15th Triennial World Congress, Barcelona, Spain

A PROBABILISTIC APPROACH FOR FAULT DETECTION AND ISOLATION IN INDUSTRIAL SYSTEMS

A. Barigozzi, L. Magni, R. Scattolini [*,1]

[*] *Dipartimento di Informatica e Sistemistica, Università di Pavia, via F errata 1, 27100 Pavia, Italy*
e-mail: {lalo.magni, riccardo.sc attolini}@unipv.it
WEB: http://conpr o.unipv.it/lab/

Abstract: A method for fault detection in industrial systems is presented. Plant devices, sensors, actuators and diagnostic tests are described as stochastic Finite State Machines. A formal composition rule of these elementary models is given to obtain: (a) the set of admissible fault signatures, (b) their conditional probability given any fault event, (c) the conditional probability of a fault giv en a prescribed signature. The modularity and flexibility of this approach make it suitable to deal with complex systems made by a large number of elementary models.

Keywords: Fault detection, probabilistic models, automata

1. INTRODUCTION

In most cases, industrial diagnostic systems are built by combining a number of information coming from many different sources, suc h as empirical kno wledge,hardware redundancy tests, statistical inference, static and dynamic analytical relations based on mass and energy balance equations, qualitative modeling of the fault propagation flows. Each one of these approaches has been extensively studied in the literature and a number of algorithms and theoretical results are now ada ysavailable, see for example the books (Basseville and Nikiforov, 1993), (P atton *et al.*, 1989), (Gertler, 1998) and the references reported there for statistical and analytical approaches, and the papers (De V ries,1990), (Visnaw adham and Johnson, 1988), (Iri *et al.*, 1979), (Kokaw a *et al.*, 1983), (Koscielny, 1995), (Guan and Graham, 1994), (Kleer *et al.*, 1992) for methods based on the so-called fault tree analysis, on propagation digraphs and on Artificial Intelligence techniques. How ever, there is still the need of an approach allo wing to merge in a rigorous and easy way all these tec hniques and possessing enhanced modularit y and flexibility characteristics for the rapid analysis and prototyping of the diagnostic strategies.

In this paper, a new approach is presented to face these requirements. The diagnostic system is supposed to be composed b y apparatuses and tests. The apparatuses are plant devices, sensors, actuators, transmission lines, softw arecode and an y other material or immaterial element of the system under diagnosis which can be subject to faults. The tests are analytical and hardware redundancies, signal analysis algorithms, logical relations betw een variables and any other source of information on the presence of faults designed with whichever technique. Both apparatuses and tests are described as stochastic Finite State Machines (FSM) whose states represent the safe or fault behavior of apparatuses or the detection of normal and abnormal conditions by the tests. The transitions betw een states are probabilistic and

[1] The authors ackno wledge the partial financial support by *MURST* Project "New techniques for the identification and adaptive con trol of industrial systems"

forced by events, which describe the occurrence of faults or normal working conditions. Associated to apparatuses and tests there are also alarms, whose status (switched off/on) is deterministically defined by the current status of the FSM. By assigning the transition probabilities and the marginal probabilities of the safe and fault events, through simple composition rules it is possible to determine the feasible configurations of alarms (the signatures) given any event and their conditional probability. This is useful in the design of the diagnostic system to assess its capability to correctly identify and isolate the faults. Moreover, it represents a fundamental aid in the tuning of the thresholds used in the diagnostic tests to assess the presence of faults. Finally, with this approach, one can also determine the probability of a fault event given any fault signature during plant operations.

The use of FSM to describe the system under diagnosis has already been presented in the literature by (Sampath *et al.*, 1996), where a fault observer was derived using the information provided by the sequence of events registered in working conditions. With respect to that work, the approach proposed here, which represents an extension to the stochastic case of the method described in (Magni *et al.*, 2000), (Magni *et al.*, 2002), puts the emphasis on the modularity of the description of the overall system, besides introducing a probabilistic point of view, which is believed to be mandatory in many practical applications.

The technique here proposed has already been used in an industrial automotive application to study a diagnostic strategy for the isolation of the faults of the throttle body, the intake manifold, the accelerator and brake pedals, the combustion chamber and a number of sensors. On the whole, a diagnostic strategy with 20 tests has been analyzed for the isolation of 21 faults, see (Ravara, 1999) for the deterministic analysis and (Barigozzi, 2000) for its extension to the stochastic case. The achieved results are totally in agreement with those provided by a standard FMEA analysis, which however required much more effort for its development. Due to its complexity, this industrial case is not reported here, except for a smaller ad more tractable subproblem (two apparatuses, one test, four fault events, three outputs). This related problem of reduced size is used in the paper as a worked example to illustrate step by step the development of the diagnostic procedure and to highlight the potentialities of this approach.

2. MODELING DIAGNOSTIC SYSTEMS WITH STOCHASTIC AUTOMATA

2.1 *Models of apparatuses and tests*

A diagnostic system is composed by apparatuses A and diagnostic tests T. The apparatuses are physical devices, such as plant elements, sensors, actuators, as well as immaterial elements composing the overall plant and automation system, such as software code or control algorithms. The diagnostic tests T are used to detect and isolate the presence of faults, and can be simple operations such as signal comparisons, or more sophisticated algorithms, like those based on consistency relations, analytical redundancies, logical propositions, see (Gertler, 1998), (Patton *et al.*, 1989).

Both apparatuses A and tests T can be described by the Finite State Machine (FSM)

$$FSM = (X, Y, E, p, h)$$

where the set of states $X = \{x_1, .., x_{|X|}\}$ describes the normal or the failed behavior of the components and the symbol $|X|$ represents the cardinality of the set X; the outputs $Y = \{y_1, .., y_{|Y|}\}$ are the available alarms; the events $E = \{e_1, .., e_{|E|}\}$ represent the occurrence of faults and govern the transition between states. Moreover p is the state transition probability, i.e.

$$p(x_i; e_j) = p_{ij} = P(X = x_i \,|E = e_j\,)$$

where P is a discrete probability measure. Obviously

$$\sum_{i=1}^{|X|} p_{ij} = 1 \quad , \quad \forall j = 1, ..., |E|$$

Finally, $h : X \to Y$ is the deterministic output transformation, $y_k = h(x_i)$, so that the current state uniquely defines the status of the alarms.

In view of the previous assumptions, the FSM is fully described by the *Event/State* (ES) and the *Output transformation* O matrices. The rows of the matrix ES correspond to the events, its columns are associated to the states and its element $ES(i,j)$ is the probability p_{ji} that the event i forces a transition to the state j, so that $\sum_{j=1}^{|X|} ES(i,j) = 1, \quad \forall i = 1, ..., |E|$. As for the matrix O, its rows correspond to the alarms, while its columns are associated to the states, hence $O(i,j)$ is equal to one if the alarm y_i is switched on in state x_j and is zero otherwise.

Example 1. Consider a sensor, hereafter called "sensor 1" subject to electrical and functional faults, described by the events ef_{s1} and ff_{s1} respectively. The electrical fault corresponds to a short circuit or to an open circuit, while a functional fault can represent a bias or a long term drift. The sensor can then be described as an apparatus, those FSM has three events: the fault events ef_{s1}, ff_{s1} and the absence of faults, or safe conditions $s = \overline{ef_{s1}} \wedge \overline{ff}_{s1}$. Moreover three states are necessary to describe its status: the Safe state (S_{s1}), the Electrical Fault state (EF_{s1}) and the Functional Fault (FF_{s1}). In EF_{s1} the measured signal is permanently out of range and an electrical test can detect the status of the apparatus setting to one an output alarm y_{s1}, while in S_{s1} and FF_{s1} one has $y_{s1} = 0$. Obviously, once ef_{s1} (ff_{s1}) has occurred, the status of the sensor is likely to be EF_{s1} (FF_{s1}), but with a quite small probability these events can lead the apparatus to be in an unexpected state. For instance, a too small or large selection of the thresholds in the analysis of the measured signal can detect safe (S_{s1}) or electrical fault (EF_{s1}) conditions in the presence of a bias, that is of a functional fault. For these reasons, the sensor model can be described by the following *Event/State* (ES_{s1}) and *Output transformation* O_s matrices

$$ES_{s1} = \begin{array}{c|c|c|c|} & S_{s1} & EF_{s1} & FF_{s1} \\ \hline s & 1 & 0 & 0 \\ \hline ef_{s1} & 0.05 & 0.9 & 0.05 \\ \hline ff_{s1} & 0.1 & 0.1 & 0.8 \\ \hline \end{array}, \qquad (1)$$

$$O_{s1} = \begin{array}{c|c|c|c|} & S_{s1} & EF_{s1} & FF_{s1} \\ \hline y_{s1} & 0 & 1 & 0 \\ \hline \end{array}$$

The analysis of ES_{s1} shows that the "failed states" EF_{s1} and FF_{s1} cannot be reached in safe conditions; conversely, the occurrence of a fault event ef_{s1} or ff_{s1} can bring to an "incorrect" state. As for the output alarm, it is activated only when the apparatus is in the state EF_{s1}. Then, in this example it is not possible to have a false alarm, while a missed or wrong detection can happen. Moreover, note that the state FF_{s1} is not detected by the measure itself, but its identification and isolation calls for other diagnostic tests.

2.2 *Composition rules*

A formal composition rule of FSM models is now derived under the following assumption.

Assumption A1 (no simultaneous faults). The fault events can occur only one at a time and, once a fault event has occurred, the diagnostic procedure is completed before the arrival of a new fault event. This also implies the independency of the fault events. ■

Note also that each elementary FSM has a different set of outputs Y. This means that an alarm of an elementary FSM does not belong to the set of alarms of any other one. Moreover, the intersection of the event sets of two FSM describing the apparatuses contains only the safe event.

Given $FSM^1 = \left(X^1, Y^1, E^1, p^1, h^1\right)$ and $FSM^2 = \left(X^2, Y^2, E^2, p^2, h^2\right)$, their synchronous composition

$$FSM^{12} = \left(X^{12}, Y^{12}, E^{12}, p^{12}, h^{12}\right)$$

is obtained according to the following rules, which can be viewed as the extension to the stochastic case of the synchronous composition rules of deterministic automata described in (Cassandras *et al.*, 1995).

- $$X^{12} = X^1 \times X^2$$
- $$Y^{12} = \left\{y_1^1, .., y^1_{|Y^1|}, y_1^2, .., y^2_{|Y^2|}\right\}$$
- $$E^{12} = E^1 \cup E^2$$
- $$\begin{aligned} p^{12}: \quad & p((x_i^1 \times x_j^2); e_k) = p_{ijk} \\ &= \begin{cases} P(x_i^1|e_k) \cdot P(x_j^2|e_k) & if\ e_k \in \left(E^1 \cap E^2\right) \\ P(x_i^1|e_k) \cdot P(x_j^2|s) & if\ (e_k \in E^1) \wedge (e_k \notin E^2) \\ P(x_i^1|s) \cdot P(x_j^2|e_k) & if\ (e_k \notin E^1) \wedge (e_k \in E^2) \end{cases} \end{aligned} \qquad (2)$$

  where s is the safe event
- $$h^{12}(x_i^1 \times x_j^2) = \begin{bmatrix} h^1(x_i^1) \\ h^2(x_j^2) \end{bmatrix}$$

In the composition of FSM models it can happen that some composite states $(x_i^1 \times x_j^2)$ are unreachable by any event, that is $p_{ijk} = 0$, $\forall k = 1, \ldots, \left|E^{12}\right|$; these states must be eliminated before proceeding in the composition of the overall model. It is easy to verify that, if $e_k \notin (E^1 \cap E^2)$ and $P(x_i|s) = 0$, $\forall x_i \neq S$, where S is the safe state, the probability of any composite state $(x_i^1 \times x_j^2)$, with $x_i^1 \neq S$ and $x_j^2 \neq S$, given any event belonging to E^{12} is always zero and this composite state $(x_i^1 \times x_j^2)$ must be removed from X^{12}, so greatly reducing the dimension of the state space to be analyzed.

The algorithmic implementation of the composition rules above is the following: given the *Event/State* matrices ES_1 and ES_2, the *Event/State* matrix ES_{12} of the composite model has a number of rows equal to $\left|E^{12}\right|$ and a number of columns equal to $\left|X^{12}\right|$. The (i, j) term of ES_{12}

corresponding to the event e_i and to the state $x_j^{12} = (x_k^1 \times x_h^2)$ is obtained as: (i) the product of the term associated with e_i and x_k^1 in ES_1 and the term associated with e_i and x_h^2 in ES_2 when $e_i \in (E^1 \cap E^2)$; (ii) the product of the term associated with e_i and x_k^1 in ES_1 and the term corresponding to s and x_h^2 in ES_2 when $(e_i \in E^1) \wedge (e_i \notin E^2)$; (iii) the product of the term associated with s and x_k^1 in ES_1 and the term corresponding to e_i and x_h^2 in ES_2 when $(e_i \notin E^1) \wedge (e_i \in E^2)$. The null columns of ES_{12} must be removed, as they represent unreachable states. Moreover, given the Output trasformation matrices O_{s1} and O_{s2}, the Output trasformation matrix O_{s12} of the composite model has a number of rows equal to $|Y^{12}|$ and a number of columns equal to $|X^{12}|$. The (i,j) term of O_{s12} corresponding to the output y_i and to the state $x_j^{12} = (x_k^1 \times x_h^2)$ is equal to the term associated with y_i and x_k^1 in O_{s1} or x_h^2 in O_{s2}. Note that y_i belongs only to Y^1 or Y^2.

By repeatedly applying the previous composition rules, one finally obtains an overall global Finite State Machine model FSM_g, with state space X^g, output space Y^g and event space E^g, whose Event/State matrix ES_g has $|E^g|$ rows, corresponding to the overall number of possible events, and $|X^g|$ columns corresponding to all the obtained composite states. The element $ES_g(i,j)$ is the probability that the system is in the $j-th$ composite state given the $i-th$ event.

Associated with FSM_g there is also the output transformation matrix O_g with $|Y^g|$ rows, corresponding to the outputs of the collected submodels, and with $|X^g|$ columns. The element $O_g(i,j)$ is one if one of the states activating the alarm y_i belongs to the composite state corresponding to column j, and is zero otherwise. The columns of O_g are the signatures corresponding to the admissible states and coincide with the configurations of alarms allowed by the adopted diagnostic strategy. Note however that two or more columns of O_g can coincide since different composite states can lead to the same configuration of alarms.

Example 2. Consider a simple system composed by two sensor and an hardware redundancy test. The FSM model of the first sensor has been described in Example 1. Then, it has three states (S_{s1}, EF_{s1}, FF_{s1}), three events (s, ef_{s1}, ff_{s1}), one alarm (y_{s1}), an Event/State matrix (ES_{s1}) and an output transformation matrix (O_{s1}) given in (1). The second sensor has also three events (s, ef_{s2}, ff_{s2}) but only two states, the safe state (S_{s2}) and the fault state (F_{s2}). A local test (y_{s2}) can detect the status. Then,

$$ES_{s2} = \begin{array}{c} \\ ef_{s2} \\ ff_{s2} \\ s \end{array} \begin{array}{cc} S_{s2} & F_{s2} \\ \hline \multicolumn{1}{|c|}{0.1} & \multicolumn{1}{c|}{0.9} \\ \hline \multicolumn{1}{|c|}{0.2} & \multicolumn{1}{c|}{0.8} \\ \hline \multicolumn{1}{|c|}{1} & \multicolumn{1}{c|}{0} \\ \hline \end{array},$$

$$O_{s2} = y_{s2} \begin{array}{cc} S_{s2} & F_{s2} \\ \hline \multicolumn{1}{|c|}{0} & \multicolumn{1}{c|}{1} \\ \hline \end{array}$$

As for the hardware redundancy test, it has two states, the "safe" state S_{t1} when no discrepancies are detected between the measures provided by the sensors and a fault state F_{t1} when these measurements are different beyond a prescribed threshold. The ES and O matrices of the test are

$$ES_{t1} = \begin{array}{c} \\ s \\ ff_{s1} \\ ff_{s2} \\ ef_{s1} \\ ef_{s2} \end{array} \begin{array}{cc} S_{t1} & F_{t1} \\ \hline \multicolumn{1}{|c|}{1} & \multicolumn{1}{c|}{0} \\ \hline \multicolumn{1}{|c|}{0.1} & \multicolumn{1}{c|}{0.9} \\ \hline \multicolumn{1}{|c|}{0.1} & \multicolumn{1}{c|}{0.9} \\ \hline \multicolumn{1}{|c|}{0} & \multicolumn{1}{c|}{1} \\ \hline \multicolumn{1}{|c|}{0} & \multicolumn{1}{c|}{1} \\ \hline \end{array},$$

$$O_{t1} = y_{t1} \begin{array}{cc} S_{t1} & F_{t1} \\ \hline \multicolumn{1}{|c|}{0} & \multicolumn{1}{c|}{1} \\ \hline \end{array}$$

By applying the composition rules previously introduced, one can compute the overall Event/State matrix ES_g

	S	F_1	F_2	F_3	F_4	F_5	F_6	F_7
ef_{s1}	0	0.05	0	0	0	0.9	0	0.05
ef_{s2}	0	0.1	0	0.9	0	0	0	0
ff_{s1}	0.01	0.09	0	0	0.01	0.09	0.08	0.72
ff_{s2}	0.02	0.18	0.08	0.72	0	0	0	0
s	1	0	0	0	0	0	0	0

where the composite states are defined as follows

$$\begin{array}{rlcrl} S = & S_{s1}S_{s2}S_{t1} & , & F_4 = & EF_{s1}S_{s2}S_{t1} \\ F_1 = & S_{s1}S_{s2}F_{t1} & , & F_5 = & EF_{s1}S_{s2}F_{t1} \\ F_2 = & S_{s1}F_{s2}S_{t1} & , & F_6 = & FF_{s1}S_{s2}S_{t1} \\ F_3 = & S_{s1}F_{s2}F_{t1} & , & F_7 = & FF_{s1}S_{s2}F_{t1} \end{array} \quad (3)$$

Correspondingly, the output transformation matrix O_g is

	S	F_1	F_2	F_3	F_4	F_5	F_6	F_7
y_{s1}	0	0	0	0	1	1	0	0
y_{s2}	0	0	1	1	0	0	0	0
y_{t1}	0	1	0	1	0	1	0	1

(4)

Note, for example, that since the alarm y_{s2} is active in the state F_{s2}, the second row of O_g has the two elements equal to 1 in the columns corresponding to F_2 and F_3, as defined in (3), which are the only two composite states incorporating F_{s2}.

The columns of O_g define the set $\Sigma_g = \{\sigma_1, \sigma_2, ..., \sigma_{|\Sigma_g|}\}$ of the signatures allowed. By using the information stored in the matrices ES_g and O_g, it is then easy to build the matrix PSE with $|\Sigma_g|$ rows and $|E^g|$ columns whose element (i,j) is the conditional probability of the signature σ_i given the event e_j. To determine its value, it suffices to select from O_g the composite states producing the configuration of alarms corresponding to σ_i and to add the conditional probabilities of these states given e_j derived from ES_g. The information provided by PSE is useful in the project of the diagnostic strategy to assess its capability to discriminate between different fault events.

Example 3. (2 Continued) The set Σ_g is composed by the following signatures

	y_{s1}	y_{s2}	y_{t1}
σ_1	0	0	0
σ_2	0	0	1
σ_3	0	1	0
σ_4	0	1	1
σ_5	1	0	0
σ_6	1	0	1

where, for example, σ_1 is the signature corresponding to the states S and F_6. By recalling (2), (4), one can compute the matrix PSE

	s	ef_{s1}	ef_{s2}	ff_{s1}	ff_{s2}
σ_1	1	0	0	0.09	0.02
σ_6	0	0.9	0	0.09	0
σ_4	0	0	0.9	0	0.72
σ_2	0	0.1	0.1	0.81	0.18
σ_3	0	0	0	0	0.08
σ_5	0	0	0	0.01	0

(5)

Note, for example, that the element $PSE(1,4)$ is simply obtained as $ES_g(3,1) + ES_g(3,7)$, and analogous computations lead to the definition of all the other elements. From PSE it is apparent that the signature σ_4 is the most probable both for ef_{s2} and ff_{s2}. This is due to the particular structure of the local alarm of the second sensor which cannot discriminate between ef_{s2} and ff_{s2}. Moreover the diagnostic isolation of the fault ff_{s2} is particularly critical also because it could generate the signature expected for ff_{s1} with an unnegligeable probability 0.18. In particular situations, this should lead to re-examination of the adopted diagnostic strategy.

Finally, by means of the Bayes Theorem, given the marginal probabilities of the events $P(e_i)$, $i = 1, ..., |E^g|$, from the matrix PSE it is possible to compute the matrix PES with the same dimensions of PSE and whose element (i,j) is the probability of the event e_j given the signature σ_i. In real time operations, this information is useful to estimate the most likely fault when a signature occurs, that is when at least one alarm is equal to 1.

Example 4. (3 Continued) Assuming the (unrealistic) hypothesis that all the events have the same marginal probability $\bar{P}$ ($\bar{P} = 0.2$), from matrix (5) one obtains the matrix PES

	s	ef_{s1}	ef_{s2}	ff_{s1}	ff_{s2}
σ_1	0.9009	0	0	0.0811	0.0180
σ_6	0	0.9091	0	0.0909	0
σ_4	0	0	0.5556	0	0.4444
σ_2	0	0.0840	0.0840	0.6807	0.1513
σ_3	0	0	0	0	1
σ_5	0	0	0	1	0

This matrix shows that the most critical situation, as it was observed also from (5), coincides with the case when signature σ_4 occurs. Also signature σ_2 appears to be critical, in fact this configuration of alarms could hide the presence of anyone of the admissible faults, although with a quite small probability for some of them. With a more realistic assumption on the marginal probabilities (i.e. $\bar{P}(s) = 0.95$, $\bar{P}(ef_{s1}) = \bar{P}(ef_{s2}) = 0.005$, $\bar{P}(ff_{s1}) = \bar{P}(ff_{s2}) = 0.02$) the following matrix PES is obtained

	s	ef_{s1}	ef_{s2}	ff_{s1}	ff_{s2}
σ_1	0.9977	0	0	0.0019	0.0004
σ_6	0	0.7143	0	0.2857	0
σ_4	0	0	0.2381	0	0.7619
σ_2	0	0.0240	0.0240	0.7788	0.1731
σ_3	0	0	0	0	1
σ_5	0	0	0	1	0

It is apparent that if, for example, σ_4 occurs, the most probable fault is now ff_{s2} instead of ef_{s2}.

3. CONCLUSIONS

In view of its characteristics of flexibility and modularity, the method here proposed is particularly useful in all the cases where the diagnostic strategy has to be frequently re-designed for the rapid evolution of the system, such as in the automotive industry. A wide library of re-usable models can be easily developed and updated. As a potential drawback of the approach here proposed, it must be noted that the definition of the transition probabilities used to describe the FSM models can be quite difficult and requires an extensive collection of data. However, it is believed that a probabilistic approach is mandatory in the field of fault detection to fully consider the elusive nature of most real life problems. It has also to be strassed that the proposed approach naturally gives the possibility to follow a top-down design approach. It has also to be remarked that the integration of the proposed method with the control system specification, design and simulation is natural in the context of hybrid systems, where the plant is described by a continuous time model, while the occurrence of faults is represented by asynchronous events modifying the system structure.

4. REFERENCES

Barigozzi, A. (2000). Approccio stocastico alla diagnostica industriale: definizione ed applicazione al controllo delle emissioni inquinanti di un motore a combustione interna. Technical report. University of Pavia (Italy). Thesis (in Italian), R. Scattolini, L. Magni and C. Siviero supervisors.

Basseville, M. and I. V. Nikiforov (1993). *Detection of Abrupt Changes: Theory and Application*. Prentice-Hall.

Cassandras, C. G., S. Lafortune and G. J. Olsder (1995). Introduction to the modelling, control and optimization of discrete event systems. In: *Trends in Control: A European Perspective* (A. Isidori, Ed.). pp. 217–292. Springer.

De Vries, R. (1990). An automated methodology for generating a fault tree. *IEEE Trans. Reliability* **39**, 79–86.

Gertler, J. J. (1998). *Fault Detection and Diagnosis in Engineering Systems*. Marcel Dekker, New York.

Guan, J. and J. H. Graham (1994). Diagnostic reasoning with fault propagation digraph and sequential testing. *IEEE Trans. on Systems, Man and Cybernetics* **24**, 1552–1558.

Iri, M., K. Aoki, E. OShima and H. Matsuyama (1979). An algorithm for diagnosis of system failures in the chemical process. *Computers Chemical Engineering* **3**, 489.

Kleer, J. De, A. K. Mackworth and R. Reiter (1992). Characterizing diagnoses and systems. *Artificial Intelligence* **56**, 197–222.

Kokawa, M., S. Miyazaki and S. Shingai (1983). Fault location using digraph and inverse direction search with application. *Automatica* **19**, 729–735.

Koscielny, J. M. (1995). Fault isolation in industrial processes by the dynamic table of states method. *Automatica* **31**, 747–753.

Magni, L., R. Scattolini and C. Rossi (2000). A fault detection and isolation method for complex industrial systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part A* **30**, 860–865.

Magni, L., R. Scattolini and C. Rossi (2002). A design methodology of diagnostic strategies for industrial systems. *International Journal of Systems Science*.

Patton, R. J., P. M. Frank and R. N. Clark (1989). *Fault Diagnosis in Dynamic Systems: Theory and Applications*. Prentice-Hall. Englewood Cliffs, NJ.

Ravara, M. (1999). Metodo di diagnostica industriale basato sugli automi astati finiti: Definizione e applicazione ad un motore a combustione interna. Technical report. University of Pavia (Italy). Thesis (in Italian), R. Scattolini and C. Rossi supervisors.

Sampath, M., R. Sengupta, S. Lafortune, K. Sinnamohideen and D. Teneketzis (1996). Failure diagnosis using discrete event models. *IEEE Transactions on Control System Technology* **4**, 105–124.

Visnawadham, N. and T. L. Johnson (1988). Fault detection and diagnosis of automated manifacturing systems. Proc. 27th Conf. Decision Contr.. Austin, TX. pp. 2301–2306.