FAULT TOLERANT CONTROL METHOD BASED ON COST AND RELIABILITY ANALYSIS

F.Guenab, D.Theilliol, P.Weber, J.C.Ponsart and D.Sauter

Centre de Recherche en Automatique de Nancy - CNRS UMR 7039 BP 239 - 54506 Vandoeuvre Cedex - France

E-mail: fateh.guenab@cran.uhp-nancy.fr
Phone: +33 383 684 465 - Fax: +33 383 684 462

Abstract: The aim of Fault Tolerant Control (FTC) is to preserve the ability of the system to reach performances as close as possible to those which were initially assigned to it. The main goal of this paper consists in the development of a FTC strategy, based on both reliability and life cost of components. Once a fault has been detected and isolated and when it is not possible to reach the nominal performances of the system, the reconfiguration task proposed in this paper needs to find all possible structures of system that preserve pre-specified performances, calculate the system reliabilities and costs for all structures and finally search the optimal structure that has a highest reliability and/or a lowest cost. The proposed approach is illustrated through simulations considering a heating system benchmark used in the Intelligent Fault Tolerant Control in Integrated Systems European project (IFATIS EU-IST-2001-32122).

Keywords: Fault Tolerant Control, System Reliability, Cost.

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 those limitations, the modern complex system use a sophisticated controllers which have been developed with fault accommodation and tolerance capabilities, in order to meet increased performance requirements. The Fault Tolerant Control system (FTC) is a control system that maintains current performances closed to desirable ones 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.

Fault Tolerant Control systems are needed in order to preserve the ability of the system to achieve the objectives it has been assigned when faults or failures occurred. Various publications reporting new development in FTC methods have flourished following the overview papers by (Patton, 1997) (Zhang and Jiang, 2003). The use of FTC to increase reliability is an interesting goal; recently some publications have introduced reliability analysis of fault tolerant control (Wu, 2001*a*), (Wu, 2001*b*), (Wu and Patton, 2003) where Markov models are used to estimate the system reliability where it's supposed that the subsystems take two states: intact (available) or failed (unavailable). The main goal of the paper consists in the integration of the components' reliability and the operating cost information, inspired by (Wu *et al.*, 2002) in order to determine an optimal FTC reconfiguration strategy.

As suggested by (Staroswiecki and Gehin, 2001), in a FTC scheme, an optimal structure for the faulty system should be determined to reach the nominal or degraded performances. In this paper, a system is considered as a set of interconnected subsystems, to each subsystem is assigned some local objectives quality production, reliability and cost level. Each subsystem may take several states, the structure of a system defines the set of the used subsystems and information about theirs states and how they are connected. The properties of the used subsystems result in global performances, reliability and cost of the complex system. Once fault is occurred, the faulty subsystems are considered able to achieve new local objectives at different degraded states. New structures of the system can be determined; to each possible structure of the system correspond reliability, cost and global performances computed from its subsystems properties. The reliabilities of different subsystems are computed online taking into account theirs operational modes, i.e. they work continuously or not, and theirs levels of loads. The optimal structure corresponds to the structure that achieves the required global objectives with highest expected reliability under a cost constraint or with lowest expected cost to achieve reliability goal, or at least new redefined global objectives. Once the optimal solution is fixed, a new structure and new control law could be exploited in order to reach the local objectives to get the corresponding global objectives. The paper is organized as follows. Notations are given in Section 2. In Section 3, a general formulation of the problem is presented and a solution is given. A simulation example is given in Section 4 to illustrate the proposed method. Finally, concluding remarks are given in the last section.

2. NOTATIONS

S	Complex System
n	Number of subsystems within the system
S_i	i^{th} subsystem $i = 1 \dots n$
γ_g^n	Nominal global objectives (system in fault free case)
$\gamma_l(S_i)$	Local objectives of subsystem i
λ_i^m	Failure rate of subsystem i
$\mathcal{S}_m$	Structure m. $\mathcal{S}_m = \{S_1^m S_2^m \dots S_{n_m}^m\}$
S_i^m	i^{th} subsystem of structure m
n_m	Number of subsystems used in structure m
M	Number of all possible structures
f_m	function gather equations of structure $\mathcal{S}_m$
$\gamma_l^m(S_i^m)$	Local objectives of i^{th} subsystem used in structure m
$\lambda_l^m(S_i^m)$	Failure rate of i^{th} subsystem used in structure m
$R_i^m(t)$	Reliability of i^{th} subsystem used in structure m, for a given time t
C_i^m	Cost of i^{th} subsystem used in structure m
γ_l^m	Set of local objectives of all subsystems used in structure m
λ_l^m	Set of failure rate of all subsystems used in structure m
γ_g^m	Global objectives of system under structure m
λ_g^m	System failure rate, using structure m
$R_g^m(t)$	Reliability of system using structure m for a given time t
C_g^m	Cost of system using structure m
R_g^*	Reliability constraint limit
C_g^*	Cost constraint limit
c_i	Initial acquisition cost of i^{th} subsystem
P	Failure cost

3. FTC METHOD

3.1 Problem Formulation

As presented in (Staroswiecki and Gehin, 2001), standard control problem is defined by: $< \gamma, \mathcal{S}, \theta, U >$ where:

γ	global objectives
$\mathcal{S}$	structure of system
θ	parameters of closed loop
U	control law

Solving this problem consists in finding a control $u \in U$ so as to achieve the global objective γ under constraints whose structure $\mathcal{S}$ and parameter θ.

In the fault free case the nominal global objectives γ^n are assumed to be achieved under the nominal control u_n and nominal constraint structure $\mathcal{S}_n$. The occurrence of faults can modify the structure $\mathcal{S}_n$, meaning that global objectives can be or not achieved under the new structure.

A new formulation of the problem $< \gamma, \mathcal{S}^*, \theta^*, U^* >$ is proposed, which has a solution and thus allows to achieve γ, by changing the system structure, parameter and control (which result from the disconnection or replacement of faulty components). In some cases, no solution exists, then global objectives must be redefined to degraded ones γ^*.

Under assumptions that there exist several structures $\mathcal{S}_m$ $(m = 1 \dots M)$ which ensure objectives γ (or at least degraded ones γ^*), the question is how to choose the best one in the sense of a given criterion J?

3.2 Problem Solution

Reliability Calculation. 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 data obtained under normal operating conditions (Cox, 1972). The operating conditions represent the operational modes, if components work continuously, or not and theirs levels of the loads (such as power, voltage . . .). In many situations and especially in the considered study, failure rate have to be obtained from components under different levels of loads, because the operating conditions of components change from structure to other.

There exist several models which are basic mathematical models that 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 the considered paper, the failure rate is modeled as follows:

$$\lambda_i(t, x) = \lambda_i(t).g(x, \beta) \qquad (1)$$

With:

$\lambda_i(t)$: baseline failure rate (Nominal Failure rate) function of time only.

$g(x, \beta)$: function (independent of time) incorporates the effects of applied loads.

x: load image.
β: Some component's parameters.

Different definitions of $g(x, \beta)$ can be used. However, the exponential form is mostly used due to its simplicity. Also, the failure rate function for the exponential distribution is constant during the useful life (Cox, 1962), but it changes from operating mode (depending on $\mathcal{S}_m$) to other via load level. The failure rate defined in (1) can be written as:

$$\lambda_i^m(t, x) = \lambda_i(t) e^{x.\beta} \quad (2)$$

It can be noticed that the loads x are considered as constants for the whole structure (or the mean of load), but it changes from structure to other. Once, the new failure rate is calculated, the reliability for a period of time T_d (desired life time) is given by:

$$R_i^m(T_d) = e^{-\lambda_i^m(T_d, x).T_d} \quad (3)$$

The reliability of a complex system is computed from its components or subsystems reliabilities and that depends on the way that the subsystems are connected (serial, parallel ...) (Gertsbakh, 2000) (*chapter I*).
Consider a series system consisting of n subsystems; the system reliability $R_g(T_d)$ is given by:

$$R_g^m(T_d) = \prod_{i=1}^{n} R_i^m(T_d) \quad (4)$$

In the parallel case, the reliability function is as follows:

$$R_g^m(T_d) = 1 - \prod_{i=1}^{n} (1 - R_i^m(T_d)) \quad (5)$$

In the case of mixed structures (serial, parallel ...), the system reliability is computed from the elementary functions (4) and (5). Where $R_i^m(T_d)$ is the i^{th} subsystem reliability used by the structure m, for specified time T_d. In the proposed paper, T_d represents the period between the fault occurrence (new structure is applied) and the reparation of faulty component which caused the structure modification or the end of the system's mission.

Cost Calculation. Let us assumed 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. The objective is to obtain the expected cost of each subsystem as a function of its reliability. Several forms of cost are possible. An expected cost function, similar to the one proposed by (Wu *et al.*, 2002) is used in this paper as follows:

$$C_i^m(R_i^m(T_d)) = \frac{(c_i + P)(1 - R_i^m(T_d))}{\int_0^{T_d} R_i^m(t) dt} \quad (6)$$

where:
c_i i^{th} subsystem initial acquisition cost
P failure cost due to the performance degradation

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 composite system's cost is given by:

$$C_g^m = \sum_i C_i^m(R_i^m(T_d)) \quad (7)$$

The proposed method. Once the fault occurred, the solution can be obtained by enlisting all possible structures $\mathcal{S}_m$ (working mode) that ensure global objectives of system, computing the new failure rates for each subsystem used by the system under the structure $\mathcal{S}_m$ according to the new operating conditions, calculating the reliabilities $R_i^m(T_d)$ and corresponding costs $C_i^m(R_i^m(T_d))$ for a desired life time T_d. System reliability and cost are computed from subsystem's properties.
Then, if the cost is fixed as a constraint, the goal is searching the structure which has the highest reliability and respects the cost limitation. If the reliability is fixed as a constraint the objective is to find the structure that has the lowest cost and respects the reliability limitation. In the case that there is no structure that ensures the global objectives, new set of structures with degraded objectives can be enlisted, and the same procedure must be done to find the optimal structure.

Consider a system composed of n subsystems: S_i with $i = 1 \ldots n$.
Each subsystem has two properties: set of local objective $\gamma_l(S_i)$ and failure rate $\lambda_l(S_i)$.

In normal working mode without faults, a nominal structure is designed from the system which uses all n subsystems and γ_g^n its global objectives called nominal objectives. The global objectives γ_g^n are reached under the local objectives $\gamma_l(S_i)$ of each subsystem.

In faulty cases, assume that there exist M structures $\mathcal{S}_m$, $m = 1 \ldots M$ where each structure $\mathcal{S}_m$ contains n_m subsystems: $\{S_1^m S_2^m \ldots S_{n_m}^m\}$. The main goal of the strategy is to select a structure among M structures which has a high reliability taking into account the cost constraint or a low cost with reliability constraint. The structure must maintain the γ_g^n objectives of the system in the faulty mode or at least degraded objectives γ_g^*. In other way, the goal is to determine which subsystems must be selected to be used in system and in which way they are connected to ensure the global objectives with cost and reliability constraints.
For each structure m:
1. Each subsystem S_i^m has a set of local objectives $\gamma_l^m(S_i^m)$ and a new failure rate λ_i^m computed from its nominal failure rate according to the new applied loads using expression (2).
For a given time T_d, the corresponding reliabilities $R_i^m(T_d)$ and costs $C_i^m(R_i^m(T_d))$ are computed using the expressions (3) and (6) respectively.

2. The set of local objectives γ_l^m of all subsystems used in the structure $\mathcal{S}_m$ is given by the following

equation:

$$\gamma_l^m = \{\gamma_l^m(S_1^m)\ldots\gamma_l^m(S_{n_m}^m)\}$$

Each structure $\mathcal{S}_m$ involves a new set of global objectives γ_g^m given by the following expression:

$$\gamma_g^m = f_m(\gamma_l^m)$$

With f_m gather only the physical equations of the n_m subsystems used in the structure $\mathcal{S}_m$.
Reliability $R_g^m(T_d)$ and cost C_g^m of system for all structures are computed using (4), (5) and (7) based on reliabilities and costs of subsystems.
3. To search the optimal solution, there are two constraints reliability and cost to be considered. If the reliability is chosen as constraint, our interest is to search the structure that has a reliability $R_g^m(T_d) \geq R_g^*$ and lowest cost.

$$C_g^{opt} = \underset{\gamma_g^m \simeq \gamma_g^n, R_g^m(T_d) \geq R_g^*}{min}(C_g^m) \qquad (8)$$

If the cost is chosen as constraint,the solution is given by the structure that has a cost $C_g^m \leq C_g^*$ and the highest reliability.

$$R_g^{opt} = \underset{\gamma_g^m \simeq \gamma_g^n, C_g^m \leq C_g^*}{max}(R_g^m(T_d)) \qquad (9)$$

Since the optimal solution is fixed, a new structure $\mathcal{S}_m$ and new control law U could be exploited in order to reach the local objectives to get the corresponding global objectives and finally this give an answer to the equation exposed in paragraph 3.1.

4. APPLICATION

4.1 Process description

The process, which is proposed as a benchmark for fault tolerant control to IFATIS European project (Leger *et al.*, 2003) is composed of three cylindrical tanks (Figure 1). Two tanks (1 and 2) are used for pre-heating liquids supplied by two pumps driven by DC motors. The liquid temperatures are adjusted in these two tanks by means of two electrical resistors. A third tank makes possible 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 resistors and Q_1, Q_2 the input flow-rates provided by the two pumps. Measurements are liquid temperatures (T_1, T_2, T_3) and liquid levels (H_1, H_2, H_3).

4.2 Control design

The control objectives are to adjust level H_3 and temperature T_3 according to reference values. The reference variables of each sub-system are computed such as the necessary power in the circuit (water and/or temperature) is equitably distributed based on the static parity equation of the system:
$H_j = 0.25(\frac{\alpha_3}{\alpha_j})^2 H_3$ where $j = 1, 2$
$T_1 = (T_2 - T_{2i})(\frac{Q_2}{Q_1}) + T_{1i}$
$T_1 = \frac{T_3(Q_2+Q_3)-(T_{1i}Q_2 - T_{2i}Q_3)}{2Q_2}$
Where T_{1i} and T_{2i} are initial temperatures of water respectively in tank1 and tank2.

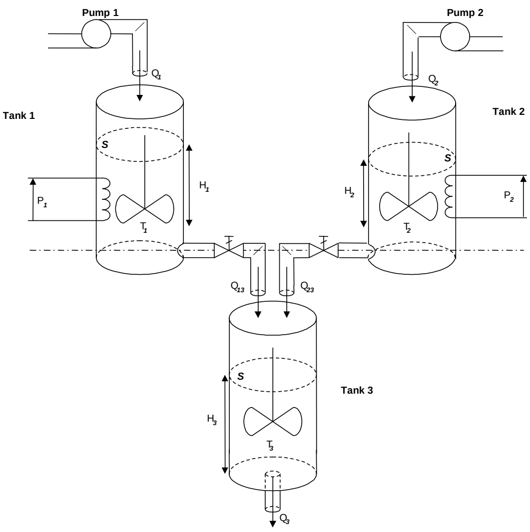

Fig. 1. Schematic of the heating system

4.3 Working Modes

For illustration purposes, a loss of power in the resistor is considered to have occurred on the tank 1. According to reconfigurability analysis of the considered system, nominal (fault free) and faulty working modes (WMs) have been defined off line when a power of β percentage in the resistor of tank 1 is lost. For reasons of computation's complexity of failure rates λ_g^1, λ_g^2 and λ_g^3, reliabilities $R_g^1(T_d)$, $R_g^2(T_d)$ and $R_g^3(T_d)$ and costs C_g^1, C_g^2 and C_g^3, no formula of functions associated to each WMs are given in the paper.

Nominal case or WM_0.
In the fault free case, all subsystems are used. According to the definition in paragraph 3.2.3, the following notation is considered:
$\gamma_g^o = \{H_3 \quad T_3\}$
$\gamma_l^o(S_1^o = Tank_1) = \{H_1 \quad T_1\}$
$\gamma_l^o(S_2^o = Tank_2) = \{H_2 \quad T_2\}$
$\gamma_l^o = \{H_1 \quad T_1 \quad H_2 \quad T_2\}$
$\gamma_g^o = f_o(\gamma_l^o)$
where

$$f_o : \begin{cases} T_3 = \dfrac{T_1\alpha_1\sqrt{H_1} + T_2\alpha_2\sqrt{H_2}}{\alpha_3\sqrt{H_3}} \\ \alpha_3 H_3 = \alpha_1\sqrt{H_1} + \alpha_2\sqrt{H_2} \end{cases}$$

When a fault is detected and isolated on the heating resistor of tank 1, three working modes have been defined.

WM1.
In the first working mode, only tank 2 and tank 3 are considered in the control loop. Tank 1 isn't used, but the global objectives are achieved. Consequently

$\gamma_g^1 = \{H_3 \quad T_3\}$
$\gamma_l^1(S_1^1 = Tank_2) = \{H_2 \quad T_2\}$
$\gamma_l^1 = \{H_2 \quad T_2\}$
$\gamma_g^1 = f_1(\gamma_l^1)$
where

$$f_1 : \begin{cases} T_3 = T_2 \\ \alpha_3 H_3 = \alpha_2 \sqrt{H_2} \end{cases}$$

WM2.
In the second working mode, the tank 1 uses its maximal power of heating resistor $P_1 = \beta * P_{1max}$ and is suppose to achieve the global objectives together with tank 2.

$\gamma_g^2 = \{H_3 \quad T_3\}$
$\gamma_l^2(S_1^2 = Tank_1) = \{H_1 \quad T_1\}$
$\gamma_l^2(S_2^2 = Tank_2) = \{H_2 \quad T_2\}$
$\gamma_l^2 = \{H_1 \quad T_1 \quad H_2 \quad T_2\}$
$\gamma_g^2 = f_2(\gamma_l^2)$
where

$$f_2 : \begin{cases} T_3 = \dfrac{T_1(\beta * P_{1max})\alpha_1\sqrt{H_1} + T_2\alpha_2\sqrt{H_2}}{\alpha_3\sqrt{H_3}} \\ \alpha_3 H_3 = \alpha_1\sqrt{H_1} + \alpha_2\sqrt{H_2} \end{cases}$$

WM3.
For this working mode the degree of freedom to choose the local objectives is unlimited. Effectively, the local objectives are given as follows:

$$H_1 = \sigma_1 H_{1max} \quad \text{with} \quad \sigma_1 \in \left[\frac{H_{1min}}{H_{1max}}, 1\right]$$

$$P_1 = \sigma_2 P_{1max} \quad \text{with} \quad \sigma_2 \in \left[\frac{P_{1min}}{P_{1max}}, 1\right]$$

For each value of H_1 and P_1, the values of H_2 and P_2 are computed based on the desired global objectives H_3 and T_3.The reliabilities and cost of the system for all permitted combination (H_1, H_2, T_1, T_2) are calculated and the local objectives in the $WM3$ are determined.
$\gamma_g^3 = \{H_3 \quad T_3\}$
$\gamma_l^3(S_1^3 = Tank_1) = \{H_1 \quad T_1\}$
$\gamma_l^3(S_2^3 = Tank_2) = \{H_2 \quad T_2\}$
$\gamma_l^3 = \{H_1 \quad T_1 \quad H_2 \quad T_2\}$
$\gamma_g^3 = f_3(\gamma_l^3)$
Where

$$f_3 : \begin{cases} T_3 = \dfrac{T_1\alpha_1\sqrt{H_1} + T_2\alpha_2\sqrt{H_2}}{\alpha_3\sqrt{H_3}} \\ \alpha_3 H_3 = \alpha_1\sqrt{H_1} + \alpha_2\sqrt{H_2} \end{cases}$$

4.4 Optimization

In all faulty working modes, the failure rates of each component are computed taking into account the new load to which the component is submitted, and also the failure rate of system in all working modes. For a desired life time T_d, the reliabilities and costs of each components are computed, and also the global reliability and cost of system.
According to our need, either the reliability of system is fixed and the optimal solution corresponds to the structure which has the lowest cost, or the cost is fixed to a limit value and the optimal solution corresponds to the structure with a highest reliability. In the two cases the global objectives of system must be maintained. If global objectives can't be preserved using inputs' values included in the permitted intervals of inputs (Q_1, Q_2, P_1, P_2), global objectives must be redefined such they can be maintained using a permitted values of inputs and directly the various step point.

4.5 Results and comments

Various scenarios have been considered to illustrate the developed strategy. Nominal failure rates are $\lambda_{Q_1} = 3.77e-6h^{-1}$, $\lambda_{Q_2} = 1.60e-5h^{-1}$, $\lambda_{R_1} = 2.56e-5h^{-1}$ and $\lambda_{R_2} = 2.21e-5h^{-1}$. The acquisition costs are $c_1(Q_1) = 500€$, $c_2(R_1) = 600€$, $c_3(Q_2) = 950€$ $c_4(R_2) = 850€$ and $P = 1000€$.
A loss of power of 3% in resistor is considered to have occurred on the $tank_1$ at time $500s$ and the desired life time is fixed at $T_d = 5000\,hours$.
The first scenario represents the fault free case, where the global objectives are $H_3 = 0.1m$, $T_3 = 23C$.
First scenario (Fault free case). Initial conditions: $H_3 = 0.1$, $T_3 = 21$. Desired references: $H_3 = 0.1$, $T_3 = 23$. Local references $H_1 = 0.2$, $H_2 = 0.2$, $T_1 = 18.5$, $T_2 = 23.5$.

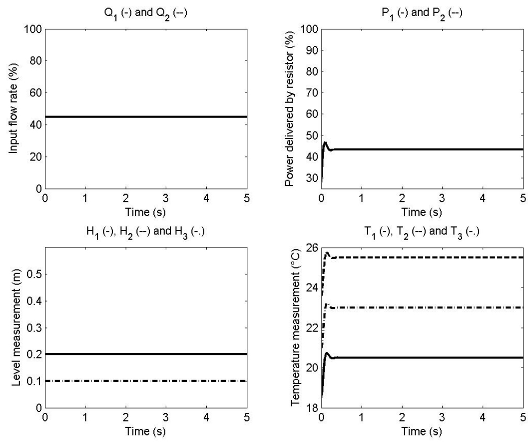

Fig. 2. Dynamic evolution of inputs and outputs variables in fault free case (Time: 1unit=10^3s)

In faulty cases, and for a desired reliability $R^* = 0.67$, the table 1 shows the values of reliabilities and costs of all structures (the given cost is unitary (€/hour)). According to formula (8) the optimal structure is represented by the structure 1 WM_1 (second scenario).

Table 1 reliabilities and costs (second scenario)

Structure 1		Structure 2		Structure 3	
$R_g^1(T_d)$	C_g^1	$R_g^2(T_d)$	C_g^2	$R_g^3(T_d)$	C_g^3
0.67	0.151	0.61	0.176	0.65	0.149

In the third scenario, the global objectives are $H_3 = 0.1m$, $T_3 = 30C$, the fault is occurred but any structure can ensure those objectives then they are redefined by the human operator to $H_3 = 0.1m$, $T_3 = 26.4C$. if the desired reliability is $R^* = 0.38$ the results are given in table 2 and figure 4. The optimal structure is the WM_3.

Table 2 reliabilities and costs (third scenario)

Structure 1		Structure 2		Structure 3	
$R_g^1(T_d)$	C_g^1	$R_g^2(T_d)$	C_g^2	$R_g^3(T_d)$	C_g^3
0.33	0.416	0.24	0.523	0.38	0.349

Second scenario. Desired references are $H_3 = 0.1$ and $T_3 = 23$. The fault is not affected global references. Following the proposed strategy, the first structure is selected according to minimal cost that ensures the reliability requirements. Global references are preserved with the following local references $H_1 = 0$, $H_2 = 0.8$, $T_1 = 0$, $T_2 = 23$. These references must be distinguished from the nominal ones.

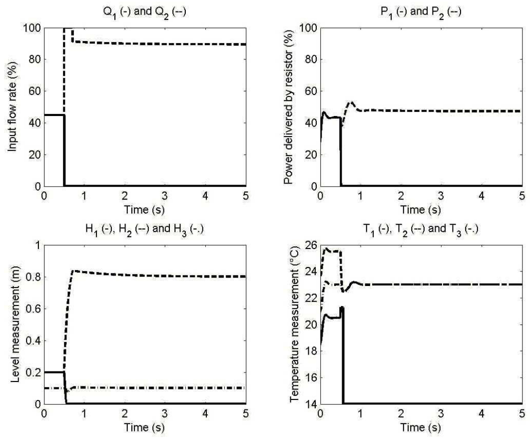

Fig. 3. Dynamic evolution of inputs and outputs variables in faulty case on heating circuit of tank1

Third scenario. Desired references are $H_3 = 0.1$ and $T_3 = 30$. The third structure is selected according to minimal optimization cost that ensures the reliability requirements $R_g^m(T_d) \geq 0.38$.

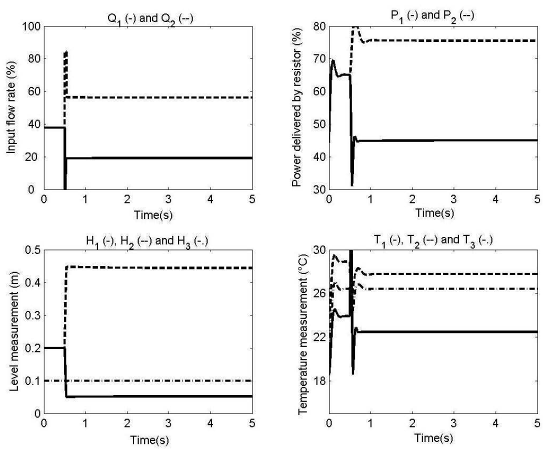

Fig. 4. Dynamic evolution of inputs and outputs variables in faulty case on heating circuit of tank1

5. CONCLUSION

This paper presents a FTC strategy, to find a new control structure for the plant, when a fault has occurred. Where either system reliability is maximized with acceptable system cost or overall system cost is minimized with a desired reliability. Once fault occurred and the global objectives of system can not be achieved using the actual structure, the proposed strategy has to switch to another structure which ensures the objectives of the system as longer as possible, or at least redefined degraded objectives, with a limiting cost. Our approach is based on the analysis of reliability and cost of the system which are computed from different reliabilities and costs of its components at a given time taking into account theirs operating conditions. Further research should be concentrated in obtaining cost-reliability functions easy to use, taking into account maintenance (cost of maintenance, cost of the new components, cost of intervention and cost of failures' consequences).

REFERENCES

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

Cox, D.R. (1972). Regression models and life tables. *J R Stat Soc B1972;34:187-220.*

Finkelstein, M. S. (1999). A note on some aging properties of the accelerated life model. *Reliability Engineering and System Safety, Volume 71, Issue 1* pp. 109–112.

Gertsbakh, I. (2000). *Reliability Theory with Applications to Preventive Maintenance.* Springer.

Leger, S., F. Hamelin and D. Sauter (2003). Fault detection and isolation dynamic systems using principal component analysis-application to a heating system benchmark. *Safeprocess'03 IFAC Symposium, Washington, USA,* pp. 543–547.

Martorell, S., A. Sanchez and V. Serradell (1999). Age-dependent reliability model considering effects of maintenance and working conditions. *Reliability Engineering and System Safety,Volume 64, Issue 1* pp. 19–31.

Mettas, A. (2000). Reliability allocation and optimization for complex systems. *Reliability and Maintainability Symposium* pp. 216–221.

Patton, R. (1997). Fault-tolerant control: the 1997 situation. *Proceedings of Safeprocess'97, (Hull - England), IFAC* pp. 1033–1055.

Staroswiecki, M. and A.L Gehin (2001). From control to supervision. *IFAC/Safeprocess'2000 Symp. on Fault Detection, Supervision and Safety for Technical Processes, Budapest (Hongrie).*

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

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

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

Wu, N.Eva., X. Wang, M. Smapath and G. Kott (2002). An operational approach to buget-constrainted reliability allocation. 15^{th} *IFAC World Congress, Barcelona, Spain* pp. 199–204.

Zhang, Y. and J. Jiang (2003). Bibliographical review on reconfigurable fault tolerant control systems. *Proceedings of Safeprocess'03, Washington, USA, IFAC* pp. 1033–1055.