Unavailability Evaluation and Allocation at the Design Stage for Electric Power Plants : Methods and Tools

Marc Bouissou & Eric Bourgade • EDF (Electricité de France) • Paris

Key Words : Availability, reliability, allocation, electric power plant, optimization, life-cycle cost

SUMMARY & CONCLUSIONS

Electricité de France is currently carrying out a project called CIDEM with the objective of integrating availability, operational feedback, and maintenance in the design of future power plants (especially nuclear power plants) in order to improve their profitability. The work reported in this paper was performed in the framework of the research part of the CIDEM project, managed by the R&D division of EDF.

The paper shows that the availability assessment of an electric power plant raises a number of specific modeling problems.

These problems are especially acute in the case of nuclear plants, for which safety procedures can affect availability.

In fact, a dynamic simulation model could easily take into account all the particular features of the plant operation. But the quantification of such models (which are not Markovian) necessarily relies on Monte-Carlo simulation, and thus is rather slow.

Computation times could still be acceptable for **evaluation** purposes. But in the design stage, we need to **allocate** the global objectives (in terms of availability, costs) to the main functions and/or components of the plant.

If the system to be studied is a bit more complex than a simple series assembly of components (which means that the sum of the components' unavailabilitites is a fairly good approximation of the global unavailability), doing an allocation requires numerous evaluations. This makes the use of a simulation model totally unthinkable.

This is why we have chosen to use only fault-tree models, *in spite of the fact that they are essentially static models*: they can be calculated in very short times, especially with the new generation of fault-tree processing codes, based on BDDs (Binary Decision Diagrams).

The paper gives the modeling schemes we had to devise in order to take into account various dynamic features, along with an estimation of the corresponding errors.

It also gives a quick description of the tools we use to carry out real studies : the FIGARO workbench, which enables the building of knowledge bases to automate the fault-tree construction, and the ARPO tool, to perform allocation, with two different methods.

1 - INTRODUCTION

The CIDEM project, which involves several EDF divisions, is aimed at developing a design process applicable to a future nuclear reactor (REP 2000 project), taking into account availability, doses, and maintenance cost goals.

The Tender Design of this reactor, the nuclear island of which is a Franco-German design, began in February 1995, and is scheduled to be completed in 1997.

In connection to this, the CIDEM team of the Engineering & Construction and Generation & Transmission Divisions is in charge of the validation of the project options proposed by NPI, the designer, with regard to the design goals.

In order to guarantee the coherence and rapidity of these validation activities, the R&D division has been working since 1993 on a project whose objectives are to develop methods and tools, including an information system.

At the present time, the global process is not yet precisely defined, although a preliminary version has been proposed[1]. However, some (partial) problems have led to operational solutions. Availability assessment and allocation are among them, and this paper gives the solutions that we have chosen.

It is organized as follows :

- section 2 defines the scope of the paper,
- section 3 lists the typical features one has to model when he wants to assess the availability of any power plant,

- section 4 lists the additional features one has to model when he wants to assess the availability of a nuclear power plant,
- section 5 is about reliability data,
- section 6 gives a brief description of the tools we use.

2 - SCOPE

This paper exclusively addresses the problem of forced plant outages due to random failures which occur during the normal operation of the plant. We neither consider planned unavailability, nor the transient stages of the restart, after a refuelling period. We only consider asymptotic availabilities.

In this context, we call:

- **availability allocation** the fact of assigning availability objectives to the components, such that the global availability goal for the plant is met, at a reasonable, if not minimal, cost.

- **availability evaluation** the quantification of the plant forced unavailability as a function of the components' availabilities.

Obviously, we need operational feedback data for both problems. In the case of allocation, it is necessary to rely on such data, in order to assign realistic objectives to the components.

We assume that all components have constant failure and repair rates, for each failure mode (a component may have several failure modes, which induce different effects on the system).

This means that for a given failure mode, with a failure rate λ, and a repair rate μ, the asymptotic unavailability equals: $\frac{\lambda}{\lambda + \mu} \cong \frac{\lambda}{\mu}$ if $\lambda << \mu$.

For the sake of the rapidity of the evaluation, we want to use a simple, static model: a fault-tree. The quantification of this kind of model assumes two important facts:

- s-independance of basic events

- an instantaneous propagation of the effects of the components' failures through the fault-tree

Unfortunately, there are dependences between components, due, for example to the existence of cold redundancies, and there is no simple, instantaneous relation between the state of the components, and the state (producing electricity, or not) of the plant. This means that none of the above mentioned hypothesis are fulfilled !

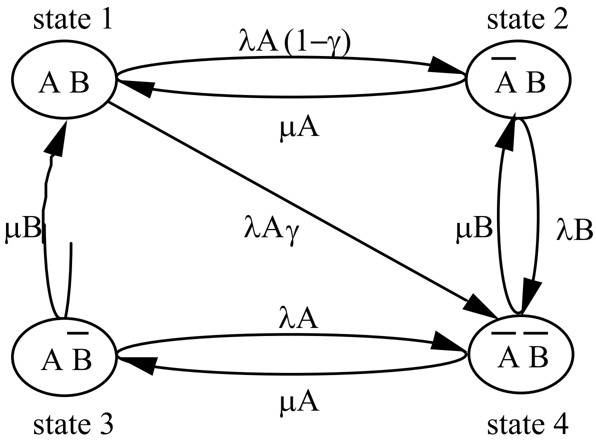
In the next sections, we will explain the solutions we have used to handle this problem, and evaluate the approximations they imply.

3 - DYNAMIC FEATURES OF ELECTRIC POWER PLANTS IN GENERAL

3.1 - Cold redundancies

a) Let us consider the case of two components A and B, where B is a cold redundancy for A

The dynamic behaviour of this mini-system is properly described by the following Markov graph, which takes into account the fact that the state of B depends on the state of A. (B may refuse to start with a probability γ). We assume that the repair rates are the same for a failure on demand and a failure during operation.



The steady-state equations representing this graph are as follows:

$$\begin{cases} -\lambda_A\pi_1 + \mu_A\pi_2 + \mu_B\pi_3 = 0 \\ \lambda_A(1-\gamma)\pi_1 - (\lambda_B + \mu_A)\pi_2 + \mu_B\pi_4 = 0 \\ -(\lambda_A + \mu_B)\pi_3 + \mu_A\pi_4 = 0 \\ \lambda_A\gamma\pi_1 + \lambda_B\pi_2 + \lambda_A\pi_3 - (\mu_A + \mu_B)\pi_4 = 0 \end{cases}$$

with $\sum_{i=1}^{4} \pi_i = 1$ (π_i: probability that the system is in state i)

Then we obtain the following unavailability for the system:

$$\overline{A}_{syst} = \pi_4 =$$

$$\frac{\lambda_A}{\lambda_A + \mu_A} \cdot \frac{(\lambda_B + \mu_A\gamma)(\lambda_A + \mu_B)}{\lambda_A(\lambda_B + \mu_A\gamma) + \mu_B(\lambda_A + \lambda_B + \mu_A + \mu_B)}$$

$\overline{A}_{syst}$ can be considered as a product $\overline{A}_A K$ where :

$\overline{A}_A = \frac{\lambda_A}{\lambda_A + \mu_A}$ is the steady-state unavailability of A, and:

$$K=\frac{(\lambda_{\mathrm{B}}+\mu_{\mathrm{A}}\gamma)(\lambda_{\mathrm{A}}+\mu_{\mathrm{B}})}{\lambda_{\mathrm{A}}(\lambda_{\mathrm{B}}+\mu_{\mathrm{A}}\gamma)+\mu_{\mathrm{B}}(\lambda_{\mathrm{A}}+\lambda_{\mathrm{B}}+\mu_{\mathrm{A}}+\mu_{\mathrm{B}})}$$

Let us study $K(\gamma)$ by calculating its derivative:

$$K'(\gamma)=\frac{\mu_A\mu_B(\lambda_A+\mu_B)(\lambda_A+\mu_B+\lambda_B+\mu_A)}{\left[\lambda_A(\lambda_B+\mu_A\gamma)+\mu_B(\lambda_A+\mu_B+\lambda_B+\mu_A)\right]^2}$$

Since $K'(\gamma)\rangle 0, \forall\gamma \in[0,1]$, we infer that $K(\gamma)$ is a monotonic, increasing function on [0,1] with:

$$K(0)=\frac{\lambda_B(\lambda_A+\mu_B)}{(\lambda_A+\mu_B)(\lambda_B+\mu_B)+\mu_A\mu_B}$$

$$K(0)=\frac{\lambda_B}{(\lambda_B+\mu_B)+\dfrac{\mu_A\mu_B}{(\lambda_A+\mu_B)}}$$

$$K(1)=\frac{\lambda_B+\mu_A}{\lambda_B+\mu_B+\mu_A}$$

So, we have

$$K(0)\langle\frac{\lambda_B}{\lambda_B+\mu_B}\langle\langle K(1)$$

The expression $\dfrac{\lambda_B}{\lambda_B+\mu_B}$ is nearer to $K(0)$, which corresponds to the most frequent situation ($\gamma\cong 0$).

This suggests the following simple approximation:

$$\overline{A}_{syst}=\overline{A}_A K(\gamma)\cong\overline{A}_A\frac{\lambda_B}{\lambda_B+\mu_B}$$

This approximation, corresponding to an active redundancy of A and B, can easily be obtained by a fault-tree.

Furthermore, one can notice that, based on the hypothesis that the failure rates are much smaller than the repair rates (but without any particular hypothesis about the failure on demand rate), a good approximation of K is:

$$K1=\frac{\lambda_B+\mu_A\gamma}{\mu_B+\mu_A}$$

We can deduct from this expression that taking the expression $\dfrac{\lambda_B}{\lambda_B+\mu_B}$ instead of K, one:

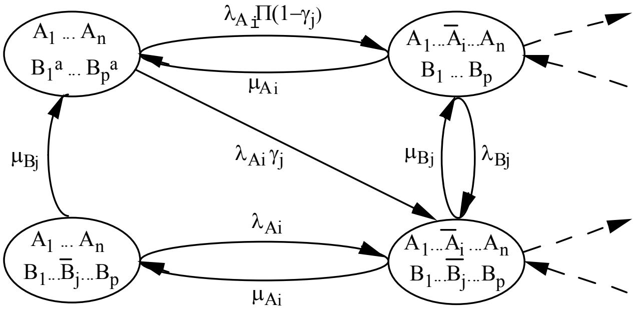
- **overestimates** the unavailability of the system (A, B), at most by a factor around 2, when γ is at most of the same order of magnitude as $\dfrac{\lambda_B}{\mu_A}$, and otherwise,
- **underestimates** it by a factor $\dfrac{1}{2}\dfrac{\gamma}{\lambda_B/\mu_A}$, which can be very large.

We have checked that with failure data of thermohydraulic components, the approximation is acceptable. Moreover, if it was not acceptable, this would mean that the failure on demand rate is so large, that the best policies for the system operation is to have both components working all the time !

So far, we have considered only the case of two elements. In fact, a much more common configuration is a redundancy of two trains, each train being a series assembly of components. One of the trains plays the role of component B in the previous example. It is supposed to start whenever the "normal" train breaks down.

b) We now consider the case of two trains ($A_1,\ldots,A_n$) and ($B_1,\ldots,B_p$) with a cold redundancy : as soon as one of the A_i fails, the stand-by train B_j has to start. Any of the B_j may refuse to start, or fail in operation.

We can compute an approximation of the steady-state unavailability of this system by adding the unavailabilities corresponding to all the paths going from the initial state to the failure state in the following Markov graph, according to the method described in [2].



We neglect the states where more than one component is failed on a given train.

For given i and j, we obtain the following contribution I_{ij} to the system unavailability:

$$I_{ij}=\frac{\lambda_{A_i}\gamma_j}{\mu_{A_i}+\mu_{B_j}}+\frac{\lambda_{A_i}\Pi(1-\gamma_j)\lambda_{B_j}}{\mu_{A_i}(\mu_{A_i}+\mu_{B_j})}$$

$$= \frac{\lambda_{A_i}\left[\mu_{A_i}\gamma_j + \Pi(1-\gamma_j)\lambda_{B_j}\right]}{\mu_{A_i}(\mu_{A_i}+\mu_{B_j})}$$

$$\cong \frac{\lambda_{A_i}\left[\mu_{A_i}\gamma_j + \lambda_{B_j}\right]}{\mu_{A_i}(\mu_{A_i}+\mu_{B_j})}$$

From this, we infer an approximation of the system unavailability:

$$\overline{A}^{appr}_{passive} = \sum_{i=1}^{n}\left(\frac{\lambda_{A_i}}{\mu_{A_i}}\sum_{j=1}^{p}\frac{\mu_{A_i}\gamma_j + \lambda_{B_j}}{\mu_{A_i}+\mu_{B_j}}\right)$$

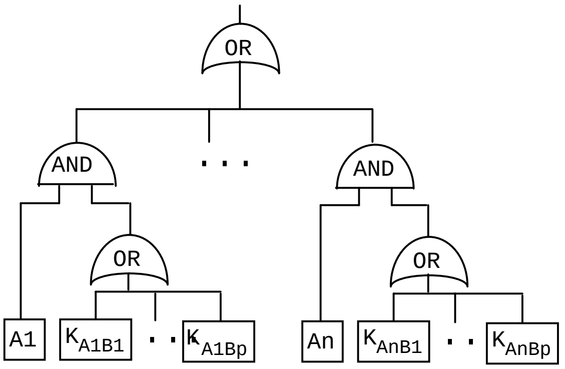
$$= \sum_{i=1}^{n}\left(\frac{\lambda_{A_i}}{\mu_{A_i}}\sum_{j=1}^{p}K_{A_iB_j}\right)$$

If we had considered the redundancy as active, taking the classical approximation of the sum of the unavailabilities of the minimal cutsets, we would have obtained the following expression:

$$\overline{A}^{appr}_{act} = \sum_{i=1}^{n}\left(\frac{\lambda_{A_i}}{\mu_{A_i}}\sum_{j=1}^{p}\frac{\lambda_{B_j}}{\mu_{B_j}}\right)$$

The form of these two expressions, if we compare it to the simple case of only two components, suggests that similar conclusions can be drawn, in regards to the validity domain of the approximation.

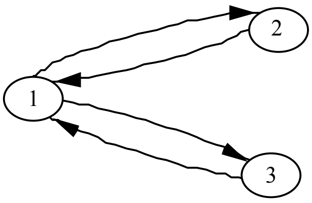
In cases where the fact of considering the stand-by train as if it was an active redundancy leads to an unacceptable approximation, there is still a possibility to use a fault-tree model, in which the coefficients $K_{A_iB_j}$ are represented by ficticious components. Here is this fault-tree, the quantification of which (by the sum of the cutsets probabilities) gives the expression $\overline{A}^{appr}_{passive}$.



3.2 - *Components working intermittently*

Some components do not work continuously, but from time to time, like safety valves in order to eliminate temporary overpressures. The (more or less) random process of the opening or closing demands will be modelled as a Poisson process with a parameter of ν.

The failures of such components may happen either when they open (with probability γ_{RO}), or when they close (with probability γ_{RC}) This can be modelled by the following Markov graph, where state 1 represents a correct function, state 2 represents the repair process consecutive to a failure to open, and state 3 represents the repair process consecutive to a failure to close:



The transition rates are as follows:

1 -> 2 : $\nu\gamma_{RO}$	1 -> 3 : $\nu(1-\gamma_{RO})\gamma_{RC}$
2 -> 1 : μ_{RO}	3 -> 1 : μ_{RC}

Using the path approximation again, we obtain the following expression for the steady-state unavailability of the component:

$$\overline{A}^{appr} = \frac{\nu(1-\gamma_{RO})\gamma_{RC}}{\mu_{RC}} + \frac{\nu\gamma_{RO}}{\mu_{RO}}$$

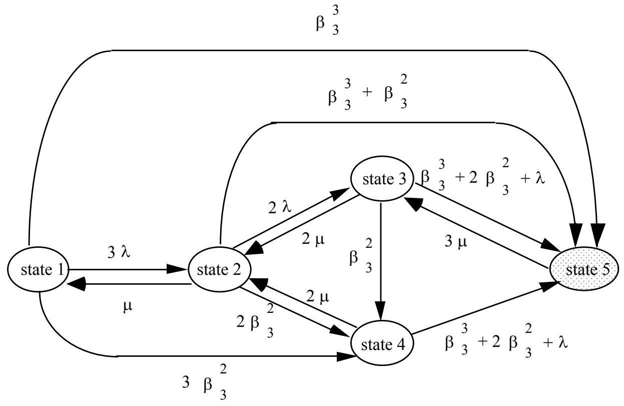
Thus, in order to model such a component in a fault-tree, we use an OR gate, with two sons, the probabilities of which are set to $\frac{\nu(1-\gamma_{RO})\gamma_{RC}}{\mu_{RC}}$ and $\frac{\nu\gamma_{RO}}{\mu_{RO}}$.

The same principle can be applied to any component subject to random challenges.

3.3 - *Common cause failures*

A common cause failure (CCF) induces the simultaneous loss of several components. But, since the components are all damaged, they need individual repairs. The repair process can take different times, depending on the number of repair teams.

In the case of a group of three identical components, we could model the dynamic behaviour of the group, taking into account individual (independant) failures, and common cause failures of all orders, by the following Markov graph, where state 1 is the perfect state, state 2 represents the loss of one component, states 3 and 4 represent the loss of 2 components, and state 5 represents the loss of all three components; β_j^i represents the occurrence rate of an event which causes the failure of i given components in a set of j elements. The transition from state 3 to state 4, which may seem strange at first sight, is represented because even when 2 components are failed, a CCF which would have affected the 2 lost components can still happen.



Again, using the path approximation, we can estimate the steady-state probability of state 5, P_5 by the following formula:

$$P_5 = \frac{3\lambda}{\mu}\frac{2\lambda}{2\mu}\frac{\beta_3^3+2\beta_3^2+\lambda}{3\mu} + \frac{3\lambda}{\mu}\frac{2\beta_3^2}{2\mu}\frac{\beta_3^3+2\beta_3^2+\lambda}{3\mu} + \frac{3\beta_3^2}{2\mu}\frac{\beta_3^3+2\beta_3^2+\lambda}{3\mu} + \frac{3\lambda}{\mu}\frac{\beta_3^3+\beta_3^2}{3\mu} + \frac{\beta_3^3}{3\mu}$$

$$P_5 = \frac{\lambda^2}{\mu^3}(\beta_3^3+2\beta_3^2+\lambda) + \frac{\lambda}{\mu^3}\beta_3^2(\beta_3^3+2\beta_3^2+\lambda) + \frac{\beta_3^2}{2\mu^2}(\beta_3^3+2\beta_3^2+\lambda) + \frac{\lambda}{\mu^2}(\beta_3^3+\beta_3^2) + \frac{\beta_3^3}{3\mu}$$

considering that we should have: $\beta_3^3 \langle\langle \lambda \quad and \quad \beta_3^2 \langle\langle \lambda$

$$P_5 \cong \frac{\lambda^3}{\mu^3} + \frac{3\lambda}{2\mu^2}\beta_3^2 + \frac{\beta_3^3}{3\mu} = P_{Markov}^{appr}$$

Obviously, we cannot find a fault-tree which exactly represents the stochastic process defined above.

However, let us consider the fault-tree defined by the following boolean equations (X_if represents the independant failure of component X, and the symbol "|" stands for "OR"):

Top <=> A_down & B_down & C_down

A_down <=> A_if | CCF_A_B | CCF_A_C | CCF_A_B_C

B_down <=> B_if | CCF_A_B | CCF_B_C | CCF_A_B_C

C_down <=> C_if | CCF_A_C | CCF_B_C | CCF_A_B_C

This fault-tree seems to be a "natural" model of a set of 3 redundant components A, B, C which are subject to CCFs. It has the following minimal cutsets:

CCF_A_B_C

(A_if & CCF_B_C), (B_if & CCF_A_C), (C_if & CCF_A_B)

(CCF_A_B & CCF_A_C), (CCF_A_B & CCF_B_C), (CCF_A_C & CCF_B_C)

(A_if & B_if & C_if)

If each leaf of this fault-tree is considered to be an independant "component", with a failure rate (λ for the "if" leaves, βij for the "CCF" on i components), and a repair rate (μ1 for the "if" leaves, μi for the "CCF" on i components), the quantification based on the cutsets yields:

$$P_{cuts} = \frac{\beta_3^3}{\mu_3+\beta_3^3} + 3\frac{\beta_3^2}{\mu_2+\beta_3^2}\frac{\lambda}{\mu_1+\lambda} + 3\left(\frac{\beta_3^2}{\mu_2+\beta_3^2}\right)^2 + \left(\frac{\lambda}{\mu_1+\lambda}\right)^3$$

$$P_{cuts} \cong \frac{\beta_3^3}{\mu_3} + 3\frac{\beta_3^2}{\mu_2}\frac{\lambda}{\mu_1} + \frac{\lambda^3}{\mu_1^{\ 3}} = P_{cuts}^{appr}$$

Thus, if we choose the following values for the μi: ($\mu_1 = \mu; \mu_2 = 2\mu; \mu_3 = 3\mu$), the quantification of the fault-tree gives about the same result as the quantification of the Markov graph, since the two expressions P_{cuts}^{appr} and P_{Markov}^{appr} become identical.

Surprisingly enough, this fault-tree can also be used as a good approximation in the case of the existence of only one repair team; this hypothesis corresponds to the same Markov graph, with all repair rates equal to μ. A demonstration similar to the previous one shows that in order to take this hypothesis into account, one only has to assign the following values to the μi:

$$(\mu_1 = \frac{\mu}{\sqrt[3]{6}}; \mu_2 = \frac{\sqrt[3]{6}}{2}\mu; \mu_3 = \mu).$$

We have made many approximations in our demonstration. To make it definitely convincing, we give a few numerical examples; table 1, in appendix, is about a system with 3 repair teams, and table 2 is about a system with only one repair team.

The approximations turn out to be remarkably accurate. In fact, the formulas could be simplified even more, because most of the unavailability is due to a simultaneous loss of the three components, by a CCF of order 3. Therefore, one can expect a large influence of the number of repair teams. The difference between the results of the first and second table confirms that influence.

4 - ADDITIONAL DYNAMIC FEATURES FOR NUCLEAR POWER PLANTS

4.1 - Technical specifications

Technical specifications are operation rules which order a plant shutdown in certain situations. They are a means to limit the risk when a component important for the plant safety becomes unavailable.

There are two kinds of technical specifications: without or with conditions on the repair time.

- without conditions: as soon as the simultaneous unavailability of the components of a given set (which can be a singleton) is detected, the plant must be shut down,
- with conditions: the plant must be shut down only when the repair time of the components exceeds a threshold T_0; otherwise, normal operation can proceed.

Technical specifications without conditions are quite easy to model in a fault-tree, by an "AND" gate, the sons of which are the components involved in the technical specification.

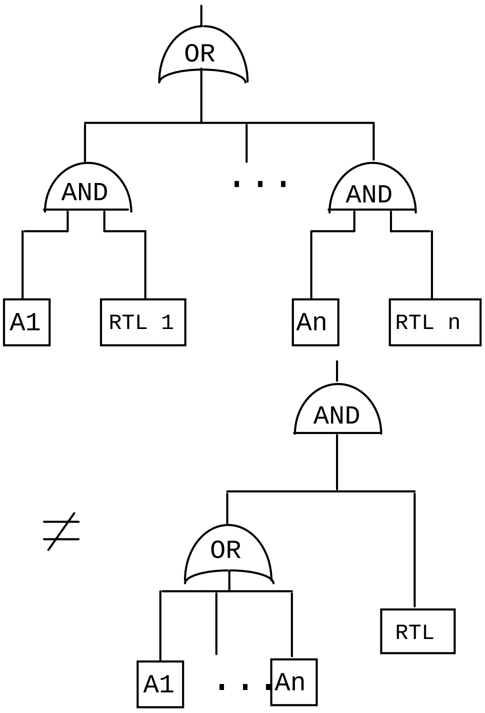
As for those with conditions, ref [9] gives the solution applicable in the case of a single component.

Let *U'* be the unavailability of the plant, due to failures of the component with a repair time greater than T_0 :

$$U' = \frac{\lambda}{\lambda + \mu} e^{-\mu T_0}$$

Therefore, this kind of technical specification can be modeled by an "AND" gate with two sons: the component itself, and a basic event of probability $e^{-\mu T_0}$.

In fact, a component generally has more than one failure mode; this could suggest two different models, which are represented in the figure below:



A1, ..., An stand for the n failure modes of the considered component. RTL1, ..., RTLn stand for the events "repair time too long" (greater than T_0), corresponding to each failure mode. Generally, the repair rates and T_0 are not the same for the different failure modes, and so the fault-tree cannot be factorized in the second form.

4.2 - Taking the plant restart time into account

Depending on the age of the nuclear fuel, and on the amount of poisons (elements which absorb neutrons) in the core, the starting process of the plant may take from 8 hours, to several days.

So, an availability model must take this time into account: in some cases, it may be far greater than the time needed to repair the component which caused a plant outage !

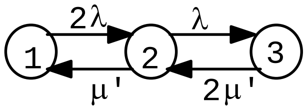
Let us consider the case of a fault-tree model: for minimal cutsets of order 1, the average plant restart time τ can simply be added to the average component repair time.

Unfortunately, if, in order to do so, we add τ to each component repair time, we may get a poor, (but, fortunately, pessimistic) approximation in the case of cutsets of order 2 or more.

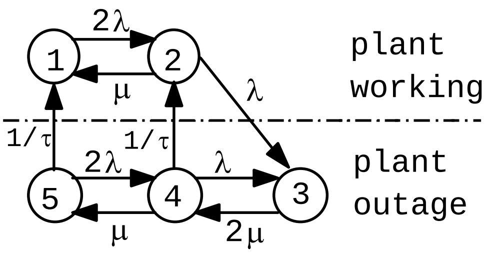
In order to show this problem, let us consider, for instance, a cutset of order 2, such as: failure of components A and B.

If μ_A and μ_B are the repair rates of A and B, let $\mu'_A = \dfrac{1}{\dfrac{1}{\mu_A} + \tau}$ and $\mu'_B = \dfrac{1}{\dfrac{1}{\mu_B} + \tau}$ be the "modified" repair rates. In order to simplify the demonstration, we now suppose that the two components have the same failure rate λ and the same repair rate μ. Therefore, $\mu'_A = \mu'_B = \mu'$

The quantification of the minimal cutset corresponds to the following implicit Markov graph (G1):



In fact, in order to get a correct estimation of the plant unavailability, we should rather use the following model (G2):



The structure of G2 does not allow the use of the path approximation. So we made various sensitivity analysis, which showed that the relative error, calculated by (result of G1 - result of G2)/result of G2 is essentially governed by the product τμ. Here is the result of such an analysis, with $\lambda = 10^{-5}$/h, and τ=24h.

1/μ (h)	relative err.	1/μ (h)	relative err.
1	1174.91%	2	575.68%
4	276.54%	8	128.47%
16	56.18%	32	22.45%
64	7.99%	128	2.51%
256	0.70%	512	0.15%
1024	-0.01%	2048	-0.03%

5 - RELIABILITY DATA

The availability assessment for a nuclear power plant cannot use the same failure (and, maybe repair) rates as a PSA (Probabilistic Safety Assessment). This would be far too optimistic, because in a PSA, minor malfunctions are not considered, as long as they do not endanger the main function of components. In an availability assessment, things are quite different: for example, a small leak may cause a plant outage, especially if it is radioactive. Therefore, the CIDEM project encompasses the definition of a database in which reliability parameters are calculated directly from operational experience, and do not rely on existing PSA databases.

6 - OUR TOOLS

Availability assessment should result in little additional effort for the designers, otherwise it might be performed too late to be useful (or even not at all !). This is why we have developed an approach based on knowledge bases.

This approach starts from a functional analysis of the main power plant functions. These functions are progressively decomposed into sub-functions, until we reach the level corresponding to the principal functions of the "elementary systems" of the power plant (there are about 250 of them in nuclear power plants).

Below this level, the knowledge base intervenes; it contains models of all the thermohydraulic components (pumps, valves, heat exchangers, check valves...) with their failure modes. This knowledge base is written in the FIGARO language, which was specifically designed for dependability assessment. This language is object-oriented, thus permitting the definition of classes and sub-classes (with multiple inheritance) and uses production rules to model the objects behaviour [3].

The FIGARO workbench tools enable the user to graphically input the layout of a system, and to automatically generate a fault-tree from this physical description.

The resulting fault-tree is a means to calculate the unavailability of the power plant induced by the system components unavailabilities. This fault-tree can be used for evaluation *and* allocation.

For probability evaluation, we use the fault-tree processing tool ARALIA. ARALIA is a recent software, developed by the Bordeaux University [4], with funding from 7 French major companies (EDF, ELF-Aquitaine, CEA, Schneider Electric, SGN, Dassault, Technicatome); it is based on state-of-the-art techniques, using Binary Decision Diagrams, that enable exact and particularly quick evaluation of a fault-tree top event probability.

By this technique, each evaluation of the (434 gates, 458 basic events, 130,112 minimal cutsets) fault-tree corresponding to the Chemical and Volume Control System of a nuclear power plant takes only 0.1 seconds on a SUN sparc 5 workstation. A dynamic model, exploited by Monte-Carlo simulation, or even by the most effective Markov solvers, could never reach such a speed.

As for allocation, a careful bibliographical review, performed in 1992 [5], [6], [7] showed that in spite of their apparent diversity, the conventional allocation methods can be classified into two categories only:

- the first category is based on weighing factors, which, most of the time, take into account the structure of the system, or the elements' availabilities (measured on similar components, in existing systems), or both.
- the second one assumes that the global cost of the system is a known function of the availabilities of the components. Then, the allocation consists in finding the availabilities which minimize this cost, under the constraint corresponding to the global availability goal.

In ref. [8], we have proposed a new method of the first category, which implements a synthesis of several methods. According to the choice of a parameter, this method can progressively be modified from a method based solely on the operational feedback, to another one, which gives preference to the structure of the system, therefore trying to avoid the existence of any weak point.

We have also proposed a method of the second category in [8], formulating it in a way as general as possible, and giving justifications for the choices we have made.

Both methods have the remarkable property of being applicable to any structure of system, through a model (usually a fault-tree) which relates the global availability of the system to the components' availabilities.

On these theoretical principles, we have developed a tool called ARPO. This tool integrates the probability evaluation modules of ARALIA, and a general purpose and robust optimization method, the Nelder and Mead "complex" method. Thanks to the use of BDD techniques, ARPO is relatively fast, even with the optimization method. Besides, the set of allocations computed (instantaneously) by the weighing factors method can be used as a starting point for the optimization method, as long as the decision variables are all unavailabilities. The most challenging task in using the optimization method seems to be the collection of data concerning costs.

7 - CONCLUSION

We have shown that, using the various modeling schemes that we have given in this paper, it is possible to build a fault-tree model that gives an acceptable approximation of the contribution of the main systems to the unavailability of an electric power plant. It is even possible to take into account features such as the technical specifications (which are specific to nuclear power plants).

To implement these ideas, we have built a knowledge base, in the FIGARO language, which can thus be used with the FIGARO workbench. This knowledge base allows the user to derive automatically a fault-tree according to the principles we have given, from a graphical input of the physical layout of a thermohydraulic system.

Such a fault-tree can be used to evaluate the impact of the studied system on the plant forced unavailability, or to allocate unavailabilitity to its components. Evaluation and allocation rely on tools of a new generation, based on Binary Decision Diagrams.

The BDDs make it possible to calculate the fault-tree so quickly, that the numerous evaluations which are necessary for allocation can still be done in reasonable times. This would be quite impossible with dynamic, simulation models of the same breakdown level.

8 - REFERENCES

[1] E. Bourgade, C. Degrave, A. Lannoy: "Performance Improvements for Electrical Power Plants: Designing-in the Concept of Availability". *Proceedings of the ESREL'96 conference,* Crete, Greece, 1996.

[2] A. Pages, M. Gondran: "Fiabilité des systèmes" *Editions.Eyrolles 1980*

[3] M. Bouissou, H. Bouhadana, M. Bannelier, N. Villatte: "Knowledge modeling and reliability processing: presentation of the FIGARO language and of associated tools." *proceedings of SAFECOMP 91*, Trondheim, Norway, 1991.

[4] ARALIA Group : "Computation of Prime Implicants of a Fault-tree Within ARALIA". *Proceedings of the ESREL'95 Conference,* Bournemouth, England, 1995.

[5] J.M. Cloarec, "Allocation F-M-D-S, recherche bibliographique : état de l'art", Report 1B1031/RT.001.E (société SOFILOG) January 1993.

[6] J.M. Cloarec, "Allocation F-M-D-S, recherche bibliographique : recensement des méthodes", Report 1B1031/RT.002.E (société SOFILOG) January 1993.

[7] G. Allain-Morin, J.M. Cloarec: "L'allocation d'objectifs de sûreté de fonctionnement en phase de spécification et de conception" *.proceedings of 9ème colloque international de fiabilité et de maintenabilité (λμ9)*, La Baule, Juin 1994.

[8] M. Bouissou, C. Brizec: "Application of Two Generic Availability Allocation Methods on a Real Life Example". *Proceedings of the ESREL'96 conference,* Crete, Greece, 1996.

[9] J.K. Vaurio: "Modeling Components and Systems with Buffers Providing a Grace Period". *Proceedings of the ESREL'96 conference,* Crete, Greece, 1996.

APPENDIX

3 repair teams	$\lambda = 10^{-5}\ \beta_3^2 = 10^{-6}$ $\beta_3^3 = 10^{-7}\ \mu = 0.05$	$\lambda = 10^{-5}\ \beta_3^2 = 5 \times 10^{-6}$ $\beta_3^3 = 5 \times 10^{-7}\ \mu = 0.05$	$\lambda = 10^{-5}\ \beta_3^2 = 10^{-6}$ $\beta_3^3 = 5 \times 10^{-7}\ \mu = 0.05$	$\lambda = 10^{-5}\ \beta_3^2 = 2 \times 10^{-6}$ $\beta_3^3 = 4 \times 10^{-7}\ \mu = 0.05$
exact quantification (Markov graph)	6.736e-7	3.384e-6	3.341e-6	2.682e-6
approximation by $P^{appr}_{Markov} = P^{appr}_{cuts}$	6.727e-7	3.363e-6	3.339e-6	2.679e-6

Table 1: Approximation of the unavailability of a set of 3 components, by a fault-tree model - case of 3 repair teams (See § 3.3).

1 repair team	$\lambda = 10^{-5}\ \beta_3^2 = 10^{-6}$ $\beta_3^3 = 10^{-7}\ \mu = 0.05$	$\lambda = 10^{-5}\ \beta_3^2 = 5 \times 10^{-6}$ $\beta_3^3 = 5 \times 10^{-7}\ \mu = 0.05$	$\lambda = 10^{-5}\ \beta_3^2 = 10^{-6}$ $\beta_3^3 = 5 \times 10^{-7}\ \mu = 0.05$	$\lambda = 10^{-5}\ \beta_3^2 = 2 \times 10^{-6}$ $\beta_3^3 = 4 \times 10^{-7}\ \mu = 0.05$
exact quantification (Markov graph)	2.028e-6	1.021e-5	1.003e-5	8.065e-6
approximation by $P^{appr}_{Markov} = P^{appr}_{cuts}$	2.024e-6	1.012e-5	1.002e-5	8.048e-6

Table 2: Approximation of the unavailability of a set of 3 components, by a fault-tree model - case of 1 repair team (See § 3.3).

BIOGRAPHY

Marc BOUISSOU & Eric BOURGADE
Electricité de France, DER/ESF,
1 av. du Général de Gaulle
92141 Clamart cedex
FRANCE
E-mail Marc.Bouissou@edf.fr
Eric.Bourgade@edf.fr
Fax: (33) 01 47 65 51 73

Marc BOUISSOU has over 12 years of experience in the reliability engineering field.
He has led the development of highly innovative tools, based on AI techniques, to support the activities of reliability engineering, and PSAs (Probabilistic Safety Assessments) for nuclear power plants.
His recent work is about RAMS allocation, computer controlled systems, architecture optimization.
He is the vice-president of the "Methodological Research" working group (with 80 members) of the french ISDF (RAMS Institute) association.
He got an engineer degree of the "Ecole des Mines de Paris" in 1980.

Eric BOURGADE has been working with EDF in the field of reliability engineering for 15 years. He has worked extensively on french PSAs and developed a specific methodology to take into account Common Cause Failures.
Then, he has initiated studies of electrical networks and especially electrical substations, as well as analysis and assessments of control systems.
He is now responsible for the methodological aspects of the CIDEM project, which aims at providing designers with tools helping them to ensure a good profitability of generating plants.
He got an engineering degree in fluid mechanics of the "Ecole Centrale de Paris" in 1979.