FP9-1: Fault Tolerant Control Systems

Youmin Zhang

Phone: 7912 7741   Office Location: FUV 0.22
Email: ymzhang@cs.aaue.dk
\\tun\web\cs\contribution\courses\fall2006\IRS9\FTC1\index.html

---

FP9-1: Fault Tolerant Control Systems

Lecture 1

Introduction to fault-tolerant control system

- What is fault-tolerant control system (FTCS)?
- Fault-tolerant vs. conventional control systems
- Overall structure of fault tolerant control systems
- Methods of designing fault tolerant control systems
- Examples

Course Outline

Part I

1. Introduction to Fault-Tolerant Control System (FTCS)
2. Characteristics of FTCS and Special Considerations in FTCS Design
3. Design of Active FTCS (AFTCS) (1)
4. Design of Active FTCS (AFTCS) (2)
5. Design of Passive FTCS (PFTCS)

What is Fault-Tolerant Control System (FTCS)?

Definition: A FTCS is a control system that possesses the ability to accommodate system component faults/failures *automatically* and is capable of maintaining overall system stability and acceptable performance in the event of such failures.

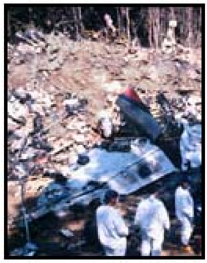
Objectives: Increase reliability, safety and automation level of modern technological/engineering systems.

Approaches: Passive FTCS (PFTCS); Active FTCS (AFTCS) - Reconfigurable FTCS (RFTCS).

Feature: The key to any FTCS – Redundancy.

Why Fault-Tolerant Control is Needed?

Motivation for FTCS Research & Development



NATIONAL TRANSPORTATION SAFETY BOARD

WASHINGTON, D.C. 20594

AIRCRAFT ACCIDENT REPORT

UNCONTROLLED DESCENT AND COLLISION WITH TERRAIN
USAIR FLIGHT 427
BOEING 737-300, N513AU
NEAR ALIQUIPPA, PENNSYLVANIA
SEPTEMBER 8, 1994

USAir Flight 427 accident

Crashed on 8 Sept. 1994

A loss of control of the airplane resulting from the movement of the rudder surface to its blowdown limit, which leads to an uncontrolled descent and collision with terrain

All 132 people on board were killed, and the airplane was destroyed by impact forces and fire.

Source:
http://www.ntsb.gov/publictn/1999/AAR9901.htm

UA Flight 585 accident

Crashed on 3 March 1991

A loss of control of the airplane resulting from the movement of the rudder surface to its blowdown limit, the same reason as in Flight 427.

Injuries: 25 Fatal; The airplane was destroyed.

Source:
http://www.ntsb.gov/NTSB/brief.asp?ev_id=20001212X16583&key=1

Two Events Called for Research on FTCS

Flight 1080

"As pilot-in-command of Delta Air Lines Flight 1080, he maneuvered his malfunctioning aircraft more than 100 miles through 8,000 feet of solid overcast to a safe landing. His professional judgment and skill merit the gratitude of America's flying public."

Flight 191 accident – failed case

Flight 1080 – successful example

Two events that motivated the research on fault-tolerant flight control

Crashed on 25 May 1979

Separation of the no.1 engine and pylon assembly procedures which led to failure of the pylon structure.

271 people were killed/injured.

Source: http://aviation-safety.net/database/1979/790525-2.htm
(more accident cases can be found in this webpage)

Safely landed on 12 April 1977

The elevator became jammed at 19 degrees up and the pilot had been given no indication that this malfunction had occurred.

Fortunately, the pilot successfully reconfigured the remaining control elements and landed the aircraft safely - clever use of actuation ***redundancy*** in the L-1011 airplane.

Faults and Faults Classification

Definition and classification

- What is a fault?
  - In the area of fault-tolerant control, a fault is regarded as any kind of malfunction in a system, and which may lead to system instability or result in unacceptable performance degradation.
  - Such a fault can occur in any component of the system such as *sensors*, *actuators*, and *system components*, as will be demonstrated in the next slides.
- Fault types/classification
  - Based on physical locations:
    - Sensors (for both output and input variables), actuators, system/plant components, and/or controllers
  - Based on effects on the system performance:
    - Additive/multiplicative faults, or abrupt/incipient faults

---

Faults and Faults Classification

A diagram associated with different faults in a controlled system

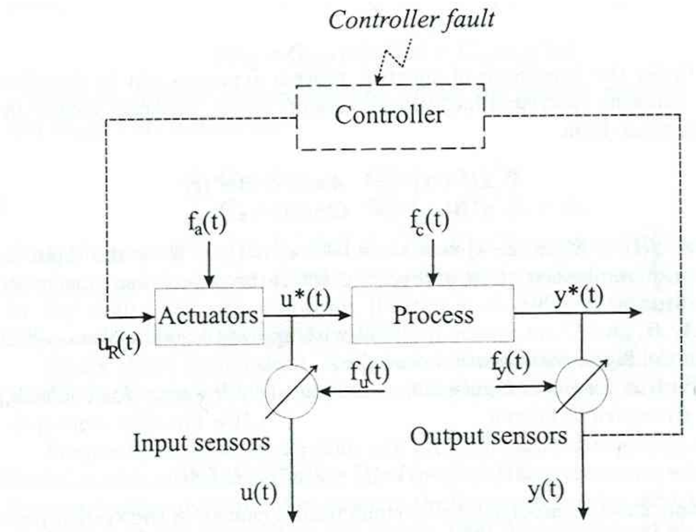


Fig. 2.4. The controlled system and fault topology. Simani *et al*, 2002

Types of Faults

(temporal/permanent persistence)

- ❑ Permanent faults:
  - ➢ Total failure of a component
  - ➢ Caused by, for example, short-circuits or melt-down
  - ➢ Remains until component is repaired or replaced
- ❑ Transient faults:
  - ➢ Temporary malfunctions of a component
  - ➢ Caused by magnetic or ionizing radiation, or power fluctuation
- ❑ Intermittent faults:
  - ➢ Repeated occurrences of transient faults
  - ➢ Caused by, for example, loose wires

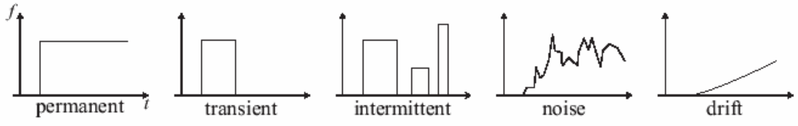
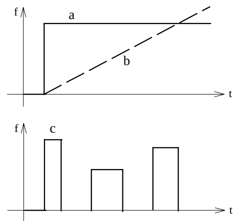


Fig. 3.1. Time behavior of fault types

Types of Faults

(Another view of classification)

- Classification based on faulty components
  - plant component faults
    - total failures
    - partial faults
  - actuator faults
    - total failures
    - partial faults
  - sensor faults
    - total failures
    - partial faults
  - controller faults
- Classification based on faulty forms
  - abrupt fault
  - incipient fault
  - intermittent fault

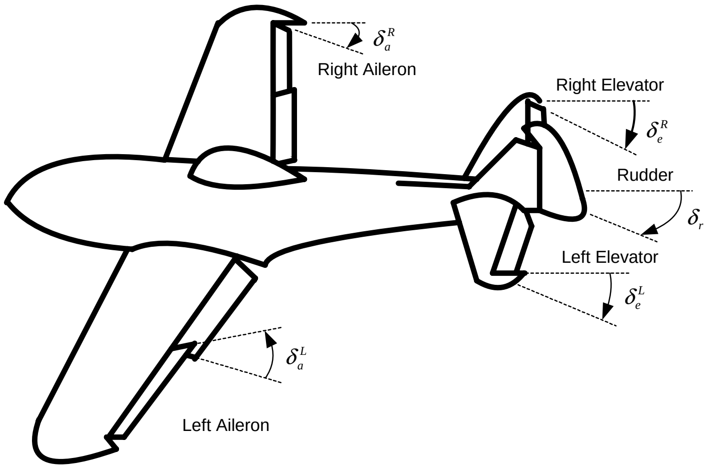


- Classification based on the ways added on the system
  - additive faults
  - multiplicative faults

Common Faults in Aircraft

(Example 1)

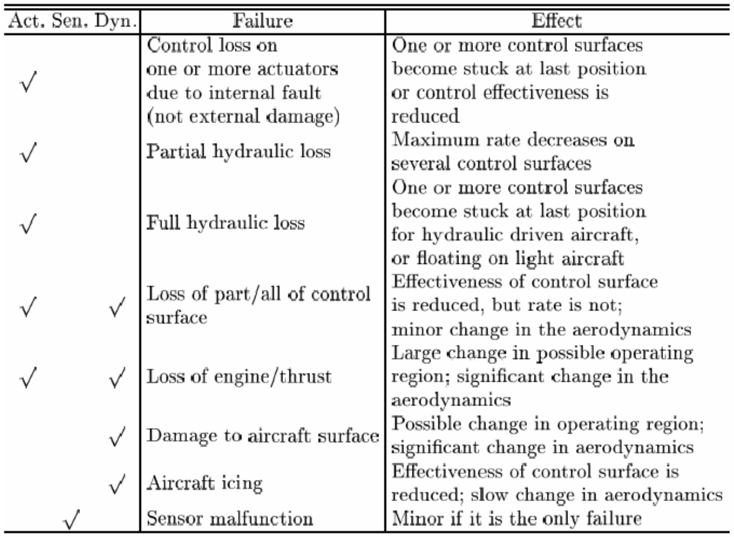
- An aircraft and its control surfaces



Common Faults in Aircraft (cont'd)

(Example 1)

Table 2.1: Typical Aircraft Failure Modes and Failure Effects



Act.	Sen.	Dyn.	Failure	Effect
√			Control loss on one or more actuators due to internal fault (not external damage)	One or more control surfaces become stuck at last position or control effectiveness is reduced
√			Partial hydraulic loss	Maximum rate decreases on several control surfaces
√			Full hydraulic loss	One or more control surfaces become stuck at last position for hydraulic driven aircraft, or floating on light aircraft
√		√	Loss of part/all of control surface	Effectiveness of control surface is reduced, but rate is not; minor change in the aerodynamics
√		√	Loss of engine/thrust	Large change in possible operating region; significant change in the aerodynamics
		√	Damage to aircraft surface	Possible change in operating region; significant change in aerodynamics
		√	Aircraft icing	Effectiveness of control surface is reduced; slow change in aerodynamics
	√		Sensor malfunction	Minor if it is the only failure

Common Faults in Other Systems

(Example 2 – a water tank system)

- System configuration
  - System: three tanks
  - Actuators: two pumps for tank #1 and #3
  - Sensors: three pressure sensors for liquid level measurement of each tank

- Fault modes
  - Actuator faults: jammed pumps
  - Sensor faults: pressure sensor malfunctions
  - System faults: leakage of any one of the three tanks

How Faults are Mathematically Modeled?

- ❑ Two types of model
  - Input-output models
    - Transfer functions
    - ARMA
  - State-space models
- ❑ Two types of representation of faults
  - Additive faults
  - Multiplicative faults
- ❑ Time behavior of faults
  - Abrupt faults (stepwise)
  - Incipient/gradual faults (drift-like)
- ❑ Severity of faults
  - Partial fault
  - Total/hard-over failure
  - Stuck/frozen fault, floating fault …

Questions:

- Are we able to handle all these types of faults?
- How to model these faults?
- How to detect and accommodate these faults in FTCS?

Modeling of System

(under normal conditions)

a. State-space model

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \end{cases}$$

$$z(t) = My(t) = \begin{bmatrix} \underline{s}_1 & 0 & \cdots & 0 \\ 0 & \underline{s}_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \underline{s}_p \end{bmatrix} \begin{bmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_p(t) \end{bmatrix}$$

$$\underline{s}_i = [s_{i1} \quad s_{i2} \quad \cdots \quad s_{iq_i}]^T$$

$$x \in \Re^{n\times 1}, u \in \Re^{m\times 1}, y \in \Re^{p\times 1}, \quad z \in \Re^{q\times 1}, \quad M \in \Re^{q\times p}$$

b. ARMA model

$$y(t) = \psi^T(t)\theta_o$$

$\psi(t)$ - Regression vector; θ_o - parameter vector

Modeling of System

(under dynamic fault conditions)

a. State-space model

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) & t < t_f \\ \dot{x}(t) = (A + \Delta A)x(t) + (B + \Delta B)u(t) & t \ge t_f \end{cases}$$

and

$$\begin{cases} y(t) = Cx(t) & t < t_f \\ y(t) = (C + \Delta C)x(t) & t \ge t_f \end{cases}$$

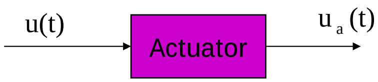
b. ARMA model

$$\begin{cases} y(t) = \psi^T(t)\theta_o & t < t_f \\ y(t) = \psi^T(t)(\theta_o + \Delta\theta) & t \ge t_f \end{cases}$$

Modeling of System

(under actuator fault conditions)

Actuator faults



$$u_a(t) = L_a u(t) + (I_{q\times q} - L_a) f_a$$

where $f_a \in \Re^{q\times 1}$ is the constant bias term, and

$$L_a = diag\{l_1, l_2, \cdots\cdots l_q\}$$

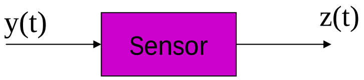
represents the operational modes of the actuators.

$$l_i = \begin{cases} 1 & t < t_f \quad \textit{functional} \\ 0 & t \geq t_f \quad \textit{failure} \end{cases}$$

Modeling of System

(under sensor fault conditions)

Sensor faults



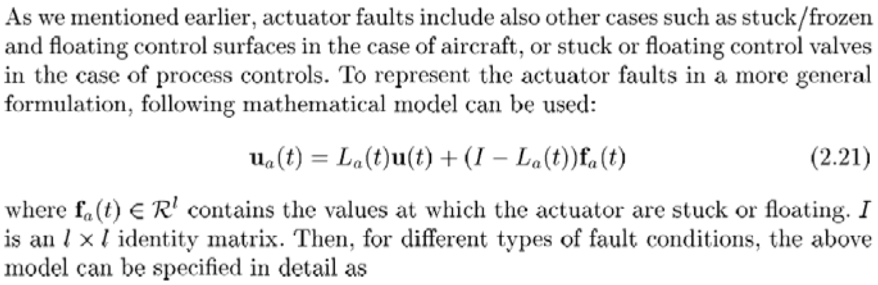
$$z(t) = L_s M y(t) + (I_{m\times m} - L_s) f_s$$

where $L_s \in \Re^{m\times m}$ represents the operational modes of the sensors, and $f_s \in \Re^{m\times 1}$ is the sensor bias.

- Compared to actuators, it is relatively easy to install multiple sensors.

Modeling of Actuator Faults

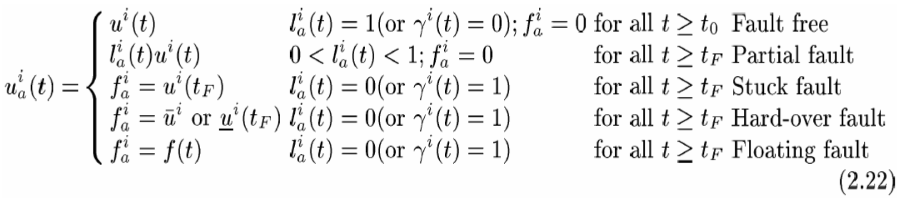
General cases including more fault scenarios (1/2)



As we mentioned earlier, actuator faults include also other cases such as stuck/frozen and floating control surfaces in the case of aircraft, or stuck or floating control valves in the case of process controls. To represent the actuator faults in a more general formulation, following mathematical model can be used:

$$\mathbf{u}_a(t) = L_a(t)\mathbf{u}(t) + (I - L_a(t))\mathbf{f}_a(t) \qquad (2.21)$$

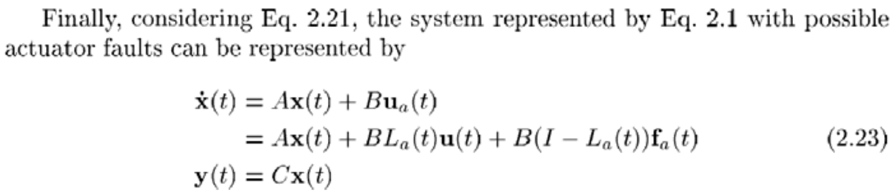
where $\mathbf{f}_a(t) \in \mathcal{R}^l$ contains the values at which the actuator are stuck or floating. I is an $l \times l$ identity matrix. Then, for different types of fault conditions, the above model can be specified in detail as



$$u_a^i(t) = \left\{ \begin{array}{llll} u^i(t) & l_a^i(t) = 1(\text{or } \gamma^i(t) = 0); f_a^i = 0 & \text{for all } t \geq t_0 & \text{Fault free} \\ l_a^i(t)u^i(t) & 0 < l_a^i(t) < 1; f_a^i = 0 & \text{for all } t \geq t_F & \text{Partial fault} \\ f_a^i = u^i(t_F) & l_a^i(t) = 0(\text{or } \gamma^i(t) = 1) & \text{for all } t \geq t_F & \text{Stuck fault} \\ f_a^i = \bar{u}^i \text{ or } \underline{u}^i(t_F) & l_a^i(t) = 0(\text{or } \gamma^i(t) = 1) & \text{for all } t \geq t_F & \text{Hard-over fault} \\ f_a^i = f(t) & l_a^i(t) = 0(\text{or } \gamma^i(t) = 1) & \text{for all } t \geq t_F & \text{Floating fault} \end{array} \right. \qquad (2.22)$$

Modeling of Actuator Faults

General cases including more fault scenarios (2/2)



Finally, considering Eq. 2.21, the system represented by Eq. 2.1 with possible actuator faults can be represented by

$$\begin{aligned} \dot{\mathbf{x}}(t) &= A\mathbf{x}(t) + B\mathbf{u}_a(t) \\ &= A\mathbf{x}(t) + BL_a(t)\mathbf{u}(t) + B(I - L_a(t))\mathbf{f}_a(t) \qquad (2.23) \\ \mathbf{y}(t) &= C\mathbf{x}(t) \end{aligned}$$

Modeling of Sensor Faults

via reduction of measurement effectiveness

Generally, sensor failures may include 1) bias; 2) drift, 3) performance degradation (loss of measurement effectiveness); and 4) freezing [42]. Similar to the above mathematical modelling to actuator faults, sensor faults can be represented similarly as following:

$$\mathbf{z}(t) = L_s(t)M\mathbf{x}(t) + (I - L_s(t))\mathbf{f}_s(t) \tag{2.24}$$

where the matrix $L_s \in \mathcal{R}^{m\times m}$ is similarly defined as in L_a and $\mathbf{f}_s(t) \in \mathcal{R}^m$ corresponds to the unknown bias term.

Similar to Eq. 2.22, various types of sensor faults can be further described as:

$$z^i(t) = \begin{cases} m^i x^i(t) & l_s^i(t) = 1; f_s^i = 0 & \text{for all } t \geq t_0 \text{ Fault free} \\ l_s^i(t) m^i x^i(t) & 0 < l_s^i(t) < 1; f_s^i = 0 & \text{for all } t \geq t_F \text{ Loss of effectiveness} \\ m^i x^i(t) + f_s^i(t) & l_s^i(t) = 0; \dot{f}_s^i(t) = 0 & \text{for all } t \geq t_F \text{ Bias} \\ m^i x^i(t) + f_s^i(t) & l_s^i(t) = 0; \left|f_s^i(t)\right| = c^i t & \text{for all } t \geq t_F \text{ Drift} \\ m^i x^i(t_F) & l_s^i(t) = 1 & \text{for all } t \geq t_F \text{ Freezing} \end{cases} \tag{2.25}$$

where m^i represents the ith column element in sensor gain matrix, M, corresponding to the ith state variable.

Modeling of Dynamic Faults

In general, system dynamic faults are malfunctions caused by changes in the plant parameters or its dynamic characteristics due to aging or wear-out of the plant components.

These changes will manifest themselves as parameter variations in the mathematical model of the system. Therefore, a fault in system dynamics can be expressed as:

$$\begin{aligned} \dot{\mathbf{x}}(t) &= A\mathbf{x}(t) + B\mathbf{u}(t) & t < t_F \\ \dot{\mathbf{x}}(t) &= (A + \Delta A)\mathbf{x}(t) + (B + \Delta B)\mathbf{u}(t) & t \geq t_F \end{aligned} \tag{2.26}$$

and

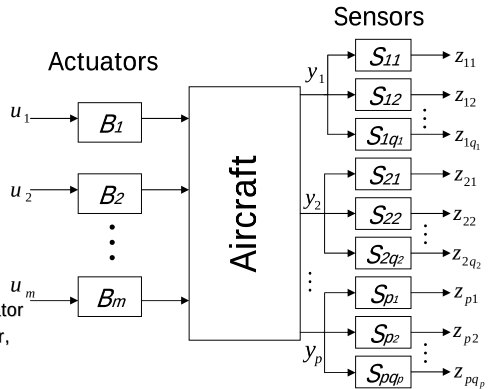
$$\begin{aligned} \mathbf{y}(t) &= C\mathbf{x}(t) & t < t_F \\ \mathbf{y}(t) &= (C + \Delta C)\mathbf{x}(t) & t \geq t_F \end{aligned} \tag{2.27}$$

where t_F is the time instant at which the fault occurred, and $\{\Delta A, \Delta B, \Delta C\}$ are the fault induced changes in the system dynamics. Usually, both of these quantities are unknown and random. This requires effective on-line parameter identification methods to be used to estimate these fault-induced changes for the purpose of fault-tolerant controller design.

How a FTCS is Built and Where the Mathematical Model Becomes Useful?

Basic Ingredients in FTCS: Redundancy

- Hardware Redundancy
  - *Sensor redundancy*
    - » Multiple dissimilar sensors with a **voting scheme**
    - » TMR (Triple Modular Redundancy)
  - *Actuator redundancy*
    - » It is usually difficult (comparing to sensor redundancy) to add extra actuator redundancy due to limitations of power, size, cost ...



Redundancy in an aircraft

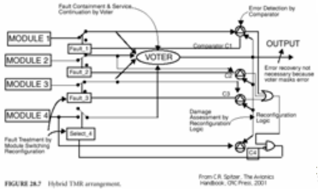


FIGURE 28.7 Hybrid TMR arrangement.

From C.R. Spitzer, The Avionics Handbook, CRC Press, 2001

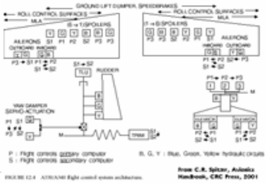


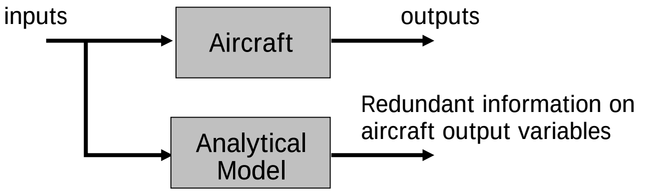
FIGURE 12.4 A330/A340 flight control system architecture.

From C.R. Spitzer, Avionics Handbook, CRC Press, 2001

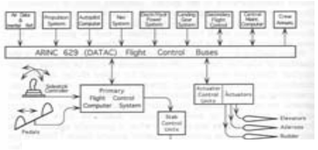
How a FTCS is Built and Where the Mathematical Model Becomes Useful?

Basic Ingredients in FTCS: Redundancy (cont'd)

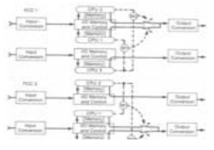
- Analytical Redundancy
  - » the mathematical model or analytical relationships among, for example, aircraft flight state variables
  - » fault detection and diagnosis scheme
  - » redundant control strategies



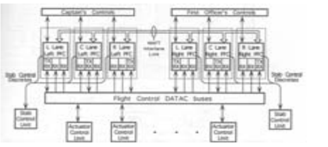
- Hybrid Redundancy: Hardware + Analytical



An electronic flight control system (FCS) architecture



An primary FCS configuration



A redundant architecture for fault tolerance—all three figures are adopted from C.R. Spitzer, Digital Avionics Systems, 2nd, McGraw-Hill, 1993

Example: Redundancy in Boeing 777

- **Primary Flight Control Surfaces**

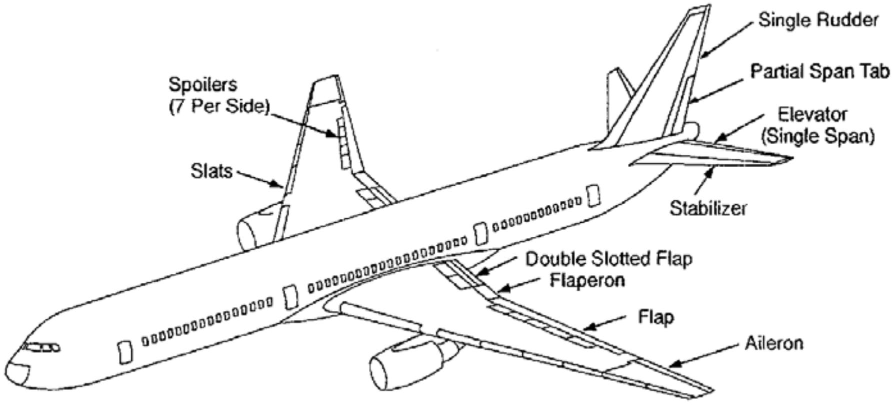


Figure 1 777 Primary Flight Controls Surfaces (Yeh, 1996)

Example: Redundancy in Boeing 777

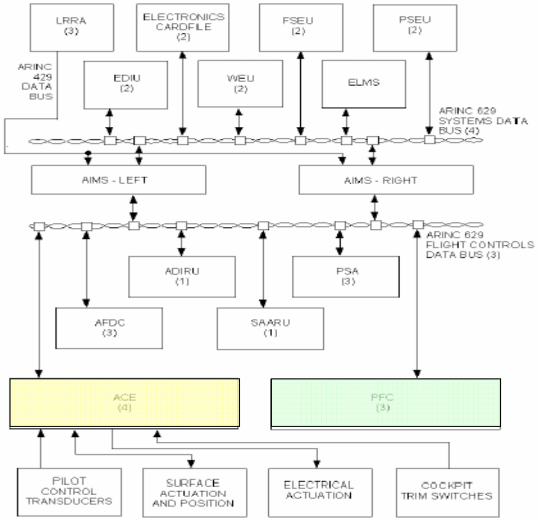


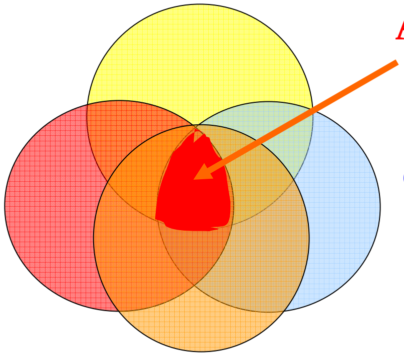
FIGURE 11.2 Block diagram of the electronic components of the 777 Primary Flight Control System, as well as the interfaces to other airplane systems.

ACE: Actuator Control Electronics
ADIRU: Air Data Inertial Reference Unit
ADM: Air Data Module (Static and Total Pressure)
AFDC: Autopilot Flight Director Computer
AIMS: Airplane Information Management System
ARINC: Aeronautical Radio Inc. (Industry Standard)
CMC: Central Maintenance Computer Function in AIMS
DCGF: Data Conversion Gateway Function of AIMS
EDIU: Engine Data Interface Unit
EICAS: Engine Indication and Crew Alerting System
ELMS: Electrical Load Management System
FBW: Fly-By-Wire
FCDC: Flight Controls Direct Current (power system)
FSEU: Flap Slat Electronic Unit
LRRA: Low Range Radio Altimeter
LRU: Line Replaceable Unit
MAT: Maintenance Access Terminal
MEL: Minimum Equipment List
MFD: Multi-Function Display
MOV: Motor-Operated Valve
PCU: Power Control Unit (hydraulic actuator)
PFC: Primary Flight Computer
PMG: Permanent Magnet Generator
PSA: Power Supply Assembly
RAT: Ram Air Turbine
SAARU: Standby Attitude and Air Data Unit
TAC: Thrust Asymmetry Compensation
WEU: Warning Electronics Unit

G.F. Bartley, 2001

Where Does the FTCS Stand?

Multidisciplinary Feature



Fault Detection and Diagnosis (FDD)

Active FTCS

(a currently active research area)

Optimal, Adaptive, Robust Control (Reliable Control or Passive FTCS)

Computing, Communication, Simulation, Implementation (hardware/software), and Display Techniques

Reconfigurable/Restructurable Control

Questions:

- What are difference between active fault tolerant control and adaptive control, robust control and reliable control?

Engineering Application Areas of FTCS

- Engineering Application Areas of FTCS
  - Aircraft/Aerospace systems
  - Ground and surface/underwater vehicles
  - Nuclear reactors and power plants
  - Chemical/Petrochemical processes
  - Autonomous robots and vehicles
  - Medical devices etc.
- Typical Faults Considered in FTCS
  - Actuator faults
  - Sensor faults
  - Structural/Dynamic faults
- Safety Criteria
  - Reliability, maintainability, and safety
- Requirement on Fault Diagnosis and Fault-Tolerant Control
  - Fault diagnosis
  - Fault-tolerant control

General Classification of FTCS

Passive FTCS (PFTCS)

Definition: Systems that are designed to tolerate a certain class of component faults *without* the need for on-line fault information

Properties:

- Tolerance to anticipated faults
- Fixed controller structure/parameters

Active FTCS (AFTCS) – Reconfigurable FTCS (RFTCS)

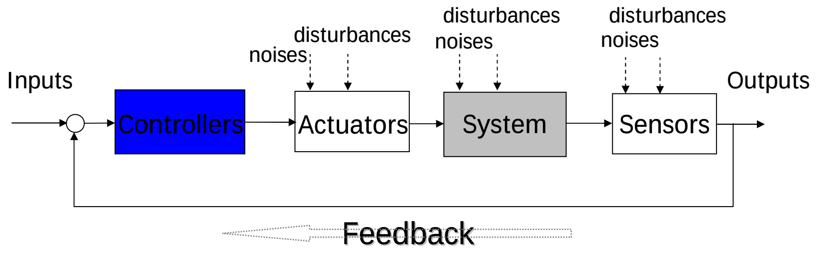
Definition: Systems that can reconfigure the control law on-line and in real-time to accommodate component faults

Properties:

- Explicit Fault Detection and Diagnosis (FDD) schemes
- Real-time decision-making and controller reconfiguration
- Accommodation of anticipated/unanticipated faults
- Acceptable degraded performance in the presence of faults

General Structure of Control Systems

- Conventional control



Elements in control systems:

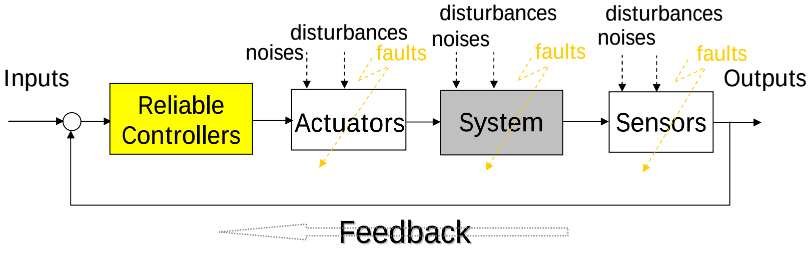
- System/Plant/Process
- Sensors
- Actuators
- Controllers

Properties of control systems:

- Stability
- Performance
- Robustness

Enhancing Robustness of Control Systems

- Robust Control versus Reliable Control - PFTCS



Elements in control systems:

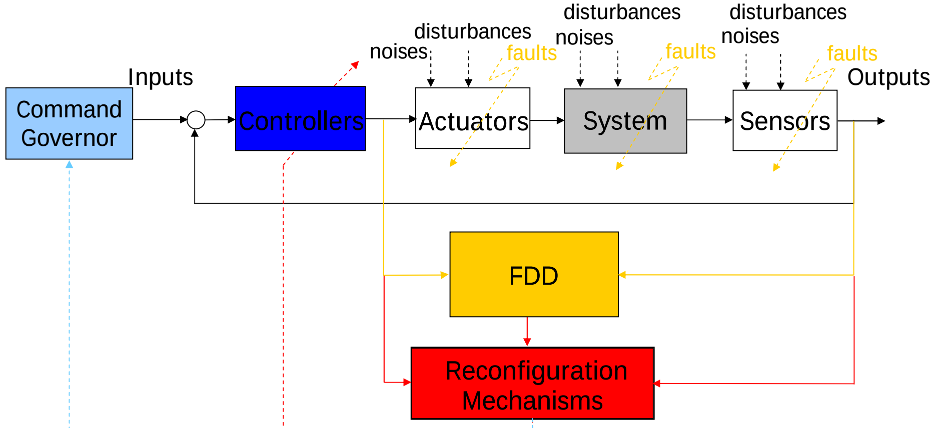
- System/Plant/Process
- Sensors
- Actuators
- Controllers

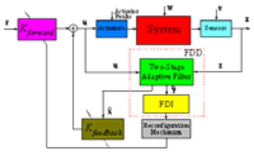
Properties of control systems:

- Stability
- Performance
- Robustness against uncertainties versus faults

General Structure of FTCS

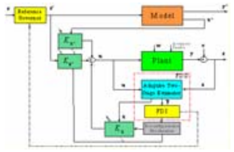
- Reconfigurable (or active fault-tolerant) control system





Three/four important parts in AFTCS:

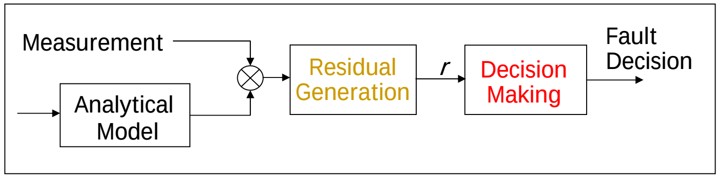
- FDD schemes
- Reconfigurable controllers
- Reconfiguration mechanisms
- Command/reference governor



Modules in AFTCS

Fault Detection and Diagnosis (FDD) Scheme

- Definition: Fault Detection and Diagnosis (FDD) is a process (or technique) to detect faults and to determine their locations and significance in a system being monitored.
- Functions of FDD



Measurement

Analytical Model

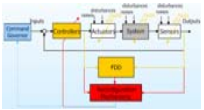
Residual Generation

r

Decision Making

Fault Decision

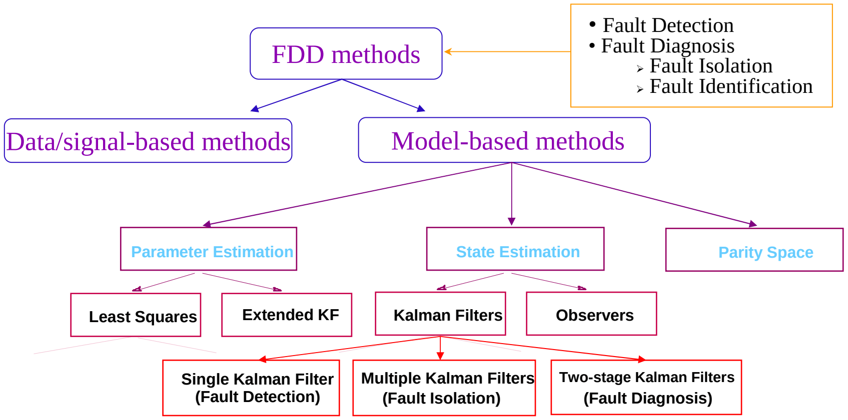
Main topic covered in FP8-1 in last semester.
How much can you still remember?



Modules in AFTCS

Fault Detection and Diagnosis (FDD) Scheme

- Existing FDD techniques:



FDD methods

- Fault Detection
- Fault Diagnosis
  - Fault Isolation
  - Fault Identification

Data/signal-based methods

Model-based methods

Parameter Estimation

State Estimation

Parity Space

Least Squares

Extended KF

Kalman Filters

Observers

Single Kalman Filter (Fault Detection)

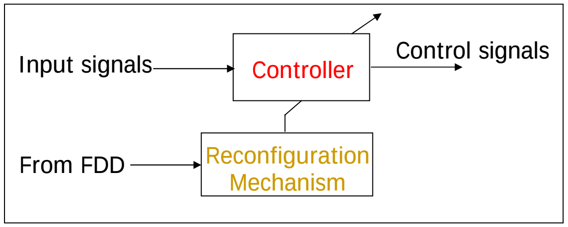
Multiple Kalman Filters (Fault Isolation)

Two-stage Kalman Filters (Fault Diagnosis)

Modules in AFTCS

Control Reconfiguration

- Purpose: To make the control system insensitive/ tolerant to the effects of failed components by modifying controller structure and/or parameters, based on the information from FDD module.
- Function of reconfigurable control



Input signals

Controller

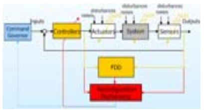
Control signals

From FDD

Reconfiguration Mechanism

- Design objective

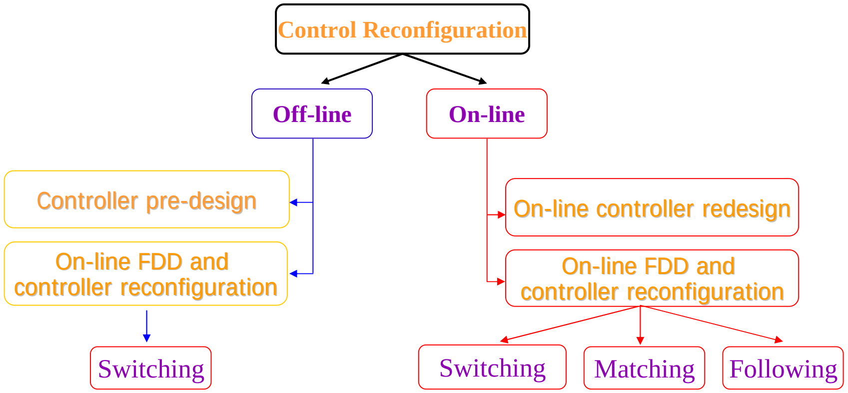
$$F\{(A_f,B_f,C_f),K_f\}\rightarrow F\{(A_n,B_n,C_n),K_n\}$$



Modules in AFTCS

Control Reconfiguration

- Existing design techniques and classification



Control Reconfiguration

Off-line

On-line

Controller pre-design

On-line FDD and controller reconfiguration

Switching

On-line controller redesign

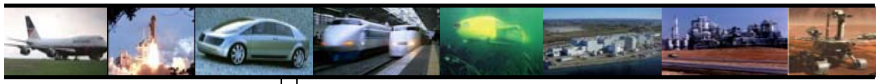
On-line FDD and controller reconfiguration

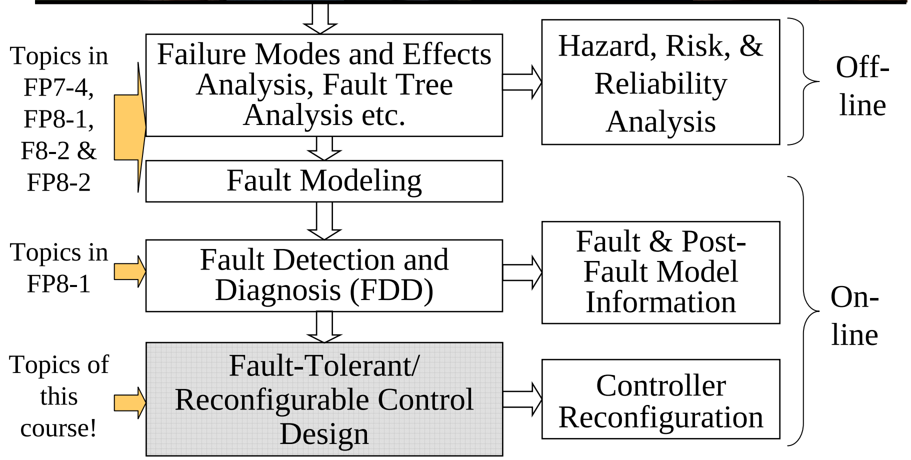
Switching

Matching

Following

Design Procedure in AFTCS





Topics in FP7-4, FP8-1, F8-2 & FP8-2

Failure Modes and Effects Analysis, Fault Tree Analysis etc.

Hazard, Risk, & Reliability Analysis

Off-line

Fault Modeling

Topics in FP8-1

Fault Detection and Diagnosis (FDD)

Fault & Post-Fault Model Information

On-line

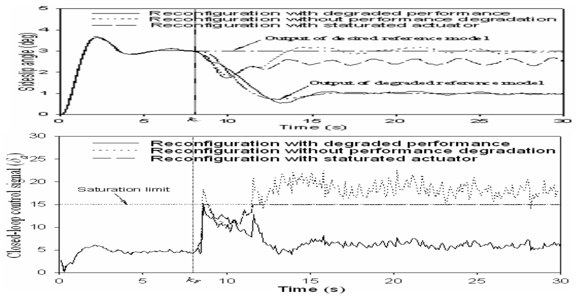
Topics of this course!

Fault-Tolerant/ Reconfigurable Control Design

Controller Reconfiguration

Design Considerations in AFTCS

An Illustrative Presentation



➢ **Three intervals**	Pre-fault	Duration of the fault	Post-fault
➢ **Stability**	Steady-state	Transient stability	Steady-state stability
➢ **Performance**	Steady-state	Transient and steady-state performance	
➢ **Control effort**	Minimal	Control redistribution without saturation	

- Bumpless transfer
- Steady-state error

- Saturation avoidance
- Control (re)allocation

These considerations have led to development of different reconfigurable control techniques

Two Main Modules:
FDD and Control Reconfiguration

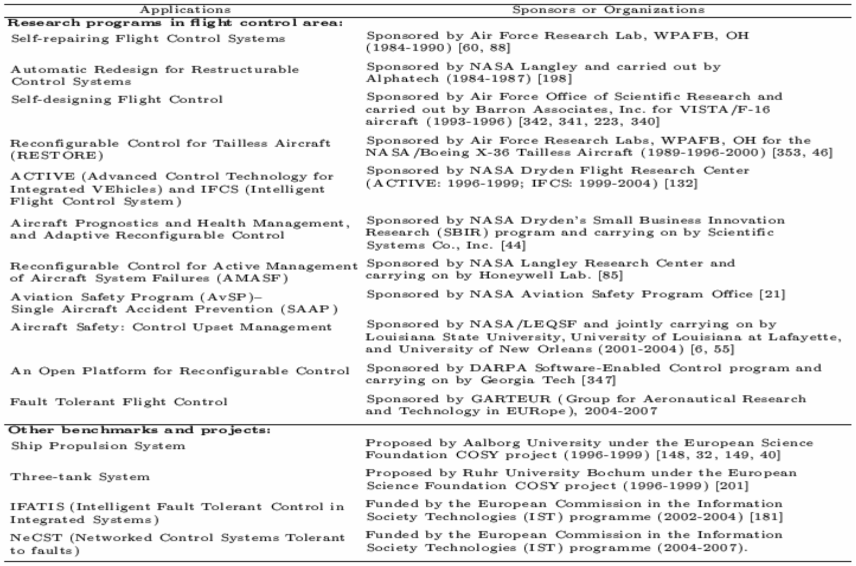
Redundancy; real-time; closed-loop; uncertainties; delays; nonlinearities…

Classification of Existing AFTCS

Criteria for Classification

- Classification Based on Control Algorithms
  - ➢ Mathematical tools used
    - ✓ Model-based
    - ✓ Intelligent
    - ✓ Combined
  - ➢ Design approach used
    - ✓ Pre-computed control laws
    - ✓ On-line automatic redesign
  - ➢ The way achieving reconfiguration
    - ✓ Switching
    - ✓ Matching
    - ✓ Following
- Classification Based on Application Fields
  - ➢ Conventional safety-critical systems
  - ➢ New application areas

Benchmarks on Fault-Tolerant Control



Applications	Sponsors or Organizations
Research programs in flight control area:	
Self-repairing Flight Control Systems	Sponsored by Air Force Research Lab, WPAFB, OH (1984-1990) [60, 88]
Automatic Redesign for Restructurable Control Systems	Sponsored by NASA Langley and carried out by Alphatech (1984-1987) [198]
Self-designing Flight Control	Sponsored by Air Force Office of Scientific Research and carried out by Barron Associates, Inc. for VISTA/F-16 aircraft (1993-1996) [342, 341, 223, 340]
Reconfigurable Control for Tailless Aircraft (RESTORE)	Sponsored by Air Force Research Labs, WPAFB, OH for the NASA/Boeing X-36 Tailless Aircraft (1989-1996-2000) [353, 46]
ACTIVE (Advanced Control Technology for Integrated VEhicles) and IFCS (Intelligent Flight Control System)	Sponsored by NASA Dryden Flight Research Center (ACTIVE: 1996-1999; IFCS: 1999-2004) [132]
Aircraft Prognostics and Health Management, and Adaptive Reconfigurable Control	Sponsored by NASA Dryden's Small Business Innovation Research (SBIR) program and carrying on by Scientific Systems Co., Inc. [44]
Reconfigurable Control for Active Management of Aircraft System Failures (AMASF)	Sponsored by NASA Langley Research Center and carrying on by Honeywell Lab. [85]
Aviation Safety Program (AvSP)– Single Aircraft Accident Prevention (SAAP)	Sponsored by NASA Aviation Safety Program Office [21]
Aircraft Safety: Control Upset Management	Sponsored by NASA/LEQSF and jointly carrying on by Louisiana State University, University of Louisiana at Lafayette, and University of New Orleans (2001-2004) [6, 55]
An Open Platform for Reconfigurable Control	Sponsored by DARPA Software-Enabled Control program and carrying on by Georgia Tech [347]
Fault Tolerant Flight Control	Sponsored by GARTEUR (Group for Aeronautical Research and Technology in EURope), 2004-2007
Other benchmarks and projects:	
Ship Propulsion System	Proposed by Aalborg University under the European Science Foundation COSY project (1996-1999) [148, 32, 149, 40]
Three-tank System	Proposed by Ruhr University Bochum under the European Science Foundation COSY project (1996-1999) [201]
IFATIS (Intelligent Fault Tolerant Control in Integrated Systems)	Funded by the European Commission in the Information Society Technologies (IST) programme (2002-2004) [181]
NeCST (Networked Control Systems Tolerant to faults)	Funded by the European Commission in the Information Society Technologies (IST) programme (2004-2007).

Challenges/Open Problems in FTCS

- Redundancy
  - Hardware versus Analytical (Software) Redundancy
  - Control Re-allocation and Re-distribution
- Modelling
  - On-line Identification for Closed-loop Systems with Reconfigurable Control
- Stability
  - Stability Analysis, Stability Guaranteed Design, and Stability Robustness
- Performance
  - Design for Graceful Performance Degradation
  - Transient/Transition Management Techniques
- Robustness
  - Dealing with FDD Uncertainties and Reconfiguration Delay, and Performance Robustness
- Nonlinearity
  - FTCS Design for Nonlinear Systems
  - Dealing with Constraints in Control Input (Actuator Saturation), State, and Output
- Integration
  - Integrated Design for AFTCS, and Integration of Passive and Active FTCS
  - Integration of Intelligent Actuator and Sensor Techniques to FTCS
  - Integration of Signal Processing, Control, Communication and Computing Technologies with Hardware and Software Implementation of Overall FTCS
- Safety and Reliability
  - Analysis and Assessment for Safety, Reliability and Reconfigurability
- Implementations and Applications
  - Real-time Issues
  - Wider Engineering Applications, beyond classic safety-critical systems
- New Development
  - Novel System Architectures, Design Approaches, and Applications

References and Reading Materials

- Reference books
  - ✓ Mufeed Mahmoud, Jin Jiang, Youmin Zhang, *Active Fault Tolerant Control Systems: Stochastic Analysis and Synthesis*, Springer-Verlag, May 1, 2003, ISBN: 3540003185.
  - ✓ Mogens Blanke, Michel Kinnaert, Jan Lunze, Marcel Staroswiecki, *Diagnosis and Fault-Tolerant Control*, Springer-Verlag, August 1, 2003, ISBN: 3540010564.
  - ✓ Chingiz Hajiyev and Fikret Caliskan, *Fault Diagnosis and Reconfiguration in Flight Control Systems*, Kluwer Academic Publishers, October 2003, ISBN 1-4020-7605-3.
  - ✓ Rolf Isermann, *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*, Springer-Verlag, Nov. 28, 2005.
- Lecture slides/notes
  - ✓ Please see the course webpage or the handouts distributed
- Course webpage
  - ✓ \\tun\web\cs\contribution\courses\fall2006\IRS9\FTC1\index.html

Readings

- Books
  - M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*, Springer, Berlin, 2003, pp. 1-26 (Chapter 1).
  - M. Mahmoud, J. Jiang, and Y. M. Zhang, *Active Fault Tolerant Control Systems: Stochastic Analysis and Synthesis*, Springer, Berlin, Germany, 2003, pp. 1-21 (Chapters 1 & 2).
- Papers
  - R. J. Patton, Fault-tolerant control: the 1997 situation, in *Proc. of IFAC Symp. on 3rd Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS)*, Hull, UK, Aug. 1997, pp. 1033-1055.
  - M. Blanke, C. Frei, F. Kraus, R. J. Patton, and M. Staroswiecki, What is fault-tolerant control? in *Proc. of the 4th IFAC Symp. on SAFEPROCESS*, Budapest, Hungary, June 2000, pp. 40-51.
  - Y. M. Zhang and J. Jiang, Bibliographical review on reconfigurable fault-tolerant control systems, in *Proc. of the 5th IFAC Symp. on SAFEPROCESS*, Washington, D.C., USA, June 2003, pp. 265-276.

Readings (cont'd)

- Lecture notes
  - Y. M. Zhang, *Introduction to Fault Tolerant Control Systems*, Fall 2005.
  - Y. M. Zhang, *Faults, Fault Analysis, and Fault Modeling*, Lecture notes #2 for FP8-1, Spring 2005.

FP9-1: Fault Tolerant Control Systems

Any comment or suggestion is welcome.