Vol.31, No.1 ACTA AUTOMATICA SINICA January, 2005

Fault-tolerant Control Systems—An Introductory Overview[1)]

Jin Jiang[1,2]

[1](*Department of Electrical & Computer Engineering, The University of Western Ontario, London,*
Ontario, N6A 5B9 Canada)

[2](*Faculty of Electrical & Electronics Engineering, East China Jiaotong University,*
Nanchang 330013 *P.R.China*)

(E-mail: jjiang@eng.uwo.ca)

Abstract This paper presents an introductory overview on the development of fault-tolerant control systems. For this reason, the paper is written in a tutorial fashion to summarize some of the important results in this subject area deliberately without going into details in any of them. However, key references are provided from which interested readers can obtain more detailed information on a particular subject. It is necessary to mention that, throughout this paper, no efforts were made to provide an exhaustive coverage on the subject matter. In fact, it is far from it. The paper merely represents the view and experience of its author. It can very well be that some important issues or topics were left out unintentionally. If that is the case, the author sincerely apologizes in advance. After a brief account of fault-tolerant control systems, particularly on the original motivations, and the concept of redundancies, the paper reviews the development of fault-tolerant control systems with highlights to several important issues from a historical perspective. The general approaches to fault-tolerant control has been divided into passive, active, and hybrid approaches. The analysis techniques for active fault-tolerant control systems are also discussed. Practical applications of fault-tolerant control are highlighted from a practical and industrial perspective. Finally, some critical issues in this area are discussed as open problems for future research/development in this emerging field.

Key words Fault-tolerant control, redundancies, safety-critical systems

1 Introduction

Modern technological systems rely heavily on sophisticated control systems to meet increased safety and performance requirements. This is particularly true in safety critical applications, such as aircraft, spacecraft, nuclear power plants, and chemical plants processing hazardous materials, where a minor and often benign fault could potentially develop into catastrophic events if left unattended for or incorrectly responded to. To prevent fault induced losses and to minimize the potential risks, new control techniques and design approaches need to be developed to cope with system component malfunctions whilst maintaining the desirable degree of overall system stability and performance levels. A control system that possesses such a capability is often known as a Fault-Tolerant Control System (FTCS).

It is important to emphasize that the key to any FTCS is the existence of system redundancies. Different design methods are merely the reflection of different philosophies in utilizing and managing such redundancies. For this simple reason, it should be emphasized that fault-tolerant control may not be suitable for any application, as redundancies always come at additional cost for extra components and with added inconvenience, such as increased weight, size, and not to mention about the cost of maintenance in the life span of these additional components. Clearly, one has to seriously analyze the problem at hand to justify the use of fault-tolerant control systems.

In any FTCS, the desirable degree of fault tolerance, the amount of required redundancies, and the potentially achievable system performance are all closely related. Considering the following scenario: suppose in an extreme, one would like to maintain the performance of a system unconditionally even in the presence of the most serious faults, it goes without saying that the system would require a significant

1) Supported by Natural Sciences and Engineering Research Council of Canada (NSERC)
Received July 29, 2004; in revised form September 10, 2004

amount of redundancies to meet this demand. Of course, the resulting system is very fault-tolerant, but at a high cost, because, by definition, redundancies are those system capabilities that are not usually required during the normal operation. On the contrary, the other extreme is that there exists no redundancy or any other safety margins in the system, any minor failure in system components would result in a total collapse of the system. The problem dealt with in fault-tolerant control systems is clearly somewhere in between these two extremes.

In order to maintain a certain level of performance in the event of system component failures, the system must possess some degrees of redundancies. However, physical and financial constraints often put utmost limits on the installed redundancies. Therefore, a viable solution is to reduce the demand on the performance whenever necessary if a fault has occurred in the system. Only the most essential part of the system is maintained. In fact, for a well engineered system, faults should be regarded as rare events rather than a common occurrence. Clearly, from a practical point of view, there is a fine line between the cost invested and the potential benefit gained. Generally speaking, from a fault-tolerant control viewpoint, more redundancies can potentially be translated into better fault-tolerance abilities. However, more redundancies will inevitably increase the complexity of the fault-tolerant control system design and implementation process.

Since the performance of a control system is very much dependent on the power and the maneuverability of the existing control actuators, so far as the control system performance is concerned, the actuators pose the utmost bounds on the achievable performance. One has to be very careful not to over-work the remaining actuators in the presence of some actuator faults, because they could very well be the only link to the survival of the entire system by keeping the system controllable. The remaining actuators should be wisely used normally to steer the system to a safe state, rather than for the completion of the mission.

Sensors are other important devices in a control system. Failures in sensors will inevitably lead to wrong control decisions, which can endanger the safe operation of the entire system. Fortunately, sensors themselves are passive devices in the sense that they do not directly participate in the control actions, rather than provide information needed for the controllers and actuators. Therefore, it is often possible to employ multiple sensors and cross-check each other's operational status to increase the overall reliability of the measurement system. It is also the trend in industries nowadays to adopt so-called "smart" sensors with self-validation and self-diagnostic capabilities. As far as the FTCS is concerned, faults in actuators are more difficult to deal with, as actuators/controllers affect the system behaviors directly. Therefore, more efforts will be placed on the FTCS against actuator failures in this paper.

The paper is organized as follows: In Section 2, the development of different aspects of fault-tolerant control systems is examined with a historical perspective. Some examples of industrial practice of fault-tolerant control techniques are briefly discussed in Section 3. Some open problems and their potential solutions are summarized in Section 4 with some future perspectives. Finally, the conclusion is drawn in Section 5 with a list of key references.

2 Development of fault-tolerant control systems: A historical view

It is important to emphasize that the design philosophy for a fault-tolerant control system is very different from that of a conventional control system. In a conventional control system design, one would not usually treat the robustness against component failures as an explicit part of the design specifications. Therefore, a design may achieve excellent performance during the normal operation, but may fail terribly even in the event of a minor malfunction in system components. On the contrary, one of the most important considerations in a FTCS design is how to maintain the system stability and acceptable level of performance in the presence of system component failures (however rare they may be). This difference in design philosophy could lead to complete different systems in the end. In addition, the different design approaches will also dictate the different resources needed, *i.e.* redundancies for FTCS. Redundancies can be in hardware or analytical forms, such as redundant sensors/actuators, or fault detection/diagnosis schemes. Their existence certainly adds to the degree of freedom in the overall control system, but they also compound the design complexity and increase the cost associated with the implementation. Clearly, this is a problem of balance between the safety and the cost. Nevertheless, it goes without saying that a properly designed fault-tolerant control system should operate satisfactorily not only in the absence but also in the presence of system component failures.

2.1 General approaches to fault-tolerant control systems

Depending on how the redundancy is being utilized, existing efforts in FTCS design can be classified into two main approaches: passive and active. In a passive approach, the conceivable system component failures are assumed to be known *a priori*, and the control system takes into account of all these failure modes in the design stage. Once the control system is designed (if it exists), it will remain fixed during the entire system operation. Even in the event of component failures, the control system should still be able to maintain the designed performance. In other words, in a passive FTCS, one has to ensure that the control system works under all possible system operating scenarios that have been considered at the design stage, including potential component failures. However, nothing can be said about the behavior of the system in the presence of un-anticipated failures. The system performance could very well be unacceptable in these cases.

Because a passive FTCS has to maintain the system stability under various component failures, from the performance viewpoint, the designed controller has to be conservative. From typical relationships between the optimality and the robustness, it is very difficult for a passive FTCS to be optimal from the performance point of view alone.

In contrast, an active FTCS reacts to the system component failures actively by properly reconfiguring its control actions so that the stability/performance of the entire system can still be acceptable. To achieve a successful control system reconfiguration, this approach relies heavily on a real-time fault detection/diagnosis scheme for the most up-to-date information about the status of the system and the operating conditions of its components. The critical issue facing any active FTCS is that there is only a limited amount of reaction time available to perform fault detection and diagnosis and control system reconfiguration. The speed, the accuracy, and the robustness of these schemes are the factors to the success of any active FTCS. If designed properly, an active FTCS will be able to deal with unforeseen faults and will have the potential to achieve optimal performance for different system operating scenarios.

Since the entire system rests on the integrated performance of both the on-line and real-time fault detection/diagnosis scheme and the real-time decisions on the control system reconfiguration, the real-time issue becomes one of the most important considerations in design and implementation of an active fault-tolerant control system. Given the fact that only a limited amount of time and information may be available, it is potentially likely that nature and the exact location of the faults may not be accurately pinpointed out for an active FTCS to act on in case of a rapidly developing fault, it would be highly desirable if one could have a FTCS that possesses the guaranteed stability property as in a passive FTCS, but also with the performance optimization attribute as in an active FTCS. This is the main motivation behind the recent development on hybrid fault-tolerant control systems by combining both active and passive approaches.

Because of the random nature of faults, their detection/diagnosis, and the corresponding control actions, it is generally less straightforward to evaluate the performance of an active fault-tolerant control system in a deterministic manner. Considerable amount of research work has been carried out to quantify faults, characteristics of fault detection/diagnosis schemes, and real-time control system reconfigurations as stochastic processes. The performance of an active FTCS can then be viewed as the result of interactions among these stochastic processes. Under this framework, the stochastic stability of active fault-tolerant control systems can be investigated.

In the next several sub-sections, the development of various types of fault-tolerant control systems will be examined in more detail with citation of key references.

2.2 Development of passive fault-tolerant control systems

Early efforts on passive fault-tolerant control were mainly concentrated on using multiple not-so-reliable controllers to achieve a reliable control system. In late 1970s and early 1980s, a multiple disjoint decentralized control structure was initially studied theoretically[1] Even though it has not been explicitly defined, clearly the redundancy lies in the employment of multiple controllers. Decentralized state feedback approaches were used to synthesize these multiple controllers. Naturally, it was shown that the reliability of the resulting control system could be improved beyond that of using an individual controller alone. Hence, fault-tolerance is achieved. There are two very important concepts in this early work: redundancy and decentralized control (often referred to as distributed control now).

It is important to emphasize that one of the necessary conditions for using a multiple controller structure is that the system should possess multiple actuators. From a theoretical point of view, a dynamic system with multiple actuators is naturally described by a multi-input system. The issues associated with redundancies and its potential use were examined in the frame of multivariable control systems. The concept of system integrity against system component failures was introduced[2]. The integrity of the control system means that the closed-loop system remains stable in the event of loop component failures. This concept has been adopted as a very important design criteria in the subsequent development of passive fault-tolerant control systems. Necessary and sufficient conditions for multivariable control systems possessing integrity against sensor failures and sensor/actuator failures have been derived in [3] and [4], respectively, based on stable coprime factorization approaches.

Theoretically, it is possible to tailor some of the existing control system design techniques to passive fault-tolerant control systems by incorporating the concept of redundant control elements. One of such examples is based on linear quadratic optimal control. A simple design approach against actuator failures was developed by solving a Riccati-type equation and using a state feedback controller implementation[5]. The stability of the system can be maintained in the presence of any combination of actuator failures. The same authors have re-examined the same problem in the frequency domain by using the transfer function matrix approach, where a necessary and sufficient condition for systems possessing integrity has been derived in terms of the return difference matrix[6]. A similar problem was also solved by means of a matrix Lyapunov equation in [7]. The similar problem has also been examined briefly from the LQR viewpoint in [8]. It should be noted that, because the methods rely on Riccati-type or Lyapunov equations, they are only applicable to open-loop asymptotically stable systems. By restricting the modes of actuator failures to a specific known set, a linear quadratic controller design approach was proposed in [9], which can handle both stable and unstable open-loop systems.

An illustrative diagram of a passive FTCS is shown in Fig. 1, where the diagonal matrix L represents the status of the actuator channels. The null value in the i-th diagonal element simply means that the i-th actuator channel has failed, and the control signal cannot get through to the system from that particular channel. A passive FTCS design problem becomes to synthesize a controller so that the closed-loop system is stable for any combination of the failure elements in L.

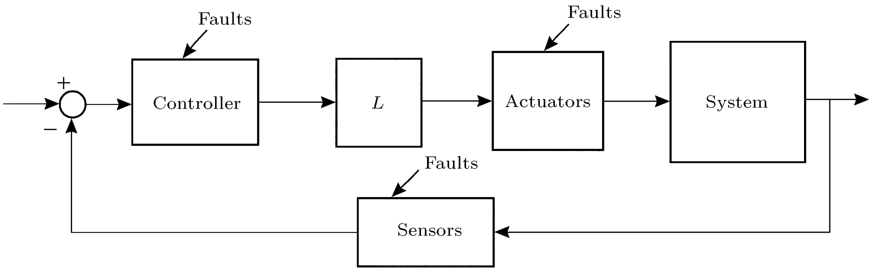

Fig. 1 Structure of passive fault-tolerant control systems

The problem of FTCS against actuator failures has also been investigated in [10] based on H_2 optimization. It has been shown that one can trade some H_2 performance for robustness against actuator failures. Design issues related to the centralized and decentralized fault-tolerant control systems with the guaranteed stability and H_2 norm-bounding have been discussed in [11] for a pre-specified set of sensor and actuator failures, where the performance of the control system in the event of component failures is measured in terms of H_∞ norm bounds. This design approach has further been extended to discrete systems using the δ operator methodology[12].

When a system component fails, it will definitely induce changes in the system. These changes can, of course, be described by failure induced parameter variations in the system. If a control system can be designed to be insensitive to these parameter changes, the fault-tolerance is then achieved. This line of reasoning has lead to the development of passive fault-tolerant control systems based on parameter space approach [13,14]. This is basically a graphically-oriented approach. With proper choice of the controller structure and other system parameters, a closed-loop system can be made insensitive to certain class of sensor and actuator failures. Even though the method can produce a passive fault-tolerant control, it generally suffers from the lack of physical meaning associated with the redundancies and the role that these redundancies play in the design and operation of the system.

If failures are only restricted to the control channels, the design of a passive FTCS can also be dealt with mathematically as a reliable stabilization problem[15], in which a set of controllers are designed to stabilize a single system. In other words, any controller in the set or a combination of them will be able to stabilize the system. This is particularly useful in dealing with controller failures. Obviously, the multiple controllers are the redundancies in such a control strategy. The dual to this reliable stabilization problem is known as simultaneous stabilization in which a single controller can be synthesized to stabilize multiple systems[16]. In the context of FTCS, the multiple systems may correspond to a single system but with different component failure modes. Unfortunately, the performance aspects of such approaches have not been incorporated in these methods.

With an improved understanding of the roles that redundant actuators play in a dynamic system, a new approach to the design of passive FTCS against actuator failures has been developed[17]. For the first time, the concept of actuator redundancies is formally introduced by linking the redundant actuators to the controllability of the system. Recognizing that different actuators have different effects to the system, the concept of dynamic pre-compensator has been proposed which equalize the dynamic properties from each actuator channel to the system output (can differ by a scaling factor at the most). Hence, it makes the design of a passive fault-tolerant control much simpler. The advantage of this approach is that the physical meaning and the role that each actuator plays become transparent in the design process and during operation. This scheme can be applied to open-loop unstable systems as well. By incorporating an PI (Proportional and Integral) control action, it is shown that this design approach can maintain not only the closed-loop stability, but also the steady-state tracking ability in the presence of actuator failures[18]. In literature, passive fault-tolerant control is also known as "reliable control".

2.3 Development of active fault-tolerant control systems

Historically, a significant amount of research on active fault-tolerant control systems was motivated by flight control systems for aircraft. As a safety-critical system, the objective is to incorporate some "self-repairing" capabilities into the on-board flight control system so that the plane can make a safe landing in the event of component failures[19]. Such an effort was accelerated in part by two accidents involving commercial aircraft in the late 1970s. One case is the Delta Airline Flight 1080 (on April 12, 1977)[20,21], one of the elevators became jammed at 19 degrees up and this malfunction was unfortunately not known to the pilot at the time. Fortunately, based on his flying experience and availability of other redundant actuations on this L-1011 aircraft, the pilot successfully reconfigured the remaining control elements and landed safely. The second case is the ill-fated American Airlines DC-10 (Flight 191, on May 25, 1979), post accident analysis has indicated that the pilot had about 15 seconds to react to the failure. If a corrective action had been taken, the plane could have been saved[21]. Obviously, under such emergency situations, an automated fault-tolerant control system could have been extremely useful to alleviate the stress endured by the pilots and the diagnostic information could have been more effectively utilized to secure the plane. For military aircraft, the concept of active fault-tolerant control is also very attractive in dealing with battle damages over enemy territories[22].

In contrast to a passive FTCS, instead of relying on a fixed controller for all conceivable situations, an active FTCS reacts to the diagnosed failures by exercising the controls accordingly (again through proper manipulation of redundancies) so that the system stability can be maintained and the performance still be acceptable[23]. In many circumstances, a compromise has to be made to accept a degraded performance in the presence of failures due to the limited amount of redundancies. In the literature, active fault-tolerant control systems are sometimes also known as self-repairing control[19], reconfigurable[24], restructurable[25].

Typically, an active FTCS is composed of the following sub-systems as shown in Fig. 2: a) fault detection/diagnosis scheme; b) controller reconfiguration mechanism, and c) reconfigurable controller. All three sub-systems have to work in harmony within the real-time constraint to achieve an effective active fault-tolerant control system.

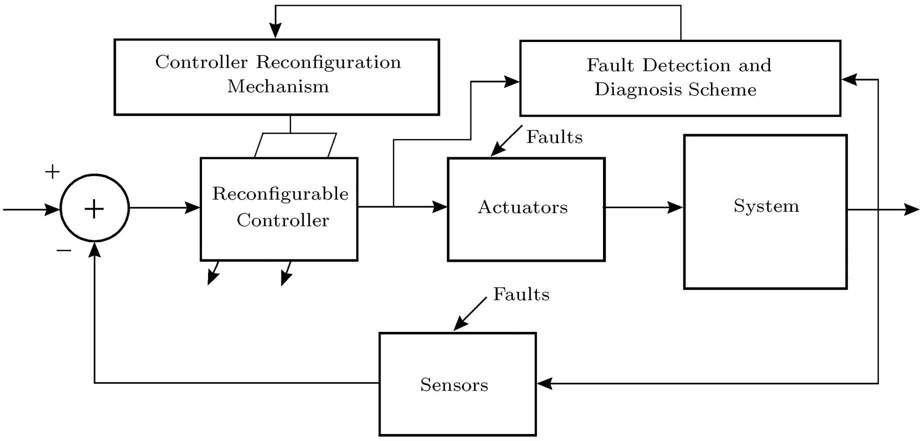
Controller Reconfiguration Mechanism
Fault Detection and Diagnosis Scheme
Faults
+
−
Reconfigurable Controller
Actuators
System
Faults
Sensors

Fig. 2 Structure of active fault-tolerant control systems

As far as the reconfigurable controller is concerned, it is usually a digital controller whose parameters and/or structure can be easily varied as directed by the controller reconfiguration mechanism. The working principle is very much like gain-scheduling controls except that the scheduling variable is the decision from the controller reconfiguration mechanism. In the literature, the research efforts on active fault-tolerant control systems have primarily been focused on: (i) fault detection/diagnosis schemes, and (ii) control system reconfiguration mechanisms. As a matter of fact, a significant amount of research has been accomplished in both areas. In comparison, relatively little work has been done to integrate the developed techniques from these two areas together to form an effectively active fault-tolerant control system.

So far as the controller implementation is concerned, there are generally two approaches: one is to design a pool of controllers off-line and stored in a database, based on the diagnostic decisions from the fault detection/diagnosis scheme, the most appropriate controller can be selected to be realized by the reconfigurable controller[24]. The other approach is to synthesize new controllers on-line in real-time. Clearly, the former is more restrictive with respect to the type of faults being able to deal with, and the latter poses an even more challenging proposition as time is an essence in dealing with faults in real-time.

A tremendous amount of work has been done in the area of fault detection/diagnosis in the last three decades. Many techniques have been developed, even though not all of them are initially geared towards active fault-tolerant control systems. The basic idea in any fault detection/diagnosis scheme is to compare the expected system behavior against the real observed one. The difference, often known as a residual, can then be used to assess the system operating condition and to flag faults in the system. The differences among various approaches lie in the way how the expected system behavior is characterized. In general, the existing techniques can be categorized as: (i) model-free; and (ii) model-based schemes. Since the design of a reconfigurable control system relies heavily on the post-fault model of the system, model-based techniques are most appropriate in this application.

Essentially, in a model-based fault detection/diagnosis scheme, one utilizes the mathematical models to quantify the expected behaviors of the system. The quantities often used are the system states, the system parameters, and the system input and output consistences. These three quantities naturally lead to three model-based fault detection/diagnosis techniques: (i) state estimation; (ii) parameter estimation; and (iii) parity equations. Several excellent surveys are available on these subjects[26~30]. In the context of FTCS, the performance of different techniques has also been compared. It was found that the state estimation based schemes are most suitable for fault detection since they are inherently fast by properly placing observer poles and have the least time delay in fault detection. However, the diagnostic information on the fault is generally not detail enough for the controller reconfiguration mechanism to use. Fortunately, parameter estimation based schemes provide an excellent complement. Thus, a combination of the state and the parameter estimation schemes have been found to be the most adequate in many FTCS applications[31].

So far as the controller reconfiguration mechanism is concerned, a lot of research has been carried out under the assumption that a perfect model of the post-fault system is already available (presumably from fault detection/diagnosis schemes), and the task of the reconfigurable control is simply to stabilize the post-fault system and to recover the original system performance as much as possible based on the post-fault system model. Certainly, the availability of the post-fault system model is a big assumption. It is seldom the case that the post-fault model is completely known. It will be shown in the later part of this section that the model uncertainties resulting from fault diagnosis processes have also been considered recently. The reported work on active FTCS dates back to 1985 when an automatic redesign approach was developed to accommodate the control element failures for a commercial aircraft[25] by redistributing the control authority of the failed control surfaces to the remaining ones.

From the point of view of performance recovery in the presence of component failures, a pseudo-inverse based controller reconfiguration method has been examined in [32]. A necessary modification to the original scheme is made so that the stability of the closed-loop system after the reconfiguration can be maintained. One advantage of the pseudo-inverse method is its simplicity in computing the reconfigured feedback controller gain matrix. By embedding the desired post-fault system performance into a reference model, a novel reconfigurable control system design using the perfect model following principle has also been proposed[33]. It is interesting to show that there is an inherent connection between the perfect model following and the pseudo-inverse approach. To ensure the closed-loop stability in the presence of component failure and to maximize the performance recovery, an eigenstructure assignment based algorithm has been developed under the state and output feedback configurations[34] as an alternative to the pseudo-inverse approach. In this approach, the stability is always guaranteed, eigenvalues and eigenvectors of the post-fault system can be placed such that the optimal performance recovery is obtained.

For a given system, if the component failures can be characterized by a finite set of failure modes, the system can be described by a set of dynamic models, known as multiple models. Based on such a multiple model representation, Maybeck and co-workers have developed adaptive control algorithms to deal with anticipated component failures[35]. The theoretical aspects of such a multiple model based adaptive control has further been examined[36]. If the actuator failures can be represented in terms of loss in their effectiveness, an integrated active fault-tolerant control system can be designed based on an Interacting Multiple Model (IMM) approach[37].

The philosophy of an integrated FTCS design is essentially to integrate all three parts of an active fault-tolerant control system in one design cycle. It is shown[38] that the simultaneous state and fault parameter estimations can be a very useful tool in this situation as it provides the latest information on the fault as well as on the state variables for feedback control. Based on the knowledge of the fault, an eigenstructure assignment based reconfiguration control technique can be used to recover the system performance as much as possible.

There are many other approaches to active fault-tolerant control system design, for example, based on Linear Matrix Inequality (LMI)[39,40], artificial neural networks[41], and intelligent controls [42∼45]. Recently, the concept of fault-tolerant control has also been extended to nonlinear systems[46,47].

Since the performance of the reconfigured system, in the presence of faults, is limited by the degree of available system redundancies, it is naturally reasonable (and often a good practice) to accept some level of performance degradation so that only the most essential aspects of the system properties can be maintained, such as stability and basic maneuverability. This is often known as graceful performance degradation. The design of active fault-tolerant control systems with graceful performance degradation has been formulated recently[48] by introducing normal and degraded system models. It has been shown that, with this approach, the remaining heathy actuators do not have to be over-stretched. The reduction in performance also involves lowering the command control input levels adequately.

Even though an active FTCS has the potential to produce less conservative performance, the entire fault detection/diagnosis and real-time control actions have to be accomplished within a finite time interval. In addition, consequences of an incorrect control decision can be even more frightening. As for safety critical systems, there is normally margin for any errors. In this regard, a passive FTCS may have its edge over an active FTCS. As a matter of fact, the most desirable technique would be the one which shares the merits of both passive and active approahces. This is exactly what a hybrid fault-tolerant control system tries to achieve.

2.4 Development of hybrid fault-tolerant control systems

The bottleneck in any active FTCS is the real-time fault detection/diagnosis scheme. Since it has to operate in a real-time environment with a limited number of measurements, which are often corrupted by noise, it is quite possible that a wrong decision could be made, or a correct decision but with considerable time delay. Time delay is very undesirable in any feedback control system, it is even more critical if the open-loop system is unstable. In the context of reconfigurable control, it was shown that excessive time delay in fault detection/diagnosis scheme will contribute adversely to the stability and the performance[49]. In a worst case, it can pose some serious safety risks. One of the solutions to such a problem is to employ a passive FTCS to provide the stability cushion and to use an active FTCS to further improve the system performance. This is basically the idea behind hybrid fault-tolerant control systems. If designed properly, a hybrid FTCS will be able to provide both the stability and optimal performance with the stability taking the precedence.

Even though the effect of imprecise fault detection/diagnosis on the overall performance of a active FTCS was examined earlier[50,51], the development of stability guaranteed hybrid fault-tolerant control systems is relatively recent. A newly developed stability guaranteed fault-tolerant control system framework is proposed in [52]. The method has a multiple controller structure, and relies on LMI optimization to deal with conflicting requirements among stability, redundancy, and graceful performance degradation. It has been shown, therein, that the stability of the closed-loop system is always ensured regardless the decision made by the fault detection/diagnosis scheme. However, a correct decision will further lead to optimal performance for the closed-loop system. The number of passive controllers is equal to the number of independent actuators, and there is always a low bound on the performance for the closed-loop system.

2.5 Analysis of fault-tolerant control systems

It is easily conceivable that the fault occurrence time is likely random in a practical system. So are the disturbances and the measurement noise, which will make the outcome of the fault detection/diagnosis scheme also non-deterministic. In turn, this will lead to a non-deterministic response in the active fault-tolerant control system. As a matter of fact, if the random nature in each part of the system can be characterized by separate random processes, the dynamic behavior of the entire system can be adequately described, on an average sense, in terms of mathematical expectations. Hence, the stochastic stability of the active FTCS can be defined and subsequently analyzed. Two Markov processes were used to represent respectively the failure of the system components and the behavior of the fault detection/diagnosis decisions in [53] where the mean square and the almost-sure asymptotic stability in probability are considered for the closed-loop system under random fault assumptions. In fact, the above idea has been further extended in a great detail in a recently published monograph[54].

Very recently, a concept of fault coverage is defined in a probabilistic framework[55]. This concept allows direct application of reliability concepts to the analysis of fault-tolerant control systems, and it even provides guidance to minimize the risk for system level failures.

For any practical safety critical systems, detailed reliability evaluations often have to be conducted both at the planning stage as well as during the course of system operation. The reliability of the associated fault-tolerant control system is also being examined at the same time from safety, reliability, redundancy and maintenance points of view[56]. Standard tools are available to carry out such analysis, for example, Failure Mode and Effect Analysis (FMEA) or fault tree and event tree analysis[57]. In fact, detailed safety and risk analyses are often an important part of the licensing process required from the regulatory agencies, such as FAA (Federal Aviation Administration) for aircraft, and NRC (Nuclear Regulatory Commission), CNSC (Canadian Nuclear Safety Commission) for nuclear power plants in the United States and Canada, respectively.

3 Fault-tolerant control from an industry perspective

It is interesting to mention that, although theoretical development in fault-tolerant control systems is still being perfected, the very same concept is certainly not new to industries. In fact, there are many fault-tolerant control techniques ranging from rudimentary to advanced ones that have been in practice for many years. These techniques are often based more on some engineering ingenuities than on rigorous mathematical foundations. However, they have played important roles in our society and daily lives.

In process industries, measurement/control signals are usually transmitted using standard 4 to 20 mA signal lines. One of the significance in using 4 mA, rather than 0 mA, as the low signal limit is to provide an inherent fault-tolerance against broken wires. In other circumstances, for the same capacity, three smaller pumps are often preferred over a large pump to provide better fault-tolerance in case pump failures. It is also a common practice that multiple sensors and transmitters are placed in strategic locations to measure the same process critical variables followed by a voting scheme to enhance the fault tolerance against sensor failures.

In computer laboratories, UPS (Uninterrupted Power Supplies) have been widely adopted as back-up (redundant) power sources in case the regular power source fails so that the important data can be saved. It is also a common practice to resort to Diesel engine powered backup generators in hospitals and key financial and information facilities to provide uninterrupted service (at least for a while) in case of power outages. Fault-tolerant control schemes employed herein could be as simple as some comparison circuits with high speed switches. Nevertheless, they offer a robust means to ensure safety under contingencies.

On board commercial jets or inside nuclear power plants, there are several layers of redundancies to provide ample protections to the key parts of the system, such as power source. In industries, the concept of these multiple layer protection is often known as “defense-in-depth”. The redundancies in each layer are mutually independent of one another to provide added protection against failures of the redundancies themselves.

In other safety critical systems, such as an elevator, broken cables or loss of power will not lead to serious consequences thanks to the safety brakes invented by Otis some 150 years ago. In many practical applications, a fault-tolerant control can be just as simple as a common sense. In nuclear reactor shutdown systems, the shutdown rods are suspended by electromagnetic devices upside down. The loss of on-site and off-site power will automatically release the rods into the reactor to shut it down safely. Any other orientation for the rods would not have the same level of fault-tolerance, as the gravity is always at presence.

In aerospace applications, the concept of redundancy has been utilized widely. Modern commercial airliners use multiple engines. A single engine is generally all it requires to land the aircraft safely. But with a single engine, the plane will not be flying as fast or as high as with multiple engines. Clearly, this is a classic example of the relationship between the redundancy and performance. Failure of some engines will not pose any immediate threat to the safety, but will have a direct effect on the attainable performance. In aerospace systems, such as satellites or space shuttles, multiple control computers are often utilized. Each system is developed independently by different teams with different tools and hardware techniques to minimize the potential risks of common mode failures.

Process control industries have been a major driving force behind industrial applications of fault-tolerant control systems. The fault-tolerance capability has been improved by moving from centralized control systems to distributed ones. Every major process control system providers, Honeywell, Siemens, Emerson, and Triconex can now provide various levels of fault tolerance. In particular, Triconex has developed systems based on a triple modular redundant (TMR) architecture using two-out-of-three voting to provide high integrity. By employing ring-shaped communication networks, the system basically achieves the capability of no single point of failure, as a break of the ring will not affect the data communications among distributed controllers. In addition, "smart" sensors and actuators which are capable of self-checking and self-verifications have become increasingly popular in process industries.

In view of the relationships among redundancy, safety and performance, one industry practice is to over-design the system to sacrifice some potential performance for safety margins. This is a typical case involving electrical power transmission. In fact, the amount of power transmitted over existing high voltage transmission lines never exceeds 35% of the thermal limit of the lines. The main reason is to provide enough safe margin to ensure that the power system stability is maintained in the even of failures (often short circuits) in the system.

In practice, before construction and commission of any safety-critical systems, detailed analysis and stress tests must be carried out in advance. One of such analyses is known as Probabilistic Safety Assessment (PSA), in which detailed propagations of the initial faults (called events) leading to the potential failures of the system are mapped out with associated probabilities. Such analysis will reveal vulnerabilities in the system by identifying potential safety hazards and design deficiencies. It has a very close relationship to fault-tolerant control system design in the sense that, once the vulnerabilities are identified, additional redundancies can be incorporated to strengthen the system and to reduce the potential risks.

It is also important to note that, once a system is in operation, the problem of fault-tolerant control will be closely related to the issue of maintenance. Different maintenance schemes for redundant systems have been developed and are in use in industries. The reliability of the redundant safety systems and the overall risks during the maintenance period are all important issues that have been considered by industry not only from productivity point of view but from safety ones.

4 Open problems and future perspectives

It might be evident from the materials presented in Sections 2 and 3 that there seems to be a considerable gap between the theoretical developments and practical applications of fault-tolerant control. The fact of matter is that many theoretical developments can be viewed as generalization from industrial practice. Many practical implementations also rely heavily on the theoretical developments. Clearly, fault-tolerant control is an engineering art as much as an engineering science. There are many unanswered questions and future prospects waiting to be explored. Some of these issues are discussed briefly in this section as challenges and future perspectives.

(a) Passive fault-tolerant control

One of the key problems in a passive fault-tolerant control system is how to effectively deal with a large number of fault scenarios and in the meantime to minimize the conservativeness of the resulting controller. As the number of potential failure scenarios increases, the overall performance of the controller becomes less and less effective for each fault. Obviously, it may not be a sensible approach to design a single controller for all conceivable failure modes. Instead, a better approach might be to group the likewise failures and then to apply distributed control technology to deal with them in groups. Clearly, this is one step towards an active FTCS.

So far, most of the existing work in passive fault-tolerant control has concentrated more or less on stability (or integrity) issues only. However, the stability alone is generally not enough for practical applications. It is also important to incorporate the performance (as well as graceful performance degradation) aspects of the system into the design process. This is still a wide open area for future research.

(b) Active fault-tolerant control

Although an active fault-tolerant control system has the potential to deliver optimal performance, however, the performance is only meaningful when the stability of the system is secured first. To ensure the closed-loop system stability, quality fault detection/diagnosis information and an effective reconfigurable control scheme have to work together within a guaranteed response time interval. This time interval usually depends on the operating conditions of the system prior to the fault. Therefore, there is always an upper bound for this interval, over which the system may not be able to recover. In general, a slower dynamic system tends to be more tolerable to failure as the rate of fault propagation is also slower. In other words, the critical time interval in this case would be relatively longer. One potential solution to deal with this critical time issue is to extend this time interval so that the good quality fault detection/diagnosis and control reconfiguration can be obtained. This is often known as "buying time". In fact, the hybrid fault-tolerant control system discussed in Section 2.4 is based exactly on this principle. By using passive fault-tolerant control, this critical time interval is extended effectively to give the active fault-tolerant control part a chance to further improve the performance. However, this is only a very preliminary result. Significantly more efforts are needed to further the research in this area.

(c) Common challenges and future perspectives

There are some issues and challenges that are common to all fault-tolerant control techniques. The most notable one is how to deal with actuator saturation in the presence of actuator faults. There are generally two philosophies to deal with this situation: (i) by re-balancing the control efforts among the remaining healthy actuators; and (ii) by reducing the overall performance level accordingly to cope with the outage of some actuators. However, there is a lack of systematic approaches to deal with such issues. Similar work exists in the literature on how to design and analyze control systems with actuator saturations[58]. It would be very interesting to see how one could extend these techniques into fault-tolerant control systems.

Generally speaking, the strength and the future of fault-tolerant control lie in its applications. A general question that everyone would like to ask is how can the fault-tolerant control techniques discussed in Section 2 be better utilized in practice? Are we on the right track as far as practical applications are concerned? To answer these questions satisfactorily, academic researchers and industrial practitioners have to work together to explore and to extend the existing techniques to practical applications. The power and benefit of fault-tolerant control can be enormous.

5 Conclusions

This paper presents a brief overview of the existing work on fault-tolerant control systems from several different viewpoints: theories, industrial practices, and potential challenges. In summary, as an emerging area in the field of automatic control, there are still a lot of work that remains to be done in this area. Because the research on this subject involves many areas across several different fields, cautions should always be exercised to ensure that there is always a clear objective on the desired level of system safety/fault-tolerance as well as those carefully identified physical constraints when designing new fault-tolerant control systems. In the wake of widespread applications of computers, particularly computer network technologies in safety-critical systems, fault-tolerant control systems will no longer be restricted to local loops or to a small number of sensors/actuators. A more system approach should be adopted with a full account of the recent advancement in distributed control technologies. To increase the safety and reliability of engineering systems and processes, the research topics should be motivated by applications and the results are for the applications. Academic researchers and industrial practitioners have to work closely together in order to harness the power that fault-tolerant control technologies yet to offer.

References

1 Siljak D D. Reliable control using multiple control systems, *International J. Control*, 1980, **31**(2): 303~329

2 MacFarlane A G I. Complex Variable Methods for Linear Multivariable Feedback Systems, Taylor and Francis Ltd. London, 1980

3 Sule V R. Design of feedback controllers with integrity, *Control Theory and Advanced Technology*, 1991, **7**(2): 285~299

4 Gundes A N. Stability of feedback systems with sensors or actuators failures: analysis. *International J. Control*, 1992, **56**(4): 735~753

5 Shimemura E, Fujita M. A design method for linear state feedback systems possessing integrity based on a solution of a Riccati-type equation, *International J. Control*, 1985, **42**(4): 887~899

6 Fujita M, Shimemura E. Integrity against arbitrary feedback-loop failure in linear multivariable control systems, *Automatica*, 1988, **24**(6): 765~772

7 Shieh L S, Dib H M, Ganesan S, Yates R E. Optimal pole-placement for state-feedback systems possessing integrity. *International J. Systems Science*, 1988, **19**(8): 1419~1435

8 Joshi S M. Design of failure-accommodation multiloop LQG-type controllers, *IEEE Transactions on Automatic Control*, 1987, **32**(8): 740~741

9 Veillette R J. Reliable Linear-quadratic state-feedback control, *Automatica*, 1995, **31**(1): 137~143

10 Colaneri P, Geromel J C, Locatelli A. Control Theory and Design, Academic Press, Toronto, 1997

11 Veillette R J, Medanic J V, Perkins W P. Design of reliable control systems, *IEEE Transactions on Automatic Control*, 1992, **37**(3): 290~304

12 Shor M H, Perkins W R, Medanic J V. Design of reliable decentralized controllers: a unified continuous/discrete formulation. *International J. Control*, 1992, **56**(4): 943~965

13 Siljak D D. Parameter space methods for robust control design: A guided tour, *IEEE Transactions on Automatic Control*, 1989, **34**(7): 674~688

14 Ackermann J E. Robust Control: Systems with Uncertain Physical Parameters, Springer-Verlag, New York, 1993

15 Vidyasagar M, Viswanadham N. Reliable stabilization using a multicontroller configuration, *Automatica*, 1982, **21**(5): 599~602

16 Vidyasagar M. Control Systems Synthesis: A Factorization Approach, North Holland System and Control Series, MIT Press, Cambridge, M.A. 1985

17 Zhao Q, Jiang J. Reliable state feedback control systems design against actuator failures, *Automatica*, 1998, **34**(10): 1267~1272

18 Jiang J, Zhao Q. Design of reliable control systems possessing actuator redundancies, *Journal of Guidance, Control, and Dynamics*, 2000, **23**(4): 709~718

19 Chandler P K. Self-repairing flight control system reliability and maintainability program executive overview, In: Proceedings of the IEEE National Aerospace and Electronics Conference, Dayton, OH, 1984, 586~590

20 McMahan, J. Flight 1080, Air Line Pilot, 1978

21 Montoya R J, Howell W E, Bundick W T, Ostro A J, Hueschen R M, Belcastro C M. Restructurable Controls, NASA Report, 1983, CP-2277

22 Zemlyakov S D, Rutkovskii V Y, Silaev A V. Reconfiguring aircraft control systems in case of failures, *Automation and Remote Control*, 1996, **57**(1): 1∼13

23 Patton R J. Fault-tolerant control: the 1997 situation, In: Proceedings of IFAC Symp: On Fault Detection, Supervision and Safety for Technical Processes, 1997, 1033∼1055

24 Moerder D D. Halyo N, Broussard J R, Caglayan A K. Application of precomputed control laws in a reconfigurable aircraft flight control system, *Journal of Guidance, Control, and Dynamics*, 1989, **12**(3): 325∼333

25 Looze D P, Weiss J L, Eterno J S, Barrett N M. An automatic redesign approach for restructurable control systems, *IEEE Control System Magazine*, 1985, 16∼22

26 Willsky A S. A survey of design methods for failure detection in dynamic systems, *Automatica*, 1976, **12**(6): 601∼611

27 Mironovski L A. Functional diagnosis of dynamic system — A survey, autom. *Remote Control*, 1980, **41**: 1122∼1143

28 Isermann R. Process fault detection based modelling and estimation methods: A survey, *Automatica*, 1984, **20**(4): 387∼404

29 Gertler J. Survey of model-based failure detection and isolation in complex plants, *IEEE Control Systems Magazine*, 1988, **8**(6): 3∼11

30 Frank P M. Fault diagnosis in dynamic system using analytical and knowledge-based redundancy — a survey and some new results, *Automatica*, 1990, **26**(3): 459∼474

31 Jiang J, Zhao Q. Should we use parameter estimation or state estimation based methods for FDI, In: Proceedings of IFAC Symposium SAFEPROCESS'97, 1997, 474∼479

32 Gao Z, Antsaklis P J. Stability of the pseudo-inverse method for reconfigurable control systems. *International Journal of Control*, 1991, **53**(3): 717∼729

33 Gao Z, Antsaklis P J. Reconfigurable control system design via perfect model following. *International J. Control*, 1992, **56**(4): 783∼798

34 Jiang J. Design of reconfigurable control systems using eigenstructure assignment, *International J. Control*, 1994, **59**(2): 395∼410

35 Maybeck P S. Application of multiple model adaptive algorithms to reconfigurable flight control, *Control and Dynamic Systems*, 1992, **52**: 291∼320

36 Narendra K S, Balakrishnan J. Adaptive control using multiple models, *IEEE Transactions on Automatic Control*, 1997, **42**(1): 171∼187

37 Zhang Y M, Jiang J. Integrated active fault-tolerant control using IMM approach, *IEEE Transactions on Aerospace and Electronic Systems*, 2001, **37**(4): 1221∼1235

38 Zhang Y M, Jiang J. Integrated design of reconfigurable fault-tolerant control systems, *Journal of Guidance, Control, and Dynamics*, 2001, **24**(1): 133∼136

39 Chen J, Patton R J, Chen Z. Active fault-tolerant flight control systems design using the linear matrix inequality method. *Transactions of the Institute of Measurement and Control*, 1999, **21**(2): 77∼84

40 Liao F, Wang J L, Yang G H. Reliable robust flight tracking control: an LMI approach, *IEEE Transactions on Control Systems Technology*, 2002, **10**(1): 76∼89

41 Wang H, Wang Y. Neural-network-based fault-tolerant control of unknown nonlinear systems. *IEE Proceedings Control Theory and Applications*, 1999, **146**(5): 389∼398

42 Stengel R F. Intelligent failure-tolerant control, *IEEE Control System Magazine*, 1991, **11**(4): 14∼23

43 Stengel R F. Toward intelligent flight control, *IEEE Transactions on Systems, Man & Cybernetics*, 1993, **23**(6): 1699∼1717

44 Rauch H E. Intelligent fault diagnosis and control reconfiguration, *IEEE Control Systems Magazine*, 1994, 6∼12

45 Rauch H E. Autonomous control reconfiguration, *IEEE Control Systems Magazine*, 1995, 37∼48

46 Kabore P, Wang H. Design of fault diagnosis filters and fault tolerant control for a class of nonlinear systems, *IEEE Transactions on Automatic Control*, 2001, **46**: 1805∼1809

47 Liang Y W, Liaw D C, Lee T C. Reliable control of nonlinear systems, *IEEE Transactions on Automatic Control*, 2000, **45**(4): 706∼710

48 Zhang Y M, Jiang J. Fault-tolerant control system design with explicit consideration of performance degradation. *IEEE Transactions on Aerospace and Electronic Systems*, 2003, **37**(3)

49 Mariton M. Detection delays, false alarm rates and the reconfiguration of control systems, *International J. Control*, 1989, **49**(3): 981∼992

50 Jiang J, Zhao Q. Fault tolerant control system synthesis using imprecise fault identification and reconfiguration control, In: Proceedings of the IEEE International Symp. on Intelligent Control, Gaithersburg, MD, 1998, 169∼174

51 Mahmoud M, Jiang J, Zhang Y M. Stabilization of active fault tolerant control systems with imperfect fault detection and diagnosis, *Journal of Stochastic Analysis and Applications*, 2003, **21**(3): 673∼701

52 Maki M, Jiang J, Hagino K. A stability guaranteed active fault-tolerant control against actuator failures, *International Journal of Robust and Nonlinear Control*, 2004

53 Srichander R, Walker B K. Stochastic stability analysis for continuous time fault-tolerant control systems, *International J. Control*, 1993, **57**(2): 433∼452

54 Mahmoud M, Jiang J, Zhang Y M. Active Fault Tolerant Control Systems: Stochastic Analysis and Synthesis, In: Lecture Notes in Control and Information Sciences, Vol.287, Springer, Berlin, Germany, 2003

55 Wu N E. Coverage in fault-tolerant control, *Automatica*, 2004, **40**(4): 537∼548

56 Goble W M. Control Systems Safety Evaluation and Reliability, 2nd edition, ISA, 1998

57 Stamtis D H. Failure Mode and Effect Analysis: FMEA from Theory to Execution, American Society for Quality, 2003

58 Hu T S, Lin Z L. Control Systems with Actuator Saturation: Analysis and Design, Birkhauser Boston, 2001

Jin Jiang Received his bachelor from Xi'an Jiaotong University, P.R.China in 1982 and master and Ph.D. degrees in 1984 and 1989, respectively, from the Department of Electrical Engineering, the University of New Brunswick, Fredericton, New Brunswick, Canada. After Ph.D., he held several appointments in Marine Institute and Lakehead University before joining the University of Western Ontario in London, Ontario, Canada in 1991. Currently, he is a Professor and NSERC/UNENE Senior Industrial Research Chair, in the Department of Electrical and Computer Engineering at The University of Western Ontario. He is also an honorary Professor at the East China Jiaotong University. His research interests are in the areas of fault-tolerant control of safety critical systems, power system dynamics and controls, and advanced signal processing for diagnostic applications.