Fault Tolerant Systems viewed as Switching Hybrid Systems

R. Hamdaoui
PhD student
Engineering school
University of Gabes, Tunisia

M.N. Abdelkrim
Professor
Engineering school
University of Gabes, Tunisia

ABSTRACT
This paper presents fault tolerant control systems FTC in a hybrid system framework. Due to the discrete nature of fault occurrence and reconfiguration, FTC systems are considered hybrid in nature. Thus, in this work, actuator fault recoverability is studied by utilizing a controllability concept of hybrid systems. The hybrid formalism allows the recoverability's analysis based on the controllability concept of hybrid systems. Fault recovery is also studied based on control energy limitation in order to determinate admissible recovery solutions.

General Terms
Diagnostic and Decision Supporting Systems, Applications of Computer Science in Modeling.

Keywords
Active fault tolerant control; switching hybrid system; actuator fault recoverability; admissibility.

1. INTRODUCTION
Active Fault Tolerant Control (AFTC) systems are systems where faults are explicitly detected and accommodated through changing of the control laws in order to recover the system to the nominal performance as much as possible. The AFTC systems merge several disciplines into a common framework to achieve this aim. The desired features are obtained through on-line fault diagnosis, automatic condition assessment and calculation of appropriate remedial actions to avoid certain consequences of a fault. Generally, these consequences become more and more undesirable as the time goes on, thus, the detection and the accommodation delays must be taken into consideration while synthesizing an active fault tolerant control approach.

A fault is a discrete event that acts on a system and its occurrence changes some of the properties of the process. The goal of fault-tolerant control is in turn to respond to the occurrence of a fault such that the faulty system is still well behaved. Thus, for both passive and active tolerance and due to the discrete nature of fault occurrence and reconfiguration, FTC systems are hybrid in nature [8], [9].

Besides, safe-critical systems are becoming more and more complicated so that the conventional LTI model is no more sufficient to describe the dynamic of this kind of complex systems. FTC system description in hybrid formalism allows studying fault recoverability as system property by studying the controllability of the hybrid system modeling the FTC system [10].

Hybrid description provides the possibility of taking the timing issue in FTC into consideration. The time issue constituted by fault detection and fault accommodation delays and their effect on the time of the system's mission is rarely studied in FTC approaches although it can be very influencing in the performances and control qualities [11]-[13].

In the hybrid description of the FTC, detection instant and accommodation or reconfiguration one can be considered as switching instants from one mode to another. Therefore, these switching instants can be optimized in order to satisfy an optimal performance index after the fault's occurrence.

This paper is organized as the first section describes how a FTC system can be viewed as a hybrid system by presenting the common characteristics and elements between both systems. The second section demonstrates the study of fault recoverability based on hybrid system's controllability. In the third section, the admissibility of the actuator recovery is studied based on control energy index and time optimization.

Theoretical results are proved by an illustrative example in the section 4. Finally, concluding remarks are provided.

2. FTC SYSTEMS AND SWITCHING HYBRID SYSTEMS
In the last few decades, there has been a huge amount of research on a special class of systems, which are called hybrid systems. Hybrid systems can be described as systems that are controlled by discrete events in the higher level, while their dynamical behaviors are governed by continuous dynamical laws in the lower level.

Switching systems are a class of hybrid systems. The behavior and control of switching hybrid systems is based on the concept of modes. Each mode corresponds to a dynamical law. Mode switching (or mode transition) refers to switching the mode of operation of the system from the current mode to the next mode according to a mode sequence. The instants when moving from one mode to another are called the switching time instants. These instants will be the critical instants related to the fault detection and recovery in the FTC system.

2.1 FTC system viewed as a switching system
Fault Tolerant Control systems are switching hybrid in nature because they obey a set of possible dynamical laws. The fault occurrence and the accommodation or reconfiguration are discrete events that dictating the continuous dynamical behavior of the system.

The continuous dynamics of switching systems is given by the following differential equation:

$$\begin{cases} \dot{x}(t) = A_i x(t) + B_i u(t) \\ y(t) = C_i x(t) \end{cases} \quad (1)$$

where $x \in X \subseteq \Re^n$ is the state vector, $y \in Y \subseteq \Re^p$ is the measure vector and $u \in U \subseteq \Re^m$ is the control vector. Matrices A_i, B_i and C_i describe a kind of specific linear dynamic at the i^{th} mode. The system is assumed to have a finite number of modes, that is $i \in Q$, and $size(Q) = l < \infty$. The set Q denotes the set of all discrete states or modes of the system. The structure of the discrete part of the plant is defined by the set of modes Q and a mode-transition function $\delta_p : Q \times \Sigma \to Q$ with $\Sigma = \Sigma_c \times \Sigma_p$ constitutes the plant's alphabet where $\zeta_c \in \Sigma_c$ denote the control events manipulating the control variables and $\zeta_p \in \Sigma_p$ denote events that result from additional physical modes, which are part of the plant itself as a result of its discrete features. Each physical mode corresponds to a unique event $\zeta_p \in \Sigma_p$ which is triggered each switching time through an event-generator function $\Gamma_p : X \to \Sigma_p$ that is corresponding to transitions between regions associated with physical modes. These elements are presented in figure 1, where q_p denotes the present mode:

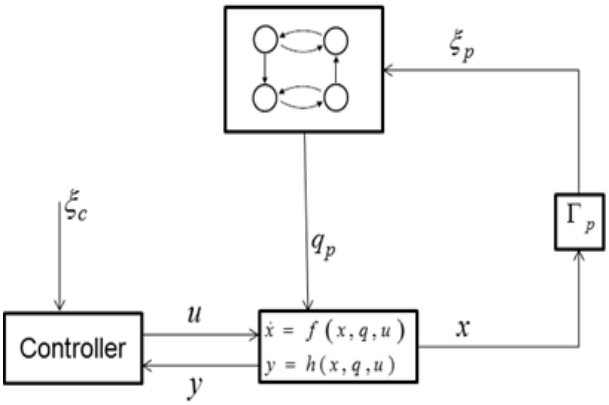

Fig 1: Hybrid System schema.

A Fault Tolerant Control system is a system that can change in a discrete way through change in states caused by faults occurrence. Plant architecture can be changed by switch-over functions. Parameters or structure of the controller can be changed by logic in a supervisor automaton that getting its input from an FDD block. While moving to describe a FTC system analogously to the switching hybrid system's description, the following elements are re-defined:

- The mode-transition function $\delta_p : Q \times \Sigma' \to Q$ with $\Sigma' = \Sigma_c \times \Sigma_p \times \Sigma_f \times \Sigma_r$ constitutes the plant's alphabet where Σ_c and Σ_p are the same, $\zeta_f \in \Sigma_f$ denote the fault events and $\zeta_r \in \Sigma_r$ are the control events reconfiguring the faulty system, as it is showed in figure 2 with q_p denoting the actual control mode.
- Another event-generator function $\Gamma_d : Y \to \Sigma_d$, with $\zeta_d \in \Sigma_d$ are the events generated from the FDD task to the supervisor automaton.
- Three modes are defined; the nominal mode stands from the initial instant of the system till the fault's occurrence that is $[t_0, t_f)$, the faulty mode stands during $[tf, t_r)$ with t_r presents the time of applying the accommodating control law and finally the reconfiguration mode is active in the interval $[t_r, t_{mis}]$ where the system enters the post-fault interval till t_{mis}, the time fixed to the system's end of mission.

Since after the fault detection at an instant called t_d, still active the faulty mode and as the instant t_d is the known one, we will replace in the cited intervals the occurrence instant t_f by t_d. These instants verify the piecewise linear inequality constraint:

$$t_0 \le t_f \le t_d \le t_r \le t_{mis} \quad (2)$$

In this work, actuator fault will be considered, caused by a loss of control factor efficiency and presented by:

$$B_f = B_n(I - \Gamma),\ \Gamma = diag(\gamma_i) \quad (3)$$

with I is the identity matrix and γ_i, $i = 1,..., p$ indicates the i^{th} actuator state, affected if $0 < \gamma_i \le 1$.

2.2 Advantages of the Switching Hybrid formalism

One principle advantage is that SH model allows the mathematical formalization of the critical time instants in the AFTC system and, thus, the possibility of study and analyzes the FDD and the FTC delays in relation with the system and the control performances. In the literature, several researches were interested by the optimal control of SH systems and a specific attention was given to the optimization of the switching instants.

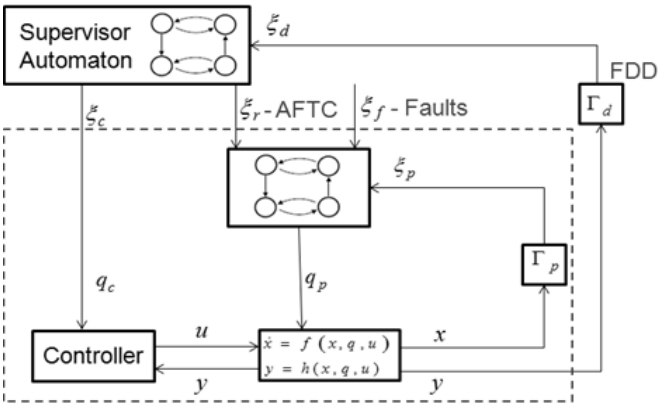

Fig 2: Fault Tolerant Control system modeled by switching system.

The cited works elaborated and used different techniques and methods in order to solve the time optimization problem, which may be usually nonconvex, such that the Luus-Jaakola optimization procedure which is a well tested, efficient direct search method for the similar optimal switched systems, the gradient-descent algorithms, the nonlinear optimization techniques to locate the switching instants in.

A second benefit of the SH model is that the fault recoverability can be viewed as system's propriety since it can be studied from the SH system's controllability.

SH system's controllability use the following definitions: **Definition 1:** Hybrid system given by the equation (1) is called controllable if there exists a timed switching mode set denoted as $\{(q_{i-1},t_i,q_i)\}_{i=1}^{l}$ and a corresponding piecewise continuous input signal $u(t)$, such that system (1) evolving under these two kinds of distinct inputs is reachable from an initial hybrid state (q_0,x_0) to an aim state (q_T,x_T) within a finite time interval $[0,T]$ [15].

We assume that there are no discontinuous state jumps during mode switches.

Definition 2: System (1) is called (completely) control reconfigurable if and only if the controllability property of the nominal system is kept by the faulty system.

Seeing that the FTC system (4) is described by a hybrid schema where the faulty mode is one of the own system modes, then, the control reconfigurability is directly guaranteed from the controllability of system (4).

Definition 3: From Definition 1 and Definition 2, an affected system viewed as a hybrid system is recoverable from a set of faults if it is control reconfigurable and thus, if its hybrid model is controllable.

3. RECOVERABILITY STUDY BASED SH CONTROLLABILITY

Hybrid systems controllability is studied in [10], [15] and [16] where necessary and sufficient conditions were defined. Motivated by these works, the controllability of system (4) returns to define the two modes controllability matrix:

$$W_c^n = \begin{bmatrix} B_n & AB_n & \cdots & A^{n-1}B_n \end{bmatrix} \quad (5)$$

$$W_c^f = \begin{bmatrix} B_f & AB_f & \cdots & A^{n-1}B_f \end{bmatrix} \quad (6)$$

Then, we can define a combined matrix W_C for the whole system expressed by:

$$W_C = \begin{bmatrix} W_c^n & W_c^f \end{bmatrix} \quad (7)$$

Equation (7) represents the controllability matrix for system (4); this latter is controllable if and only if W_C is of full row rank.

Theorem 1: The AFTC system (4) with nominal and faulty modes is controllable if the controllability matrix W_C defined in (7) is of full row rank.

Proof: With respect to the piecewise LTI property of (4), the continuous state at t_{mis} can be expressed as:

$$\begin{aligned} x(t_{mis}) &= e^{A(t_{mis}-t_d)}e^{A(t_d-t_0)}x(t_0) \\ &+\int_{t_0}^{t_d} e^{A(t_{mis}-t_d)}e^{A(t_d-\tau)}B_n u(\tau)d\tau \\ &+\int_{t_d}^{t_{mis}} e^{A(t_{mis}-\tau)}B_f u(\tau)d\tau \end{aligned} \quad (8)$$

By setting $\bar{x}_{mis} = x(t_{mis}) - e^{A(t_{mis}-t_d)}e^{A(t_d-t_0)}x(t_0)$ and by defining the following expressions:

$$\begin{cases} T_n = e^{A(t_{mis}-t_d)}e^{A(t_d-t_0)} \\ T_f = e^{A(t_{mis}-t_d)} \end{cases}$$

The relation (8) can be expressed as:

$$\begin{aligned} \bar{x}_{mis} &= T_n\int_{t_0}^{t_d} e^{A(t_d-\tau)}B_n u(\tau)\,d\tau \\ &+T_f\int_{t_d}^{t_{mis}} e^{A(t_{mis}-\tau)}B_f u(\tau)\,d\tau \end{aligned} \quad (9)$$

Denoting the i^{th} additive term on the right-hand side of (9) by X_i, we have:

$$X_i = T_i\int_{t_{i-1}}^{t_i} e^{A(t_i-\tau)}B_i u(\tau)\,d\tau \quad (10)$$

Divide interval $[t_{i-1},t_i]$ into n subintervals, and denote the dividing points as $t_{i-1,0}...t_{i-1,n}$ with the property $t_{i-1,0} < ... < t_{i-1,n}$.

Then we can define the piecewise continuous input $u(t)$ as a piecewise constant function, denoted as $j=1,..,n$ with $j=1,..,n$.

According to the Cayley–Hamilton Theorem [16], the exponential matrix e^{At} can be expressed as:

$$e^{At} = \alpha_0(t)I + \cdots + \alpha_{n-1}(t)A^{n-1} = \sum_{i=0}^{n-1}\alpha_i(t)A^i \quad (11)$$

By using the input $u(t)$ definition and relation (11), the equation (10) becomes:

$$X_i \square T_i W_i F U_i = T_i \left[B_i \quad AB_i \quad \cdots \quad A^{n-1} B_i \right] \begin{bmatrix} \int_{t_{i-1,0}}^{t_{i-1,1}} \alpha_0 (t_i - \tau) d\tau & \cdots & \int_{t_{i-1,n-1}}^{t_{i-1,n}} \alpha_0 (t_i - \tau) d\tau \\ \vdots & \ddots & \vdots \\ \int_{t_{i-1,0}}^{t_{i-1,1}} \alpha_{n-1} (t_i - \tau) d\tau & \cdots & \int_{t_{i-1,n-1}}^{t_{i-1,n}} \alpha_{n-1} (t_i - \tau) d\tau \end{bmatrix} \left[U_{i-1,1} \quad \cdots \quad U_{i-1,n} \right]^{\mathrm{T}} \quad (12)$$

In (12), the matrix F constructed by using the expansion coefficients of e^{At} is the same for both nominal and faulty mode since the matrix A is the same and there exists a real sequence $\{t_d, t_{mis}\}$ which satisfies $t_0 < t_d < t_{mis}$ and makes F nonsingular [16].

The relation (9) is thus rewritten as:

$$\bar{x}_{mis} = T_n W_c^n F U_n + T_f W_c^f F U_f \quad (13)$$

Lemma 1: For a set of matrices $\{T_i\}_{i=1}^k$ where each T_i has the form $T_i \square I + \varepsilon_i E_i$ and E_i is a constant matrix; there exists a set of ε_i (are small enough); such that there are P_i matrices with the same order as T_i so that:

$$rank\left(\left[T_1 P_1 \quad \cdots \quad T_k P_k\right]\right) \geq rank\left(\left[P_1 \quad \cdots \quad P_k\right]\right) \quad (14)$$

By using Lemma 1 and by considering the assumption that the controllability matrix W_c is of full row rank, and then we get

$$rank\left(\left[T_n W_c^n \quad T_f W_c^f\right]\right) \geq rank\left(\left[W_c^n \quad W_c^f\right]\right) = n .$$

4. ADMISSIBILITY OF FAULT RECOVERY

As it was mentioned in Remark 1, the hybrid controllability can response to the actuator fault recovery by control reconfiguration in absence of system constraints, however, this is practically unrealistic.

Control energy limitation and\or time deadlines are considered as system limitations that deciding about the fault recoverability's admissibility [12], [14].

4.1 Control energy admissibility

Staroswiecki in [14] defined the recovery measure as being the maximum loss of efficiency allowable for a control solution that still achieves the objective in the presence of fault. This solution is the so-called admissible solution satisfying the admissibility conditions specified by the selected discussion criterion. This loss of efficiency can be defined by a maximum cost of controlling the faulty system, whatever the initial state in the unit sphere or by a maximum loss of efficiency in the faulty system control, whatever the control objective. The energy is given by:

$$J(u,t) = \int_0^{\infty} \left[u^{\mathrm{T}}(t) u(t) \right] dt \quad (15)$$

In this work, we consider a normalized function depending on the initial conditions $L\left(x(0)\right) \geq 1$, $t_0 = 0$, such that:

$$L\left(x(0)\right) = \frac{\lambda}{\hat{J}\left(x(0)\right)} \quad (16)$$

$\hat{J}\left(x(0)\right)$ is the optimal cost resulting from minimizing (15) and λ defines a uniform bound for the energy spent in controlling the faulty system, whatever the initial state in the unit sphere. The definition of this bound results from the theorem of the continuous dependence of the differential equations solutions considering the initial condition $x(0) \in \Re^n$ such that $\|x(0)\| = 1$ [17]. The maximum cost is then given by the maximum eigenvalue of $K_n(0)$ solution of the Riccati equation, then, the energy limit is $\lambda_{max}\left(K_n(0)\right)$.

This previous analysis explains that in this case of energy limitation, even when the hybrid controllability of the system (nominal and faulty modes) is satisfied, fault can be unrecoverable if the reconfiguration solution is not admissible considering the energy constraint.

Then the recovery conditions are:

1- The faulty system is hybrid controllable;
2- The spent energy for recovery is lower than the maximum value.

4.2 Temporal admissibility

Time delays in fault diagnosis and in fault tolerance can cause stability problems in feedback control systems if they are very important. In another side, if these delays are very short so that the consequences are FDD uncertainties, imprecise post-fault model or even performances violation by causing actuator saturation or excessive control energy [11], [12].

Thus, it is quite interesting to look for optimal delays that guarantying acceptable performance degradation and achievement of temporal and physical system constraints, here the end time of the system's mission and the control energy.

When considering the fault detection instant and the reconfiguration instant as switching instants between modes in a hybrid system, it is possible to optimize these critical instants based on the parameterization of the switching instants in the problem of optimal fault tolerant control [18].

5. NUMERICAL APPLICATION

Considering the system given by the following matrices:

$$A = \begin{bmatrix} -0.0565 & 29.072 & -175.610 & 9.6783 & 1.6022 \\ -0.0601 & -0.7979 & -0.2996 & 0 & 0 \\ 9.218\times10^{-3} & -0.0179 & -0.1339 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$B_n = \begin{bmatrix} -0.1339 & 0.1339 & 2.0092 \\ 2.3491 & -2.3491 & 0.7703 \\ 0.0444 & -0.0444 & -1.3575 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad (17)$$

$$C = [0 \quad 0 \quad 0 \quad 0 \quad 1]$$

This model represents the lateral-directional dynamics of a McDonnell F-4C Phantom flying at Mach 0.6 at an altitude of 35000 ft, where the model is in [19]. The control objective is to regulate a disturbed yaw angle to the origin $y(=x_5)=0(radian)$. The control inputs u_1, u_2 and u_3 correspond to the left aileron, the right aileron and the rudder surface displacement, respectively.

The system has three actuators $I=\{a,b,c\}$, in the nominal mode $\lambda_{\max}(K_n)=19.6246$ energy unit, with K_n is the nominal control gain solution of Riccati equation.

Considering the actuator faults scenarios given by a total failure of one or two actuators, assuming that one fault occurring during the functional time of the system. A failure in the actuator *a* is characterized by the matrix:

$$B_f = \begin{bmatrix} 0 & 0.1339 & 2.0092 \\ 2.3491 & 0 & 0.7703 \\ 0.0444 & -0.0444 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Under all these faulty situations, the faulty system still controllable; hybrid controllability is verified for all scenarios. However, Table 1 shows that the fault is recoverable, regarding the energy limit defined as $2\lambda_{\max}(K_n)$, just for two situations; a failure in the first actuator *a* or the second one *b*. Solutions written in bold in Table 1 are the admissible recovery solutions.

Table 1. Actuator set and their characteristics

Actuators set	$\lambda_{\max}$
$\{a,b,c\}$	**19.6246**
$\{a,b\}$	$1.0747.10^3$
$\{a,c\}$	**19.7667**
$\{b,c\}$	**19.7667**
$\{a\}$	$1.0981.10^3$
$\{b\}$	$1.0981.10^3$
$\{c\}$	80.7268

6. CONCLUSION

This work studied a representation of an active fault tolerant control AFTC system within a hybrid system framework. The fault recovery was firstly viewed as a system property that can be guaranteed by the hybrid system's controllability. Then, the fault recoverability was studied based on an energy limitation and a second necessary condition was determined other than the control reconfigurability.

In future work, the hybrid formalism for AFTC systems will be used to study the temporal issue in AFTC and to find optimal diagnosis and reconfiguration delays to achieve AFTC performances optimization.

7. REFERENCES

[1] Veillette, R. 1992. Design of reliable control systems, IEEE Transactions on Automatic Control 37(3), pp. 290-304.

[2] Veillette, R. 1995. Reliable linear-quadratic state-feedback control, Automatica 31(1), pp. 137-143.

[3] Ferreira, P. 2002. Tracking with sensor failures, Automatica , 38(9), pp. 1621-1623.

[4] Chen, J., Patton, R., Chen, Z.1998. Lmi approach to fault tolerant control of uncertain systems. Proceeding of IEEE ISIC/CIRA/ISAS Joint Conference, Gaithersburg, MD, USA, pp. 14-17.

[5] Hamada, Y., Shin, S., Sebe, N. 1996. A design method for fault-tolerant control systems based on H1 optimization. Proceeding of the 35th Conference on Decision and Control, Kobe, Japan, pp. 1918-1919.

[6] Kanev, S., Verhaegen, M. 2008. Controller reconfiguration for non linear systems. Control Engineering Practice, pp.1223-1235.

[7] Diao, Y., Passino, KM. 2002. Intelligent fault-tolerant control using adaptive and learning methods. Control Engineering Practice, pp. 801-817.

[8] Blanke, M., Frei, C.W., Kraus, F., Patton, R.J. and Staroswiecki, M. 2000. What is fault-tolerant control, Preprints of 4th IFAC Symposium on Fault Detection Supervision ans Safety for Technical Processes, SAFEPROCESS.

[9] Blanke, M. 2001. Enhanced maritime safety through diagnosis and fault tolerant control, Proceeding of 5th IFAC Conference CAMS.

[10] Frei, W.C., Karus, F.J., Blanke, M. 1999. Recoverability viewed as a system property, Proceeding of European Control Conference.

[11] Zhang, Y.M., Jiang, J. 2006. Issues on integration of fault diagnosis and reconfigurable control in active fault tolerant control systems, 8th IFAC SAFEPROCESS, 1513-1524.

[12] Hamdaoui, R., Abdelkarim, M.N. 2011. Temporal analysis of actuator fault recovery based on optimal control, International Review of Automatic Control, vol 4, n°4.

[13] Hamdaoui, R., Ponsart, J.C., Theilliol, D. 2011. Actuator fault recovery study based on post-fault time analysis, Proceedings of 18th IFAC World Congress, Milano, 2011.

[14] Staroswiecki, M. 2003. Actuator faults and the linear quadratic control problem, 42nd IEEE Conference on Decision and Control, 959-965.

[15] Yang, Z. 2002. An algebraic approach towards the controllability of controlled switching linear hybrid systems, Automatica, vol 38, n°7.

[16] Yang, Z. 2006. Reconfigurability analysis for a class of linear hybrid systems, Proceedings of 6th IFAC safeprocess, Beijing, PR China.

[17] Lee, E.B., Markus, L. 1967. Foundations of optimal control theory, John Wiley, New York.

[18] Xu, X., Antsaklis, P.J. 2004. Optimal control of switched systems based on parameterization of the switching instants, Automatic Control, IEEE Transactions, Vol. 49, n°1.

[19] Maki, M., Jiang, J., Hagino, K.. 2004. A stability guaranteed active fault tolerant control system against actuator failures, International Journal of Robust and Nonlinear Control, Vol. 14, 1061-1077.