A DESIGN APPROACH TO FAULT TOLERANT CONTROL OF DISTRIBUTED SYSTEMS

Marta Capiluppi
(mcapiluppi@deis.unibo.it)

CASY - DEIS
University of Bologna
Summary

• Why distributed systems?
• A modular/hierarchical FTC architecture:
  - Synthesis → functionality oriented design procedure
  - Analysis → reliability analysis of complex diagnosis systems
• Applications:
  - The two-tanks system
  - The robotic manipulator
• Conclusions and future works

Results realised in the framework of European Project IFATIS: Intelligent Fault Tolerant control in Integrated Systems (EU-IST-2001-32122); http://ifatis.uni-duisburg.de
Distributed systems

- **COMPOSABILITY:** system properties follow from subsystem properties
- **SCALABILITY:**
  - no limits to the extensibility of a system
  - complexity do not depend on the system size
- **DEPENDABILITY:** welldefined error-containment regions
Distributed systems: fault propagation

Fault

1. Detect the failed node
2. Isolate all nodes in the error containment region to avoid propagation
3. Redistribute tasks and resources
A modular/hierarchical FTC architecture

The architecture must follow the distributed nature of the system
3-levels modular architecture for fault tolerant control of distributed systems
The supervisor

- FDI Decision Unit
- Events generator Unit
- Decision logic

- Objectives Performance
- Resources limitations

- Diagnosis signals
- Confidences Indeces
- Actual Working modes
- Resource Needs

- New Working Modes
- New objectives

04/04/2005  Marta Capiluppi - CASY research survey
Hierarchy of the supervisor

- FTC/FTM cell
- Local reconfiguration and mode control
- Function Monitor
- Resource Needs
- Resource and reconfiguration manager
- Resource and Reconfiguration Manager
- HW
- SW
- WM (WItnessing Manager)

- Diagnostic signals
- Interfaces with plant
A first functional analysis on the system in the sense of IEC standard 61499 → main functionalities of the system → function blocks

Further decomposition → functionalities/fault trees

**Functionalities Tree:**
1. Global functionalities
2. Local functionalities

**Fault Tree:**
1. Faults
2. Failures
3. Failure modes (structural analysis)
GLOBAL OBJECTIVE

LOCAL OBJECTIVE 1

LOCAL OBJECTIVE 2

LOCAL OBJECTIVE 3

LOCAL OBJECTIVE 4

FM1

FM2

FM3

Residual generation $\Rightarrow$ residual matrix

Sensitivity to different failures
$\Rightarrow$ Associate residual signals to loss of functionalities at different levels
$\Rightarrow$ Failure Modes (FM)

E.g.: Structural analysis to detect faults at different levels
Hierarchy for reconfiguration

Possible reconfiguration actions

- Working Modes (WM)

Reconfigure some functionalities after a fault at different levels

- Associate WMs to the reconfigurable functionalities

E.g.: Structural analysis to identify reconfigurable functionalities
The Two-Tanks System (1/2)

\[
S_1 \dot{L}_1 = Q_1 - Q_{12} - Q_{F1}
\]

\[
S_2 \dot{L}_2 = Q_2 + Q_{12} - Q_{F2}
\]

\[
Q_{12} = \text{sign}(L_1 - L_2)(k_1 V_{12} + k_2)\sqrt{|L_1 - L_2|}
\]

\[
Q_{F1} = R_1 \sqrt{L_1}
\]

\[
Q_{F2} = R_2 \sqrt{L_2}
\]

Sensors:
L_1, L_2, Q_1, Q_2, Q_{12}, Q_{F1}, Q_{F2}

Actuators:
Q_1, Q_2

Control objectives:
\[
y_1 = R_1 \sqrt{L_1} + R_2 \sqrt{L_2} = y_1^*
\]

\[
y_2 = \frac{R_1 \sqrt{L_1}}{R_2 \sqrt{L_2}} = y_2^*
\]
The Two-Tanks System (2/2)

Faults:
- $\bar{Q}_2 \rightarrow$ Actuator fault on pump 2
- $\bar{R}_{12} \rightarrow$ HW fault on valve $V_{12}$
- $\delta Q_{F2} \rightarrow$ Leakage fault on tank 2
- $\delta L_2 \rightarrow$ Sensor fault on level sensor 2

First system decomposition

Residual generation

System Structural Properties

Residual signals

Residual matrix

<table>
<thead>
<tr>
<th></th>
<th>$\bar{Q}_2$</th>
<th>$\bar{R}_{12}$</th>
<th>$\delta Q_{F2}$</th>
<th>$\delta L_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r_1$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$r_2$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$r_3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$r_4$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

04/04/2005

Marta Capiluppi - CASY research survey
Two-tanks: Hierarchy for diagnosis

FTC

NO \( y_1^*, y_2^* \)

or

NO \( L_1^* \)

NO \( L_2^* \) \( r_2 \)

or

NO \( Q_1^* \)

NO \( Q_{F2}^* \) \( r_4 \)

or

\( \delta Q_{F2} \)

REGULATOR

ACTUATOR

\( \bar{Q}_2 \)

FTM

NO \( L_{2est} \)

r_{2/r4}

\( \delta L_2 \)

NO \( f(L_2) \)

NO \( Q_{F2m} \)

\( \delta Q_{F2} \)

r_{1/r3}

NO \( L_{2m} \)
Two-tanks: Reconfiguration actions

Nominal Working Modes:
- WM0 – Nominal WM for decoupled tanks (valve V_{12} closed)
- WM0’ – Nominal WM for coupled tanks (valve V_{12} open)

Faulty Working Modes:
- WM1/2 – Reconfiguration after fault \( \bar{Q}_2 \) (valve V_{12} closed), choosing control objective \( y_1 \) or \( y_2 \)
- WM3/4 – Reconfiguration after fault \( \bar{Q}_2 \) (valve V_{12} open), choosing control objective \( y_1 \) or \( y_2 \)
- WM5 – Zero-impact reconfiguration after leakage fault (robust control).
- WM6 – Zero-impact reconfiguration after sensor fault \( \delta L_2 \) managed by FTM.
- WM8 – Zero-impact reconfiguration after fault on valve V_{12}.

<table>
<thead>
<tr>
<th>Nominal WM</th>
<th>( y_1^* )</th>
<th>( y_2^* )</th>
<th>( \bar{Q}_2 )</th>
<th>( \bar{R}_{12} )</th>
<th>( \delta Q_{F2} )</th>
<th>( \delta L_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>WM0</td>
<td>✔</td>
<td>--</td>
<td>WM1</td>
<td>--</td>
<td>WM5</td>
<td>WM6</td>
</tr>
<tr>
<td>WM0</td>
<td>--</td>
<td>✔</td>
<td>WM2</td>
<td>--</td>
<td>WM5</td>
<td>WM6</td>
</tr>
<tr>
<td>WM0’</td>
<td>✔</td>
<td>--</td>
<td>WM3</td>
<td>WM8</td>
<td>WM5</td>
<td>WM6</td>
</tr>
<tr>
<td>WM0’</td>
<td>--</td>
<td>✔</td>
<td>WM4</td>
<td>WM8</td>
<td>WM5</td>
<td>WM6</td>
</tr>
</tbody>
</table>
Two-tanks: Hierarchy for reconfiguration

Local reconfiguration and mode control

FTC

WM1/2
WM3/4

y₁*, y₂*

L₁*

L₂*

Q₂*

Qₚ₂*

REGULATOR

ACTUATOR

FTM

WM5

L₂est

WM5/6

L₂m

or

f(L₂)

Qₚ₂m
Two-tanks: decision logic specifications (I)

Fault Tree FTC

Top level supervisor (2)

First level supervisor (1)
Two-tanks: decision logic specifications (II)

Fault Tree FTM

FTM supervisor (3)

Global supervisor

Switch redundant hardware: valve $V_{12} \rightarrow$ valve $V'_{12}$
Two-tanks: Final architecture

PP: Control objectives

PP: Measure level 2

Connecting valves V12, V12'

04/04/2005
Marta Capiluppi - CASY research survey
Two-tanks: Experimental Results

Fault on pump 2 at time $t=2000$ sec and set-point changes.

Control Objective $y_1^*$

Control Objective $y_2^*$
Reliability analysis

- Reliability: probability that a given item is still performing its function after a given amount of time
- Reliability of the diagnostic system: capability of not generating false alarms and missed diagnosis
- Automatic procedure to compute the reliability of the distributed system as a function of the “quality” of local FDI filters and of the “quality” of the components subject to faults
- Procedure for the offline and online design of the FDI units
- Offline: suitably sizing the Fault Tolerant Modules to achieve a prescribed reliability for the whole system ➔ optimal dimensioning of the physical components and diagnostic algorithms
- Online: statistical residual matrix ➔ measure of the probability of right detection and isolation
Reliability of components and function monitoring

- The fundamental index for reliability of components is
  
  **Failure rate** $\lambda(t)$: how many items, over a statistically identical population of components, failed at time $t$.

- Reliability function:
  
  $$ R(t) = e^{-\int_0^t \lambda(x)dx} $$
  
  $$ R = R(T) = e^{-\lambda T} = \text{const.} $$

- The fundamental indexes for residual signals are **missed diagnosis rate** $\lambda_{MD}(t)$ and **false alarms rate** $\lambda_{FA}(t)$

- They can be computed through a Monte Carlo method
Reliability analysis at different levels

GLOBAL OBJECTIVE

LOCAL OBJECTIVE 1

LOCAL OBJECTIVE 2

LOCAL OBJECTIVE 3

LOCAL OBJECTIVE 4

\[ r_1 ; \lambda_{MD}^1 ; \lambda_{FA}^1 \]

\[ r_2 ; f(\lambda_1, \lambda_2) \]

\[ r_3 ; \lambda_{MD}^3 ; \lambda_{FA}^3 \]

or

or

Function Monitor

Loss of j-th functionality

\[ g(\lambda_1, \lambda_2, \lambda_3) \]

\[ \lambda_j \]

\[ \lambda_{MD}^i ; \lambda_{FA}^i \]

\[ \lambda_1 ; \lambda_2 ; \lambda_3 \]

\[ r_i \]
Computing reliability of each elementary cell

Safety critical systems:
Stay into the safe zone, tolerate false alarms do not allow missed diagnosis.

- Safe Reliability Function (SRF) = probability of being in state H+R

To enhance SRF:
Enhance physical components \( \downarrow \lambda_j \)
Enhance residual sensitivity \( \downarrow \lambda_{MD} - \uparrow \lambda_{FA} \)

High performance systems:
Stay into the performant zone, do not allow false alarms and missed diagnosis.

- Performance Reliability Function (PRF) = probability of being in state H

To enhance PRF:
Enhance physical components \( \downarrow \lambda_j \)
The robot manipulator (1/2)

6DoF Manipulator with a gripper

Sensors:
• 7 encoders
• Optical 3D sensor in the gripper
• Compliant force-torque sensor between wrist and gripper

Actuators:
• 7 actuators

Problem: “Peg in Hole” ➔ 4 phases:
1. robot moves from home position to peg position (position control)
2. gripper picks peg (hybrid force - position control)
3. robot moves from peg position to hole position (position control)
4. peg fitted in hole (hybrid force - position control + optical 3D sensor)
3 functionalities
• **Trajectory tracking**: this functionality is used for phases 1 and 3 of the problem;
• **Peg Picking**: phase 2 of the problem;
• **Peg Fitting into hole**: phase 4 of the problem.

\[
B(q)\ddot{q} + N(q, \dot{q}) = \tau_c + \tau_f + J(q)^T(F_m + F_f) + J_c(q)^TF_c
\]

**Fault scenario**
• fault of the force-torque sensor (**FTF**)
• fault of the optical 3D sensor (**3DF**)
• fault of actuator (**AFi**) or encoder (**EFI**) integrated into the i-th joint (i= 1 ...,6)
• fault on gripper actuator (**AF7**) or encoder (**EF7**)
• collisions with unexpected obstacles (**CF**)
Robot: Residual generation

• Use of generalized momenta and neuro-fuzzy residual evaluation
  ➔ residual signals sensitive to all considered faults but 3DF
• Electric test for fault 3DF
• To augment the detectability of encoders faults
  ➔ residual signals generated via electrical tests

- \( r_i \) (\( i = 1, \ldots, 7 \)) residual generated as observation error for the generalized momentum of joint \( i \)
- \( r_{ti} \) (\( i = 1, \ldots, 7 \)) residual generated through electric test for encoder of joint \( i \)
- \( r_8 \) and \( r_9 \) residuals generated using a neuro-fuzzy elaboration of residuals \( r_1, \ldots, 7 \) and external sensors
- \( r_{3D} \) residual generated through electric tests for optical 3D sensor.

Robot: Reliability analysis

 conducts peg picking

 E1: finger position

 E2: force

 E3: actuator

 E4: sensor

 AF7

 EF7

 FTF

 Reliability

 \[ R_{FA} \] \[ R_{MD} \]

 \[ r_{t7} \] \[ 0.99 \] \[ 0.99 \]

 \[ r_{7} \] \[ 0.94 \] \[ 0.98 \]

 \[ r_{8} \] \[ 0.99 \] \[ 0.96 \]

 Failure rate

 \[ \lambda \] \[ 50 \] \[ 100 \] \[ 80 \]

 Statistical Residual Matrix for safe state

 RS

 \[ r_{t7} \] \[ 0 \] \[ 0.999 \] \[ 0 \]

 \[ r_{7} \] \[ 0.999 \] \[ 0.9981 \] \[ 0.9985 \]

 \[ r_{8} \] \[ 0 \] \[ 0 \] \[ 0.9969 \]

 Statistical Residual Matrix for reliable state

 RR

 \[ r_{t7} \] \[ 0 \] \[ 0.8958 \] \[ 0 \]

 \[ r_{7} \] \[ 0.8942 \] \[ 0.8505 \] \[ 0.8677 \]

 \[ r_{8} \] \[ 0 \] \[ 0 \] \[ 0.9139 \]
Robot: Reconfiguration actions

Nominal WM:
WM0: System achieves the “Peg in Hole” problem

Faulty WMs:
WM1: zero-impact reconfiguration after an actuator fault AFi (new trajectory computation)
WM2: zero-impact reconfiguration after an encoder fault EFi (using an estimation of joint position)
WM3: reconfiguration after fault FTF on force sensor (only position control can be used)
WM4: reconfiguration after 3DF (for fitting only force – position control)
WM5: STOP after collision
Robot: Hierarchy for reconfiguration

FTC1

WM1

WM1

position of joint 1

position of joint 6

actuator

sensor

actuator

sensor

AF1

EF1

AF6

EF6

FTC2

WM2

WM2

finger position

collision

CF

FTC3

WM4

WM5

peg fitting

WM3

WM3

control

monitor

trajectory tracking

force

3DF

FTF

FTF

E2: force

E3: actuator

E3: sensor

E1: finger position

E1: peg picking

r1

r6

r7

r1, r7

r9

r1

r3D

r8
Conclusions and future works (1/2)

• Higher level structure for fault tolerant control of distributed systems:
  ✓ Synthesis: design procedure for modular architecture
  ✓ Analysis: procedure to compute reliability of the system
• What’s left?
  ✓ A deeper look: from nominal to reconfigured behavior
    ➔ what happens when the fault occurs?
  ✓ Why not hybrid systems representation?
Conclusions and future works (2/2)

Randomized algorithms for FTC

» System with fault = uncertain system

» Faults as uncertainties

\[
x(k + 1) = A(f)x(k) + B_1(f)d(k) + B_2(f)u(k)
\]
\[
e(k) = C_1(f)x(k) + D_{11}(f)d(k) + D_{12}(f)u(k)
\]
\[
y(k) = C_2(f)x(k) + D_{21}(f)d(k) + D_{22}(f)u(k)
\]

The vector of faults is \( f = [f_1, \ldots, f_n] \)
\[
f_i(k) = (1 + w_{f,i}(k)\delta_i)g_i(k)
\]

Fault estimate uncertainty (bounded)

» Random variable with given probability

Nominal value
Future works (1/2)

Dealing with detection and isolation time intervals

Nominal operating conditions $\xrightarrow{\text{fault}}$ Faulty operating conditions $\xrightarrow{\text{fault estimate}}$ Reconfigured operating conditions

- Certain system
- Uncertain system
- Predetermined reconfiguration actions

- Fault severity
- Randomized algorithms to determine whether the system is still reconfigurable or not
- FDI time

04/04/2005 Marta Capiluppi - CASY research survey
Future works (2/2)

- Use of randomized algorithms to deal with FDI time and fault reconfiguration possibilities
- Possible representation with hybrid systems
- Extension of the presented procedure
- A possible real application: “waste to energy” industrial plants (model and control for simulations)

Main publications

- IFATIS Deliverables and Reports
- C. Bonivento, M. Capiluppi, L. Marconi, A. Paoli – An integrated design approach to multilevel fault tolerant control of distributed systems. 16th IFAC World Congress, Praha, July 2005.