Collection de notes internes de la Direction des Etudes et Recherches

POURQUOI LES TECHNIQUES MARKOVIENNES ONT ETE UTILISEES PAR EDF DANS L'ETUDE PROBABILISTE DE SURETE DE LA CENTRALE DE PALUEL ?

WHY MARKOVIAN TECHNIQUES WERE USED IN EDF'S PSA OF PALUEL ?

EDF
Electricité de France

EDF
Electricité de France

Direction des Etudes et Recherches

SERVICE RÉACTEURS NUCLÉAIRES ET ECHANGEURS
Département Etudes de Sûreté et de Fiabilité

Février 1991

DUBREUIL CHAMBARDEL A.

POURQUOI LES TECHNIQUES MARKOVIENNES ONT ETE UTILISEES PAR EDF DANS L'ETUDE PROBABILISTE DE SURETE DE LA CENTRALE DE PALUEL ?

WHY MARKOVIAN TECHNIQUES WERE USED IN EDF'S PSA OF PALUEL ?

Pages : 10

92NB00029

Diffusion : J.-M. Lecœuvre
EDF-DER
Service IPN, Département SID
1, avenue du Général-de-Gaulle
92141 Clamart Cedex

ISSN 1161-0611

SYNTHÈSE :

Cette note présente trois exemples d'évaluation de système réalisés lors de l'étude probabiliste de sûreté de la centrale de PALUEL, où les techniques Markoviennes ont dû être appliquées pour diverses raisons.

Les méthodes utilisées sont brièvement décrites ainsi que leurs avantages et inconvénients techniques.

Enfin, cette note présente les développements de la méthode en cours à EDF.

3/4

EXECUTIVE SUMMARY :

This paper presents three examples of system assessments made on occasion of a probabilistic safety assessment in PALUEL power plant, for which the Markovian techniques had to be used due to various reasons.

The methods used are briefly described as well as the technique advantages and drawbacks. Lastly, this paper gives the developments brought about by EDF.

WHY MARKOVIAN TECHNIQUES WERE USED IN EDF's PSA of PALUEL?

INTRODUCTION

Electricité de France has carried out a large-scale Probabilistic Safety Assessment of PALUEL power plant from 1986 to 1989. The assessment widely used Markovian techniques to study the reliability of electric, thermohydraulic or control systems.

THE UTILIZATIONS

Let us take three examples :

The first one relates to the Component Cooling System (CCS) reliability study.

The CCS is operated continously and comprises two different paths which each consist of two pumps and two half-exchangers.

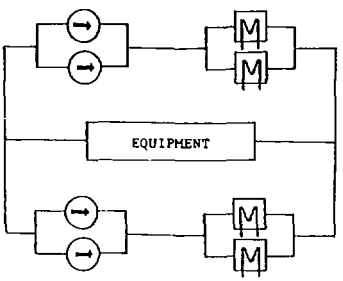

FIG. 1. CCS flow diagram

Only one pump is in service. If it fails to operate, the other pump on the same path starts. If they both fail to run, a pump starts on the other path and the equipment cooling is switched to this path. For increased safety, the operator shifts to another pump so that the number of startups and operating hours be equivalent for each pump.

Each pump operating time consequently varies with:

- the other pumps' operating time,
- the repair time,
- the shifting frequency for the line in service.

Assessing the reliability of a single pump is, therefore, impossible without taking the availability of the other pumps into consideration.

The Markovian graphs, which take account of the time relations, are particularly well-suited to such a study.

By way of example, the probability for a yearly total loss of the CCS system as modelled by a Markovian graph is 2.5 10-5. It would have been 1.5 10-3, and, then, overestimated by a factor of 60, if the CCS system bad been modelled by means of a fault tree (where all the components are assumed to be simultaneously operated).

The second example relates to the Digital Integrated Protection System (DIPS) which manages the major information delivered by protection transducers and initiates the saving action through four Redundant Acquisition Processing Units (RAPU).

The DIPS is permanently operated. There can be two types of failure. The first one, which can be detected through self-checking, makes the RAPUs' redundancy level fall from 2/4 to 1/3. The other one, which cannot be detected by self-checking, makes this level fall without the operator's knowledge. These failures are detected by periodical testing.

Each RAPU has several "operation" steps, namely:
- a real-operation step (protection transducer monitoring),
- a testing step,
- a repair step (where needed),
- an operation step...

The testing steps of the RAPUs are staggered, and each RAPU's operation is then modelled by means of a graph over each of its operation steps.

After a few cycles (about thirty, so that the probabilities of the graph states converge toward the probabilities of steady states), the simultaneous outage of several RAPUs making the delivery of a protection signal fail, is considered.

For this purpose, all the RAPU's graphs are aggregated into a single graph.

Certain fault tree processing code like PHAMISS developed by ECN (Netherlands) allow components to be taken into account with staggered tests. However, the components have only two possible alternative states (in service or not); the DIPS system components have three states:
- in service
- failure detected, test or repair (the redundancy being 1 in 3)
- undetected failure (the redundancy being 2 in 3)

In addition, there may be exponential (failure or repair) or constant time (testing or operation step) transition laws, which is more than current fault tree processing codes allow.

Lastly, all the possible states of the four RAPUs, and not only their failure state, are of interest. On each emergency shutdown request, each RAPU requests the opening of two out of the 8 trip breakers. The undetected outage of RAPU disables the two associated circuit-breakers. When detected, the failure makes the two circuit-breakers switch off.

All the RAPU outage cases must be combined with the failure of the available trip breakers to assess the emergency shutdown failure probability. This is made possible using only graphs whereas as many fault trees as RAPU outage combinations would be necessary.

Assessments through fault trees being impossible, no comparison of the results achieved using the two methods has been made.

The third example relates to the study of the 6.6 Kv total emergency supplied distribution loss or voltage loss on the two LHA-LHB switchboards.

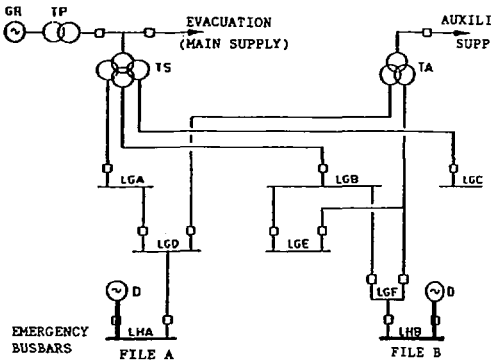

FIG. 2. 6.6 kV distribution system

The two LH switchboards are supplied from the main power line via the stepdown transformer (ST). If the main power line ceases to function, the LH switchboards supply switches to the auxiliary transformer (AT). In case of auxiliary power supply failure, the two LH switchboards are supplied from their own diesel generating set. Additionally, local actions allow the resupply of a unit from an adjacent one within an hour.

Many configurations exist for the electric distribution. Its loss being assessed over one year, there are many possibilities for equipment repair. The equipment required operating time much varies (from a few minutes to one year), which justifies the use of Markovian techniques.

Besides, the duration of the voltage loss and the state of the reactor at that time must be known to assess the consequences of the voltage loss upon the LH switchboards from the viewpoint of core meltdown.

The operating specifications prescribe to switch a unit formerly operated at its nominal power, to a RHRS state as soon as the electric distribution is low enough. The time between the application of specifications and the total distribution loss can, therefore, be used to switch the unit to RHRS conditions.

The loss of emergency supplied voltages is quantified by detecting the sequences (successive failures and repairs) leading from the steady-state operating conditions to the failure conditions. Each sequence is "distributed" over the event trees used for modelling accident scenarios resulting from the voltage loss (each event tree corresponding to a well-

defined state of the reactor operated at its nominal power or under RHRS conditions..). A specific failure state, and, consequently, a given power source restoring time, correspond to each sequence. The event trees are then quantified separately for each initiating sequence, the assessment taking account of the possible elimination of the initiator (see [1]).

A quantification of the loss of emergency supplied electric voltage as close as possible to the real operating conditions and as detailed and accurate, would have been very hard to achieve in the absence of Markovian techniques and, principally, much less resistant to the changes in reliability data or functional hypotheses.

As an indication, the PSA made on PALUEL power plant involved the use of 200 fault trees, 300 event trees and 1300 Markov graphs (in particular, for studying the long-term results of primary breaks).

In addition to the above mentioned systems, the auxiliary feed water system, the safety injection system and that used for containment spray in case of long required operating time have been modelled with the aid of Markov graphs.

THE METHODS USED

We have used the conventional Markov graph construction techniques, namely:

- Construction of macro-components for complex systems,
- Counting of all the system possible states,
- Definition and computation of the transition rates from one state to another in the graph (and possibly using small-size fault trees for modelling and quantifying the transition rates if macro-components are to be used),
- Quantification of the graph using a matric or sequential method (see the end of the paragraph).

Introducing the common mode failures is easy:

Example:

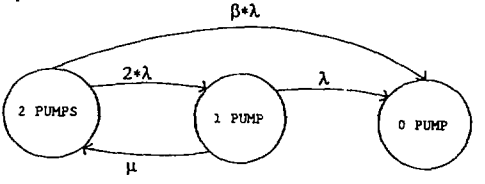

FIG. 3. Markov graph for two pumps running simultaneously

where λ : failure rate of a pump
β : common mode failure rate of two pumps
μ : repair rate of a pump.

"Run-start" common mode failures have been introduced for the components operated under normal-standby conditions (a component in service, the other on standby which starts in case that the first one fails to operate). These failures correspond to the failure to operate of a component, and to the loading failure of one (or more) component due to a common mode failure.

Example:

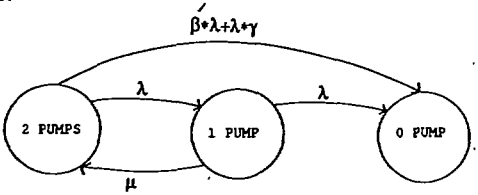

FIG. 4. Markov graph for two pumps running under normal/standby conditions

where γ : loading failure rate of a pump
β : common mode failure rate
"Run-Start" of the two pumps

A major problem raised by the use of Markov graphs is that the number of graph states grow exponentially with the number of components.

The graph of a system with n components, each having two states (on-off) may have 2n states, failing any simplification.

EDF has chosen to use an inferential sequence generator (ISG [2]). There is no description of the graph, but only of the "occurrence rules" allowing the happenings to be defined as a function of the system state, the "interaction rules" enabling the effects of an event to affect the whole system, and the "failure rules" allowing one to establish whether the system is operative or not in a given state.

The ISG code permits local exploration into a graph type model without any need for building it entirely. It generates the sequences (successive failures and repairs) from the proper operation state to the failure state.

The systems under study can thus correspond to graphs of unlimited size. The number of rules drafted varies with the number of components in a quasi linear manner.

The only limitation is the number of explored sequences which must be held within reasonable values owing to CPU reasons. It is limited by a probabilistic cut off and a length criterion (maximum number of transitions in a sequence).

ADVANTAGES AND DRAWBACKS OF THE MARKOVIAN TECHNIQUES

The use of the Markovian techniques within the scope of the PSA 1300 is grounded on EDF's intent to have realistic, detailed probabilistic models available for further carrying out of sensitivity study owing to these techniques:

- the repairs of components can be taken into account (certain fault tree processing codes also, but there are not so many),
- the reliability and availability computations can be carried out (same remark as above regarding the fault trees),
- the normal/standby operating sequences and, more generally, all the changes in the configuration of the system under study can be considered,
- multistep system operating sequences (the system mission and/or configuration vary with each step) can be taken into account.

In addition, the sequential computation of a graph allows the visualization of the progress of alternate failures and repairs as time

passes, leading to system failure, and the computation of the probability of measures being taken before the complete loss of the system (operator' action, switching of the reactor to a RHRS state...).

Using Markovian techniques is made uneasy due to the complexity of the graphs to be processed in case of complex systems. The techniques applied for state aggregation which aim to minimize the number of states or sequential computations in order not to build the complete graph, general permit the problem to be reduced to a reasonable size. The simplification however, are sometimes hard to control since they involve approximations.

Major works upon the state aggregation in the Markovian procedures have started [3]. They are intended to define the appropriate aggregation techniques and to develop a simple method for computing a majorant for the error resulting from aggregations.

The works have proven that the error due to aggregations might be very important if the latter were not judiciously defined (over- or under-evaluation of the results of one (or more) decade). Conversely, the errors are only a few percent if two values (one for short operating times, the other for long operating times) are selected for equivalent failure and repair rates of macro-components.

A rapid method for computing the error made when using conventional aggregation methods has been developed and has proven to be very accurate (a few percent of error over the initial error).

CONCLUSIONS

The use of Markovian techniques allows much more realistic modelling than fault trees, for repairable systems that have a variable configuration or a role which changes as time passes.

The Markovian models must often be simplified, or processed in a simpler way, owing to sizing problems, which implies a few approximations. Most often, the latter are much lower, provided that the modelling be properly made, than those induced by modelling applying a fault tree type method which disregards the time dependences and obliges to avoid a few failures out-of-hand (for example, the long-term loss of safety injection or containment spray systems after a primary break: the French PSAs study these scenarios over a one-year period).

The Markovian techniques often are much profitable and, in some cases essential though they must be applied deliberately. This explains why EDF wants to plant method-selection aid tools for establishing a reliability engineer's work station (a complex plant could thus be automatically broken down into package units which would probably not represent its constituent systems. Each unit would be processed through the appropriate method).

Electricité de France will, therefore, intensify the utilization of these techniques.

REFERENCES

1. A. Villemeur, M. Bouissou and A. Dubreuil Chambardel, Accident sequences: methods to compute probabilities (PSA'87-Zurich)
2. M. Bouissou, Un outil général d'évaluation de la fiabilité et disponibilité des systèmes complexes : présentation du logiciel GSI, (EDF memorandum)
3. F. Kervegant and A. Dubreuil Chambardel, Estimation des approximations engendrées par les agrégations d'états dans les processus Markoviens, (EDF memorandum)