Abstract: Fault detection and isolation is becoming one of the most important aspects in vehicle control system design. In order to achieve this FDI schemes, particular vehicle subsystems integrated with a controller have been proposed. In this paper a suitable framework is presented that utilizes a hierarchical FDI scheme in association with a propagation digraph, representing the propagation aspects of faults, and allows to reduce the computational effort. An example of application to a brake-by-wire system is described. Copyright ©2002 IFAC

Keywords: Diagnosis, Fault detection, Hierarchical decision making, Monitoring, Graphs

1. INTRODUCTION

Failure analysis and diagnosis of large-scale systems have received considerable attention in recent years (Guan and Graham, 1994; Koscielný, 1995; Scattolini, 2000). Fundamental issues facing the design of a diagnostic system include what knowledge to represent, the representation scheme and the inference strategy that perform the actual diagnosis. These systems have evolved from the previous ones based on heuristic knowledge of symptom-fault associations to the more recent ones based on structure, behavior and functionality of the device and subsystem to be diagnosed (Kokawa et al., 1983; Narayanan and Viswanadham, 1987; Padalkar et al., 1991).

In the application of knowledge based methodologies to large-scale systems, two basic model representations can be encountered: the signed directed digraph and the propagation digraph. While in the signed directed digraph (Kramer and Jr., 1987) a qualitative model is defined by analysis of the causal relationships between variables, in the propagation digraph (Kokawa et al., 1983; Narayanan and Viswanadham, 1987) the failure or fault propagations from subsystems to other subsystems is described by a digraph.

A fault detection system for on-line application to large scale plants must satisfy certain requirements (Padalkar et al., 1991). First, it must provide guaranteed response times, completing the diagnosis in a deterministic amount of time. Second, it must be able to reason about time, because much information can be deducted from time events. Third, it must use as much as possible all the information available from improving and speeding the diagnosis. The fundamental issues of how to model the system and how to develop a diagnostic procedure arise in this contest. Moreover, the following questions arise in developing diagnostic systems:

- how to interpret various fault symptoms to formulate the final diagnosis;
- how to deal with the occurrence at different time instants of different symptoms for a same fault;
- how to ensure the proper diagnostic reasoning for different set of available measuring signals;
- how to distinguish between single/multiple faults;
• how to use redundant information to verify the diagnosis.

In this paper, a method that makes use of fault propagation digraphs to describe the propagative nature of the faults is proposed. In this way, it is possible to model the system at any desired level of granularity depending on the level of details that is desired, and on the applications.

In contrast to the conventional methods as described in Gertler (1998), Patton et al. (1989) and Frank (1990), this paper presents a new framework for hierarchical fault detection and isolation (FDI) that combine qualitative models with quantitative models. The idea is to use a model propagation digraph together with model-based FDI to identify and localize the origin of the fault with a reduced computational effort by allowing only a limited number of fault detection units (FDUs) to run on-line while other FDUs are available under request whenever a failure is detected. Moreover, the propagation digraph may allow the detection and isolation of other type of faults for which the available FDI doesn’t guarantee isolation.

The paper is organized as follows. In the next section the modelling procedure is presented; in Section 3 the failure identification process is described. Section 4 deals with the proposed hierarchical FDI scheme while applied to an automotive electric brake system.

2. MODEL FORMULATION

In this framework, some terminologies are introduced. In the following sections, a failure will indicate a malfunction due to a fault while a failure source represents the starting subsystem or sub-device from which failures have propagated. A diagnostic test consists of a residual generator plus a residual evaluation which outputs a result indicating the normal or abnormal operating condition of the tested device or subsystem (Pisu et al., 2000).

System failures occur in two stages: failure sources and failure propagations. So, a process for failure analysis must first try to locate the failure sources, and then determine the cause of the failure. The framework given in this section for model-based failure analysis can be summarized as in Fig. 1 and is divided in two phases: a failure source location phase and a failure cause identification phase. At each phase correspond a failure model and a failure analysis process.

The framework is structurally divided in two components, one representing the knowledge about fault propagation, and the other one representing the hierarchical model-based FDI for a certain set of faults (sensor faults, and/or actuators faults, and/or parameter, etc.). The fault propagation model may take into account for propagations of faults that are not considered in the hierarchical FDI.

Fig. 1. A framework for model-based failure analysis.

The failure analysis is divided in two parts, the first is the failure source location process that utilizes the model constituted by the hierarchical level-structured fault propagation digraph, and the second is failure cause identification process which utilizes a hierarchical model-based FDI (Pisu et al., 2001). The source location process operates on individual structures of the hierarchical fault propagation model. It backtracks along all feasible fault propagation paths in a structure starting from the elements that are indicated to be faulty by the FDUs and locates the set of elements which may be the sources of failure. This backtracking is subject to probability constraints imposed by the failure relations between elements and temporal constraint imposed by the failure relations and detection time of the FDUs.

The plant devices, instrumentation elements, diagnostic tests and fault propagation can be modelled by a digraph composed of nodes and arcs (Guan and Graham, 1994; Kokawa et al., 1983; Scattolini, 2000).

Specifically, a node can represent:

i) a device or a failure mode of a device;
ii) a connecting element or dummy node necessary to properly model the fault propagation;
iii) a fault detection unit (FDU) as described in Fig. 2 (Pisu et al., 2001);

Fig. 2. Fault Detection unit.

It must be noticed that, whenever nodes are used to modelling failures, multiple nodes are necessary to describe a device and its possible faults. An example is represented in Fig. 3 where a sensor is represented
can be now used to specify a fault propagation digraph because any other case can be treated by a proper use of dummy nodes (Fig. 4).

It is assumed that a fault detection unit is connected to only one node. This hypothesis is not restrictive because any other case can be treated by a proper use of dummy nodes (Fig. 4).

In general, we can represent the set of nodes \( V \) of a system \( S \), excluding the diagnostic tests, by

\[
V = \{v_1, \ldots, v_n\}
\]

A fault propagation relation \( R \) on \( V \) can be defined such that \( v_i \xrightarrow{R} v_j \) means that a fault in node \( v_i \) can propagate to node \( v_j \). This fault propagation relation can be now used to specify a fault propagation digraph \( G \) for \( S \)

\[
G = (V, E)
\]

where \( E \) is the edge set defined by

\[
E = \{e_{ij} = (v_i, v_j) \mid v_i \xrightarrow{R} v_j, \; i = 1..n, \; j = 1..n\}
\]

A column vector \( D \) associated to the FDU can be defined as follows

\[
D = \text{col}(d_i)
\]

with \( d_i = 1 \) if the node \( v_i \) is connected to a FDU and \( d_i = 0 \) otherwise. We also define a set \( D^{(1)} \) of nodes connected to FDUs running online and a set \( D^{(2)} \) of nodes connected to FDUs available under request to the failure analysis process.

At each direct edge \( e_{ij} \) in the graph \( G \) a weight \( w_{ij} = (P_{ij}, t^l_{ij}, t^u_{ij}) \) is associated, where \( P_{ij} = P(v_i, v_j) \), \( 0 < P_{ij} \leq 1 \) is the probability that a failure in node \( v_i \) propagates directly to node \( v_j \), and \( t^l_{ij}, t^u_{ij} \) are respectively the lower and upper bound of the failure propagation time between nodes \( v_i \) and \( v_j \) when \( i \neq j \). When \( i = j \), \( t^l_{ij} \) and, \( t^u_{ij} \) represent the lower and upper bound of the failure propagation time between nodes \( v_i \) and the fault detection unit \( d_i \).

To the digraph \( G \) it is possible to associate the so called adjacency matrix \( A \) given by

\[
A = [a_{ij}]
\]

where \( a_{ij} = 1 \) if \( e_{ij} \in E \) and \( a_{ij} = 0 \) otherwise.

From the adjacency matrix \( A \), it is possible to compute (Narayanan and Viswanadham, 1987; Guan and Graham, 1994) the reachability matrix \( P \) defined as

\[
P = [p_{ij}] = (I + A)^k = (I + A)^{k-1} \neq (I + A)^{k-2} \tag{2}
\]

where \( k \in \mathbb{Z}_+ \), \( I \) is an identity matrix, and the operators are Boolean.

The reachability matrix corresponding to the graph of Fig. 5 is

\[
P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \tag{3}
\]

From the matrix \( P \) it is possible to define the reachability set or descendant set of a given node \( v_i \) as

\[
R(v_i) = \{v_j \in V \mid p_{ij} \neq 0\} \tag{4}
\]

and the ancestor set or antecedent set as

\[
A(v_i) = \{v_j \in V \mid p_{ji} \neq 0\} \tag{5}
\]

On the basis of this information, four additional matrices for fault location are calculated

a) Shortest time matrix \( T_e = [t_{e_{min}}] \) obtained by applying the Warshall-Floyd method (Floyd, 1962) to the matrix \( T_1 = [t^l_{ij}] \). The element \( t_{e_{min}} \) is the minimum failure propagation time corresponding to the shortest path from \( v_k \) to the FDU linked at the node \( v_m \).
b) **Biggest time matrix** $T_b = [t_{b_{lm}}]$ obtained from the
matrix $T_u = [t_{ij}]$ where $t_{b_{km}}$ is the maximum failure propagation time between node $v_k$ and the
FDU linked at the node $v_m$ along the shortest path with probability 1.

c) **Shortest time matrix** $T_f = [t_{f_{kl}}]$ obtained by
applying the Warshall-Floyd method to a matrix $T_1$
obtained from $T_1$ by replacing all the $t_{ij}$ s.t. $P_{ij} \neq 1$ with
$\infty$.

d) **Failure propagation probability matrix** $T_{F} = [q_{k|l}]$
where $q_{k|l} = \prod_{(i,j) \in E(k,l)} P_{ij}$ and $q_E(k,l)$ is the shortest
path from $v_k$ to $v_l$.

Using the matrix $P$, the digraph $G$ can be partitioned
into classes $V_1, \ldots, V_m$ as

$V_1 = \{v_i \in G \mid R(v_i) \cap A(v_i) = A(v_i)\}$;
$V_j = \{v_i \in G - V_1 - \cdots - V_{j-1} \mid (R(v_i) - V_1 - \cdots - V_{j-1}) \cap (A(v_i) - V_1 - \cdots - V_{j-1})$
$\subseteq (A(v_i) - V_1 - \cdots - V_{j-1}), \ j = 2, \ldots, m$ (6)

where $m$ is such that $G - V_1 - \cdots - V_m = \emptyset$.

This procedure is called level-structuring (Narayanan and
Viswanadham, 1987) and the resulting digraph is
called level-structured digraph.

The classes so obtained satisfy the following properties

1) $\bigcup_{i=1}^{m} V_i = V$
2) $V_i \cap V_j = \emptyset$ for $i \neq j$
3) For $v_i, v_j \in G$ either $p_{ij} = p_{ji} = 1$ ($v_i$ and $v_j$
in a loop) or $p_{ij} = p_{ji} = 0$ ($v_i$ and $v_j$ are
disconnected).
4) Edges leaving vertices in a class $V_i$ can go only to
vertices in classes $V_j$ such that $i < j$.

An example of level-structured digraph is shown in
Fig. 6. Now, a graph with a single node $S$ forms the

$H = \{L_i\} \ i = 1, \ldots, n$
where $L_i$ denotes the $i^{th}$ level in the hierarchy and

$L_i = \{G_{ij}\}, \ j = 1, \ldots, m$

![Fig. 6. Level-structuring digraph.](image)

Fig. 7. A hierarchical fault propagation model for a
braking and steering systems.

Each $G_{ij}$ is a level-structured digraph $(V_{ij}, E_{ij})$
that corresponds to a node $v_i$ in the $(i-1)$th level. An example
of hierarchical fault propagation model is shown in
Fig. 7.

The number of levels in the hierarchy depends on
how finely the actual system being modelled can be
subdivided recursively into distinct subsystems that
are analyzable in terms of fault propagation.

The propagation of faults within $S$ may now be
characterized as follows. For each digraph $G_{ij}$ at each
level $L_i$ of the hierarchical fault propagation model,
a failure occurring at node $v_i \in G_{ij}$ at time $t_0$ will
propagate to the nodes $\{v_j\}, v_j \in G_{ij}$, by time $t_1$
only if each node $v_j$ satisfies the constraints

- $p_{ij} = 1$
- There exists at least one path $q_E$ from $v_i$ to $v_j$
in $G_{ij}$ such that $\prod_{(i,j) \in E(k,l)} P_{ij} \geq P_{\text{threshold}}$ where
$P_{\text{threshold}}$ is a heuristically estimated threshold
probability and the product is taken over all
edges in $q_E$.
- In the set of paths satisfying the previous conditions,
there exists a path $q_E$ that satisfies the
constraint $\sum_{(i,j) \in E(k,l)} t_{lm} \leq t_1 - t_0$.
- Among the paths satisfying the previous constraints,
there is at least one path $q_E$ such that
for all nodes $v_k \in q_E$ and for all $v_j$ in the set
of normal diagnosed nodes at time $t_1$, $t_k < t_s$, with
$t_k = \sum_{(i,j) \in E(k,l)} t_{lm}$ and $t_s = \min \{t_{b_{xy}}\}$.

3. THE FAILURE IDENTIFICATION PROCESS

In order to determine a procedure to identify a fault
in the system, some assumptions on the FDUs of the
hierarchical model-based FDI are necessary:
• The FDU are false alarm free.
• Every kind of single fault that is included in the propagating digraph can be detected by some active FDU, i.e. there exists a technical tool indicating if the node is faulty or not.
• In the set of activable FDUs for a given non-decomposable node, there exists at least one that allows to isolate a single fault in this node within a desired amount of time $T_d$. This means that all the nodes for which this condition is not satisfied have at least one FDU running on-line in their reachable set able to isolate the fault within $T_d$ sec.

3.1 The failure location procedure for a level-structured tree

A hierarchical level-structured tree is a hierarchical level-structured digraph where, after removing all FDU and dummy nodes, each level appears to be a set of different trees having one root and one level of leaves. An example of this type is shown in Fig. 8.

![Fig. 8: A hierarchical level-structured tree.](image)

In the case of level-structured tree, a more efficient algorithm that allows the failure source location faster than an algorithm for a generic structure can be determined. The reason is supported by the fact that, in many cases, it is possible to find an, eventually approximated, hierarchical structure for the system under study or for some of the subsystems of interest that form the system itself. In this cases, to have a dedicated algorithm may result in a faster location of the fault and reduction of the computational effort than a general algorithm. The algorithm presented is valid only for single fault in a single tree and for a specific level i.

Let define

$D_{L_i}^{(1)}$ the set of node in $D^{(1)}$ that are abnormal at level i,
$D_{L_i}^{(2)}$ the set of node in $D^{(2)}$ that are available at level i,
$D_{L_i}^{(1)}$ the set of node in $D^{(1)}$ that are normal at level i,
$\Delta_i$ the set of dummy nodes at level i,
$\Omega_{L_i}$ the set of nodes at level i that can be excluded to be faulty from the FDUs in $D_{L_i}^{(1)}$,

$C_i$ the set of candidate nodes at level i,
$\phi_1(v)$ the set of nodes in $D_{L_i}^{(1)}$ reachable from the node v with probability 1,
$\phi_2(v)$ the set of nodes in $D_{L_i}^{(2)}$ reachable from the node v with probability 1,
$t_0$ the starting time fault location for the actual tree,
$t_k$ the time at which the diagnostic test $d_k$ switches to abnormal.

A first selection of candidates for the failure origin is constituted by the set $C_i = \bigcap_k A(v_k) - \Delta_i - \Omega_{L_i}$, $v_k \in D_{L_i}^{(1)}$. If the graph is as $S_1$ (Fig. 8) then the reduction of this set of candidates is obtained with the following algorithm

1. If $|C_i| = 0$ then activate multiple fault diagnosis.
2. If $|C_i| = 1$ then if decomposable return $C_i$ else run the FDU corresponding to the $\min(t_{f_{k_i}})$ with $v_k \in \phi_2(v_i)$ that allows isolation. If diagnosis is abnormal then return $C_i$ as failure source else return $C_i = \emptyset$.
3. Calculate $T = \{v \in C_i|class(v) = 1\}$, $\{v\}$ = $C_i - T$.
4. From all $v_l \in T$ eliminate the nodes s.t. $t_{b_{l_k}} < t_{f_{l_i}}$ where $v_k \in \phi_1(v_l)$ and $v_l \in D_{L_i}^{(1)}$. Let $\Gamma = \{v\}$ = set of eliminated nodes. Set $D_{L_i}^{(1)} = D_{L_i}^{(1)} - \bigcup_j R(v_j) - \Gamma$, $v_j \in T$.
5. From all $v_l \in T$ eliminate the nodes s.t. $\max_k\{t_{c_{l_k}} + t_0 - t_k\} \geq \min_j\{t_{b_{l_j}}\}$ with $v_k \in D_{L_i}^{(1)}$, and $v_j \in \phi_1(v_l)$.
6. For all $v_l \in T$ that are not decomposable, if possible, run the FDU corresponding to the $\min(t_{f_{l_i}})$ with $v_k \in \phi_2(v_l)$ that allows isolation. If the diagnosis is abnormal then $C_i = \{v\}$ else re-calculate $\Omega_{L_i}$ and $T = T - \{v_l\} - (T \cap \Omega_{L_i})$.
7. If $|T| = 0$ then $C_i = \{v\}$, go to step 2.
8. If $|T| \geq 1$ and $v$ is not decomposable, then run the FDU in $\phi_2(v)$ corresponding to the shortest time that allows isolation. If $v$ is normal then return $C_i = T$, else $C_i = \{v\}$ and go to step 2. Otherwise $v$ is decomposable $C_i = T \cup \{v\}$ and exit.

For a graph as $S_2$ (Fig. 8), it is necessary to change in step 3 the set $T = \{v \in C_i|class(v) = 1\}$ with the set $T = \{v \in C_i|class(v) = 2\}$.

4. AN EXAMPLE: THE ELECTRIC BRAKE SYSTEM

In Fig. 9 an example of level-structured tree for an electric brake system is presented. The picture is a detailed view of level 3 and 4 of Fig. 7. Level 3 and level 4 contain graphs similar to $S_2$ in Fig. 8. The FDUs in level 3 are only for detection while in level 4 they perform isolation.
Fig. 9. Level-structuring digraph for brake system.

The arcs without label have weight \((1, 0 \text{ sec}, 0 \text{ sec})\) while the other weights are given by \(w_{11} = w_{33} = w_{44} = w_{66} = (1, 0.2 \text{ sec}, 0.32 \text{ sec}), w_{22} = w_{55} = (1, 0.04 \text{ sec}, 0.2 \text{ sec}), w_{11}^{lf} = \cdots = w_{rr}^{rt} = (1, 0.004 \text{ sec}, 0.04 \text{ sec}), w_{22}^{lf} = \cdots = w_{rr}^{rt} = (1, 0.04 \text{ sec}, 0.16 \text{ sec}), w_{brk}^{lf} = w_{brk}^{rt} = (1, 0.04 \text{ sec}, 0.24 \text{ sec})\).

In level 4, the FDU2s in the systems LF, RF, LR, RR are available on request, while all the others are running on-line and it is desired to isolate the fault within \(T_\delta = 0.4 \text{ sec}\) from its detection.

A step fault in the caliper force sensor of the LF wheel is injected at \(t_0 = 2 \text{ sec}\). After 80 msec, FDU2 in level 3 turns abnormal and the algorithm is activated. By applying the algorithm to the tree in level 3, the set of candidates attained is \(C_3 = \{ \text{LF, RF, BRK + P} \}\). Then the algorithm steps to level 4 at \(t_0 = 2.088 \text{ sec}\). A priority is assigned to the BRK system with respect to the others because a fault in this unit is more critical than a fault in a wheel system. Because no fault is detected, the algorithm is applied then to the LF subsystem (the wheel subsystems have same priority). The candidate nodes in the LF subsystem are all the nodes not dummies, i.e. \(C_{lf} = \{ \text{DC motor, Position sensor, Current sensor, } F_{cal} \text{ sensor} \}\). From FDU1\(_{lf}\), because the upper-bound in \(w_{11}^{lf}\) is equal to the lower-bound in \(w_{22}^{lf}\), at step 5 the set of candidates is reduced to \(C_{lf} = \{ F_{cal}, \}\). At step 6, by activating the FDU2\(_{lf}\) the fault is isolated after at most 0.16 sec in the caliper force sensor.

5. CONCLUSION

In this paper, a hierarchical model-based FDI scheme using digraphs has been presented. By combining model-based methodologies and qualitative methods, a reduction of the computational effort is attained. Future research will be conducted on the analysis of multiple faults and to develop algorithms for more general digraph structures.

REFERENCES