DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Socrates Lectures

Ancona July 6, 2004

Diagnosis and Fault-tolerant Control – with marine examples

Mogens Blanke
Automation at Ørsted•DTU
Technical University of Denmark (DK)

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

- Fault-tolerant control includes real-time fault diagnosis and take actions to avoid severe consequences of faults. Software makes "intelligent" assessment and remedial actions.
- The need is evident in many areas of application
- Autonomous systems clearly need fault-tolerant methods
- Ad hoc methods have been practiced for decades, a systematic methodology has evolved during the last.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 2.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Areas of particular interest

Fault-tolerant control

Created by the need for safety, reliability and availability.

Touches on fundamental properties of controlled systems and the control architectures.

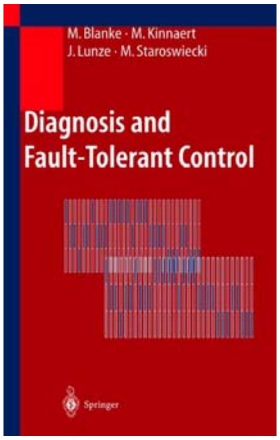
Diagnosis

The essential means to determine whether faults have occurred and thereafter locate their cause

M. Blanke 2004 Diagnosis& Fault-tolerant Control 3.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Material for Socrates Lectures



This ´short course is based on the book:

Diagnosis and Fault-tolerant Control. By M. Blanke, M. Kinnaert, J. Lunze and M. Staroswiecki.

Springer, 2003. 565 pp. ISBN 3-540-01056-4.

And on

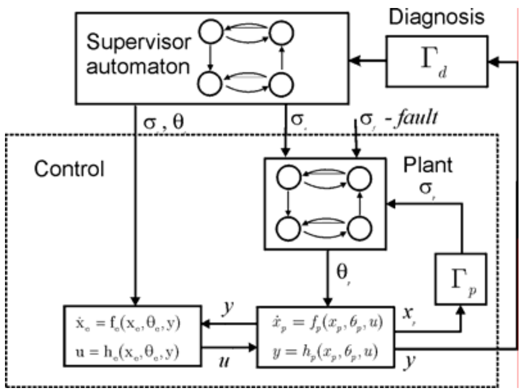
SaTool Users Manual by T. Lorentzen and M. Blanke, Oersted•DTU, Technical University of Denmark, April 2004.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 4.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Hybrid Structure of Plant + Controller



The standard problem in control

Objective: O

Structure: S

Parameters: θ

Control law: U

The control problem:

Solve $\langle O, S, \theta, U \rangle$

The system can be changed by events, some of which are faults. We may change the controller and/or the system by action of a supervisor.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

A Hybrid System

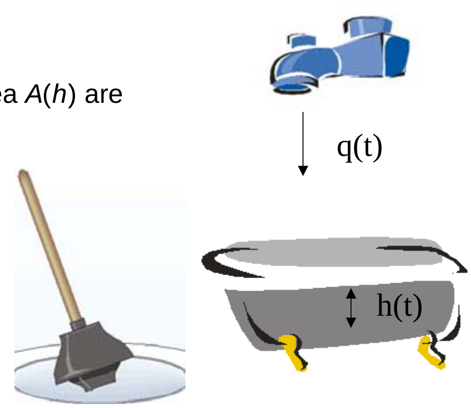
A bathtub is a hybrid system.

Dynamic relation between input flow *q*, height *h* and area *A*(*h*) are

$$\dot{h}(t) = \frac{1}{A(h)} q(t)$$

Holds only until the edge is reached:

$$\dot{h}(t) = 0 \quad \text{for} \quad h = h_{edge}$$



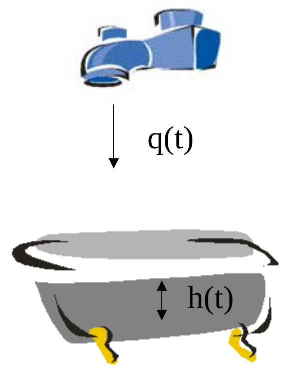
DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

A Hybrid System

Dynamic relation between
input flow q, height h and area $A(h)$ are

$$\dot{h}(t) = \frac{1}{A(h)} q(t) \quad \text{for } 0 \le h < h_{edge}$$

$$\dot{h}(t) = 0 \quad \text{for } h \ge h_{edge}$$

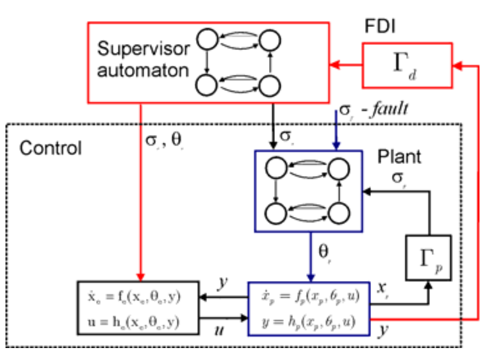


M. Blanke 2004 Diagnosis& Fault-tolerant Control 7.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Fault-accommodation

Fault accommodation



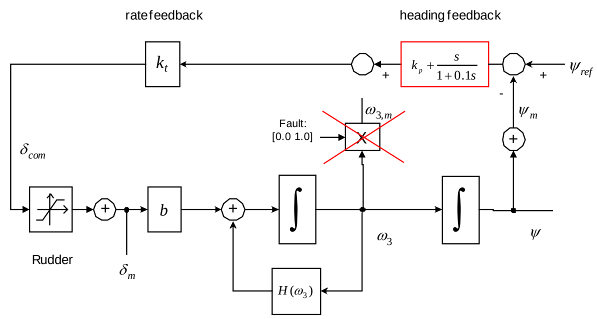
Change control parameters or structure to avoid the consequences of a fault.

Input-output between controller and plant is unchanged.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 8.

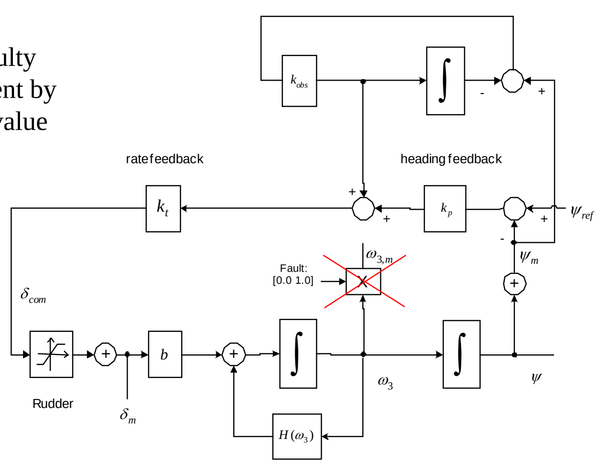
Handling of fault - reconfiguration

- Fault reconfiguration: a sensor failure in inner loop.
- Switch to differentiating control when fault is diagnosed



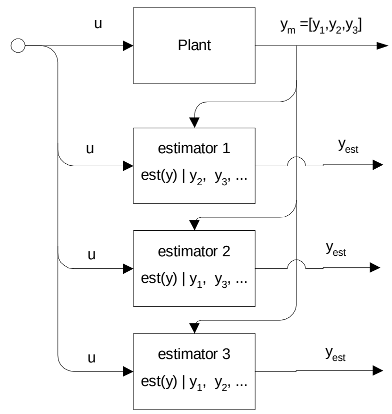
Handling of sensor fault by estimation

Replace faulty measurement by estimated value



DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Sensor fusion subject to faults



Simple sensor fusion

$\mathbf{y}(t) = \mathbf{S}\mathbf{y}_{valid}(t) + (\mathbf{I} - \mathbf{S})\hat{\mathbf{y}}(t)$

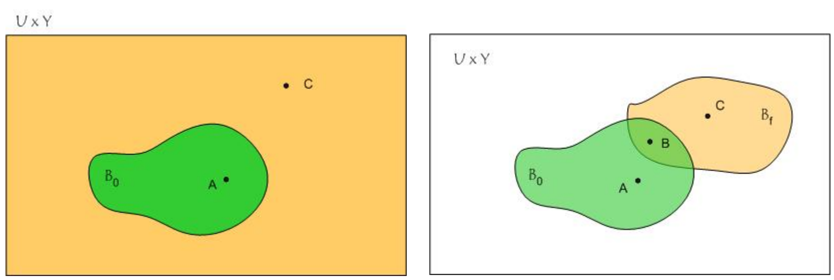
$\mathbf{S}$ is diagonal, $s_{i,i} \subset [0,1]$

- Faulty sensor measurement is replaced by an estimate, which is used in the feedback loop

M. Blanke 2004 Diagnosis& Fault-tolerant Control 12.

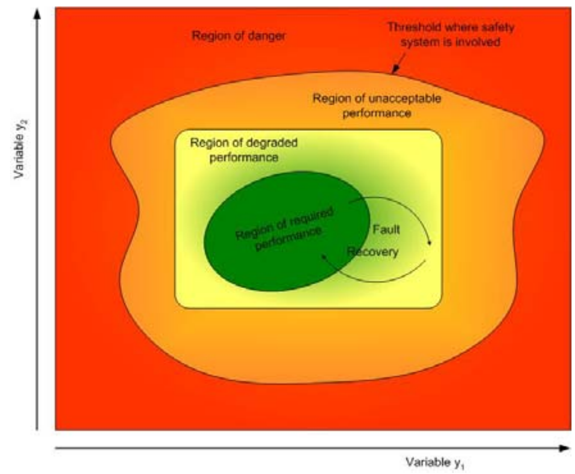
DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Diagnosis and behaviours

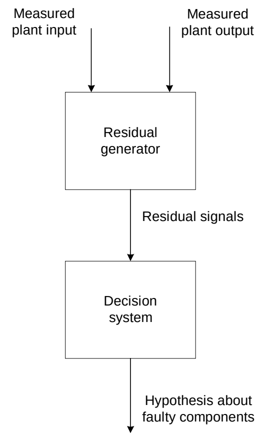


M. Blanke 2004 Diagnosis& Fault-tolerant Control 13.

Fault-tolerant versus safety problem



Fault diagnosis

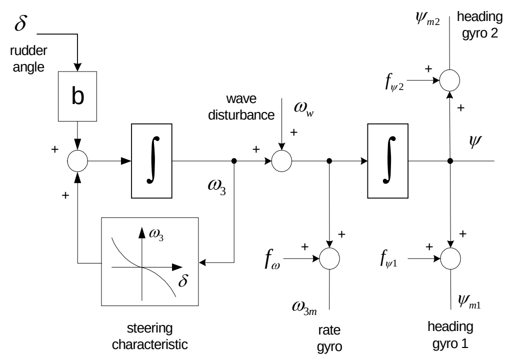


- Observe input-output behaviour to determine whether the system is ”normal” or ”faulty”
- A fault diagnosis can be achieved when redundant information is available
- Results:
  1. Hypothesis that a fault is present
  2. Hypothesis about which fault has occurred

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Running example: ship steering



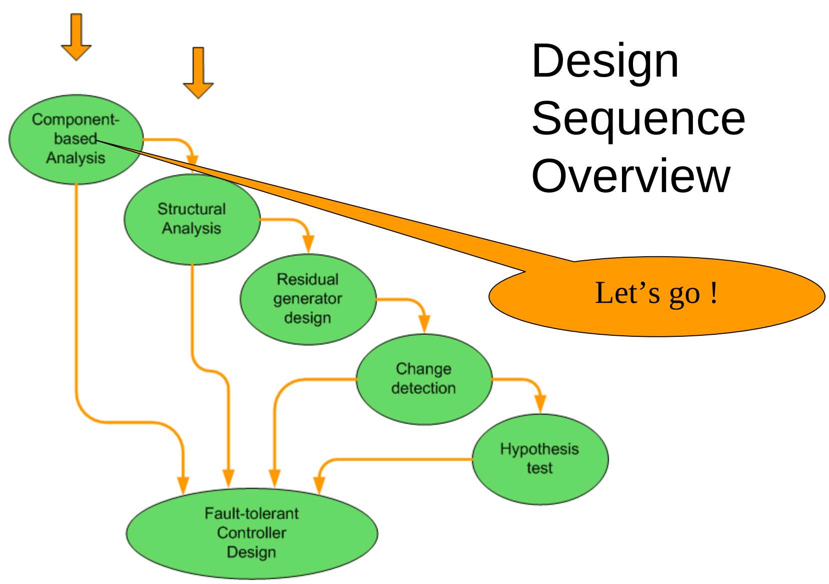
$$\dot{\omega}_3(t) = b\left(\delta(t) + H(\omega_3(t))\right)$$
$$\dot{\psi}(t) = \omega_3(t) + \omega_w(t)$$
$$\psi_{m1}(t) = \psi(t) + f_{\psi 1}(t)$$
$$\psi_{m2}(t) = \psi(t) + f_{\psi 2}(t)$$
$$\omega_{3m}(t) = \omega_3(t) + \omega_w(t) + f_\omega(t)$$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 16.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Design Sequence Overview



M. Blanke 2004 Diagnosis& Fault-tolerant Control 17.

Component-based Analysis

Chapter 4 in Diagnosis and Fault-tolerant Control

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

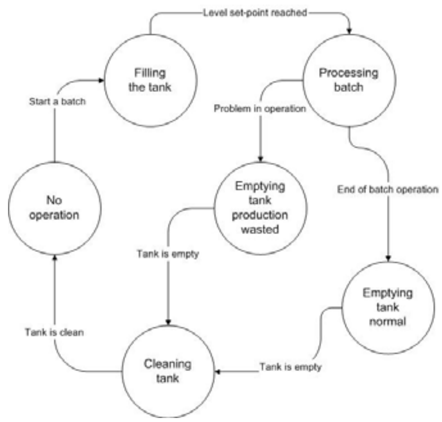
Contents

- Component faults / failure
- Fault propagation analysis (FPA)
- Component-based description for FPA
- Exercise: Battery charger

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Generic component model for a process tank (batch process)



Use-modes:

UM0: No operation

UM1: Filling the tank

UM2: Processing batch

UM3: Emptying via normal pipe

UM4: Empty via waste outlet

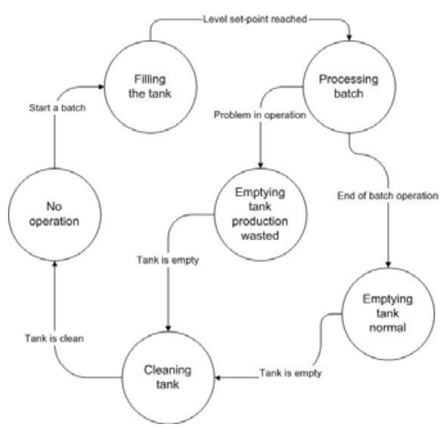
UM5: Cleaning the tank

M. Blanke 2004 Diagnosis& Fault-tolerant Control 20.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Generic component model - objectives



Objectives:

O-0: No action (um 0)

O-1: Reach full level (um 1)

O-2: Regulate temperature (um 2)

O-3: Reach empty level (um 3,4)

O-4: Clean tank (um 5)

O-5: Protect environmet (um1,2,3,4,5)

M. Blanke 2004 Diagnosis& Fault-tolerant Control 21.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Generic component model

Services are:
input-output behaviour, requests, activation conditions, resources

service :=< consumed variables, produced variables, procedure, request, activation condition, resources >

For component # k, service #i:

$S(k) = \{s_i(k), i \in I_s(k)\}$

$s_i(k) = \{cons_i(k), prod_i(k), proc_i(k), reqst_i(k), active_i(k), res_i(k)\}$

A system has different operating modes. The normal modes are denoted use-modes.

This leads to a FORMAL definition of a generic component

M. Blanke 2004 Diagnosis& Fault-tolerant Control 22.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Fundamental System Properties

•Which fault-tolerant properties can a particular system obtain?

•Which faults can be handled as desired?

•Means of analysis:

- Fault propagation *(with severity assessment) (chapter 4)*
- Analysis of structure *(to show available redundancy) (chapter 5)*
- Design of diagnostic algorithms for specific faults *(chapter 6)*
- How to obtain fault-tolerance *(how and which is better) (chapter 7)*
- Analysis of coverage *(likelihood to recover) (research topic – not treated in the book)*

M. Blanke 2004 Diagnosis& Fault-tolerant Control 23.

Paradigm for a systematic approach

Correct fundament if and only if all generic faults are included, which have an effect on component behaviour (*behaviour is the relation between input and output*)

The design is consistent when based on complete component fault information

Our systematic approach has the following steps:

- List of end effects (on the object) (method)
- Consequence and severity of these end effects (designeer)
- List of faults to detect (method)
- Required reaction to each fault that could cause high severity end effects (designer with support of tool)

Faults and their effects

For a chosen component (or function block):

Characterize the output signal (variable) as <low, high, fluctucting, undefined> organize in columns of a table (failure modes and effects matrix)

Row entries are: <input, faults>
Faults are <internal faults, interface faults>

This not a common FMEA scheme – it is FMEA information organized conveniently for analysis of fault propagation

turn rate signal	low	high	fluctuating	undefined
output	electric short	electric short	wire defect	wire defect
input	ships rate low	ships rate	supply power	dismounted
parts	defect: electrical mechanical	defect: electrical	unit damaged	unit damaged

The FMEA matrix for the rate gyro is defined by considering a generic failure of the rate gyro, which can cause any of the output signal conditions, given as input from the physical rate of turn of the ship.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Propagation of component failures/effects

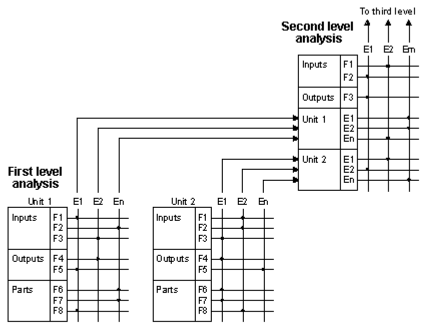


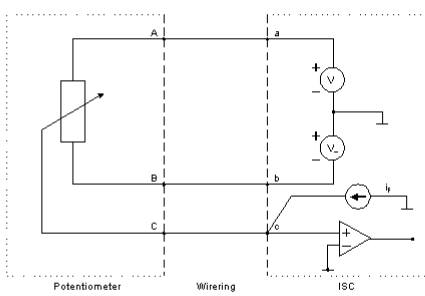
Figure 2.1: Failure Mode and Effect Analysis scheme illustrated graphically. Two component levels are shown.

Output signals (effects) from components (function blocks) at level one propagate to components (function blocks) at level two according to the way components are interconnected

M. Blanke 2004 Diagnosis& Fault-tolerant Control 26.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Fault propagation matrix for potentiometer



Interface to potentiometer with supply range offset and current injection into point "C" to obtain adequate detectability for any fault

The potentiometer has voltage at pin C as output

Comp. / effect	Too low signal	Not related to angle	Fluctu-ating signal	Too high signal
Input	broken wire at A short at A-B	Loss of supply	vibration	broken wire at A, short-circuit A-C
Output	short B-C	Broken wire at C	loose connec-tion	
Comp.		stuck, shaft or, element broken	Wiper fault	

M. Blanke 2004 Diagnosis& Fault-tolerant Control 27.

Fault propagation matrix for potentiometer

	V_l	V_{udf}	V_{fl}	V_h
…				
F_4 loose wire	0	0	1	0
f_3 break at C	0	1	0	0
f_2 short A-B	1	0	0	0
f_1 break at A	1	0	0	1
i_l	1	0	0	0
i_h	0	0	0	1
i_{fl}	0	0	1	0

Comp./ effect	Too low signal	Not related to angle	Fluctu-ating signal	Too high signal
Input	broken wire at A short at A-B	Loss of supply	vibration	broken wire at A, short-circuit A-C
Output	short B-C	Broken wire at C	loose connec-tion	
Comp.		stuck, shaft or, element broken	Wiper fault	

Fault propagation as boolean expression

Fault propagation expressed as Boolean expression

$$\begin{bmatrix} V_l \\ V_{udf} \\ V_{fl} \\ V_h \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} f_4 \\ f_3 \\ f_2 \\ f_1 \\ i_l \\ i_h \\ i_{fl} \end{bmatrix}$$

Boolean mapping

Fault Propagation Analysis provides FMEA –matrix schemes for the observable effect of component failure:

Boolean mapping of component faults $f_c \in \mathfrak{F}$ onto end effects $e_c \in \mathfrak{E}$:

$$M: \mathfrak{F} \times \mathfrak{E} \rightarrow \{0,1\};$$

$$m_{ij} = \begin{cases} 1 \text{ if } f_{ci} = 1 \Rightarrow e_{ci} = 1 \\ 0 \text{ otherwise} \end{cases}$$

Algebra for fault propagation analysis

FMEA matrix representation

$e_{ci} \leftarrow M_i^f \otimes f_{ci}$ defined by

$e_{cik} \leftarrow (m_{ik1} \wedge f_{ci1}) \vee (m_{ik2} \wedge f_{ci2})....$

Fault propagation

$$e_{ci} \leftarrow M_i^f \otimes \begin{bmatrix} f_{ci} \\ e_{ci-1} \end{bmatrix}$$

System FPA desctiption

$e \leftarrow M \otimes f_c$

Reverse analysis

System FPA description

$e \leftarrow M \otimes f_c$

Reverse analysis through the coding set M^T

a) $f_c \leftarrow M^T \odot e$ defined by

$f_{ci} \leftarrow (e_1 = m_{i1}) \wedge (e_2 = m_{i2}) \wedge ...$

is applied to licate a single faults but mai fall short if there are simultaneous faults

b) $f_c \leftarrow M^T \otimes e$ defined by

$f_{ci} \leftarrow (m_{ik1} \wedge e_{ci1}) \vee (m_{ik2} \wedge e_{ci2})....$

is more conservative but can work for simultaneous faults

Reverse analysis – potentiometer case

$f_c \leftarrow M^T \otimes e$ defined by

$f_{ci} \leftarrow (e_1 \wedge m_{i1}) \vee (e_2 \wedge m_{i2}) \vee ...$

$$\begin{bmatrix} f_4 \\ f_3 \\ f_2 \\ f_1 \\ i_l \\ i_h \\ i_{fl} \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} V_l \\ V_{udf} \\ V_{fl} \\ V_h \end{bmatrix}$$

Connection of components

Connection of two components:
note f_{c1} could be composed by <f_1,i_1…>

$$e_{c2} \leftarrow \left[M_2 \otimes \begin{bmatrix} I & 0 \\ 0 & M_1 \end{bmatrix} \right] \otimes \begin{bmatrix} f_{c2} \\ f_{c1} \end{bmatrix} \Leftrightarrow$$

$$e_{c2} \leftarrow [M_2, M_2 \otimes M_1] \otimes \begin{bmatrix} f_{c2} \\ f_{c1} \end{bmatrix}$$

It is easy to obtain a propagation matrix for the total system.

Given a list of all component faults we get the complete set of end effects.

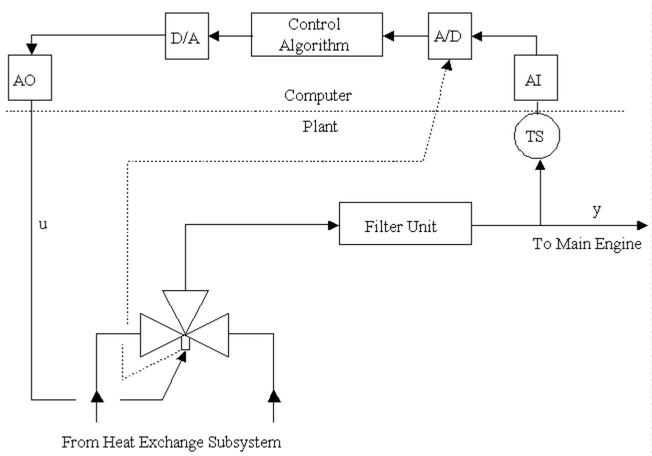
This method is inherently correct !

Closed loop problem

- Logical closed loops pose special problems
- Be aware there is a difficulty

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Temperature control with motor driven valve



M. Blanke 2004 Diagnosis& Fault-tolerant Control 40.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Relay controlled valve motor

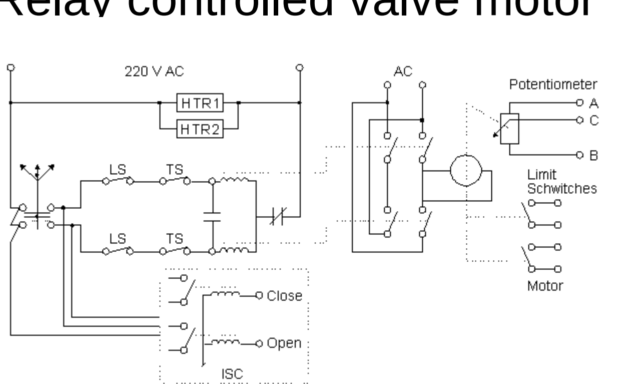
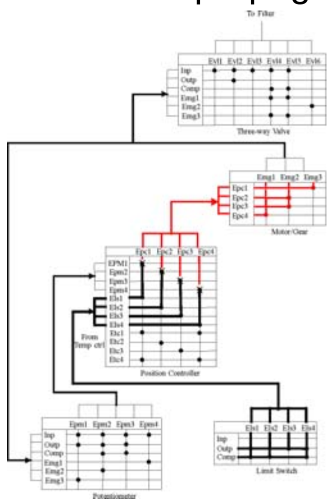


Figure 4.4: Operation of 3-way valve actuator with relay operated induction motor. Abbreviations are: o:open, c:close, s:stop, HTR:Heater, LS:Limit Switch, TS:Torque Switch.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 41.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Fault propagation for valve motor loop



- Example: position control loop for a valve.
- Includes potentiometer feedback (position) and limit switches (end stop detection)
- A fault in a limit switch will propagate as shown with bold line
- We could stop the propagation of the fault where the red lines begin.
- The means is fault detection and accommodation.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 42.

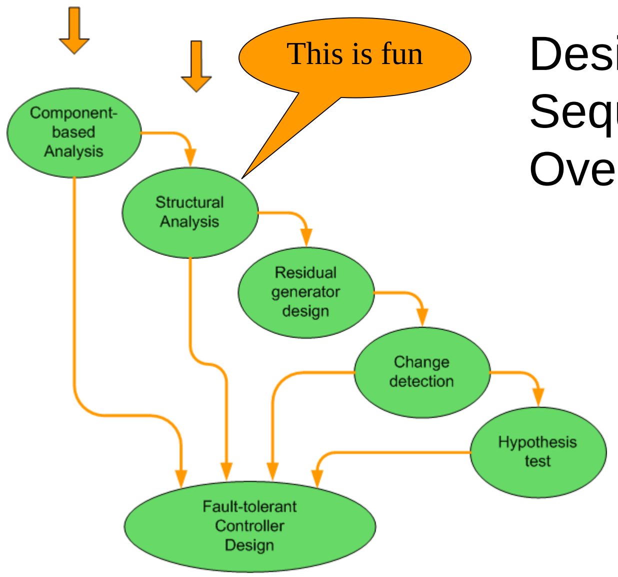
DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Analysis based on structure

Sections 5.1 – 5.3, pp 99-122

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Design Sequence Overview



M. Blanke 2004 Diagnosis& Fault-tolerant Control 44.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

What is a graph

Citations on graph theory in this lecture are from Shaum's outlines: Graph Theory by V. K. Balakrishnan, McGraw-Hill, 1997.

"A graph G consists of a set of Vertices
and a collection E of pairs of vertices called edges
.
A graph is symbolically represented as G = (V, E).
The order of a graph is its number of vertices,
the size of a graph is the number of its edges."

M. Blanke 2004 Diagnosis& Fault-tolerant Control 45.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Digraph for linear system

Example 5.2

$$c_1 : \dot{x}_1 = \frac{d}{dt} x_1$$

$$c_2 : \dot{x}_1 = a x_2$$

$$c_3 : \dot{x}_2 = \frac{d}{dt} x_2$$

$$c_4 : \dot{x}_2 = b x_1 + c x_2 + d u$$

Graph represented as the incidence matrix:

	u	x_1	x_2	$\dot{x}_1$	$\dot{x}_2$
c_1	0	1	0	1	0
c_2	0	0	1	1	0
c_3	0	0	1	0	1
c_4	1	1	1	0	1

M. Blanke 2004 Diagnosis& Fault-tolerant Control 46.

DANMARKS TEKNISKE UNIVERSITET

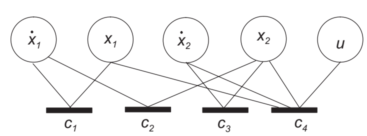
Ørsted•DTU

Bipartite graph

Graph represented as incidence matrix:

	u	x_1	x_2	$\dot{x}_1$	$\dot{x}_2$
c_1	0	1	0	1	0
c_2	0	0	1	1	0
c_3	0	0	1	0	1
c_4	1	1	1	0	1

Or drawn as a bipartite graph:



"A **simple** graph is one with no parallel edges and loops. A **bipartite** graph is a simple graph in which the set of vertices can be partitioned into two sets such that every edge is between a vertex in C and a vertex in Z: $G = (C, Z, E)$."

M. Blanke 2004 Diagnosis& Fault-tolerant Control 47.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Structural Model

Consider : $\dot{x}(t) = g(x(t), u(t), \theta)$
$y(t) = h(x(t), u(t), \theta)$

Behaviour of a model: (C,Z) with

Z = $\{z_1, z_2, .. z_n\}$ are variables and parameters: $Z = x \cup u \cup y \cup \theta$

C = $\{c_1 ... c_m\}$ a set of constraints: $C = g \cup h$ where

g is the set of differential constraints: $\dot{x}_i(t) - g_i(x(t), u(t), \theta), i = 1, \ldots, n$

h is measurement constraints: $y_j(t) - g_j(x(t), u(t), \theta), i = 1, \ldots, p$

Definition 5.3:

The structural model of the system (C,Z) is a bi-partite graph (C, Z, E) where $E \subset C \times Z$ is the set of edges defined by:

$(c_i, z_j) \in E$ if the variable z_j appears in constraint c_i

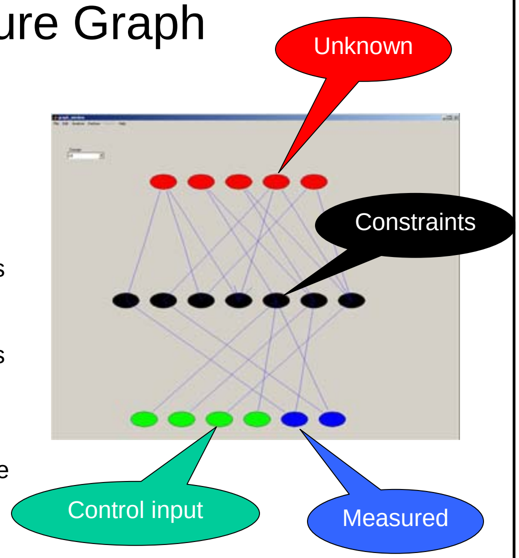
M. Blanke 2004 Diagnosis& Fault-tolerant Control 48.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Structure Graph

Structural analysis

A graph-based technique where principal relations between variables express the system's properties. Measured and controlled quantities in the system are related to variables through functional relations, which need not be explicitly stated. The user specifies a list of these relations that together describe the functionality of the system considered. A list of such variables and functional relations constitute the system's structure graph.

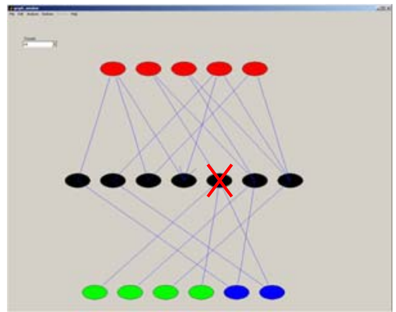


M. Blanke 2004 Diagnosis& Fault-tolerant Control 49.

A Fault is a Violation of a Constraint

Faults

Normal operation means all functional relations are intact for the system. Should faults occur, one or more functional relations cease to be valid. In the structure graph, one or more nodes of the graph will disappear when a fault occurs.

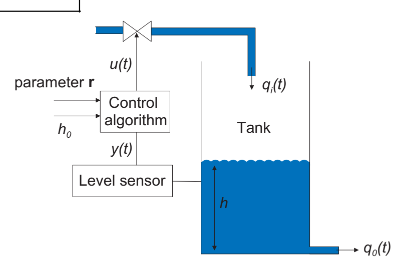


SaTool is an implementation of structural analysis theory. It will analyze a structure graph and provide knowledge about fundamental properties of the system in normal and faulty conditions.

Single tank system example 5.3

Tank	c_1 :	$\dot{h}(t)$	=	$q_i(t) - q_o(t)$
Input valve	c_2 :	$q_i(t)$	=	$\alpha u(t)$
Output pipe	c_3 :	$q_o(t)$	=	$k\sqrt{h(t)}$
Level sensor	c_4 :	$y(t)$	=	$h(t)$
Control algorithm	c_5 :	$u(t)$	=	$\begin{cases} 1 & \text{if } y(t) < h_0 \\ 0 & \text{otherwise} \end{cases}$

differential constraint: $c_6 : \dot{h}(t) = \dfrac{dh(t)}{dt}$



DANMARKS TEKNISKE UNIVERSITET

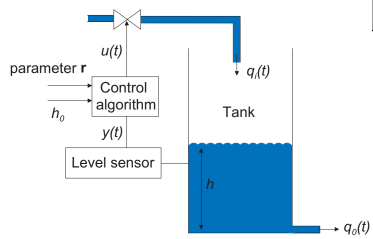
Ørsted•DTU

Single tank system example 5.3

$$c_1: \quad \dot{h}(t) = q_i(t) - q_o(t)$$
$$c_2: \quad q_i(t) = \alpha u(t)$$
$$c_3: \quad q_o(t) = k\sqrt{h(t)}$$
$$c_4: \quad y(t) = h(t)$$
$$c_5: \quad u(t) = \begin{cases} 1 & \text{if } y(t) < h_0 \\ 0 & \text{otherwise} \end{cases}$$
$$c_6: \quad \dot{h}(t) = \frac{dh(t)}{dt}$$

Three views

	u	y	h	$\dot{h}$	q_i	q_0
c_1	0	0	0	1	1	1
c_2	1	0	0	0	1	0
c_3	0	0	1	0	0	1
c_4	0	1	1	0	0	0
c_5						
c_6	0	0	1	1	0	0

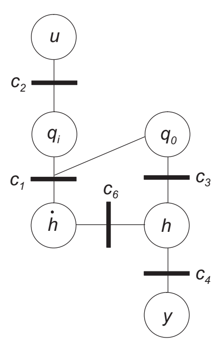


M. Blanke 2004 Diagnosis& Fault-tolerant Control 52.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Example 5.3: tank system

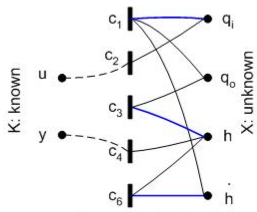


	u	y	h	$\dot{h}$	q_i	q_0
c_1	0	0	0	1	1	1
c_2	1	0	0	0	1	0
c_3	0	0	1	0	0	1
c_4	0	1	1	0	0	0
c_5						
c_6	0	0	1	1	0	0

Every column in the incidence matrix corresponds to a circle vertex.
Every row corresponds to a bar vertex in the bipartite graph.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 53.

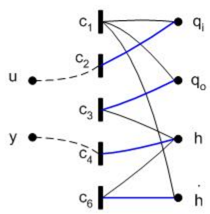
Complete matching



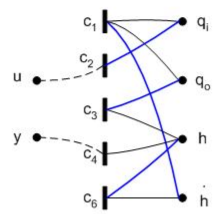
Incomplete in X and C

A matching M is a subset of edges such that no edge have common node (neither in C nor in X).

Let $|M|$ be number of edges in M, then $|M| \le \min(|C|, |X|)$



Complete in X - c_1 is unmatched



Complete in X - c_4 is unmatched

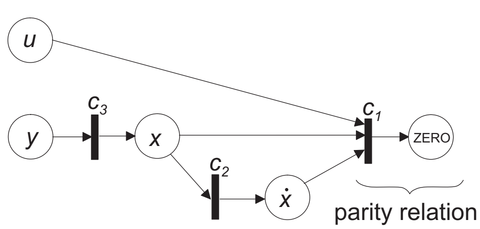
A matching is complete in X if $|M| = X$.

It is complete in C if $|M| = |C|$.

Figure: One incomplete and two complete matchings in X for the tank example.

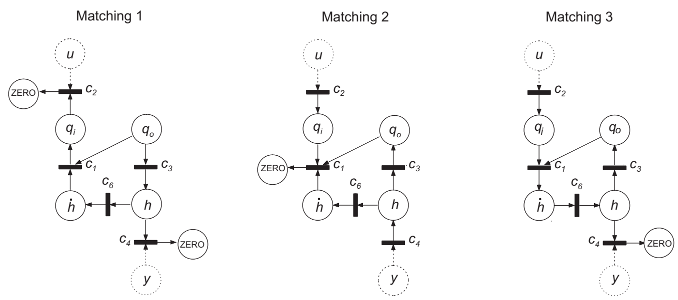
DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Unmatched constraint



DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Matching on the single tank



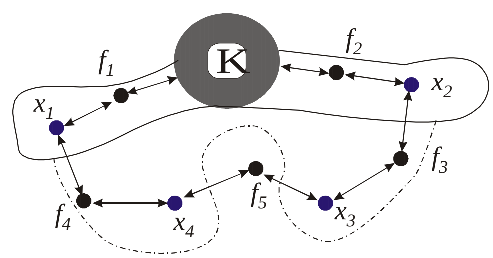
M. Blanke 2004 Diagnosis& Fault-tolerant Control 56.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

The ranking algorithm to find matchings

1. Mark all known variables
2. Find all constraints with one unmatched variable. Mark these and the corresponding variables.
3. If there exist unmarked constraints with all variables marked, flag these.
4. Continue

The principle of a matching algorithm: start with a known variable.
Successively calculate unknown variables using the constraints



M. Blanke 2004 Diagnosis& Fault-tolerant Control 57.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Ranking Algorithm

Given: incidence matrix or structure graph

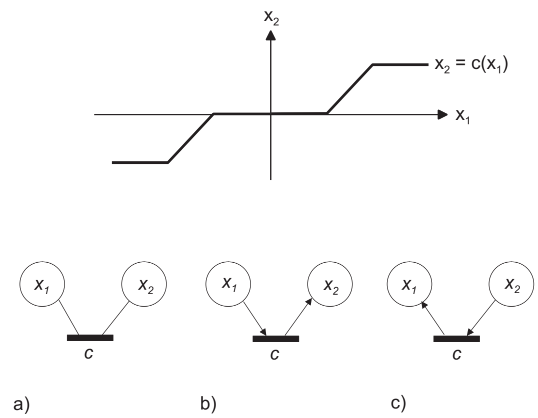
1. Mark all known variables, i = 0.
2. Find all constraints with exactly one unmarked variable. Associate rank i with these constraints. Mark these constraints and the associated variable.
3. If there are unmarked constraints whose variables are all marked, mark them and connect them with the pseudo-variable zero.
4. set i = i+1
5. if there are unmarked variables or constraints, continue with step 2.

Result: Ranking of the constraints.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 58.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Non invertible constraints



M. Blanke 2004 Diagnosis& Fault-tolerant Control 59.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

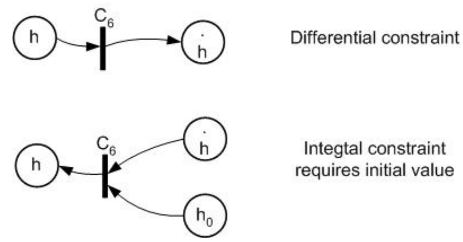
Differential and integral constraints

Differential constraint

$$c_6 : \dot{h} = \frac{dh}{dt}$$

Integral constraint

$$c_6 : h(t) = \int_0^t \dot{h}(\tau)d\tau + h(0)$$



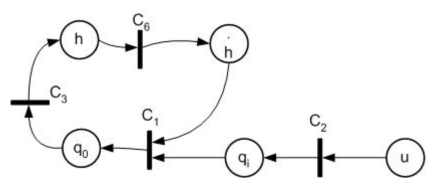
M. Blanke 2004 Diagnosis& Fault-tolerant Control 60.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Differential loop

Consider loops in the oriented graph associated with matching.

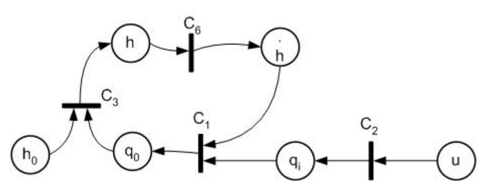


General form of differential loop

$$z_l = g(x_l, \theta_l, u_l)$$

$$z_l = \frac{dx_l}{dt}$$

Unique solution only if $x_l(0)$ is known



M. Blanke 2004 Diagnosis& Fault-tolerant Control 61.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Dealing with loops

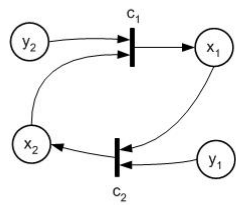
Example 5.15:

$c_1: \quad ay_1 + bx_1 + cx_2 = 0$

$c_2: \quad \alpha y_2 + \beta x_1 + \gamma x_2 = 0$

has the incidence matrix

	y_1	y_2	x_1	x_2
c_1	1	0	1	1
c_2	0	1	1	1



Note: Solvability condition: $b\gamma - c\beta \neq 0$
can't be seen from structure properties.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 62.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

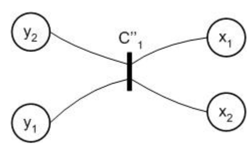
Loops: condense into single node

Algebraic loop

Example 5.15:

$c_1: \quad ay_1 + bx_1 + cx_2 = 0$

$c_2: \quad \alpha y_2 + \beta x_1 + \gamma x_2 = 0$



Condense the two equations to:

$c_1'': \quad ay_1 + \alpha y_2 + (b+\beta)x_1 + (c+\gamma)x_2 = 0$

	y_1	y_2	x_1	x_2
c_1''	1	1	1	1

M. Blanke 2004 Diagnosis& Fault-tolerant Control 63.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

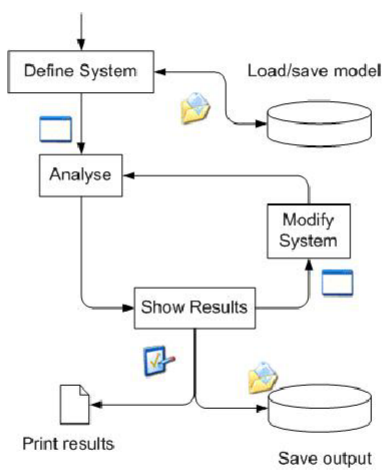
Dealing with loops

- Graphs are oriented while Matching is performed.
- Loops can often be reduced:
  - Algebraic loops by re-formulation of the problem
  - Differential loops if initial condition is known (or can be estimated)
  - Loops with non-invertible coefficients (use manifold of solutions if solutions exist)

M. Blanke 2004 Diagnosis& Fault-tolerant Control 64.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Development cycle using SaTool



SaTool supports:

•Define system structure

•Analyse structure graph

•Show results

•Modify system

•Load/save models

•Save/print results

M. Blanke 2004 Diagnosis& Fault-tolerant Control 65.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

SaTool – A tool for Structural Analysis

Features

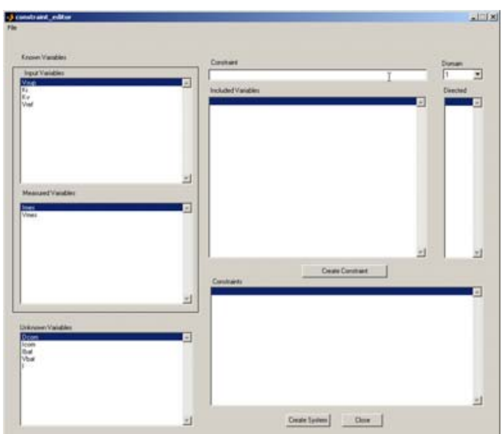
- Matlab ® based (version 6.5 or later)
- Graphical representation of structure as a graph
- Easy point and click manipulation of system structure
- Matching by ranking
- Backtracing
  - Recursive algorithm

Matlab ® is a trademark of the Math Works Inc. USA.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 66.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

SaTool - enter system



SaTool
(ref: Lorentzen and Blanke, 2004)

Analyse system structure

Automatic generation of parity relations for diagnosis

M. Blanke 2004 Diagnosis& Fault-tolerant Control 67.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Formulation for structural analysis

Constraints for ship steering example

$c_1 : \dot{\omega}_3(t) = b\left(\delta(t) + H(\omega_3(t))\right)$

$c_2 : \dot{\psi}(t) = \omega_3(t) + \omega_w(t)$

$c_3 : \psi_{m1}(t) = \psi(t)$

$c_4 : \psi_{m2}(t) = \psi(t)$

$c_5 : \omega_{3m}(t) = \omega_3(t) + \omega_w(t)$

$c_6 : \dfrac{d\omega_3}{dt} = \dot{\omega}_3(t)$

$c_7 : \dfrac{d\psi}{dt} = \dot{\psi}(t)$

Known variables

δ ruddder angle

ψ_{m1} heading gyro 1

ψ_{m2} heading gyro 2

ω_{3m} turn rate gyro

H a non-linear function of ω_3

Unknown variables

ω_3 physical turn rate

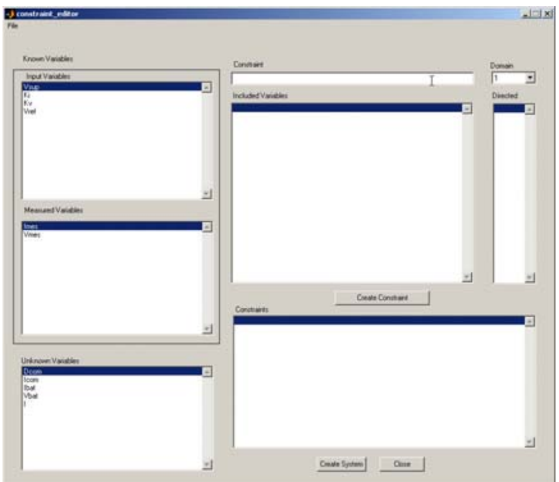
ψ physical heading

ω_w distrurbance from waves

M. Blanke 2004 Diagnosis& Fault-tolerant Control 68.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

The Constraint Editor

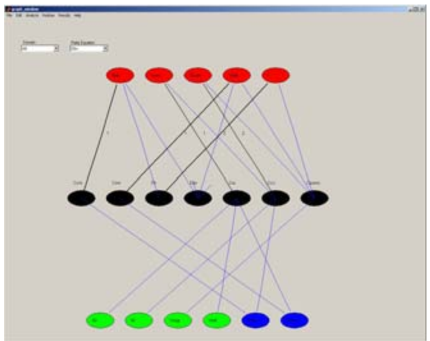


M. Blanke 2004 Diagnosis& Fault-tolerant Control 69.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

SaTool - analyse system



Graphical and text based output.

Shows fundamental properties:

- Which faults can not be detected

- Which faults can not be isolated

- Which parity relations need be used to diagnose a particular fault

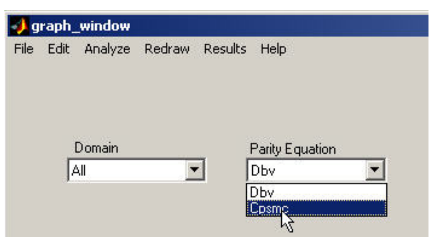
- What can be done if a particular constraint is violated (fault occurred)

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

View the results (1)

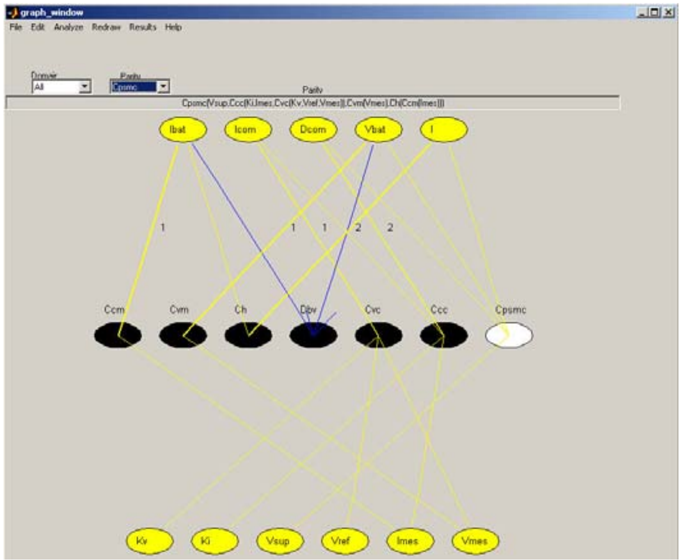
- Select a parity equation from the dropdown menu



- Result
  – Parity Relation
  – Included variables yellow

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU



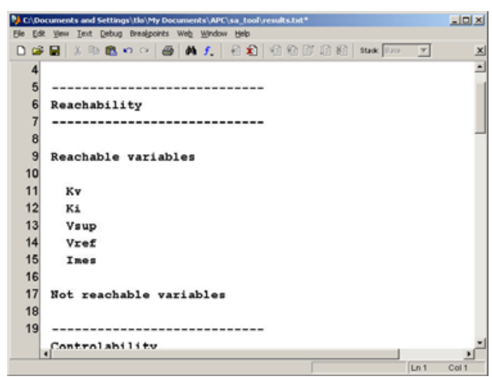
M. Blanke 2004 Diagnosis& Fault-tolerant Control 73.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Viewing the results

- Press **Results:**
  - The matlab editor opens and shows the results in a text file



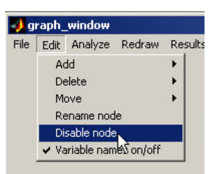
M. Blanke 2004 Diagnosis& Fault-tolerant Control 74.

Results

- Reachability
  - Can I reach the unknown variables from the known variables
  - Requirement for observability
- Controllability
  - Can I reach the unknown variables from the input variables
- Parity relations
  - Which relations exists
- Detectability
  - Which faults can be detected with the found parity relations
- Isolability
  - Which faults can be isolated with the found parity relations

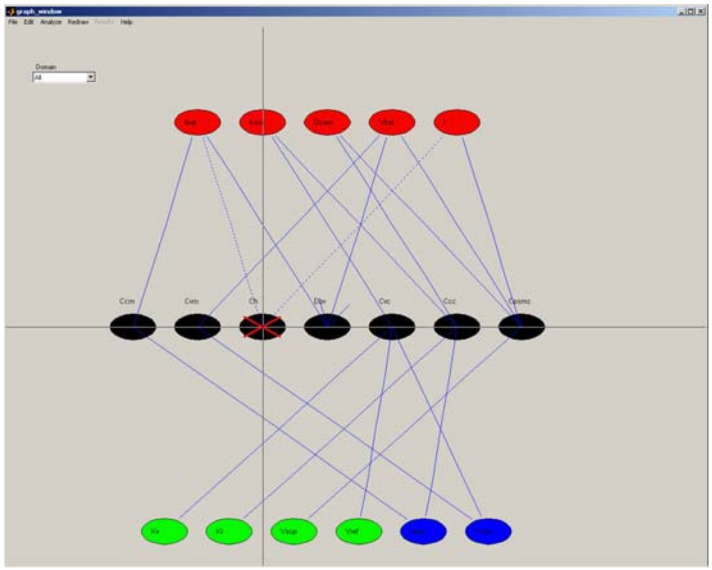
Investigate the effect of a structural fault

- Faults can be modeled by disabling nodes
  - Select **Disable Node** from the edit menu



  - Click on a node to disable it
  - Perform a new analysis
- The result shows if the system can be reconfigured in case of faults

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU



DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Results for Diagnosis

SaTool provides automatically generated (nonlinear) parity relations.
Use these as residual generators

$r(t) = \tilde{g}(c_i(X,K))$

$r \simeq 0$ when constraints in $\tilde{g}$ are valid

$r \neq 0$ when constraints in $\tilde{g}$ are violated

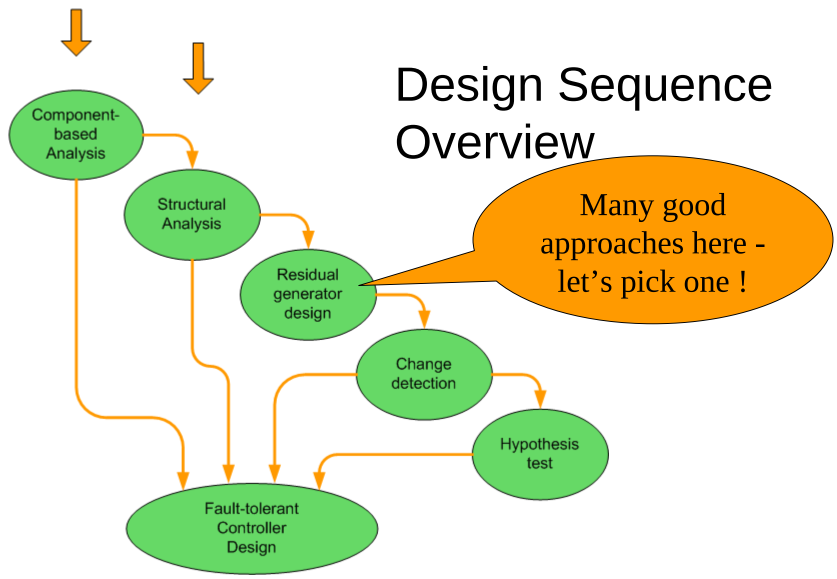
In order to investigate dynamic properties, we wish to analyse the case of linear parity relations.

Problem: given a linear system

Determine: a residual generator

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Design Sequence Overview



M. Blanke 2004 Diagnosis& Fault-tolerant Control 79.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Design of residual generataors

Chapter 6.1-6.3

Design of residual generator - notation and general model

$$\dot{\mathbf{x}}(t) = \mathbf{g}\left(\overline{\mathbf{x}}(t), \overline{\mathbf{u}}(t), \overline{\mathbf{d}}(t), \overline{\mathbf{f}}(t)\right), \qquad \overline{\mathbf{x}}(0) = \mathbf{x}_0$$
$$\overline{\mathbf{y}}(t) = \mathbf{h}\left(\overline{\mathbf{x}}(t), \overline{\mathbf{u}}(t), \overline{\mathbf{d}}(t), \overline{\mathbf{f}}(t)\right)$$

- **x** be a state vector - velocity position, turn rates and angles
- **u** be a control signal, e.g. rudder angle, propeller thrust
- **y** be a vector of measured quantities
- **f** faults represented as a vector and
- **d** be disturbances

Detailed design of fault diagnosis

Linear case:
Let variables without a bar denote deviation from the point of linearization, $\mathbf{x}(t) = \overline{\mathbf{x}}(t) - \overline{\mathbf{x}}_0(t)$

$$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) + \mathbf{E}_x\mathbf{d}(t) + \mathbf{F}_x\mathbf{f}(t), \qquad \mathbf{x}(0) = \mathbf{0}$$
$$\mathbf{y}(t) = \mathbf{C}\mathbf{x}(t) + \mathbf{D}\mathbf{u}(t) + \mathbf{E}_y\mathbf{d}(t) + \mathbf{F}_y\mathbf{f}(t)$$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Fault detection - detectability

Problem (6.1)
Given a model of the process, determine a stable residual generator such that:
- With no fault (f(t)=0) r(t) $\rightarrow$ 0
- r(t) is affected by f(t)

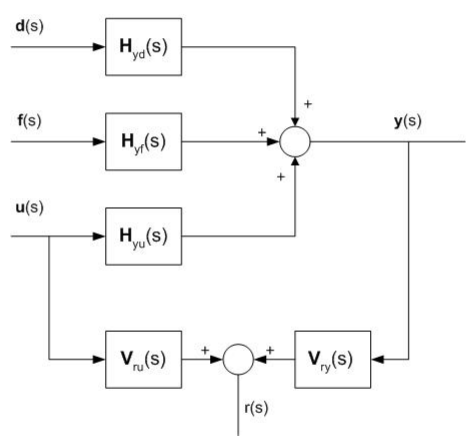
Or:

$\forall t, u(t), d(t), x(0), z(0)$: $f(t)=0 \Rightarrow r(t) \rightarrow 0$

$\exists t,\ r(t) \neq 0 \Leftrightarrow \exists t,\ f(t) \neq 0$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Residual generator



Residual generator design

Residual generator

$$\mathbf{r}(s) = \mathbf{V}_{ru}(s)\mathbf{u}(s) + \mathbf{V}_{ry}(s)\mathbf{y}(s) \Rightarrow$$

$$\mathbf{r}(s) = \left(\mathbf{V}_{ru}(s) + \mathbf{V}_{ry}(s)\mathbf{H}_{yu}(s)\right)\mathbf{u}(s) + \mathbf{V}_{ry}(s)\mathbf{H}_{yd}(s)\mathbf{d}(s)$$
$$+\mathbf{V}_{ry}(s)\mathbf{H}_{yx}(s)\mathbf{x}(o) + \mathbf{V}_{ry}(s)\mathbf{H}_{yf}(s)\mathbf{f}(s)$$

Design goal: make $\mathbf{r}(s)$ independent of $\mathbf{u}(s)$ and $\mathbf{d}(s)$

We desire $\mathbf{V}_{ry}(s)\mathbf{H}_{yf}(s) \neq \mathbf{0}$ but it is not guaranteed that this can be achieved with this design goal.

Residual generator - parity space approach

The problem is to make $\mathbf{r}(s)$ independent of $\mathbf{u}(s)$ and $\mathbf{d}(s)$:

$$\left(\mathbf{V}_{ru}(s) + \mathbf{V}_{ry}(s)\mathbf{H}_{yu}(s)\right)\mathbf{u}(s) + \mathbf{V}_{ry}(s)\mathbf{H}_{yd}(s)\mathbf{d}(s) = \mathbf{0}$$

$$\Leftrightarrow$$

$$\begin{pmatrix}\mathbf{V}_{ry}(s) & \mathbf{V}_{ru}(s)\end{pmatrix}\begin{pmatrix}\mathbf{H}_{yu}(s) & \mathbf{H}_{yd} \\ \mathbf{I} & \mathbf{0}\end{pmatrix} = \mathbf{0}$$

This problem has the form:

given **A**(s), find all **x**(s) that satisfy **x**(s)**A**(s)=**0**

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Nullspace design of residual generator

Let $\begin{pmatrix} \mathbf{H}_{yu}(s) & \mathbf{H}_{yd}(s) \\ \mathbf{I} & \mathbf{0} \end{pmatrix} = \mathbf{H}(s) \equiv \frac{1}{h(s)} \tilde{\mathbf{H}}(s)$

Algorithm:

1. Find the nullspace N_l of $\tilde{\mathbf{H}}(s)$
2. Determine $\left(\tilde{\mathbf{V}}_{ry}(s) \quad \tilde{\mathbf{V}}_{ru}(s) \right) \subset N_l \left(\tilde{\mathbf{H}}(s) \right)$
3. Let $\mathrm{F}(s) \equiv \left(\tilde{\mathbf{V}}_{ry}(s) \quad \tilde{\mathbf{V}}_{ru}(s) \right)$
4. Let a residual generator be $\mathbf{r}(s) = \frac{1}{\mathrm{p}(s)} \mathbf{Q}(s) \mathbf{F}(s) \begin{pmatrix} \mathbf{y}(s) \\ \mathbf{u}(s) \end{pmatrix}$

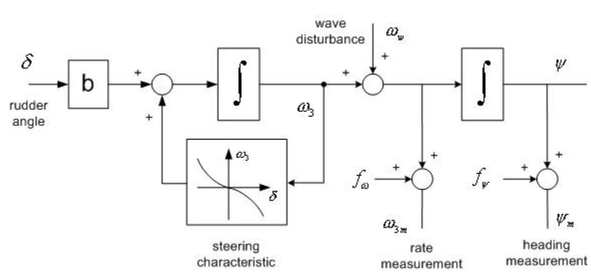
where p(s) is a stable, scalar polynomial to make $\frac{1}{\mathrm{p}(s)} \mathbf{Q}(s) \mathbf{F}(s)$ causal

Q(s) is "arbitrary", nonzero.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 89.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Ship example: gyro fault diagnosis



M. Blanke 2004 Diagnosis& Fault-tolerant Control 90.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Ship example continued

$$\begin{aligned}\dot{\omega}_3 &= b(\delta + H(\omega_3,\delta)) \\ \dot{\psi} &= \omega_3 + \omega_{3w} \\ \psi_m &= \psi + f_\psi \\ \omega_{3m} &= \omega_3 + \omega_{3w} + f_{\omega_3} \\ \delta_m &= \delta\end{aligned}$$

and $\frac{\partial H}{\partial r} = H_1 < 0 \Big|_{r=0} \Rightarrow$ stable

M. Blanke 2004 Diagnosis& Fault-tolerant Control 91.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Example: Heading and rate measurements

$$\mathbf{H}(s) = \frac{1}{s(s-bh_1)}\begin{pmatrix} bs & s(s-bh_1) \\ b & (s-bh_1) \\ b & (s-bh_1) \\ s(s-bh_1) & 0 \end{pmatrix}, \quad bh_1 < 0$$

has the left nullspace basis

$$\mathbf{F}(s) = \frac{1}{s}\begin{pmatrix} -1 & s & 0 & 0 \\ -1 & 0 & s & 0 \end{pmatrix}$$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 92.

Ship example continued

Measurements are rate gyro + gyro angle

$$\begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} \omega_{3m} - \hat{\omega}_3 \\ \psi_m - \hat{\psi} \end{bmatrix} = \begin{bmatrix} 1 \\ s^{-1} \end{bmatrix} \omega_{3w} + \begin{bmatrix} f_\omega \\ f_\psi \end{bmatrix}$$

Insensitivity to wave input:

$r_1(s)=W(s)\begin{bmatrix} 1 \\ s^{-1} \end{bmatrix} = 0 \Rightarrow W(s)=\begin{bmatrix} -s^{-1} & 1 \end{bmatrix}$ and

$r_1(s)=f_\psi - s^{-1} f_\omega$

Residual generator

Residual generator

$$\mathbf{r}(s) = \frac{h(s)}{p(s)} \mathbf{Q}(s)\mathbf{F}(s) \begin{pmatrix} \mathbf{y}(s) \\ \mathbf{u}(s) \end{pmatrix} \equiv \begin{pmatrix} \mathbf{V}_{ry}(s) & \mathbf{V}_{ru}(s) \end{pmatrix} \begin{pmatrix} \mathbf{y}(s) \\ \mathbf{u}(s) \end{pmatrix}$$

Residual generator for the specific case

$$\begin{pmatrix} r_1(s) \\ r_2(s) \end{pmatrix} = \begin{pmatrix} \frac{1}{s} & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} \omega_{3m}(s) \\ \psi_{m1}(s) \\ \psi_{m2}(s) \\ \delta(s) \end{pmatrix}$$

A "natural" choice that is independent of ship's dynamics

Response to faults

Residual response to faults and initial condition

$$\mathbf{r}(s) = \frac{1}{p(s)}\mathbf{Q}(s)\mathbf{F}(s)\begin{pmatrix} \mathbf{H}_{yf}(s) & \mathbf{H}_{yx}(s) \\ \mathbf{0} & \mathbf{0} \end{pmatrix}\begin{pmatrix} \mathbf{f}(s) \\ \mathbf{x}_0 \end{pmatrix}$$

In the spscific case

$$\begin{pmatrix} r_1(s) \\ r_2(s) \end{pmatrix} = \begin{pmatrix} \frac{1}{s} & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}\begin{pmatrix} f_\omega(s) \\ f_{\psi 1}(s) \\ f_{\psi 2}(s) \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \omega_3(0) \\ \psi(0) \end{pmatrix}.$$

Fault estimation given isolation

$$\mathbf{H}_{rf}(s) = \begin{pmatrix} \frac{1}{s} & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

$$f_\omega \text{ isolated } \Rightarrow \hat{f}_\omega(s) = s r_1(s)$$

$$f_{\psi 1} \text{ isolated } \Rightarrow \hat{f}_{\psi 1}(s) = 0.5\left(r_2(s) - r_1(s)\right)$$

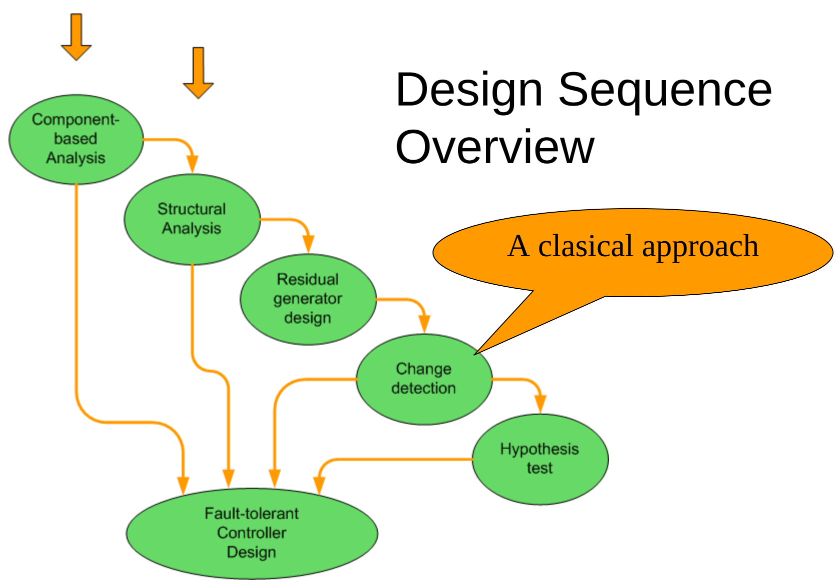
$$f_{\psi 2} \text{ isolated } \Rightarrow \hat{f}_{\psi 2}(s) = r_2(s)$$

Change Detection

Diagnosis and fault-tolerant control
Section 6.4

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

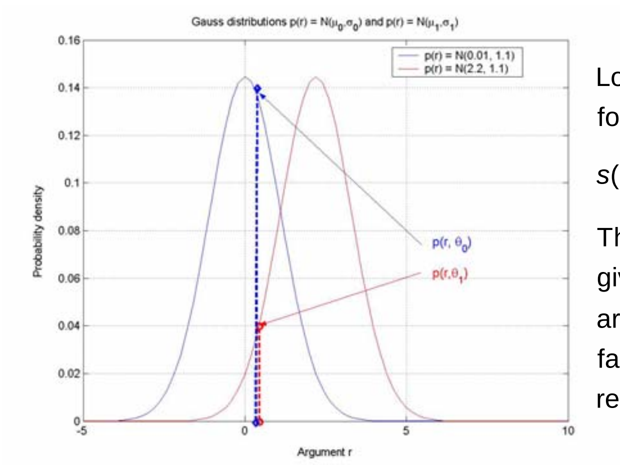
Design Sequence Overview



DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Log-likelihood ratio



Log likelihood ratio for an observation r(i):

$$s(r(i)) = \ln \frac{p(r(i)\,|\,\theta_1)}{p(r(i)\,|\,\theta_0)}$$

The two distributions are given because θ_1 and θ_0 are our hypotheses for fault and no fault, respectively.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 99.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Cusum detection

The cumulative sum (CUSUM) is a summation of the log-likelihood ratio

$$S(j) = \sum_{k=1}^{j} s(k)$$

The CUSUM will integrate up when s>0 and down for s<0.

When S pass a threshold, a decision can be taken about the hypotheses: normal condition - faulty condition.

The decision to decide between θ_0 and θ_1 is

accept θ_0 when $S \le a$

accept θ_1 when $S \ge h$

continue to observe and test when $a < S < h$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 100.

Recursive cusum – gaussian residual

Assume a Gaussian distribution if the residual $r = N(\mu_0, \sigma_0^2)$, i.e. with mean μ_0 and variance σ_0^2, when there is no fault, hypothesis θ_0

$$p(r_i \mid \theta_0) = \frac{1}{\sigma_0 \sqrt{2\pi}} \exp\left(-\frac{(r_i - \mu_0)^2}{2\sigma_0^2} \right)$$

The fulaty condition, hypothesis θ_1, has $r_i = N(\mu_1, \sigma_1^2)$

The log likelihood ratio is then

$$s_i = \ln\left(\frac{p(r_i \mid \theta_1)}{p(r_i \mid \theta_0)} \right) = \ln \frac{\sigma_0}{\sigma_1} + \frac{(r_i - \mu_0)^2}{2\sigma_0^2} - \frac{(r_i - \mu_1)^2}{2\sigma_1^2}$$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Recursive cusum – specific change

Problem 1. Given r=N(μ,σ^2), let a fault imply a change in mean from μ_0 to μ_1, with unchanged variance σ before and after the fault, the log-likelihood ratio is then

$$s_i = \frac{(\mu_1 - \mu_0)^2}{\sigma^2} \left(r - \frac{\mu_0 + \mu_1}{2} \right)$$

Problem 2: Given r=N(μ,σ^2), let a fault imply a change in variance from σ_0^2 to σ_1^2, with unchanged mean μ before and after the fault, the log-likelihood ratio is then

$$s_i = \ln \frac{\sigma_0}{\sigma_1} + \frac{\sigma_1^2 - \sigma_0^2}{\sigma_1^2 \sigma_0^2} (r_i - \mu)^2$$

Different uses of the CUSUM tests

CUSUM testing can be made in a number of ways. We treat sequential and recursive approaches (2 and 3 are equivalent).

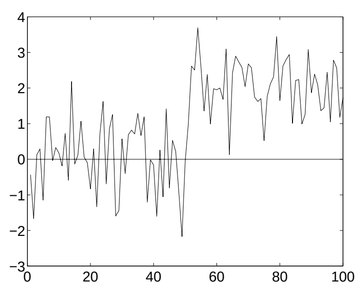
Observe that condition ”fault” means g(k) will increase, ”no-fault” will make g(k) decrease.

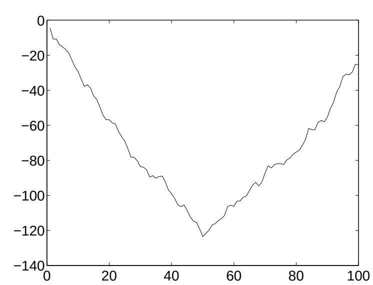
1. Compute g(k) until an upper or lower limit is reached. No hypothesis can be made until either limit is reached. This is a sequential test.
2. Compute g(k) and store g_{min}= min(g(k)). If g(k)- g_{min} > h hypothesis θ_1 is assumed. Otherwise θ_0 .
3. Let *g(k)=max(g(k),0)* and stop test when a threshold *h* is reached. Assume ”no-fault” until h is reached. Recursive test.

Sequential test and the cusum function

Sequential cusum test for change in mean:

$$g(k) = g(k-1) + \frac{\mu_1 - \mu_0}{\sigma^2}\left(r(k) - \frac{\mu_1 + \mu_0}{2}\right)$$





DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Sequential test

Test between two hypotheses:
θ_0: mean value is μ_0, θ_1: mean value is μ_1

Algorithm for sequential test:

$$g(k) = g(k-1) + \frac{\mu_1 - \mu_0}{\sigma^2}\left(r(k) - \frac{\mu_1 + \mu_0}{2}\right)$$

if $(g(k) < a)$, θ_0 is true; $g(k) = 0$; end;

if $(g(k) > h)$, θ_1 is true; $g(k) = 0$; end;

M. Blanke 2004 Diagnosis& Fault-tolerant Control 105.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Choice of limits for hypothesis test

With two limits for the hypothesis test a and h,

these can be chosen to give specified probabilities for false alarm and missed detection

P_f : false detection propability

P_m: missed detection propability

Decker´s result: Choose $h = \ln(\frac{1-P_M}{P_F})$, $a = \ln(\frac{P_M}{1-P_F})$

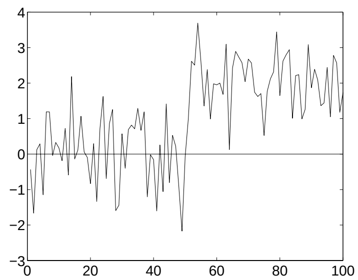
M. Blanke 2004 Diagnosis& Fault-tolerant Control 106.

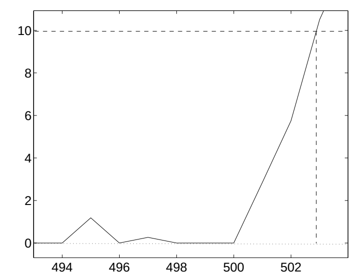
DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Recursive form of CUSUM

Cumulative sum for recursive change detection:

$$g(k) = \max\left(0, g(k-1) + \frac{\mu_1 - \mu_0}{\sigma^2}\left(r(k) - \frac{\mu_1 + \mu_0}{2}\right)\right)$$

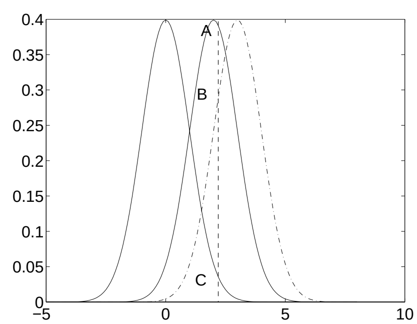


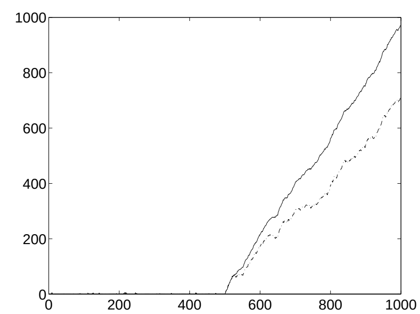


M. Blanke 2004 Diagnosis& Fault-tolerant Control 107.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Cusum test – change of test value





The test quantity is $\frac{1}{2}(\mu_0 + \mu_1)$. The "gain" is $\frac{\mu_1 - \mu_0}{\sigma^2}$

Fig. 6.11 shows sensitivity to change in test quantity.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 108.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Time to detect and time between false alarms - Average Run Length (ARL)

Let a signal z(k) have mean μ_s and variance σ^2.

The time it takes to reach h is $\hat{L}(\mu_s,\sigma,h)=$

$$\begin{cases} \frac{\sigma^2}{2\mu_s^2}\left(\exp\left(-\left(2.0\frac{\mu_s h}{\sigma^2}+2.2232\frac{\mu_s}{\sigma}\right)\right)+\left(2.0\frac{\mu_s h}{\sigma^2}+2.2232\frac{\mu_s}{\sigma}\right)-1\right), & \mu_s \neq 0 \\ \left(\frac{h}{\sigma}+1.1166\right)^2, & \mu_s = 0 \end{cases}$$

With $\mu_s = \mu_1$, the ARL is the average time to detect:

With $\mu_s = \mu_0$, the ARL is the average time between false alarms.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 109.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Mean and variance for cusum test

The CUSUM test for a mean value change was

$$s(r_i)=\frac{\mu_1-\mu_0}{\sigma^2}\left(r_i-\frac{\mu_1+\mu_0}{2}\right);$$

If $E\{r_i\}=\mu_0$,
$$\begin{cases} \mu_s \equiv E_{\mu_0}\{s(r_i)\} = -\frac{(\mu_1-\mu_0)^2}{2\sigma^2} \\ \sigma_s^2 \equiv E\left\{(s(r_i)-\mu_s)^2\right\} = \frac{(\mu_1-\mu_0)^2}{\sigma^2} \end{cases}$$

If $E\{r_i\}=\mu_1$,
$$\begin{cases} \mu_s \equiv E_{\mu_1}\{s(z)\} = \frac{(\mu_1-\mu_0)^2}{2\sigma^2} \\ \sigma_s^2 \equiv E\left\{(s(z)-\mu_s)^2\right\} = \frac{(\mu_1-\mu_0)^2}{\sigma^2} \end{cases}$$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 110.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

ARL for the CUSUM

For the case of fault

$\hat{\tau}_{detect} = \hat{L}(\mu_s, \sigma_s, h) = \hat{L}(\frac{(\mu_1 - \mu_0)^2}{2\sigma^2}, \frac{(\mu_1 - \mu_0)^2}{\sigma^2}, h)$ is mean time to detect.

For the case of no-fault

$\hat{\tau}_{false\ alarm} = \hat{L}(\mu_s, \sigma_s, h) = \hat{L}(-\frac{(\mu_1 - \mu_0)^2}{2\sigma^2}, \frac{(\mu_1 - \mu_0)^2}{\sigma^2}, h)$ is mean time between false alarms.

This result is a key design parameter.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 111.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

ARL for CUSUM

Design procedure:
Given $\mu_1 - \mu_0$ and σ^2,
- determine h to give small low τ_{detect} (3-20 samples)
- check that false alarm time is 10^6 - 10^8 samples or more.

If design objective is not met,
- decrease σ^2 (filter) and/or
- increase μ_1

The last step means to make the detector less sensitive, larger size of fault is deeded for detection.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 112.

Change detection - unknown magnitude of fault

The Generalized Likelihood Ratio test

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Change of unknown magnitude

Given: the magnitude of a change in mean is unknown.

Assume a hypothetical change instant j, then we would have

$$S_j^k(\theta_1) = \sum_{i=j}^{k} \ln \frac{p_{\theta 1}(z(i))}{p_{\theta 0}(z(i))}$$

Estimate both the instant of change, $\hat{\mathrm{k}}_0$, and the magnitude, $\hat{\theta}_1$.

$$(\hat{\mathrm{k}}_0, \hat{\theta}_1) = \arg\left\{ \max_{1\le j\le k} \max_{\theta 1} S_j^k(\theta_1) \right\}$$

Decision GLR (generalised likelihood test) function is

$$g(k) = \max_{1\le j\le k} \max_{\theta 1} S_j^k(\theta_1)$$

GLR test for unknown magnitude

For Gaussian signals, $S_j^k(\mu_1) = \sum_{i=j}^{k} \ln \frac{p_{\theta 1}(z(i))}{p_{\theta 0}(z(i))} = \frac{\mu_1 - \mu_0}{\sigma^2} \sum_{i=j}^{k} \left(z(i) - \frac{\mu_1 + \mu_0}{2} \right)$

Maximum with respect to $\mu_1 \Rightarrow \frac{\partial S_j^k(\mu_1)}{\partial \mu_1} = 0$

$$\frac{\partial S_j^k(\mu_1)}{\partial \mu_1} = \frac{1}{\sigma^2} \sum_{i=j}^{k} \left(z(i) - \frac{\mu_1 + \mu_0}{2} \right) - \frac{\mu_1 - \mu_0}{\sigma^2} \frac{k-j+1}{2} = 0$$

$$\Rightarrow \sum_{i=j}^{k} z(i) - \sum_{i=j}^{k} \frac{\hat{\mu}_1 + \mu_0}{2} - (\hat{\mu}_1 - \mu_0) \frac{k-j+1}{2} = 0$$

$$\Rightarrow \sum_{i=j}^{k} z(i) - (\hat{\mu}_1 + \mu_0) \frac{k-j+1}{2} - (\hat{\mu}_1 - \mu_0) \frac{k-j+1}{2} = 0$$

$$\Rightarrow \hat{\mu}_1 = \frac{1}{k-j+1} \sum_{i=j}^{k} z(i)$$

GLR test for unknown mean after change

$S_j^k(\mu_1) = \frac{\hat{\mu}_1 - \mu_0}{\sigma^2} \sum_{i=j}^{k} \left(z(i) - \frac{\hat{\mu}_1 + \mu_0}{2} \right)$ and $\hat{\mu}_1 = \frac{1}{k-j+1} \sum_{i=j}^{k} z(i) \Rightarrow$

$$S_j^k(\mu_1) = \frac{1}{\sigma^2} \left(\frac{1}{k-j+1} \sum_{i=j}^{k} z(i) - \mu_0 \right) \sum_{i=j}^{k} \left(z(i) - \frac{1}{2} \left(\frac{1}{k-j+1} \sum_{i=j}^{k} z(i) + \mu_0 \right) \right)$$

note that $\sum_{i=j}^{k} \frac{1}{k-j+1} \sum_{i=j}^{k} z(i) = \sum_{i=j}^{k} z(i)$, and $\frac{1}{k-j+1} \sum_{i=j}^{k} \mu_0 = \mu_0$, hence

$$S_j^k(\mu_1) = \frac{1}{\sigma^2} \frac{1}{k-j+1} \left(\sum_{i=j}^{k} (z(i) - \mu_0) \right) \frac{1}{2} \left(\sum_{i=j}^{k} (z(i) - \mu_0) \right)$$

$g(k) = \frac{1}{2\sigma^2} \max_{1 \le j \le k} \frac{1}{k-j+1} \left(\sum_{i=j}^{k} (z(i) - \mu_0) \right)^2$ is the GLR decision function

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

GLR test for unknown mean after change

Sequential GLR test using a record of length M:

Choose M equal to or larger than the maximum detection deley

$$g(k) = \frac{1}{2\sigma^2} \max_{k-M+1 \le j \le k} \frac{1}{k-j+1} \left(\sum_{i=j}^{k} \left(z(i) - \mu_0 \right) \right)^2$$

Accept H_0 if $g(k) \le h$

Accept H_1 if $g(k) > h$

Estimated change occurrence $j_0 = \arg\left\{ \frac{1}{2\sigma^2} \max_{k-M+1 \le j \le k} \frac{1}{k-j+1} \left(\sum_{i=j}^{k} \left(z(i) - \mu_0 \right) \right)^2 \right\}$

Estimated magnitude of change $\hat{\mu}_1 = \frac{1}{k-j_0+1} \sum_{i=j_0}^{k} z(i)$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Sequential GLR test with record length M

"Fake" example with M = 4, $\sigma^2 = 0.5$.

Start at $k = 8$, $j \subset [k-M, k]$

z	0	0	0	0	2	2	2	2	2	2
k	5	6	7	8	9	10	11	12	13	14
$\sum_{i=j}^{k} z$	0	0	0	0	2	4	6	8	8	8
$g(8)_{j=5..8}$	0	0	0	0						
$g(9)_{j=6..9}$		1	1.33	2	4					
$g(10)_{j=7..10}$			4	5.33	8	4				
$g(11)_{j=8..11}$				9	12	8	4			
$g(12)_{j=9..12}$					16	12	8	4		

$\frac{1}{4}(0+0$

$\frac{1}{2}(2+2)^2$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Change detection

Vector residual

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Change detection for vector residual

- Thus far, change detection was considered for **scalar** signals.
- When a residual **vector** is available, the effect of a particular fault may appear in seveal components of the residual.
- It is advantagageous for diagnosis to consider the entire signature a fault will make in the components of the residual vector.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Vector valued residual

Given: A residual vector $\mathbf{r}(k) = \begin{bmatrix} r_1 \\ r_2 \\ . \\ r_n \end{bmatrix}$

When a fault occurs it has a

signature in the residual, e.g. $\mathbf{r}(k) = \begin{bmatrix} 1 & 1 & & 0 \\ -1 & 1 & .. & 1 \\ 1 & -1 & & -1 \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ .. \\ f_N \end{bmatrix}$

Problem: How can we distinguish f_1 from f_2

M. Blanke 2004 Diagnosis& Fault-tolerant Control 122.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Gaussian random vector process

If the random process is vector valued $\mathbf{x}(t)$ of dimension n,

$$p(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^n \det(\mathbf{Q})}} \exp\left(-\frac{(\mathbf{x}-\boldsymbol{\mu})^T \mathbf{Q}^{-1} (\mathbf{x}-\boldsymbol{\mu})}{2}\right)$$

where $\mathbf{Q}$ is the covariance $\mathbf{Q}=\mathrm{E}\left\{(\mathbf{x}-\boldsymbol{\mu})^T(\mathbf{x}-\boldsymbol{\mu})\right\}$ and

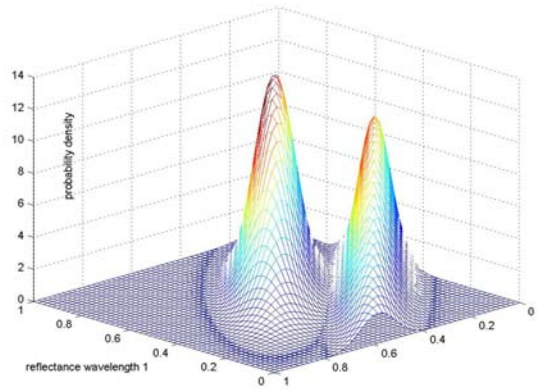
$\boldsymbol{\mu}$ is the mean value $\boldsymbol{\mu} = \mathrm{E}\left\{\mathbf{x}\right\}$.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 123.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Two dimensional case



M. Blanke 2004 Diagnosis& Fault-tolerant Control 124.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Change detection with vector residual

Known (assumed) magnitude (vector) is caused by the fault:

Hypothesis θ_o : Distribution is $N(\boldsymbol{\mu}_0,\mathbf{Q})$

Hypothesis θ_1 : Distribution is $N(\boldsymbol{\mu}_0,\mathbf{Q})$ up to time $i<k_0$ but distribution is $N(\boldsymbol{\mu}_1,\mathbf{Q})$ for time $i \geq k_0$.

Problem: diagnose whether has changed by a known mean vector.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 125.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Known μ_1 vector – cusum vector case

$$s(\mathbf{z}_k) = \ln \frac{p_{\boldsymbol{\mu}1}}{p_{\boldsymbol{\mu}0}} \Rightarrow$$

$$s(\mathbf{z}_k) = -\frac{1}{2}(\mathbf{z}_k - \boldsymbol{\mu}_1)^T \mathbf{Q}^{-1}(\mathbf{z}_k - \boldsymbol{\mu}_1) + \frac{1}{2}(\mathbf{z}_k - \boldsymbol{\mu}_0)^T \mathbf{Q}^{-1}(\mathbf{z}_k - \boldsymbol{\mu}_0) \quad \text{is scalar}$$

$$= \frac{1}{2}\left(\boldsymbol{\mu}_1^T\mathbf{Q}^{-1}\mathbf{z}_k + \mathbf{z}_k^T\mathbf{Q}^{-1}\boldsymbol{\mu}_1\right) - \frac{1}{2}\left(\boldsymbol{\mu}_0^T\mathbf{Q}^{-1}\mathbf{z}_k + \mathbf{z}_k^T\mathbf{Q}^{-1}\boldsymbol{\mu}_0\right) - \frac{1}{2}\boldsymbol{\mu}_1^T\mathbf{Q}^{-1}\boldsymbol{\mu}_1 + \frac{1}{2}\boldsymbol{\mu}_0^T\mathbf{Q}^{-1}\boldsymbol{\mu}_0$$

$$= \frac{1}{2}\left(\boldsymbol{\mu}_1^T\mathbf{Q}^{-1}\mathbf{z}_k + \left(\mathbf{z}_k^T\mathbf{Q}^{-1}\boldsymbol{\mu}_1\right)^T\right) - \frac{1}{2}\left(\boldsymbol{\mu}_0^T\mathbf{Q}^{-1}\mathbf{z}_k + \left(\mathbf{z}_k^T\mathbf{Q}^{-1}\boldsymbol{\mu}_0\right)^T\right) - \frac{1}{2}\left(\boldsymbol{\mu}_1^T\mathbf{Q}^{-1}\boldsymbol{\mu}_1 - \boldsymbol{\mu}_0^T\mathbf{Q}^{-1}\boldsymbol{\mu}_0\right)$$

$$= \left(\boldsymbol{\mu}_1^T - \boldsymbol{\mu}_0^T\right)\mathbf{Q}^{-1}\mathbf{z}_k - \frac{1}{2}\left(\boldsymbol{\mu}_1^T - \boldsymbol{\mu}_0^T\right)\mathbf{Q}^{-1}\left(\boldsymbol{\mu}_1 + \boldsymbol{\mu}_0\right) \Rightarrow$$

$$s(\mathbf{z}_k) = -\left(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_0\right)^T \mathbf{Q}^{-1}\left(\mathbf{z}_k - \tfrac{1}{2}\left(\boldsymbol{\mu}_0 + \boldsymbol{\mu}_1\right)\right) \quad \text{is scalar}$$

Scalar decision function: $g(k) = \max\left(0,\ g(k\text{-}1) + s(\mathbf{z}_k)\right)$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 126.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Known dynamic profile and magnitude

Hypothesis H_o : Distribution is $N(\boldsymbol{\mu}_0, \mathbf{Q})$

Hypothesis H_1 : Distribution is $N(\boldsymbol{\mu}_0, \mathbf{Q})$ up to time i<k_0 but distribution is $N(\boldsymbol{\mu}_0 + \boldsymbol{\rho}(i - k_0), \mathbf{Q})$ for time $i \geq k_0$
where $\boldsymbol{\rho}(i - k_0)$ is a knovn vector profile.

Problem: diagnose a known profile
of known magnitude (fault signature in the residual vector).

M. Blanke 2004 Diagnosis& Fault-tolerant Control 127.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Known dynamic profile and magnitude

A decision function is again derived from the sum of the log-likelihood ratio

$$S_j^k = \sum_{i=1}^{k} \ln \frac{p(\mathbf{z}_i \mid \boldsymbol{\mu}_0 + \boldsymbol{\rho}(i-j))}{p(\mathbf{z}_i \mid \boldsymbol{\mu}_0)} =$$

$$-\frac{1}{2}\sum_{i=j}^{k}\left(\mathbf{z}_i - \boldsymbol{\mu}_0 - \boldsymbol{\rho}(i-j))^T \mathbf{Q}^{-1}\left(\mathbf{z}_i - \boldsymbol{\mu}_0 - \boldsymbol{\rho}(i-j)\right)$$

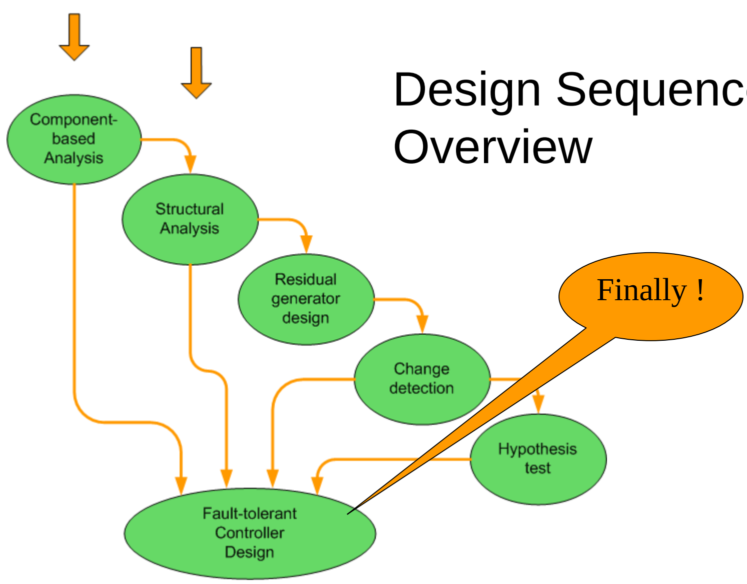
$$+\frac{1}{2}\sum_{i=j}^{k}\left(\mathbf{z}_i - \boldsymbol{\mu}_0)\right)^T \mathbf{Q}^{-1}\left(\mathbf{z}_i - \boldsymbol{\mu}_0)\right)$$

$$S_j^k = \sum_{i=j}^{k} \boldsymbol{\rho}^T(i-j) Q^{-1}\left(\mathbf{z}_i - \boldsymbol{\mu}_0\right) - \frac{1}{2}\sum_{i=j}^{k} \boldsymbol{\rho}^T(i-j)\mathbf{Q}^{-1}\boldsymbol{\rho}(i-j)$$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 128.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Design Sequence Overview



M. Blanke 2004 Diagnosis& Fault-tolerant Control 132.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

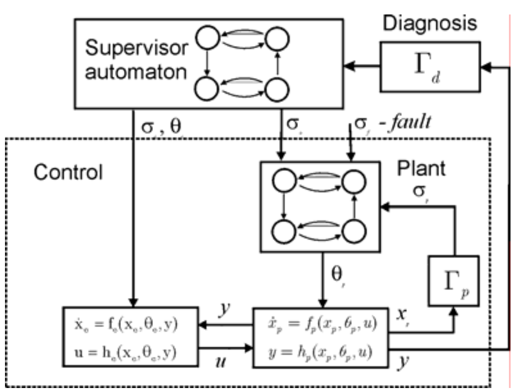
Fault-tolerant control

Chapter 7.1-7.3

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Structure of Plant + Controller



The standard control problem

Objective: O

Structure: S

Parameters: θ

Control law: U

The control problem:

Solve $\langle O, S, \theta, U \rangle$

A system with control is a hybrid entity. The system can be changed by events, some of which are faults. We may change the controller and/or the system by action of a supervisor.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 134.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Diagnosis -> Fault-tolerant

- **Diagnosis**
- Fault detection
- Fault isolation
- Evaluation to get confirmed hypothesis
- Fault estimation

- **Fault-tolerant methods**
- Assess estimated structure
- Is diagnosis unambiguous,
  - determine fault-accommodation action
- If not,
  - react according to highest severity
  - accommodate both/all possible scenarios
- Reconfigure in time

M. Blanke 2004 Diagnosis& Fault-tolerant Control 135.

DANMARKS TEKNISKE UNIVERSITET

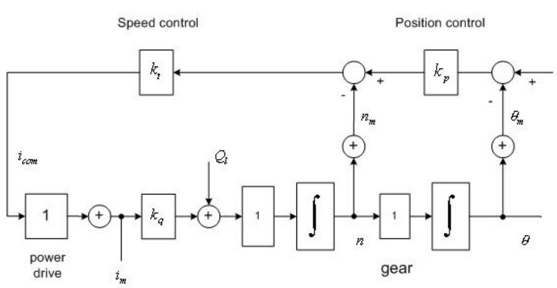
Ørsted•DTU

Standard control problem - example

Objective:

Obtain bandwidth > 2 rad/s, loop damping > 0.2

load suppression better than 0.5 of nominal in range [0, 0.5] rad/s,



$$\theta(s) = \frac{k_p k_t k_q}{s^2 + k_t k_q s + k_p k_t k_q} \theta_{ref}(s)$$

Compare with standard form

$$\theta(s) = \frac{\omega_b^2}{s^2 + 2\varsigma\omega_b s + \omega_b^2} \theta_{ref}(s)$$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 136.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Standard control problem - example

Solution:
Bandwidth >= 2 rad/s, loop damping >= 0.2
load suppression better than 0.5 of nominal in range [0, 0.5] rad/s,

Steady state error due to fixed value of Q_l is

$$\lim_{t\to\infty}\left(\theta-\theta_{ref}\right)=\frac{1}{k_p k_t k_q}Q_l$$

Nominal solution: $U: i_{com}=k_t\left(k_p\left(\theta_{ref}-\theta_m\right)-n_m\right);$

Choose ς=0.5 as nominal value.

$$k_p k_t \geq 4\frac{1}{k_q};\ \frac{k_p}{k_t}\geq 1 \Rightarrow k_t^2=4\frac{1}{k_q}; k_p=k_t$$

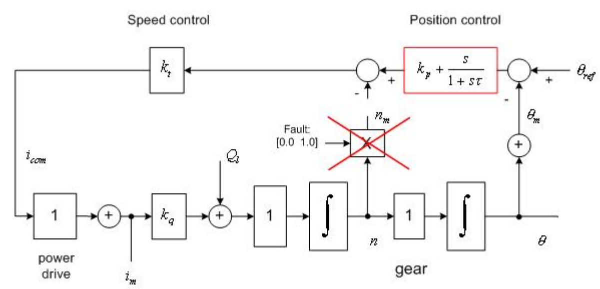
Control error is is $\theta-\theta_{ref}\rightarrow\frac{1}{4}\left(\frac{1}{\omega_b^2}\right)Q_l$ for $t\rightarrow\infty$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 137.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Handling of fault - reconfiguration

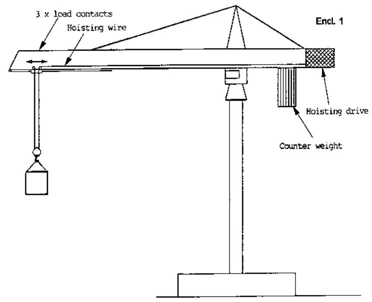
- Fault reconfiguration: a sensor failure in inner loop.
- Switch to differentiating control when fault is diagnosed



M. Blanke 2004 Diagnosis& Fault-tolerant Control 138.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU



A stop using the emergency brake subjects the structure to large stresses. An x-ray certification is required after each emergency stop. Graceful degradation pays off - a potential application for fault-tolerant control.

The real thing

By courtesy from C. Thybo

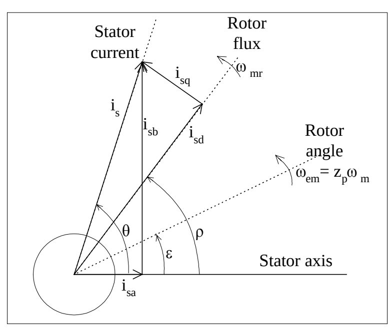
M. Blanke 2004 Diagnosis& Fault-tolerant Control

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Handling of faults – Induction Motor

- High performance controller that needs several sensor inputs is replaced (at run time)



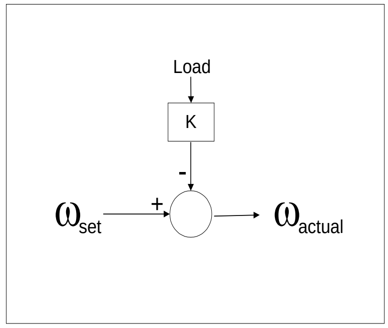
- Flux vector control - high performance, measurement needed

M. Blanke 2004 Diagnosis& Fault-tolerant Control

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Handling of sensor faults – induction motor

- High performance controller that needs several sensor inputs is replaced (at run time) with scalar control that can run with remaining sensors but with reduced performance



- Scalar control - low performance, no sensors

M. Blanke 2004 Diagnosis& Fault-tolerant Control

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Fault-tolerance against sensor faults

Chapter 7.1 - 7.2

Handling of sensor faults by reconfiguration

Reconfiguration: Failed sensor measurement is replaced by an estimate, which is used in the feedback loop

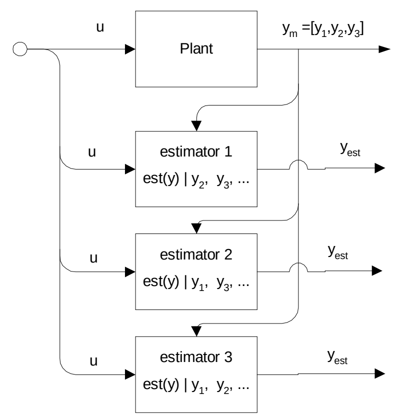
$$y_k = (1 - H(f_k))y_k + H(f_k)\hat{y}(f_k)$$

Condition for observer k to exist

$(A, [c_1, .., c_{k-1}, c_{k+1}, .., c_m])$ is observable

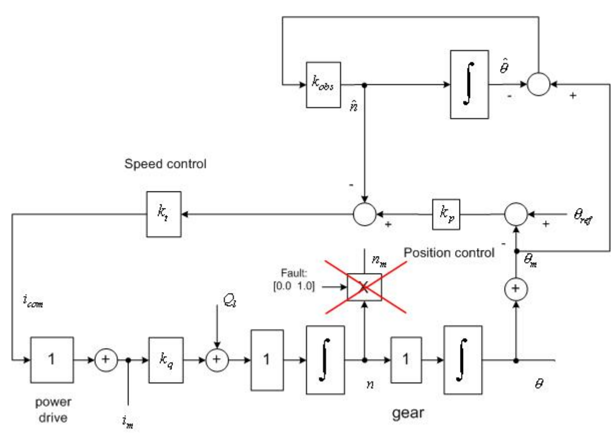
where c_i is a column of C

If not fully observable, the unobservable subsystem must at least be stable

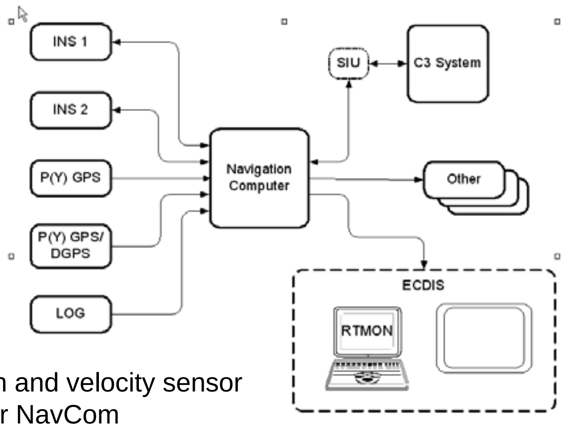


DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Handling of sensor fault by output estimation



Application - marine navigation



Position and velocity sensor input for NavCom

Application to marine navigation

Navigation computer to make fault-tolerant sensor fusion for

- Inertial navigation units
- GPS receivers (L1,L2) and diff. GPS and L1 only types
- Ship's log
- Conventional gyro units
- Vertical gyro
- Output of position data: 1Hz, attitude data: 16Hz.

A comercial product from is available with algorithms by the author.

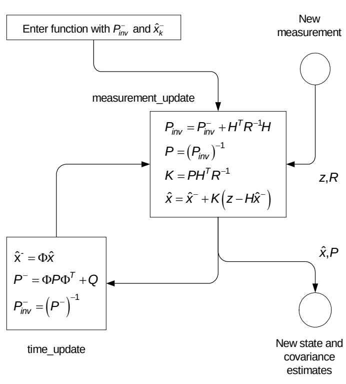
DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Fault-tolerant sensor fusion - main issues

- Data arrive asynchroneously
- Data have different sampling rates
- Each new data package need be validated before it is included in the sensor fusion solution
- Data from a particular sensor may stop without warning
- Faults can develop arbitrarily (abrupt, incipient, intermittent)
- Faults on certain sensors may be correlated (GPS)
- Noise on different sensor types is often uncorrelated

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Optimal sensor fusion



1. Compute inverse covariance:

$$\mathbf{P}_k^{-1} = (\mathbf{P}_k)^{-1} + \mathbf{C}_k^T \mathbf{R}_k^{-1} \mathbf{C}_k$$

$$\mathbf{P}_k = \left(\mathbf{P}_k^{-1}\right)^{-1}$$

$$\mathbf{K}_k = \mathbf{P}_k \mathbf{C}_k^T \mathbf{R}_k^{-1}$$

2. Update estimate

$$\hat{\mathbf{x}}_k = \hat{\mathbf{x}}_k^- + \mathbf{K}_k \left(\mathbf{y}_k - \mathbf{C}_k \hat{\mathbf{x}}_k^-\right)$$

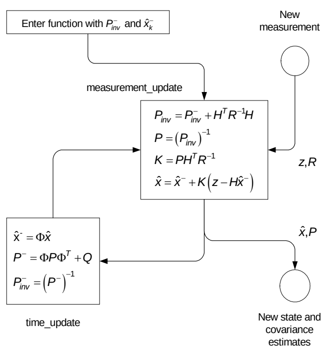
3. Predict in time

$$\hat{\mathbf{x}}_{k+1}^- = \mathbf{\Phi}_k \hat{\mathbf{x}}_k$$

$$\mathbf{P}_{k+1}^{-1} = \mathbf{\Phi}_k \mathbf{P}_k \mathbf{\Phi}_k^T + \mathbf{Q}_k$$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Inverse covariance updating



Measurements that are uncorrelated may be updated when independent sensor packages arrive:

$$\mathbf{P}_k^{-1} = (\mathbf{P}_k)^{-1} + \left[\mathbf{C}_1^T, \mathbf{C}_2^T, \mathbf{C}_3^T\right] \begin{bmatrix} \mathbf{R}_1^{-1} & 0 & 0 \\ 0 & \mathbf{R}_2^{-1} & 0 \\ 0 & 0 & \mathbf{R}_3^{-1} \end{bmatrix} \begin{bmatrix} \mathbf{C}_1 \\ \mathbf{C}_2 \\ \mathbf{C}_3 \end{bmatrix}$$

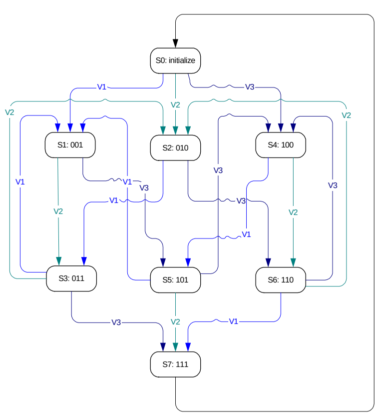
$$= (\mathbf{P}_k)^{-1} + \mathbf{C}_1^T \mathbf{R}_1^{-1} \mathbf{C}_1 + \mathbf{C}_2^T \mathbf{R}_2^{-1} \mathbf{C}_2 + \mathbf{C}_3^T \mathbf{R}_3^{-1} \mathbf{C}_3$$

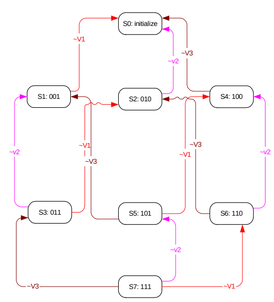
This allows asynchronous or missing data

M. Blanke 2004 Diagnosis& Fault-tolerant Control 149.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

State logic – asynchroneus events





- Treatment of sensor data as random events in time – shown as state-event diagrams for 3 sensors

M. Blanke 2004 Diagnosis& Fault-tolerant Control 150.

Consistent implementation

State event logic in consistent implementation:

change state: s(k+1) ← S(s(k),e(k))

computations: r(t) ← R(s(k),e(k))

$s \in \{0,1,2,3,4,5,6\}$,

$e \in \{v_1, v_2, v_3, \neg v_1, \neg v_2, \neg v_3\}$

Three sets of sensor events: valid and not-valid

State transition matrix

$$S(s,e)=\begin{bmatrix} 1 & 2 & 3 & 0 & 0 & 0 \\ 1 & 3 & 5 & 0 & 1 & 1 \\ 3 & 2 & 6 & 2 & 0 & 2 \\ 5 & 6 & 4 & 4 & 4 & 0 \\ 3 & 7 & 3 & 2 & 1 & 3 \\ 5 & 7 & 5 & 4 & 5 & 1 \\ 7 & 6 & 6 & 6 & 4 & 2 \end{bmatrix}$$

Generation of state-event logics

State event logic in consistent implementation:

change state: s(k+1) ← S(s(k),e(k))

computations: r(t) ← R(s(k),e(k))

$s \in \{0,1,2,3,4,5,6\}$,

$e \in \{v_1, v_2, v_3, \neg v_1, \neg v_2, \neg v_3\}$

Three sets of sensor events: valid and not-valid

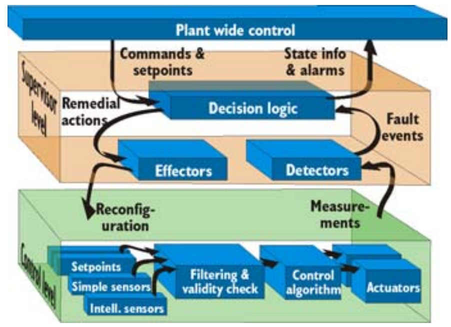
Essential to make a correct implementation:

1. Make analytic generation of state-event automata.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Architecture for implementation

- An architecture is necessary for Fault-tolerant control implementation
- Include detectors and fault-accommodation according to prior analysis
- On-line decision and optimization is possible
- An autonomous supervisor is an adequate control archi-tecture for complex systems
- A development procedure was suggested and refined



M. Blanke 2004 Diagnosis& Fault-tolerant Control 153.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Application in Space

- Fault-tolerant ideas applied to the Danish Ørsted satellite- in operation in space since 23 Feb 1999 - and still active.
- Sensor fusion between
  - Star imager
  - Sun sensors
  - Magnetometer and Earth-B-field model
- Gives
  - Attitude
  - Angular velovity estimate

M. Blanke 2004 Diagnosis& Fault-tolerant Control 154.

Actuator Faults

Actuator faults

Let $\boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)$ describe the action of the faulty actuator:

$$\dot{\mathbf{x}}(t) = \mathbf{A}x(t) + \sum_{i\in I_N} \mathbf{b}_i u_i(t) + \sum_{i\in I_F} \boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)$$

Two solutions:

1. We may use an estimate $\hat{\boldsymbol{\beta}}$ and redesign using

$$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \sum_{i\in I_N} \mathbf{b}_i u_i(t) + \sum_{i\in I_F} \hat{\boldsymbol{\beta}}_i\left(u_i(t),\theta_i\right)$$

2. We may use the non-faulty actuators only, and redesign using

$$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \sum_{i\in I_N} \mathbf{b}_i u_i(t)$$

Actuator fault - fault estimation (1)

Let $\boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)$ describe the action of the faulty actuator:

$$\dot{\mathbf{x}}(t)=\mathbf{A}x(t)+\sum_{i\in I_N}\mathbf{b}_i u_i(t)+\sum_{i\in I_F}\boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)$$

Two solutions:

1. We may use an estimate $\hat{\boldsymbol{\beta}}$ and compensate, if possible using

$$\dot{\mathbf{x}}(t)=\mathbf{A}\mathbf{x}(t)+\left(\sum_{i\in I_N}\mathbf{b}_i u_i(t)-\sum_{i\in I_F}\hat{\boldsymbol{\beta}}_i\left(u_i(t),\theta_i\right)\right)+\sum_{i\in I_F}\boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)$$

2. We may use the non-faulty actuators only, and redesign using

$$\dot{\mathbf{x}}(t)=\mathbf{A}\mathbf{x}(t)+\sum_{i\in I_N}\mathbf{b}_i u_i(t)$$

Actuator fault - fault estimation (2)

Let $\boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)$ describe the action of the faulty actuator. Then

$$\sum_{i\in I_N}\mathbf{b}_i u_i(t)+\sum_{i\in I_F}\boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)=\mathbf{0}$$

would outbalance the fault.

One might use an estimate of $\hat{\boldsymbol{\beta}}$ and redesign using

$$\dot{\mathbf{x}}(t)=\mathbf{A}\mathbf{x}(t)+\sum_{i\in I_N}\mathbf{b}_i u_i(t)-\sum_{i\in I_F}\hat{\boldsymbol{\beta}}_i\left(u_i(t),\theta_i\right)+\sum_{i\in I_F}\boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)$$

$$\dot{\mathbf{x}}(t)=\mathbf{A}\mathbf{x}(t)+\mathbf{B}_f u_f(t)+\mathbf{B}_f u_{comp}(t)+\sum_{i\in I_F}\boldsymbol{\beta}_i\left(u_i(t),\theta_i\right)\Rightarrow$$

$$\mathbf{B}_f u_{comp}(t)=-\sum_{i\in I_F}\hat{\boldsymbol{\beta}}_i\left(u_i(t),\theta_i\right)$$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Actuator fault - fault estimation (3)

If the pseudoinverse of $\mathbf{B}_h$ exists, then a solution to compensator design is

$$\mathbf{u}_{comp}(t) = -\left(\mathbf{B}_f^T \mathbf{B}_f\right)^{-1} \mathbf{B}_f^T \sum_{i \in I_F} \hat{\boldsymbol{\beta}}_i \left(u_i(t), \theta_i\right)$$

However, this does not necessarily give a trajectory of $\mathbf{x}$(t) close to the desired - when $\mathbf{B}_f \neq \mathbf{B}$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 159.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Actuator faults – optimal control approach

- Linear quadratic optimal control gives the ”LQ solution” to the state feedback problem.
- If not all states are measured, a state-observer is employed.

Let the system be:

$$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) = \mathbf{A}\mathbf{x}(t) + \sum_{i \in I} \mathbf{B}_i \mathbf{u}_i(t)$$

LQ optimal control: minimize the index

$$J((0,\infty), \mathbf{u}, \mathbf{x}_0) = \frac{1}{2}\int_0^\infty \left(\mathbf{u}^T \mathbf{R}\mathbf{u} + \mathbf{x}^T \mathbf{Q}\mathbf{x}\right) dt \quad \mathbf{Q} \geq 0,\ \mathbf{R} > 0,\ \mathbf{x}(0) = \mathbf{x}_0$$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 160.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

LQ optimal control – nominal system

A solution to the LQ problem requires $(\mathbf{A},\mathbf{B})$ is controlable.

The steady state controller $\mathbf{L}$ is obtained as:

$$\mathbf{u}(t) = -\mathbf{R}^{-1}\mathbf{B}^T\mathbf{S}\mathbf{x}(t) = -\mathbf{L}\mathbf{x}(t)$$

where $\mathbf{S}$ is the (stable) solution to the steady state Riccati equation

$$\mathbf{0} = \mathbf{A}^T\mathbf{S} + \mathbf{S}\mathbf{A} - \mathbf{S}\mathbf{B}\mathbf{R}^{-1}\mathbf{B}^T\mathbf{S} + \mathbf{Q}$$

The closed-loop system

$\dot{\mathbf{x}}(t) = \left(\mathbf{A} - \mathbf{B}\mathbf{R}^{-1}\mathbf{B}^T\mathbf{S}\right)\mathbf{x}(t)$ is stable.

The value of the "cost" index is $J((0,\infty),\mathbf{x}_0) = \mathbf{x}_0{}^T\mathbf{S}\mathbf{x}_0$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

All stabilizing state feedback controllers

Let a stabilizing LQ feedback law be

$$\mathbf{u}_1(t) = -\mathbf{R}^{-1}\mathbf{B}^T\mathbf{S}_1\mathbf{x}(t) = -\mathbf{L}_1\mathbf{x}(t)$$

the feedback gain matrix is $\mathbf{L}_1 = \mathbf{R}^{-1}\mathbf{B}^T\mathbf{S}_1$

and let $\mathbf{S}_1$ be the solution to

$$\mathbf{0} = \mathbf{A}^T\mathbf{S}_1 + \mathbf{S}_1\mathbf{A} - \mathbf{S}_1\mathbf{B}\mathbf{R}^{-1}\mathbf{B}^T\mathbf{S}_1 + \mathbf{Q}$$

Then

$$J\left(\left(t_1,\infty\right),\mathbf{x}_1\right) = \mathbf{x}_1^T\mathbf{S}_1\mathbf{x}_1$$

is the measure of "cost" starting at $\mathbf{x}_1$ at time t_1.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Actuator fault at time t_f

Given: No actuator fault $t \subset [0, t_f]$, an actuator fault $t \subset [t_f, \infty]$

Assume the faulty actuators can be described by a linear model:

$\hat{\boldsymbol{\beta}}(u_i(t), \hat{\theta}_i) = \hat{\mathbf{b}}_i u_i(t), i \in I_F$

Then the model of the faulty system is

$$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \sum_{i \in I_N} \mathbf{b}_i u_i(t) + \sum_{i \in I_F} \hat{\boldsymbol{\beta}}_i \left(u_i(t), \theta_i\right) \Rightarrow$$

$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}_f \mathbf{u}(t)$ with $\mathbf{x}(t_f) = \mathbf{x}_f$ at the time the fault occurs

M. Blanke 2004 Diagnosis& Fault-tolerant Control 163.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Actuator fault at time t_f

With $\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}_f \mathbf{u}(t)$ with $\mathbf{x}(t_f) = \mathbf{x}_f$ at t_f

the trajectory for $t \subset \left[t_f, \infty\right]$ is optimised using

$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}_f \mathbf{u}(t)$

$\mathbf{u}(t) = \mathbf{R}^{-1}\mathbf{B}_f^T \mathbf{S}_f \mathbf{x}_f(t).$

where $\mathbf{S}_f$ be the solution to

$\mathbf{0} = \mathbf{A}^T \mathbf{S}_f + \mathbf{S}_f \mathbf{A} - \mathbf{S}_f \mathbf{B}_f \mathbf{R}^{-1} \mathbf{B}_f^T \mathbf{S}_f + \mathbf{Q}$

and $\mathbf{S}_f$ is symmetric ($\mathbf{S}_f = \mathbf{S}_f^T$)

M. Blanke 2004 Diagnosis& Fault-tolerant Control 164.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Actuator fault at time t_f – total cost

If the index "consumed" from $t \subset \left[0, t_f\right]$ is $J\left(\left(0, t_f\right), x_o\right)$

Then $J\left(\left(\left(0, t_f\right), x_o\right), \left(\left(t_f, \infty\right), x_f\right)\right) = J\left(\left(0, t_f\right), x_o\right) + \mathbf{x}_f^T \mathbf{S}_f \mathbf{x}_f$

instead of $J\left(\left(0, \infty\right), x_o\right) = \mathbf{x}_0^T \mathbf{S} \mathbf{x}_0$

$J\left(\left(0, \infty\right), x_o\right) = J\left(\left(0, t_f\right), x_o\right) + \mathbf{x}_f^T \mathbf{S} \mathbf{x}_f$

$\Rightarrow J\left(\left(0, t_f\right), x_o\right) = \mathbf{x}_0^T \mathbf{S} \mathbf{x}_0 - \mathbf{x}_f^T \mathbf{S} \mathbf{x}_f$

$\Rightarrow J\left(\left(\left(0, t_f\right), x_o\right), \left(\left(t_f, \infty\right), x_f\right)\right) = \mathbf{x}_0^T \mathbf{S} \mathbf{x}_0 + \mathbf{x}_f^T \left(\mathbf{S}_f - \mathbf{S}\right) \mathbf{x}_f$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 165.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Ship steering - example (1)

Given (ship with H_1=0 and two rudders)

$$\frac{d}{dt}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \frac{k}{I}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$$

Optimization criterion

$$\text{J}=\int_0^\infty \left(x^T Qx + u^T Ru\right) dt,\ \text{Q} = \begin{bmatrix} 1 & 0 \\ 0 & 100 \end{bmatrix}; R = 100 * \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Find the optimal controller for

- the nomonal case (k/I = 1/26.8 N / kgm^2)
- case when one actuator is defect $B = \frac{k}{I}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

M. Blanke 2004 Diagnosis& Fault-tolerant Control 166.

Ship steering – example (2)

Define problem for Matlab *lqr* function:

$$\mathbf{A} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}; \ \mathbf{B}_0 = \frac{1}{26.8}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\mathbf{Q} = \begin{bmatrix} 1 & 0 \\ 0 & 100 \end{bmatrix}; \mathbf{R} = 100 * \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Find the optimal controller for

1)the nomonal case:

$[\mathbf{K},\ \mathbf{S},\ \lambda] = lqr(\mathbf{A}, \mathbf{B}_0, \mathbf{Q}, \mathbf{R})$

2) Case when one actuator is defect $\mathbf{B}_2 = \frac{1}{26.8}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

$[\mathbf{K}_2,\ \mathbf{S}_2,\ \lambda] = lqr(\mathbf{A}, \mathbf{B}_2, \mathbf{Q}, \mathbf{R})$

Ship steering – example (3)

Results:

Nominal case (no fault)

$$\mathbf{K}_0 = \begin{bmatrix} 4.35 & 0.71 \\ 4.35 & 0.71 \end{bmatrix}; \ \mathbf{S}_0 = \begin{bmatrix} 11668 & 1895 \\ 1895 & 732 \end{bmatrix}; \lambda_{cl} = \text{-}0.162 \pm j0.162$$

Fault on actuator 2:

$$\mathbf{K}_2 = \begin{bmatrix} 7.32 & 1.0 \\ 0 & 0 \end{bmatrix}; \ \mathbf{S}_2 = \begin{bmatrix} 19623 & 2680 \\ 2680 & 616 \end{bmatrix}; \lambda_{cl} = \text{-}0.137 \pm j0.137$$

Test response from initial condition in closed loop

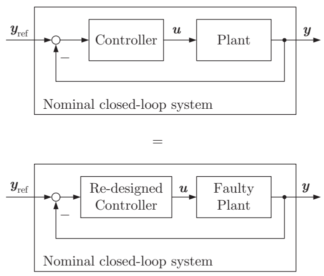
$\mathbf{A}_{cl0} = \mathbf{A} - \mathbf{BK}_0$ (case 0) $\mathbf{A}_{cl2} = \mathbf{A} - \mathbf{B}_2\mathbf{K}_2$

sys =ss($\mathbf{A}_{cl}$,$\mathbf{A}_{cl}$,$\mathbf{C}$,$\mathbf{D}$) with $\mathbf{C}$=eye(2,2); $\mathbf{D}$ = 0*eye(2,2)

step(sys)

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Model-matching state-feedback



The nominal (no fault) system in closed state feedback loop:

$$\dot{\mathbf{x}}(t) = \left(\mathbf{A} - \mathbf{BK}\right)\mathbf{x}(t)$$

$$\mathbf{y}(t) = \mathbf{Cx}(t)$$

after the fault occurs,

$$\dot{\mathbf{x}}(t) = \mathbf{A}_f\mathbf{x}(t) - \mathbf{B}_f\mathbf{u}(t)$$

$$\mathbf{y}(t) = \mathbf{C}_f\mathbf{x}(t)$$

with new state feeedback controller:

$$\dot{\mathbf{x}}(t) = \left(\mathbf{A}_f - \mathbf{B}_f\mathbf{K}_f\right)\mathbf{x}(t)$$

$$\mathbf{y}(t) = \mathbf{C}_f\mathbf{x}(t)$$

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Model-matching state-feedback (2)

Ideal if we could obtain $\mathbf{A} - \mathbf{BK} = \mathbf{A}_f - \mathbf{B}_f\mathbf{K}_f$

This is only rarely possible (requires redundant actuators).

Consider the relaxed condition:

$$\exists\, \mathbf{L}_f \subset \{\mathbf{L}_{stab}\} : \min \left\| \left(\mathbf{A} - \mathbf{BK}\right) - \left(\mathbf{A}_f - \mathbf{B}_f\mathbf{K}_f\right) \right\| \quad ?$$

If the pseudo-inverse of $\mathbf{B}_{\mathrm{f}}$ exists

$$\mathbf{B}_f\mathbf{K}_f = \mathbf{A}_f - \left(\mathbf{A} - \mathbf{BK}\right) \Rightarrow \mathbf{L}_f = \left(\mathbf{B}_f^T\mathbf{B}_f\right)^{-1}\mathbf{B}_f^T\left(\mathbf{A}_f - \mathbf{A} + \mathbf{BK}\right)$$

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Model-matching output-feedback sensor fault

Let the controller be

$\mathbf{u}(t) = -\mathbf{K}\mathbf{y}(t) \Rightarrow$

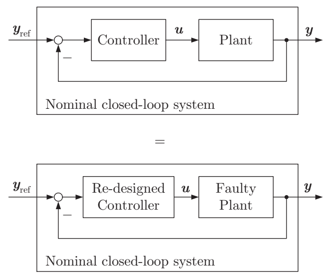
$\dot{\mathbf{x}}(t) = \left(\mathbf{A} - \mathbf{B}\mathbf{K}\mathbf{C}\right)\mathbf{x}(t)$

$\mathbf{y}(t) = \mathbf{C}\mathbf{x}(t)$

After the a sensor fault occurs,

$\dot{\mathbf{x}}(t) = \left(\mathbf{A} - \mathbf{B}\mathbf{K}_f\mathbf{C}_f\right)\mathbf{x}(t)$

$\mathbf{y}(t) = \mathbf{C}_f\mathbf{x}(t)$



Exact model matching if $\mathbf{K}_f\mathbf{C}_f = \mathbf{K}\mathbf{C}$.

If $\mathbf{C} = \mathbf{L}\mathbf{C}_f$ then $\mathbf{K}_f = \mathbf{K}\mathbf{L}$ gives exact model matching and we use $\mathbf{u}(t) = -\mathbf{K}\mathbf{L}\mathbf{y}(t)$ after the fault occurs.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 171.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Model-matching output-feedback actuator fault

Let the controller be

$\mathbf{u}(t) = -\mathbf{K}\mathbf{y}(t) \Rightarrow$

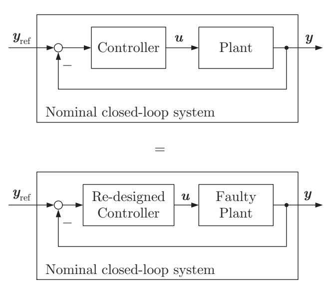
$\dot{\mathbf{x}}(t) = \left(\mathbf{A} - \mathbf{B}\mathbf{K}\mathbf{C}\right)\mathbf{x}(t)$

$\mathbf{y}(t) = \mathbf{C}\mathbf{x}(t)$

After the a sensor fault occurs,

$\dot{\mathbf{x}}(t) = \left(\mathbf{A} - \mathbf{B}_f\mathbf{K}_f\mathbf{C}\right)\mathbf{x}(t)$

$\mathbf{y}(t) = \mathbf{C}\mathbf{x}(t)$



Exact model matching if $\mathbf{B}_f\mathbf{K}_f = \mathbf{B}\mathbf{K}$.

Possible if $\mathbf{B}_f\mathbf{M} = \mathbf{B}$, then $\mathbf{K}_f = \mathbf{M}\mathbf{K}$ gives exact model matching and we use $\mathbf{u}(t) = -\mathbf{M}\mathbf{K}\mathbf{y}(t)$ after the fault has occurred.

M. Blanke 2004 Diagnosis& Fault-tolerant Control 172.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Ship steering example – example (4)

$$\mathbf{B} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \frac{k}{I}; \quad \text{normal case}$$

$$\mathbf{B}_f = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \frac{k}{I}; \quad \text{case of fault on rudder 2}$$

$$\mathbf{M} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \Rightarrow \mathbf{B}_\mathrm{f}\mathbf{M} = \mathbf{B} \Rightarrow \text{model matching}$$

hence switch to $\mathbf{u}(t) = -\mathbf{MK}_0\mathbf{y}(t)$ after the fault is diagnosed

$$\text{or} \begin{bmatrix} u_1(t) \\ u_2(t) \end{bmatrix} = -\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 4.35 & 0.71 \\ 4.35 & 0.71 \end{bmatrix} \begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix} = -2 \begin{bmatrix} 4.35 & 0.71 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix}$$

a rather obvious choice when one out of two parallel actuators fail !

M. Blanke 2004 Diagnosis& Fault-tolerant Control 173.

DANMARKS TEKNISKE UNIVERSITET
Ørsted•DTU

Summary

- Component-based and Structural analysis
  - Coping with complexity and nonlinear behaviour
- Stringent methods for linear case
  - Fault diagnosis
  - Sensor fusion
- Fault-tolerant Control
  - Sensor faults
  - Actuator faults
- Full scale applications
  - Inverter for crane, Satellite attitude control, Sensor fusion for navigation

M. Blanke 2004 Diagnosis& Fault-tolerant Control 178.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

Acknowledgements

- Michel Kinnaert (residual generator design)
- Michelle Basseville and Igor Nikiforov (change detection)
- Marcel Staroswiecki (structural analysis and LQ-FTC)
- Jan Lunze (fault-tolerant design ideas)

- Roozbeh Izadi-Zanamabadi (SA & applications)
- Claus Thybo (Inverter application)
- Torsten Lorentzen (SaTool)

M. Blanke 2004 Diagnosis& Fault-tolerant Control 179.

DANMARKS TEKNISKE UNIVERSITET

Ørsted•DTU

M. Blanke 2004 Diagnosis& Fault-tolerant Control 180.