A Fault Recovery Procedure based on Bayesian Reasoning and Decision Analysis

Maria Carmela Vitelli*, Giuseppina Formato†, Alfredo Vaccaro*
*Department of Engineering
University of Sannio
I-82100 Benevento – Italy
Email: {vitelli,vaccaro}@unisannio.it
† Consorzio di Ricerca Sistema ad Agenti – CORISA
Dipartimento di Informatica
University of Salerno
I-84084 Fisciano (SA) – Italy
Email: gformato@corisa.it

***Abstract*—System fault detection and recovery deals with a decision problem under uncertainty in which we first attempt to isolate a fault according to information we collect regarding the system behavior, and after to recovery from the failure by the application of some recovery actions. In this paper we propose a method which makes use of Bayesian networks to reason under uncertainty and decision analysis to search the best recovery action.**

***Keywords*-FDIR, Fault detection, Fault isolation, Fault recovery, Decision analysis, Bayesian reasoning**

I. Introduction

Modern aerospace systems require more and more operational continuity and reliability. According to this requirement, a fault should be promptly detected in order to prevent undesirable failures and to limit their effect and propagation.

In order to isolate causes that most likely originate the malfunctioning behaviour an initial approach consists in identifying the possible faults underlying the failure. There are different approaches to fault identification. Some of them are based on deterministic decision rules [1], [2], [3], [4], others on black box models [5], [6], [7], [8], and still others on grey-box modelling, reasoning about a posteriori probabilities, i.e. based on Bayesian networks [9], [10], [11].

The latter approach seems to be very promising, because Bayesian networks allow to build and to reason about models that are able to relate faults to observations and possibly recovery actions [12]. Moreover, data mining techniques can be used to build the training of these models [13], [14].

Due to the uncertainty, a plurality of faults may occur in a given time with a probability that can change according to the evidence collected. In addition, each fault can be solved by different actions differing in terms of payoff. Each action can be applied to solve multiple faults.

In this paper we present a fault detection and recovery procedure based on Bayesian reasoning and decision analysis in order to determine what is the recovery action to choose. This paper is structured as follows: Section 2 provides some preliminaries for a common understanding; Section 4 provides details on how to build the Bayesian network; Section 4 explains how to perform decision analysis in order to find an optimal recovery action; Section 5 outlines conclusions.

A typical scheme underlying a Fault Detection, Isolation and Recovery architecture is showed in Fig. 1.

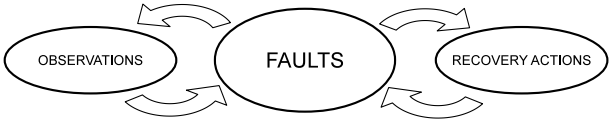


Figure 1. FDIR logic scheme

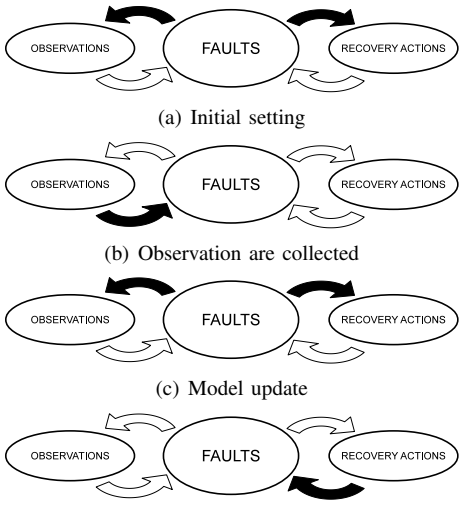
In this scheme faults play a key role. They collect all the possible failure sources. The main purpose of FDIR is to identify the possible faults causing the failure and to recovery the system to the normal operating mode. Generally faults are not viewable directly and are represented as hidden states. Observations represent the collection of events and are able to provide information about hidden fault states. They can be considered as probes whose aim is to discover the source of failure. Recovery actions are a set of procedures used to restore a nominal (or degraded) operating mode.

A FDIR procedure is an iterative process which collects information by observation events with the purpose to solve the failure and restore a normal system operating mode. A typical FDIR procedure is outlined in Fig.2. This procedure is also known as *troubleshooting*.

In the context of Bayesian troubleshooting, faults are indicated with an occurring probability. In a more formal way, let $\mathcal{F} \equiv \{F_1, \ldots, F_n\}$ be the set of all possible faults. Each fault F_i is represented with a priori probability $p(F_i)$. There are independent faults and mutually exclusive faults. In that case,

$$\sum_{i=1}^{n} p(F_i) = 1 \tag{1}$$

978-1-4799-2069-3/14/$31.00 ©2014 IEEE



(a) Initial setting

(b) Observation are collected

(c) Model update

(d) Recovery actions are taken

Figure 2. FDIR reasoning steps

More in general, a relationship can be established between faults, so that

$$p(F_i) = Pr(F_i|F_1, \ldots, F_{i-1}) \tag{2}$$

Generally fault frequency represents the source for estimating $p(F_i)$. Probability can be constant or varying over the time, e.g. considering the Weibull distribution. We explicitly observe, that Eq.(2) does not mean to establish a causal but only a probabilistic relationship between faults. In other terms, it does not mean that fault F_i depends on faults $F_1, \ldots, F_n$; only the related probability does. We preferred to consider the given order of faults, but any other sorting would lead to the same model outcomes.

Let $(O) \equiv \{O_1, \ldots, O_m\}$ be the collection of observations and $\mathcal{A} \equiv \{A_1, \ldots, A_p\}$ be the collection of repairing actions. The relationship between observations and faults is given by

$$p(O_j) = Pr(O_j|F_1, \ldots, F_n) \tag{3}$$

that represents the probability of having an (state of) observation O_j given the (state of) faults $F_1, \ldots, F_n$. Relationship between observations can be *positive* or *negative*. A positive relationship occurs when the existence of fault entail the event observation. While a negative relationship occurs when the existence of fault denies the event observation.

The relation between actions and faults is given by

$$p(A_h) = Pr(Recovery|F_1, \ldots, F_n) \tag{4}$$

that represents the probability the action A_h recovers the system from a failure given the (state of) faults $F_1, \ldots, F_n$.

When an event $O_j = e$ is observed, then the failure body is enriched of evidence ξ. This will change the probability a posteriori of faults.

$$\begin{aligned} p'(F_i) &= Pr(F_i|F_1, \ldots, F_{i-1}, \xi + e) \\ &= \frac{\sum_{F_{i+1}, \ldots, F_n} Pr(F_1, \ldots, F_n, \xi + e)}{\sum_{F_i, \ldots, F_n} Pr(F_1, \ldots, F_n, \xi + e)} \end{aligned} \tag{5}$$

where

$$\begin{aligned} &Pr(F_1, \ldots, F_n, \xi + e) \\ &\quad = Pr(O_j = e|F_1, \ldots, F_n, \xi) \cdot Pr(F_1, \ldots, F_n|\xi) \end{aligned} \tag{6}$$

Initially the body of evidence ξ is empty and probability

$$\begin{aligned} &Pr(F_1, \ldots, F_n|\xi) = Pr(F_1, \ldots, F_n) \\ &= Pr(F_1) \cdot Pr(F_2|F_1) \cdot \ldots \cdot Pr(F_n|F_1, \ldots, F_{n-1}) \end{aligned} \tag{7}$$

After, at each step new events enrich the body of evidence, and according to Eq.(5) the fault probability is updated. When an attempt to recover from failure fails by trying an action A_h, new evidence is added as well.

II. Bayesian Network

To reason about fault detection and recovery we can build Bayesian network. The full set of probabilistic dependencies is provided by Eq.(2). However, we expect that each fault F_i depends only on a subset of preceding faults $F_1, \ldots, F_{i-1}$. For instance we could consider

$$\begin{aligned} p(F_1) &= Pr(F_1) \\ p(F_2) &= Pr(F_2|F_1) \\ p(F_3) &= Pr(F_3|F_1) \\ p(F_4) &= Pr(F_4) \\ p(F_5) &= Pr(F_5|F_4) \end{aligned}$$

This leads to consider a Bayesian network as that outlined in Fig.3. Faults are considered in a order that avoids cycles in the graph. This ensures that graph in Fig.3 is appropriate for a Bayesian network.

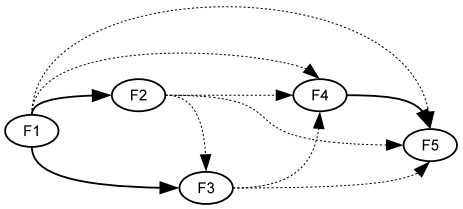


Figure 3. Fault Bayesian Network

After according to conditional probabilities whose general form is expressed by Eq.(3) and Eq.(4) observations $\mathcal{O}$ and

actions $\mathcal{A}$ can be added. Also in this case, observation and actions could be related only to some faults. If we assume

$$p(O_1) = Pr(O_1|F_1, F_2, F_4)$$
$$p(O_2) = Pr(O_2|F_1)$$
$$p(O_3) = Pr(O_3|F_3)$$
$$p(O_4) = Pr(O_4|F_3, F_5)$$

and

$$p(A_1) = Pr(A_1|F_2, F_4)$$
$$p(A_2) = Pr(A_2|F_5)$$
$$p(A_3) = Pr(A_3|F_1, F_2, F_3)$$

Elements in $\mathcal{O}$ are not linked by probabilities in Eq.(3) and the conditioning part is all in $\mathcal{F}$; same property stands for actions in $\mathcal{A}$. Therefore, the resulting graph is appropriate for a Bayesian network because it is still acyclic.

The model considered so far makes the assumptions that observations have place independently instead of being part of a failure scenario, in which observations might happen jointly during a system failure. Indeed, Eq.(3) shows how observation probability depends on faults but not on other observations.

A scenario is a probabilistic model in which a collection of *contextual observations* are inter-dependent. Formally, a scenario S is a collection of contextual observations $\mathcal{O}_S \equiv \{O'_{S,1}, \ldots, O'_{S,p}\}$, related each other by conditional probabilities

$$p(O'_{S,l}) = Pr(O'_{S,l}|O'_{S,1}, \ldots, O'_{S,l-1}, \mathcal{O}) \qquad (8)$$

Each contextual observation O'_l is linked to one observation O_j and is not shared among different scenarios. On the other hand, each observation O_j can be linked to multiple contextual observations O'_l.

As defined in Eq.(8) and depicted in Fig.4, observations can link to scenarios.

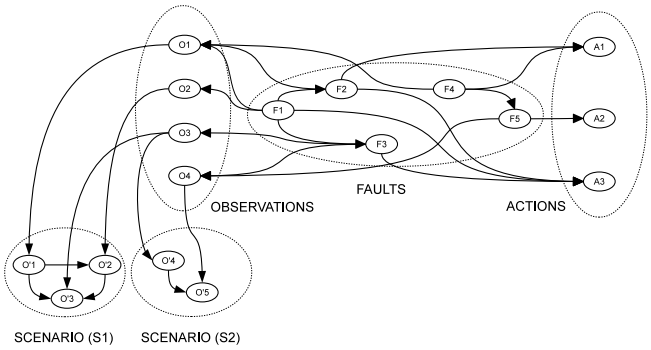


Figure 4. Scenario-Observation-Fault-Action (SOFA) Network

In this case we assumed two scenarios, S_1 and S_2. The first makes use of contextual observations O'_1, O'_2, O'_3, whose conditional probabilities are

$$p(O'_1) = Pr(O'_1|O_1)$$
$$p(O'_2) = Pr(O'_2|O_2)$$
$$p(O'_3) = Pr(O'_3|O_3)$$

Instead for the scenario S_2, we have contextual observations O'_4 and O'_5, and

$$p(O'_4) = Pr(O'_4|O_3)$$
$$p(O'_5) = Pr(O'_5|O_4)$$

Eq.(3) does not express actual probabilities values. They represents transpositions, by which variables in $\mathcal{O}$ are mapped over variables on $\mathcal{O}'_{\mathcal{S}}$. They are used to decouple scenarios from observations. In Tab.I are presented their conditional probability tables (CPTs).

Table I
TRANSPOSITION CPT

		O_j			
		$o_{j,1}$	$o_{j,2}$	$\ldots$	$o_{j,r}$
O'_l	$o'_{l,1}$	1	0	$\ldots$	0
	$o'_{l,2}$	0	1	$\ldots$	0
	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
	$o'_{l,r}$	0	0	$\ldots$	1

Since dependencies are from observations to scenarios, and scenarios are acyclic, the whole graph is still acyclic, therefore it is appropriate to model a Bayesian network.

III. DECISION ANALYSIS

Decision Analysis is a set of systematic methodologies aimed at supporting a decision maker (i.e. individuals or organizations) in solving complex decision problems in a formal manner. Typically the decision problem can be formalized, quite apart from the specific applicative context, as the problem of choosing from a set of mutually exclusive alternatives the one which is optimal in some sense. Frequently, some elements of decision process may not be uniquely assessed, due to the lack of precise knowledge about the alternative consequences In this case a lack of determinism is introduced in the problem solution. Uncertainties in decision analysis stem from the unpredictable states of nature which cannot be influenced by the decision maker and whose occurrence is often probabilistic in nature [15], [16].

An important role is played by the *Decision Matrix*. For the various hypotheses it contains the outcomes of each

alternative. In particular, given a set of n mutually exclusive alternatives

$$\Lambda = \{a_1, \ldots, a_i, \ldots, a_n\} \tag{9}$$

and a set of m exhaustive and mutually exclusive hypotheses

$$\Pi = \{s_1, \ldots, s_j, \ldots, s_m\} \tag{10}$$

the decision matrix D can be defined as

$$D = \begin{bmatrix} d_{1,1} & d_{1,2} & \cdots & d_{1,m} \\ d_{2,1} & d_{2,2} & \cdots & d_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n,1} & d_{n,2} & \cdots & d_{n,m} \end{bmatrix} \tag{11}$$

where the generic element $d_{i,j}$ represents the outcome (a.k.a. payoff) of the alternative a_i when the hypothesis s_j occurs.

In the context outlined by this paper, alternatives are made of recovery actions, while hypotheses are the possible faults (or failure modes) for the system being analyzed.

With the identification of the row vector of the decision matrix which is optimal in some sense it's possible to solve the decision problem. To address this issue, a function (i.e. a suitable real-valued function defined on the set of all row vectors of the decision matrix) should assess the overall value of each row vector (i.e. the overall value of each alternative under the various hypotheses).

$$V : \Lambda \to \mathbb{R} \tag{12}$$

which depends on payoff values expressed by rows in D, that is

$$V(a_i) = \mathcal{V}(d_{i,1}, \ldots, d_{i,m}) \tag{13}$$

where

$$\mathcal{V} : \mathbb{R}^m \to \mathbb{R} \tag{14}$$

that is marginally monotonic, i.e.,

$$\begin{aligned} &\mathcal{V}(d_1, \ldots, d_j, \ldots, d_m) \\ &\qquad \leq \mathcal{V}(d_1, \ldots, d_j + \delta, \ldots, d_m) \\ &\qquad\qquad \forall \delta > 0,\ \forall j = 1..m \end{aligned} \tag{15}$$

so that an alternative becomes preferrable to another if it entails better scores over the different hypotheses.

The expected payoff value is a typical paradigm frequently adopted in defining the valuation function. According to this paradigm the function V assumes the following structure

$$V(a_i) = \mathcal{V}(d_{i,1}, \ldots, d_{i,m}) = \sum_{j=1}^{m} p_j d_{i,j} \tag{16}$$

where p_j denotes the probability of the hypotheses s_j while $V(a_i)$ represents the mean of the random payoff when the alternative a_i is chosen.

In this case the solution of the decision problem is the alternative which maximizes the expected payoff value

$$a_{opt} = \left\{ a_{i^*}, i^* = \arg\max_{i=1..n} V(a_i) \right\} \tag{17}$$

To solve a decision problem, another strategy can be applied by defining the Regret Matrix [16]. The elements $r_{i,j}$ of this matrix can be obtained by following two steps:

1) Identify for each hypothesis (i.e. for each column of the decision matrix) the maximal payoff

$$M_j = \max_{i=1..n} d_{i,j} \tag{18}$$

2) Calculate the regret of having selected the other alternatives if the hypothesis s_j indeed occurred by the probability p_j

$$r_{i,j} = p_j \cdot (M_j - d_{i,j}) \tag{19}$$

When the regret matrix has been computed, to solve the decision problem is applied the minimax regret rule (i.e. by selecting the alternative for which the maximum regret is as small as possible).

$$a_{opt} = \left\{ a_{i^*}, i^* = \arg\min_{i=1..n} \left(\max_{i=1..m} r_{i,j} \right) \right\} \tag{20}$$

In many circumstances, since recovery actions refers to a limited subset of fault and each fault is covered by a limited subset of recovery action, when decisions are referred to fault identification and recovery, the matrix D is generally sparse. An example is given by Eq.(21).

$$D = \begin{bmatrix} 10 & & & \\ & 5 & 20 & \\ 20 & 2 & & 10 \end{bmatrix} \tag{21}$$

Missing elements indicate the absence of relations between the recovery action and some faults. This means that any value assignment (e.g., giving zero or infinity) would result to be arbitrary, biasing the analysis.

In this case we can perform a decision by choosing

$$a_{opt} = \left\{ a_{i^*}, i^* = \arg\max_{i=1..n} U(a_i) \right\} \tag{22}$$

in which U is made of two components

$$U(a_i) = V_s(a_i) + R(a_i) \tag{23}$$

The first component takes into the account the expected payoff for those scenarios covered by the action a_i, so

$$V_s(a_i) = \sum_{j \in S(a_i)} p_j d_{i,j} \tag{24}$$

The second components takes in the account the regret for choosing an action that could not match the given hypothesis (i.e. failure mode), so it can be expressed as

$$R(a_i) = \sum_{j \notin S(a_i)} p_j \min_{h \neq i} d_{h,j} \tag{25}$$

When an action covers all possible cases, $U(a_i) = V(a_i)$ according to Eq.(16). While when an action does not cover

the possible hypotheses, $U(a_i) = R(a_i)$ as defined in Eq.(20).

As an example, let us consider that priori probabilities are

$$p = \begin{bmatrix} 0.2 & 0.3 & 0.1 & 0.4 \end{bmatrix} \quad (26)$$

We have

$$U(a_1) = V_s(a_1) + R(a_1) = (0.2 \cdot 10) + (0.3 \cdot 2 + 0.1 \cdot 20 + 0.4 \cdot 10) = 2 + 6.6 = 8.6 \quad (27)$$

$$U(a_2) = V_s(a_2) + R(a_2) = (0.3 \cdot 5 + 0.1 \cdot 20) + (0.2 \cdot 10 + 0.4 \cdot 10) = 3.5 + 6 = 9.6 \quad (28)$$

$$U(a_3) = V_s(a_3) + R(a_3) = (0.2 \cdot 10 + 0.3 \cdot 5 + 0.4 \cdot 10) + (0.1 \cdot 20) = 8.6 + 2 = 10.6 \quad (29)$$

The action a_3 results as the best option. If after collecting evidence ϵ, we have

$$p|\epsilon = \begin{bmatrix} 0 & 0.2 & 0.7 & 0.1 \end{bmatrix} \quad (30)$$

we get

$$U(a_1) = 0 + 15.4 = 15.4 \quad (31)$$

$$U(a_2) = 15 + 1 = 16 \quad (32)$$

$$U(a_3) = 1.4 + 14 = 15.4 \quad (33)$$

and best option becomes a_2. We notice that $V_s(a_1) = 0$, as scenarios covered by actions a_1 became impossible after collecting the evidence ϵ. So the value associated to action a_1 is only related to its regret value $R(a_1)$.

IV. Conclusion

In this paper we proposed a fault detection and recovery method based on Bayesian networks and Decision Analysis. The model is able to select the best option according to which hypotheses are becoming prominent after some evidence concerning the system failure being observed. In order to overcome matrix sparsity we proposed a selection criterion based on a combination of expected payoff and regret function. In the future, we aim at testing this method in different conditions.

References

[1] S. Abdelwahed, G. Karsai, and G. Biswas, "System diagnosis using hybrid failure propagation graphs," in *The 15th International Workshop on Principles of Diagnosis*. Citeseer, 2004.

[2] I. Hwang, S. Kim, Y. Kim, and C. Seah, "A survey of fault detection, isolation, and reconfiguration methods," *Control Systems Technology, IEEE Transactions on*, vol. 18, no. 3, pp. 636–653, 2010.

[3] A. Misra, "Senor-based diagnosis of dynamical systems," Ph.D. dissertation, Vanderbilt University, 1994.

[4] F. SalarKaleji and A. Dayyani, "A survey on fault detection, isolation and recovery (fdir) module in satellite onboard software," in *International Conference on Recent Advances in Space Technologies (RAST)*, 2013, pp. 545 – 548.

[5] S. Ierace, P. Marinaro, P. Tatavitto, and L. Troiano, "Profiling the power usage of industrial machinery by ann," in *Soft Computing and Pattern Recognition (SoCPaR), 2010 International Conference of*, 2010, pp. 413–418.

[6] S. Ierace, R. Pinto, L. Troiano, and S. Cavalieri, "Neural network as an efficient diagnostics tool: A case study in a textile company," vol. 1, no. PART 1, 2010, pp. 122–127.

[7] L. Troiano, M. Tipaldi, A. Di Cerbo, M. Hoping, D. De Pasquale, and B. Bruenjcs, "Satellite fdir practices using timed failure propagation graphs," vol. 11, 2012, pp. 8524–8531.

[8] S. Rampone, V. Pierro, L. Troiano, and I. Pinto, "Neural network aided glitch-burst discrimination and glitch classification," *International Journal of Modern Physics C*, vol. 24, no. 11, 2013.

[9] M. Paakko, P. Myllymäki, N. Holsti, and H. Tirri, "Modern ai approaches for building robust fdir components."

[10] S. Bottone, D. Lee, M. O'Sullivan, and M. Spivack, "Failure prediction and diagnosis for satellite monitoring systems using bayesian networks," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2008, pp. 1–7.

[11] D. Codetta-Raiteri, L. Portinale, S. Di Nolfo, and A. Guiotto, "Arpha: a software prototype for fault detection, identification and recovery in autonomous spacecrafts," *Acta Futura*, vol. 5, pp. 99–110, 2012.

[12] L. Troiano and D. De Pasquale, "Supporting complexity in modeling bayesian troubleshooting," in *ICEIS (2)*, J. Filipe and J. Cordeiro, Eds. SciTePress, 2010, pp. 344–349.

[13] L. Troiano, G. Scibelli, and C. Birtolo, "A fast algorithm for mining rare itemsets," in *ISDA*. IEEE Computer Society, 2009, pp. 1149–1155.

[14] L. Troiano and G. Scibelli, "A time-efficient breadth-first level-wise lattice-traversal algorithm to discover rare itemsets," *Data Mining and Knowledge Discovery*, pp. 1–35, 2013. [Online]. Available: http://dx.doi.org/10.1007/s10618-013-0304-3

[15] H. Brachinger and P. Monney, *Encyclopedia of Life Support Systems (EOLSS)*. Oxford, UK: Eolss Publishers, 2002, ch. Decision analysis, in optimization and operations research., pp. 933–978.

[16] S. Hansson, *An Overview of Decision Theory*, ser. SKN rapport. National Board for Spent Nuclear Fuel (Statens kärnbränslenämnd) (SKN), 1991. [Online]. Available: http://books.google.it/books?id=z-WDNAAACAAJ