DRASTIC CUT OF MAN'S WORK IN RELIABILITY STUDIES BY USING AN EXPERT SYSTEM

M. BOUISSOU
EDF
Direction des etudes et recherches
Service RNE
1, av. du General de Gaulle
92141 Clamart
FRANCE tel : (1) 47 65 55 07

N. VILIATTE
University Pierre et Marie Curie
4 place Jussieu
75005 Paris
FRANCE

ABSTRACT

We show here how we have been able, thanks to the use of artifical intelligence techniques, to find a neat solution to the problem of the automation of reliability studies. We have introduced rule-based representation at two levels :

- the modelling of the studied system, which is very general and versatile, and nevertheless quantifiable because of the rule-base representation.
- the storage of the reliability engineers knowledge about failure modes and effects for conventional components.

The productivity of the reliability studies has been substantially improved with this approach.

KEYWORDS : reliability - reliability model - automation - expert system - event sequences.

I INTRODUCTION

As systems involved in human activity become increasingly sophisticated and as their destructive power grows, the need for more and more complex reliability and safety studies is more acutely felt.

Some attempts /1/ /2/ have been made to automate reliability studies using an algorithmic approach, but they have been limited because the models used were not general enough, and could hardly allow the introduction of knowledge on studied systems. Therefore, EDF (Electricity de France) has chosen a different and original approach, based on expert systems, which involves two levels of rules :

- A knowledge level, using first order rules. This level is the expert system concerning the studied systems.
- A modelling level, which results from the application of the knowledge rules to a minimum, simplified (essentially topological) description of the studied system.

According to the nature of the studied system, two types of modelling are used.

- If there are no dependencies between the components of the studied system, modelling can be simple, and results, in a straightforward way, to a very commonly used reliability model, called fault-tree. An expert system called EXPRESS, building fault-trees for thermo-hydraulic systems is now operational /3/.
- But, if there are dependencies (for example, a diesel generator starts when a normal power supply fails), another type of modelling has to be used, either to solve the whole problem, or as a complement to the fault-tree. This is why we have created a new model that makes it possible to Introduce all the information on the propagation of interactions throughout the system, whereas the fault-tree model cannot. At the same time, we have created a specialized inference engine called GSI, able to derive from this model a fully automatic computation of a system failure probability. GSI is designed to take into account all the dependencies in the calculation of the system failure probability.

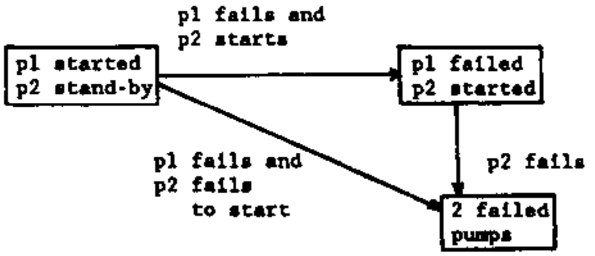
Since GSI (as conventional programs that deal with fault-trees) does not contain any knowledge about studied systems, we have introduced the reliability engineers' knowledge in an expert system, that can automatically generate the GSI model of a system, from the minimum information needed to describe it.

But, of course, GSI can be used without the expert system.

In this paper, we shall first list the main features of the GSI model, secondly explain how the associated expert system works, and finally give the performance data for these tools with two illustrative examples.

When there are dependencies between the components, the model generally used is the state graph.

Here is an example of state graph for a 2 pump system, where the second pump starts when the first one fails.



The use of such models has been considerably limited so far by the fact that the number of states increases very quickly with the size of the system (for example, a system with N components, if each component has only two states (working, failed) may have 2 states !). Moreover, a slight modification of the hypotheses about the system thouroughly changes the graph ! This is why we have developed :

1) a reliability calculation method /6/, based on sequences of events, that can be used for big graphs (over 10 states), whereas conventional methods are limited to graphs covering about 100 states at most. The "secret" of the method lies simply in the omission of what is negligible, and in the awareness of the extent of what has been neglected.

2) the GSI rule based model /4/,/5/, to replace the transition matrix of the graph.That model contains all the information necessary to build the matrix automatically,but is, of course, much more readable, modular, modifiable... /8/.

II THE GSI MODEL :

Such a model, associated with the specialized inference engine we have developed (Generation of Sequences by Inference), is a real expert system for the system modelled.

By merely introducing minor changes in the facts or rules such information as the system failure probability for different missions, with different initial states..can easily be obtained.

What is this model like ? It includes :

- a list of components and variables of the system, with their initial state.
- 3 distinct rule bases :
  - the interaction rule base describing the propagation of information through the system. Example,

    if water-supply - "none" or
    power-supply - "none" or pump - "failed"
    then pump-flow :- 0

    This is one of the types of rules used in diagnosis problems.(For example, see the "simulation rules" of /9/).

  - the occurrence rule base, indicating what can happen in the current state of the system. Examples,

    if diesel-generator - "operating"
    then possible
    (diesel-generator :- "short-failure"),
    (diesel-generator :- "long-failure")

    if diesel-generator - "required-to-start"
    then possible
    (diesel-generator :- "operating")
    (diesel-generator :- "fail-to-start")

  - the failure rule base, indicating whether the system is failed. Example,

    if (pump-flowl + pump-flow2)<100
    then failure :- "yes"

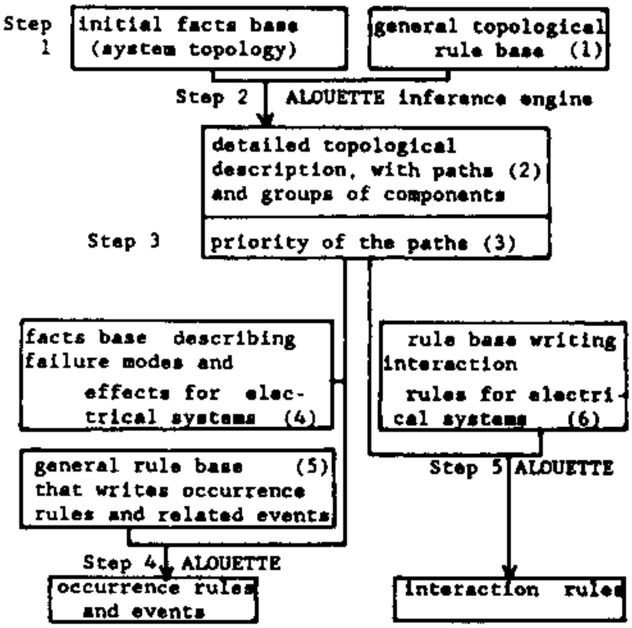
With this qualitative knowledge, GSI can automatically generate the sequences between any given initial state of the system and a failed state. If, moreover, the occurrence rates of the events listed in the occurrence rules are entered into GSI, it can compute their probabilities. An expert system has then been created for the studied system.

III ENTERING THE RELIABILITY ENGINEERS' KNOWLEDGE

GSI is a general tool which, itself, does not contain knowledge about the studied systems. So, it is interesting to automate the writing of the GSI model as much as possible by using an expert system. So far, we have created such a knowledge base for power supply systems, and we are going to describe its use.

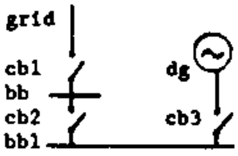
To implement that knowledge-base, we have used the general-purpose ALOUETTE inference engine./?/.

The following diagram shows the different steps (automatically linked) of the creation of a complete GSI model, using the expert system.



GSI model

Here, this general procedure is illustrated by an example of a very simple system:



<u>First step</u> :

The user defines the topology of the system and the nature of its components, which obviously is the minimum information that can be given to describe a system.

Here are examples of facts taken from the description for the above example :

```
( grid , next-item , cbl )
( cbl  , next-item , bb  )
( bbl  , target , yes )
( grid , source , yes )
( dg   , source , yes )
( grid , nature , grid )
( bb   , nature , busbar)
( dg   , nature , diesel-generator )
( cbl  , nature , circuit-breaker )
```

Step 2 :

A general rule base (1) (56 rules), valid for any electrical or hydraulic system, builds the paths from a source to a target using these initials facts. This rule base is also used by EXPRESS. In our example, two paths are created : bbl-by-grid and bbl-by-dg.

Step 3 :

At this point, the user must indicate the priorities of the different possible paths to the expert system.
In our example, he will have to enter the two facts :

```
( bbl-by-grid , priority , 1 )
( bbl-by-dg   , priority , 2 )
```

SteP 4 :

Some general facts (4), valid for any electrical system, are grouped with the facts (2), and (3). They describe all that can happen to electrical components, according to their nature, and their state. For example, a circuit-breaker can open inadvertently, only if it is closed, and operable. This event Involves two variables,which represent :

- the position of the c.b. (closed/open)
- its operating state (OK / failed)

This is described in the facts base by the following facts :

```
( circuit-breaker, failure-mode , inadv-opening)
( inadv-opening, initial-condition , initl )
( inadv-opening, Initial-condition , init2 )
( initl , name , component )
( initl , value, OK )
( Init2 , name , state )
( init2 , value , closed )

( inadv-opening, result, resull )
( Inadv-opening, result, resul2 )
( resull , name , component )
( resull , value, failed )
( resul2 , name , state )
( resul2 , value, open )
```

The other failure modes taken into account so far are :

- stuck-open or stuck-closed circuit-breakers
- short-circuits on the grid, the transformers, the bus-bars
- loss of power on the grid
- diesel generator failure to start upon demand and while operating.

The description adopted for failure modes makes it easy to introduce new ones ; for example, it may be useful to distinguish between the different failure modes of the same component according to the different repair times of the various failures.

A general rule base (5) (37 rules), valid for any system, uses the above-mentioned description and the whole topological facts base (2)+(3) to automatically generate the occurrence rules and the description of the events GSI needs.
For example, with the above mentioned failure mode, this rule base will write the following occurrence rule, concerning cbl :

```
if cbl = "OK" and cbl-state = "closed"
 then x possible
```

where x is just the reference number of the corresponding event, with its description :
comment that will appear in GSI outputs, translation in GSI language, and failure rate.

```
x : inadvertent-opening of cbl ;
 cbl := "failed" and cbl-state := "open" :
 1.E-6
```

__Step 5__ :

A rule base (6) (57 rules) containing knowledge about electrical systems, generates the GSI interaction rules.
Here are some interactions that are taken into account in the model :
all the possible paths from sources to targets are identified, and among them,the path with the highest priority is chosen. A path is "possible" if all its components are operable.
The priorities will be expressed by rules such as :

```
if bbl-by-grid = "possible"
   and bbl-by-dg = "possible"
then path-bbl-by-grid := "chosen"
```

Once a path has been chosen, if it is different from the actually used path, orders are given to the circuit breakers by rules such as :

```
if path-bbl-by-dg  =  "chosen" and
   cb2-state = "closed"
then cb2 := "ordered-to-open"

if path-bbl-by-dg = "chosen"
   and cb3-state = "open"
   and cb2-state = "open"
then cb3 := "ordered-to-close"
```

These rules are linked : they specify that the circuit-breaker cb3 can not be closed before the opening of cb2.
The ALOUETTE rule which generated these two rules is presented below :

```
if nature(p) = path,
   member(p) = (x1),
   nature(x1) = circuit-breaker,
   next-item(x1) = (y),
   nature(x2) = circuit-breaker,
   (x2) <> (x1),
   next-item(x2) = (y),
   source(p) = (s),
   target(p) = (t).
   then
   write 'if ', t,'-by-',s,' = "chosen"'
   write ' and ', x2,'-state = "closed"'
   write ' then ' , x2 , ' := "ordered-to-open"'
   write 'if ', t,'-by-',s,' = "chosen"'
   write ' and ', x1,'-state = "open"'
   write ' and ', x2,'-state = "open"'
   write ' then ' , x1 , ' := "ordered-to-close"'
```

Once the whole GSI input file has been generated, GSI can be run ; it automatically gives the reliability of the system, and the most probable sequences. This is very useful to detect the weak points of the system.

In our example, GSI generates the following interesting sequences, showing the effects of incorrect responses of the circuit-breakers, (their numbers refer to their places in the output file, where they are arranged in decreasing order of probability. The total number of sequences with no repair is 155.)

```
short-circuit of grid * 9.87E-6 *
opening of cbl        *         *
cb2 stuck-closed      *         *
          :           *         *
short-circuit of grid * 9.86E-6 *
cbl stuck-closed      *         *
opening of cb2        *         *
closing of cb3        *         *
dg fails to start     *         *
```

For our very simple example, the general knowledge of the expert system proved to be sufficient to describe all the functioning rules of the studied system.

Of course, it is not always true, for an obvious reason : the expert system is given only minimum information describing an electrical system, and, of course, it can not guess its particular features.

This is why a review of the automatically created GSI model is necessary. At this point by slight modifications, the user can easily introduce for instance the repair priorities (a frequent type of dependencies), the fact that a certain circuit-breaker has a higher failure rate than the others, because it works under adverse conditions....etc (See /4/,/8/ for a full example of GSI model and of effects of modifications) .

IV PERFORMANCES

* A "hand-made" GSI model has been built for the 6.6kv power supply of the Paluel French nuclear power plant. 3.5 engineer-months were required to develop this model and find all the results. By conventional methods, it had taken 8 enginneer-months.

Of course many other results were simultaneously obtained. The model includes 30 components ; each of them has at least 3 states (for example : operable, short failure, long failure).

This model is run some 2' on an IBM 3090 with a probability threshold that gives a satisfactory precision. The number of selected sequences is 1677.

* The application of the expert system to a simplified version of the system quoted above, Incorporating ; 10 circuit-breakers, 4 busbars, 2 diesel-generators, 2 transformers, 2 grids, gives the following CPU times for the steps described in section III ;

- step 2 : 10s
- steps 4 and 5 : 13s
- Compilation of the GSI model : 15s
- GSI model run, with a good precision (the neglected sequences represent 1% of the result) : 53s. 1752 sequences were selected.

V CONCLUSION :

The adoption of an easily modifiable, rule-based, quantification model (the GSI model) proved to be very efficient, because it permits a two step modelling procedure.

1) the expert system, from the minimum information needed to describe the studied system, automatically creates a preliminary version of the model.

2) then, the reliability engineer transforms that sketch in a final, very detailed model.

In the design phase of a system, the first step provides enough information, and is quick enough. It takes less than one hour to change some facts in the topological description of the system and spot the weak points of the new design.

In a detailed reliability study, It is possible to go much further by refining the GSI model. But the time needed is still negligible, when compared to the time that it would take with conventional methods.

REFERENCES :

/1/ G.E. APOSTOLAKIS - S.L. SALEM - J.S. WU - CAT : a computer code for the automated construction of fault trees. EPRI report NP 705 1978.

/2/ J. ANCELIN - E. CHATY - M. CARRE : Notice d'utilisation du code GO d'analyse automatique de la fiabilite. EDF report HT-13-34-81 1981.

/3/ M. GONDRAN - J.F. HERY - J.C. LALEUF : Une aide aux etudes de fiabilite par systemes experts. 5th international conference on reliability and maintenability. BIARRITZ, October 1986.

/4/ M. BOUISSOU : Recherche et quantification automatiques de sequences accidentelles pour un systeme reparable. 5th international conference on reliability and maintenability. BIARRITZ, October 1986.

/5/ M. BOUISSOU Une approche systeme expert dans les etudes de fiabilite : l'algorithme GSI. (generation de sequences par inferences). EDF report HT-13-85-85 November 1985.

/6/ M. BOUISSOU : Nouvelle methode de calcul de la fiabilite par les sequences d'etats dans un graphe d'etats - le programme GRAFFITI- EDF Report HT/13/18/84 October 1984.

/!/ D. MULET-MARQUIS, P. BENHAMOU : ALOUETTE : un environnement logiciel pour 1'utilisation de bases de connaissances. EDF Report HI/5302/02 January 1986.

/8/ M. BOUISSOU : Comparaison entre une etude de fiabilite classique, et 1'equivalent utilisant GSI : Exemple du 6.6 kv de la centrale de Paluel EDF Report HT/53/1/86. soon to be published.

/9/ R. DAVIS Diagnostic reasoning based on Structure and Behaviour. Artificial Intelligence vol 24 pp 347-410 (1985).