PACT: a PAssive / ACTive approach to fault tolerant stability under actuator outages

M. Staroswiecki$^1$, D. Berdjag$^1$, B. Jiang$^2$ and K. Zhang$^2$

1 SATIE, ENS Cachan, USTL, CNRS, UniverSud
61 avenue du Président Wilson, 94235 Cachan Cedex, France
2 College of Automation Engineering
Nanjing University of Aeronautics and Astronautics
29 YuDao Street, 210016 Nanjing, P.R. China

Abstract—This paper addresses actuator outages, or any actuator fault under the reconfiguration strategy. Based on the lattice structure of the set of system configurations, a frame that guarantees stability by mixing both the passive and active fault tolerance strategies is proposed. The proposed PACT designs a bank of controllers, with minimal number of control laws, and minimal instability during switching.

Keywords. Fault tolerant control, Reliable control, Actuator outages

I. INTRODUCTION

Fault tolerant control (FTC) aims at guaranteeing stability and performances (at least in a degraded sense) under system component failures. FTC approaches can be classified according to (a) the kind of faults they address, (b) the objective that is to be preserved in the presence of these faults, and the strategy that is selected (c) for the design and (d) for the implementation of the resulting control law.

(a) Actuators and sensors, being the weak components of most control systems, have received considerable attention. When specific kinds of faults (actuator outages, sensor losses [3], [4, 6, 21, 27]) or specific FTC strategies (system reconfiguration [2]) are considered, the set of the system situations to be tackled is known in advance. This paper addresses actuator outages or any actuator fault under the reconfiguration strategy (i.e. switching faulty actuators off).

(b) Many elaborate objectives are considered in the literature, involving different control approaches (state or output feedback, sliding modes, $H_\infty$ or $H_2$ optimal control) [5, 7, 12, 13, 21, 22, 23, 25], for regulation, tracking, disturbance attenuation. However, stability must be insured for all applications [3, 6, 8, 20]. It is the only objective addressed in this paper, for the sake of clarity and concision. Guaranteed performance design, in the single or multiple objective frame, can be addressed in a similar way.

(c) FTC design can be carried out through active or passive schemes. Active fault tolerance (AFT) designs control laws that are dedicated to each fault of interest, see e.g. [8, 13] for applications to actuator faults. In passive fault tolerance (PFT) or in reliable control, a single controller is designed for all or a subset of the faults. The feasibility is proven in specific cases [20, 22, 23] but most often, only sufficient existence conditions are given, e.g. in terms of a Matrix Inequalities solvability problem [6, 7]. Surprisingly, when dealing with actuator outages, the particular lattice structure of the set of faults is not exploited. A recent work [24] proposed a way to combine some advantages of PFT and AFT. In this paper, based on the lattice structure of the set of faults, a PAssive / ACTive (PACT) frame that guarantees stability by mixing both strategies is proposed.

(d) In the presence of a fault, the control law is redesigned on line when fault accommodation is concerned (i.e. the faulty system, with new model and new parameters, is controlled). Fault accommodation rises many real time issues, associated with the delays that are necessary to identify the model of the faulty system and to compute the new solution to the control problem (assuming there exists one), see e.g. [12, 26]. When the set of faults is known in advance, as in the case of actuator outages, FTC can be developed off-line and implemented in a bank of control laws [9, 10, 11]. The proposed PACT designs such a bank of controllers, thus relaxing the real time constraints: switching from an impaired control law to the appropriate fault tolerant one only needs the fault to be detected and isolated, therefore avoiding the on-line fault estimation and control re-design steps. Note that fault detection and isolation delays are still present and are addressed in this paper.

The paper is organized as follows: Section 2 models the system and the faults, emphasizing the existence of a lattice of system configurations. Section 3 presents the PACT fault tolerant strategy, while Section 4 discusses the problem of switching the control law in response to the faults. An application example is given in Section 5 followed by some concluding remarks.

II. PRELIMINARIES

A. System model

Consider the LTI system

$$\dot{x} = Ax + Bu \quad (1)$$

where $x \in \mathbb{R}^n$ is the state vector, and $u \in \mathbb{R}^m$ is the control vector. It is assumed that the state can be reconstructed from measurements and is available, i.e. sensors and sensor faults are not considered (see [16], [17] for a complete treatment...
of sensor faults). Since we are only interested in stability, no external input (noise, disturbance) is considered.

B. Faults

The considered faults are actuator outages, therefore matrix $B$ can take values $B_i, i \in \mathcal{I} = \{0, 1, \ldots\}$ where index $i = 0$ is associated with the nominal system (or nominal configuration), while index $i \neq 0$ is associated with fault mode $n^i$ (or configuration $n^i$). Notations are as follows:

- $S_i$ is the set of actuators that are available in configuration $n^i, i \in \mathcal{I}$,
- configuration $n^i$ is the pair $(A, B_i)$ where $B_i = B_0S_i$, and

$$\Sigma_i = \text{diag} \{\sigma_i(k), k = 1, \ldots, m\}$$

with $\sigma_i(k) = 1$ if actuator $k$ belongs to configuration $i$, and $\sigma_i(k) = 0$ otherwise. Therefore, $B_i$ contains a subset $Z_i$ of zero columns, that are associated with the actuators such that $\sigma_i(k) = 0$ (failed or switched-off actuators).

Nota: in the sequel we indulge ourselves a slight abuse by which the same notation stands for a set of configurations and for the set of their indexes, for example $(A, B_i) \in \mathcal{I}$ or $(A, B_i), i \in \mathcal{I}$.

C. The lattice of system configurations

From the definition of the faults, it follows that $\mathcal{I} = \{0, 1, 2, \ldots, 2^m - 1\}$ and the set of system configurations has a lattice structure, based on the partial ordering

$$(A, B_i) \succeq (A, B_j) \iff Z_i \subseteq Z_j$$

Definitions.

(1) The predecessors of a configuration $(A, B)$ are $\mathcal{P}(A, B) = \{(A, B_j): (A, B) \succeq (A, B_j)\}$ while its successors are defined by $\mathcal{S}(A, B) = \{(A, B_k): (A, B) \succeq (A, B_k)\}$. Note that a configuration $(A, B)$ belongs both to $\mathcal{P}(A, B)$ and $\mathcal{S}(A, B)$.

(2) Let $\mathcal{I} \subseteq \mathcal{I}$ be a subset of configurations, $(A, B) \in \mathcal{I}$ is minimal in $\mathcal{I}$ if $\mathcal{S}(A, B) \cap \mathcal{I} = (A, B)$.

III. PASSIVE/ACTIVE STABILIZATION

The fault tolerance specification that is considered in this paper is $\alpha$-stability.

Definitions.

(1) A closed-loop matrix $F$ is $\alpha$-stable (or has a stability margin $\alpha$) if $\Lambda(F) \in \mathcal{C}_\alpha$ where $\Lambda(F)$ is the spectrum of $F$ and $\mathcal{C}_\alpha = \{z \in \mathcal{C}: \text{Re}(z) \leq -\alpha\}$.

(2) A configuration $(A, B)$ is recoverable if it can be $\alpha$-stabilized, i.e. there exists a state feedback $K$ such that $F = A + BK$ is $\alpha$-stable.

Let $\mathcal{I}_{\text{recovery}} \subseteq \mathcal{I}$ be the set of recoverable faults, it obviously includes all configurations $(A, B)$ that are controllable, and all stabilizable configurations such that the non-controllable modes are $\alpha$-stable. Note that imposing $\alpha$-stability for the controllable modes and accepting simple stability for the non-controllable modes is an extension of the fault tolerance specification that results in $\mathcal{I}_{\text{recovery}} = \mathcal{I}_{\text{stability}}$ where $\mathcal{I}_{\text{stability}}$ is the set of stabilizable configurations.

A. Main result

Theorem 1: Let $u = -R^{-1}B_0^TH$ where $R > 0$ is a diagonal matrix, and $H = H^T \geq 0$. If $u$ stabilizes a configuration $(A, B)$ where $B = B_0\Sigma$ then it stabilizes all configurations in $\mathcal{P}(A, B)$. Moreover, if the closed loop matrix $A - BR^{-1}B_0^TH$ is $\alpha$-stable then, all configurations in $\mathcal{P}(A, B)$ are $\alpha$-stable when controlled by $u$.

Proof: Let $F = A - BR^{-1}B_0^TH$ be the closed-loop matrix associated with configuration $(A, B)$ and the control law $u$. Since $F$ is $\alpha$-stable and $H = H^T \geq 0$, one has

$$H(F + \alpha I) + (F + \alpha I)^T H \leq 0$$

which writes, since $\Sigma$ and $R^{-1}$ are diagonal

$$HA + A^T H \leq 2HB_0\Sigma R^{-1}B_0^TH - 2\alpha H$$

(2)

Let now $F' = A - BR^{-1}B_0^TH$ be the closed loop matrix associated with a configuration $(A, B') \succ (A, B)$ with $B' = B_0\Sigma'$ under the same control law $u$. Considering the Lyapunov function $V(x) = x^THx$ one has

$$\dot{V} = x^T [HA + A^T H - 2HB_0\Sigma' R^{-1}B_0^TH] x$$

From (2) it follows that

$$HA + A^T H - 2HB_0\Sigma' R^{-1}B_0^TH \leq 2HB_0(\Sigma - \Sigma') R^{-1}B_0^TH - 2\alpha H$$

Since $\Sigma$ and $\Sigma'$ are diagonal, one has $\Sigma - \Sigma' = \text{diag}(\zeta)$ and $(A, B') \succ (A, B)$ implies $\zeta \in \{-1, 0\}$ from which it follows that $(\Sigma - \Sigma') R^{-1} \leq 0$. Therefore, a sufficient condition for $F'$ to be $\alpha$-stable is that $(A, B') \in \mathcal{P}(A, B)$, hence the result.

Remark 1:

(1) The propagation of $\alpha$-stability from a configuration to all its predecessors is a direct consequence of the partial ordering on the lattice of configurations. This result extends the one in [23] as $u$ needs not be optimal for a given quadratic cost function, and $\alpha \neq 0$.

(2) Theorem 1 expresses a sufficient $\alpha$-stability condition: a control law $u$ that $\alpha$-stabilizes $(A, B)$ may obviously $\alpha$-stabilize more configurations than the ones in $\mathcal{P}(A, B)$.

B. A Passive/Active (PACT) Fault Tolerance Strategy

A PACT Fault Tolerance Strategy is defined by a bank of control laws that contains at least one $\alpha$-stabilizing control law for any recoverable fault situation $(A, B)$. Let $\mathcal{I}_{\text{recovery}} \subseteq \mathcal{I}$ be the set of minimal recoverable configurations in $\mathcal{I}$.

The following corollary characterizes a PACT with respect to the set $\mathcal{I}_{\text{recovery}}$.

Corollary 2: Let $\{H_i, i \in \mathcal{I}_{\text{recovery}}\}$ be a set of matrices such that

$$i \in \mathcal{I}_{\text{recovery}} \iff H_i = H_i^T \geq 0 \quad \Lambda(H_i) \in \mathcal{C}_\alpha$$

(3)

where for each $i \in \mathcal{I}_{\text{recovery}}, F_i = A - B_iR^{-1}B_0H_i$ is the closed-loop matrix associated with configuration $(A, B_i)$ under the state feedback $R^{-1}B_0H_i$. Then, every configuration in $\mathcal{I}_{\text{recovery}}$ can be $\alpha$-stabilized by at least one of the control laws $u_i = -R^{-1}B_0H_i x, i \in \mathcal{I}_{\text{recovery}}$. 

7820
Proof: From the main result, the control law \( u_i = -R^{-1}B_0H_ix,i \in I^\ast \) \( \alpha \)-stabilizes all the predecessors of configuration \( i \). Moreover, one has

\[
\mathcal{I}_{\text{recov}} = \bigcup_{i \in \mathcal{I}_{\text{recov}}} \mathbb{P}(A,B_i)
\]

i.e. the set of recoverable configurations is covered by the union of the predecessors of its minimal elements. \( \blacksquare \)

Remark 2:
(1) If a fault results in a non-recoverable configuration, fault tolerance is not possible and the system objective must be reconfigured (see [2], [18]).
(2) A widely spread approach to reliable control design is as follows: given a design specification (i.e. a set of configurations \( (A,B_i),i \in \mathcal{I} \subseteq \mathcal{I}_{\text{recov}} \), establish matrix inequalities that insure the existence of a state feedback \( K \) and a set of Lyapunov functions \( V_i(x) = x^TL_ix \) such that

\[
i \in \mathcal{I}: L_i(A + \alpha I + B_iK) + (A + \alpha I + B_iK)^TL_i \leq 0
\]

(4)

Let \( \mathcal{I}^\ast \) be the set of minimal configurations in \( \mathcal{I} \), it follows from Theorem 1 that writing \( i \in \mathcal{I}^\ast \) instead of \( i \in \mathcal{I} \) in (4) gives the same result, while eliminating useless constraints. Moreover, choosing \( \mathcal{I} = \mathcal{I}_{\text{recov}} \) is obviously associated with the research of a passive fault tolerance design. At the best of our knowledge, the problem of how to choose \( \mathcal{I} \subseteq \mathcal{I}_{\text{recov}} \) when existence conditions are not satisfied for \( \mathcal{I} = \mathcal{I}_{\text{recov}} \) has not been addressed (see [19] for a study of the trade-off that must be achieved when only a subset of the recoverable faults can be recovered by reliable control). Note that there is no trade-off implied by the PACT strategy since it provides solutions that recover from any recoverable fault.

(3) A straightforward way of finding a set \( \{H_i,i \in \mathcal{I}_{\text{recov}}\} \) such that (3) holds is as follows: let \( Q = C^TFC \geq 0 \) be given such that \( (A,C) \) is observable, then conditions (3) are satisfied by

\[
i \in \mathcal{I}_{\text{recov}}^\ast: H_i = W_i^\ast
\]

where \( W_i^\ast \) is the unique stabilizing solution of the algebraic Riccati equation

\[
(A + \alpha I)^TW_i^\ast + W_i^\ast(A + \alpha I) - W_i^\ast BR^{-1}B^TW_i^\ast + Q = 0
\]

This is easily proven from the solution of the Linear Quadratic optimal control problem associated with the cost \( J = \int_0^\infty e^{2\omega t}[x^TQx + u^TRu]dt \) (see [1]), which is the case originally considered by [23] (for \( \alpha = 0 \)).

(4) Whatever the fault situation, \( \{H_i,i \in \mathcal{I}_{\text{recov}}^\ast\} \) provides a bank of control laws among which at least one is \( \alpha \)-stabilizing. However, it might be possible to find a PACT bank with less control laws, as we shall see now.

C. A domination relation on the set of minimal stabilizable configurations
The property that a control law associated with a minimal stabilizable configuration \( (A,B_i) \) \( \alpha \)-stabilizes all its predecessors \( \mathbb{P}(A,B_i) \) does not exclude the possibility that it also \( \alpha \)-stabilizes other configurations. For a given set of matrices \( \{H_i,i \in \mathcal{I}_{\text{recov}}^\ast\} \) we define a domination relation \( \mathcal{D} \) on the set of minimal recoverable configurations as follows

\[
i,j \in \mathcal{I}_{\text{recov}}^\ast: (A,B_i) \mathcal{D} (A,B_j) \iff (F_{j/i}) \in C_\alpha
\]

where \( F_{j/i} \equiv A - B_jR^{-1}B_i^TH_i \).

It follows that if configuration \( (A,B_i) \) dominates configuration \( (A,B_j) \) then the control law \( u_i = -R^{-1}B_0H_ix,i \in \mathcal{I}_{\text{recov}}^\ast \) \( \alpha \)-stabilizes all configurations \( \mathbb{P}(A,B_i) \cup \mathbb{P}(A,B_j) \). A bank of controllers that achieves PACT fault tolerance for the whole set of stabilizable configurations is found on the basis of the previous corollary restated as:

Corollary 3: Let \( \{H_i,i \in \mathcal{I}_{\text{recov}}^\ast\} \) be a set of matrices such that

\[
i \in \mathcal{I}_{\text{recov}}^\ast \begin{cases} H_i = H_i^T \geq 0 \\ \Lambda(F_{j/i}) \in C_\alpha \end{cases}
\]

and let \( \mathcal{D}_{\text{recov}}^\ast \subseteq \mathcal{I}_{\text{recov}}^\ast \) be the set of non-dominated configurations in \( \mathcal{I}_{\text{recov}}^\ast \). Then, every configuration in \( \mathcal{I}_{\text{recov}}^\ast \) can be \( \alpha \)-stabilized by at least one of the control laws \( u_i = -R^{-1}B_0H_ix,i \in \mathcal{I}_{\text{recov}}^\ast \).

Remark 3: If \( \mathcal{D}_{\text{recov}}^\ast \) contains only one control law, a purely passive fault tolerant control that guarantees \( \alpha \)-stability has been found.

IV. SELECTION AND SWITCHING OF CONTROLLERS
Associated with each stabilizable configuration \( (A,B) \), define \( \mathcal{D}_{\text{recov}}^\ast(A,B) \) as:

\[
\mathcal{D}_{\text{recov}}^\ast(A,B) = \mathcal{D}_{\text{recov}}^\ast \cap \mathcal{S}(A,B)
\]

\( \mathcal{D}_{\text{recov}}^\ast(A,B) \) contains all minimal recoverable configurations whose associated control law \( \alpha \)-stabilizes configuration \( (A,B) \). Unless \( \mathcal{D}_{\text{recov}}^\ast(A,B) \) is a singleton, the problem of selecting the control law to be applied to \( (A,B) \) arises. Since no performance consideration is taken into account, the choice only impacts the system stability during the transitions from one configuration to another.

Let \( t_f \) be the time at which a fault occurs, and \( t_{f/c} > t_f \) the time at which the PACT switches-on the appropriate control law (since there is no on-line control re-design, the delay is only caused by fault detection and isolation and control switching). During \( t_{f/c} - t_f \) the "new" configuration is still controlled as was the "old" one, and instability can take place, possibly in such a way that physical limits are trespassed (see [12], [26] for the consideration of FDI / FTC delays).

Assume \( (A,B) \) is controlled by \( u_i = R^{-1}B_0H_ix \), for some \( i \in \mathcal{D}_{\text{recov}}^\ast(A,B) \), and consider the transition \( (A,B) \rightarrow (A,B_j) \) where \( (A,B_j) \in \mathcal{S}(A,B) \). The closed-loop matrix that applies on \( [t_f,t_{f/c}] \) is \( F_{j/i} = A - B_jR^{-1}B_i^TH_i \), and it may be stable or not. Accordingly, characterize \( F_{j/i} \) by \( \tilde{\lambda}_{j/i} \equiv \max_{\lambda \in \Lambda(F_{j/i})} \text{Re} \lambda \). The selection procedure

\[
i(A,B) = \arg \min_{i \in \mathcal{D}_{\text{recov}}^\ast(A,B) \subseteq \mathcal{S}(A,B)} \tilde{\lambda}_{j/i}
\]

results in the \( H_i(A,B) \) that "minimizes" the instability associated with the "worst" change of configuration between \( (A,B) \) and any of its successors.

7821
Remark 4:

(1) $\alpha$-stability may or not be satisfied during the transients, since $\tilde{\lambda}_{j/i}(A,B)$ may take any value.

(2) Since any configuration $(A,B_j) \in S(A,B)$ could occur after configuration $(A,B)$ the worst case impairment in the decision procedure (7) has been selected in the whole set $S(A,B)$, which may result in a very conservative choice (for example if the worst transition concerns the simultaneous failure of many actuators). Based on the classical argument that the probability of multiple simultaneous faults decreases exponentially with the number of faults (if faults are independent), conservativeness can be limited by considering only transitions from $(A,B)$ to a selected subset $\tilde{S}(A,B)$ of its successors, i.e. $i(A,B) = \arg \min_{i \in \mathcal{P}_{\text{recov}}(A,B)} \max_{j \in \tilde{S}(A,B)} \tilde{\lambda}_{j/i}$. For example, securing only single fault transitions would consider $\tilde{S}(A,B) = S_1(A,B)$, the successors that differ from $(A,B)$ by only one actuator.

(3) For those configurations such that $\tilde{\lambda}_{j/i}(A,B) > 0$, guaranteeing practical fault tolerance calls for control under state constraints, and rests on solving the following problem: given a set $\mathcal{P}^*$ of admissible safe states, given the respective values of $\tilde{\lambda}_{j/i}(A,B)$ and the FDI delay $t_{f/e} - t_f$, find a set $\mathcal{P}^*_f$ such that $x(t_f^e) \in \mathcal{P}^*_f \implies x(t_f^e) \in \mathcal{P}^*$ and monitor the constraint $x(t) \in \mathcal{P}^*_f$ (note that while the monitoring of equality constraints is the subject of the whole model-based FDI theory, the monitoring of inequality constraints has received very little attention, see [14, 15]).

V. APPLICATION EXAMPLE

Consider the system with four actuators $a,b,c,d$ respectively associated with the first, second, third and fourth column of $B_0$

$$A = \begin{pmatrix}
0.5 & -2 & 0 & -1 \\
2 & 0.5 & 1 & 0.2 \\
1 & 0 & 2 & 1 \\
0 & 0 & 0 & -1
\end{pmatrix},
$$

$$B_0 = \begin{pmatrix}
0.5 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0.5 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}$$

Matrix $A$ is unstable, having the set of eigenvalues $\Lambda(A) = \{0.5 \pm 2j; -1; 2\}$. Let $\alpha = 0.1$ be the stability margin specification. Using straightforward notations, the recoverable configurations are

$$\mathcal{J}_{\text{recov}} = \{abcd, abc, abd, bcd, acd, ac, cd, bc, bd, ad, d\}$$

The minimal recoverable configurations are given by

$$\mathcal{J}^{*}_{\text{recov}} = \{d, ac, bc\}$$

In order to select an appropriate set $\{H_i, i \in \mathcal{J}^{*}_{\text{recov}}\}$, Remark 4 (3) is used. Using $K = I_{4 \times 4}$ and $Q = I_{4 \times 4}$, the solutions of the algebraic Riccati equations (5) are

$$W_d^* = \begin{pmatrix}
22.70 & 0.97 & -3.1 & -5.25 \\
0.97 & 37.72 & -59.13 & -5.90 \\
-3.1 & -59.13 & 143.67 & 23.99 \\
-5.25 & -5.90 & 23.99 & 6.62
\end{pmatrix},
$$

$$W_{ac}^* = \begin{pmatrix}
8.89 & 2.4697 & 0 & -0.75 \\
2.47 & 10.4037 & 0 & 3.17 \\
0 & 0 & 16.2462 & 5.31 \\
-0.75 & 3.17 & 5.31 & 3.60
\end{pmatrix},
$$

$$W_{bc}^* = \begin{pmatrix}
3.50 & -0.92 & 0 & -1.02 \\
-0.92 & 2.72 & 0 & 1.09 \\
0 & 0 & 16.25 & 5.31 \\
-1.02 & 1.09 & 5.31 & 2.93
\end{pmatrix}$$

It follows that the PACT based on $\mathcal{J}^{*}_{\text{recov}} = \{d, ac, bc\}$ allows to recover from all recoverable faults, by using the control laws $u_d = -R^{-1}B_d^TW_d^*x$ for configurations in $\mathcal{P}(A,B_d) = \{abcd, abd, bcd, acd, cd, bd, ad, d\}$, $u_{ac} = -R^{-1}B_{ac}^TW_{ac}^*x$ for configurations in $\mathcal{P}(A,B_{ac}) = \{abcd, abc, acd, ac\}$ and $u_{bc} = -R^{-1}B_{bc}^TW_{bc}^*x$ for configurations in $\mathcal{P}(A,B_{bc}) = \{abcd, abc, bcd, bc\}$, as shown by Table I.

<table>
<thead>
<tr>
<th>$\mathcal{J}_{\text{recov}}$</th>
<th>$u_d$</th>
<th>$u_{ac}$</th>
<th>$u_{bc}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$abcd$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$abc$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$abd$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$bcd$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$acd$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$ac$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$cd$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$bc$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$bd$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$ad$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$d$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

TABLE II
DOMINATION RELATION ON $\mathcal{J}^{*}_{\text{recov}}$

As several $\alpha$-stabilizing control laws are found for configurations $abcd, abc, bcd, acd$, the appropriate one is selected using the selection procedure (7). Table 4 shows the values $\tilde{\lambda}_{j/i}$ that characterize, for each configuration $j \in \mathcal{J}_{\text{recov}}$, the
impairment between its $\alpha$-stabilizing control laws and its worst successor. The control law to be selected appears on the last row of the table. Note that configurations $\{d, bc, ac\}$ being minimal, any further fault leads to a non stabilizable successor (since $A$ is unstable) hence the blank in the corresponding cells.

In order to illustrate the effect of the selection procedure, assume that the system nominal configuration $abcd$ is active on the time window $[0, 100]$ and a failure of actuator $c$ occurs at time $t_f = 100x$. Under a $t_{ftc} = 10s$ diagnosis delay, Figures 1 and 2 display the third state trajectory and its derivative, associated with the two $\alpha$-stabilizing control laws $u_d$ and $u_{bc}$, showing the interest of choosing $u_d$ to minimize the effect of control switching. The initial condition was $x(0) = (-15, 15, -5)$.

**Remark 6:** An ultimate simplification of the PACT scheme is obtained by using the single control law $u_d$, at the cost of not satisfying the $\alpha$-stability specification for configuration $\{bc\}$. Indeed, in that case, although the fault is recoverable, the implemented control law will not allow to recover from it. This trade-off in the favor of simplicity can be done if the probability of actuators $a$ and $d$ failing is reasonably low.

VI. Conclusion

When actuator/sensor outages are considered, or when system reconfiguration is used preferably to fault accommodation, the set of faults for which fault tolerance is wished is known in advance, and has a lattice structure. Based on the minimal recoverable configurations, this paper has developed a mixed passive / active approach that is able to stabilize all the recoverable configurations, resulting in a large simplification of the diagnosis and the reconfiguration procedures, all the more as the existence of a domination relation on the set of minimal recoverable faults allows to decrease the number of control laws to be implemented. When several control laws are possible, the paper has also proposed a selection strategy aimed at minimizing the instability that might occur during the fault detection and isolation delay, when a new configuration switches on, and is still controlled by the control law associated with the previous configuration.

VII. Acknowledgments

This work has been developed in the project SIRASAS (Stratégies Innovantes et Robustes pour l‘Autonomie des Systèmes Aéronautiques et Spatiaux) supported by the Fondation de Recherche pour l‘Aéronautique et l‘Espace.

REFERENCES

<table>
<thead>
<tr>
<th></th>
<th>abc</th>
<th>bcd</th>
<th>acd</th>
<th>ac</th>
<th>cd</th>
<th>bc</th>
<th>bd</th>
<th>ad</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_{a}$</td>
<td>-0.83</td>
<td>0.09</td>
<td>-0.61</td>
<td>0.09</td>
<td>-0.28</td>
<td>X</td>
<td>-0.57</td>
<td>X</td>
<td>-0.57</td>
</tr>
<tr>
<td>$u_{bc}$</td>
<td>0.8</td>
<td>0.062</td>
<td>0.79</td>
<td>0.84</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>-0.57</td>
<td>X</td>
</tr>
</tbody>
</table>

**TABLE IV**

WORST IMPAIRED EIGENVALUES


[27] Q. Zhao and J. Jiang (1998), Reliable state feedback control system design against actuator failures, Automatica, 34 (10) : 1267 - 1272.