Fault tolerant control system design: A reconfiguration strategy based on reliability analysis under dynamic behavior constraints

Fateh Guenab, Didier Theilliol, Philippe Weber, Youmin Zhang, Dominique Sauter

FAULT TOLERANT CONTROL SYSTEM DESIGN: A RECONFIGURATIN STRATEGY BASED ON RELIABILITY ANALYSIS UNDER DYNAMIC BEHAVIOR CONSTRAINTS

F. Guenab[(°)], D. Theilliol[(°)], P. Weber[(°)], Y.M. Zhang[(+)] and D. Sauter[(°)]

[(°)]Centre de Recherche en Automatique de Nancy (CRAN - UMR 7039) Nancy-University, CNRS
BP 239 - 54506 Vandoeuvre Cedex - France.
Email: fateh.guenab@cran.uhp-nancy.fr
Phone: +33 383 684 465 - Fax: +33 383 684 462
[(+)]Department of Computer Science and Engineering - Aalborg University Esbjerg
Niels Bohrs Vej 8, 6700 Esbjerg - Denmark.

Abstract: The main goal of this paper is to develop a fault tolerant control system that incorporates both reliability and dynamic performance of the system for control reconfiguration. Once a fault has been detected and isolated, the reconfiguration strategy proposed in this paper tries to find possible structures of the faulty system that preserve pre-specified performance, calculate the system reliability, compute new controller gains and finally search the optimal structure that has the "best" control performance with the highest reliability. The proposed approach is illustrated through a simulation example.

Keywords: Fault Tolerant Control, System Reliability, Pseudo Inverse Method, 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 tolerance capabilities, in order to meet reliability and performance requirements. The Fault Tolerant Control (FTC) system is a control system that can maintain system performance closely to the desirable one and preserves stability conditions, not only when the system is in fault-free case but also in the presence of faulty component, or at least ensures degraded performances which can be accepted as a trade-off. FTC has been motivated by different goals for different applications; it could improve reliability and safety in industrial processes and safety-critical applications such as flight control and nuclear power plant operation (Zhang and Jiang, 2003).

Fault tolerant control systems are needed in order to preserve the ability of the system to achieve the objectives that has been assigned when faults or failures occurred. (Staroswiecki and Gehin, 2001) proposes a terminology on fault tolerant control problems. The main goal of FTC is to increase system's reliability. Some publications have introduced reliability analysis for fault tolerant control systems. In, (Wu, 2001a), (Wu, 2001b), (Wu and Patton, 2003) Markov models are used to dictate the system reliability where it's supposed that the sub-systems take two states intact (available) or failed (unavailable). Also (Staroswiecki *et al.*, 2004) have proposed a sensor reconfiguration based on physical redundancy where the reliability analysis provided some information in order to select the optimal redundant sensors. More recently, (Guenab *et al.*, 2005) have proposed a FTC system for complex system composed with various sub-systems. The FTC method provides an optimal structure in order to achieve desired objectives with highest reliability under a cost constraint or with lowest cost to achieve reliability goal, or at least degraded objectives. It can be noticed that the criterion used for determining the optimal structure in (Guenab *et al.*, 2005) is only limited to static consideration. In this paper, the dynamic behavior of the faulty and reconfigured closed-loop system is taking into account. In this context, complex system is considered as a set of interconnected sub-systems, each sub-system is assigned some local objectives with respect to quality production, reliability and also dynamic performance. Each sub-system may take several states, and specific controllers' gains. In fault-free case, the structure of a system defines the set of the used sub-systems and information about their states and how they are connected. Once fault is occurred, the faulty sub-systems are considered able to achieve new local objectives at different degraded states. New structures of the system can be determined; each possible structure of the system corresponds to reliability and global performance computed from its sub-system properties. Concerning the redesign of controller for each sub-system after fault occurrence, the revisited Pseudo-Inverse Method (PIM) developed by (Staroswiecki, 2005) is considered here in order to illustrate the concept of the method. Moreover, the revisited PIM seems to be less conservative than the original one (Gao and Antsaklis, 1991) by redesigning the controller gain through a bounded dynamic behavior assignable by the reconfigured closed-loop system. The optimal structure corresponds to the structure that achieves the required global objectives (static and dynamic) with highest reliability. Once the optimal solution is fixed, a new structure and new control law could be exploited in order to reach the global objectives closed as possible as nominal ones.

The paper is organized as follows. Section 2 is dedicated to define the set of complex systems which is considered in this study and the associated standard problem of FTC. Section 3 is devoted to the design of the FTC system under 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 method. Finally, concluding remarks are given in the last section.

2. PROBLEM STATEMENT

A large class of systems can be described by hierarchical structures, also called as systems with multiple levels, and there are good reasons for organizing the control of the systems in this way, for example reduction in complexity of communication and computation. Our interest is for hierarchy with two levels: global and local, as shown in the following structure S_m:

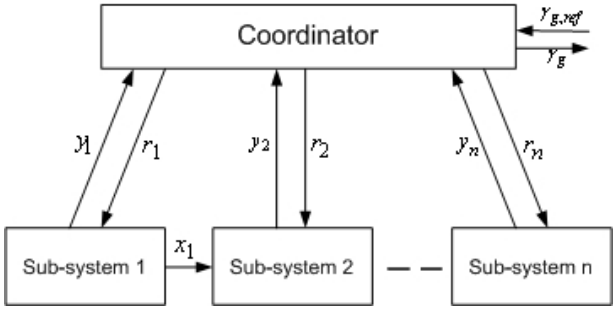

Figure 1. General scheme of hierarchical structure

The considered system is composed of n sub-systems s_i, $i = 1,\ldots,n$, described by the following classical linear state representation:

$$\dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) \qquad (1)$$

Each sub-system s_i has its own associated controller that implements the following control law:

$$u_i(t) = -K_i x_i(t) + G_i r_i(t) \qquad (2)$$

where K_i and G_i are synthesized in order that the closed-loop system follows its reference model described as follows:

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

The highest level, called coordinator, is designed as an optimal feedback controller. It defines local references r_i and computes the global objective γ_g from local outputs y_i of each sub-system s_i.

In this paper, we assume that sub-systems are dynamically independent, which means that matrix A is block diagonal. Moreover, we suppose that sub-system s_i has impact on sub-system s_{i+1} **or** inversely: matrix A is supposed to be triangular. Based on a nominal hierarchical structure of the system, the paper aims at to propose an answer to a question: how is it possible to maintain the global objective γ_g when fault occur? Before going to envision a solution let us define the control problem by the triplet $< \gamma_g, C, U >$, in the spirit of (Staroswiecki and Gehin, 2001), where:

- γ_g Global objectives
- C A set of constraints given by the structure S of system and parameters θ of closed-loop system
- U A set of control laws

In fault-free case, this problem could be solved by defining a control law $u \in U$, such that the controlled system achieves the global objectives γ_g under constraints whose structure S and parameters θ are equivalent to design controllers of all sub-systems used by the structure and to define their references to achieve γ_g. It is assumed that nominal global objectives γ_g^{nom} are achieved under the nominal control law u_{nom} and the nominal structure S_{nom} which uses some sub-systems. The fault occurrence is supposed to modify the structure S_{nom} for which the objectives can be or can not be achieved under a new structure.

The fault tolerant control problem is then defined by $< \gamma_g, C, U >$, which has a solution that could achieve γ_g^{nom} by changing the structure, parameters and/or control law of the post-fault system (which results in the disconnection or replacement of faulty sub-systems). In some cases, no solution may exist, and then global objectives must be redefined to the degraded ones, denoted as γ_g^d.

Under assumptions that there exist several structures S_m $m=(1,\ldots,M)$, the problem statement is formulated by the following question: how to choose the optimal structure in the sense that for a given criterion J the chosen structure can maintain the objectives γ_g^{nom} (or degraded ones γ_g^d)? An answer will be provided in the following section where impact of references on the reliability and its computation, controllers design in fault-free and faulty cases, performance evaluation criteria will be presented in the hierarchical structure framework.

3. FTC SYSTEM 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). The reliability analysis of components consists of analyzing times to failure from data obtained under normal operating conditions (Cox, 1972). In many situations and especially in the considered study, failure rate have to be 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 failure level in order to estimate the failure rate λ (Martorell *et al.*, 1999) (Finkelstein, 1999). Proportional hazards model introduced by (Cox, 1972) is used in this paper. The failure rate is modelled as follows:

$$\lambda_i(t,x) = \lambda_i(t)g(x,\beta) \qquad (4)$$

where $\lambda_i(t)$ represents the baseline failure rate (nominal failure rate) function of time only for the i^{th} sub-system or component and $g(x,\beta)$ is a function (independent of time) taking into account the effects of applied loads with x defining an image of the load and β defining some parameters of the sub-system or component.

Various definitions of $g(x,\beta)$ exist in the literature. However, the exponential form is commonly used. Also, the failure rate function for the exponential distribution is constant during the useful life (Cox, 1962), but it changes from one operating mode (depending on the structure S_{nom}) to another according to a load level. Under this assumption, the failure rate (4) is rewritten as:

$$\lambda_i^m(t,x) = \lambda_i(t)e^{\beta x_m} \qquad (5)$$

It can be noticed that various load levels (or mean load levels) x_m are considered as constants for the i^{th} sub-system or component, but it changes from one hierarchical structure to another. Once the new failure rate is calculated, the reliability for a period of time T_d (desired life time) is given by:

$$R_i^m(T_d) = e^{-\lambda_i^m(T_d,x)T_d} \qquad (6)$$

where $R_i^m(T_d)$ represents the i^{th} sub-system reliability used by the structure S_m for specified time T_d. It should be remarked that T_d represents the period of time between the fault occurrence and the reparation of faulty component which caused the structure modification or the end of the system's mission.

The reliability of a complex system is computed from its components or sub-systems reliabilities and that usually depends on the way that the sub-systems are connected (serial, parallel…).

The reliability of a complex system with n series sub-systems is given by:

$$R_g^m(T_d) = \prod_{i=1}^{n} R_i^m(T_d) \qquad (7)$$

and with n parallel sub-systems is given by:

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

In general case, the system reliability is computed from a combination of the elementary functions (7) and (8).

3.2 Nominal Controller Design

In fault-free case, let us assume that (A_i, B_i) with $i=1,\ldots,n$ is controllable according to the state-space representation defined in equation (1). Classically, the design of the control law (2) is established such that closed-loop of the system (1) is equivalent to a specified reference model defined in (3). The solution (K_i, G_i) is obtained by solving the equations:

$$\begin{aligned} A_i - B_i K_i &= M_i \\ B_i G_i &= N_i \end{aligned} \qquad (9)$$

A unique solution is defined as follows

$$\begin{aligned} K_i &= B_i^+(A_i - M_i) \\ G_i &= B_i^+ N_i \end{aligned} \qquad (10)$$

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

If (10) can not be fulfilled, as presented by (Huang and Strangel, 1990), approximate solutions are computed through the optimization of the following criteria:

$$J_{i1} = \left\| A_i - B_i K_i - M_i \right\|_F^2 \qquad (11)$$

and

$$J_{i2} = \left\| B_i G_i - N_i \right\|_F^2 \qquad (12)$$

where $\left\| . \right\|_F$ is the Frobenius norm.

Unfortunately, the solution of this standard method has several drawbacks. Extensions of the Pseudo-Inverse Method (PIM) have been proposed to overcome those drawbacks. Using constrained optimization (Gao and Antsaklis, 1991) and (Staroswiecki, 2005) synthesized a suitable $\left(K_i^*, G_i^*\right)$ which guarantees the stability with successful results in faulty cases, when the i^{th} faulty sub-system is described by the fault corrupted state space representation as:

$$\dot{x}_i(t) = A_i^f x_i(t) + B_i^f u_i(t) \qquad (13)$$

where *f* stands for fault condition.

In this paper, in order to redesign the controller dedicated to each i^{th} faulty sub-system, the recent revisited PIM (Staroswiecki, 2005) has been considered rather than classical PIM.

Under the assumptions that FDD scheme provides suitable information, the revisited PIM can provide an appropriate $\left(K_i^*, G_i^*\right)$ with a degree of freedom in order to solve (9) concerning the dynamic behavior of the faulty closed loop sub-system.

As presented previously, the control problem is defined by $< \gamma, C, U >$, in faulty-case and for each sub-system, the triplet is equivalent to:

$$\begin{aligned} &\gamma_i : \begin{cases} \dot{x}_i(t) = M_i x_i(t) + N_i r_i(t) \\ (M_i, N_i) \in \boldsymbol{\mathcal{M}}_i \times \boldsymbol{\mathcal{N}}_i \end{cases} \\ &C_i : \dot{x}_i(t) = A_i^f x_i(t) + B_i^f u_i(t) \\ &U_i : u_i(t) = -K_i^f x_i(t) + G_i^f r_i(t) \end{aligned} \qquad (14)$$

where (M_i, N_i) are in the sets of admissible reference models $\boldsymbol{\mathcal{M}}_i \times \boldsymbol{\mathcal{N}}_i$. In faulty case, $\boldsymbol{\mathcal{M}}_i$ is defined by:

$$\boldsymbol{\mathcal{M}}_1 = \left\{ M_i \,\middle|\, \phi_{1i}(M_i) \le 0 \quad and \quad \phi_{2i}(M_i) > 0 \right\} \qquad (15)$$

where functions ϕ_{1i} and ϕ_{2i} describe any matrix M_i which has suitable dynamic behaviors, i.e. stability and appropriate time response. The functions $\phi_{2i}(M_i) > 0$ can be rewritten as $-\phi_{2i}(M_i) < 0$ and (15) is equivalent to a unique function $\phi_i(M_i) < 0$:

$$\boldsymbol{\mathcal{M}}_i = \left\{ M_i \;\middle|\; \phi_i(M_i) \le 0 \right\} \qquad (16)$$

In this paper, for simplicity reason but without loss of generality, we assume that for each sub-system the set $\boldsymbol{\mathcal{M}}_i$ is defined such that any matrix in $\boldsymbol{\mathcal{M}}_i$ has eigenvalues lie within a suitable percentage of eigenvalues in the fault-free based on the knowledge on the system.

Similar to $\boldsymbol{\mathcal{M}}_i$, $\boldsymbol{\mathcal{N}}_i$ is defined as:

$$\boldsymbol{\mathcal{N}}_i = \left\{ N_i \;\middle|\; \varphi_i(N_i) \le 0 \right\} \qquad (17)$$

As suggested by (Staroswiecki, 2005) but handled with the Frobenius norm, we thus propose that the control problem in faulty case is equivalent to find $\left(K_i^*, G_i^*\right)$ as follows:

$$\begin{cases} K_i^* = \arg \min\limits_{\phi_i(A_i^f - B_i^f K_i^f) \le 0} \left\| A_i^f - B_i^f K_i^f - M_i \right\|_F^2 \\ G_i^* = \arg \min\limits_{\varphi_i(B_i^f G_i^f) \le 0} \left\| B_i^f G_i^f - N_i \right\|_F^2 \end{cases} \qquad (18)$$

For illustration, let us consider an elementary reference model $\dot{x}(t) = Mx(t)$ with

$$M = \begin{pmatrix} 5.648 & -3.112 & 12.136 \\ 4.648 & -1.112 & 10.136 \\ -3.648 & 1.112 & -8.136 \end{pmatrix}$$

and with their eigenvalues being $\tau_1^* = -1$, $\tau_2^* = -1.2$ and $\tau_3^* = -1.4$.
It can be checked that any matrix belongs to the set

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

has eigenvalues $\tau_1 = \beta\tau_1^*$, $\tau_2 = \beta\tau_2^*$ and $\tau_3 = \beta\tau_3^*$ with $\beta = [0.9,\ 1.1]$. Thus, $\mathcal{M}$ defines the set of all reference models in which its eigenvalues lie within $\pm 10\%$ of eigenvalues of M.

In order to choose the optimal structure and the optimal controller associated with each sub-system among the hierarchical architecture under the reliability constraint, we focus our attention in the next subsection to define pertinent performance indicator for both steady-state and dynamic performances.

3.3 Performance Criteria

The FTC system should reduce or try to limit the difference between the dynamic and steady-state behavior of the nominal system and 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 sub-system s_i, denoted by f such that:

$$\gamma_g = f(y_i),\ i = 1,\ldots,n \qquad (19)$$

The following normalized indicator is proposed to provide a global steady-state performance evaluation of structure $\mathcal{S}_m$:

$$J_{steady}^{m} = \left| \frac{\gamma_g^{nom} - \gamma_g^{m}}{\gamma_g^{nom}} \right| \qquad (20)$$

where γ_g^{nom} represents the global objective of the nominal (fault-free) structure $\mathcal{S}_{nom}$ and γ_g^m denotes the global objective of the reconfigured system under structure $\mathcal{S}_m$. It can be noticed that the global objective γ_g is computed on-line based on eq. (19).
About the dynamic performance evaluation, the main goal is to obtain the eigenvalues of reconfigured system close to the nominal ones. Let's consider the normalized error between nominal and reconfigured i^{th} sub-system in term of eigenvalues, then the maximal error of i^{th} sub-system can be formulated as:

$$\varepsilon_i^m = \max \left| \frac{\tau_j^{nom} - \tau_j^m}{\tau_j^{nom}} \right|,\quad j = 1,\ldots,k_i \qquad (21)$$

where each i^{th} sub-system has k_i eigenvalues τ_j, $j = 1,\ldots,k_i$ for nominal structure and τ_j^m for the reconfigured structure $\mathcal{S}_m$ which are computed online based on synthesized controller gains using (18).

Based on equation (21), the dynamic performance associated to the reconfigured structure $\mathcal{S}_m$ (composed of n_m sub-systems) is quantified by the largest normalized error and then is evaluated as follows:

$$J_{dyn}^{m} = \max(\varepsilon_i^m),\quad i = 1,\ldots,n_m \qquad (22)$$

3.4 FTC System Design

Consider a nominal system composed of n sub-systems: s_i with $i = 1,\cdots,n$. Each sub-system has following properties: set of local objectives $\gamma_l(s_i)$ (outputs), set of eigenvalues τ_i and failure rate $\lambda_l(s_i)$.

Without faults, a nominal structure is designed which uses all n sub-systems and its nominal global objectives γ_g^{nom} reached under the local objectives $\gamma_l(s_i)$ of each sub-system.
In faulty cases, M structures $\mathcal{S}_m$, $m = 1,\cdots,M$ are assumed to be suitable where each structure $\mathcal{S}_m$ contains n_m sub-systems: $\{s_1^m \quad s_2^m \quad \cdots \quad s_{n_m}^m\}$. The main goal of the method is to select a structure among M structures which ensure

global objectives γ_g^m close to nominal case γ_g^{nom}, also without neglected dynamic properties (in term 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 minimum performance criterion (24) under reliability constraints. For a desired time period T_d, the constraint is defined as the reliability larger than a limited value, i.e. $R_g^m(T_d) \geq R_g^*$.

Under the assumption that FDD scheme will provide necessary information in terms of detection, isolation and fault magnitude estimation, for each available reconfigured structure S_m, following procedure needs to be carried out:

1. At local level:

- for all combined sub-systems' references, to each sub-system s_i^m new failure rate $\lambda_i^m(s_i^m)$ is computed from its baseline failure rate according on the new applied loads which depends to various local references and a set of local objectives (outputs) $\gamma_l^m(s_i^m)$ are calculated taking into account the fault's magnitude.
- new controllers based on the synthesized gains (K_i^*, G_i^*) (18) are designed and ε_i^m (21) are evaluated.
- For a given time period T_d, the corresponding reliability $R_i^m(T_d)$ of each sub-system is computed using eq. (6).

2. At global level:

- each structure S_m involves a new set of global objectives (outputs) γ_g^m as presented in (19).
- the reliability $R_g^m(T_d)$ of system for all structures is computed using (7) and (8).
- for each reconfigured structure, from (20) a minimum performance of static index $J_{steady,opt}^m$ is evaluated using

$$J_{steady,opt}^m = \min_{R_g^m(T_g) \geq R_g^*} \left(J_{steady}^m \right) \qquad (23)$$

and dynamic index J_{dyn}^m is computed using (22).

3. To determine the optimal solution, the objective of FTC system is to find the structure that has a reliability $R_g^m(T_d) \geq R_g^*$ and with minimum performance of index J.

The criterion J is evaluated using equations (22) and (23) as follows:

$$J = \alpha J_{steady,opt}^m + (1-\alpha) J_{dyn}^m \qquad (24)$$

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

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

$$S_m^{opt} = \arg \min_{m \; R_g^m(T_g) \geq R_g^*} (J) \qquad (25)$$

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

4. SIMULATION EXAMPLE

4.1 System Description

Let us consider a LTI system given by:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \end{cases} \qquad (26)$$

where,

$$B = \begin{pmatrix} 1 & 1 & -1 & \vdots & 0 & 0 & 0 & \vdots & 0 & 0 \\ 0 & 0 & 0 & \vdots & 1 & 1.5 & -2 & \vdots & 0 & 0 \end{pmatrix}^T,$$

$$C = \begin{pmatrix} 1 & -0.2 & 1.1 & \vdots & 0 & 0 & 0 & \vdots & 0 & 0 \\ 0 & 0 & 0 & \vdots & 0 & 0 & 0 & \vdots & 2.5 & 4.2 \end{pmatrix} \text{ and}$$

$$A=\left(\begin{array}{ccc:ccc:cc} -1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 \\ -2 & 4 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & -4 & 1 & 0 & 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & -2.1 & 2.4 & 4.3 & 0 & 0 \\ 0 & 0 & 0 & -1 & 3 & 1.5 & 0 & 0 \\ 0 & 0 & 0 & 2 & -1 & 2.4 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & -1.35 & -1.8 & -2.25 & -3.15 & 2.65 \\ 0 & 0 & 0 & -1.35 & -1.8 & -2.25 & -1.2 & 3.25 \end{array}\right)$$

The system is physically decomposed into 3 sub-systems as illustrated in the following figure:

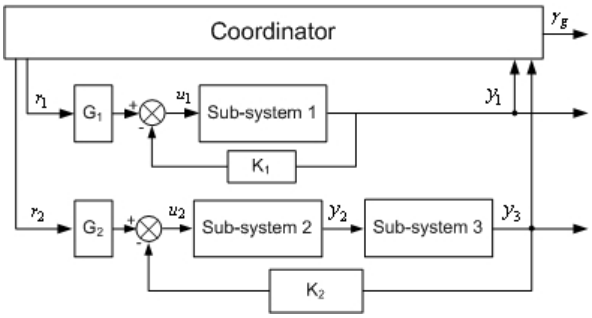

Figure 2. Block diagram decomposition

The global objective is defined by $\gamma_g(t) = y_1(t) + y_3(t)$.

The functional decomposition (in reliability sense) corresponds to:

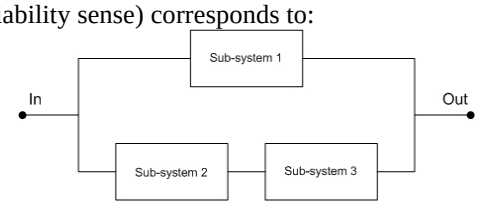

Figure. 3. Functional decomposition

In the nominal case, the reliability of the entire system is equivalent to $R_g^n(T_d) = 1 - \left(1 - R_1^n(T_d)\right)\left(1 - R_2^n(T_d)R_3^n(T_d)\right)$.

4.2 A Set of Reconfigured Structures

Three reconfigured structures are supposed to be involved in the fault tolerant control system design for this simulation example. In the first one, only sub-system 1 is used; sub-systems 2 and 3 are switched-off. The global objective depends only on the first local objective $\gamma_g = y_1$. In the second structure, only sub-systems 2 and 3 are used and the global objective depends only on the local objective of sub-system 3 i.e. $\gamma_g = y_3$. In the third structure, all sub-systems are used with the following available local objectives (in our case local references):

$$y_{1ref} = \sigma_1 y_{1,\max} \quad with \quad \sigma_1 = \left[\frac{y_{1,\min}}{y_{1,\max}}, 1\right] \qquad (27)$$

$$y_{3ref} = \sigma_2 y_{3,\max} \quad with \quad \sigma_2 = \left[\frac{y_{3,\min}}{y_{3,\max}}, 1\right] \qquad (28)$$

The global objective, reliability and performance criterion J of the system for all permitted combination of (y_1, y_3) are computed on line.

4.3 Results and Comments

To illustrate the method, three cases are simulated:

1) the nominal (fault-free) case;
2) the system with loss of control effectiveness of 10% at $t_f = 500s$ in input u_2 without control reconfiguration;
3) the reconfigured system after a fault of loss of control effectiveness of 10% in input u_2 is considered at $t_f = 500s$.

a) Nominal (fault free) case

Assume that global objective is $\gamma_g^{nom} = 12$ and for illustration purpose local objectives (y_1, y_3) take several values $(5,7)$ and $(8,4)$ as presented in Figure 4. The controller gains are $K_1 = [-6.648 \;\; 5.112 \;\; -9.136]$, $G_1 = [0.933]$, and $K_2 = [-4.9097 \;\; -7.7213 \;\; -14.9458 \;\; -2.6408 \;\; 12.8908]$ $G_2 = [-0.3767]$ in order to reach the following eigenvalues $(-1.4 \;\; -1.1999 \;\; -1)$ for the sub-system 1 and $(-2.9966 \;\; -2.5077 \;\; -1.9937 \;\; -1.5021 \;\; -0.9998)$ for the sub-systems 2 and 3. The validation of the controllers in the hierarchical architecture is shown in Figure 4. According to the coordinator level, the reference outputs (y_1 and y_3) at the local level are step changes of their corresponding operating values. The

corresponding control inputs (u_1 and u_2) for step changes in the reference inputs are also presented. The dynamic responses demonstrate that the various controllers are synthesized correctly in order to reach the nominal global objective of $\gamma_g^{nom} = 12$.

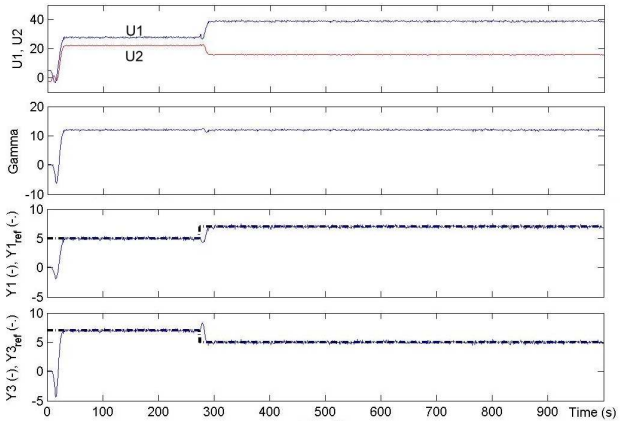

Figure 4. Dynamic evolution of input and output variables in nominal case.

b) Faulty cases without reconfiguration

A faulty case without reconfiguration is simulated for a fault with 10% loss of control input u_2 which occurs at $t_f = 500s$. Based on the same controllers as nominal case, the local objective y_3 cannot be achieved for both dynamic and steady-state performances. This leads to that the global objective cannot be achieved as shown in Figure 5. The eigenvalues of the faulty sub-systems are (-2.9297, -2.5941, -1.7835+1.8373i, -1.7835−1.8373i and -0.2391), at steady-state, there is difference between output (solid line) and the reference (broken line).

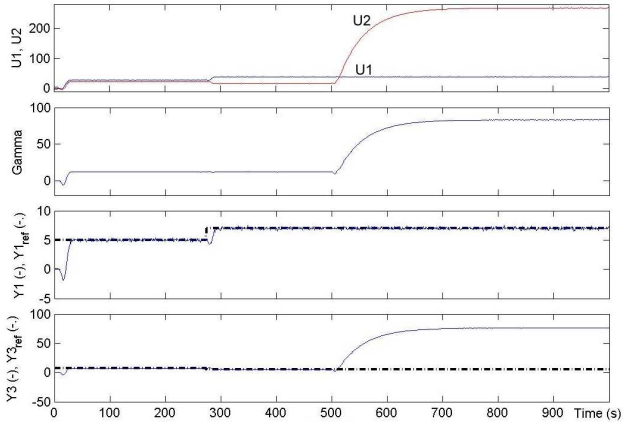

Figure 5. Dynamic evolution of inputs and outputs variables in faulty case without FTC.

c) Faulty case with reconfiguration

The same fault is considered as previously. For a desired reliability $R^* = 0.55$ and a desired life time of $T_d = 10000s$, under assumption that the fault is detected, isolated and the fault magnitude is estimated. In our simulation example, there exists a unique value of reliability and criterion J for reconfigured structure n°1 or n°2, defined in §4.2. On the other hand, for the structure n°3, the reliability and the static criterion (20) are evaluated as shown in Figures 6 and 7 using all permitted combination of (y_{1ref}, y_{3ref}) given in (27) and (28).

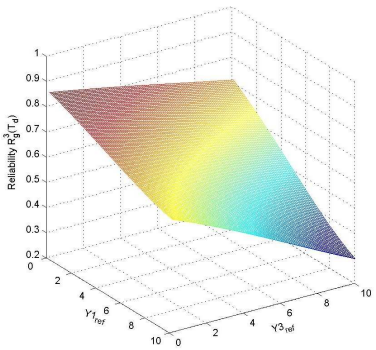

Figure 6. Reliability for structure n°3

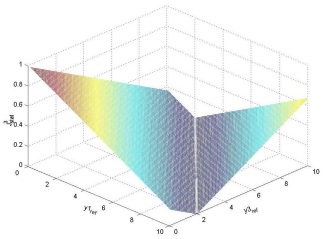

Figure 7. Steady-state criterion J^3_{steady} for structure n°3

According to (24), J^3_{opt} is equal to 0.0202 and reliability $R^3_g(T_d) = 0.64$ for references $y_{1ref} = 10$, $y_{3ref} = 2$ (as shown in Figures 6 and 7).

The controller gains are designed using (18) and dynamic index is computed using (21) and (22) for all structures.

Table 1 shows the values of reliability and performance criterion J of all structures. Based on (25), the optimal structure is chosen to be equivalent to the structure n°3.

Table 1 Reliabilities and criterions

Structure n°1		Structure n°2		Structure n°3	
$R^1_g(T_d)$	J^1	$R^2_g(T_d)$	J^2	$R^3_g(T_d)$	J^3_{opt}
0.24	0.1035	0.08	0.0852	0.64	0.0202

Thus, after fault occurrence, the nominal system is switched to the new structure, as shown in figure 8 and the references are $y_{1ref} = 10$, $y_{3ref} = 2$ and the outputs are $y_1 = 10$, $y_3 = 2$ and $\gamma^3_g = 12$. The FTC system preserves the dynamic and steady-state performance of the system in the presence of fault. It can be noted that the controller gains are $K_2 = [-7.0138 \quad -11.0305 \quad -21.3512 \quad -3.7725 \quad 18.4153]$ $G_2 = [-0.3767]$, $K_1 = [-6.648 \quad 5.112 \quad -9.136]$ and $G_1 = [0.933]$.
Those new controllers ensure new eigenvalues $(-3.0006 \quad -2.4935 \quad -2.0135 \quad -1.4899 \quad -1.0025)$ and $(-1.4 \quad -1.1999 \quad -1)$ which are close to the nominal ones.

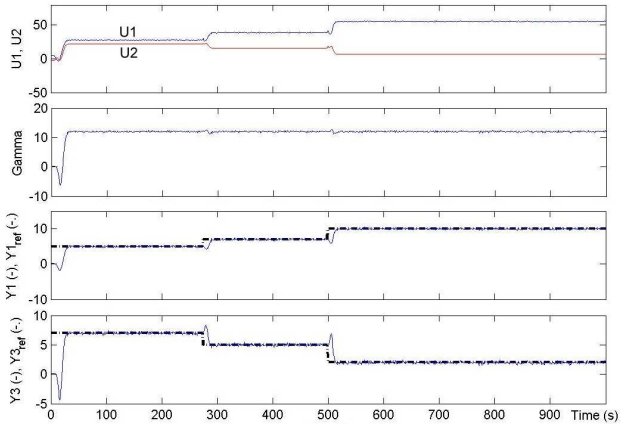

Figure 8. Dynamic evolution of inputs and outputs variables in the faulty case with FTC.

5. CONCLUSIONS

This paper has presented a fault tolerant control system design strategy which can incorporate reliability analysis and performance evaluation into the reconfigurable control structure selection based on hierarchical architecture of complex systems. Once a fault occurred and the global objectives of system can not 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 the human safety. The application of this method to a simulation example gives encouraging results.

REFERENCES

Cox, D.R. (1962). *Renewal theory*. Methuen and Co, London.

Cox, D.R. (1972). *Regression models and life tables. JR Stat Soc;* vol. 34: pp.187-220.

Finkelstein, M. S. (1999). A note on some aging properties of the accelerated life model. *Reliability Engineering and System Safety*, vol. 71, pp.109–112.

Gao Z., and P.J. Antsaklis, (1991). Stability of the pseudo-inverse method for reconfigurable control systems. *Int. Journal of Control.* vol 53, pp 717-729.

Gertsbakh, I. (2000). *Reliability theory with applications to preventive maintenance*. Springer.

Guenab F., D.Theilliol, P.Weber, J.C.Ponsart and D.Sauter (2005). Fault tolerant control method based on costs and reliability analysis. *16th IFAC Word Congress*, Prague, Czech Republic.

Huang, R., F. and C. Y. Strangel (1990). Restructurable control using proportional-integral implicit model following. *J. Guidance, Control and Dynamics* 13, 303-309.

Martorell, S., A. Sanchez and V. Serradell (1999). Age-dependent reliability model considering effects of maintenance and working conditions. *Reliability Engineering and System Safety*, vol. 64, pp.19–31.

Staroswiecki, M. (2005). Fault tolerant control: the pseudo-inverse method revisited. *16th IFAC Word Congress*, Prague, Czech Republic.

Staroswiecki, M. and A.L. Gehin (2001). From control to supervision. *Annual Reviews in Control*, vol. 25, pp.1-11.

Staroswiecki, M., G. Hoblos and A. Aitouche (2004). Sensor network design for fault tolerant estimation. *Int. J. Adapt. Control Signal Process*, vol. 18, pp.55-72.

Wu, N. Eva (2001*a*). Reliability of fault tolerant control systems: Part I. *IEEE Conference on Decision and Control, Orlando, Florida, USA.*

Wu, N. Eva (2001*b*). Reliability of fault tolerant control systems: Part II. *IEEE Conference on Decision and Control, Orlando, Florida, USA.*

Wu, N. Eva. and Ron J. Patton (2003). Reliability and supervisory control. *IFAC Safeprocess, Washington DC, USA*, pp. 139–144.

Zhang, Y.M. and J. Jiang (2003). Bibliographical review on reconfigurable fault-tolerant control systems. *IFAC Safeprocess, Washington DC, USA*