FAULT DIAGNOSIS AND FAULT-TOLERANT CONTROL

Paul M. Frank
Fellow IEEE, University Duisburg-Essen, Duisburg, Germany

Mogens Blanke
Technical University of Denmark, Lyngby, Denmark

Keywords: Fault diagnosis, Fault detection, Fault isolation, Fault analysis, Fault-tolerant control, Supervisory control, Residual generation, Residual evaluation, Reconfiguration.

Contents

Summary

Reliability, availability, and safety with respect to man and environment are among the primary requirements of automated engineering systems in the face of faults occurring in their components. In this article we present the fundamentals and basic approaches to technical fault detection and isolation (FDI) and fault tolerant control (FTC). The relevant definitions and concepts of fault diagnosis are given. The model-free approaches to FDI discussed include the physical redundancy approach, the signal-based approach and the plausibility check. The principle of the model-based methodology is outlined and a classification of the different residual generation approaches with respect to the types of models used is given. The analytical model-based approach is addressed in more detail with a focus on analytical modeling of the system, modeling of faults, analytical residual generation schemes, the role of structured residuals, and the concept of robust residual generation. Very briefly, the non-analytical approaches of residual generation and the methods of residual evaluation are discussed, and a historical review of the development of model-based residual generation methods is given. The discussion of fault-tolerant control comprises the determination of appropriate reactions to faults, and - at an example - the analysis based on system structure, analytical redundancy, and structural controllability and observability. The fault-tolerant control structure using diagnosis is illustrated and the principles of active and passive approaches to fault-tolerant control are explained. As far as the control problem is concerned, several control strategies are given depending on where the faults in the system occur; this discussion includes the concept of logic-based switching controller.

1. Introduction

All real systems in nature – physical, biological and engineering systems – can malfunction and fail due to faults in their components. The chances for failures are increasing with the system’s complexity. The complexity of engineering systems is permanently growing due to the growing system size and degree of automation, and accordingly increasing are the chances for faults and, at the same time, aggravating the consequences of system failures for man and environment. Therefore, increased attention has to be paid to the reliability, safety and fault tolerance in the design and operation of technical systems in industrial automation. But obviously, compared to the high standard of perfection that nature has developed with the “self-healing” and “self-repairing” mechanisms in complex biological organisms, the fault management in engineering systems is far behind their technological capabilities and is still in its infancy.

In technical automatic control systems, defects may happen in sensors, actuators, the components of the plant itself, or within the hardware or software of the control equipment. Component faults can develop into a failure of the whole system. This effect can easily be amplified by the closed loop. The closed loop may also hide an incipient fault from being observed until a situation is reached in which a failing of the whole system is unavoidable. Even making the closed loop robust or reliable by robust or reliable control, respectively, can not solve the problem in full. It may ensure to retain stability of the closed loop and continue its mission with the desired or tolerable degraded performance in the presence of faults, but when the faulty part continues to miss-function, it may cause damage to man and environment due to the impact of the faults (i.e., leakages in gas tanks or in oil pipes etc.). So, robust and reliable control using available hard- or software redundancy may be efficient ways to maintain the functionality of the control process, but it can not guaranty environmental compatibility or safety of the whole system.

A realistic fault management has to provide dependability which includes both reliability and safety. Dependability is a fundamental requirement in industrial automation, and a cost-effective way to provide dependability is fault-tolerant control (FTC). The key issue of FTC is that local faults are prevented from developing into a system failure that can end the mission of the system, and/or cause safety hazards by the faulty devises or the whole system for man and environment. Because of its increasing importance in industrial automation, FTC has become an emerging topic in control theory.

Automation for safety-critical systems, where no failure can be tolerated, requires redundant hardware to accomplish systems that are not affected by any single failure. Fail-operational systems are made insensitive to any single component fault. Fail-safe systems perform a controlled shut-down to a safe state when a measurement indicates a critical fault. Robust control ensures stability and pre-assigned performance of the control loop in the presence of faults within a specified range. In contrast, fault-tolerant control monitors on-line the system behavior and diagnoses critical faults in the components, and after detection of the faults it causes appropriate remedial actions in order to prevent faults from developing into a failure. Depending on the special purpose of application, the overall FTC system has to keep the plant availability despite the faults, possibly with reduced performance, and, if the faults may cause damage or endanger man or environment, handles them by system reconfiguration, e.g., by shutting down the faulty devices and substituting their function. The basic schematic arrangement of the FTC framework is shown in Figure 1. Its four basic functional units are: the plant, i.e., the controlled object including actuators and sensors, the controller (i.e., control devices), configuration commander, and the supervisory system which includes fault diagnosis (FD).

It can be seen that the implementation of a fault tolerant control framework requires multi-level automation, i.e., the control level needs to be complemented by at least one further level, the supervision level (sometimes this is organized in several higher levels of information or knowledge processing and logical decision making). The purpose of the supervision level is to observe the process in order to maintain the desired plant availability and avoid damages and accidents. Traditional approaches to the accomplishment of this task are:

- monitoring, i. e., checking of operating conditions, system states and measurable signals (magnitudes, tolerances, limit values, trends),
- giving alarms and instructions to human operators to take proper actions,
- setting reference input and tolerances,

- provide automatic protection of the process.

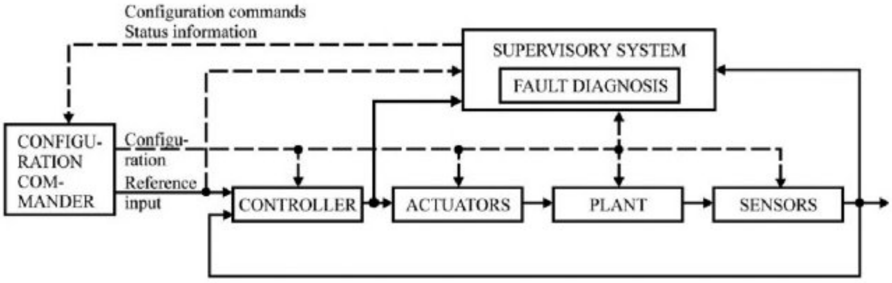

Figure 1: Basic scheme of a fault-tolerant control system

In advanced fault-tolerant control systems, fault diagnosis has become a key issue of the tasks of the supervision level. Note that the traditional non-model-based FD methods can only cope with the FD problem in an incomplete manner. Their advantage is their simplicity and reliability and that they do not need detailed knowledge of the system, which is often not available or too expensive. Their crux with respect to fault tolerance is, however, that only relatively large changes (sudden and long drifting faults) are detectable and that reliable results are only available in steady state operation of the system. Also, early detection of small abrupt and incipient faults and a full and systematic fault diagnosis are impossible. These deficiencies can be overcome with more sophisticated methods of fault diagnosis, where the model-based methodology plays a fundamental role. The model-based approaches make use of dynamic models of the system under consideration and are thus capable of detecting small faults, performing high-quality fault diagnosis by determining time, size and cause of a fault, and are applicable to dynamic system operation. At the occurrence of faults they detect the faults by generating discrete event signals from which an automatic reconfiguration commander can be triggered in order to do fault accommodation. But not only that model-based fault diagnosis is an essential ingredient of fault-tolerant control, it is also a basic tool for off-line tasks such as condition-based maintenance and repair, which is carried out according to the information obtained by condition monitoring of the system. Hence model-based fault diagnosis is an important issue in all kinds of advanced engineering systems.

In this article, we present the fundamentals of technical fault diagnosis and fault-tolerant control with focus on the advanced model-based approaches to fault detection and isolation (FDI) using all kinds of models such as analytical, knowledge-based or data-based models.

2. Fault Diagnosis: Basic Definitions and Concepts

The goal of a fault diagnosis system is to discover malfunctions, i.e., faults, in the functional units of a control system that cause undesired or unacceptable system behavior.

2.1. Faults

The faults of interest that can occur in an automatic control system may be classified in four major categories (see Figure 2):

- Sensor faults. These are measurement errors caused by defects in sensors such as short cut, offset, bias, power breakdown, sticking, scaling error, hysteresis, etc.
- Actuator faults. These are errors caused by defects in actuators such as damages of bearings, loss of momentum, defects in gears, ageing effects, etc.
- Component faults. These are undesired changes in the system operation caused by defects within the body of the plant such as cracks, ruptures, fractures, leaks, power breakdown, loosening of parts, or critical abnormal parameter variations due to sudden changes of conditions, or external obstacles such as collisions, clogging of outflow pipes, etc..
- Control unit faults. These are control errors caused by defects in the hardware or errors in the software of the electronic control framework of an automated system. Examples are power breakdown, dropout of network elements or computers, electromagnetic disturbances, software shortcuts, etc.

Even though a fault-free functioning of the electronic part of an automatic control system is a prerequisite for perfect performance and hence control unit faults are very important in any fault management system, we concentrate in this article on faults in the physical part of the control system including sensors, actuators and body of the plant, because usually this part works under rougher conditions thus being more subject to faults than the electronic control devices or computers which usually operate in a well-defined and protected environment.

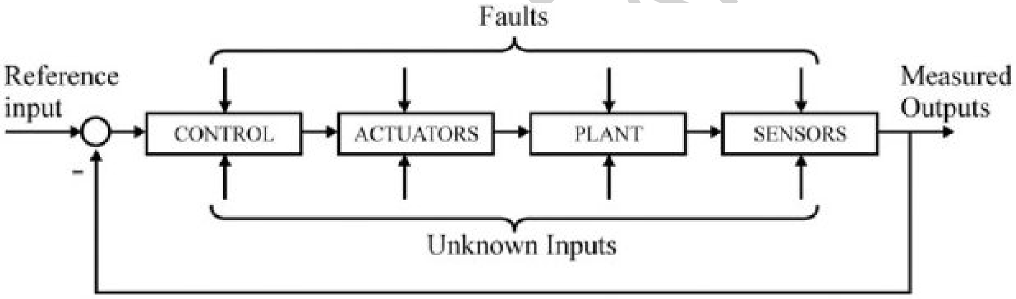

Figure 2: Faults and unknown input in automatic control systems

2.2. Unknown Inputs

Besides the faults, there are always unknown inputs acting on the plant. By unknown inputs we mean disturbances, measurement and system noise and, in the case of model-based approaches, parameter variations (model mismatches) associated with the modeling of the plant. They have to be properly distinguished from faults due to the fact that their effects are not mission-critical, which means that they can be tolerated and do not need to be detected. However, they may cause great problems in fault detection systems, because if they are misinterpreted as faults by the diagnosis system, they lead to false alarms, and already a relatively small false alarm rate can make a diagnosis system totally useless. The main task of any fault detection system is therefore to keep the false alarm rate zero or at least extremely small despite the existing unknown inputs and at a satisfactory fault sensitivity. Robustness to unknown inputs is a fundamental problem of the model-based methodology, and it is basically in conflict with the demand for high fault sensitivity.

-
-
-

Bibliography

Blanke M., Kinnaert M., Lunze J and Staroswiecki M. (2003). Diagnosis and Fault-tolerant Control. Springer Verlag. [This textbook presents effective methods for fault-diagnosis and fault-tolerant control for processes that are described by analytical models, by discrete-event models or that can be dealt with as quantized systems]

Blanke M. Izadi-Zamanabadi R., Bøgh S. A. and Lunau C. P. (1997): Fault Tolerant Control - A Holistic View. Control Engineering Practice 5, pp 693-702

Chen J., Patton R.J. (1998). Robust Model-based Fault Diagnosis for Dynamic Systems. Kluwer Academic Publishers. [This book presents the subject of model-based fault detection and isolation in a unified framework]

Frank P.M., Keller L. (1984). Entdeckung von Instrumentenfehlanzeigen mittels Zustands-schätzung in technischen Regelungssystemen. VDI Fortschrittsberichte, Reihe 8, Nr. 80. VDI Düsseldorf. [This book presents the basic concept and applications of the dedicated observer scheme for sensor fault detection]

Frank P.M. (1987). Advanced fault detection and isolation schemes using non-linear and robust observers (Invited Survey Paper). Proceedings of the 10th IFAC World Congress Munich, pp. 63-68. [An early survey paper on non-linear and robust model-based fault detection and isolation]

Frank P.M. (1990). Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy, Automatica 26, pp. 459-474. [An early survey of the state of the art in model-based fault detection and isolation with emphasis on observer schemes]

Frank P.M., Ding X. (1994). Frequency domain approach to optimally robust residual generation and evaluation for model-based fault diagnosis. Automatica 30(4), pp. 789-804. [A unified approach to model-based residual generation in the frequency domain]

Frank P.M., (1994). Enhancement of robustness in observer-based fault detection. International Journal of Control 59 (4) pp. 955-981. [A comprehensive survey of model-based fault detec-tion and isolation with robustness properties]

Frank P.M. (1996). Analytical and qualitative model-based fault diagnosis – A survey and some new results, European Journal of Control, 2 (1), pp.6-23. [A survey of the state of the art in model-based fault detection and isolation methods with emphasis on qualitative approaches]

Gertler J. (1998). Fault Detection and Diagnosis in Engineering Systems. Marcel Dekker. [A self-contained reference/text book featuring the model-based approach to fault detection and diagnosis in engineering systems]

Isermann R. (1984). Process fault detection based on modelling and estimation methods: A survey. Automatica 20, pp. 387-404. [An early survey of model-based fault diagnosis systems]

Isermann, R. (1997). Supervision, fault-detection and fault-diagnosis methods – an introduction. Control Engineering Applications, Vol. 5, pp. 639-652. [outlines the basic ideas and state of the art]

Isermann, R., Ballé, P. (1997). Trends in the application of model-based fault detection and diagnosis of technical processes. Control Engineering Applications, Vol. 5, pp. 709-719. [provides the definitions worked out in the Technical Committee SAFEPROCESS]

Mahmoud M., Jiang J. and Zhang Y (2003). Active Fault Tolerant Control Systems – Stochastic Analysis and Synthesis. Springer Lecture Notes in Control and Information Sciences Vol. 287. [This book treats fault-tolerant control from a probabilistic point of view with stability and transition probabilities discussed from a common problem formulation]

Mangoubi R. S. (1998). Robust Estimation and Failure Detection – a Concise Treatment. Springer. [This book treats the diagnosis problem using mathematical methods from robust analysis and estimation]

Patton R.J., Frank P.M., Clark R.N., eds. (1989). Fault Diagnosis in Dynamic Systems, Theory and Application. Prentice Hall. [A multi-authored book summarizing the early work on model-based FDI and fault diagnosis]

Patton R.J., Frank P.M., Clark R.N., eds. (2000). Issues of Fault Diagnosis for Dynamic Systems. Springer. [A multi-authored book presenting basic contributions of the 1990'ties to model-based FDI]

Willsky A.S.(1976). A survey of design methods for failure detection in dynamic systems. Automatica 12, pp. 601-611. [The earliest comprehensive survey of model-based fault detection approaches with emphasis on statistical evaluation techniques]

Biographical Sketches

Paul M. Frank received the degrees of Dipl.-Ing. in Electrical Engineering in 1959, Doctor Ing. in 1966 and Habilitation in 1973, all from the University of Karlsruhe, Germany. From 1959 – 1976 he has been an Assistant Professor and Associate Professor at the University of Karlsruhe. 1974 – 1975 he spent a year as a scholar and guest professor at the University of Washington, Seattle, U.S.A. From 1976 – 1999 he has been a full professor and head of the department of Measurement and Control at the Gerhard-Mercator-University of Duisburg, 1980/81 chairman of the faculty of Electrical Engineering. From 1977 - 2000 he has been a permanent guest lecturer at the Ecole Nationale Supérieure de Physique de Strasbourg, ENSPS, France. Since 1999 he is a professor emeritus. A co-founder of the German-French Institute of Automation and Robotics IAR 1986, he holds the position of a honorary president since 2000. Prof. Frank was president of the European Union Control Association, EUCA, from 1999 – 2001. Prof. Frank holds three honorary doctor degrees, from the University of Iasi, Romania 1994, the Université de Haute Alsace, Mulhouse, France, 1997, and the Technical University of Cluj-Napoca, Romania, 1998, and he has received medals of merit from several universities. He is a member of VDI/VDE-GMA and a Fellow of IEEE.

Prof. Frank's main interests are in automatic control with focus on fault diagnosis and fault tolerant control systems, analysis and design of robust control systems, sensitivity theory, fuzzy and neuro techniques in control and system supervision. He has published or edited seven books and published more than 460 papers in technical journals and international conferences, organized the European Control Conference 1999, and he is co-editor of several technical journals.

Mogens Blanke is professor of automatic control at the Section of Automation at Ørsted-DTU of the Technical University of Denmark. His research interests comprise autonomous and fault-tolerant systems, fault diagnosis, systems architecture design to obtain desired safety properties, systems modeling, identification and control. His experiences result from the development of fault-tolerant design methods for the Danish Ørsted satellite, from the design of marine automation systems and from the design of fault-tolerant steering-by-wire architectures for transportation systems.