases} u_{j,\max}^{\mathrm{adm}} & \text{if} \quad u_{j,\max}^{\mathrm{adm}} \le u_j, \\ u_j & \text{if} \quad u_{j,\min}^{\mathrm{adm}} \le u_j \le u_{j,\max}^{\mathrm{adm}}, \\ u_{j,\min}^{\mathrm{adm}} & \text{if} \quad u_j \le u_{j,\min}^{\mathrm{adm}}. \end{cases} \tag{27}$$

The admissible control set is determined by the definition of the upper and lower control limits. These constraints should be included in the MPC problem formulation in order to avoid any actuator saturation and to let the MPC optimizer find the appropriate control signal $u_{\mathrm{adm}}$.

**4.3.2. Degraded objective set.** On the analogy of (7), the following index can be used, where $o$ represents the objective:

$$\varepsilon_o = \frac{\|o_{\mathrm{nom}} - o\|_2}{\|o_{\mathrm{nom}}\|_2}. \tag{28}$$

with $o \in O_{\mathrm{deg}}$, which means that $\varepsilon_o \le \varepsilon_o^{\mathrm{deg}}$ where $\varepsilon_o^{\mathrm{deg}}$ is a threshold fixed by the operator. In practice, the value of the threshold is defined as $\varepsilon_\pi^{\mathrm{deg}}$. $\varepsilon_o \le \varepsilon_\pi^{\mathrm{deg}}$ leads to the following bounds:

$$(1 - \varepsilon_\pi^{\mathrm{deg}}) \|o_{\mathrm{nom}}\|_2 \le \|o\|_2 \le (1 + \varepsilon_\pi^{\mathrm{deg}}) \|o_{\mathrm{nom}}\|_2 \tag{29}$$

Finally, the degraded objective set, $O_{\mathrm{deg}}$, is given by

$$O_{\mathrm{deg}} \triangleq \Big\{ o_{\mathrm{deg}} : (1 - \varepsilon_\pi^{\mathrm{deg}}) \|o_{\mathrm{nom}}\|_2 \le \|o_{\mathrm{deg}}\|_2 \le (1 + \varepsilon_\pi^{\mathrm{deg}}) \|o_{\mathrm{nom}}\|_2 \Big\}. \tag{30}$$

The optimum degraded objective should be as closed as possible to the nominal objective or the required performance. Then, it can be obtained by minimizing the following quadratic function under constraints on the control and objective:

$$o_{\mathrm{deg}}^* = \arg \min_{\substack{u_{\mathrm{adm}} \in U_{\mathrm{adm}} \\ o_{\mathrm{deg}} \in O_{\mathrm{deg}}}} \left( \|o_{\mathrm{deg}} - o_{\mathrm{nom}}\|_2 \right). \tag{31}$$

**4.4. Reference management.** As mentioned previously, the following function is defined to generate the reference trajectory input:

$$y_{\mathrm{ref}}(k) = o(k) - \tau \left( o(k) - y_{\mathrm{ref}}(k-1) \right). \tag{32}$$

where $y_{\mathrm{ref}}(0)$ means the initial condition and $\tau$ represent the system dynamics, with $\tau \in [0, 1]$ , a positive real number. After fault detection and diagnosis, the reconfigured reference trajectory, $y_{\mathrm{ref}}^{\mathrm{deg}}$, is

$$y_{\mathrm{ref}}^{\mathrm{deg}}(k) = o_{\mathrm{deg}}^*(k) - \tau \left( o_{\mathrm{deg}}^*(k) - y_{\mathrm{ref}}^{\mathrm{deg}}(k-1) \right). \tag{33}$$

**4.5. Fault tolerant MPC controller.** The control signal delivered by the MPC controller is calculated by minimizing the following cost function $J$ with the prediction horizon $h_p$ :

$$\begin{aligned} J &= \min_{u(k),\dots,u(k+h_p-1)} \sum_{i=0}^{h_p-1} \Big[ (y_{\mathrm{ref}}(k+i) - y(k+i))^T \\ &\quad Q\,(y_{\mathrm{ref}}(k+i) - y(k+i)) + u(k+i)^T R u(k+i) \Big], \end{aligned} \tag{34}$$

subject to the constraints

$$\begin{gathered} y_{\min}(k+i) \le y(k+i) \le y_{\max}(k+i), \\ u_{\min}(k+i) \le u(k+i) \le u_{\max}(k+i), \\ |\Delta u(k+i)| \le \Delta u_{\max}(k+i), \end{gathered}$$

where $y(k+i)$ is the output, $u(k+i)$ the control and $\Delta u(k+i)$ the change in the control action from one instant to another, for each discrete time $(k+i)$. The terms $\max$ and $\min$ refer to upper and lower limits, respectively. The weighting matrices $Q$ ($Q = Q^T$) and $R$ ($R = R^T$) of the cost function are positive definite and they are used to tune the MPC control law.

After fault occurrence, the cost function becomes

$$\begin{aligned} J_{\mathrm{deg}} &= \min_{u_{\mathrm{adm}}(k),\dots,u_{\mathrm{adm}}(k+h_p-1)} \sum_{i=0}^{h_p-1} \Big[ \Big( y_{\mathrm{ref}}^{\mathrm{deg}}(k+i) - y(k+i) \Big)^T \\ &\quad Q \Big( y_{\mathrm{ref}}^{\mathrm{deg}}(k+i) - y(k+i) \Big) \\ &\quad + u_{\mathrm{adm}}(k+i)^T R u_{\mathrm{adm}}(k+i) \Big], \end{aligned} \tag{35}$$

subject to the constraints

$$\begin{aligned} & y_{\min}(k+i) \le y(k+i) \le y_{\max}(k+i), \\ & u_{\min}^{\mathrm{adm}}(k+i) \le u_{\mathrm{adm}}(k+i) \le u_{\max}^{\mathrm{adm}}(k+i), \\ & |\Delta u(k+i)| \le \Delta u_{\max}(k+i). \end{aligned}$$

## 5. Numerical example

The system to be studied is a hydrothermal process which consists of a tank with natural racking and electric heating (Boussaid *et al.*, 2008). In this plant, the fluid is introduced into the tank with a controlled flow $q_e$, using the control input $u_q$. The fluid is evacuated with the flow $q_s$ through a manual valve $V_m$. The electric heating system allows the temperature of the fluid to increase by modulation of the current in resistance $R$ using the order $u_e$. An agitator is used to homogenize the temperature of the fluid in the tank. This system is shown in Fig. 4.

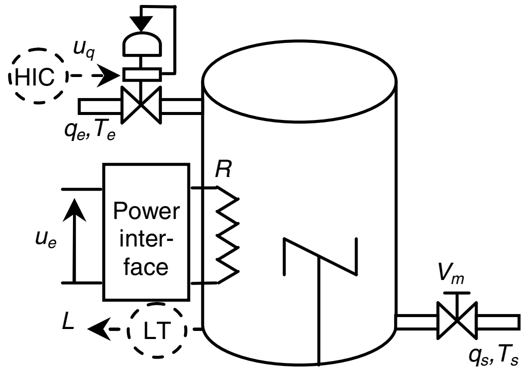

Fig. 4. System description.

The characteristics of the installation are as follows:

- the tank has a section $S$ of 0.5 m$^2$,
- the resistance $R$ is 2.42 Ω,
- the level sensor used delivers 1 V/m,
- the temperature gauge used delivers 10 mV/ °C,
- the gain of the electro-valve $K_e$ is 2 l/mn/V,
- the manual valve $V_m$ is partially open, $q_s = 0.2L$,
- the sampling period $T_{\text{ech}}$ is 5 s,
- $L$ denotes the level and $T$ denotes the temperature.

The nominal system $S_{\text{nom}} : (A_n, B_n, C_n)$ is fully described by the following matrices:

$$A_n = \begin{bmatrix} 0.9967 & 0 \\ 0 & 0.1353 \end{bmatrix},$$
$$B_n = \begin{bmatrix} 0.0511 & -0.0256 \\ 0 & 0.0169 \end{bmatrix},$$
$$C_n = \begin{bmatrix} 0.0078 & 0 \\ 0 & 0.0085 \end{bmatrix}.$$

The control and output vectors are $u = \begin{bmatrix} u_e & u_q \end{bmatrix}^T$ and $y = \begin{bmatrix} T_s & L \end{bmatrix}^T$.

The calculation of the two controls $u_e$ and $u_q$ is performed by the MPC controller. The parameters of the function cost include

- the prediction horizon: $h_p = 2$,
- the output constraints: $\{0 \le T_s(k) \le 100\}$ [°C] and $\{0 \le L(k) \le 10\}$[m],
- the control constraints: $\{0 \le u_e(k) \le 10\}$[V], $\{0 \le u_q(k) \le 10\}$ [V] and $|\Delta u(k)| \le 0.5$ [V],
- the relaxation matrices:

$$Q = 10^{-3} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad R = 10^{-1} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

- the nominal objectives (required performances):

$$o_T^{\text{nom}} = 20\,[^\circ\text{C}] \text{ and } o_L^{\text{nom}} = 8\text{ [m]}.$$

In order to define the different performance regions, the following performance index thresholds are considered:

$$\varepsilon_\pi^{\text{nom}} = 5\%, \qquad \varepsilon_\pi^{\text{deg}} = 20\%,$$

$$O_{\text{nom}} \triangleq \Big\{ o^{\text{nom}} = \begin{bmatrix} o_T^{\text{nom}} & o_L^{\text{nom}} \end{bmatrix}^T : 19 \le \|o_T^{\text{nom}}\|_2 \le 21, 7.6 \le \|o_L^{\text{nom}}\|_2 \le 8.4 \Big\},$$

$$O_{\text{deg}} \triangleq \Big\{ o^{\text{deg}} = \begin{bmatrix} o_T^{\text{deg}} & o_L^{\text{deg}} \end{bmatrix}^T : 16 \le \|o_T^{\text{deg}}\|_2 < 19, 21 < \|o_T^{\text{deg}}\|_2 \le 24, 6.4 \le \|o_L^{\text{deg}}\|_2 < 7.6, 8.4 < \|o_L^{\text{deg}}\|_2 \le 9.6 \Big\},$$

$$O_{\text{un}} \triangleq \Big\{ o^{\text{un}} = \begin{bmatrix} o_T^{\text{un}} & o_L^{\text{un}} \end{bmatrix}^T : \|o_T^{\text{un}}\|_2 < 16, 24 < \|o_T^{\text{un}}\|_2, \|o_L^{\text{un}}\|_2 < 6.4, 9.6 < \|o_L^{\text{un}}\|_2 \Big\}.$$

The following figures show the results of simulations performed in MATLAB. Figure 5 presents the response of the nominal plant (fault-free system). It shows the two outputs, the tank temperature [°C] and level [m], and their corresponding control signals, i.e., the electric valve and resistance control signals [V]. Notice that the nominal reference trajectories and the control limits are represented here with dashed lines.

In the experiment, a fault on the controlled valve actuator occurs at time 50. It is assumed that the reconfiguring action starts three seconds after the fault occurrence. To study the impact of the fault on the system performance, three cases are considered as follows.

*Case 1:* $\hat{\gamma}_1^k = 0$ for all $k$ and

$$\hat{\gamma}_2^k = \begin{cases} 0, & k < 50, \\ 0.16, & k \ge 50. \end{cases}$$

The admissible control set is

$$U_{\text{adm}} = \Big\{ u_{\text{adm}} = \begin{bmatrix} u_e^{\text{adm}} & u_q^{\text{adm}} \end{bmatrix}^T : 0 \le u_e^{\text{adm}} \le 10, 0 \le u_q^{\text{adm}} \le 8, 4 \Big\}.$$

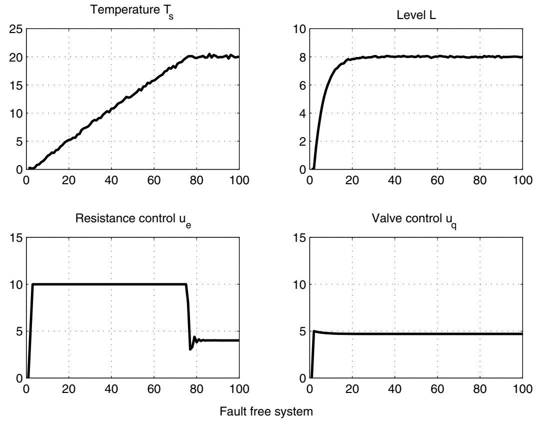

Fig. 5. Nominal plant outputs and controls.

The degraded objective is

$$o_T^{\deg *} = \arg \min_{\substack{u_{\mathrm{adm}} \in U_{\mathrm{adm}} \\ o_T^{\deg} \in O_{\deg}}} \left( \| o_T^{\deg} - 20 \|_2 \right) = 20,$$

$$o_L^{\deg *} = \arg \min_{\substack{u_{\mathrm{adm}} \in U_{\mathrm{adm}} \\ o_L^{\deg} \in O_{\deg}}} \left( \| o_L^{\deg} - 8 \|_2 \right) = 8.$$

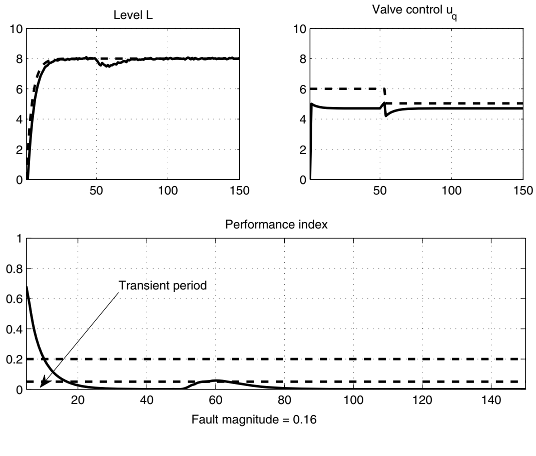

Fig. 6. Low severity fault effect.

The effects of the fault on system performance are shown in Fig. 6. After fault occurrence, the valve control remains within the admissible limits and the performance index slightly deviates and returns to its nominal value. The large magnitude of the performance index between time 0 and time 20 corresponds to a transient response of the system.

*Case 2:* $\hat{\gamma}_1^k = 0$ for all $k$ and

$$\hat{\gamma}_2^k = \begin{cases} 0, & k < 50, \\ 0.27, & k \geq 50. \end{cases}$$

The admissible control set is

$$U_{\mathrm{adm}} = \Big\{ u_{\mathrm{adm}} = \begin{bmatrix} u_e^{\mathrm{adm}} & u_q^{\mathrm{adm}} \end{bmatrix}^T : \\ 0 \leq u_e^{\mathrm{adm}} \leq 10, 0 \leq u_q^{\mathrm{adm}} \leq 7.3 \Big\}.$$

The degraded objective is

$$o_L^{\deg *} = \arg \min_{\substack{u_{\mathrm{adm}} \in U_{\mathrm{adm}} \\ o_L^{\deg} \in O_{\deg}}} \left( \| o_L^{\deg} - 8 \|_2 \right) = 7.3.$$

In this case, the fault is more severe than in Case 1. It can be noticed that the performance index (shown in Fig. 7) does not return to the nominal value. Then, the nominal objective cannot be achieved. Nevertheless, the new degraded reference applied to the system allows the valve control to remain within the admissible limits and the level value follows the new set-point.

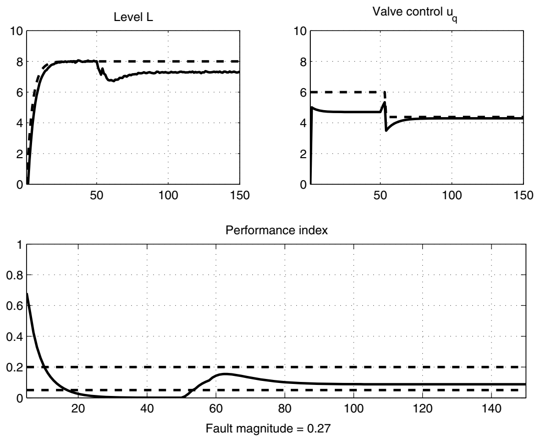

Fig. 7. Medium severity fault effect.

*Case 3:* $\hat{\gamma}_1^k = 0$ for all $k$ and

$$\hat{\gamma}_2^k = \begin{cases} 0, & k < 50, \\ 0.43, & k \geq 50. \end{cases}$$

The admissible control set is

$$U_{\mathrm{adm}} = \Big\{ u_{\mathrm{adm}} = \begin{bmatrix} u_e^{\mathrm{adm}} & u_q^{\mathrm{adm}} \end{bmatrix}^T : \\ 0 \leq u_e^{\mathrm{adm}} \leq 10, 0 \leq u_q^{\mathrm{adm}} \leq 5.7 \big\}.$$

The degraded objective is

$$o_L^{\deg *} = \arg \min_{\substack{u_{\mathrm{adm}} \in U_{\mathrm{adm}} \\ o_L^{\deg} \in O_{\deg}}} \left( \| o_L^{\deg} - 8 \|_2 \right) = 5.7.$$

The deterioration of the performance is critical since the performance index, shown in Fig. 8, is outside the degraded performance region. It is clear that the controls still operate on the admissible interval values.

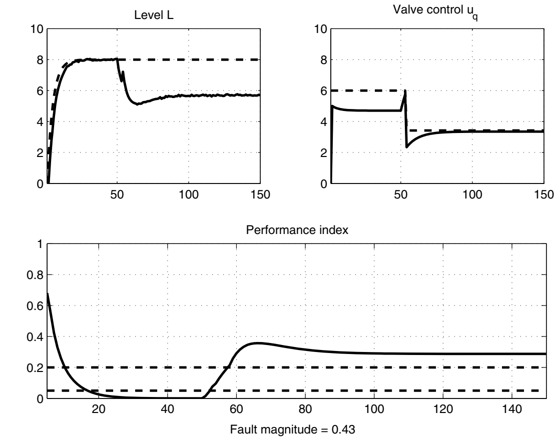

Fig. 8. High severity fault effect.

The evolution of the performance index with respect to the actuator fault magnitude, shown in Fig. 9, is valuable information which helps the operator in decision making. For this specific case, the degraded performance region corresponds to the fault magnitude comprised between 0.24 and 0.36.

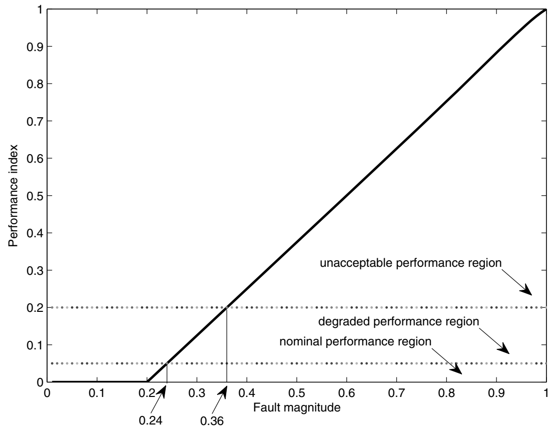

Fig. 9. Evolution of the performance index.

## 6. Conclusion

This paper presented an active fault tolerant control system design strategy. The strategy is based on the computation of a degraded reference trajectory with respect to an admissible control set. The new reference trajectory is determined on the basis of an optimization algorithm which ensures the lower possible performance degradation. The impact of the faults on the system performances is evaluated by a specific index. This index provides useful information to the operator for the supervision of the process.

## References

Aubrun, C., De Cuypere, P. and Sauter, D. (2003). Design of a supervised control system for sludge dewatering process, *Control Engineering Practice* **11**(1): 27–37.

Bemporad, A. and Morari, M. (1999). Robust model predictive control: A survey, *in* A. Garulli, A. Tesi and A. Vicino (Eds.), *Robustness in Identification and Control*, Lecture Notes in Control and Information Sciences, Vol. 245, Springer, London, pp. 207–227.

Blanke, M., Kinnaert, M., Lunze, J. and Staroswiecki, M. (2006). *Diagnosis and Fault-Tolerant Control*, 2nd Edn., Control Systems Series, Springer-Verlag, Heidelberg.

Boussaid, B., Aubrun, C., Ben Gayed, K. and Abdelkrim, M. (2009). FTC approach based on predictive governor, *Proceedings of the 7th IEEE International Conference on Control and Automation, ICCA 2009, Chrischurch, New Zealand*, pp. 2088–2093.

Boussaid, B., Hamdaoui, R., Aubrun, C., Bengayed, K. and Abdelkrim, N. (2008). A fault tolerant predictive control applied to hydro-thermal system, *Proceedings of CIFA 2008, Bucarest, Romania*, pp. 1–6.

Cannon, M. and Kouvaritakis, B. (2005). Optimizing prediction dynamics for robust MPC, *IEEE Transactions on Automatic Control* **50**(11): 1892–1897.

Ding, B., Xi, Y. and Li, S. (2004). A synthesis approach of on-line constrained robust model predictive control, *Automatica* **40**(1): 163–167.

Guerra, P., Puig, V. and Witczak, M. (2006). Robust fault detection with unknown input set-membership state estimators and interval models using zonotopes, *Proceedings of the 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2006, Beijing, China*, pp. 1303–1308.

Jiang, J. and Zhang, Y. (2002). Graceful performance degradation in active fault tolerant control systems, *Proceedings of the 15th IFAC World Congress b'02, Barcelona, Spain*.

Jiang, J. and Zhang, Y. (2006). Accepting performance degradation in fault-tolerant control system design, *IEEE Transactions on Control Systems Technology* **14**(2): 284–292.

Korbicz, J., Kościelny, J., Kowalczuk, Z. and Choleva, W. (2004). *Fault Diagnosis: Models, Artificial Intelligence, Applications*, Springer-Verlag, Berlin/Heidelberg/New York, NY, p. 920.

Lunze, J. and Richter, J. (2008). Reconfigurable fault-tolerant control: A tutorial introduction, *European Journal of Control* **14**(5): 359–386.

Maciejowski, J. (2002). *Predictive Control with Constraints*, Prentice Hall, Harlow.

Marusak, P.M. and Tatjewski, P. (2008). Actuator fault tolerance in control systems with predictive constrained setpoint optimizers, *International Journal of Applied Mathematics and Computer Science* **18**(4): 539–551, DOI: 10.2478/v10006-008-0047-2.

Noura, H., Theilliol, D., Ponsart, J. and Chamssedine, A. (2009). *Fault-tolerant Control Systems: Design and Practical Applications*, Advances in Industrial Control, Springer-Verlag, London.

Patton, R. (1997). Fault-tolerant control systems: The 1997 situation, *Proceedings of the IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, Kingston Upon Hull, UK*, pp. 1033–1054.

Puig, V. (2010). Fault diagnosis and fault tolerant control using set-membership approaches: Application to real case studies, *International Journal of Applied Mathematics and Computer Science* **20**(4): 619–635, DOI: 10.2478/v10006-010-0046-y.

Tatjewski, P. (2010). Supervisory predictive control and online set-point optimization, *International Journal of Applied Mathematics and Computer Science* **20**(3): 483–495, DOI: 10.2478/v10006-010-0035-1.

Theilliol, D., Join, C. and Zhang, Y. (2008). Actuator fault tolerant control design based on a reconfigurable reference input, *International Journal of Applied Mathematics and Computer Science* **18**(4): 553–560, DOI: 10.2478/v10006-008-0048-1.

Theilliol, D., Zhang, Y. and Ponsart, J. (2009). Fault tolerant control system against actuator failures based on reconfiguring reference input, *Proceedings of the International Conference on Advances in Computational Tools for Engineering Applications, Beyrout, Libanon,* pp. 1–6.

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. (2003). Bibliographical review on reconfigurable fault-tolerant control systems, *Proceedings of the 5th IFAC Symposium on Fault Detection, Supervision and safety for Technical Processes, SAFEPROCESS 2003, Washington, DC, USA*, pp. 265–276.

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

Zhang, Y., Jiang, J. and Thelliol, D. (2008). Incorporating performance degradation in fault tolerant control system design with multiple actuator failures, *International Journal of Control, Automation, and Systems* **6**(3): 327–338.

**Boumedyen Boussaid** was born in 1972 in Matmata, Tunisia. He received a Ph.D. in control engineering in 2011 from the University of Nancy and the National School of Engineers of Gabès, and an engineering degree in 1997 in electrical engineering from the National School of Engineers of Tunis. Since 1999 he has been an assistant professor in the Department of Electrical Engineering at High Institute of Technology, University of Gabès. He is currently a member of the Research Centre in Automation of Nancy (CRAN) and the research unit on Modeling, Analysis and Control of Systems (MACS). His research interests focus on constrained control and fault tolerant control areas with application to wind turbines.

**Christophe Aubrun** received a Ph.D. in control engineering from the University of Nancy, France, in 1992. He is currently a member of the Research Centre in Automation of Nancy (CRAN). Since 2005 he has been a professor in the Department of Electrical Engineering, Institute of Technology, University of Nancy. He has been involved in many projects with industry as well as European projects. His research interests lie in complex systems diagnosis and fault tolerant control areas with particular applications to water treatment processes and networked control systems.

**Mohamed Naceur Abdelkrim** was born in 1958 in Metouia, Tunisia. He received the diploma of technical sciences in electrical construction in 1980 and the diploma of deep studies in 1981 from the High Normal School of Technical Education of Tunis. He also received a Ph.D. in automatic control in 2003 from the National School of Engineers of Tunis. He began teaching in 1981 at the National School of Engineers of Tunis and since 2003 he has been a professor of automatic control at the National School of Engineers of Gabès. He is currently the head of the research unit on Modeling, Analysis and Control of Systems (MACS).

**Mohamed Koni Ben Gayed** received a Ph.D. in automatic and industrial data processing from the University of Lille, France, in 1987. He is currently a member of the research team on Modeling, Analysis and Control of Systems (MACS). His field of research is automation, including control, supervision, safety as well as man/machine interaction. He also teaches with the ISET of Gabès, Tunisia.

Received: 6 March 2010
Revised: 2 November 2010
Re-revised: 7 February 2011