Int. J. Appl. Math. Comput. Sci., 2011, Vol. 21, No. 3, 431–439
DOI: 10.2478/v10006-011-0032-z

amcs

RECONFIGURABILITY ANALYSIS FOR RELIABLE FAULT–TOLERANT CONTROL DESIGN

AHMED KHELASSI, DIDIER THEILLIOL, PHILIPPE WEBER

Research Centre for Automatic Control of Nancy (CRAN), CNRS UMR 7039
Nancy University, BP 70239, 54506 Vandœuvre Cedex, France
e-mail: ahmed.khelassi@cran.uhp-nancy.fr

In this paper the integration of reliability evaluation in reconfigurability analysis of a fault-tolerant control system is considered. The aim of this work is to contribute to reliable fault-tolerant control design. The admissibility of control reconfigurability is analyzed with respect to reliability requirements. This analysis shows the relationship between reliability and control reconfigurability defined generally through Gramian controllability. An admissible solution for reconfigurability is proposed according to reliability evaluation based on energy consumption under degraded functional conditions. The proposed study is illustrated with a flight control application.

Keywords: fault-tolerant control system, reconfigurability, reliability, actuator faults.

1. Introduction

Manufacturing systems consist of many different components, which ensure their operation and high-quality production. In order to fulfil the growing of economic demands for high plant availability and system safety, dependability is becoming an essential need in industrial automation. In this context, in order to satisfy these requirements, Fault-Tolerant Control (FTC) is introduced. The aim of FTC systems is to keep a plant available by the ability to achieve the objectives that have been assigned to the system in faulty behavior and accept reduced performances when critical faults occur (Blanke *et al*., 2006). Thus, increasing systems autonomy involves the capability to compensate the impact of component faults and to keep the system available as long as possible. Within this framework, the main goal of FTC is to improve the reliability of the system, which is rarely associated with an objective criterion that guides design (Li *et al*., 2007).

However, it is difficult to establish a functional linkage between the overall system reliability and the control performance requirement.

In active fault-tolerant control, information obtained from fault diagnosis is considered in controller redesign (Noura *et al*., 2009). In fact, process diagnosis should not only indicate fault occurrence but also identify fault location and magnitudes (Tharrault *et al*., 2008). This assumption will make controller re-design possible. After fault occurrence, fault accommodation can be a solution to maintain the performance requirements by adapting the controller parameters (Marusak and Tatjewski, 2008), or by the generation of an additional control law (Blanke *et al*., 2001). Moreover, if fault accommodation cannot be achieved, a complete control loop has to be reconfigured. Then, a new control law has to be designed and the controller structure has to be changed (Zhang and Jiang, 2008). After reconfiguration, the original control objectives are achieved, although degraded performances can be accepted.

Still, the study of the system property is necessary to determine which failure modes could severely affect plant dependability. Only few attempts are focused on fundamental FTC property analysis, where some studies are often defined as fault detectability and fault isolability (Patton, 1997). The concept of reconfigurability was introduced as control system quality under given faulty conditions. In fact, introduced by Moore (1981), the second order mode has been proposed as a reconfigurability measure (Wu *et al*., 2000). LTI system reconfigurability can be also evaluated using the controllability and observability Gramians (Frei *et al*., 1999). In the work of Staroswiecki (2002), performance-based control reconfigurability is evaluated as the ability of the system considered to keep or recover some admissible performances when a fault occurs. Moreover, reconfigurability evaluation is proposed for a general quadratic control problem

by Staroswiecki (2003). Yang (2006) shows that the reconfigurability measure can be viewed as an intrinsic reconfigurability property or as reconfigurability property performance. All these approaches have been considered off-line. Gonzalez-Contreras *et al*. (2009) have recently introduced on-line reconfigurability analysis by using input/output data.

This work contributes to reliable fault-tolerant control systems design which achieves the control objective after fault occurrence with high overall system reliability. Indeed, in order to improve system dependability, reliability analysis is considered to establish an admissible solution of reconfigurability based on the required energy consumption.

This paper is organized as follows. Section 2 formulates the fault-tolerant control problem and defines the reconfigurability concept for actuator faults. Admissibility for fault tolerance is defined according to the energy limitation. In Section 3, reliability estimation in degraded functional conditions is introduced. The impact of actuator faults on reliability is illustrated in order to include the reliability requirements in the reconfigurability problem. A solution for the reconfigurability limit under reliability requirements is proposed to evaluate the ability of the reconfigurable system to recover the encountered faults until the end of the mission. Section 4 is devoted to illustrate this analysis based on an aircraft application. Finally, conclusions are given in the last section.

2. Description of the control reconfigurability problem

2.1. Problem statement. Consider a system in a fault-free case modeled by a linear state-space representation:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t), \\ y(t) = Cx(t), \end{cases} \tag{1}$$

with the state vector $x(t) \in \mathbb{R}^n$, the control vector $u(t) \in \mathbb{R}^m$, the output vector $y(t) \in \mathbb{R}^r$ and matrices $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times m}, C \in \mathbb{R}^{r\times n}$.

Actuator faults can be defined as any abnormal operations in the control effectors such that the controller outputs cannot be delivered to the manipulated variables entirely. After actuator fault occurrence at $t = t_f$, the control law applied to the plant is interrupted or modified. In this study, the loss of effectiveness control is considered and the system (1) can be represented in the faulty case as follows (Khelassi *et al*., 2010):

$$\begin{cases} \dot{x}(t) = Ax(t) + B_f u(t), \\ y(t) = Cx(t), \end{cases} \tag{2}$$

where the control matrix B_f can be written in relation to the nominal control input matrix B and the control effectiveness factors γ^i, $i = 1, \ldots, m$, as

$$B_f = B(I_m - \Gamma), \quad \Gamma = \begin{pmatrix} \gamma_1 & & & 0 \\ & \gamma_2 & & \\ & & \ddots & \\ 0 & & & \gamma_m \end{pmatrix},$$

with $\gamma_i \in [0 \;\; 1]$. In fact, $\gamma_i = 0$ denotes the healthy i-th control actuator. Nevertheless, when $0 < \gamma_i < 1$, the fault considered is a partial loss in control effectiveness. Moreover, when $\gamma_i = 1$, a failure is considered and the i-th actuator is out of order.

Indeed, the reconfigurability property can be discussed as the ability of the system considered to recover some admissible performances taking into account fault occurrence. According to Yang (2006), reconfigurability can be defined as follows.

Definition 1. The system (1) is called (*completely*) *reconfigurable* if and only if the controllability property of the nominal system is kept by the faulty system.

For an LTI system, reconfigurability evaluation is based on the limitation of energy consumption, which defines an admissible solution in the degraded functional (Staroswiecki, 2002). It can be checked through the controllability Gramian of the system. However, to ensure fault recovery until the end of the mission, fault tolerance evaluation related to actuator reliability can be introduced. In this context, reconfigurability analysis for reliable fault-tolerant control design can be defined based on energy limitation, according to the reliability requirement.

2.2. Reconfigurability based on the controllability Gramian. As proposed by Staroswiecki (2002) and for control reconfigurability analysis, the controllability Gramian appears to be useful in reference to the following: (i) to guarantee the controllability condition of the system proving the existence of a solution; (ii) there exists at least one admissible solution, with respect to some specific energy limitations, taking the system state from $x(0) = x_0 \in \mathbb{R}^n$ to the origin $x(\infty) = 0$.

This problem involves the minimization of the energy consumed by the system. The criterion used is represented as follows.

Criterion 1. Minimize the functional

$$\mathcal{J}(u, x_0) = \int_0^\infty \|u(t)\|^2 \, \mathrm{d}t, \tag{3}$$

to transfer $x(0) = x_0$ to $x(\infty) = 0$, where $x_0 \in \mathbb{R}^n$, and $x(\infty)$ stands for $\lim_{t\to\infty} x(t)$. where $\|\cdot\|$ is the Euclidian norm. Other criteria could be used (see Staroswiecki, 2003).

For the LTI system (1), the solution of (3) is obtained by the Hamiltonian equation from optimal control theory,

$$u(t) = B^T P x(t), \tag{4}$$

where P is the unique solution of the Lyapunov equation defined as

$$A^T P + PA = -BB^T. \tag{5}$$

For the criterion (3), the matrix P^{-1} is the controllability Gramian W_c of the control law $u(t)$. In fact, W_c defines energy consumption required to transfer the system state to the origin. Moreover, W_c is invertible since the pair (A, B) is controllable, defined analytically as follows:

$$W_c = \int_0^\infty e^{At} B B^T e^{A^T t} \mathrm{d}t. \tag{6}$$

The optimal value of the criterion (3) is obtained on $[0, \infty)$ from optimal control theory as follows:

$$\mathcal{J}(x_0) = x_0^T W_c^{-1} x_0. \tag{7}$$

As illustrated by Staroswiecki (2002), Eqn. (7) shows that the actuator performance depends on the control objective x_0. However, actuator performance can be characterized independently of the control objective, which leads to the worst energetic control problem: Transfer the system state $x(0) = x^*$ to $x(\infty) = 0$ where

$$x^* = \arg\max \mathcal{J}(x_0), \tag{8}$$

and the actuator performance is thus evaluated according to the maximum eigenvalue of the matrix W_c^{-1} interpreted as the maximum energy which might be required to transfer the system $x(0) = x^*$ to the origin. The minimum cost associated with (1) in this case can be defined as

$$\mathcal{J}^* = \mathcal{J}(x^*) = \max(\Lambda(W_c^{-1})), \tag{9}$$

where $\Lambda(W_c^{-1})$ is the set of the eigenvalues of W_c^{-1}.

Fault reconfiguration strategies consider the control problem associated with the faulty system. In the degraded functional and for FTC design, the constraint (1) being replaced by the constraint (2) from $t = t_f$,

$$\begin{array}{ll} \dot{x}(t) = Ax(t) + Bu(t), & t \in [0, t_f), \\ \dot{x}(t) = Ax(t) + B_f u(t), & t \in [t_f, \infty). \end{array} \tag{10}$$

Let $\mathcal{J}_f(x_0)$ be the minimum cost of the criterion (3) associated with (10), where the initial condition $x_f = x(t_f)$ is considered on the interval $[t_f, \infty)$. From Bellman's optimality principle, the minimum cost $\mathcal{J}_f(x_0)$ can be obtained in a degraded mode according to the control effectiveness factors γ as

$$\mathcal{J}_f(x_0) = \mathcal{J}_{0f} + x_f^T W_c(\gamma)^{-1} x_f, \tag{11}$$

where $\mathcal{J}_{0f}$ is the cost already spent between $t = 0$ and $t = t_f$. $W_c(\gamma)$ is the solution of the following Riccati equation:

$$AW_c(\gamma) + W_c(\gamma)A^T = -B_f(\gamma)B_f^T(\gamma). \tag{12}$$

In fact, $W_c(\gamma)$ is an invertible and positive matrix, since the pair $(A, B_f(\gamma))$ is kept controllable. The value of $\mathcal{J}_{0f}$ can be expressed as

$$\mathcal{J}_{0f} = \mathcal{J}(x_0) - x_f^T W_c^{-1} x_f. \tag{13}$$

Therefore, the cost associated with the accommodated system can be obtained from (7) and (13) according to the initial conditions as follows:

$$\mathcal{J}_f(x_0) = x_0^T W_c^{-1} x_0^T + x_f^T (W_c(\gamma)^{-1} - W_c^{-1}) x_f. \tag{14}$$

Indeed, for $t_f = \infty$, which defines the lack of occurrence of faults, the associated cost is equal to the nominal case, $x_0^T W_c^{-1} x_0$. However, for $t_f = 0$, fault occurrence is considered when the system is started, and the cost in this case is $x_f^T W_c^{-1}(\gamma) x_f$.

According to Staroswiecki (2002), fault tolerance can be evaluated as follows.

Definition 2. The system is *fault tolerant* with respect to the fault occurring at time $t = t_f$ for the control objective x_0 if and only if the accommodation or the reconfiguration problem has an admissible solution.

Definition 3. In the degraded mode, the solution to the FTC problem is admissible with respect to the control objective x_0 if and only if

$$\mathcal{J}_f(x_0) \leq \mathcal{J}_{\mathrm{pth}}, \tag{15}$$

where $\mathcal{J}_{\mathrm{pth}}$ is a predefined cost corresponding to the worst acceptable degraded mode.

Indeed, admissibility depends on the time of fault occurrence. Since t_f is obviously unknown beforehand, it can only be checked on-line when a fault is detected and isolated. Therefore, it is interesting to look for sufficient conditions which could be checked off-line. Indeed, the control objective can be reached by an admissible solution using the faulty system from the beginning by considering the worst case value of x_f in the previous conditions (Staroswiecki, 2003). The worst case situation is that in which the fault occurrence time is $t_f = 0$. Therefore, $x_f = x_0$ and fault tolerance can be evaluated based on the following indicator:

$$\sigma(\gamma) = \max \Lambda(W_c^{-1}(\gamma)), \tag{16}$$

where $\Lambda(W_c^{-1})$ is the set of the eigenvalues of W_c^{-1}.

Remark 1. The actuator performances can be characterized independently of the control objective by the maximum eigenvalue of $W_c^{-1}(\gamma)$, which is interpreted as the maximum energy required to transfer the system state to the origin. This energy value corresponds to the worst case, which can occur in a given degraded mode.

An index of reconfigurability based on the maximum required energy (16) is proposed by normalization as illustrated by Khelassi *et al*. (2009). Fault tolerance is evaluated by means of the energy cost corresponding to the worst situation in which the system is still controllable for an admissible solution:

$$\rho(\gamma) = \frac{\sigma(\gamma) - \sigma_{\min}}{\sigma_{\max} - \sigma_{\min}}, \tag{17}$$

where $\sigma_{\max}$ is the maximum required energy of the worst degraded functional condition, $\sigma_{\min}$ is the maximum required energy consumed in the nominal situation $\gamma = 0$. Due to the normalization of the energetic indicator (16), the values of the index (17) vary between 0 and 100%. The index (17) can be interpreted as an image of system behavior degradation in terms of energy.

Lemma 1. *In the degraded mode, the solution of the FTC problem is admissible with respect to a control objective if*

$$\rho(\gamma) \leq \rho_{\text{pth}}, \tag{18}$$

where ρ_{pth} is a predefined energetic threshold, which represents the acceptable degraded functional mode when a control solution is found. The value of ρ_{pth} corresponds to an admissible required energy.

Remark 2. The set of admissible solutions which satisfy the relation (18) is established in order to guide the design of a fault tolerant control system. However, the problem is how define the value of the threshold ρ_{pth} based on specified requirements.

In the following section, a solution of the admissibility problem based on the reliability requirement is proposed.

3. Reconfigurability based on reliability analysis

As presented previously, reconfigurability based on the controllability Gramian is applied to evaluate the system performances, which can be achieved by a fault-tolerant control scheme. To improve system dependability, it is crucial to ensure that the reconfigured system can provide the energy required to achieve the control objective until the end of the mission.

Proposition 1. *The mean operating time of the system can be estimated by a reliability measure. For reliable-fault-tolerant control design, the problem (3) can be reformulated as an energetic minimization problem with respect to a reliability requirement such that*

$$J(x_0) = \int_0^\infty \|u(t)\|^2 \, \mathrm{d}t, \tag{19a}$$

subject to

$$R(t) \geq R_{\text{pth}}, \tag{19b}$$

where $R(t)$ is the overall system reliability; R_{pth} is a predefined threshold, which defines the minimal value of the acceptable reliability value in the degraded mode.

The aim of this section is to establish a solution for choosing the admissibility threshold ρ_{pth} based on reliability analysis. In fact, ρ_{pth} is the normalization of a predefined energetic threshold σ_{pth} required to define the acceptable degraded modes which can be tolerated for reliable design.

3.1. Reliability computation.

Definition 4. *Reliability* is defined as the probability that units, components, equipment and systems will accomplish their intended function for a specified period of time under some stated conditions and in specific environments (Gertsbakh, 2000).

In this study, an exponential distribution is considered to model reliability. In fact, reliability evolution is characterized by a given failure rate. Thus, failure rates are obtained from components under different levels of loads. Several mathematical models have been developed to define the load function in order to estimate the failure rate λ (Martorell *et al*., 2009). Among them, the proportional hazard model introduced by Cox (1972) is used in this paper.

Definition 5. The *failure rate* is modeled as follows:

$$\lambda_i = \lambda_i^0 \times g(\ell, \vartheta), \tag{20}$$

where λ_i^0 is the baseline failure rate (nominal failure rate) for the i-th subsystem or component and $g(\ell, \vartheta)$ is a function (independent of time) which models the effects of the employed load on component health. Here ℓ corresponds to the load and ϑ represents some component parameters.

Different definitions of $g(\ell, \vartheta)$ exist in the literature. However, the exponential form, assumed to be related directly to the control input, is commonly used in actuator reliability evaluation. For the nominal functional conditions, Eqn. (20) can be written as follows:

$$\lambda_i = \lambda_i^0 \times e^{\alpha u_{\text{nom}}^i}, \tag{21}$$

where α is a fixed factor depending on the actuator property, u_{nom}^i is the nominal control law delivered by the i-th actuator in the fault-free case to achieve the control objective. Thus, actuator reliability can be evaluated as follows:

$$R_i(t) = e^{-\lambda_i t}. \tag{22}$$

3.2. Reliability evaluation under degraded functional conditions. As explained by Guenab *et al*. (2006), the estimated value of the failure rate changes according to the increase of control input. However, even when actuator faults occur, the control law is modified in order to recover the impact of a fault on system behavior. Thus, the energy required to tolerate the fault increases, and a new failure rate which characterizes actuator reliability degradation and the load can be estimated. In fact, the relationship between the required energy in degraded modes and reliability evolution can be established. Let the linearized dynamics of the normal system at a trim condition be given by (1). Suppose now that one or more actuators are suddenly damaged or experience a partial loss of their control effectiveness (2). Then the system dynamics can be expressed by

$$\dot{y} = C\dot{x} = CAx + CB_f u. \tag{23}$$

At the current state $x(t)$, suppose that the reference baseline system control law for the desired behavior would produce input $u_{\rm nom}$ if all of the control actuators were healthy. Then the desired rate of the controlled output would be

$$\dot{y}_{\rm nom} = C\dot{x} = CAx + CBu_{\rm nom}. \tag{24}$$

FTC seeks an input control u that makes the right-hand side of (23) as close as possible to that of (24), that is,

$$Bu_{\rm nom} = B_f u, \tag{25}$$

where, consequently, y will remain close to $y_{\rm nom}$ for

$$u = (I - \Gamma)^{-1} u_{\rm nom}. \tag{26}$$

Therefore, based on (21) and (26), the failure rate and the reliability of the actuator under degraded functional conditions can be established according to the loss of effectiveness factors γ_i and $u^i_{\rm nom}$ as follows:

$$\lambda_i(\gamma) = \lambda_i^0 e^{(1-\gamma_i)^{-1}\alpha u^i_{\rm nom}}, \tag{27}$$

$$R_i(t,\gamma) = e^{-\lambda_i(\gamma)t}. \tag{28}$$

The overall system reliability depends on the way in which their components and subsystems are connected. In this context, for a system with q series sub systems, reliability is given by

$$R_g(t) = \prod_{i=1}^{q} R_i(t,\gamma), \tag{29}$$

and with q parallel subsystems it is calculated as follows:

$$R_g(t) = 1 - \prod_{i=1}^{q} (1 - R_i(t,\gamma)), \tag{30}$$

The reliability of complex systems is computed from a combination of the elementary functions (29) and (30).

Lemma 2. *In degraded functional conditions, the overall system reliability can be characterized by a baseline failure rate and the loss of effectiveness factors which give an image of the mean operating time of the reconfigured system.*

3.3. Reconfigurability with respect to reliability requirements. For reliable fault-tolerant control design, the admissible required energy corresponding to the acceptable degraded modes (18) is defined based on reliability evaluation. The reconfigurable reliable system achieves the control objective until the end of the mission with a high probability.

Definition 6. The system is *fault tolerant and reliable* with respect to the fault occurring at time $t = t_f$ for the control objective x_0 if the accommodation or the reconfiguration problem has an admissible solution with respect to the reliability requirement.

Lemma 3. *For the exponential distribution, the reliability constraint $R(t) \geq R_{\rm pth}$ is satisfied for every t during the mission, if the constraint is satisfied* a priori *at the end of the mission $t = t_m$.*

In order to compute the value of the admissible energy required under degraded functional conditions $\sigma_{\rm pth}$, we define the set of the acceptable degraded functional modes as follows:

$$\gamma^* = \{\gamma \in \mathbb{R}^m,\ \ R(t_m,\gamma) \geq R_{\rm pth}\}, \tag{31}$$

where γ^* is the set of effectiveness factors corresponding to degraded functional conditions which respect the reliability requirements. Based on (31) and (18), reliable fault-tolerant control design is available for an admissible solution defined by the required energy of the worst acceptable degraded case $\sigma_{\rm pth}$, corresponding to the maximum energy required for γ^*.

Definition 7. In degraded functional conditions, the solution of a reliable fault-tolerant control problem is *admissible with respect to a control objective* if

$$\rho(\gamma) \leq \rho_{\rm pth}, \tag{32}$$

where

$$\rho_{\rm pth} = \frac{\sigma_{\rm pth} - \sigma_{\min}}{\sigma_{\max} - \sigma_{\min}} \tag{33}$$

and

$$\sigma_{\rm pth} = \max(\sigma(\gamma^*)). \tag{34}$$

In fact, the indicator (33) is a reconfigurability index for reliable fault-tolerant control design, found based on energy with respect to reliability requirements.

4. Aircraft simulation example

To illustrate the different steps of the proposed approach, the model of an aircraft simulation used by Wu *et al.* (2000) is proposed. The plant model has two inputs (elevon command and canard command) and two outputs (angle of attack, pitch rate and pitch angle). This example is considered with two actuators in order to simplify the illustration of results. The values of the nominal failure rates associated to the actuators are presented in Table 1.

Table 1. Failure rates of elementary components.

Baseline failure rates	
λ_1^0	$9 \cdot 10^{-6}\,\mathrm{h}^{-1}$
λ_2^0	$5 \cdot 10^{-6}\,\mathrm{h}^{-1}$

The control objectives were originally specified on vertical transition, pitch pointing and direct lift. Around an operating point, the state-space description of the plant model is given by (1) with

$$A = \begin{bmatrix} -0.0226 & -36.6 & -18.9 & -32.1 \\ 0 & -1.9 & 0.983 & 0 \\ 0.0123 & -11.7 & -2.63 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 & 0 \\ -0.414 & 0 \\ -77.8 & 22.4 \\ 0 & 0 \end{bmatrix},$$

$$C = \begin{bmatrix} 0 & 5.73 & 0 & 0 \\ 0 & 0 & 0 & 5.73 \end{bmatrix}.$$

The factors γ_1 and γ_2 of the actuator loss of effectiveness are introduced for each column of B by (2). The elevons are regarded as the primary control effectors, and the canards as the secondary, which could also produce secondary effects to the vehicle's lateral and directional motion when used differentially. First, the controllability Gramian is calculated by using the Lyapunov equation (12) for each degraded state, which is defined according to the different values of (γ_1, γ_2) with $0 \leq \gamma_i < 1$. In order to study the control reconfigurability of the plant, the index based on the normalization of energy consumption is calculated from (17). After reliability evaluation, this index is compared with the energy threshold ρ_{pth} found according to (33), which defines the worst acceptable degraded performance. Indeed, for this application, the overall system reliability is evaluated for each degraded functional mode according to (30). The failures rate are obtained according to (27).

The predefined reliability threshold $R_{\mathrm{pth}} = 95\%$ is fixed for this application. This value means that, after fault occurrence and for all reconfigurable degraded states, the probability that the system accomplishes the control objective until the end of the mission t_m should be higher than 0.95. The mission duration is considered for $t_m = 600$ min.

Figure 1 shows the evaluation of the overall system reliability $Rg(t_m)$ under degraded conditions, where the x and y axes represent respectively the studied actuators loss of effectiveness (γ_1, γ_2). In fact, the overall system reliability in each degraded mode (defined according to (γ_1, γ_2)) is compared with the reliability threshold R_{pth} which should be fulfilled after reconfiguration.

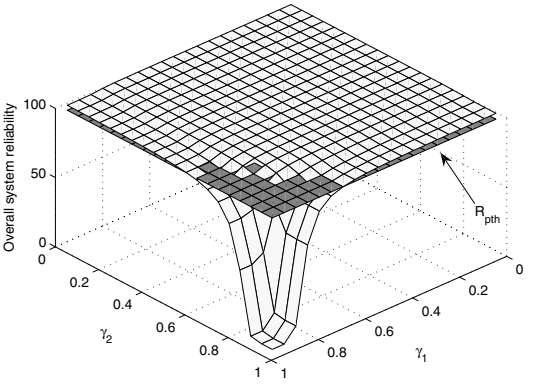

Fig. 1. Reliability evaluation at the end of the mission.

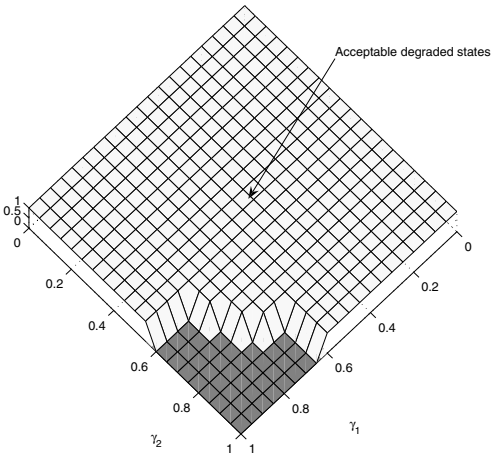

Fig. 2. Acceptable degraded states based on reliability evaluation.

The comparison of the overall system reliability and R_{pth} is shown in Fig. 2 where the result defines the set of the acceptable degraded states γ^*. Unity is assigned to the degraded modes that satisfy the reliability requirements and are considered as able to be tolerated if the required energy is admissible (31).

According to (34), the admissible required energy σ_{pth} which defines the maximum acceptable cost for reli-

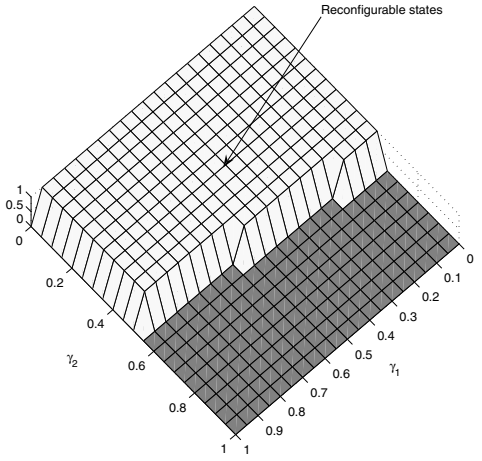

Fig. 3. Control reconfigurability based on energy with respect to reliability requirements.

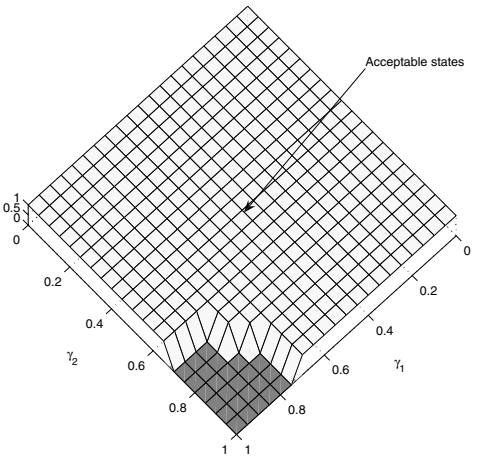

Fig. 4. Acceptable degraded states based on reliability evaluation.

able fault-tolerant control design can be found. By normalization, the reconfigurability index (33) and the energetic threshold $\rho_{\rm pth}$ are obtained. The acceptable degraded modes can be found according to (32). In fact, Fig. 3 shows the reconfigurable modes found according to admissibility solution (32) and the evaluation of the proposed reconfigurability index. Unity is assigned to the set of the reconfigurable states under degraded functional conditions defined according to the actuator loss of effectiveness (γ_1, γ_2).

These results show the advantage of integrating reliability analysis for reliable fault-tolerant control design. In fact, as can be shown, the maximum energy required to both tolerate actuator faults and achieve the control objective until the end of the mission with a high probability can established by using reliability analysis. For reliable fault-tolerant control design, the reconfigurable modes considered, which comply with the obtained energy threshold, minimize the energy consumption under degraded functional conditions and maintain the control objective until the predefined final time of the mission. All these admissible states minimize energy consumption and guarantee that the overall system reliability is above $R_{\rm pth}$.

However, since reliability is a probability measure in time, we evaluate the ability of reliable fault-tolerant control system design for different mission durations. The impact of time on actuator degradation can be shown for $t_m = 300$ min in Fig. 4. The acceptable degraded modes (31) which respect the reliability requirements are wider than in the previous scenario. Unity is assigned to the set γ^*. In fact, for a small mission period, the actuator degrades less rapidly and the set of the acceptable degraded modes is more extensive. By evaluation of the reconfigurability index (17) compared with (33), the corresponding reconfigurable modes are shown in Fig. 5. For this scenario, the proposed reliable fault-tolerant control design is able to tolerate more severe faults under more severe degraded conditions compared with the first scenario.

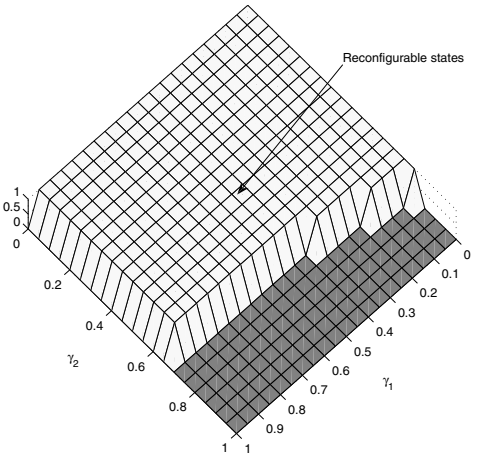

Fig. 5. Control reconfigurability for $t_m = 300$ min.

5. Conclusion

A reconfigurability index based on energy consumption with respect to reliability requirements has been proposed in this paper. The results obtained in this study prove that the solution for the admissibility of reliable design can be established by using overall system reliability evaluation, in addition to the energy criterion. Indeed, an admissible solution for control reconfigurability based on reliability analysis is proposed. This relation characterizes those states that are reachable (by acceptable degraded func-

tional conditions) in terms of energy consumption. For the proposed approach, on-line reliability computation of the system is not necessary. However, for an admissible solution characterized by the proposed reconfigurability index, the decision on reconfiguration can be made on-line.

In fact, the obtained results represent the data base of reconfigurable degraded functional modes for reliable fault-tolerant control design which can be checked and verified on-line. Moreover, it would be interesting as a future work to study system reconfigurability by evaluating the overall system reliability analytically. The aim is to guarantee the control objectives after a fault occurrence by energy minimization until the end of the mission with a high probability.

References

Blanke, M., Kinnaert, M., Lunze, J. and Staroswiecki, M. (2006). *Diagnosis and Fault Tolerant Control*, Control Systems, Vol. 2, Springer-Verlag, London.

Blanke, M., Staroswiecki, M. and Wu, E. (2001). Concepts and method in fault-tolerant control, *Proceedings of the American Control Conference, ACC 2001 Arlington, VA, USA,* Vol. 4, pp. 2606–2620.

Cox, D. (1972). Regression models and life tables, *Journal of the Royal Statistical Society* **34**(2): 187–220.

Frei, C., Karus, F. and Blanke, M. (1999). Recoverability viewed as a system property, *Proceedings of the European Control Conference, IEEE ECC'99, Budapest, Hungary*.

Gertsbakh, I. (2000). *Reliability Theory with Applications to Preventive Maintenance*, Springer-Verlag, Berlin/Heidelberg.

Gonzalez-Contreras, B., Theilliol, D. and Sauter, D. (2009). Online reconfigurability evaluation for actuator faults using input/output data, *7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Barcelona, Spain*, pp. 674–679.

Guenab, F., Theilliol, D., Weber, P., Zhang, Y. and Sauter, D. (2006). Fault tolerant control design: A reconfiguration strategy based on reliability analysis under dynamic behavior constraints, *Prococeedings of the 6th IFAC SAFEPROCESS'06, Beijing, China*, pp. 1387–1392.

Khelassi, A., Theilliol, D. and Weber, P. (2009). Reconfigurability for reliable fault-tolerant control design, *7th Workshop on Advanced Control and Diagnosis, ACD'09, Zielona Góra, Poland*.

Khelassi, A., Weber, P. and Theilliol, D. (2010). Reconfigurable control design for over-actuated systems based on reliability indicators, *Proceedings of the Conference on Control and Fault-Tolerant Systems, IEEE SysTol 2010, Nice, France*, pp. 365–370.

Li, H., Zhao, Q. and Yang, Z. (2007). Reliability modeling of fault tolerant control systems, *International Journal of Applied Mathematics and Computer Science* **17**(4): 491–504, DOI: 10.2478/v10006-007-0041-0.

Martorell, S., Sanchez, A. and Serradell, V. (2009). Age-dependent reliability model considering effects of maintenance and working conditions, *Reliability Engineering and System Safety* **64**(1): 19–31.

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

Moore, B. (1981). Principal component analysis in linear systems: controllability observability and momdel reduction, *IEEE Transactions on Automatic Control* **26**(1): 17–32.

Noura, H., Theilliol, D., Ponsart, J. and Chamssedine, A. (2009). *Fault Tolerant Control Systems: Design and Practical Application*, Springer, Dordrecht/Heidelberg/London.

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

Staroswiecki, M. (2002). On reconfigurability with respect to actuator failures, *Proceedings of the 15th IFAC World Congress, IFAC 2002, Barcelona, Spain*, pp. 775–780.

Staroswiecki, M. (2003). Actuator faults and the linear quadratic control problem, *Proceedings of the 42nd Conference on Decision and Control, IEEE CDC'03, Maui, HI, USA*, pp. 959–965.

Tharrault, Y., Mourot, G., Ragot, J. and Maquin, D. (2008). Fault detection and isolation with robust principal component analysis, *International Journal of Applied Mathematics and Computer Science* **18**(4): 429–442, DOI: 10.2478/v10006-008-0038-3.

Wu, N., Zhou, K. and Salmon, G. (2000). Control reconfigurability of linear time-invariant systems, *Automatica* **36**(11): 1767–1771.

Yang, Z. (2006). Reconfigurabillity analysis for a class of linear hybrid systems, *Proceedings of 6th IFAC SAFEPROCESS'06, Beijing, China*, pp. 974–979.

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

Ahmed Khelassi received his M.Sc. degree in automatic engineering from the University of Bordeaux 1, France, in 2008. He is a Ph.D. student in the Research Centre for Automatic Control of Nancy (CRAN) at Nancy University, associated with the National Research Center for Science CNRS (UMR 7039). His research interests include fault-tolerant control, diagnosis, safety, reliability and aerospace systems.

Didier Theilliol received the Ph.D. degree in control engineering from Nancy University (France) in 1993. Since 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 plants, or aerospace domains. His current research interests include model-based fault diagnosis method synthesis and reliable active fault-tolerant control system design for LTI, LPV, multi-linear systems. Prof. Theilliol has published over 70 journal and conference papers.

Philippe Weber received the M.Sc. degree in automatic control and signal processing in 1995 from Henri Poincar Nancy University, France, and the Ph.D. degree in 1999 from the National Polytechnic Institute of 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 Center for Science CNRS (UMR 7039). He focuses his interest on modeling problems in maintenance, prognosis and dynamic reliability. He develops fault-tolerant control systems including reliability analysis. Since 2000 his research interest has been focused on modeling methods based on Bayesian networks.

Received: 8 March 2010
Revised: 6 November 2010
Re-revised: 27 December 2010