Chapter 1
Fault Tolerant Control and Hybrid Systems

Both research areas of fault tolerant control (FTC) and hybrid systems (HS) have been developed separately for several decades, and fruitful results appeared respectively. However, until now, the FTC problem of HS has not yet attracted enough attention, and needs to be investigated due to its academic meaning as well as practical one. Many modern complex systems have to be modeled by HS and their safety and reliability are quite important. This naturally motivates to study FTC for HS, which is the topic of this book. In this chapter, we shall describe the relations between HS and FTC, and present some examples of HS as well as their fault behaviors. Based on these examples, we formulate the problems to be solved in this book.

1.1 Background

1.1.1 Hybrid Systems

HS are dynamical systems that often consist of continuous time (CT) and/or discrete time (DT) processes interfaced with some logical or decision-making (LDM) process. The continuous/ discrete time (C/DT) component may consist of differential/difference equations or continuous/discrete time state models. The LDM component might be a finite automaton or a more general discrete event system. The C/DT processes affect the state transitions of the LDM, and the LDM processes affect the dynamic motions of the C/DT processes [22, 80]. The study of HS is motivated by the fundamentally hybrid nature of many real life systems, e.g., circuit systems, flight management system, process control and intelligent transportation systems. Over the last decade, significant progress has taken place in modeling and simulation [80], verification [122], [46], stability [22], [47] and controller synthesis [110], [123] for HS.

The HS considered in this book can be illustrated using Fig.1.1, which consists of a series of continuous/discrete time modes (*N* maybe a finite or infinite number) and a switching logic. These modes are switched among each other according to a switching law generated from the switching logic. The framework in Fig.1.1 is general and covers several different kinds of HS that have different switching properties

H. Yang et al.: Fault Tolerant Control Design for Hybrid Systems, LNCIS 397, pp. 1–9.
springerlink.com

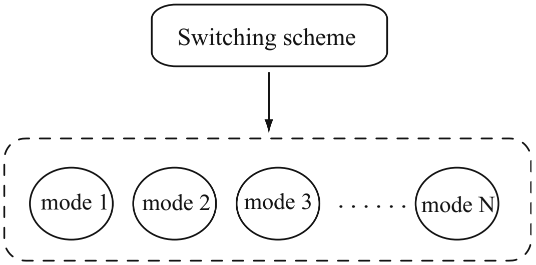

Fig. 1.1 The HS model

or performance requirements. Let us take three interesting examples which will be discussed in details in the following chapters.

Example 1.1: [138] A simplified CPU processing control system is shown in Fig.1.2. The key control problem is to deal with the trade-off between the high-speed computing and the physical constraints. The CPU needs to operate at high clock frequency (voltage) to realize high-speed computing, while a high clock frequency spends much energy and raises the CPU temperature, which often leads to hardware trouble.

The system is naturally modeled as a HS with two modes.

Mode 1 (busy mode): the amount of CPU tasks is large while CPU temperature is not too high.

Mode 2 (usual mode): the amount of CPU tasks is not large and more energy is used for decreasing the temperature.

A state dependent switching law could be designed i.e., switching occurs when the temperature or the amount of CPU reaches some given values.

Example 1.2: [140] A hose insertion task shown in Fig. 1.3 is a typical example of manipulation of deformable objects. The fingertip of the robot arm inserts a deformable hose on the plug. The motion of the hose and the fingertip are restricted in $x_1 - x_2$ plane. The completed work is to insert the hose onto the plug. Such task

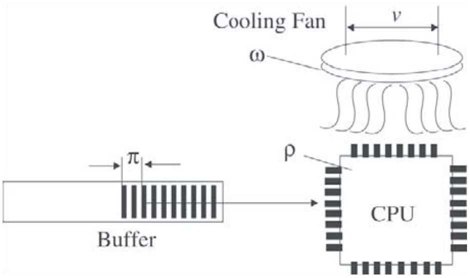

Fig. 1.2 The CPU model

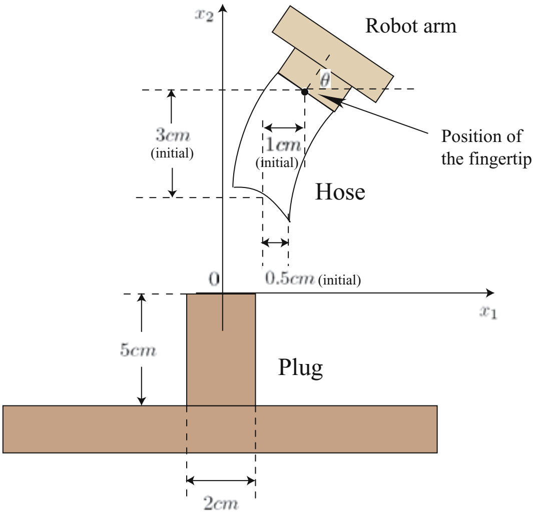

Fig. 1.3 Hose insertion task

can be modeled as a HS according to different contact configurations between the hose and the plug when the fingertip is at different positions.

Example 1.3: [139] Consider a traffic flow control problem in intelligent transportation systems at the terminator of the bridge, where six roads are interconnected with the bridge, as in Fig. 1.4. The roads r_1^{out}, r_2^{out} and r_3^{out} are the output roads to which the autonomous vehicles (AVs) go from bridge, whereas the roads r_1^{in}, r_2^{in} and r_3^{in} are the input roads from which AVs go to the bridge. There is a supervisor consisting of a series of internal logic lights (similar to traffic lights for man-driven cars) for input roads, such that the traffic flows from each input roads get into the bridge with the prescribed sequence. The overall system is also a hybrid system involves the interaction of continuous (AVs flows) and discrete dynamics (traffic lights).

It can be seen from the above examples that the structure of HS is very special and complex, the analysis of fundamental properties of HS is also difficult and quite different from that of the non-hybrid systems. This is because both continuous and discrete dynamics and their relations have to be fully taken in account. The general models of HS include hybrid automata [80], hybrid inclusions [42], and switched systems [48]. These modes capture both continuous and discrete dynamics of HS, under which some properties of HS can be analyzed systematically.

The stability and performance of HS are related to many factors including the initial states, the decreasing rate of Lyapunov function of each continuous mode, the frequency of switching, the switching sequence, etc. Two basic stability methods can be applied: multiple Lyapunov functions (MLFs) technique [22, 13, 156] and dwell-time scheme [72, 125, 129]. MLFs method claims that the stability of HS can be achieved if the value of each mode's Lyapunov function 1) does not increase

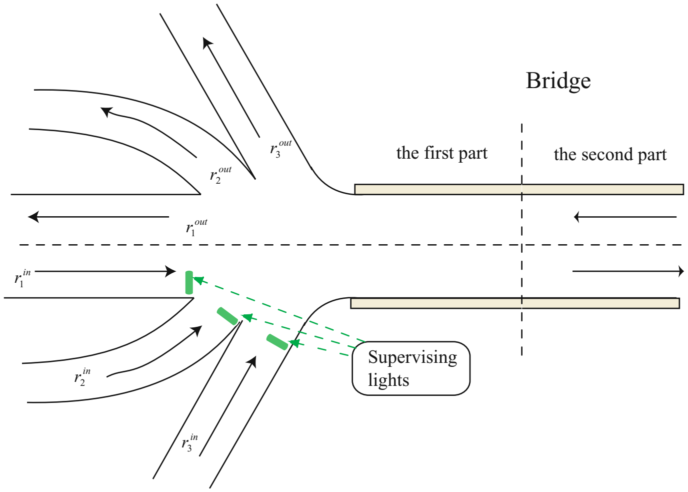

Fig. 1.4 One terminator of the bridge

when the mode works and 2) is non-increasing over the consecutive time sequence when the corresponding mode is just switched on. The dwell-time scheme introduces a minimum time interval called “dwell time”, and claims that the HS is stable if the interval between any two consecutive switching instants is not smaller than the “dwell time”. The above two methods have been extended to HS with various switching properties and stability requirements.

The control design of HS consists of continuous controller design in each continuous mode and switching scheme design (e.g., switching instants design, switching sequence design, this is also called “discrete controller design” [122]). The former one is similar to that for non-hybrid systems. Each continuous mode can often be stabilized by its corresponding continuous controller. However, the individual stability of each mode is not enough to make HS stable. The latter one is special and more required for HS, which plays an important role to stabilize the HS globally.

It will be shown throughout the book that the above two stability methods are the basis of FTC design for HS, and both controller design clues will be followed. The reader is refer to several excellent survey papers [22, 42] for the analysis of other interesting properties of HS which is not closely related to the topic of the book and thus is omitted here.

1.1.2 Fault Tolerant Control

Faults in automated processes will often cause undesired reactions and shut-down of a controlled plant, and the consequences could be damages to technical parts of the plant or to its environment, so fault diagnosis (FD) and FTC are highly required for modern complex control systems. FD is concerned with detecting, isolating and estimating the faults [18, 23, 36, 95], while Fault Tolerant Control (FTC) aims at guaranteeing the system goal to be achieved in spite of faults [10, 54, 154].

In the past 30 years, fruitful results have been obtained in the area of FTC. Generally speaking, FTC can be categorized into two main classes: passive and active. Passive FTC is designed with the consideration of a set of presumed failure modes. The resulting control system performance tends to be conservative. It also has the limitation to deal with unanticipated faults. In contrast, Active FTC reacts to the occurrence of system faults on-line in real-time in an attempt to maintain the overall system stability and performance. Two main potential advantages of Active FTC are 1) the ability to deal with previously unknown faults with explicit FD and controller reconfiguration, and 2) the possibility to achieve the optimal performance. The reader are referred to [154] for more detailed development and bibliography.

1.2 FTC Problems of HS

Although the FD problem for HS has been addressed in some literatures recently using Petri net technique in [155], bond graphs method in [90], observer techniques in [126], and parity space method in [20], etc., until now, few results have been reported about FTC for HS.

It is well known that the stability of HS is achieved under quite rigorous conditions as stated previously. Most of existing results are devoted to off-line analysis and design, such that the HS works well as what is expected. However, faults may abruptly change system behavior, FTC strategy must be applied on-line to keep the system performance including stability of the HS in spite of faults. This prevents many classic FTC methods for non-hybrid systems from being applied to HS.

Two main kinds of faults have been defined for HS [20] with respect to the process (C/DT or LDM) that is affected by : One is a *continuous fault* that affects each continuous system mode, which corrupts the continuous state behavior of the related mode. Recall example 1.1, if there exists a fault in voltage input channel or clock frequency input channel, the system behavior may become unexpected in busy mode or usual mode. Another one is a *discrete fault* that affects the switching sequence. In example 1.2, if there exists an abrupt change of the fingertip's position due to physical faults of the robot arm, the prescribed motion sequence may be changed. In example 1.3, the discrete faults represent the unexpected behaviors of traffic lights, whereas the continuous faults describe the abnormal situations of AVs flows.

Now we define a general HS model with faults.

Definition 1.1. *A* hybrid automaton with fault *is a collection*

$$\mathscr{H} = (Q, X, U, V, \mathscr{F}, Y, \digamma, Init, Inv, E, G, R) \tag{1.1}$$

where

- *$Q = \{1, 2, \ldots, N\}$ is the finite set of discrete states;*
- *X is the set of continuous states;*
- *U defines the set of continuous inputs;*
- *V defines the set of discrete inputs;*

- *$F = F_c \cup F_d$ denotes the set of faults, with F_c and F_d respectively, continuous and discrete.*
- *$\mathscr{F}$: $Q \times X \times U \times F_c \rightarrow X$ represents the set of vector fields for each mode;*
- *Y is the set of continuous outputs;*
- *Init $\subseteq Q \times X$ is the set of initial states;*
- *Inv: $Q \rightarrow 2^X$ assigns to each mode an invariant set;*
- *$E : V \times F_d \rightarrow Q \times Q$ is the set of discrete transitions between modes;*
- *$G : E \times F_d \rightarrow 2^X$ defines a guard set related to each $(i, i') \in E$, where the system can be switched from mode i to i'.*
- *$R : Q \times Q \times X \rightarrow X$ is the set of reset maps.*

The above model is an extension of usual hybrid automaton as in e.g., [80] and [46] to the faulty cases. This model is also more general than that in [155] where only the parameter faulty cases are considered.

It can be seen from model (1.1) that

- Continuous faults F_c corrupt the equality constraints of the related mode. Such kind of faults are similar to that considered in non-hybrid systems.
- discrete faults F_d affect the mode transitions by changing discrete transition set E or the guard sets G. Both the switching instants and switching sequences may be changed unexpectedly. Such faults are special for HS.

The FTC objective for HS is concerned with the system requirement, i.e., to guarantee the system goal to be achieved in spite of continuous and discrete faults. In this book, two main system requirements are considered:

- Continuous performance goal, e.g., the origin of the HS is stable (Lyapunov stable, asymptotical stable, input-to-state stable) and the output regulation/tracking problem is solvable.
- Discrete specification goal, i.e., the HS has to satisfy some constraints on discrete modes, e.g., the switching sequence.

To investigate continuous performance goal, a class of HS (1.1) named switched systems are considered which take the form

$$\begin{aligned} \dot{x} &= g_\sigma(x, u_\sigma, f_\sigma) \\ y &= h_\sigma(x) \end{aligned} \tag{1.2}$$

where $x \in X$, $u_\sigma \in U$, $y \in Y$, $f_\sigma \in F_c$. $\sigma(t) : [t_0, \infty) \rightarrow Q$ denotes the *switching function*, which is assumed to be a piecewise constant function continuous from the right. The *dwell period* of a mode represents the time period during which this mode is activated. The switched system model (1.2) emphasizes the vector fields $\mathscr{F}$ in (1.1), and captures the behavior of continuous dynamics using ordinary differential equations. The affect of the switching on each continuous mode is also clearly represented. Such model allows us to analyze FTC problems using continuous system theories, and to extend the existing FTC techniques of non-hybrid systems to the hybrid cases.

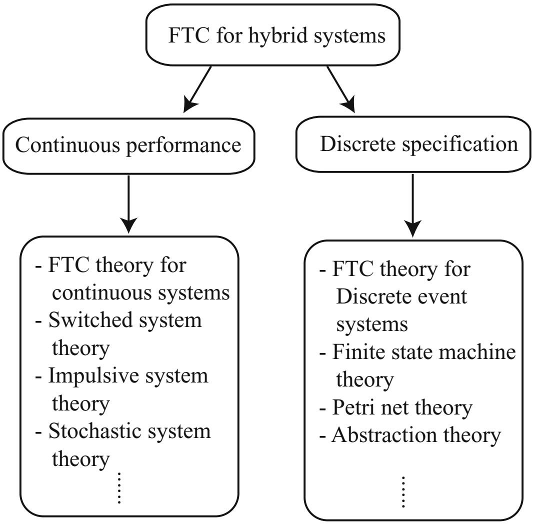

Fig. 1.5 The FTC clue for HS

Four kinds of switchings are considered:

- *Time-dependent switching*. Such switching occurs at a certain time instant. These switching instants can be prescribed *a priori* and fixed, or designed arbitrarily by engineers. The continuous states x are continuous at switching instants.
- *State-dependent switching*. Such switching occurs whenever the states reach some given surfaces or satisfy an inequality. x are also continuous at switching instants.
- *Impulsive switching*. Under such switching, x abruptly change due to the impulse effect at each switching instant.
- *Stochastic switching*. Such switching is governed by some random processes, i.e. Markov process.

The above various switchings are related with the guard set G, the discrete transitions set E and the reset maps set R in (1.1), which determines switching properties of system (1.2). As for above different HS, the continuous performance can be investigated using various continuous system theories as shown in Fig 1.5. Some existing FTC results for non-hybrid systems could be potentially applied and combined with the stability conditions of HS. The main idea is to design the FTC law in each faulty mode and develop an appropriate switching scheme such that the continuous performance goal is maintained.

As for the discrete specification goal, one natural idea is to reconfigure the discrete part of the HS after faults occur to maintain such specification. The continuous system theories are limited in this case. However, the discrete-event system (DES) supervisory control theories can be applied as also indicated in Fig. 1.5.

A well known DES model named finite state machines will be utilized to abstract the discrete part of (1.1) as

$$(Q, E, T_d, Q_{d0}, Q_{dm})$$

where T_d denotes the activated discrete transition, $Q_{d0} = \bigcup_{\forall(x,q)\in Init} q$. $Q_{dm} \subseteq Q$ is the set of marked states. Such mode captures the behavior of discrete dynamics. The affect of the switching sequences is particularly emphasized. DES supervisory control theory [101] can be developed to reconfigure the switching sequence after faults occur, which, together with some criteria imposed on continuous dynamics of HS, achieves the discrete specification goal.

Another important HS model named Hybrid Petri net (HPN) originating from the DES model Petri net (PN) are also considered. HPN inherits all the advantages of the PN and effectively captures behaviors including concurrency, synchronization and conflicts, which often appear in complex systems, e.g., the traffic flow control problem in example 1.3. A HPN structure is the 5-tuple

$$(P, T, Pre, Post, h)$$

where P is a set of places, T is a set of transitions; The set of places P (resp. transitions T) is split into two subsets: discrete places (resp. discrete transitions) and continuous places (resp. continuous transitions). *Pre* and *Post* assign the weights between transitions and places. More detailed formulations will be given in Section 5.2. HPN is closely connected with hybrid automaton (1.1), a hybrid automaton can be constructed associated with a given HPN as reported in [109]. Different control schemes can be designed for continuous part and discrete part of HPNs respectively such that the desired discrete specifications are maintained.

One of the motivations of HS research arises from the hybrid control problem. HS may present different control configurations. Commutation from one configuration to another one is described using discrete event system model as claimed in [117]. Thus the controlled system becomes hybrid due to the switching control. Some novel supervisory FTC techniques are also developed based on HS methods to improve non-hybrid (linear and nonlinear) performance during FTC period. The hybrid automaton model (1.1) can be applied after a minor modification, where each mode denotes respectively faulty or healthy situations of the system. All the switching among modes can be controlled by the user. The discrete fault disappears.

1.3 The Structure of the Book

The rest of this book is organized as follows: Chapters 2-3 provide new theoretical developments of FTC analysis and design for HS with time-dependent and state-dependent switchings respectively. Chapter 4 discusses the HS with impulsive and stochastic switchings based on some results in Chapter 2. These new approaches are based on continuous system theories and FTC goals aim at maintaining the continuous performance. The switched system model (1.2) is utilized in Chapters 2, 4

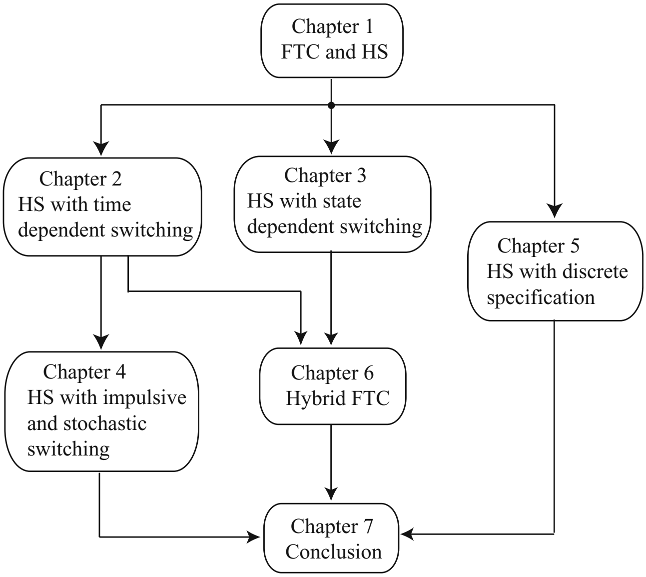

Fig. 1.6 The chapter relations

and Section 3.3. Chapter 5 considers the HS with discrete specifications, FTC issue is addressed from DES point of view and the discrete specification goal is emphasized. HPNs model is applied in Section 5.2. The Hybrid automaton model (1.1) is considered in Sections 3.2 and 5.1. As an important related issue of HS, supervisory control problems are addressed in Chapter 6, some new supervisory FTC results are reported based on HS approaches developed in Chapters 2-3. A four-wheel-steering and four-wheel-driving electric vehicle in LAGIS laboratory is particularly focused on whose actuator faults are analyzed systematically and the hybrid fault tolerant tracking control approach is applied. In the final Chapter, several future research directions are predicated related to FTC of HS.

Fig.1.6 shows the relations among chapters. One can follow the arrowhead sequence to read the book. the reader who is interested in continuous system FTC theories can read Chapters 2, 3 and 4. The reader who focuses on supervisory control can read Chapters 2, 3 and 6. Chapter 5 is independent from Chapters 2-4 and 6, the reader who cares about DES only can read Chapter 5 directly.