Detection and isolation of faults and attacks

Claudio De Persis

University of Groningen
Sapienza University of Rome

Current problems in Control Theory
In honor of Prof. Alberto Isidori

Department of Computer Control and Management Engineering
Sapienza University of Rome
September 24 2012

Fault detection and isolation

Fault

A fault in a device (airplane, ship, robot, etc.) is a deviation of the structure of the system or of its parameters from a nominal situation

Fault detection and isolation

Fault detection and isolation is an engineering field dealing with methods for

- Revealing the presence of such deviations (fault detection)
- Differentiating between possible faults and disturbances (fault isolation)

It is a discipline at the crossroad of multiple engineering branches

- Automatic control
- Computer engineering
- Signal processing
- ...

Model-based fault detection

In model-based fault detection the device under monitoring is described by a mathematical model

- Systems of linear ordinary differential equations

$$\begin{aligned} \dot{x} &= Ax + Bu + Lm + Pw \\ y &= Cx \end{aligned}$$

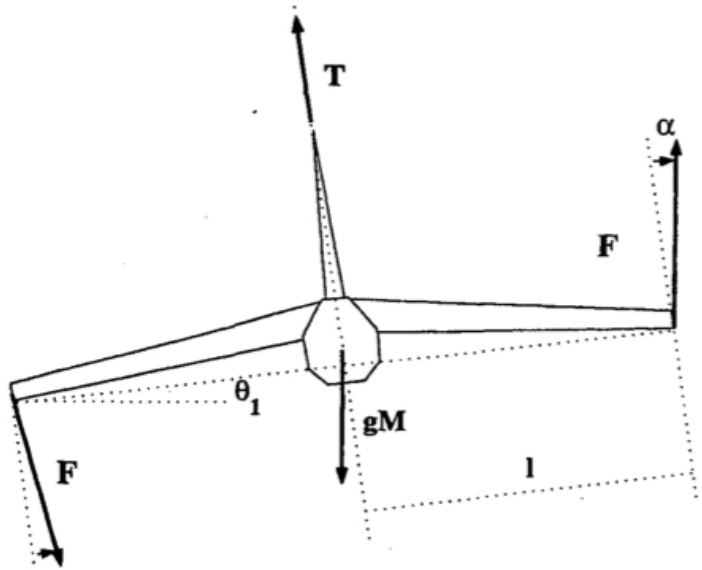
- Systems of nonlinear ordinary differential equations

$$\begin{aligned} \dot{x} &= \underbrace{f(x)}_{\textit{dynamics}} + \underbrace{g(x)u}_{\textit{control}} + \underbrace{\ell(x)m}_{\textit{faults}} + \underbrace{p(x)w}_{\textit{disturbance}} \\ \underbrace{y}_{\textit{measurements}} &= h(x) \end{aligned}$$

Example: VTOL aircraft

Simplified equations of motion of a VTOL aircraft in a vertical lateral plan

x_1, x_2 horizontal position and velocity
y_1, y_2 vertical position and velocity
θ_1, θ_2 roll angle and velocity



$$y = h(x) \begin{pmatrix} x_1 \\ x_2 \\ \theta_1 \\ \theta_2 \end{pmatrix} = h(x)$$

$$\underbrace{\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{y}_1 \\ \dot{y}_2 \\ \dot{\theta}_1 \\ \dot{\theta}_2 \end{pmatrix}}_{\dot{x}} = \underbrace{\begin{pmatrix} x_2 \\ 0 \\ y_2 \\ -g \\ \theta_2 \\ 0 \end{pmatrix}}_{f(x)} + \underbrace{\begin{pmatrix} 0 & 0 \\ -\sin(\theta_1) & \cos(\theta_1) \\ 0 & 0 \\ \cos(\theta_1) & \sin(\theta_1) \\ 0 & 0 \\ 0 & \frac{\ell M}{J}\frac{\cos(\alpha)}{\sin(\alpha)} \end{pmatrix}}_{g(x)} \underbrace{\begin{pmatrix} \frac{1}{M}T \\ \frac{2\sin(\alpha)}{M}F \end{pmatrix}}_{u}$$

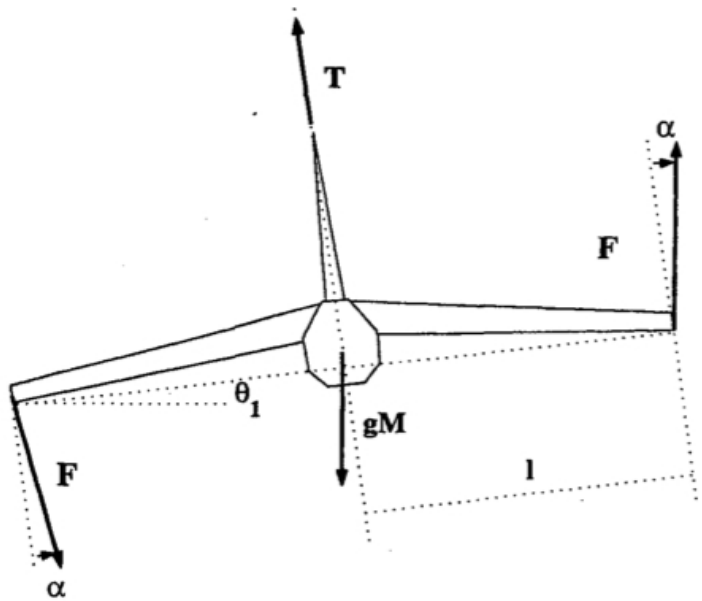
Example: VTOL aircraft

A power loss of the actuators can be modeled as

$$m_i = -(1+\varphi_i)u_i, \quad \varphi_i \in [-1, 0]$$

to obtain the system

$$\dot{x} = f(x) + g(x)u + \underbrace{g(x)}_{\ell(x)} m$$



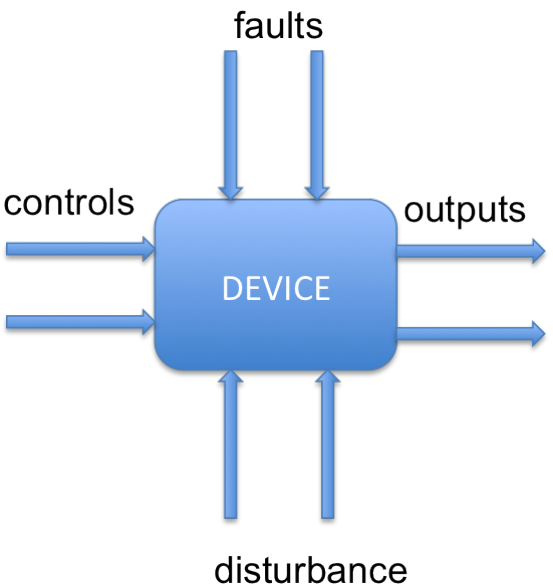
DP-DE SANTIS-ISIDORI. Nonlinear actuator fault detection and isolation for a VTOL aircraft. *American Control Conference* (2001) 4449–4454.

Fault detection

The monitored system

$$\begin{aligned} \dot{x} &= \underbrace{f(x)}_{\textit{dynamics}} + \underbrace{g(x)u}_{\textit{control}} + \underbrace{\ell(x)m}_{\textit{faults}} + \underbrace{p(x)w}_{\textit{disturbances}} \\ \underbrace{y}_{\textit{measurments}} &= h(x) \end{aligned}$$

can be depicted as

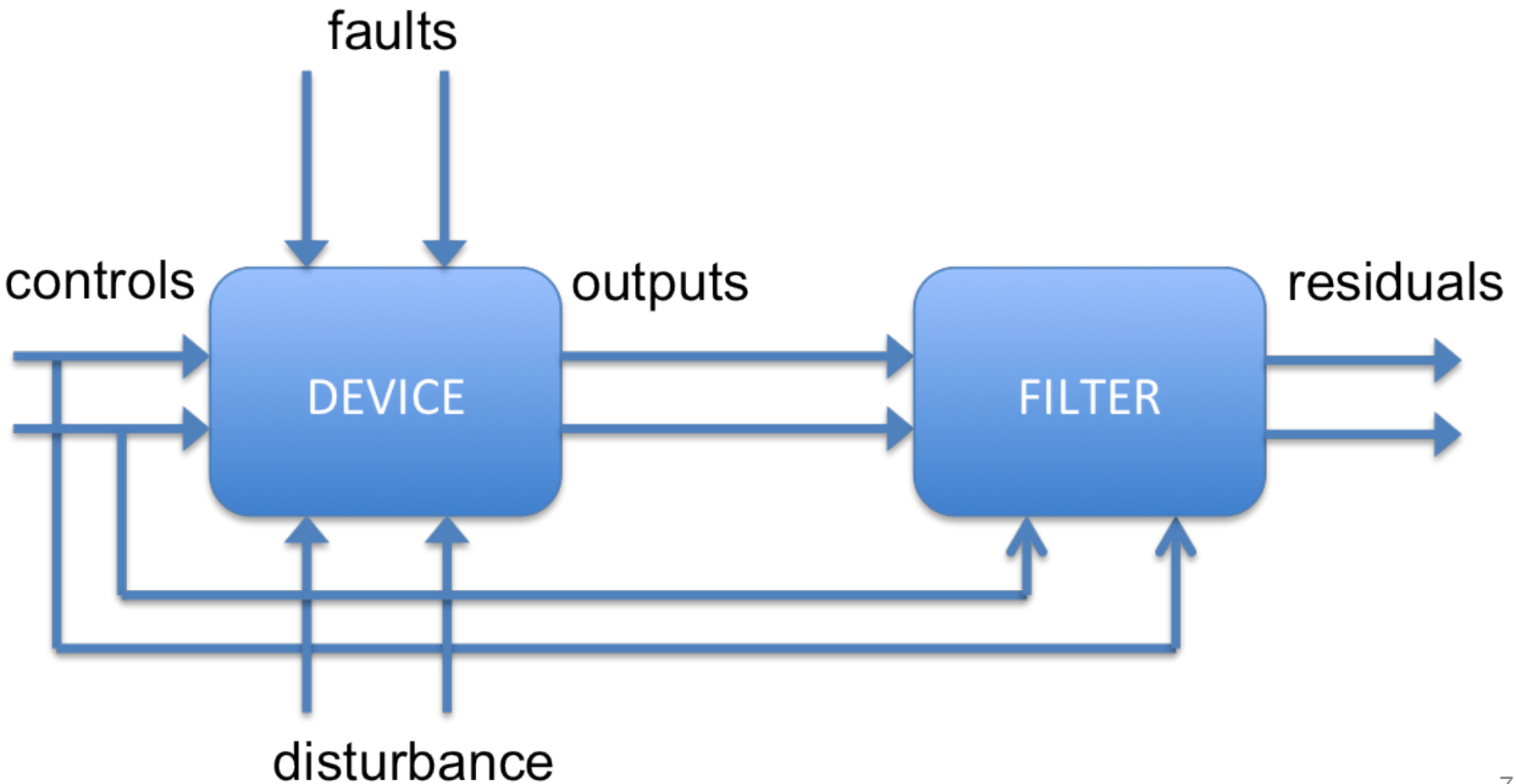


Fault detection

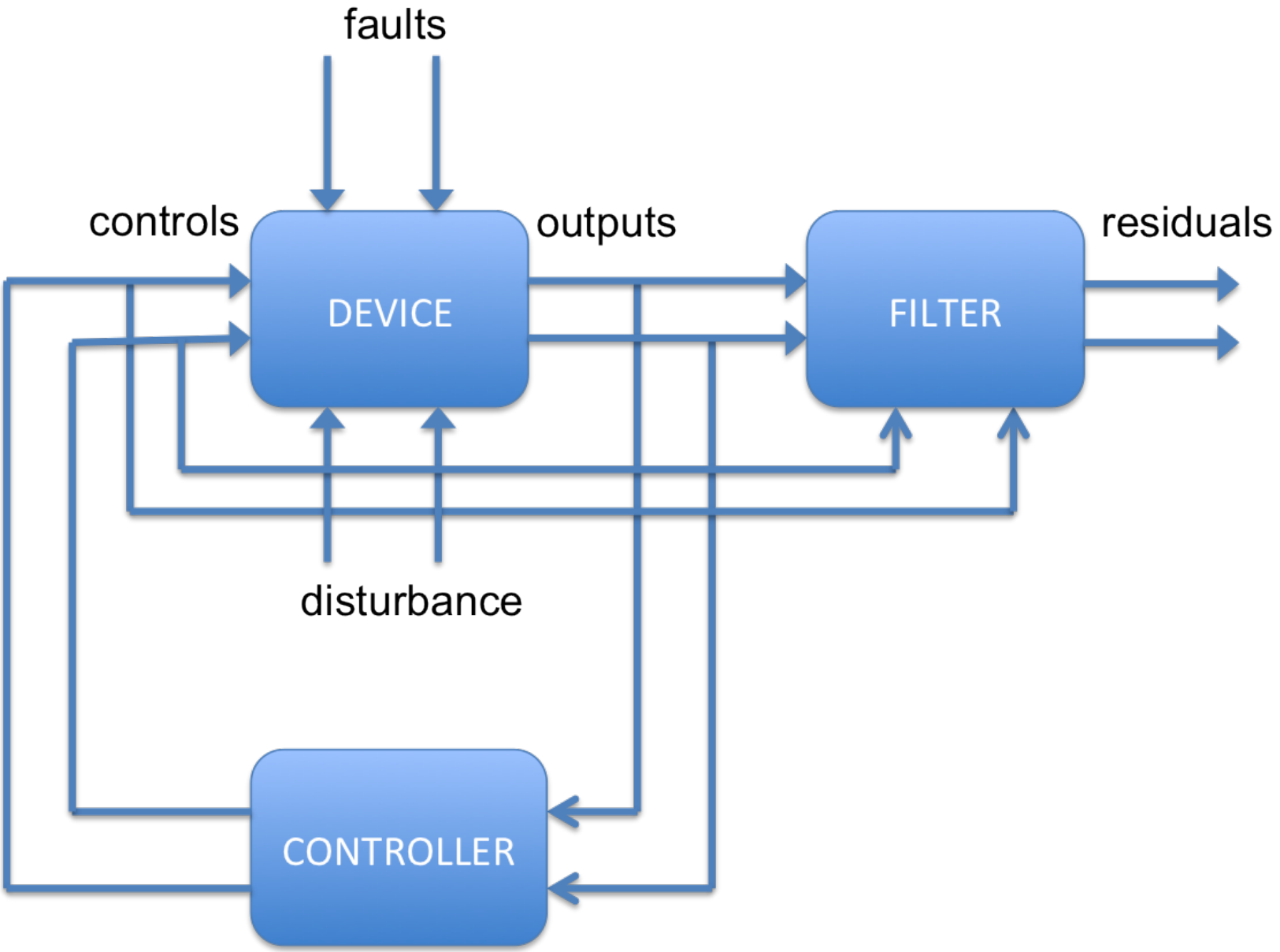
The fault detection is carried out by a diagnostic filter

- It is a dynamical system with the measured signals u, y as inputs
- It generates diagnostic signals (residuals) r

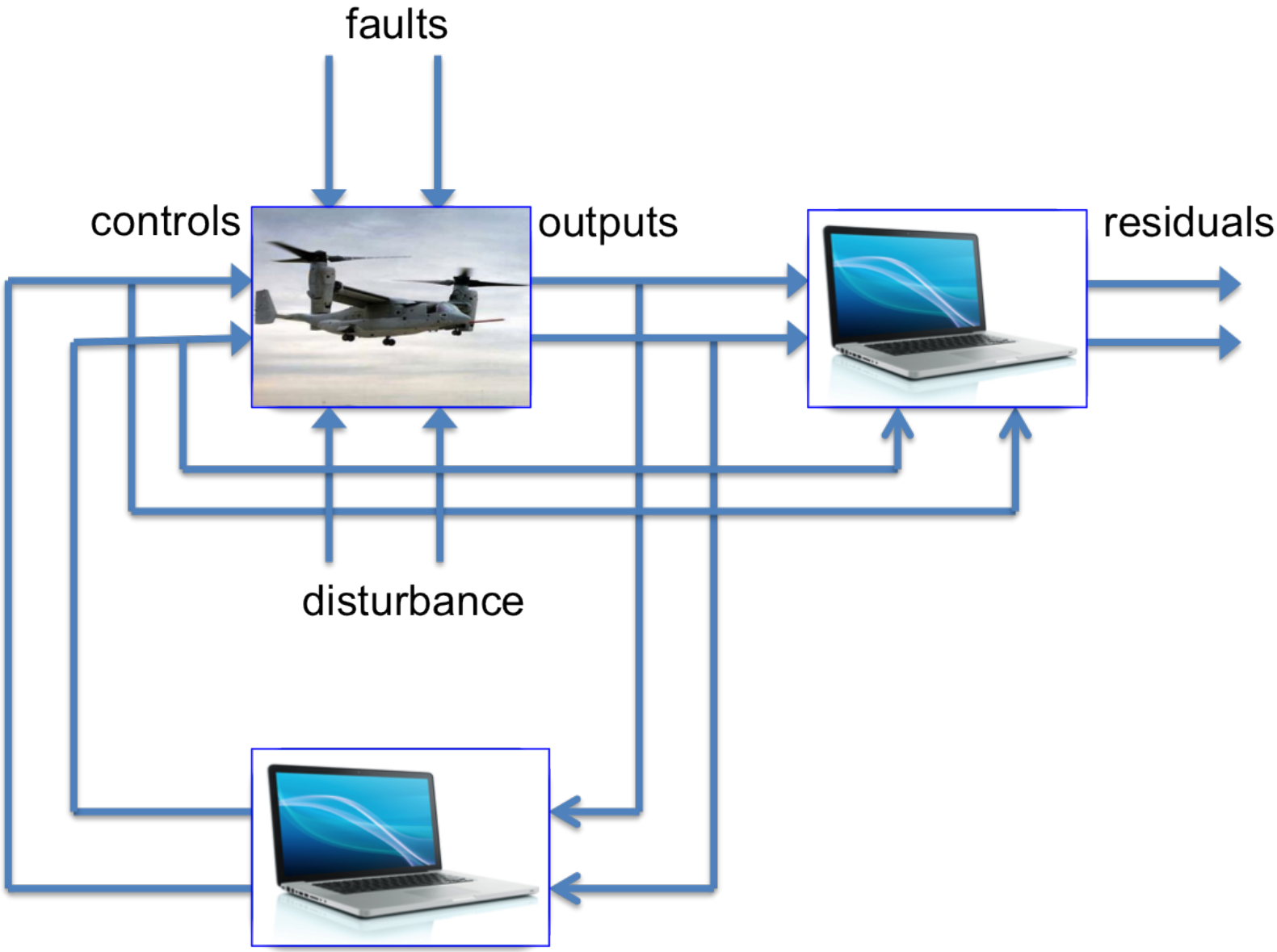
$$\dot{\xi} = \varphi(\xi, y) + \chi(\xi, y)u, \quad r = \psi(\xi, y)$$



Fault detection



Fault detection

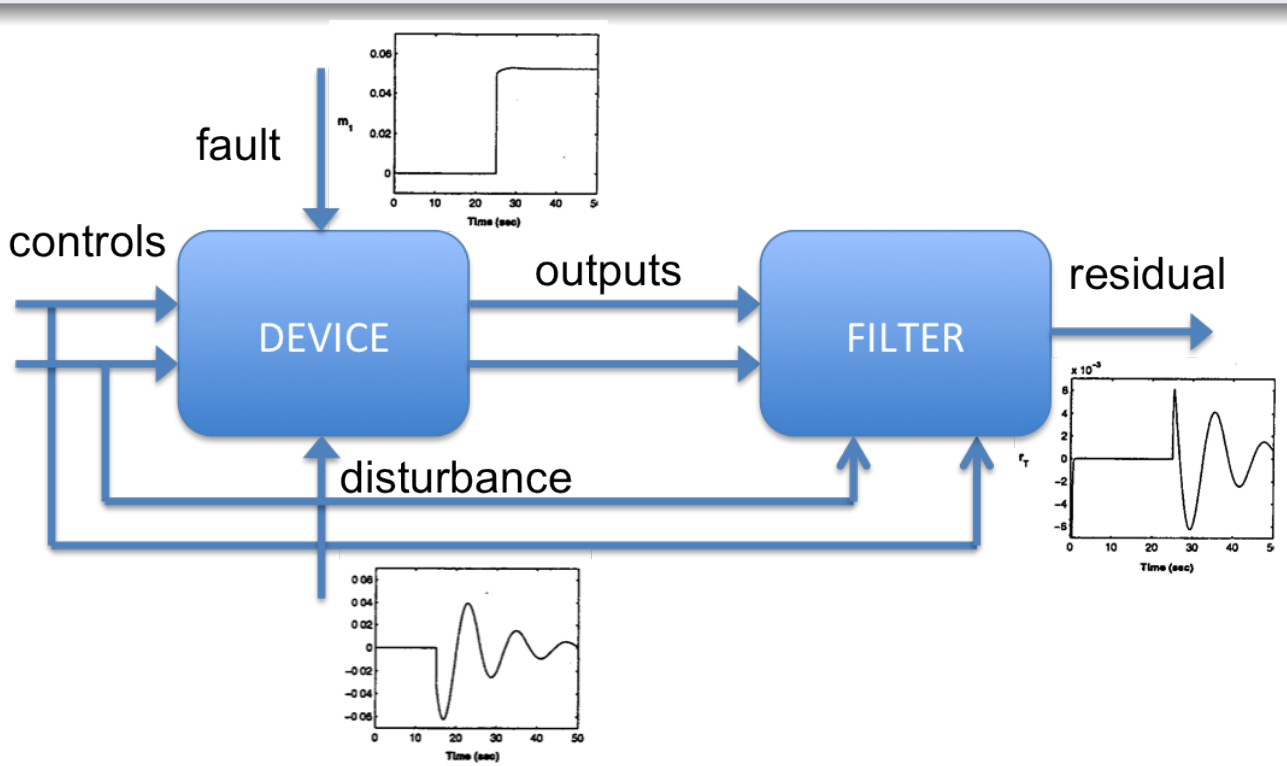


Fault detection

Fundamental problem of residual generation (FPRG)

Given a device affected by a fault m and a disturbance w, find a filter which generates a diagnostic signal r called "residual" such that

- r depends "non trivially" by m, i.e. it is affected by m
- r depends "trivially" by w, i.e. it is unaffected by w
- r converges to zero whenever $m = 0$

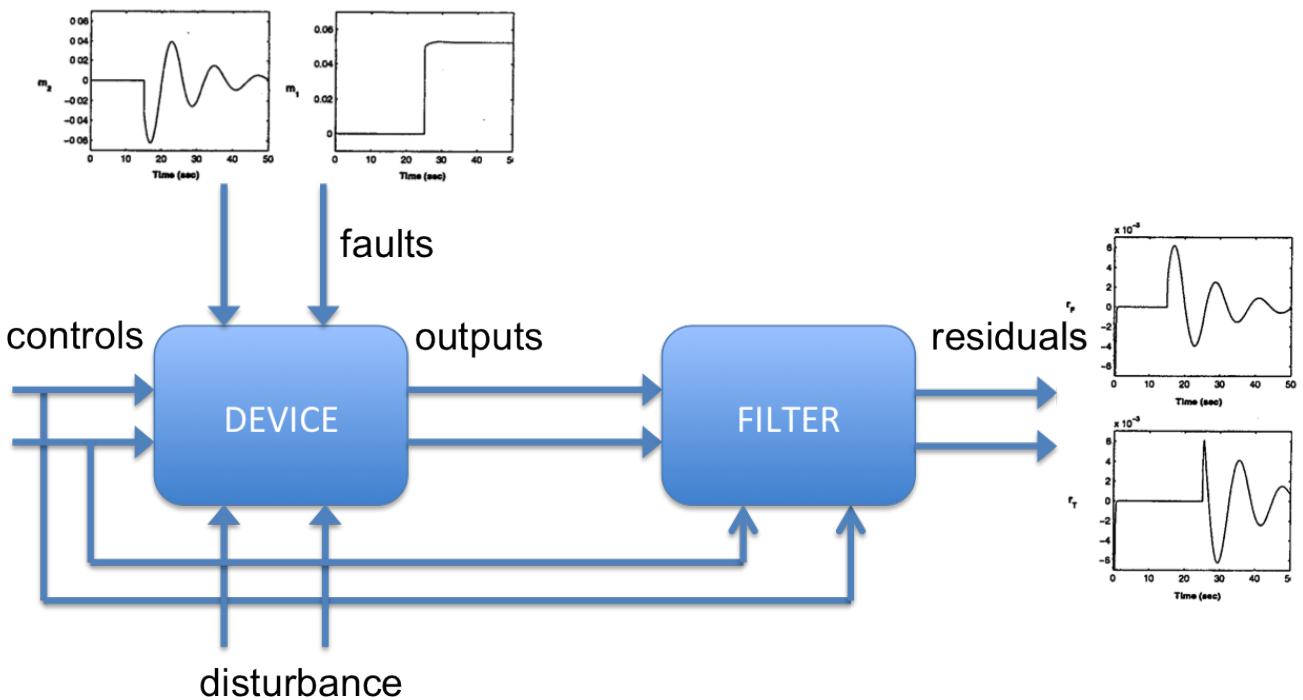


Extended problem of residual generation (EPRG)

Fault detection and isolation

Given a device affected by faults $m_1 \dots m_s$ and a disturbance w, find a filter which generates diagnostic signals $r_1 \dots r_s$ such that

- r_i depends "non trivially" by m_i, $i = 1, \dots, s$
- r_i depends "trivially" by w, m_j for all $j \neq s$
- r_i converges to zero whenever $m_i = 0$



Fundamental problem of residual generation

- F(E)PRG formulated for linear systems by Massoumnia-Willsky-Verghese at the end of the '80s
- The analysis was based on the linear geometric control theory introduced by Basile-Marro and Morse-Wonham at the end of the '60s
- Solving FPRG $\Rightarrow$ solving the EPRG

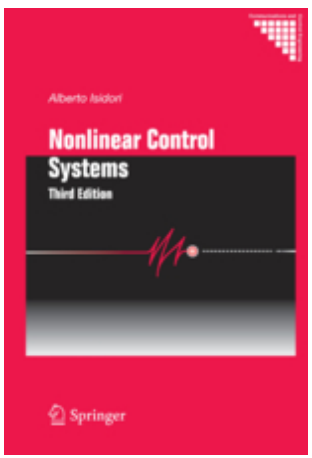
Limitations

- Most of the engineering devices are nonlinear
- Tools for the solution of the problem were not available
- Filter syntesis for nonlinear systems is much more difficult than for linear systems

Fundamental problem of residual generation

Device + filter

$$\begin{pmatrix} \dot{x} \\ \dot{\xi} \end{pmatrix} = \begin{pmatrix} f(x) \\ \varphi(\xi, y) \end{pmatrix} + \begin{pmatrix} g(x) \\ \chi(\xi, y) \end{pmatrix} u + \overbrace{\begin{pmatrix} \ell(x) \\ 0 \end{pmatrix}}^{\ell^e} m + \overbrace{\begin{pmatrix} p(x) \\ 0 \end{pmatrix}}^{p^e} w$$
$$r = \psi(\xi, h(x))$$



The germs of the solution were provided in Alberto's work

r depends "non trivially" by $m \Leftrightarrow \ell^e \notin (\Omega^e)^\perp$

r depends "trivially" by $w \Leftrightarrow p^e \in (\Omega^e)^\perp$

Unobservability distributions

- The missing geometric concept was named *unobservability distribution*
- It plays a fundamental role in the solution of the problem
- It can be computed from f, g, p, h via suitable algorithms

$$
\begin{array}{lcl}
S_0 & = & \operatorname{span}\{p\} \\
S_{k+1} & = & S_k + [g, S_k \cap \ker\{dh\}] \\
S_k & \to & S_*^p
\end{array}
\qquad
\begin{array}{lcl}
Q_0 & = & (S_*^p)^\perp \cap \operatorname{span}\{dh\} \\
Q_{k+1} & = & Q_k \cap (L_g Q_k + \operatorname{span}\{dh\}) \\
Q_k & \to & Q_*^p
\end{array}
$$

DP-ISIDORI. On the observability codistributions of a nonlinear system. *Systems & Control Letters*, 40 (2000) 297–304.

Solution of the FPRG

System

$$\begin{aligned} \dot{x} &= f(x) + g(x)u + \ell(x)m + p(x)w \\ y &= h(x) \end{aligned}$$

Fundamental problem of residual generation (FPRG)

Given a device affected by a fault m and a disturbance w, find a filter which generates a diagnostic signal r called "residual" such that

- r depends "non trivially" by m, i.e. it is affected by m
- r depends "trivially" by w, i.e. it is unaffected by w
- r converges to zero whenever $m = 0$

Theorem

There exists a solution to the FPRG $\Leftrightarrow \ell \notin (Q_*^p)^\perp$

Synthesis of the diagnostic filter

$$\ell \notin (Q_*^p)^\perp \text{ implies } \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \Phi(x), \quad \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \Psi(y)$$

so that

$$\begin{aligned} \dot{z}_1 &= f_1(z_1, z_2) + g_1(z_1, z_2)u + \ell_1(z)m \\ \dot{z}_2 &= f_2(z) + g_2(z)u + \ell_2(z)m + p_2(z)w \\ \dot{z}_3 &= f_3(z) + g_3(z)u + \ell_3(z)m + p_3(z)w \\ y_1 &= h_1(z_1) \\ y_2 &= z_2 \end{aligned}$$

with

- $\ell_1(z) \neq 0$ for every z
- f_1, g_1, h_1 (locally weakly) observable

DP-ISIDORI. A geometric approach to nonlinear fault detection and isolation. *IEEE Transactions on Automatic Control*, 46, 6 (2001), 853–865

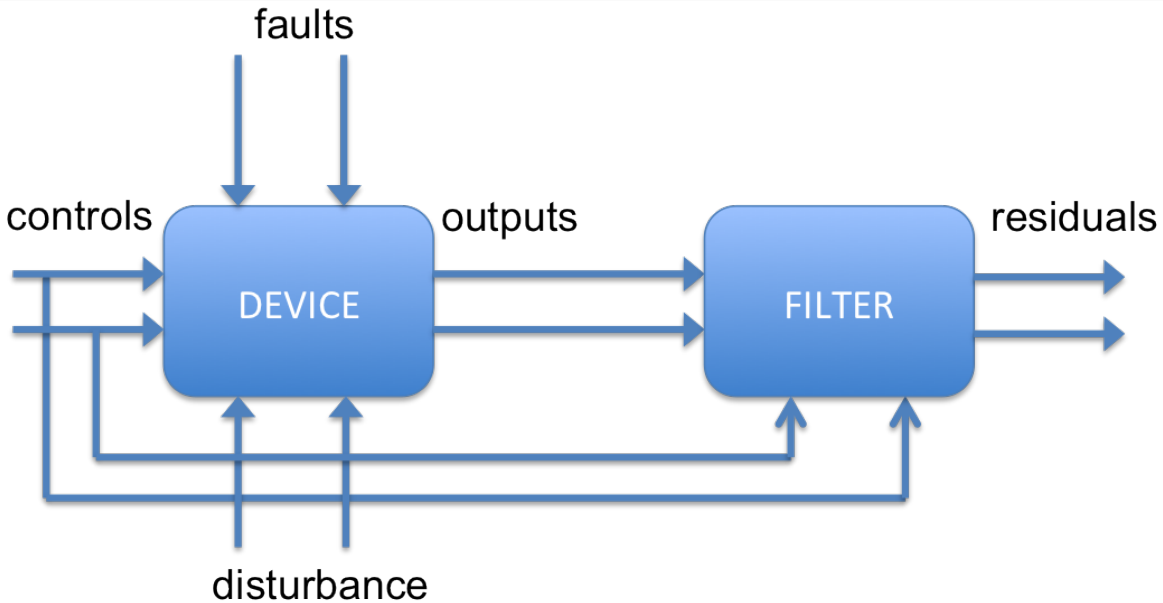
Solution of the FPRG

The process

$$\begin{aligned} \dot{z}_1 &= f_1(z_1, y_2) + g_1(z_1, y_2)u + \ell_1(z)m \\ &\dots \\ y_1 &= h_1(z_1), \quad y_2 = z_2 \end{aligned}$$

The diagnostic filter

$$\begin{aligned} \dot{\xi} &= \varphi(\xi, u, y) &&= f_1(\xi, y_2) + g_1(\xi, y_2)u + G(y_1 - h_1(\xi)) \\ r &= \psi(\xi, y) &&= y_1 - h_1(\xi) \end{aligned}$$



Cyber-attacks

The Washington Post

Posted at 12:44 PM ET, 11/18/2011

Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says

By Ellen Nakashima

Foreign hackers caused a pump at an Illinois water plant to fail last week, according to a preliminary state report. Experts said the cyber-attack, if confirmed, would be the first known to have damaged one of the systems that supply Americans with water, electricity and other essentials of modern life.

A hacker succeeded in breaking in the control system of a pumping station turning one of the pumps on and off frequently until it burned out

Cyber-attacks

- *Networked Control Systems* (NCS) are used to control large scale infrastructures (electric networks, gas and water distribution systems)
- The use of the network exposes the control system to possible external attacks
- Examples of these attacks include the so-called "deception attacks" in which the sensors measurements and the control actions are manipulated (for example with the addition of spurious signals) to compromise the functioning of the whole infrastructure

Hydraulic networks

Hydraulic networks consist of the interconnection of four kinds of components (pumps, valves, tanks and pipes)

There exist mathematical models to describe them

$$\begin{aligned} \dot{s} &= Dq \\ \dot{q} &= \varphi(D^T q) + Bu \\ y &= h(q) \end{aligned}$$

where

- s level in the tank, q flow in the pipes
- y measured pressure, u actuator pressure
- φ constitutive relation of the components
- D incidence matrix (network topology)
- B pumps location matrix in the network

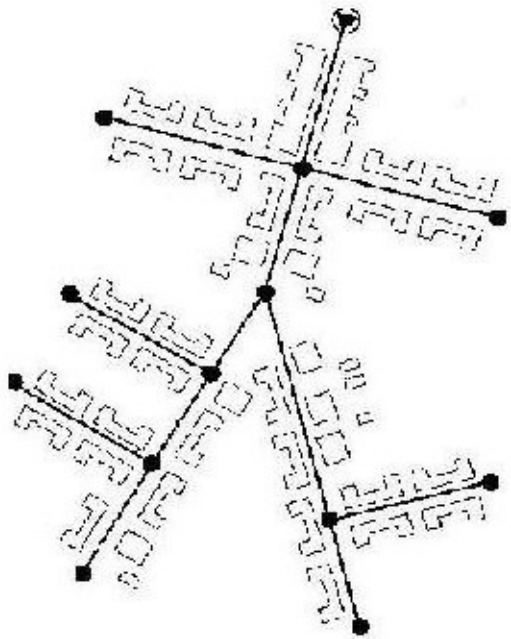


Figure: L. Fabrizi. Water supply in small communities.

DP-KALLESØE. Pressure regulation in nonlinear hydraulic networks. *IEEE-TCST*, 19(6) (2011), 1371–1383

Attacks on hydraulic networks

Many type of attacks on the network can be included in the model

$$\begin{aligned} \dot{s} &= Dq + \overbrace{m_s}^{offtake} \\ \dot{q} &= \varphi(D^T q) + B(u + \overbrace{m_u}^{actuator\ attack}) + \overbrace{m_q}^{offtake} \\ y &= h(q) + \overbrace{m_y}^{sensor\ attacks} \end{aligned}$$

The geometric methods constitute a very powerful tool for the detection of cybernetic attacks.

Limitations

- The geometric methods lead to centralized filters
- The attacks are carried out by intelligent entities that may know the device they are attacking and the possible attack detectors

Conclusions

- Geometric approach to fault detection for nonlinear systems
- Complete characterization of the solution
- Large impact on many engineering fields
- Cyber-security of Networked Control Systems