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 Ferrata 1, 27100 Pavia, Italy
  e-mail: {lalo.magni, riccardo.scattolini}@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 given 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, such as empirical knowledge, 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 available; see for example the books (Basseville and Nikiforov, 1993), (Patton et al., 1989), (Gertler, 1998) and the references reported there for statistical and analytical approaches, and the papers (De Vries, 1990), (Visaladh and Johnson, 1988), (Iri et al., 1979), (Kockawa et al., 1983), (Koscielny, 1995), (Guan and Graham, 1994), (Kee et al., 1992) for methods based on the so-called fault tree analysis, on propagation digraphs and on Artificial Intelligence techniques. However, there is still the need of an approach allowing to merge in a rigorous and easy way all these techniques and possessing enhanced modularity 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 by apparatuses and tests. The apparatuses are plant devices, sensors, actuators, transmission lines, software and another 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 between 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 between states are probabilistic and

1 The authors acknowledge the partial financial support by MURST Project "New techniques for the identification and adaptive control 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., 1999), 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), (Parrot 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

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

Finally, $h: X \rightarrow Y$ 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

$$\sum_{i=1}^{|X|} ES(i, j) = 1 \quad \forall i = 1, ..., |E|.$$  

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 I" subject to electrical and functional faults, described by the events $e_{f_{x_1}}$ and $f_{x_1}$, 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, these FSM has three events: the fault events \( e_{f1_s} \), \( f f_{s1} \) and the absence of faults, or safe conditions \( s = e_{f1_s} \lor \neg f f_{s1} \). Moreover three states are necessary to describe its status: the Safe state \( S_{s1} \), the Electrical Fault state \( E F_{s1} \) and the Functional Fault \( F F_{s1} \). In \( E F_{s1} \), 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 \( F F_{s1} \) one has \( y_{s1} = 0 \). Obviously, once \( e_{f1_s} \) \( (f f_{s1}) \) has occurred, the status of the sensor is likely to be \( E F_{s1} \) \( ( F F_{s1} ) \), 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 \( ( E S_{s1} ) \) and Output transformation \( O_{s1} \) matrices

\[
ES_{s1} = \begin{bmatrix} S_{s1} & EF_{s1} & FF_{s1} \\ e_{f1_s} & 1 & 0 & 0 \\ f f_{s1} & 0.05 & 0.9 & 0.05 \\ 0.1 & 0.1 & 0.8 & 0.1 \end{bmatrix}
\]

\[
O_{s1} = y_{s1} \begin{bmatrix} S_{s1} & EF_{s1} & FF_{s1} \\ 0 & 1 & 0 \end{bmatrix}
\]

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 \( e_{f1_s} \) or \( f f_{s1} \) can bring to an “incorrect” state. As for the output alarm, it is activated only when the apparatus is in the state \( E F_{s1} \). 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 \( FSM_1 = (X^1, Y^1, E^1, p^1, h^1) \) and \( FSM_2 = (X^2, Y^2, E^2, p^2, h^2) \), their synchronous composition

\[
FSM^{12} = (X^{12}, Y^{12}, E^{12}, p^{12}, h^{12})
\]

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).

- \( X^{12} = X^1 \times X^2 \)
- \( Y^{12} = \{ y_1, \ldots, y_1^1, y_2, \ldots, y_2^2 \} \)
- \( E^{12} = E^1 \cup E^2 \)
- \( p^{12} : p((x^1_i, x^2_j); e_k) = p_{ijk} \)
  \[
  p = \begin{cases} 
  P(x^1_i | e_k) \cdot P(x^2_j | e_k) & if \ e_k \in (E^1 \cap E^2) \\
  P(x^1_i | e_k) \cdot P(x^2_j | e_k) & if \ (e_k \in E^1) \land (e_k \notin E^2) \\
  P(x^1_i | e_k) \cdot P(x^2_j | e_k) & if \ (e_k \notin E^1) \land (e_k \in E^2)
  \end{cases}
  \]

where \( s \) is the safe event

- \( h^{12}(x^1_i \times x^2_j) = \left[ \begin{array}{c} h^1(x^1_i) \\
  h^2(x^2_j) \end{array} \right] \]

In the composition of FSM models it can happen that some composite states \( (x^1_i \times x^2_j) \) are unreachable by any event, that is \( p_{ijk} = 0, \forall k = 1, \ldots, |E^{12}| \); 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 \( P(x_i | e_k) = 0, \forall i \notin S \), where \( S \) is the safe state, the probability of any composite state \( (x^1_i \times x^2_j) \), with \( x^1_i \notin S \) and \( x^2_j \notin S \), given any event belonging to \( E^{12} \) is always zero and this composite state \( (x^1_i \times x^2_j) \) 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 \( E S_{1} \) and \( E S_{2} \), the Event/State matrix \( E S_{12} \) of the composite model has a number of rows equal to \(|E^{12}|\) and a number of columns equal to \(|X^{12}|\). The \((i, j)\) term of \( E S_{12} \).
corresponding to the event \( e_i \) and to the state \( x^1_i = (x^1_i \times x^2_i) \) is obtained as: (i) the product of the term associated with \( e_i \) and \( x^1_i \) in \( E S_1 \) and the term associated with \( e_i \) and \( x^2_i \) in \( E S_2 \) when \( e_i \in (E^1 \cap E^2) \); (ii) the product of the term associated with \( e_i \) and \( x^1_i \) in \( E S_1 \) and the term corresponding to \( s \) and \( x^2_i \) in \( E S_2 \) when \( (e_i \in E^1) \land (e_i \notin E^2) \); (iii) the product of the term associated with \( s \) and \( x^1_i \) in \( E S_1 \) and the term corresponding to \( e_i \) and \( x^2_i \) in \( E S_2 \) when \((e_i \notin E^1) \land (e_i \in E^2) \). The null columns of \( E S_{12} \) must be removed, as they represent unreachable states. Moreover, given the Output transformation matrices \( O_{s1} \) and \( O_{s2} \), the Output transformation matrix \( O_{s12} \) of the composite model has a number of rows equal to \( \lvert Y^1 \rvert \) and a number of columns equal to \( \lvert X^{12} \rvert \). The \((i, j)\) term of \( O_{s12} \) corresponding to the output \( y_i \) and to the state \( x^1_j = (x^1_i \times x^2_i) \) is equal to the term associated with \( y_i \) and \( x^1_j \) in \( O_{s1} \) or \( x^2_j \) 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 \( E S_g \) has \( \lvert E^g \rvert \) rows, corresponding to the overall number of possible events, and \( \lvert X^g \rvert \) columns corresponding to all the obtained composite states. The element \( E S_g(i, j) \) 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 \( \lvert Y^g \rvert \) rows, corresponding to the outputs of the collected submodels, and with \( \lvert X^g \rvert \) 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 \((S_{a1}, EF_{a1}, FF_{a1})\), three events \((s, efa1, jfa1)\), one alarm \((ya1)\), an Event/State matrix \((ES_{a1})\) and an output transformation matrix \((O_{a1})\) given in (1). The second sensor has also three events \((s, efa2, jfa2)\) but only two states, the safe state \((S_{a2})\) and the fault state \((F_{a2})\). A local test \((ya2)\) can detect the status. Then,

\[
ES_{a2} = \begin{pmatrix}
S_{a2} & F_{a2} \\
\frac{ef_{a2}}{s} & 0.1 & 0.9 \\
\frac{ff_{a2}}{s} & 0.2 & 0.8 \\
\end{pmatrix}
\]

\[
O_{a2} = \begin{pmatrix}
S_{a2} & F_{a2} \\
y_{a2} & 0 & 1 \\
\end{pmatrix}
\]

As for the hardware redundancy test, it has two states, the "safe" state \( S_{a1} \) when no discrepancies are detected between the measures provided by the sensors and a fault state \( F_{a1} \) when these measurements are different beyond a prescribed threshold. The \( E S \) and \( O \) matrices of the test are

\[
ES_{a1} = \begin{pmatrix}
S_{a1} & F_{a1} \\
\frac{ef_{a1}}{s} & 0.1 & 0.9 \\
\frac{ff_{a1}}{s} & 0.1 & 0.9 \\
\frac{efa_{a1}}{s} & 0 & 1 \\
\frac{jfa_{a1}}{s} & 0 & 1 \\
\end{pmatrix}
\]

\[
O_{a1} = \begin{pmatrix}
S_{a1} & F_{a1} \\
y_{a1} & 0 & 1 \\
\end{pmatrix}
\]

By applying the composition rules previously introduced, one can compute the overall Event/State matrix \( E S_g \)

\[
\begin{array}{cccccccc}
& \frac{S}{F_1} & \frac{F_2} & \frac{F_3} & \frac{F_4} & \frac{F_5} & \frac{F_6} & \frac{F_7} \\
\frac{e_{f_{a2}}}{s} & 0 & 0.05 & 0 & 0 & 0.9 & 0.05 & 0 \\
\frac{e_{f_{a1}}}{s} & 0 & 0.1 & 0 & 0.9 & 0 & 0 & 0 \\
\frac{f_{a1}}{s} & 0.01 & 0.09 & 0 & 0 & 0.01 & 0.09 & 0.08 & 0.72 \\
\frac{f_{a2}}{s} & 0.02 & 0.18 & 0.08 & 0.72 & 0 & 0 & 0 & 0 \\
\frac{s}{s} & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]

where the composite states are defined as follows

\[
S = S_{a1} S_{a2} S_{a1}, \quad F_{a1} = EF_{a1} S_{a2} S_{a1} \\
F_{a1} = S_{a1} S_{a2} F_{a1}, \quad F_{a2} = EF_{a2} S_{a2} S_{a1} \\
F_{a2} = S_{a1} F_{a2} S_{a1}, \quad F_{a3} = FF_{a2} S_{a2} S_{a1} \\
F_{a3} = S_{a1} F_{a2} F_{a1}, \quad F_{a7} = FF_{a2} F_{a1} S_{a1}
\]

Correspondingly, the output transformation matrix \( O_g \) is

\[
\begin{array}{cccccccc}
& \frac{S}{F_1} & \frac{F_2} & \frac{F_3} & \frac{F_4} & \frac{F_5} & \frac{F_6} & \frac{F_7} \\
y_{a1} & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
y_{a2} & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
y_{a1} & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\end{array}
\]

Note, for example, that since the alarm \( y_{a2} \) is active in the state \( F_{a2} \), 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 \( F_{a2} \).

The columns of \( O_g \) define the set \( \Sigma_g = \{\sigma_1, \sigma_2, ..., \sigma_p; g\} \) of the signatures allowed. By using the information stored in the matrices \( E S_g \) and \( O_g \), it is then easy to build the matrix \( PSE \) with \( \lvert \Sigma_g \rvert \) rows and \( \lvert \Sigma_g \rvert \) columns whose element \((i, j)\) is the
conditional probability of the signature $\sigma_i$ given the event $e_j$. To determine its value, it suffices to select from $\Omega_T$ the composite states producing the configuration of alarms corresponding to $\sigma_i$ and to add the conditional probabilities of these states given $e_j$ derived from $ES_j$. 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 $\Sigma_g$ is composed by the following signatures

$$
\begin{array}{cccc}
\sigma_1 & y_{11} & y_{12} & y_{13} \\
\sigma_2 & y_{21} & y_{22} & y_{23} \\
\sigma_3 & y_{31} & y_{32} & y_{33} \\
\sigma_4 & y_{41} & y_{42} & y_{43} \\
\sigma_5 & y_{51} & y_{52} & y_{53} \\
\sigma_6 & y_{61} & y_{62} & y_{63}
\end{array}
$$

where, for example, $\sigma_1$ is the signature corresponding to the states $S$ and $F_0$. By recalling (2), (4), one can compute the matrix $PSE$

$$
\begin{array}{cccc}
\sigma_1 & e_{f_{11}} & e_{f_{22}} & f_{f_{11}} & f_{f_{22}} \\
\sigma_2 & 1 & 0 & 0 & 0.09 & 0.02 \\
\sigma_3 & 0 & 0.9 & 0 & 0.09 & 0 \\
\sigma_4 & 0 & 0 & 0.9 & 0 & 0.72 \\
\sigma_5 & 0 & 0 & 0.1 & 0 & 0.18 \\
\sigma_6 & 0 & 0 & 0 & 0 & 0.08 \\
\end{array}
$$

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 $\sigma_4$ is the most probable both for $e_{f_{22}}$ and $f_{f_{22}}$. This is due to the particular structure of the local alarm of the second sensor which cannot discriminate between $e_{f_{22}}$ and $f_{f_{22}}$. Moreover the diagnostic isolation of the fault $f_{f_{22}}$ is particularly critical also because it could generate the signature expected for $f_{f_{11}}$ with an unnegligible 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 $P(e_i)$, $i = 1, \ldots, |E|$, 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 $\sigma_i$. 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 $\hat{P}$ ($\hat{P} = 0.2$), from matrix (5) one obtains the matrix $PES$

$$
\begin{array}{cccc}
\sigma_1 & e_{f_{11}} & e_{f_{22}} & f_{f_{11}} & f_{f_{22}} \\
\sigma_2 & 0.9009 & 0 & 0 & 0.0811 & 0.0189 \\
\sigma_3 & 0 & 0.9009 & 0 & 0.0009 & 0 \\
\sigma_4 & 0 & 0 & 0.5556 & 0 & 0.4444 \\
\sigma_5 & 0 & 0.0840 & 0.0840 & 0.6807 & 0.1513 \\
\sigma_6 & 0 & 0 & 0 & 1 & 0 \\
\end{array}
$$

This matrix shows that the most critical situation, as it was observed also from (5), coincides with the case when signature $\sigma_4$ occurs. Also signature $\sigma_2$ 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. $\hat{P}(\sigma) = 0.95$, $\hat{P}(e_{f_{11}}) = \hat{P}(e_{f_{22}}) = 0.005$, $\hat{P}(f_{f_{11}}) = \hat{P}(f_{f_{22}}) = 0.02$) the following matrix $PES$ is obtained

$$
\begin{array}{cccc}
\sigma_1 & e_{f_{11}} & e_{f_{22}} & f_{f_{11}} & f_{f_{22}} \\
\sigma_1 & 0.9077 & 0 & 0 & 0.0019 & 0.0004 \\
\sigma_2 & 0 & 0.7443 & 0 & 0.2557 & 0 \\
\sigma_3 & 0 & 0 & 0.2381 & 0 & 0.7619 \\
\sigma_4 & 0 & 0 & 0.0240 & 0.0240 & 0.7788 & 0.1731 \\
\sigma_5 & 0 & 0 & 0 & 1 & 0 \\
\end{array}
$$

It is apparent that if, for example, $\sigma_4$ occurs, the most probable fault is now $f_{f_{22}}$ instead of $e_{f_{22}}$.

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 stressed 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


