International Journal of Systems Science
Vol. 42, No. 1, January 2011, 219–233

Taylor & Francis
Taylor & Francis Group

Design of a fault tolerant control system incorporating reliability analysis and dynamic behaviour constraints

F. Guenab[a], P. Weber[a], D. Theilliol[a]* and Y.M. Zhang[b]

[a]*Faculté des Sciences et Techniques, BP 239, Centre de Recherche en Automatique de Nancy, Nancy Université, CNRS, 54506 Vandoeuvre Cedex, France;* [b]*Department of Mechanical and Industrial Engineering, Concordia University, Montreal, Quebec, Canada, H3G 1M8*

(*Received 10 October 2008; final version received 15 October 2009*)

In highly automated aerospace and industrial systems where maintenance and repair cannot be carried out immediately, it is crucial to design control systems capable of ensuring desired performance when taking into account the occurrence of faults/failures on a plant/process; such a control technique is referred to as fault tolerant control (FTC). The control system processing such fault tolerance capability is referred to as a fault tolerant control system (FTCS). The objective of FTC is to maintain system stability and current performance of the system close to the desired performance in the presence of system component and/or instrument faults; in certain circumstances a reduced performance may be acceptable. Various control design methods have been developed in the literature with the target to modify or accommodate baseline controllers which were originally designed for systems operating under fault-free conditions. The main objective of this article is to develop a novel FTCS design method, which incorporates both reliability and dynamic performance of the faulty system in the design of a FTCS. Once a fault has been detected and isolated, the reconfiguration strategy proposed in this article will find possible structures of the faulty system that best preserve pre-specified performances based on on-line calculated system reliability and associated costs. The new reconfigured controller gains will also be synthesised and finally the optimal structure that has the 'best' control performance with the highest reliability will be chosen for control reconfiguration. The effectiveness of this work is illustrated by a heating system benchmark used in a European project entitled intelligent Fault Tolerant Control in Integrated Systems (IFATIS EU-IST-2001-32122).

Keywords: fault tolerant control systems; system reliability; pseudo-inverse method; hierarchical structure; control reconfiguration

1. Introduction

In most conventional control systems, controllers are designed for fault-free systems without taking into account the possibility of fault occurrence. In order to overcome these limitations, modern complex systems use sophisticated controllers which are developed with fault accommodation and fault tolerance capabilities to meet reliability and performance requirements. A fault tolerant control system (FTCS) is a control system that can maintain system performance close to the desirable one and preserves stability conditions not only when the system is in a fault-free case but also in the presence of faulty components in the system, or at least can ensure expected degraded performances that can be accepted as a trade-off (Zhang, Jiang, and Theilliol 2008). Fault tolerant control (FTC) has been motivated by different goals for different applications (Noura, Theilliol, and Sauter 2000; Theilliol, Noura, and Ponsart 2002; Zhang and Jiang 2008). The main goal of FTCS design is to improve reliability and safety of industrial processes and safety-critical systems. Various approaches for FTCS design have been suggested in the literature. Overviews on the development of FTCS have been provided in survey articles by Patton (1997) and Zhang and Jiang (2008), as well as books by Hajiyev and Caliskan (2003), Mahmoud, Jiang, and Zhang (2003), Blanke *et al.* (2006) and Ducard (2009).

Developed methods can be generally categorised into two groups (Patton 1997; Zhang and Jiang 2008): passive and active approaches. Passive FTC deals with a presumed set of process component failures considered in the controller design stage. Active FTC is characterised by an on-line fault diagnosis process and control reconfiguration mechanism. Fault detection and diagnosis (FDD) refers to the task of inferring the occurrence of faults in a system/process and to find their root causes using various knowledge-based and data-based strategies as outlined by quantitative models (Venkatasubramanian, Rengaswamy, Yin,

*Corresponding author. Email: didier.theilliol@cran.uhp-nancy.fr

ISSN 0020–7721 print/ISSN 1464–5319 online

DOI: 10.1080/00207720903513319
http://www.informaworld.com

and Kavuri 2003a), qualitative models (Venkatasubramanian, Rengaswamy, and Kavuri 2003b) and historical data (Venkatasubramanian, Rengaswamy, Kavuri, and Yin 2003c). Several books have been published, for example Gertler (1998) Chen and Patton (1999), Chiang, Russell, and Braatz (2001), Simani, Fantuzzi, and Patton (2003), Isermann (2006), Witczak (2007), and Ding (2008). Based on the information provided by the fault diagnosis module, a control reconfiguration mechanism is designed in order to reduce and compensate for the effects of fault-induced changes in the system. Advanced and sophisticated controllers have been developed along the lines of active FTC, as outlined in Zhang and Jiang (2008). Issues on integration of FDD and FTC have also been discussed in Jiang and Zhang (2006). Among those developments, some publications have introduced reliability analysis for FTCS. Wu (2001a, 2001b) and Wu and Patton (2003) have used Markov models to dictate the system reliability where subsystems are supposed to reach two states: intact (available) or failed (unavailable). Staroswiecki, Hoblos, and Aitouche (2004) proposed a sensor reconfiguration strategy based on physical redundancy where the reliability analysis provides some information for selecting the optimal redundant sensors. In a similar way, He, Wang, and Zhou (2009) have considered the reliability of sensor faults in the filtering design issue. Recently, Guenab, Theilliol, Weber, Ponsart, and Sauter (2005) proposed a FTC strategy for complex systems composed of various subsystems. The FTC method provides an optimal structure in order to achieve desired objectives with highest reliability under a cost constraint or with lowest cost for achieving the reliability goal.

In this article, the dynamic behaviour of the faulty and reconfigured closed-loop system is taken into account in the design of a FTCS. In this context, complex systems are considered as a set of interconnected subsystems. Each subsystem is assigned some local objectives with respect to quality, reliability and dynamic performance. Each subsystem may take several states, and specific controller gains. In the fault-free case, the structure of the control system is defined based on the set of subsystems connected. Once a fault occurs, the faulty subsystems are assumed being able to achieve local objectives at degraded levels. New structures of the system can then be determined based on the degraded objectives. Each possible structure of the system corresponds to reliability and global performance computed from its subsystem properties. The optimal structure is chosen based on the structure that achieves the required global objectives (static and dynamic) with highest reliability. Once the optimal solution is determined, a new structure and a new control law can be exploited in order to achieve the global objectives as close as possible to the nominal one. From the redesign of a controller for each subsystem, the revisited pseudo-inverse method (PIM) developed by Staroswiecki (2005) is used.

The article is organised as follows. Section 2 is dedicated to defining a set of complex systems. Section 3 is devoted to the design of the FTCS under a hierarchical structure. After some definitions are introduced, a solution is developed under a general formulation. A simulation example is considered in Section 4 to illustrate the performance and effectiveness of the proposed method. Finally, concluding remarks are given in the last section.

2. Problem statement

A large class of systems is described by hierarchical structures (Singh and Titli 1978), also called systems with multiple levels, and there are good reasons for organising the control of systems in this way, such as a reduction in the complexity of communication and computation. The considered approach relies on a hierarchical structure with two levels: a global and a local level. Most of the distributed and interconnected systems, such as manufacturing, automated transportation, chemical processes and the automotive industry can be represented under a hierarchical structure with two main levels.

Under the hierarchical control structure assumption, the global level, called coordinator, is designed as an optimal controller. It defines the nominal global objective γ_g^{nom} with the associated local references r_i and computes the global objective γ_g based on the local output y_i of each subsystem s_i. From instance, in a distillation column, the global objective could be the concentration of alcohol in a liquid and the local objectives correspond to the temperature on each stage.

At the local level, the structure is assumed to be composed of n multi-input multi-output subsystems s_i, $i = 1, \ldots, n$, described by a set of linear state-space representations:

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) \\ y_i(t) = C_i x_i(t) \end{cases}, \tag{1}$$

where u_i is the control input vector and y_i is the output vector. A_i, B_i and C_i are constant matrices with appropriate dimensions.

Each subsystem s_i has a controller designed for a normal operation with following feedback-feedforward control structure for command tracking:

$$u_i(t) = -K_i^{\text{feedback}} x_i(t) + K_i^{\text{feedforward}} r_i(t), \tag{2}$$

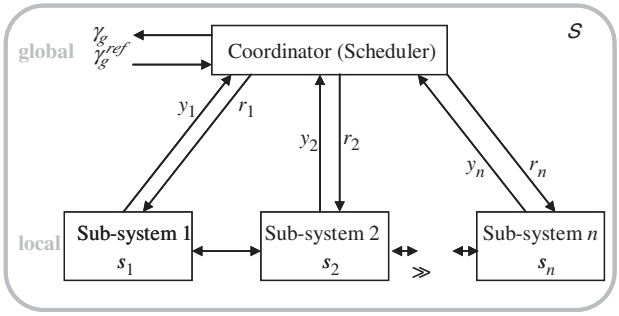

Figure 1. General scheme of hierarchical structure.

where the matrices K_i^{feedback} and $K_i^{\text{feedforward}}$ are synthesised such that the closed-loop behaviour follows the reference model described as follows:

$$\dot{x}_i(t) = M_i x_i(t) + N_i r_i(t), \tag{3}$$

where M_i and N_i matrices are designed in order to describe a desired reference model, which specifies the desired dynamic characteristics of the subsystem under the normal condition.

For a more convenient point of view, subsystems are assumed to be decoupled, which means that matrix A_i is block diagonal. Moreover, subsystem s_i is coupled to subsystem s_{i+1} or inversely.

Figure 1 presents an illustrative scheme of a hierarchical structure.

Due to abnormal operation or material ageing, actuator or component faults can occur in the system. Therefore, the linear state-space model representation defined in (1) may become

$$\begin{cases} \dot{x}_i(t) = A_i^f x_i(t) + B_i^f u_i(t) \\ y_i(t) = C_i x_i(t) \end{cases}, \tag{4}$$

where A_i^f (respectively B_i^f) represents the state (input) matrix in the presence of faults f on the plant/process such as components (actuators).

The occurrence of such faults may result in an unsatisfactory performance and may lead the system to become unstable. Consequently, it is important to design control systems for being able to maintain system performance and reliability. This article aims to design a FTCS in order to maintain nominal or achieve admissible performances despite a fault. A fault detection and isolation (FDI) module is assumed to generate suitable information for control reconfiguration. Before tackling this problem, let us recall the control problem in a general way as suggested by Staroswiecki and Gehin (2001) based on the triplet $\langle \gamma_g, C, U \rangle$, where γ_g are global objectives, C is a set of constraints given by the structure S and parameters Θ of a closed-loop system and U is a set of control laws.

In the fault-free case, the control problem could be solved by a control law $u \in U$ such that the controlled system can achieve the global objectives γ_g under a constraint C. A structure S and parameters Θ are defined and the controller gains of all subsystems and their associated references to achieve the global objectives γ_g are designed. Consequently, the reference global objectives γ_g^{ref} are achieved under the nominal control law u_{nom} with the nominal structure S_{nom}. In a faulty case, the structure S_{nom} is assumed to be modified. Under the presence of faults, the global objectives can be or cannot be achieved under a new structure. In this context, the FTC problem should be able to find a solution to the triplet $\langle \gamma_g, C, U \rangle$. According to a reconfigurability analysis on the distributed and interconnected systems established *a priori* as proposed in Blanke et al. (2006) and associated articles such as Staroswiecki and Gehin (1998), M structures S_m, $m = 1, \ldots, M$, could be considered as reconfigurable ones. A reconfigurable structure consists of changing the structure S_{nom}, parameters Θ and/or control law $u \in U$ of the post-fault system to achieve the global objectives γ_g^{ref}. Among M structures S_m, a solution can be provided by the disconnection or replacement of faulty subsystems. in some cases, no solution may exist, and then global objectives must be redefined to degraded ones, noted as γ_g^d. Then the problem statement is formulated by the following question: how does one choose an optimal structure in the sense that for a given criterion J the selected structure can maintain the objectives γ_g^{ref} (or degraded ones γ_g^d)? This article aims to provide a solution to the above problem based on reliability analysis under dynamic behaviour constraints in the hierarchical structure framework.

3. FTCS design

3.1. *Reliability computation*

Reliability is the ability that units, components, equipment, products and systems will perform their required functions for a specified period of time without failure under stated conditions and specified environments (Gertsbakh 2000). Reliability analysis of components consists of analysing time to a failure from data obtained under normal operating conditions (Cox 1972). In many situations and especially in the considered study, failure rates are obtained from components under different levels of loads: the operating conditions of components change from one structure to another. Several mathematical models have been developed to define the failure level in order to estimate the failure rate λ (Finkelstein 1999; Martorell, Sanchez, and Serradell 1999). The proportional hazards model

introduced by Cox (1972) is used in this article. The failure rate is modelled as follows:

$$\lambda_i(t, \ell) = \lambda_i(t)\, g(\ell, \vartheta), \tag{5}$$

where $\lambda_i(t)$ represents the baseline failure rate (nominal failure rate) function of time for the i-th subsystem/component and $g(\ell, \vartheta)$ is a function (independent of time) taking into account the effects of applied loads with ℓ presenting an image of the load and ϑ defining some parameters of the subsystem/component.

Different definitions of $g(\ell, \vartheta)$ exist in the literature. However, the exponential form is commonly used. Moreover, the failure rate function for the exponential distribution is constant during the useful life but it can change from one operating mode to another according to a load level for the structure S_{nom}. Under these conditions, the failure rate (5) can be rewritten as

$$\lambda_i^m(t, \ell) = \lambda_i(t) e^{\vartheta \times \ell_m}. \tag{6}$$

It can be noticed that load levels (or mean load levels) ℓ_m are assumed constants for the i-th subsystem/component. If an event occurs on the system, based on a novel (or not) load value applied to the component, a new failure rate is calculated. Then the reliability for a period of desired lifetime, noted as T_d, is commonly calculated as follows:

$$R_i^m(T_d) = e^{-\lambda_i^m(T_d, \ell_m) \times T_d}, \tag{7}$$

where $R_i^m(T_d)$ represents the reliability of i-th subsystem used by the structure S_m for the specified time T_d. It should be pointed out that T_d represents the time period between the fault occurrence and the reparation of the faulty component which caused the structure modification.

From complex systems, a global reliability $R_g^m(T_d)$ is computed based on the reliabilities of elementary components or subsystems. Indeed, the global reliability $R_g^m(T_d)$ usually depends on the subsystem's connection which can generally be decomposed on elementary combinations of serial and parallel components. Therefore, the computation of the global reliability $R_g^m(T_d)$ is both based on the reliability of

– n serial subsystems as defined by

$$R_g^m(T_d) = \prod_{i=1}^{n} R_i^m(T_d). \tag{8}$$

– n parallel subsystems as represented by:

$$R_g^m(T_d) = 1 - \prod_{i=1}^{n} (1 - R_i^m(T_d)), \tag{9}$$

where $R_i^m(T_d)$ represents the i-th subsystem reliability.

3.2. *Cost computation*

Let us assume that the system uses all n subsystems. The subsystems' reliabilities are computed at a given time T_d and for each subsystem a cost is associated with it. The objective is to obtain the expected cost of each subsystem as a function of its reliability. Several forms of cost are possible, for example Mettas (2000) and Wu, Wang, Smapath, and Kott (2002). An expected cost function, proposed by Mettas (2000) is used in this article as follows:

$$C_i^m(R_i^m(T_d)) = \frac{\varsigma_i + P}{\int_0^\infty R_i^m(t)\mathrm{dt}}, \tag{10}$$

where ς_i is the initial acquisition cost (price) of i-th subsystem, P is the failure cost due to the performance degradation and $\int_0^\infty R_i^m(t)\mathrm{dt}$ is the mean time to failure of i-th subsystem.

In our case, we propose the formula of the cost over the operating time T_d. At $t = T_d$ there is a probability $(1 - R_i^m(T_d))$ of the component having failed with the associated costs represented by $(\varsigma_i + P)$. This cost is not constant over the operating time T_d. During an interval $[0 \quad T_d]$, the cost is given by

$$C_i^m(R_i^m(T_d)) = \frac{(\varsigma_i + P)(1 - R_i^m(T_d))}{\int_0^{T_d} R_i^m(t)\mathrm{dt}}. \tag{11}$$

The originality of the cost C_i^m is that it is computed according to a desired operating time T_d. Once costs of all subsystems are computed, the cost of the composite system is given by

$$C_g^m = \sum_i C_i^m(R_i^m(T_d)). \tag{12}$$

3.3. *Reconfigurable controller gain synthesis based on an admissible model matching method*

Under the assumption that each multi-input multi-output subsystem s_i $(\forall\, i = 1, \ldots, n)$ defined by Equation (1) or Equation (4) are controllable, the control laws $u_i(t) = -K_i^{\text{feedback}} x_i(t) + K_i^{\text{feedforward}} r_i(t)$ are synthesised such that the closed-loop behaviours are close to a specified reference model $\dot{x}_i(t) = M_i x_i(t) + N_i r_i(t)$, respectively. The controller gains $(K_i^{\text{feedback}}, K_i^{\text{feedforward}})$ are commonly synthesised by solving the following equations:

$$\begin{aligned} A_i - B_i K_i^{\text{feedback}} &= M_i, \\ B_i K_i^{\text{feedforward}} &= N_i, \end{aligned} \tag{13}$$

with a unique solution defined as follows:

$$\begin{aligned} K_i^{\text{feedback}} &= B_i^+ (A_i - M_i), \\ K_i^{\text{feedforward}} &= B_i^+ N_i, \end{aligned} \tag{14}$$

where B_i^+ is the left pseudo-inverse of B_i.

If (13) is not fulfilled, optimal solutions, as presented by Huang and Stengel (1990), should be computed through the following criteria:

$$J_{i1} = \left\| A_i - B_i K_i^{\text{feedback}} - M_i \right\|_F^2, \tag{15}$$

and

$$J_{i2} = \left\| B_i K_i^{\text{feedforward}} - N_i \right\|_F^2, \tag{16}$$

where $\|\cdot\|_F$ represents the Frobenius norm.

Using constrained optimisation, Gao and Antsaklis (1991) synthesised suitable gains based on the PIM which guarantees the closed-loop system stability with successful results in faulty cases for achievable performances where, instead of considering one single reference (closed-loop) behaviour M (respectively N for tracking), a family of reference models $\mathfrak{M}$ (respectively $\mathfrak{N}$ for tracking) that are acceptable are provided. In this article, in order to redesign the controller dedicated to each i-th faulty subsystem, the idea of the recently revisited PIM, developed by Staroswiecki (2005), has been adopted. Under the assumptions that the FDI scheme provides necessary information, the revisited PIM can provide an appropriate controller $(\tilde{K}_i^{\text{feedback}}, \tilde{K}_i^{\text{feedforward}})$ with a degree of freedom for solving Equation (13). As presented in Section 2, the control problem is defined by the triplet $\langle \gamma_g, C, U \rangle$. In faulty cases and for each subsystem, the triplet is equivalent to

$$\begin{aligned} &\gamma_i\colon \dot{x}_i(t) = M_i x_i(t) + N_i r_i(t), (M_i, N_i) \in \mathfrak{M}_{\text{i}} \times \mathfrak{N}_{\text{i}} \\ &C_i\colon \dot{x}_i(t) = A_i^f x_i(t) + B_i^f u_i(t) \\ &U_i\colon u_i(t) = -\tilde{K}_i^{\text{feedback}} x_i(t) + \tilde{K}_i^{\text{feedforward}} r_i(t) \end{aligned}, \tag{17}$$

where (M_i, N_i) are among the sets of admissible reference models $\mathfrak{M}_{\text{i}} \times \mathfrak{N}_{\text{i}}$.

In faulty cases, $\mathfrak{N}_{\text{i}}$ is defined by

$$\mathfrak{M}_i = \left\{ M_i \middle| \phi_{1i}(M_i) \le 0 \quad \text{and} \quad \phi_{2i}(M_i) > 0 \right\}, \tag{18}$$

where functions ϕ_{1i} and ϕ_{2i} describe any matrix M_i which has suitable dynamic behaviour, i.e. stability and appropriate time response. The functions $\phi_{2i}(M_i) > 0$ can be rewritten as $-\phi_{2i}(M_i) < 0$ and (18) is equivalent to a unique function $\phi_i(M_i) < 0$:

$$\mathfrak{M}_{\text{i}} = \left\{ M_i \middle| \quad \phi_i(M_i) \le 0 \right\}. \tag{19}$$

In this article, for simplicity and without loss of generality, the set $\mathfrak{M}_{\text{i}}$ is defined such that any matrix in $\mathfrak{M}_{\text{i}}$ has its eigenvalues lying within a suitable interval. According to the knowledge of the system, this bounded interval is designed in the fault-free condition.

From illustration, an elementary reference model $\dot{x}(t) = Mx(t)$ with its associated eigenvalues being equal to $\tau_1^* = -1$, $\tau_2^* = -1.2$ and $\tau_3^* = -1.4$ is considered. Let the set $\mathfrak{M}$ of admissible reference models be defined by (19) with $\phi(M) \le 0$ corresponding to $\pm 10\%$ of nominal eigenvalues. It can be verified that any matrix belonging to

$$\mathfrak{M} = \left\{ M = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \middle| \begin{cases} -a-e-i-3.96 \le 0 \\ a+e+i+3.24 \le 0 \\ -bd+ai-gc+ei+ea \\ \quad -fh-5.1788 \le 0 \\ bd-ai+gc-ei-ea+fh \\ \quad +3.4668 \le 0 \\ -gbf+afh+gce+dbi \\ \quad -aei-dch-2.2361 \le 0 \\ gbf-afh-gce-dbi+aei \\ \quad +dch+1.2247 \le 0 \end{cases} \right\}$$

has its eigenvalues $\tau_1 = \beta\tau_1^*$, $\tau_2 = \beta\tau_2^*$ and $\tau_3 = \beta\tau_3^*$ with $\beta = [0.9, 1.1]$.

Similar to $\mathfrak{M}_{\text{i}}$, $\mathfrak{N}_{\text{i}}$ is defined as $\mathfrak{N}_i = \left\{ N_i \middle| \varphi_i(N_i) \le 0 \right\}$.

According to the previous sets of admissible reference models, the control problem is equivalent to finding $(\tilde{K}_i^{\text{feedback}}, \tilde{K}_i^{\text{feedforward}})$ as follows:

$$\begin{cases} \tilde{K}_i^{\text{feedback}} = \arg \min\limits_{\phi_i(M_i) \le 0} \left\| A_i^f - B_i^f K_i^{\text{feedback}} - M_i \right\|_F^2 \\ \tilde{K}_i^{\text{feedforward}} = \arg \min\limits_{\varphi_i(N_i) \le 0} \left\| B_i^f K_i^{\text{feedforward}} - N_i \right\|_F^2 \end{cases}. \tag{20}$$

Compared to Staroswiecki (2005), it should be noted that the admissible model matching problem is handled with the Frobenius norm applied to guarantee both the static and dynamic behaviours of the closed-loop system.

In order to choose the optimal structure and the optimal controller associated with each subsystem among the hierarchical architecture under the reliability constraint, the next subsection is dedicated to defining pertinent indicators for both steady-state and dynamic performances.

3.4. *Performance criteria*

The FTCS should reduce or try to limit the difference between the dynamic and steady-state behaviour of the nominal system and the reconfigured system. The global objective γ_g is allowed to be determined by some algebraic and differential equations, based on local outputs y_i of each subsystem s_i, denoted by f such that

$$\gamma_g = f(y_1, \ldots, y_i, \ldots, y_n),\ i = 1, \ldots, n. \tag{21}$$

The following normalised indicator is proposed to provide a global steady-state performance evaluation of structure S_m:

$$J^m_{\text{steady}} = \left| \frac{\gamma^{\text{nom}}_g - \gamma^m_g}{\gamma^{\text{nom}}_g} \right|, \tag{22}$$

where γ^{nom}_g represents the global objective of the nominal (fault-free) structure S_{nom} and γ^m_g denotes the global objective of the reconfigured system under structure S_m. It can be noticed that the global objective γ_g is computed on-line based on Equation (22).

About the dynamic performance evaluation, the main goal is to obtain the eigenvalues of the reconfigured system close to the nominal ones. Let us consider the normalised error between a nominal and reconfigured i-th subsystem in terms of eigenvalues, then the maximal error of i-th subsystem can be formulated as:

$$\varepsilon^m_i = \max \left| \frac{\tau^{\text{nom}}_j - \tau^m_j}{\tau^{\text{nom}}_j} \right|, j = 1, \ldots, k_i, \tag{23}$$

where each i-th sub-system has k_i eigenvalues τ_j, $j = 1, \ldots, k_i$ for the nominal structure and τ^m_j for the reconfigured structure S_m, which are computed on-line based on synthesised controller gains using Equation (20).

Based on Equation (23), the dynamic performance associated with the reconfigured structure S_m (composed of n_m subsystems) is quantified by the largest normalised error and is then evaluated as follows:

$$J^m_{\text{dyn}} = \max(\varepsilon^m_i),\ i = 1, \ldots, n_m. \tag{24}$$

3.5. *FTCS design*

Consider a nominal system composed of n subsystems: $s_i,\ i = 1, \ldots, n$. Each subsystem has the following properties: a set of local objectives $\gamma_l(s_i)$ (outputs), a set of eigenvalues τ_i and a failure rate $\lambda_i(t, \ell_n)$, with ℓ_n the nominal level of loads of the subsystems. For the sake of simplicity, let us consider only constant failure rates $\lambda_i(\ell_n)$. Without faults, a nominal structure is designed which uses all n subsystems and its nominal global objectives γ^{nom}_g achieved under the local objectives $\gamma_l(s_i)$ of each subsystem.

In faulty cases, M structures $S_m,\ m = 1, \ldots, M$, are assumed to be suitable where each structure S_m contains n_m subsystems: $\{ s^m_1 \ \ s^m_2 \ \ \cdots \ \ s^m_{n_m} \}$. The main goal of the method is to select a structure among M structures which ensures global objectives γ^m_g close to the nominal case γ^{nom}_g, also without neglected dynamic properties (in terms of reference model, in particular eigenvalues) and for safety reason under some reliability constraints. An optimal structure among the hierarchical architecture will be determined such that it has a minimum performance criterion (27) under the reliability constraints. From a desired time period T_d, the constraint is defined as the reliability larger than a limited value, i.e. $R^m_g(T_d) \geq R^*_g$ and cost $C^m_g \leq C^*_g$, where R^*_g and C^*_g are defined as constant thresholds defined *a priori*.

Then, for each available reconfigured structure S_m, the following procedure needs to be carried out:

At the local level:

(1) For all combined subsystems' references and each subsystem s^m_i new failure rate $\lambda^m_i(\ell_m)$ are computed from their baseline failure rates according to the new applied loads which depend on various local references and a set of local objectives (outputs). $\gamma^m_l(s^m_i)$ are calculated by taking into account the fault magnitude.
(2) New controllers based on the synthesised gains $(\tilde{K}^{\text{feedback}}_i, \tilde{K}^{\text{feedforward}}_i)$ (Equation (20)) are designed and ε^m_i (Equation (23)) are evaluated.
(3) For a given time period T_d, the corresponding reliability $R^m_i(T_d)$ of each subsystem is computed using Equation (7) and the corresponding cost $C^m_i(R^m_i(T_d))$ is calculated using Equation (11).

At the global level:

(1) Each structure S_m involves a new set of global objectives (outputs) γ^m_g as presented in Equation (21).
(2) The reliability $R^m_g(T_d)$ of the system for all structures is computed using Equations (8) and (9).
(3) The cost C^m_g of the system is computed using Equations (11) and (12).

From each reconfigured structure, from Equation (22), a minimum performance of static index $J^m_{\text{steady, opt}}$ is evaluated using

$$J^m_{\text{steady, opt}} = \min_{R^m_g(T_g) \geq R^*_g,\, C^m_g \leq C^*_g} (J^m_{\text{steady}}) \tag{25}$$

and dynamic index J^m_{dyn} is computed using Equation (24).

To determine the optimal solution, the objective of FTCS is to find the structure that has a reliability $R^m_g(T_d) \geq R^*_g$, the cost $C^m_g \leq C^*_g$ and with minimum performance of index J. The criterion J is evaluated using Equations (24) and (25) as follows:

$$\mathsf{J} = \alpha J^m_{\text{steady, opt}} + (1 - \alpha) J^m_{\text{dyn}}, \tag{26}$$

where α is a weighting constant which determines the relative weight placed on the steady-state and dynamic performance.

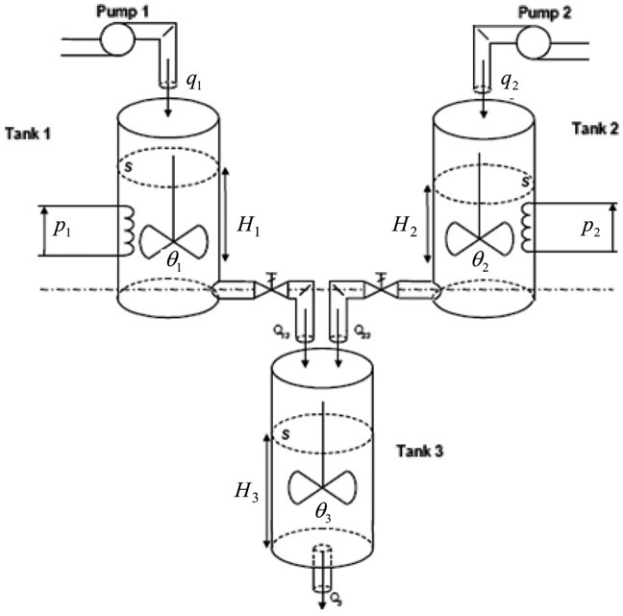

Figure 2. Schematic diagram of the heating system.

Thus the optimal reconfigured structure for a complex system defined as a hierarchical architecture is obtained as follows:

$$S_m^{opt} = \arg \min_{m \; R_g^m(T_g) \geq R_g^*, C_g^m \leq C_g^*} (\mathrm{J}). \tag{27}$$

Once the optimal solution is selected, a new structure S_m^{opt} and a new control law could be exploited in order to satisfy both the local objectives and the corresponding global objectives.

4. Application

The effectiveness and performance of the proposed method are illustrated over a wide range of simulations in the faulty case on a heating system benchmark (Leger, Hamelin, and Sauter 2003). Figure 2 shows the schematic diagram of the entire plant.

4.1. *Process description and control design*

The process is composed of three cylindrical tanks. Two tanks (1 and 2) are used for pre-heating liquids supplied by two pumps. The liquid temperature is adjusted with thermal resistance. A third tank is dedicated for the mixing of the two liquids issued from the pre-heating tanks.

The system instrumentation includes four actuators and six sensors. Control signals p_1, p_2 are powers delivered by the two thermal resistances and q_1, q_2 the input flow rates which are provided by the two pumps. Measurements are liquid temperatures $(\theta_1, \theta_2, \theta_3)$ and

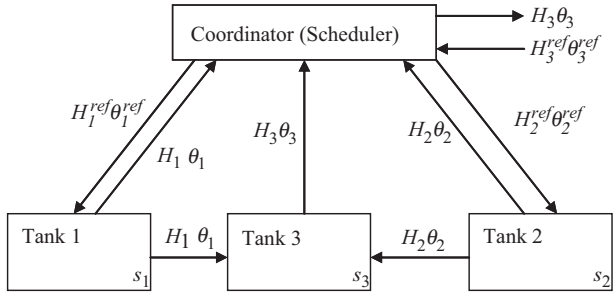

Figure 3. Physical decomposition of the heating system.

liquid levels (H_1, H_2, H_3). A nonlinear system representation is considered to describe the hydraulic and thermal dynamic behaviours in tank 1 and tank 2 such as

$$\begin{cases} \dot{H}_1(t) = & \frac{1}{S}(q_1(t) - \alpha_1\sqrt{H_1(t)}) \\ \theta_1(t) = & \frac{1}{SH_1(t)}\left(\frac{p_1(t)}{\mu c} - (\theta_1(t) - \theta_{1,i})q_1(t)\right) \end{cases}, \tag{28}$$

where S is the tank cross-sectional area, α represents the outflow coefficient, μc corresponds to the thermal constant and finally $\theta_{1,i}$ is the initial condition for the liquid temperature in the tank 1.

According to the instruments available on the heating system in each subsystem s_i, the previous equation can be rewritten as:

$$\begin{aligned} \dot{x}(t) &= f(x(t), u(t)) \\ y(t) &= x(t), \end{aligned} \tag{29}$$

where $x \in \Re^n$ is the state vector, $y \in \Re^m$ is the output vector, $u \in \Re^p$ is the input vector and f a nonlinear function.

According to Equation (29), the system is decomposed into three subsystems such as shown in Figure 3.

The global objectives are to adjust two main reference values: the fluid level H_3^{ref} and the fluid temperature T_3^{ref} in the last tank following static parity equations:

$$H_3 = \left(\frac{\alpha_1\sqrt{H_1} + \alpha_2\sqrt{H_2}}{\alpha_3}\right)^2, \tag{30}$$

$$\theta_3 = \frac{\theta_1\alpha_1\sqrt{H_1} + \theta_2\alpha_2\sqrt{H_2}}{\alpha_3\sqrt{H_3}}. \tag{31}$$

Due to the fact that the process operates in multiple operating regimes, an attractive alternative to nonlinear modelling problem is to use a multi-linear model approach. This approach is successfully used for some nonlinear systems in the control field and consists of partitioning the operating range of a system into separate regions in order to synthesize a global representation. The reader can refer to

Murray-Smith and Johansen (1997) for a comprehensive review on the multiple models strategy, and also for well-developed identification method and modelling problems. A polytopic representation is also used in multi-model representation for nonlinear system modelling and control, as for example in Narendra and Balakrishnan (1997), Tayebi and Zaremba (2002), Ozkan, Kothare, and Georgakis (2003), Wan and, Kothare (2003), Athans, Fekri, and Pascoal (2005) and Toscano and Lyonnet (2006). In this article, the dynamic behaviour of the heating system is assumed to be approximated by a set of N linear time invariant (LTI) models. Consequently, the heating system is formulated as blended multiple models such as

$$\begin{cases} x(t) = \sum_{j=1}^{N} \tilde{G}_j(x(t), u(t))\rho_j(t) \\ y(t) = x(t) \end{cases}, \tag{32}$$

where $\tilde{G}_i$ represents an LTI model established in the vicinity of the j-th equilibrium operating point defined by the set (y_j^e, u_j^e) and ρ denotes a weighting or validity function.

Each LTI model is defined such as

$$\tilde{G}_j(x(t), u(t)) = A_j^o x(t) + B_j^o u(t) + \Delta x_j^o \tag{33}$$

with (A_j^o, B_j^o) being system matrices invariant with appropriate dimensions defined for the j-th operating point, generally established from a first-order Taylor expansion around predefined operating points. Δx_j^o represents a constant vector depending on the j-th linear model and is equal to $\Delta x_j^o = x_j^e - A_j^o x_j^e + B_j^o u_j^e$. It is worthwhile to point out that design of the weighting or validity function ρ is the main task in the multi-model approach. Owing to the main goal of the article, the weighing function ρ is assumed to be assessed directly from output measurements around the j-th operating point as suggested by Toscano and Lyonnet (2006) in a stirred tank reactor.

In the blended multi-model framework, each subsystem s_i has its own associated controller defined for a j-th operating point that implements the following control law:

$$u(t) = -\left(\sum_{j=1}^{N} \tilde{K}_j^{\text{feedback}} \rho_j\right) y(t) + \left(\sum_{j=1}^{N} \tilde{K}_j^{\text{feedforward}} \rho_j\right) r(t), \tag{34}$$

where $\tilde{K}_j^{\text{feedback}}$ and $\tilde{K}_j^{\text{feedforward}}$ are synthesised in order that the closed-loop system follows its reference model.

In the fault-free case, the global objectives are achieved if and if only the reference variables of each subsystem are also reached. This provides a reliability block diagram (RBD) such as shown in Figure 4.

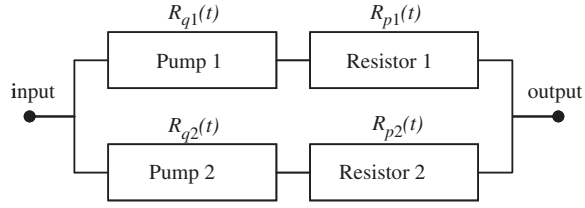

Figure 4. RBD of the heating system.

In the nominal case, the reliability of the entire system is equivalent to $R_g^{\text{nom}}(t) = 1 - (1 - R_{q1}^{\text{nom}}(t) \times R_{p1}^{\text{nom}}(t))(1 - R_{q2}^{\text{nom}}(t) \times R_{p2}^{\text{nom}}(t))$ with a cost function $C_g^{\text{nom}}(t) = C_{q1}^{\text{nom}}(t) + C_{p1}^{\text{nom}}(t) + C_{q2}^{\text{nom}}(t) + C_{p2}^{\text{nom}}(t)$ (see Table A1 for the values of parameters).

4.2. *A set of reconfigured structures*

For illustration purposes, a loss of power in the resistor is considered to occur on the first tank. Three reconfigured structures or working modes are supposed to be involved in the FTCS design.

In the first structure, noted as S_1, only tank 2 and tank 3 are considered in the control loop. The global objectives are achieved without the first tank as

$$H_3 = \left(\frac{\alpha_2\sqrt{H_2}}{\alpha_3}\right)^2, \tag{35}$$

$$\theta_3 = \theta_2. \tag{36}$$

In the second structure, noted as S_2, the heating resistor of the first tank is jammed to its maximal power, i.e. $p_1(t) = (1 - \beta^f) \times p_1^{\max}$. The global objective dedicated to the fluid temperature is affected as follows:

$$\theta_3 = \frac{\theta_1(\beta * p_{\max}^1)\alpha_1\sqrt{H_1} + \theta_2\alpha_2\sqrt{H_2}}{\alpha_3\sqrt{H_3}}. \tag{37}$$

The last one considers, noted as S_3, the nominal structure of the system with an actuator fault. In this working mode, the available local objectives are unlimited.

The reliability and cost functions formula with component failure rates and prices are given in Table A2 for the different structures.

4.3. *Results and analyses*

4.3.1. *Fault-free case*

Different scenarios have been conducted under simulated environments. The validation of the hierarchical controllers under a multiple model framework is shown in Figures 5–7 with respect to fixed global objectives ($H_3^{\text{ref}} = 0.2\,\text{m}$ and $\theta_3^{\text{ref}} = 21^\circ\text{C}$) for a range

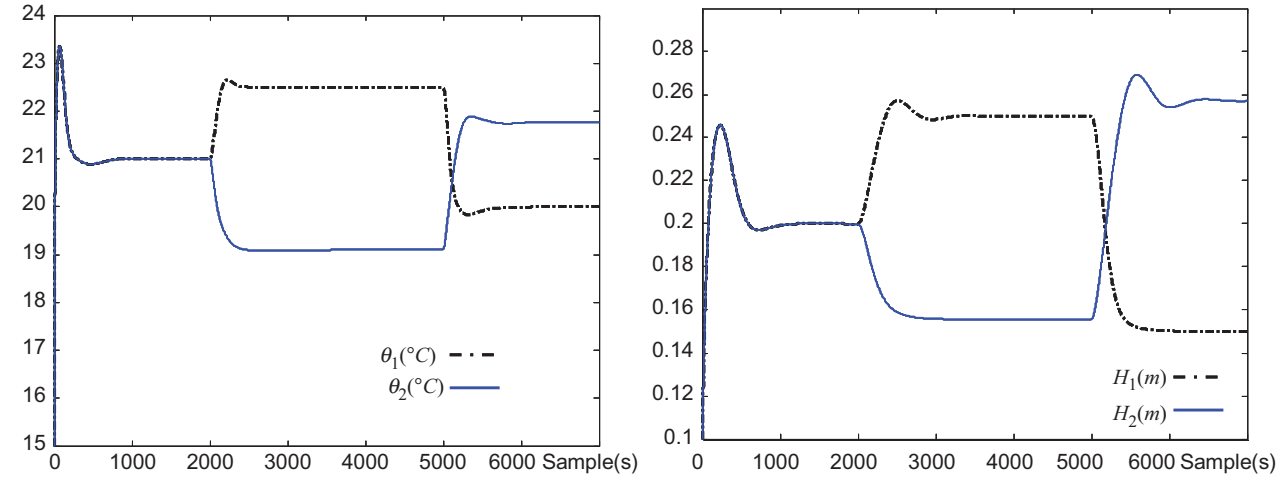

Figure 5. Dynamic evolution of local output variables in the fault-free case.

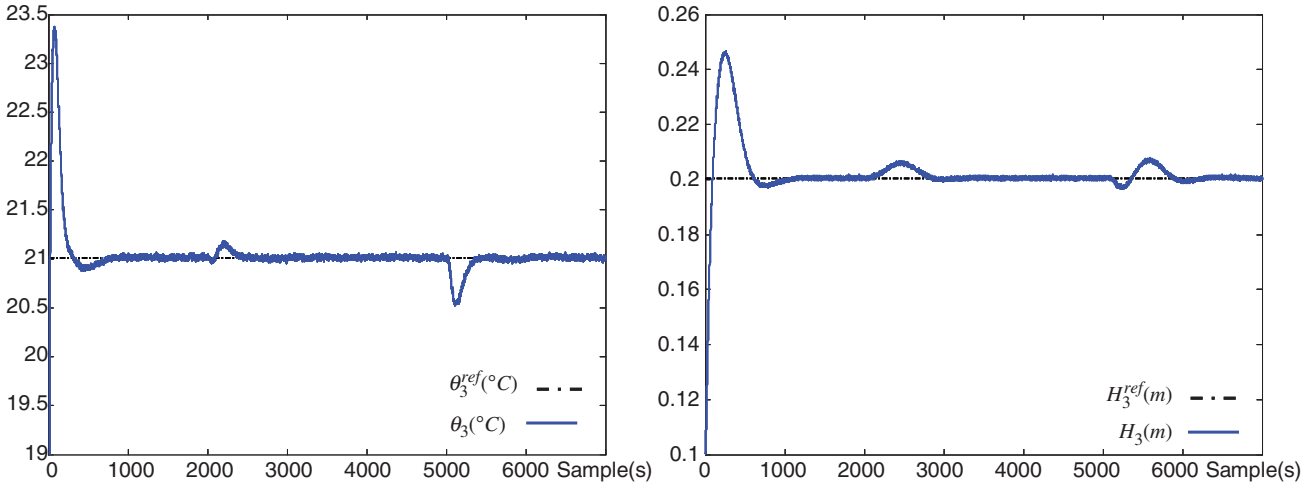

Figure 6. Dynamic evolution of global objectives in the fault-free case.

of 7000 s. Even though some local objectives take several steps and the initial conditions are not close to the reference inputs, the dynamic responses demonstrate that the hierarchical controllers are synthesised correctly (Figure 5). As presented in Figure 6, the fluid level and the fluid temperature in the last tank reach their reference values. The hierarchical controllers preserve the global objective of the system in the presence of step-type reference inputs. Figure 7 shows the corresponding control inputs.

4.3.2. *Actuator fault case without reconfiguration*

A gain degradation of the power in the resistor due to material ageing or a failure, which is equivalent to 70% loss of effectiveness, is supposed to occur at 3500 s. Then, if the output of the controller is equal to P, the power in the resistor applied to the water is equal to $0.3P$ due to the fault. Based on the same controllers as the nominal case, only the local objective θ_1 cannot be achieved for both dynamic and steady-state performances. The consequence of an actuator fault on the local objective is illustrated in Figure 8. The result is that the global objective cannot be achieved, as shown in Figure 9. Due to the fact that the local objectives take several steps, θ_3 is directly affected by the nominal controllers established in the fault-free case: the power designed by the control law in the resistor is saturated as presented in Figure 10. Compared to the dynamic behaviour in the fault-free case, the actuator fault affects only the fluid temperature.

4.3.3. *Actuator fault case with reconfiguration*

The same fault is considered as previously. It is equivalent to a 70% loss of effectiveness occurring at 3500 s. Once the fault is isolated and its magnitude is estimated, the reconfiguration task (FTCS design) is

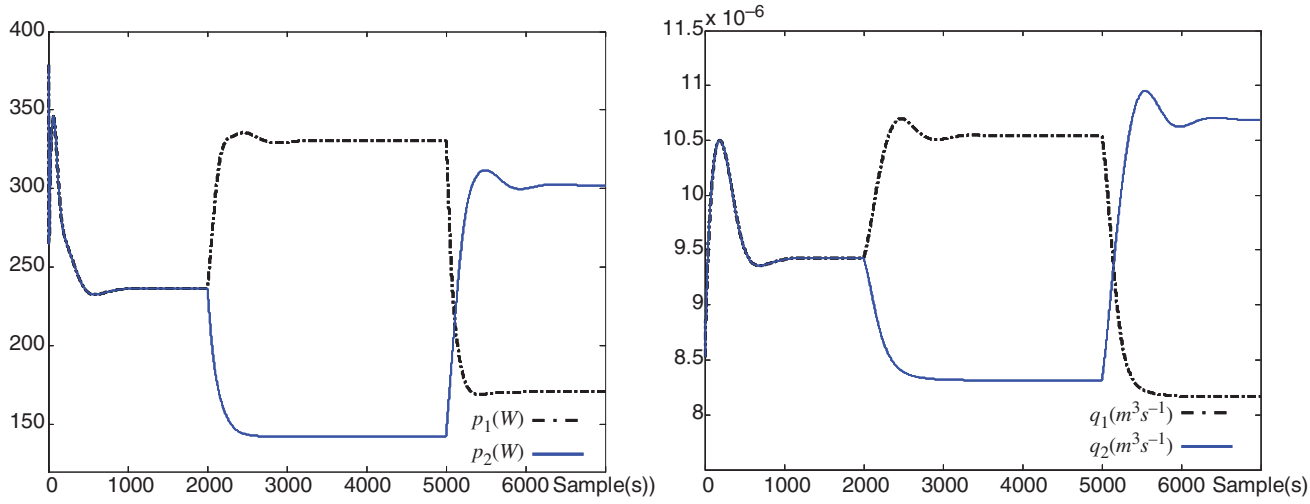

Figure 7. Dynamic evolution of local input variables in the fault-free case.

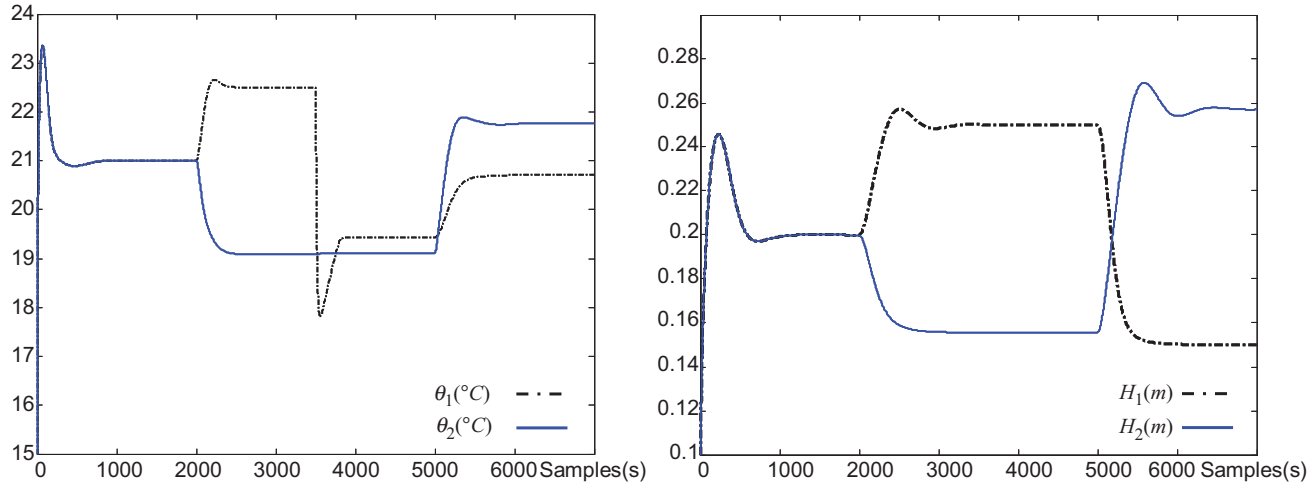

Figure 8. Dynamic evolution of local output variables in the faulty case.

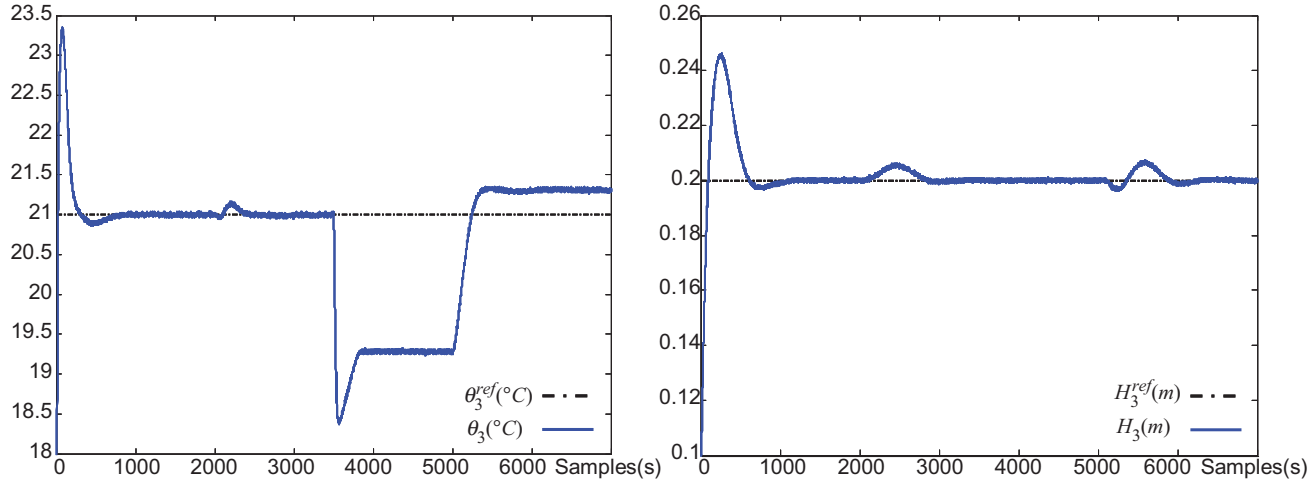

Figure 9. Dynamic evolution of global objectives in the faulty case.

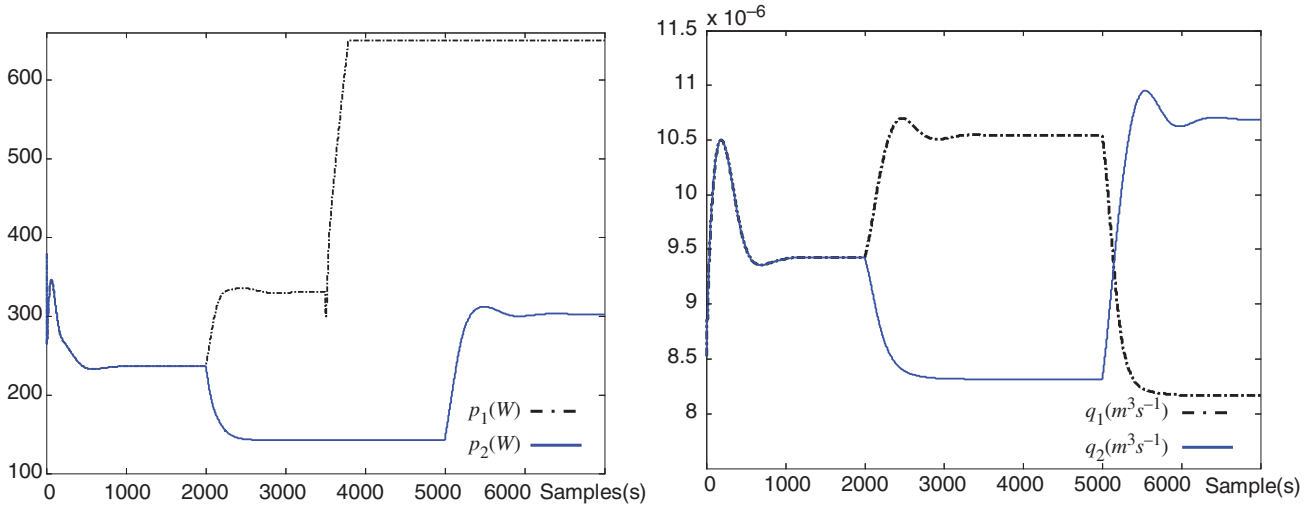

Figure 10. Dynamic evolution of local input variables in the faulty case.

Table 1. Local and global performances of the system under structures S_1, S_2 and S_3.

	S_1	S_2	S_3
H_1	–	0.20	0.1683
θ_1	–	19.9481	17.2711
H_2	0.8	0.20	0.2174
θ_2	20.978	22.023	22.6701
R_{q1}	–	0.9060	0.9129
R_{p1}	–	0.2258	0.7972
R_{q2}	0.76	0.9169	0.9135
R_{p2}	0.79	0.8607	0.8210
C_{q1}	–	0.0188	0.0173
C_{p1}	–	0.2143	0.0326
C_{q2}	0.0427	0.0158	0.0165
C_{p2}	0.0472	0.0255	0.0335
H_3	0.2	0.2	0.1920
θ_3	20.978	20.974	20.1431
J_{steady}	0.001	0.0012	0.0806
J_{dyn}	0	$9.1665*10^{-5}$	$9.1665*10^{-5}$
J	$5.0*10^{-4}$	$1.0583*10^{-3}$	$4.0345*10^{-2}$
C_g	0.0899	0.2743	0.1000
$R_g(T_d)$	0.60	0.8323	0.9319

performed in order to reduce the fault effects on the system and select an optimal structure in order to reach the nominal global objectives.

Table 1 illustrates values of the local and the global objectives of the system, reliabilities and the performance indices for all the structures. The criterion J is defined as $\mathsf{J} = \alpha J^m_{\text{steady, opt}} + (1-\alpha) J^m_{\text{dyn}}$ and it is evaluated using Equations (24), (25) and (26) with $\alpha = 0.5$.

Note that the value of desired reliability is $R^* = 0.55$ and the desired lifetime is $T_d = 10000$ s. According to the constraints R^* and C^* and the performance indices J^m in the structure S_1. Since J^1 has minimal value, it is selected as optimal. Thus, after fault occurrence, the faulty system is switched to the new structure S_1. This leads to the disconnection of the tank 1. The local objectives of tank 2 are applied; they correspond to $\theta_2 = 20.978^\circ$C and $H_2 = 0.8$ m, as shown in Figure 11.

The disconnection of tank 1 is carried out by the immediate zero setting of p_1 and q_1 values and closing the connection between tank 1 and tank 3 (Figure 12). This justifies the fall of the level H_3 to 0.05 m, which is equal to $\left(\frac{\alpha_2\sqrt{H_2}}{\alpha_3}\right)^2$ and an increase in temperature θ_3. After transitory duration, the level H_3 and the temperature θ_3 take the values of desired references, as illustrated in Figure 13. These variations of references allow illustration of the effectiveness of the control law p_2 and q_2, which allows reduction of differences between references and actual outputs. The outputs H_2 and θ_2 coincide with the values of references H_2^{ref} and θ_2^{ref}, and the global outputs H_3 and θ_3 coincide with their references. Due to a time delay of a few seconds between fault occurrence and fault diagnosis, the switching procedure generates a time response and an overshoot of the compensated outputs: this dynamic behaviour could be reduced according to a fault diagnosis method. Note that the controller gains of tank 2 are not changed and they take the same values of nominal gains, because the considered fault influences only the disconnected tank (tank 1).

5. Conclusions

This article has presented an FTCS design strategy which can incorporate reliability analysis and performance evaluation into the reconfigurable control structure selection based on the hierarchical architecture of complex systems. Such a strategy requires many computations and is consequently time consuming.

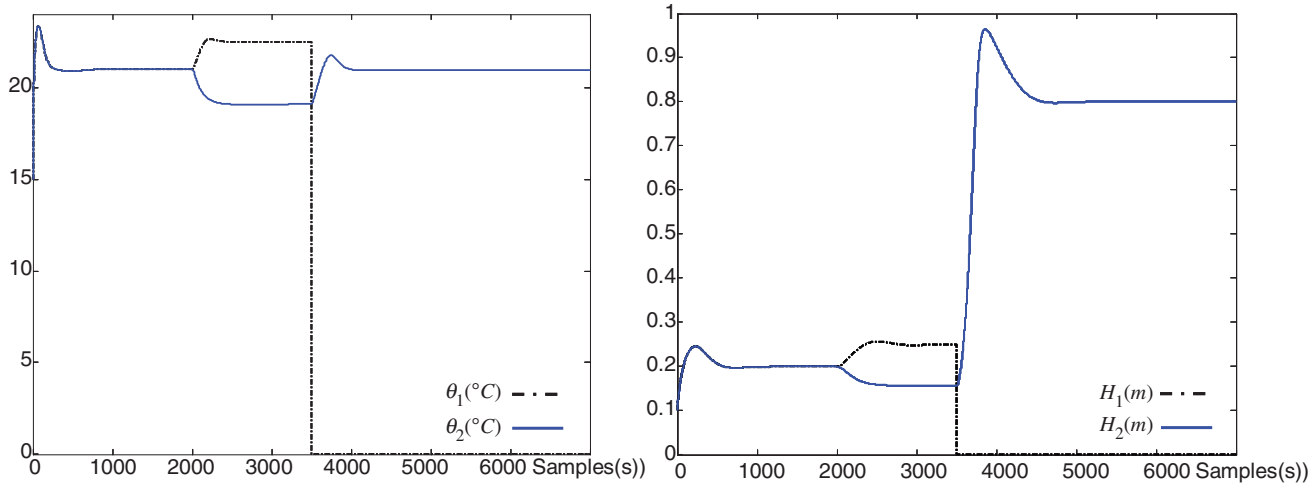

Figure 11. Dynamic evolution of local output variables in the faulty case with FTC.

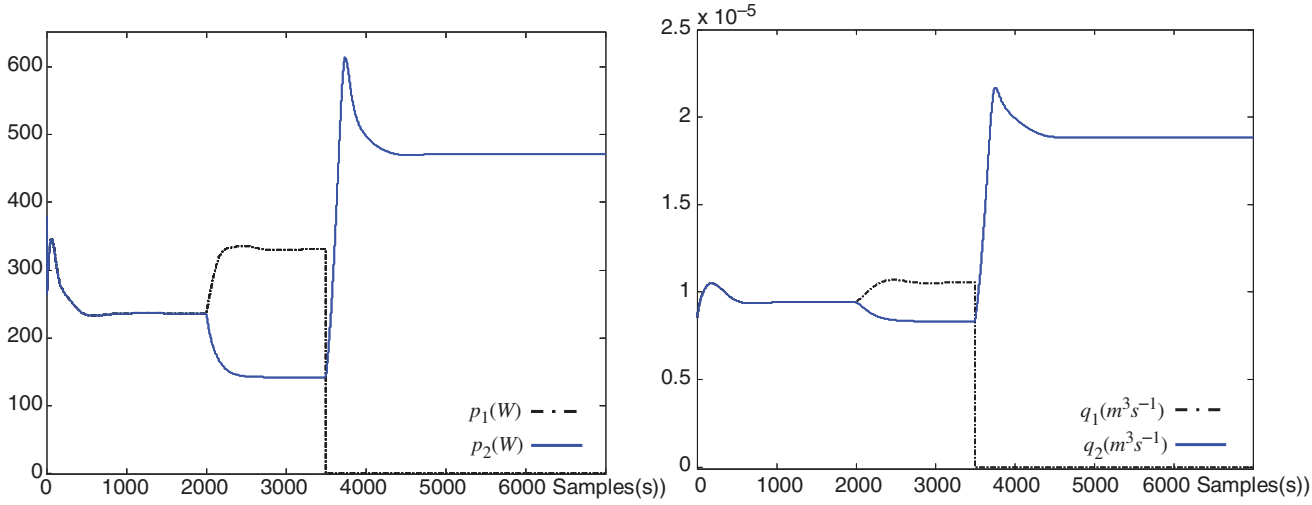

Figure 12. Dynamic evolution of local input variables in the faulty case with FTC.

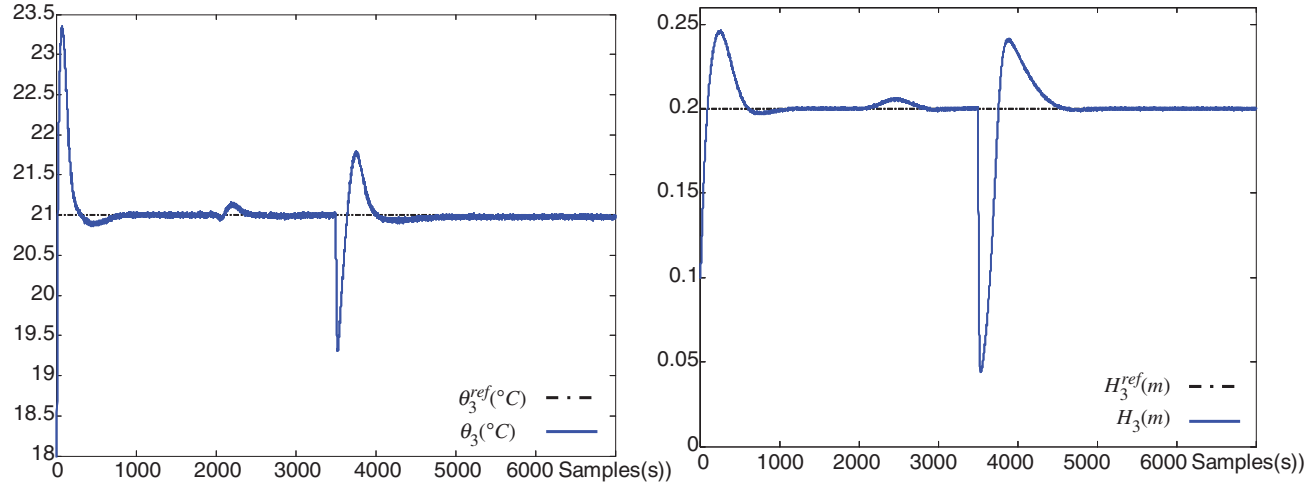

Figure 13. Dynamic evolution of global output variables in the faulty case with FTC.

This constraint can be a limitation in order to apply the developed method to a process with a very low-sampling period. Once a fault occurs and the global objectives of system cannot be achieved using the current structure, the proposed FTC strategy will switch to another structure. The selected structure will guarantee an optimal steady-state and dynamic performance of the reconfigured system according to the 'highest' reliability in order to ensure the dependability of the system and human safety under cost constraints. The effectiveness and performance of the FTCS design strategy have been illustrated on the entire operating conditions of a nonlinear thermal and hydraulic system. Several issues could be investigated in future work. For instance, the proposed approach requires some information about the location, the amplitude and the type of the fault. They are not available unless a FDI module is designed and integrated with the FTCS. Moreover, in order to consider the proposed strategy for processes with a very high sampling period, it is crucial to develop techniques which prove to be less time consuming.

Acknowledgement

Partial support from the European project IFATIS (IFATIS EU-IST-2001-32122) is greatly acknowledged.

Notes on contributors

Fateh Guenab received his State Engineering degree in Automatic Control in 2000 from Setif University, Algeria, his MSc degree in Automatic Control from Institut National Polytechnique de Grenoble, France, in 2003, and his PhD degree in Automatic Control and Signal Processing in 2007 from Henri Poincaré University, Nancy France. Since october 2007, he has occupied a postdoctoral position at Heudiasyc, CNRS Research Unit, Compiègne, France. His research interests are focused on fault tolerant control systems, reconfigurable control systems, safety and reliability of systems.

Philippe Weber received his MS degree in Automatic Control and Signal Processing in 1995 from the University Henri Poincaré, Nancy, France, and his PhD degree in 1999 from Institut National Polytechnique de Grenoble, Grenoble, France. He has been an Assistant Professor at Nancy University since 2000, and a member of the Research Centre for Automatic Control (CRAN) associated with the National Research Centre of Science CNRS (UMR 7039). He focuses his interest on modelling problems in maintenance, prognosis, decision-making processes and dynamic reliability. He develops fault tolerant control systems including reliability analysis. Since 2000 his research interest has been focused on modelling methods based on Bayesian networks.

Didier Theilliol received his PhD degree in Control Engineering from Nancy University (France) in 1993. Since September 2004, he has been a Full Professor in the Research Centre for Automatic Control of Nancy (CRAN) at Nancy-University where he co-ordinates and leads national, European and international R&D projects in steel industries, wastewater treatment plant and aerospace domains. His current research interests include model-based fault diagnosis method synthesis and active fault-tolerant control system design for LTI, LPV, multi-linear systems including reliability analysis. He is a chair of the Intelligent Control and Diagnosis working group where different French and German research teams are involved. He has published over 70 journal and conference articles.

Youmin Zhang received his PhD degree in 1995 from the Department of Automatic Control, Northwestern Polytechnical University, Xian, P.R. China. He held several teaching and research positions in Northwestern Polytechnical University, University of New Orleans, Louisiana State University, State University of New York at Binghamton, the University of Western Ontario, and Aalborg University Esbjerg. He is currently an Associate Professor in the Department of Mechanical and Industrial Engineering at Concordia University, Canada. His current research interests are in the areas of fault diagnosis and fault-tolerant (flight) control systems, cooperative control of unmanned aerial vehicles, dynamic systems modelling, identification and control and signal processing. He has published over 150 journal and conference articles. He is a senior member of AIAA, senior member of IEEE and a member of the IFAC Technical Committee on Fault Detection, Supervision and Safety for Technical Processes.

References

Athans, M., Fekri, S., and Pascoal, A. (20052005), 'Issues on Robust Adaptive Feedback Control', *16th World IFAC Congress*, Prague: Czech Republic.

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2006), *Diagnosis and Fault-tolerant Control* (2nd ed.), London: Springer-Verlag.

Chen, J., and Patton, R.J. (1999), *Robust Model-based Fault Diagnosis for Dynamic Systems*, Norwell, MA: Kluwer academic.

Chiang, L., Russell, E., and Braatz, R. (2001), *Fault Detection and Diagnosis in Industrial Systems*, New-York: Springer-Verlag.

Cox, D.R. (1972), 'Regression Models and Life Tables', *Journal of the Royal Statistical Society*, 34, 187–220.

Ding, S.X. (2008), *Model-based Fault Diagnosis Techniques – Design Schemes, Algorithms and tools*, London: Springer-Verlag.

Ducard, G.J.J. (2009), *Fault Tolerant Flight Control and Guidance Systems – Practical Methods for Small Unmanned Aerial Vehicles*, London: Springer-Verlag.

Finkelstein, M.S. (1999), 'A Note on Some Ageing Properties of the Accelerated Life Model', *Reliability Engineering and System Safety*, 71, 109–112.

Gao, Z., and antsaklis, P.J. (1991), 'Stability of the Pseudo-inverse Method for Reconfigurable Control Systems', *international Journal of Control*, 53, 717–729.

Gertler, J.J. (1998), *Fault Detection and Diagnosis in Engineering Systems*, New York: Marcel Dekker.

Gertsbakh, I. (2000), *Reliability theory with Applications to Preventive Maintenance*, London: Springer-Verlag.

Guenab, F., Theilliol, D., Weber, P., Ponsart, J.C., and Sauter, D. (2005), 'Fault tolerant Control Method Based on Costs and Reliability analysis', *16th Word IFAC Congress*, Prague: Czech Republic.

Hajiyev, C., and Caliskan, F. (2003), *Fault Diagnosis and Reconfiguration in Flight Control Systems*, Boston: Kluwer Academic.

He, X., Wang, Z., and Zhou, D. (2009), 'Robust H-infinity Filtering for Time-delay Systems with Probabilistic Sensor Faults', *IEEE Signal Processing Letters*, 16, 442–445.

Huang, C.Y., and Stengel, R.F. (1990), 'Restructurable Control Using Proportional-integral Implicit Model Following', *Journal of Guidance, Control and Dynamics*, 13, 303–309.

Isermann, R. (2006), *Fault-diagnosis Systems: An Introduction from Fault Detection to Fault tolerance*, Berlin, Germany: Springer.

Jiang, J., and Zhang, Y.M. (2006), 'Accepting Performance Degradation in Fault-tolerant Control System Design', *IEEE Transactions on Control Systems Technology*, 14, 284–292.

Leger, S., Hamelin, F., and Sauter, D. 'Fault Detection and Isolation Dynamic Systems Using Principal Component Analysis: Application to a Heating System Benchmark,' in *5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes,* Washington, USA, 2003, pp. 543–547.

Mahmoud, M., Jiang, J., and Zhang, Y.M. (2003), 'Active Fault tolerant Control Systems: Stochastic Analysis and Synthesis', *Lecture Notes in Control and information Sciences* (Vol 287), Berlin, Germany: Springer-Verlag.

Martorell, S., Sanchez, A., and Serradell, V. (1999), 'Age-dependent Reliability Model Considering Effects of Maintenance and Working Conditions', *Reliability Engineering and System Safety*, 64, 19–31.

Mettas, A. Reliability Allocation and Optimization for Complex Systems, in *Proceedings of the annual Reliability and Maintainability Symposium, institute Electrical and Electronics Engineers*, Piscataway, NJ, pp. 216–221, 2000.

Murray-Smith, R., and Johansen, T. (1997), *Multiple Model Approaches to Modelling and Control*, London: Taylor and Francis.

Narendra, K., and Balakrishnan, J. (1997), 'Adaptive Control Using Multiple Models', *IEEE Transactions on Automatic Control*, 42, 171–187.

Noura, H., Theilliol, D., and Sauter, D. (2000), 'Actuator Fault-tolerant Control Design: Demonstration on a Three-tank-system', *international Journal of Systems Science*, 31, 1143–1155.

Ozkan, L., Kothare, M., and Georgakis, C. (2003), 'Control of a Solution Copolymerization Reactor Using Multi-model Predictive Control', *Chemical Engineering Science*, 2, 765–779.

Patton, R.J. *Fault-tolerant Control: The 1997 Situation*, in IFAC Symposium Safeprocess'97, Kingston Upon Hull, UK, pp. 1033–1055, 1997.

Simani, S., Fantuzzi, C., and Patton, R.J. (2003), *Model-based Fault Diagnosis in Dynamic Systems using Identification Techniques*, New York: Springer.

Singh, M.G., and Titli, A. (1978), *Systems Decomposition, Optimisation and Control*, Oxford: Pergamon Press.

Staroswiecki, M., and Gehin, A.L. (1998), 'Analysis of System Reconfigurability Using Generic Component Models', *UKACC Control'98*, Swansea, UK.

Staroswiecki, M., and Gehin, A.L. (2001), 'From Control to Supervision', *Annual Reviews in Control*, 25, 1–11.

Staroswiecki, M., Hoblos, G., and Aitouche, A. (2004), 'Sensor Network Design for Fault tolerant Estimation', *International Journal of Adaptive Control and Signal Processing*, 18, 55–72.

Staroswiecki, M. (2005), 'Fault Tolerant Control: The Pseudo-inverse Method Revisited', *16th Word IFAC Congress*, Prague: Czech Republic.

Tayebi, A., and Zaremba, M. (2002), 'Iterative Learning Control for Non-linear Systems Described by a Blended Multiple Model Representation', *International Journal of Control*, 75, 1376–1384.

Theilliol, D., Noura, H., and Ponsart, J.C. (2002), 'Fault Diagnosis and Accommodation of a Three-tank-system Based on Analytical Redundancy', *ISA Transactions*, 41, 365–382.

Toscano, R., and Lyonnet, P. (2006), 'Robustness analysis and Synthesis of a Multi-PID Controller Based on an Uncertain Multimodel Representation', *Computers and Chemical Engineering*, 31, 66–77.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., and Kavuri, S.N. (2003a), 'A Review of Process Fault Detection and Diagnosis. Part I: Quantitative Model-based Methods', *Computers and Chemical Engineering*, 27, 293–346.

Venkatasubramanian, V., Rengaswamy, R., and Kavuri, S.N. (2003b), 'A Review of Process Fault Detection and Diagnosis. Part II: Qualitative Models-based Methods', *Computers and Chemical Engineering*, 27, 313–326.

Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N., and Yin, K. (2003c), 'A Review of Process Fault Detection

and Diagnosis: Part III. Process History Based Methods', *Computers and Chemical Engineering*, 27, 327–346.

Wan, Z., and Kothare, M. (2003), 'Efficient Scheduled Stabilizing Model Predictive Control for Constrained Nonlinear Systems', *International Journal of Robust and Nonlinear Control*, 13, 331–346.

Wang, Z., Huang, B., and Unbehauen, H. (1999), 'Robust Reliable Control for a Class of Uncertain Nonlinear State Delayed Systems', *Automatica*, 35, 955–963.

Witczak, M. (2007), 'Modelling and Estimation Strategies for Fault Diagnosis of Non-linear systems: From analytical to Soft Computing Approaches', *Lecture Notes in Control and information Sciences* (Vol 354),Berlin, Germany: Springer.

Eva, N., Wu, X., Wang, Smapath, M., and Kott, G. (2002), 'An Operational Approach to Budget-constrainted Reliability Allocation', in 15th Word IFAC Congress, Barcelona, Spain, pp. 199–204.

Eva Wu, N. (2001a) Reliability of Fault Tolerant Control Systems: Part I, in *40th IEEE Conference on Decision and Control*, Orlando, FL, USA, pp. 1460–1465.

Eva Wu, N. (2001b) Reliability of Fault tolerant Control Systems: Part II, in *40th IEEE Conference on Decision and Control*, Orlando, FL, USA, pp. 1466–1471.

Eva Wu, N., and Patton, R.J. (2003) Reliability and Supervisory Control, in *5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Washington, DC, USA, pp. 139–144.

Zhang, Y.M., and Jiang, J. (2008), 'Bibliographical Review on Reconfigurable Fault-tolerant Control Systems', *Annual Reviews in Control*, 32, 229–252.

Zhang, Y.M., Jiang, J., and Theilliol, D. (2008), 'Incorporating Performance Degradation in Fault Tolerant Control System Design with Multiple Actuator Failures', *International Journal of Control, Automation, and Systems*, 6, 327–338.

Appendix: Reliability and costs parameters

Table A1. Failure rate (λ), load (ϑ), price (ς) and failure cost (P) parameters.

Component	q_1	p_1	q_2	p_2
$\lambda(\text{hour}^{-1})$	3.77e-6	5.77e-6	3.21e-6	4.25e-6
ϑ	10.211e + 4	5.000e-3	10.548e + 4	8.000e-3
ς(€)	900	440	820	700
P (€)	1000	1000	1000	1000

Table A2. Reliability (R) and Cost (C) functions.

Structure S_1	$R_g^1(t) = R_{q2}^1(t) \times R_{p2}^1(t)$
	$C_g^1(t) = C_{q2}^1(t) + C_{p2}^1(t)$
Structure S_2	$R_g^2(t) = 1 - (1 - R_{q1}^2(t) \times R_{p1}^2(t))$
	$\times (1 - R_{q2}^2(t) \times R_{p2}^2(t))$
	$\times$ with $p_1(t) = (1 - \beta^f) \times p_1^{\max}$
	$C_g^2(t) = C_{q1}^2(t) + C_{p1}^2(t) + C_{q2}^2(t) + C_{p2}^2(t)$
	$\times$ with $p_1(t) = (1 - \beta^f) \times p_1^{\max}$
Structure S_3	$R_g^3(t) = 1 - (1 - R_{q1}^3(t) \times R_{p1}^3(t))$
	$\times (1 - R_{q2}^3(t) \times R_{p2}^3(t))$
	$C_g^3(t) = C_{q1}^3(t) + C_{p1}^3(t) + C_{q2}^3(t) + C_{p2}^3(t)$