GEOMETRIC AND HIERARCHICAL FDI
FOR THE IFATIS TWO-TANK PILOT PLANT

Raffaella Mattone and Alessandro De Luca

Dipartimento di Informatica e Sistemistica
Università di Roma "La Sapienza", Italy
E-mail: {mattone,deluca}@dis.uniroma1.it

Abstract: In the control of complex dynamic plants, fault detection and isolation (FDI) is a prerequisite for a fault tolerant control architecture. In order to increase the reliability and robustness of the fault diagnosis, it is fundamental that the FDI system is given a hierarchical structure, reflecting, as far as possible, the natural decomposition of the plant into physical and/or logical subsystems. Through the use of the *IFATIS* two-tank benchmark, we illustrate the design and implementation of a hierarchical system for the detection and isolation of non-concurrent faults of sensors and actuators, based on the processing of suitably selected residuals, designed with geometric techniques. The FDI performance is demonstrated by realistic simulations performed on the identified model of the real system, including actual levels of input and measurement noise.

Keywords: Fault detection, fault isolation, hierarchical systems, nonlinear systems.

1. INTRODUCTION

In the control of complex dynamic plants, the problem of automatically detecting the occurrence of a faulty behavior in one or more of the hardware components is crucial for a reliable continuous operation. In fact, fault detection and isolation (FDI) is a prerequisite for a fault tolerant control architecture: when the system supervisor has recognized the type and location of a fault, it can activate a reconfiguration of the sensing, actuating, communication, and control devices so as to minimize performance degradation or even recover full operation.

An FDI system is typically a dynamic system where each output signal (residual) is excited in response to the occurrence of a different fault, as a result of the processing of nominal commanded inputs and measured outputs of the monitored plant. The set of available sensors and actuators may be fixed, or be a sub-product of the control and FDI design, whenever the integrated design of the overall system is allowed. A natural requirement for the FDI system is that it is able to diagnose the failure of any hardware device used to control the system and/or detect and isolate a fault, at least under the assumption of non-concurrency of faults. Whenever a model of the nominal (faultless) plant is available, the residual generation naturally relies on the knowledge of the static and/or dynamic equations governing the system. A relevant example in the class of model-based FDI methods is constituted by the geometric techniques introduced in (De Persis and Isidori, 2001) and recently developed and extended in (Mattone and De Luca, 2003 and 2004), that are applicable to a wide class of nonlinear systems affine in the (control and fault) inputs.

The reliability of the designed FDI system (and thus, of the whole fault-tolerant control system) depends on the accuracy of the available model and on the quality of the used hardware equipment (sensors and actuators). In order to increase the overall reliability and robustness of fault diagnosis (e.g., by limiting the propagation effects of false/missed FDI alerts), but also to optimize the distribution of the computational load and improve the modularity and reusability of the code, it is fundamental that the FDI module is given a hierarchical structure, reflecting, as far as possible, the natural decomposition of the control system into physical or logical subsystems (Bonivento *et al.*, 2004). Most FDI techniques, including geometric methods, do not allow the automatic inclusion of such "structural" requirements in the design, so that the obtained residual generators must be reorganized "by hand", in order to fit a particular system architecture. On the other hand, geometric techniques provide analysis tools that may support the selection of suitable subsets of residuals within the set of all independent diagnostic signals that can be generated for the considered system. Thus, the desired architecture can be established for the final FDI system, before the actual design of residuals.

Through the use of a simple case study (a two-tank pilot plant used as benchmark in the *IFATIS* project, see Sect. 2), we illustrate in this paper the design and implementation of a geometric, hierarchical system for the detection and isolation of non-concurrent faults of sensors and actuators (Sects. 3-4). In particular, we show how the needed set of measurements follows from the requirements on the control and FDI systems. The performance of the designed FDI system is demonstrated in Sect. 5 by realistic simulations for an identified model of the real plant, including the actual levels of input and measurement noise.

2. THE IFATIS TWO-TANK PILOT PLANT

We consider hereafter the system schematized in Fig. 1, corresponding to a real pilot plant used as benchmark in the EU Project *IFATIS*. It is constituted by two tanks, with fluid levels L_1 and L_2, connected by a controlled interconnection valve. The control inputs are the flows Q_1 and Q_2, fed by hydraulic pumps driven by tensions V_1 and V_2, and the (inverse of the) throttling R_{12} of the interconnection valve, driven by the input tension V_{12}. The controlled outputs are the sum and ratio of the tank output flows Q_{F1} and Q_{F2}, directly related to L_1 and L_2 through the nonlinear characteristics of the output valves. The evolution of the state variables L_1 and L_2 is modelled by

$$S_1\dot{L}_1 = Q_1 - Q_{12} - Q_{F1}, \qquad (1)$$

$$S_2\dot{L}_2 = Q_2 + Q_{12} - Q_{F2}, \qquad (2)$$

where the known nonlinear mappings

$$Q_1 = \pi_1(V_1), \quad Q_2 = \pi_2(V_2), \qquad (3)$$

$$Q_{F1} = \varphi_1(L_1), \quad Q_{F2} = \varphi_2(L_2), \qquad (4)$$

and

$$Q_{12} = \frac{1}{R_{12}(V_{12})}\cdot\varphi_{12}(|L_1 - L_2|)\cdot \mathrm{sign}(L_1 - L_2), \qquad (5)$$

describe the identified characteristics of the pumps and valves as a function of the corresponding input voltages and fluid levels, and S_1, S_2 are the sections of Tank 1 and Tank 2, respectively (see Hamelin *et al.* (2004) for details). For this system, measures of the two tank levels L_1 and L_2, and of the flows Q_{F1}, Q_{F2} and Q_{12} are available. The effects of all disturbances and model mismatches have been modelled as additive noise on the measured outputs, that resulted to be described by zero mean normal distributions with standard deviations $s_{L1} = s_{L2} = 0.015$, $s_{QF1} = s_{QF2} = 0.034$, and $s_{Q12} = 0.037$.

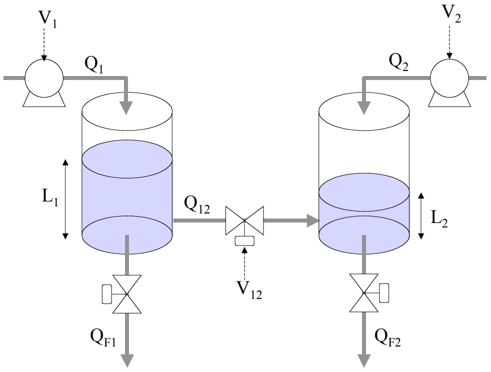

Fig. 1. The 2-tank pilot plant.

3. DESIGN OF THE FDI SYSTEM

The fault diagnosis system for the considered plant is based on the following requirements and realistic assumptions:

1. The FDI system must be able to operate in any dynamic situation, i.e., at steady state as well as during the control transient.
2. No special time profile for the fault quantities is assumed.
3. Any hardware device used to control the system and/or detect and isolate a fault, may fail itself.
4. The probability of concurrent failure of different hardware devices is negligible.
5. The structure of the FDI system should reflect as close as possible the natural decomposition of the controlled plant into the local subsystems constituted by the two tanks, each characterized by the local quantities Q_i, L_i,

Q_{Fi}, $i = 1,2$, and having in common just the input R_{12} and the measurement Q_{12}.

As a first step in the design of the FDI system, we just consider the hardware devices that are used for controlling the system, i.e., the two pumps providing Q_1 and Q_2, the interconnection valve with throttling R_{12}, and the two sensors for levels L_1 and L_2. According to requirement 3, all considered devices might be affected by faults. We define then the following fault quantities:

$$f_{Q1} = Q_{1a} - Q_{1c}, \qquad f_{Q2} = Q_{2a} - Q_{2c},$$
$$f_{R12} = \frac{1}{R_{12a}} - \frac{1}{R_{12c}}, \tag{6}$$
$$f_{L1} = L_{1a} - L_{1m}, \qquad f_{L2} = L_{2a} - L_{2m},$$

where subscripts 'a', 'c' and 'm' stay for *actual*, *commanded*, and *measured*, respectively.

From the geometric approach of Mattone and De Luca (2003) it follows that, with the chosen set of measures, a maximum number of three independent residual generators can be designed for the considered system affected by the faults in (6). The resulting *residual matrix*[1] is given in Table 1. A possible set of such residual generators is reported below[2], where only available values (i.e., *commanded* or *measured*) are used (subscripts are omitted):

$$\begin{aligned}\dot{\xi}_1 &= \frac{1}{S}\pi_1(V_1) - \frac{1}{S}\frac{\varphi_{12}(|L_1 - L_2|)}{R_{12}(V_{12})}\cdot \mathrm{sign}(L_1 - L_2)\\ &\quad - \frac{1}{S}\varphi_1(L_1) + K_1(L_1 - \xi_1)\\ r_1 &= L_1 - \xi_1,\end{aligned} \tag{7}$$

$$\begin{aligned}\dot{\xi}_2 &= \frac{1}{S}\pi_2(V_2) + \frac{1}{S}\frac{\varphi_{12}(|L_1 - L_2|)}{R_{12}(V_{12})}\cdot \mathrm{sign}(L_1 - L_2)\\ &\quad - \frac{1}{S}\varphi_2(L_2) + K_2(L_2 - \xi_2)\\ r_2 &= L_2 - \xi_2,\end{aligned} \tag{8}$$

$$\begin{aligned}\dot{\xi}_3 &= \frac{1}{S}\pi_1(V_1) + \frac{1}{S}\pi_2(V_2) - \frac{1}{S}\varphi_1(L_1)\\ &\quad - \frac{1}{S}\varphi_2(L_2) + K_3(L_1 + L_2 - \xi_3)\\ r_3 &= L_1 + L_2 - \xi_3,\end{aligned} \tag{9}$$

with $K_i > 0$, $i = 1,\ldots,3$. It can be readily verified that the residual generators in eqs. (7-9) are nonlinear observers for the dynamics of the variables L_1, L_2 and $L_1 + L_2$, respectively, and that, in the absence of faults, the dynamics of the residuals satisfies

$$\dot{r}_i = -K_i r_i, \quad i = 1,\ldots,3.$$

By looking at the residual matrix in Table 1, one realizes that the three designed residual generators are not sufficient to isolate all potential faults affecting the system. In particular, it is not possible to discriminate between the failures f_{L1} and f_{L2} of the two level sensors, since they affect the same set of residuals (the corresponding rows of the residual matrix are equal).

Table 1. Residual matrix relating faults $f_{Q1},\ldots, f_{L2}$ of eq. (6) to the residuals $r_1,\ldots, r_3$ of eqs. (7-9)

Residual **Fault**	r_1	r_2	r_3
f_{Q1}	1	0	1
f_{Q2}	0	1	1
f_{R12}	1	1	0
f_{L1}	1	1	1
f_{L2}	1	1	1

In order to get further diagnostic signals, the available measures of flows Q_{F1} and Q_{F2} can be used. As a result, the following static residual generators can be also defined

$$r_4 = Q_{F1} - \varphi_1(L_1), \tag{10}$$

$$r_5 = Q_{F2} - \varphi_2(L_2). \tag{11}$$

Correspondingly, the two fault quantities

$$f_{QF1} = Q_{F1a} - Q_{F1m}, \quad f_{QF2} = Q_{F2a} - Q_{F2m}, \tag{12}$$

must be also considered, associated to the possible failure of the introduced flow sensors. It can be readily verified that, with the introduction of the two further residuals r_4 and r_5, all rows of the resulting residual matrix (corresponding to columns 1,3,5-7 of Table 2) are different, so that all considered faults may be detected and isolated by processing the residuals $r_1,\ldots,r_5$. However, in order to gain further freedom in the optimization of the FDI system, one can exploit also the information provided by the available sensor for flow Q_{12}. The following further diagnostic signal is introduced

[1] This matrix, whose entry (i, j) is '1' if the i-th fault affects the j-th residual, can be computed on the basis of the system and fault vector fields, before the actual design of residual generators.

[2] Input and output noise has not been considered in the design, but will be suitably taken into account in the logical processing of residuals.

$$r_6 = |Q_{12}| - \frac{\varphi_{12}(|L_1 - L_2|)}{R_{12}(V_{12})}, \qquad (13)$$

together with the fault quantity

$$f_{Q12} = Q_{12a} - Q_{12m}. \qquad (14)$$

Moreover, the measure of flow Q_{12} can be used in eqs. (7-8) instead of the model-based term (5), in order to get alternative definitions r_1' and r_2' of residuals r_1 and r_2. These are more convenient for the purpose of a hierarchical decomposition of the FDI system. In fact, in r_1' and r_2' no cross-dependence on the local level measurements L_1 and L_2 are present. At this stage, the residual matrix is given in Table 2.

Table 2. Residual matrix relating faults $f_{Q1},\dots,f_{Q12}$ to residuals $r_1,\dots,r_6$, r_1', r_2'

Residual **Fault**	r_1	r_1'	r_2	r_2'	r_3	r_4	r_5	r_6
f_{Q1}	1	1	0	0	1	0	0	0
f_{Q2}	0	0	1	1	1	0	0	0
f_{R12}	1	0	1	0	0	0	0	1
f_{L1}	1	1	1	0	1	1	0	1
f_{L2}	1	0	1	1	1	0	1	1
f_{QF1}	0	0	0	0	0	1	0	0
f_{QF2}	0	0	0	0	0	0	1	0
f_{Q12}	0	1	0	1	0	0	0	1

Clearly, not all residuals in Table 2 have to be implemented. In particular, the selected columns of the residual matrix must have all different rows (to allow fault isolation under the assumption of non-concurrency) and, possibly after reordering rows and columns, must exhibit a block-diagonal structure (in order to recover the desired modular and hierarchical architecture for the FDI system). It is readily verified that these requirements are fulfilled by the set of residuals $\{r_1', r_4, r_6, r_2', r_5\}$, as in Table 3. As a consequence of this structure, the designed FDI system has the modular and hierarchical structure shown in Fig. 2, with the eight outputs one-to-one corresponding to the faults listed in Table 3. The two local FDI modules are in charge of computing the residuals that are only affected by local quantities, respectively r_1', r_4 for *Local FDI 1* (tank 1) and r_2', r_5 for *Local FDI 2* (tank 2). Residual r_6 has to be computed by a centralized *FDI Manager*, since it requires the availability also of common quantities. The FDI modules in Fig. 2 contain also the *isolation logics*, which is a combinatorial mapping of each feasible set of affected and unaffected residuals into a single isolated fault. In particular, the evaluation of local residuals allow the isolation of local faults of the tank level and output-flow sensors, while the discrimination of faults of the input pumps or of the interconnection valve needs the further evaluation of residual r_6 and thus the intervention of the FDI Manager.

Table 3. Residual matrix/isolation logics relating faults $f_{Q1},\dots,f_{QF2}$ to residuals r_1', r_4, r_6, r_2', r_5. The block-diagonal structure has been evidenced

Residual **Fault**	r_1'	r_4	r_6	r_2'	r_5
f_{Q1}	1	0	0	0	0
f_{L1}	1	1	1	0	0
f_{QF1}	0	1	0	0	0
f_{R12}	0	0	1	0	0
f_{Q12}	1	0	1	1	0
f_{Q2}	0	0	0	1	0
f_{L2}	0	0	1	1	1
f_{QF2}	0	0	0	0	1

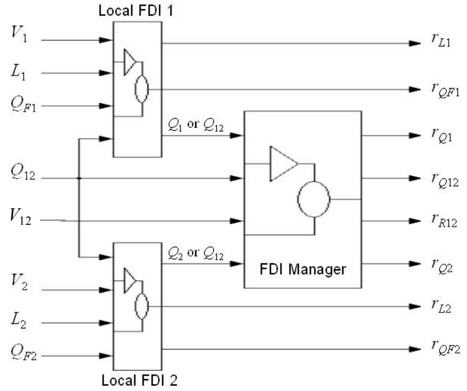

Fig. 2. Hierarchical structure of the designed FDI system.

4. IMPLEMENTATION DETAILS

The FDI system described in Sect. 3 has been implemented using Simulink. The used dynamic equations in the FDI system have been discretized by Euler method, with sampling time $T = 1$ s. In the dynamics of r_1' and r_2', observation gains $K_1 = K_2 = 0.1$ were found satisfactory. In order to deal with unmodelled input and measurement noise, the selected analogic residuals are processed by the following *dynamic thresholding* algorithm:

1. Each residual r in the columns of Table 3 is compared with a fixed threshold, defined from the observed amplitude of the residual in the absence of faults, resulting in a boolean residual *r_dig*. The chosen thresholds were, respectively, 0.04, 0.05, 0.04, 0.08 and 0.08.

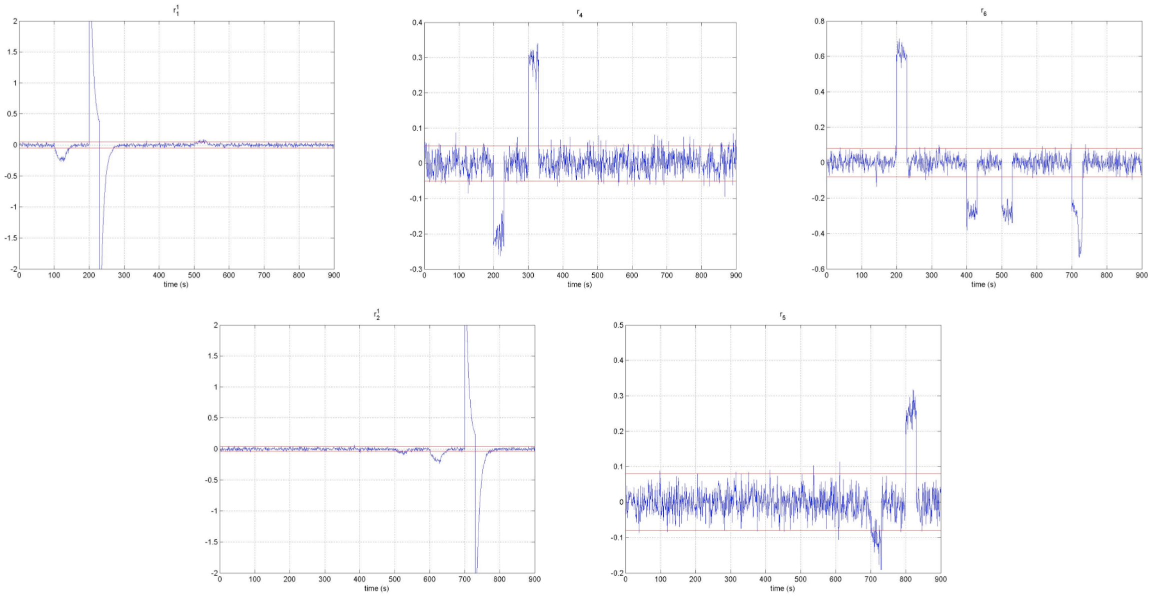

Fig. 3. Behaviour of residuals r_1', r_4, r_6 , r_2', r_5 (from top left to bottom right). Residual thresholds are also indicated.

2. Each residual *r_dig* is filtered to eliminate spurious '1' and '0', or oscillations between these two values. This is obtained by switching the residual value only after it has been stable on the new value for a fixed number of samples (respectively, corresponding to $T_{on} = 2$ s and $T_{off} = 5$ s). The resulting signal is *r_filt*.
3. The isolation logics is then evaluated on *r_filt*, providing the final boolean output vector *r_isol* = (r_{Q1},…,r_{QF2}). In order to deal with the different residual dynamics and avoid incorrect isolation during transients, the evaluation of the combinatorial mapping of Table 3 is enabled only after at least one of the *r_filt* components has been 'on' for $T_{detect} = 8$ s. For the same reason, *r_isol* is reset to zero only after vector *r_filt* has been 'off' for at least $T_{reset} = 2$ s. Isolation is considered unsuccessful if it has been enabled, but no component of *r_isol* has been set to '1'.

At the cost of a small delay in the diagnosis, this algorithm adds robustness to the FDI scheme.

5. SIMULATION RESULTS

The implemented FDI system has been tested on the identified model of the real plant given by Hamelin *et al.* (2004). The system was under open-loop control, being, in particular,

$$V_1 = 2.7\left(1 + 0.4 \sin 0.02\pi\, t\right), \qquad [\mathrm{V}]$$
$$V_2 = 1.4983\left(1 + 0.4 \sin 0.02\pi\, t\right), \qquad [\mathrm{V}]$$
$$V_{12} = 6. \qquad [\mathrm{V}]$$

The simulated scenario was a sequence of non-concurrent faults occurring in the same order used to list the faults in Table 3, at times $t_i = 100 \cdot i$ s, $i = 1,\ldots,8$. In all cases, the fault consists of a constant bias on the actuator input voltage or on the sensor output voltage, respectively, with a fault duration of 30 s. In particular, with obvious meaning of symbols, it has been set

bias_V1	= 0.5	[V]	(10% of available range)
bias_L1	= 3.16	[V]	(40% of available range)
bias_QF1	= 0.2922	[V]	(40% of available range)
bias_V12	= -6	[V]	(100% of available range)
bias_Q12	= 0.28	[V]	(15% of available range)
bias_V2	= 0.5	[V]	(10% of available range)
bias_L2	= 3.02	[V]	(40% of available range)
bias_QF2	= 0.249	[V]	(30% of available range)

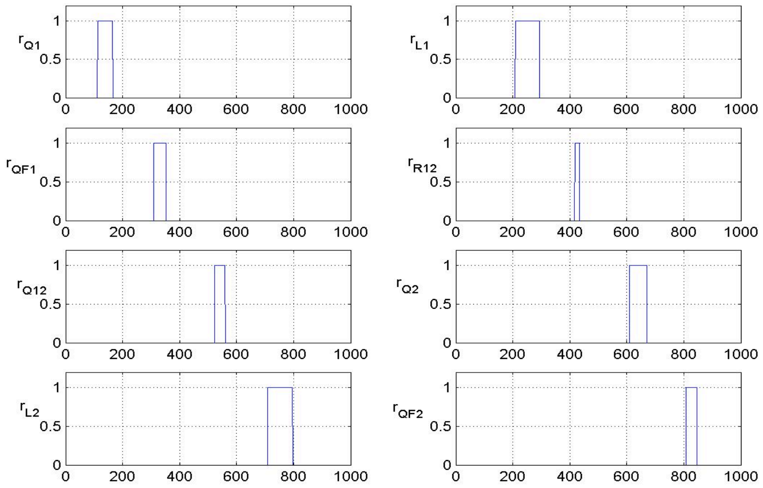

Fig. 4. Behaviour of residuals r_{Q1},…, r_{QF2} (from top left to bottom right).

The differences in the chosen fault severities depend on the different sensitivity of the FDI system to each fault. In particular, the biases were empirically chosen to be approximately twice the minimum values that can be detected and isolated with acceptable reliability. The only critical fault is that of the interconnection valve. In fact, the sensitivity to this actuator fault basically depends on the levels L_1 and L_2. We can only say that, with the given FDI design, the minimum detectable bias on the flow Q_{12} through the valve is 0.23 10^{-4} [m^3/s] (or 0.14 [V], expressed in the units of the flow sensor).

The behaviour of the relevant diagnostic signals during the described fault scenario is shown in Figs. 3-4. In particular, it can be observed in Fig. 3 that a set of multiple residuals is excited by the occurrence of each fault, in agreement with Table 3. In Fig. 4, the final boolean outputs of the FDI system show a correct fault isolation. The delays in the individuation of the fault intervals are due to the dynamic thresholding mechanism.

6. CONCLUSIONS

Through the use of a nonlinear case study (the *IFATIS* two-tank pilot plant), we have illustrated the design and implementation of a modular and hierarchical FDI system for the detection and isolation of actuator and sensor faults. Starting from the natural requirements and realistic assumptions for the diagnostic system, we have motivated the use of further sensors beside those strictly necessary for control purposes. Using geometric nonlinear techniques, a set of diagnostic signals has been designed, from which a suitable subset of residuals has been selected, satisfying the desired FDI architecture and functionality.

The performance of the designed FDI system has been demonstrated by numerical simulations performed on the identified model of the real plant, including actual levels of input and measurement noise.

7. ACKNOWLEDGEMENTS

This work was supported by the EU project EU-IST-2001-32122 *IFATIS.*

8. REFERENCES

Bonivento, C., M. Capiluppi, L. Marconi and A. Paoli (2004): An integrated design approach to multilevel Fault Tolerant Control of distributed systems. *16th IFAC World Congress.* Praha, CZ.

De Persis, C. and A. Isidori (2001): A geometric approach to nonlinear fault detection and isolation. *IEEE Trans. on Automatic Control.* **46**(6), 853-865.

Hamelin, F., H. Jamouli and D. Sauter (2004): The two tanks pilot plant. *IFATIS report IFAN014R01.*

Mattone, R. and A. De Luca (2003): Detection and isolation of sensor faults in nonlinear systems: A case study. *Workshop on Advanced Control and Diagnosis.* Duisburg, D. pp. 49-54.

Mattone, R. and A. De Luca (2004): Fault set detection and isolation for nonlinear systems. *Automatica.* Submitted for publication.