FP9-1: Fault Tolerant Control Systems

Youmin Zhang

Phone: 7912 7741 Office Location: FUV 0.22
Email: ymzhang@cs.aau.dk

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

US Air 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.

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

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, 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.

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

Flight 1080 – successful example
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.

Flight 191 accident – failed case
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.

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

A diagram associated with different faults in a controlled system

Controller fault
Controller

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](image)

Common Faults in Aircraft
(Example 1)

- An aircraft and its control surfaces

![Diagram of an aircraft and control surfaces](image)

<table>
<thead>
<tr>
<th>Control Surface</th>
<th>Failure</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>All control surfaces</td>
<td>One or more control surfaces become stuck at last position or control effectiveness is reduced.</td>
<td></td>
</tr>
<tr>
<td>Right elevator</td>
<td>Partial hydraulic loss</td>
<td>Maximum rate decreases on several control surfaces for hydraulic driven aircraft, or floating on light aircraft.</td>
</tr>
<tr>
<td>Left elevator</td>
<td>Full hydraulic loss</td>
<td>One or more control surfaces become stuck at last position.</td>
</tr>
<tr>
<td>Right elevator</td>
<td>Loss of part/all of control surface</td>
<td>Effectiveness of control surface is reduced, but rate is not; minor change in the aerodynamics.</td>
</tr>
<tr>
<td>Right elevator</td>
<td>Loss of engine/thrust</td>
<td>Large change in possible operating region; significant change in the aerodynamics.</td>
</tr>
<tr>
<td>Left elevator</td>
<td>Damage to aircraft surface</td>
<td>Possible change in operating region; significant change in aerodynamics.</td>
</tr>
<tr>
<td>All control surfaces</td>
<td>Aircraft icing</td>
<td>Effectiveness of control surface is reduced; slow change in aerodynamics.</td>
</tr>
<tr>
<td>Left elevator</td>
<td>Sensor malfunction</td>
<td>Minor if it is the only failure.</td>
</tr>
</tbody>
</table>
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
\[
\begin{align*}
\dot{x}(t) &= Ax(t) + Bu(t) \\
y(t) &= Cx(t)
\end{align*}
\]
\[
z(t) = My(t) = \begin{bmatrix} s_{11} & 0 & \cdots & 0 \\
0 & s_{22} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & s_{pp}
\end{bmatrix}
\begin{bmatrix} y_1(t) \\
y_2(t) \\
\vdots \\
y_p(t)
\end{bmatrix}
\]
\[
s_1 = [s_{11} s_{12} \cdots s_{1p}]^T
\]
\[
x \in \mathbb{R}^{n \times 1}, u \in \mathbb{R}^{m \times 1}, y \in \mathbb{R}^{p \times 1}, z \in \mathbb{R}^{q \times 1}, M \in \mathbb{R}^{q \times p}
\]
b. ARMA model
\[
y(t) = \psi^T(t) \theta_o
\]
\[
\psi(t) \ - \ Regression \ vector; \ \theta_o \ - \ parameter \ vector
\]

Modeling of System
(under dynamic fault conditions)

a. State-space model
\[
\begin{align*}
\dot{x}(t) &= Ax(t) + Bu(t) \\
\dot{x}(t) &= (A + \Delta A)x(t) + (B + \Delta B)u(t)
\end{align*}
t < t_f
\]
and
\[
\begin{align*}
y(t) &= Cx(t) \\
y(t) &= (C + \Delta C)x(t)
\end{align*}
t < t_f
\]
t >= t_f
\]
b. ARMA model
\[
\begin{align*}
y(t) &= \psi^T(t) \theta_o \\
y(t) &= \psi^T(t)(\theta_o + \Delta \theta)
\end{align*}
t < t_f
\]
t >= t_f
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 \( f_a \in \mathbb{R}^q \) is the constant bias term, and
\( L_a = \text{diag} \{l_1, l_2, \ldots, l_q\} \)
represents the operational modes of the actuators.

\[ l_i = \begin{cases} 
1 & t < t_f \text{ functional} \\
0 & t \geq t_f \text{ failure} 
\end{cases} \]

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:

\[ u_a(t) = L_a u(t) + (I - L_a(t)) f_a(t) \] (2.21)

where \( f_a(t) \in \mathbb{R}^l \) 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

\[
\begin{align*}
    u_a(t) &= \begin{cases} 
        u^i(t) & t < t_f \\
        l_a^i(t) & t = t_f \\
        l_a^f(t) & t_f < t 
    \end{cases} \\
    f_a(t) &= \begin{cases} 
        0 & t < t_f \\
        f^i_a(t) & t = t_f \\
        f^f_a(t) & t_f < t 
    \end{cases}
\end{align*}
\]

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

\[
\begin{align*}
    \dot{x}(t) &= Ax(t) + Bu_a(t) \\
    &= Ax(t) + BL_a(t)u(t) + B(I - L_a(t)) f_a(t) \\
    y(t) &= Cx(t)
\end{align*}
\] (2.23)

Sensor faults

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

where \( L_s \in \mathbb{R}^{m \times m} \) represents the operational modes of the sensors, and \( f_s \in \mathbb{R}^{m \times 1} \) is the sensor bias.

• Compared to actuators, it is relatively easy to install multiple sensors.
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]. Similarly to the above mathematical modelling to actuator faults, sensor faults can be represented similarly as following:

\[ z(t) = L_a(t) M x(t) + (1 - L_a(t)) f_a(t) \]  

(2.24)

where the matrix \( L_a \in \mathbb{R}^{m \times m} \) is similarly defined as in \( L_a \) and \( f_a(t) \in \mathbb{R}^m \) corresponds to the unknown bias term.

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

\[
z^i(t) = \begin{cases} 
  m^i x(t) & L^i_a(t) = 1; f^i_a = 0 \quad \text{for all } t \geq t_0 \quad \text{Fault free} \\
  m^i x(t) + f^i_a(t) & L^i_a(t) = 0; f^i_a(t) = 0 \quad \text{for all } t \geq t_F \quad \text{Loss of effectiveness} \\
  m^i x(t) + f^i_a(t) & L^i_a(t) = 0; |f^i_a(t)| = c^i t \quad \text{for all } t \geq t_F \quad \text{Drift} \\
  m^i x(t) & L^i_a(t) = 1 \quad \text{for all } t \geq t_F \quad \text{Freezing} 
\end{cases}
\]

(2.25)

where \( m^i \) represents the \( i \)th column element in sensor gain matrix, \( M \), corresponding to the \( i \)th state variable.

---

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 \( u^m \) sensor redundancy) to add extra actuator redundancy due to limitations of power, size, cost ...

---

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:

\[
\begin{align*}
\dot{x}(t) &= A x(t) + B u(t) & t < t_F \\
\dot{x}(t) &= (A + \Delta A) x(t) + (B + \Delta B) u(t) & t \geq t_F
\end{align*}
\]

(2.26)

and

\[
\begin{align*}
y(t) &= C x(t) & t < t_F \\
y(t) &= (C + \Delta C) x(t) & t \geq t_F
\end{align*}
\]

(2.27)

where \( t_F \) is the time instant at which the fault occurred, and \( \{\Delta A, \Delta B, \Delta C\} \) are the \( f \) 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 (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**

---
Example: Redundancy in Boeing 777

- Primary Flight Control Surfaces

![Image of Boeing 777 Flight Controls](image-url)

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

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)

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

ACE: Actuator Control Electronics
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
EDU: 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
MEB: 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
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: Properties of control systems:
- System/Plant/Process
- Sensors
- Actuators
- Controllers
- 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**

  ![Diagram](Image)

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

**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**

  ![Diagram](Image)

  ![Diagram](Image)

  Design objective

\[ F\{A_f, B_f, C_f, K_f\} \rightarrow F\{A_n, B_n, C_n, K_n\} \]

**Existing design techniques and classification**

- **Off-line**
  - Controller pre-design
  - On-line FDD and controller reconfiguration

- **On-line**
  - On-line controller redesign
  - On-line FDD and controller reconfiguration

  ![Diagram](Image)
### 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** → **Fault Modeling**
- **Topics in FP8-1**
- **Fault Detection and Diagnosis (FDD)** → **Fault & Post-Fault Model Information** → **Controller Reconfiguration**
- **Topics of this course!**

### Design Considerations in AFTCS

- **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

These considerations have led to development of different reconfigurable control techniques...

### 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

<table>
<thead>
<tr>
<th>Application</th>
<th>Sponsor or Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by Air Force Research Lab, WPAFB, OH (1994-1996) [96, 97]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by NASA Langley and carried out by Alphatech [1984-1986] [198]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by Air Force Office of Scientific Research and carried out by Boeing, Inc. for USAF/P-18 aircraft (1991-1993) [92, 95, 96]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by NASA Dryden's Small Business Innovation Research (SBIR) program and carried out by Scientific Systems Co., Inc. [14]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by NASA Langley Research Center and the Institute of Aviation Safety Management [21]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by NASA Dryden and the Institute of Aviation Safety Management [21]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by NASA Aviation Safety Program Office [21]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by NASA/DRSE and jointly carrying out by Louisiana State University, University of Louisiana at Lafayette, and University of New Orleans [2005-2006] [5, 55]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by DARPA, Software-Enabled Control program and carrying out by Georgia Tech [547]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by DAREUS (Group for Aeronautical Research and Technology in Europe), 2004-2007</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Sponsored by DAREUS (Group for Aeronautical Research and Technology in Europe), 2004-2007</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Proposed by Aalborg University under the European Science Foundation COST project [1996-1997] [198, 32, 192, 46]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Proposed by Ruhr University Bochum under the European Science Foundation COST project [1996-1997] [201]</td>
</tr>
<tr>
<td>Aircraft System Faults (AMCF)</td>
<td>Funded by the European Commission in the Information Society Technologies (IST) programme (2002-2006) [181]</td>
</tr>
</tbody>
</table>
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**

- **Lecture slides/notes**
  - Please see the course webpage or the handouts distributed

- **Course webpage**
  - \tun\web\ics\contribution\courses\fall2006\IRS9\FTC1\index.html

Readings

- **Books**

- **Papers**
FP9-1: Fault Tolerant Control Systems

Any comment or suggestion is welcome.