15th Triennial World Congress, Barcelona, Spain

# RECONFIGURABILITY OF FAULT-TOLERANT HYBRID CONTROL SYSTEMS

**Zhenyu Yang** *and* **David L. Hicks**

*Department of Computer Science and Engineering, Aalborg University Esbjerg, Niels Bohrs Vej 8, 6700 Esbjerg, Denmark, yang,hicks@cs.aue.auc.dk*

Abstract: A fundamental property of fault-tolerant systems, called reconfigurability, is discussed for a class of hybrid control systems based on the hybrid controllability concept. A faulty hybrid system is reconfigurable if it preserves the property of hybrid controllability under assumption that the nominal system is hybrid controllable. The approaches proposed in (Yang *et al.*, 1998; Yang and Blanke, 2000) for the analysis of hybrid controllability are extended for the reconfigurability analysis. In addition, the modelling of the faulty system and the functional redundancy are also discussed and illustrated by examples.

Keywords: Fault-tolerance, Reconfigurability, Hybrid Systems

## 1. INTRODUCTION

Fault-tolerance in control is the ability of a controlled system to maintain or gracefully degrade control objectives despite the occurrence of a fault. A large amount of work has been done for Continuous/Discrete-Time Dynamical Systems (C/DTDS) as reviewed by (Patton, 1997; Blanke *et al.*, 2001) and Discrete Event Dynamical Systems (DEDS) as the work done by (Sampath *et al.*, 1995). However, there is little work focusing on the fault-tolerance analysis of systems which contain a mixture of continuous/discrete-time and discrete-event dynamics.

A system with a mixture of continuous/discrete-time and discrete-event dynamics is usually referred to as a *Hybrid System (HS)* (Branicky *et al.*, 1998; Lemmon *et al.*, 1999; Tittus and Egardt, 1998). Based on the HS framework, (Blanke *et al.*, 2001) abstractly formalized the fault-tolerance problem as the procedure of solving the problem [**O**,**S**, **P**,**U**] based on a control objective **O**, a class of control law **U**, and a set (**S**,**P**) of possible structures and parameters. By focusing on the LTI systems which can be regarded as a kind of special HS, (Frei *et al.*, 1999) discussed recoverability using the controllability and observability gramians and (Wu *et al.*, 2000) explored control reconfigurability by using the second-order modes. However, these results can not be directly applied to general HS with respect to the mixture of two distinct dynamics in HS. Like most typical system properties, e.g., stability (Branicky *et al.*, 1998) and controllability (Tittus and Egardt, 1998; Yang and Blanke, 2000), the fault-tolerant properties need to be re-examined for hybrid systems. Since the general analysis often leads to an undecidable or NP-hard problem for hybrid systems (Bemporad *et al.*, 2000; Blondel and Tsitsiklis, 1999), here we focus on the reconfigurability analysis of a class of hybrid systems.

Reconfiguration means to change the input-output between the controller and plant through change of the controller structure and parameters, so as to maintain the original control objective(Blanke *et al.*, 2001). The reconfigurability can be evaluated according to different control objectives, such as satisfying some performance requirements or preserving some system properties. Motivated by the work in (Frei *et al.*, 1999; Blanke *et al.*, 2001), we discuss the configurability for a class of hybrid systems based on the hybrid controllability concept. The approaches originally proposed for hybrid controllability analysis in (Yang *et al.*, 1998; Yang and Blanke, 2000) can be extended for the reconfigurability analysis.

The rest of this paper is organized as follows: Section 2 introduces the HIOA as a formal model for the considered systems and discusses the fault scenario. Section 3 formulates the reconfigurability problem. Section 4 discusses the reconfigurability analysis. Section 5 presents some examples to illustrate the proposed approach. Finally, we conclude the paper in Section 6.

## 2. HIOA MODELLING

A kind of hybrid automata named *Hybrid Input/Output Automata (HIOA)* used in (Yang *et al.*, 1998; Yang and Blanke, 2000) is employed as the formal model of considered systems. Other similar formulations can be found in(Lemch *et al.*, 2001; Tittus and Egardt, 1998).

### 2.1 Hybrid Input-Output Automata - HIOA

**Definition 1**: A HIOA model is defined as a tuple

$$M \hat{=} \langle Q, X, U, \Sigma, \Delta, \Phi_X, \theta_0, D_X, \Gamma \rangle, \qquad (1)$$

where the components are:

• A set $Q$ of *discrete states* with $Q \hat{=} Q_p \times Q_c$, where $Q_p/Q_c$ denotes a set of *discrete internal/input states.*

• A set of *continuous variables* used to describe local continuous-time dynamics, which includes [1]: Piecewise continuous state (input) $X$ ($U$) with $X : T \mapsto X_D$ ($U : T \mapsto U_D$), where $T$ represents the time and $X_D \subseteq \mathcal{R}^n$ ($U_D \subseteq \mathcal{R}^r$).

• A set $\Sigma$ of *events*, where $\Sigma \hat{=} \Sigma_p \cup \Sigma_c$ and $\Sigma_p \cap \Sigma_c = \phi$. $\Sigma_p$ is a set of *internal events*, which represent all possible discrete actions triggered by the internal evolving mechanism of the controlled plant. $\Sigma_c$ is a set of *input events*, which represent all possible discrete inputs from the outside, such as those discrete activities triggered by the controller or environment. Within the HIOA model events belong to $\Sigma_p/\Sigma_c$ can not be synchronized, i.e.,$\delta \| \sigma \Rightarrow (\delta \in \Sigma_p \wedge \sigma \in \Sigma_c) \vee (\delta \in \Sigma_c \wedge \sigma \in \Sigma_p)$. Therefore, all discrete behaviors in HIOA$^+$ can be represented by $\Sigma_{\|} \hat{=} \Sigma \cup \{\delta \| \sigma \mid \delta, \sigma \in \Sigma\}$.

• A partial *transition function* [2] $\Delta : Q \times \Sigma_{\|} \mapsto Q$, which describes the transfer relationship between discrete states, e.g.,

$$\Delta((q_p, q_c), \sigma) \hat{=} \begin{cases} (q'_p, q_c), & \sigma \in \Sigma_p \\ (q_p, q'_c), & \sigma \in \Sigma_c \end{cases} \qquad (2)$$

• A partial *jumping function* $\Phi_X : X_D^{q\sigma} \times Q \times \Sigma_{\|} \mapsto X_D^{\sigma q'}$, which specifies the discontinuous jumps of continuous states when some event occurs, is defined as (assume $\sigma$ occurs at point $t$)

$$\Phi_X(X(t^-), q, \sigma) \hat{=} \begin{cases} X(t^+), \text{ where } \sigma \in \Sigma_p, \\ \Delta(q,\sigma) = q', X(t^-) \in X_D^{q\sigma}, \\ \text{and } X(t^+) \in X_D^{\sigma q'}. \\ X(t^+) = X(t^-) = X(t), \\ \text{where } \sigma \in \Sigma_c, \Delta(q,\sigma) = q', \\ \text{and } X(t) \in X_D^{q\sigma} \cap X_D^{\sigma q'}. \end{cases} \qquad (3)$$

Here $X_D^{q\sigma}$ is called the *jumping set* of transition $q \to q'$ and is defined as:

$$X_D^{q\sigma} \hat{=} \{x | x \in \Gamma_X(q), \text{ and } \Phi_X(x, q, \sigma) \in \Gamma_X(q')\}. \qquad (4)$$

$X_D^{\sigma q'}$ is the *reachable set* of transition $q \to q'$ and is defined as:

$$X_D^{\sigma q'} \hat{=} \{x | x \in \Gamma_X(q'), \text{ and } \exists x' \in \Gamma_X(q), \text{ satisfies } \Phi_X(x', q, \sigma) = x\}, \qquad (5)$$

where $\Gamma_X(q)(\Gamma_X(q'))$ is the projection of $\Gamma(q)(\Gamma(q'))$ into real space $X_D$.

• A set of *initial states* $\theta_0 \hat{=} (Q_0, X_0)$ with $Q_0 \subseteq Q$ and $X_0 \subseteq X_D$.

• A *continuous dynamic operator* $D_X : Q \mapsto (T \times X_D \times U_D \mapsto dX_D)$, is specified as:

$$D_X(q) : \dot{X}(t) = f_q(t, X(t), U(t)), \qquad (6)$$

with $X(t_{q_0}) = X_{q0}$.

• A *mode invariant function* $\Gamma : Q \mapsto X_D \times U_D$, which specifies the restrictions to the continuous state and input with respect to different discrete states. q$\hat{=}(q, X, U, D_X(q), \Gamma(q))$ is called a *mode of HIOA.*

### 2.2 Fault Scenario

Within hybrid systems, the system characteristics and parameters are classified into two distinct groups: those for continuous dynamic and those for discrete dynamic. Therefore, the fault modelling in hybrid systems need to be within the lines of these two groups.

From the description (1), it can be seen that the discrete dynamic of the considered system is

[1] In order to avoid the observability problem for hybrid systems, which is still open, here we assume all the continuous states can be observed directly.

[2] Here we only consider the deterministic case, the nondeterministic case can be defined similarly as the nondeterministic automaton.

described by sets $Q$, $\Sigma$ and function $\Delta$. Their relationship is constrained by some quantitative conditions in HIOA, which are expressed in (3) and related sets (4) and (5). For example, one internal event, denoted as $\sigma_p \in \Sigma_p$, is said to occur at some time in the HIOA model, if and only if at this point, the following two conditions are satisfied:

(1) $\exists q_1, q_2 \in Q_p, q_c \in Q_c$, such that $\Delta((q_1, q_c), \sigma_p) = (q_2, q_c)$; and
(2) $\exists x_1 \in X_D^{q_1\sigma_p}, x_2 \in X_D^{\sigma_p q_2}$, such that $\Phi_X(x_1, (q_1, q_c), \sigma_p) = x_2$.

The continuous dynamic of the considered system is described by (6), and further constrained by $\Gamma$. Within each mode, the system must keep the corresponding $\Gamma(q)$ *valid*, otherwise, the system will leave this mode and an internal event will be triggered.

With respect to the possible effect on different dynamics, faults in hybrid systems can be divided into different categories, such as:

• *Qualitative faults*: these kinds of faults only affect the discrete dynamic of the considered system, and they can be further distinguished as:

*(a) Completely Qualitative (CQ) faults*: With these kinds of faults, some events in $\Sigma$ or discrete states in $Q$ will disappear, or some new events or discrete states will appear after a fault occurs. For example, consider the gear shifting operation of an automobile power system. When some gear position can not be switched into due to some possible mechanical problem, then in the model of this faulty system, the corresponding discrete state of this gear position will disappear. In the HIOA framework, the disappeared events or states can be modelled as that the jumping set (4) and/or the reachable set (5) of the corresponding event or state intersect with the empty set.

*(b) Distorted Qualitative (DQ) faults*: these kinds of faults partially affect constraints of the discrete dynamic, i.e., they may distort some related jumping and/or reachable sets of some transitions, or distort the mode invariance $\Gamma(q)$ of some mode $q \in Q$, such that the discrete dynamic may change with respect to these changed constraints. For example, consider again the automobile power system, some gear position may lose some efficiency due to wear or a mechanical problem such that the vehicle speed can not reach the expected maximum within this position. That means the mode invariance corresponding to this position shrinks, like the relationship $\Gamma^f(q) \subset \Gamma(q)$. Within the HIOA framework, the DQ faults can be modelled as the intersection or union of related sets with some specific sets.

• *Quantitative faults*: These kinds of faults only affect the local continuous dynamic of the considered system, i.e., causing some deviations of characteristics of the dynamic description (6). The fault modelling methods for continuous dynamical systems can be used directly for modelling this kind of faults, such as (Patton, 1997).

• *Hybrid faults*: These kinds of faults combine the effects of the qualitative and quantitative faults together, i.e., they not only affect the continuous dynamic but also the discrete dynamic as well.

It can be observed that from the hierarchical point of view, the quantitative fault has a "local and low" effect on the system dynamic, the qualitative fault has a "global and high" effect while the hybrid fault has both effects together. In general, if we use the HIOA model

$$M^n \hat{=} \langle Q^n, X, U, \Sigma^n, \Delta^n, \Phi^n, \theta_0, D^n, \Gamma^n \rangle. \quad (7)$$

to denote the *nominal system*, then the *faulty system* can be obtained as

$$M^f \hat{=} \langle Q^f, X, U, \Sigma^f, \Delta^f, \Phi^f, \theta_0, D^f, \Gamma^f \rangle. \quad (8)$$

from $M^n$ through (i) deleting those discrete states from $Q^n$ within which all the reachable sets changed to be empty due to the fault(s) so as to get $Q^f$; (ii) deleting those events from $\Sigma^n$ for which the jumping set or reachable set becomes empty so as to get $\Sigma^f$; (iii) adjusting functions $\Delta^n, \Phi^n, D^n$ and set $\Gamma^n$ so as to fit the new sets $Q^f$ and $\Sigma^f$, and (iv) modifying the structure and/or parameters of (6) if necessary.

we make further assumptions about the considered systems with respect to the undecidable problem:

- All the input signals of the HIOA$^+$ are from the hybrid controller;
- Within any mode $\mathbf{q}$, any pair of jumping sets related to internal events if they exist, such as $\sigma_1, \sigma_2 \in \Sigma_p$, has the property $X_D^{q\sigma_1} \cap X_D^{q\sigma_2} = \phi$; and
- Within each mode $\mathbf{q}$, any pair consisting of a jumping set and a reachable set related to internal events, such as $\sigma_1, \sigma_2 \in \Sigma_p$, has the property $X_D^{q\sigma_1} \cap X_D^{\sigma_2 q} = \phi$.

## 3. RECONFIGURABILITY FORMULATION

Within the HIOA model, any hybrid state, denoted as $(q, x)$, is called a *valid state*, once $x \in \Gamma_X(q)$. Then we can have:

**Definition 2**(Yang and Blanke, 2000): Given two valid states $(q_0, x_0)$ and $(q_f, x_f)$, once a mode evolving process, denoted as

$$\alpha_\pi \hat{=} \langle (\mathbf{q}_{0_1} \rightarrow \mathbf{q}_{0_2} \rightarrow \cdots \rightarrow \mathbf{q}_{0_m}) \wedge \mathcal{U}_0 \lceil [t_0, t_1) \rangle \rightarrow$$

$$\langle(\mathbf{q}_{1_1} \rightarrow \mathbf{q}_{1_2} \rightarrow \cdots \rightarrow \mathbf{q}_{1_m}) \wedge \mathcal{U}_1\lceil(t_1, t_2)\rangle \rightarrow \cdots \rightarrow$$
$$\langle(\mathbf{q}_{n_{\pi 1}} \rightarrow \mathbf{q}_{n_{\pi 2}} \rightarrow \cdots \rightarrow \mathbf{q}_{\pi_m}) \wedge \mathcal{U}_{n_\pi}\lceil(t_{n_\pi}, t_{n_\pi+1})\rangle, \quad (9)$$

determined by an input (control) hybrid sequence, denoted as:

$$\pi \hat{=} \langle \mathcal{U}_0\lceil[t_0, t_1)\ \delta_1\ \mathcal{U}_1\lceil(t_1, t_2)\ \delta_2\ \cdots\ \delta_{n_\pi}$$
$$\mathcal{U}_{n_\pi}\lceil(t_{n_\pi}, t_{n_\pi+1})\rangle, \quad (10)$$

satisfies the conditions:

- $(q_f, x_f)$ can be reachable from $(q_0, x_0)$ within finite time, and
- $\Gamma(q_{i_j})$ is always satisfied when the system stays in $\mathbf{q}_{i_j}$ for $i = 0, 1, \cdots, n_\pi$ and $i_j = 1, 2, \cdots, i_m$, where $i_m$ are integers, $\mathbf{q}_{0_1} = \mathbf{q}_0$ and $\mathbf{q}_{\pi_m} = \mathbf{q}_f$.

Then $\pi$ in (10) is called a *Permitted Control Sequence (PCS) from* $(q_0, x_0)$ *to* $(q_f, x_f)$.

Here $\delta_i \in \Sigma_c$, and there is $\Delta(q_{(i-1)m}, \delta_i) = q_{i1}$ for $i = 1, \cdots, n_\pi$. $\mathcal{U}_i\lceil(t_i, t_{i+1})$ denotes a specific real-time regulation, such as a feedback control law $\mathcal{U}_i \hat{=} \mathcal{K}_i(X(t))$, which is executed within $(t_i, t_{i+1})$. $\langle(\mathbf{q}_{i_1} \rightarrow \cdots \rightarrow \mathbf{q}_{i_m}) \wedge \mathcal{U}_i\lceil(t_i, t_{i+1})\rangle$ denotes the case that the mode transition evolves from $\mathbf{q}_{i_1}$ to $\mathbf{q}_{i_m}$ within $(t_i, t_{i+1})$ and within all $\mathbf{q}_{i_1}, \cdots, \mathbf{q}_{i_m}$ the executing real-time regulation is $\mathcal{U}_i$.

**Definition 3**(Yang and Blanke, 2000): A HS is called *hybrid controllable*, once for any pair of valid states, there exists at least one PCS from the initial state to the final one.

Assume the nominal system $\mathcal{M}^n$ described by (7) is hybrid Controllable with respect to definition 3, then:

**Definition 4**: The faulty system $\mathcal{M}^f$ described by (8) is reconfigurable (with respect to controllability) if $\mathcal{M}^f$ is still hybrid controllable.

It is obvious that the reconfigurability is the ability of $\mathcal{M}^f$ to preserve the hybrid controllability. This definition seems a hard condition for discussions of LTI systems (Frei *et al.*, 1999; Blanke *et al.*, 2001; Wu *et al.*, 2000), but it will be seen through the following analysis and examples that for hybrid systems, this definition is reasonable with respect to the quite flexible structure and dynamics of hybrid systems.

## 4. RECONFIGURABILITY ANALYSIS

### *4.1 A Unified Approach towards Reconfigurability*

The unified approach proposed in (Yang and Blanke, 2000) for hybrid controllability can be used for the reconfigurability analysis directly. This approach contains of three steps:

*Step 1: Global Analysis in DEDS Level.* In this stage we just consider the reachability problem for discrete states, i.e., this analysis is under assumption that the evolving process of continuous-time dynamic (6) and the jumping function (3) already satisfy the properties required by this analysis. This analysis can be copied by any methods for reachability analysis in DEDS theory (Yang and Blanke, 2000).

*Step 2: Discrete-Path Searching Algorithm.* Due to the existence of a continuous-time dynamic within each mode, different paths with loops and different cyclic numbers may cause different reachability analysis results, such as examples in (Tittus and Egardt, 1998; Yang *et al.*, 1998). Therefore, this discrete-path searching algorithm need not only find all the possible minimum-size paths, but also find all the cyclic ones. The inputs required by this algorithm are: (a) number of discrete states $size(Q^f)$; (b) a vector $E \hat{=} [E_i]_{i=1,\cdots,size(Q^f)}$, each $E_i$ represents the number of arcs leaving from node $q_i$; (c) a path table $R = [r(i,k)]$, where $r(i,k)$ is the node number of the $k$th destination from $q_i$. The outputs are the minimum-size path array $P$ and cyclic path array $H$. The detailed description of this algorithm can be found in (Yang and Blanke, 2000).

*Step 3: Local Analysis in Quantitative Level.* This analysis considers the problem of whether the DES-reachability analyzed in step 1 and discrete-paths acquired in step 2 can be really implemented in the hybrid system level or not. We can see that the mode transition sequences corresponding to the found discrete paths have two kinds of forms: so-called *basic-sequences* (without any loops) and *cyclic-sequences*. The *iterative backward method* proposed in (Tittus and Egardt, 1998; Yang and Blanke, 2000) can be used for this examination. In the following, we propose a corresponding *iterative forward method* for this analysis.

Assume the initial and final valid states are given as $(q_1, x_1)$ and $(q_2, x_2)$. Firstly, consider a basic-sequence, which is denoted as a mode transition corresponding to a possible discrete path: $\alpha \hat{=} (\mathbf{q}_1 \rightarrow \mathbf{q}_{m1} \rightarrow \mathbf{q}_{m2} \rightarrow \cdots \rightarrow \mathbf{q}_{mn} \rightarrow \mathbf{q}_2)$. With respect to the continuous dynamic (6) in $\mathbf{q}_1$, a reachable set within mode $\mathbf{q}_1$ can be obtained as:

$$R_{q_1}(x_1) \hat{=} \{x | x \in \Gamma_X(q_1) \wedge (\exists U(t), t_f, \text{satisfying}$$
$$(X(t), U(t))\lceil[t_0, t_f] \in \Gamma(q_1) \wedge (t_0 \le t_f < \infty),$$
$$\text{such that } \varphi_1(t_f, U(t_f), x_1, t_0) = x)\}. \quad (11)$$

where $\varphi_1(t, U, X_0, t_0)$ is the solution of (6) with initial time $t_0$, state $X_0$ and operating real-time regulation $U(t)$ in $\mathbf{q}_1$. Then, a set called the *jumping set of transition* $\mathbf{q}_1 \rightarrow \mathbf{q}_{m1}$ *with respect to* $(q_1, x_1)$, denoted as $\Theta_1(x_1)$, can be defined as:

$$\Theta_1(x_1) \hat{=} R_{q_1}(x_1) \cap X_D^{q_1 \sigma_{1,m1}}. \quad (12)$$

Considering the function (3), the image set in $\mathbf{q}_{m1}$ of $\Theta_1(x_1)$ is:

$$\Omega_{m1}(x_1) = \{x|(x \in X_D^{\sigma_{1,m1}q_{m1}})\wedge$$
$$(\exists x' \in \Theta_1(x_1) \text{ such that } \Phi(x', q_1, \sigma_{1,m1}) = x)\}. \quad (13)$$

Then, within the mode $\mathbf{q_{m1}}$, a reachable set can be obtained as:

$$R_{q_{m1}}(x_1) \hat{=} \{x|x \in \Gamma_X(q_{m1}) \wedge (\exists U(t), t_f, x', \text{satisfying}$$
$$(X(t), U(t))\lceil[t_0, t_f] \in \Gamma(q_{m1}) \wedge (t_0 \le t_f < \infty) \wedge (x' \in \Omega_{m1}(x_1)),$$
$$\text{such that } \varphi_{m1}(t_f, U(t_f), x', t_0) = x)\}. \quad (14)$$

Actually, set $R_{q_{m1}}(x_1)$ contains all the possible states that are reachable from the set $\Omega_{m1}(x_1)$ within mode $\mathbf{q_{m1}}$. Therefore, similar to the analysis of mode $\mathbf{q_1}$, a jumping subset like (12) can be defined with respect to $\Phi$ as $\Theta_{m1}(x_1) \hat{=} R_{q_{m1}}(x_1) \cap X_D^{q_{m1}\sigma_{m1m2}}$. Then we can get the image set of this set in mode $\mathbf{q_{m2}}$ like the form (13). This analysis can proceed until we get the reachable set $R_{q_2}(x_1)$, which has the same formula as (14) instead of $\Omega_{mn}(x_1)$ by $\Omega_{m1}(x_1)$.

This forward analysis can also be used for the cyclic loop analysis. Then we have the fact that $(q_2, x_2)$ can be reached from $(q_1, x_1)$ by the considered system through the evolution sequence $\alpha$ if and only if $x_2 \in R_{q_2}(x_1)$.

**Proposition 5**: For two given valid states $(q_1, x_1)$ and $(q_2, x_2)$, $(q_2, x_2)$ can be reached from $(q_1, x_1)$ within the considered system within finite time if and only if:

(1) $q_2$ is reachable from $q_1$ in the DEDS level; and
(2) there exists at least one mode transition sequence corresponding to a reachable discrete path which satisfies $x_2 \in R_{q_2}(x_1)$.

Under assumption that the nominal system (7) is hybrid controllable, then:

**Theorem 6**: The faulty system (8) is reconfigurable (with respect to the controllability) if and only if for any arbitrary valid $(q_1, x_1)$ and $(q_2, x_2)$ of (8), $(q_2, x_2)$ can be reached from $(q_1, x_1)$ within finite time.

**Proof**: Follow definition 3, 4 and proposition 5.

Specially, when considered faults have some specific characteristics, the proposed analysis procedure can be simplified. For example, when the considered fault is a kind of DQ fault, the first and second step are not necessary in the reconfigurability analysis, and within step three only those reachable sets like (11) and (14) related to the faulty modes need to be reanalyzed. The same situation exists for the consideration of quantitative faults. However, when a hybrid-fault occurs, all three steps need to be performed.

When the considered system has some specific characteristics, some further results can be obtained, such as for controlled-switching linear systems(Yang *et al.*, 1998).

### *4.2 Reconfigurability of Linear Switched Systems*

Consider a class of linear switched systems (LSS), denoted as:

$$\begin{cases} \dot{x}(t) = A(\sigma(t))x(t) + B(\sigma(t))u(t), \\ y(t) = C(\sigma(t))x(t) \end{cases} \quad (15)$$

where the state $x(t) \in R^n$, (controllable) input $u(t) \in R^m$ and output $y(t) \in R^p$. $\sigma(t) : R^+ \mapsto N$ is a piecewise constant switching function mapping from $R^+$ to an integer set $N$. Matrices $A(\sigma), B(\sigma)$ and $C(\sigma)$ are piecewise constants depending on values of $\sigma$. We further assume the system satisfies the following: (i) $\sigma(t)$ is left-continuous, and any time interval within which $\sigma(t)$ is constant is no less than a *dwelling time* (Liberzon and Morse, 1999); (ii) the switching time and corresponding destination of switching of $\sigma(t)$ both can be determined by the control design, as well as the continuous-time control signal $u(t)$ within each selected mode; and (iii) there is no discontinuous state jumps during mode switches. A sufficient condition for the controllability of LSS was proposed in (Yang *et al.*, 1998) and it can be extended for the reconfigurability analysis.

When some fault(s) happens in the considered nominal system, which can be denoted as $M^n \hat{=} \{(A_i, B_i)\}_{i=1}^q$, the faulty system can be denoted as $M^f \hat{=} \{(A_i^f, B_i^f)\}_{i=1}^q$. Then, we have:

**Theorem 7**: System $M^f$ can be reconfigured with respect to the considered fault if:

$$W_C^f \hat{=} [W_1^f \ \cdots \ W_q^f] \hat{=} [B_1^f \ \cdots \ (A_1^f)^{n-1}B_1^f$$
$$\cdots \ B_q^f \ \cdots \ (A_q^f)^{n-1}B_q^f]. \quad (16)$$

is of full row rank.

**Proof**: Follow the theorem in (Yang *et al.*, 1998).

If some fault happens such that some mode will disappear from the nominal system, and we assume that the subsystem $(A_q, B_q)$ can not appear in the faulty system, then:

**Theorem 8**: System $M^f$ can be reconfigured with respect to the considered fault if:

$$W_C^f \hat{=} [W_1 \ \cdots \ W_{q-1}] \hat{=} [B_1 \ \cdots \ A_1^{n-1}B_1$$
$$\cdots \ B_q \ \cdots \ (A_{q-1})^{n-1}B_{q-1}]. \quad (17)$$

is of full row rank.

**Remark 9**: If $M^f$ satisfies the condition in theorem 7 or 8, it can be noticed that the nominal

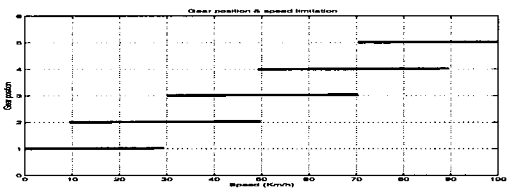

Fig. 1. Gear position vs Speed Limitation

system $M^n$ has ***dual functional redundancy*** with respect to the considered fault. Similarly, if the faulty system can still preserve the controllability when a further subsystem is isolated, we say the nominal system has ***triple redundancy*** with respect to the considered fault. If the above properties are always true when the isolated subsystem(s) is any subsystem of (15), then we say $M^n$ has dual/triple redundancy.

## 5. ILLUSTRATIVE EXAMPLES

We consider an automobile power system with gear shifting operation as our first example. Assume the gear-position-vs-speed-limitation as shown in Fig.1. With respect to the detailed description of this system, it can be observed that the nominal system is hybrid controllable. When a fault happens such that the gear stick can not switch into one position, The faulty system has only four modes available in comparison to the five modes in the nominal system. However, this faulty system is still hybrid controllable through the proposed analysis, i.e, this faulty system is reconfigurable. When the gear is stuck in some position, it can be seen that this faulty system is not reconfigurable with respect to the speed limitation periods, which correspond to the set of mode invariance.

In the second example, we consider a binary-mode LSS, whose parameters under nominal case are:

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, B_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}. \; A_2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, B_2 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

It can be checked that the nominal system is hybrid controllable. When some fault happens such that in mode-1 the matrix $B_1$ changes to be $B_1 \hat{=} [1\ 0\ 0]^T$, i.e., the second actuator is out of order. Through the proposed approach for reconfigurability analysis, it can be observed that this faulty system is reconfigurable with respect to this considered fault.

## 6. CONCLUSIONS

Based on the hybrid controllability concept, the reconfigurability regarded as a kind of system property is discussed for a class of hybrid control systems. The faulty system can be reconfigured with respect to the considered faults if it preserves the nominal property about hybrid controllability. A unified approach for the reconfigurability analysis is proposed and some further results are obtained for a class of linear switching systems. Finally, some examples are provided to illustrate the proposed approaches.

## REFERENCES


Bemporad, A., G. Ferrari-Trecate and M. Morari (2000). Observability and controllability of piecewise affine and hybrid systems. *IEEE Automatic Control* **45**(10), 1864–1876.

Blanke, M., M. Staroswiecki and N.E. Wu (2001). Concepts and methods in fault-tolerant control. In: *Proc. of ACC01.*

Blondel, V.D. and J.N. Tsitsiklis (1999). Complexity of stability and controllability of elementary hybrid systems. *Automatica* **35**(3), 479–490.

Branicky, Michael S., Vivek S. Borkar and Sanjoy K. Mitter (1998). A unified framework for hybrid control: Model and optimal control theory. *IEEE Automatic Control* **43**(1), 31–45.

Frei, C.W., F.J. Kraus and M. Blanke (1999). Recoverability viewed as a system property. In: *Proc. of ECC99.*

Lemch, E.S., S. Sastry and P.E. Caines (2001). Global controllability of hybrid systems with controlled and autonomous switchings. pp. 375–386. Number 2034 In: *LNCS*. Springer-Verlag.

Lemmon, M.D., K.X. He and I. Markovsky (1999). Supervisory hybrid systems. *IEEE Control Systems* **19**(4), 34–41.

Liberzon, D. and A. S. Morse (1999). Basic problems in stability and design of switched systems. *IEEE Control Systems* pp. 59–70.

Patton, R.J. (1997). Fault-tolerant control: The 1997 situation. In: *IFAC SafeProcess'97*. pp. 1033–1055.

Sampath, M., R. Sengupta and S. Lafortune (1995). Diagnosability of discrete-event systems. *IEEE AC* **40**(9), 1555–1574.

Tittus, M. and B. Egardt (1998). Control design for integrator hybrid systems. *IEEE Automatic Control* **43**(4), 491–500.

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

Yang, Z. and M. Blanke (2000). A unified approach for controllability analysis of hybrid control systems. In: *Proc. of IFAC CSD2000.* Bratislava, Slovak Republic. pp. 158–163.

Yang, Z., M. Verhaegen, Y.J. Wang and Z.J. Chen (1998). Hybrid controllability of linear switched systems. In: *Proc. of 37th CDC.* Tampa,FL, USA. pp. 3920–3925.