Production d'énergie (hydraulique, thermique et nucléaire)

UN SYSTEME D'INFORMATION POUR PRENDRE EN COMPTE LA FIABILITE ET LA MAINTENANCE A LA CONCEPTION

AN INFORMATION SYSTEM SUPPORTING DESIGN FOR RELIABILITY AND MAINTENANCE

97NB00142

DIRECTION DES ÉTUDES ET RECHERCHES
SERVICE ENSEMBLES DE PRODUCTION
DÉPARTEMENT SURVEILLANCE DIAGNOSTIC MAINTENANCE

EDF
Electricité de France

Septembre 1997

RIT J.F.
BERAUD M.T.

UN SYSTEME D'INFORMATION POUR PRENDRE EN COMPTE LA FIABILITE ET LA MAINTENANCE A LA CONCEPTION

AN INFORMATION SYSTEM SUPPORTING DESIGN FOR RELIABILITY AND MAINTENANCE

Pages : 14

97NB00142

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

ISSN 1161-0611

SYNTHÈSE :

EDF développe l'approche CIDEM pour prendre en compte la disponibilité, le retour d'expérience et la maintenance à la conception de centrales électriques.

Les études concernées dépendent étroitement des hypothèses et les résultats mutuels sur la fiabilité et le mode d'exploitation de la centrale. Par conséquent, un système d'information qui supporte ces études doit être soigneusement élaboré. Parallèlement à l'effort de recherche portant sur le développement des méthodes CIDEM, nous avons construit un tel système.

EXECUTIVE SUMMARY :

EDF is currently developing a methodology to integrate availability, operating experience and maintenance in the design of power plants.

This involves studies that depend closely on the results and assumptions of each other about the reliability and operations of the plant. Therefore a support information system must be carefully designed. Concurrently with development of the methodology, a research oriented information system was designed and built. It is based on the database model of a logistic support repository that we tailored to our needs.

1 Purpose of the Information System

1.1 Designing Nuclear Power Plants for Improved Operation and Maintenance

Electricité de France is currently developing a methodology, CIDEM, which stands for "Design integrating availability, operating experience and maintenance", for the design of power plants.

CIDEM is based on a reviewing process described by Degrave and Martin-Onraet (1995). Along the project, designs are submitted to the CIDEM team which evaluates them with respect to criteria of availability, maintenance costs and personnel exposure to radiation.

This evaluation is preferably decomposed into an allocation and consolidation process so that the plant, along with the criteria, can be broken down into manageable components.

Among the studies conducted in the project, we have selected three types for the scope of the information system and hence the scope of this paper:

- analysis of operating experience, which consists in establishing, through delving into events database of related plants or generic reliability data bases, reliability data that will be the comparison basis for the values expected from the design;

- allocation and prediction of forced unavailability, using a reliability model according to the method given by Bourgade et al. (1996);

- accounting for maintenance which confronts the design and its allocated availability to the cost and performance of the maintenance program; such a program, a valuable by-product of the study, is the collection of the main maintenance tasks, along with their frequency, selected according to the Reliability Centered Maintenance (RCM) method described by Jacquot (1996); the whole study, detailed by Degrave et al. (1996) and Degrave et al. (1997), follows the principles of Integrated Logistic Support (ILS).

1.2 Sharing Information for Consistency and Efficiency

Considering the complexity of a nuclear plant and the length of its design and life cycle, the CIDEM studies, highly data consuming, need assistance to handle a large amount of information. In their guidelines for improving the operations and maintenance of nuclear power plants, Mazour et al. (1996) state the need for a data repository that must be filled by the end of the design and should be the foundation for an information system supporting operations. In addition, they suggest that the contents of such a repository should be jointly defined as soon as possible.

Following this recommendation, we conducted a research oriented effort for the design of an information system concurrently with the development of the CIDEM methodology.

A demonstration software was implemented so that experience is gained about the actual interest and feasibility of integrating studies through shared information. The demonstration is based on case studies on the Chemical and Volume Control System of the European Pressurized Reactor, a program involving EDF in the design of a new nuclear power plant.

This paper relates the approach taken to design and build the information system and the first conclusions that can be drawn after its completion.

We contend that building a system meeting all the afore mentioned needs is a novel experience. It sheds an interesting light on the status of the relations between the three connected domains of systems reliability analysis, operations feedback analysis and maintenance optimization. On a more practical level, we hope to present to the reader attempting a similar endeavor enough elements to reproduce and go beyond what we achieved.

2 DESIGNING THE INFORMATION SYSTEM

2.1 A First Building Block: the Logistic Support Analysis Repository Model

Designing an information system meant to support a work process not yet defined appears to be difficult if not objectionable. Yet there is a growing tendency on reducing the length of the design cycle and information system building, not being a productive task with respect to the design, is under considerable pressure and must be anticipated. However, as long as the methodology of design for reliability and maintenance evolves, which is still the case in the European Pressurized Reactor project, the information system cannot be final.

Nonetheless, we took an opportunity to play an active role in the definition and the organization of an integrated design process by concurrently designing the information system.

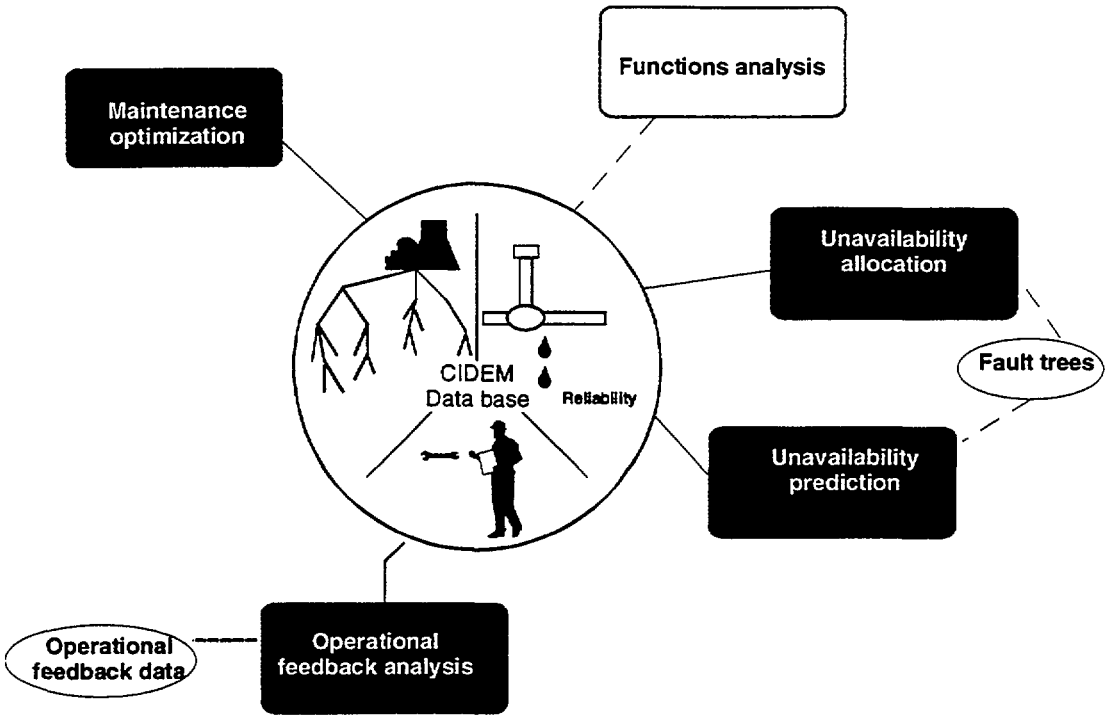

FIG. 1 – *Basic system architecture*

Avoiding new development to handle each type of studies, we relied on pre-existing computer tools. Thus we integrated software from the EDF failure reporting system (see Lannoy and Procaccia (1996)), reliability analysis tools described by Bouissou and Bourgade (1997) and our RCM workstation (see Jacquot (1996)). Rather, we focused on the means to make these tools work together.

We did this by the means of a centralized database (see figure 1), that would simplify data exchange mechanisms, store the common data and implement a common perspective on the main reliability and maintenance concepts.

We must emphasize that we do not look for a repository that would cover all data and concepts used in the project, rather we aim to centralize shared data and coincidental concepts. As an example, operational feedback events, as well as fault trees, were not selected for inclusion in the central database; they are managed by a relevant particular tool.

Yet, we realized that an existing software collection is not enough to design quickly and efficiently the model of the desired centralized database. Joint design tends to drift into long discussions and disambiguation of basic concepts like failure or repair.

This is why we used, as a working hypothesis, the framework of the US Department of Defense DOD (1991) norm on integrated logistic support (MIL-STD-1388). This norm is two fold, the first part (1388-1A) describes a methodology for, among other goals, integrating reliability and maintenance studies in the design process. Although we did not use this part as a project wide reference, we felt that the scope was adequate.

The second part (1388-2B) describes the model of a data base supporting these studies. Its main components are a data dictionary of about 500 Data Element Definitions (DED), a collection of tables defining links between the data and a collection of reports that specify how data should be extracted and organized.

2.2 A tailoring process

The 1388 model is supposed to be tailored to the needs of each project. A selection among the reports can serve as a functional specification from which a subset of data and tables can be inferred.

We took a slightly different approach since our need was putting together already existing tools and studies types. We chose to tailor the data dictionary by selecting only the subset of the DED that defines information exchanged between at least two studies, augmenting them with our own DED if need be. About 65 data element definitions were selected from the norm and 15 added for our needs.

It soon appeared to us that the definitions were very terse; we strongly needed the relation information to grasp the supposed meaning of the data. The table form given by the norm is not adequate for easy understanding, we reformulated the tables into an entity-relationship model for the selected data (a entity-relationship model containing all 500 or so DED would have greatly simplified our task).

A simplified version of the model is shown on figure 2. The three subsets of data sketched on figure 1 are made apparent in the structure of the graph: on the top and left-hand sides are data related to the tree-like description of the plant; on the right-hand side are data related to reliability, around the failure mode entity, on the bottom are data related to maintenance, around the task entity.

3 The 1388 Model and CIDEM

3.1 A Rough but Workable Framework

Our first comment on the adequacy of the 1388 norm is that it did act as an effective catalyst to build a common model. One must also admit that a data dictionary is very limited to define the concepts revolving around the function, reliability and operations of a system. Moreover, although it must have been a tremendous effort, this kind of dictionary is more a compilation of concepts founding pre-existing MIL standards and theory has made progress since then.

For example, the model relies on the implicit assumption that all failure laws follow an exponential distribution function with a time independent parameter; the definition for the failure rate is actually the definition for the maximum likelihood estimate and the difference between demand related and time related failures is considered a mere question of unit. Accepting these as simplifications based on pragmatism, we proceeded further on.

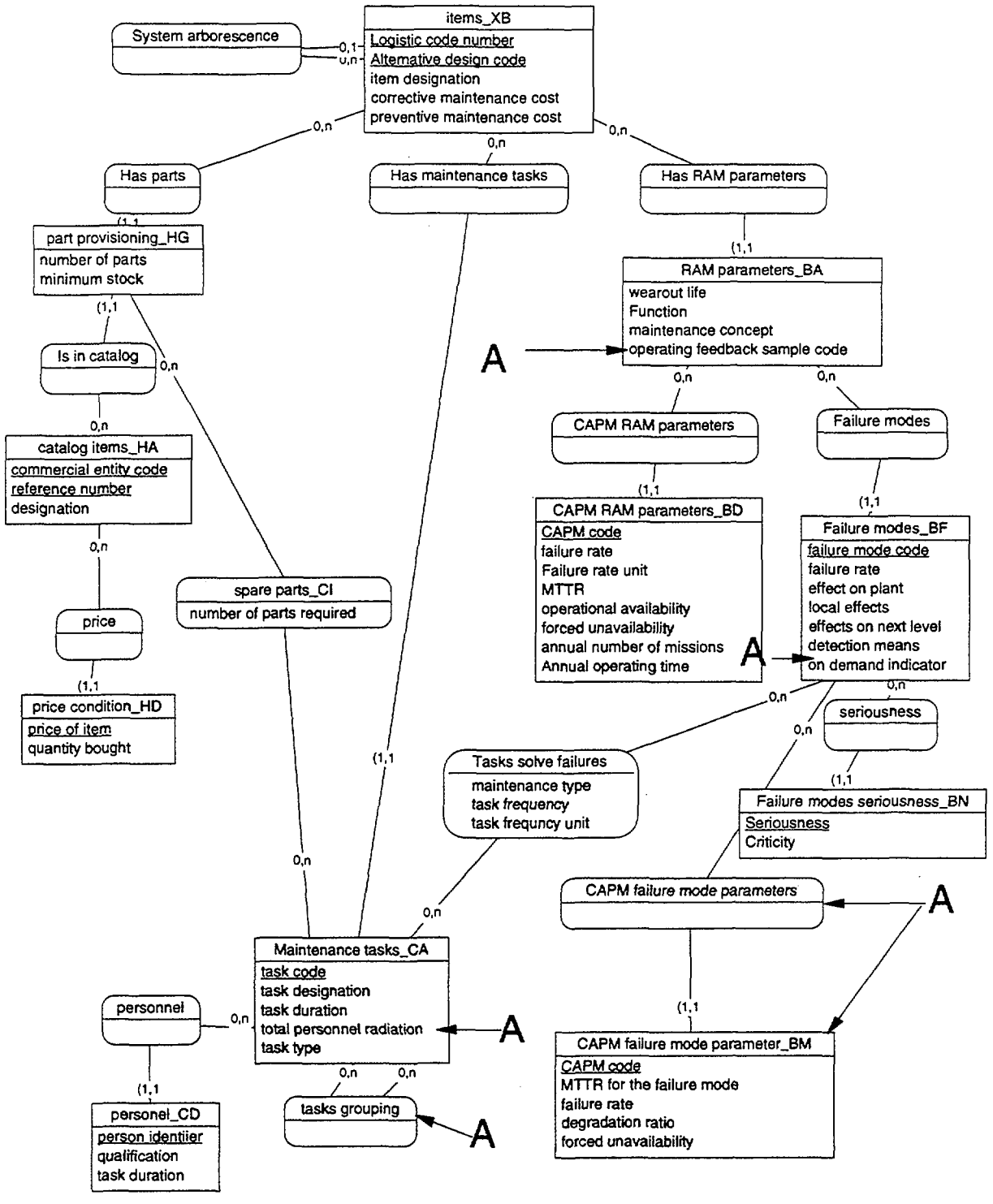

FIG. 2 – *A simplified conceptual model*

3.2 The New Perspectives of 1388

Several aspects of the rationale underlying the 1388 model were new to us and we found them useful.

3.2.1 System break down

The whole model is organized around a hierarchical breakdown of the system, a power plant in our case. The resulting tree structure (that we will call *plant breakdown* in the following) is strictly enforced. While there is nothing revolutionary in this, two points must be emphasized:

- most data is related to a tree node, that is a particular, well identified, subset of the plant; there is no mechanism to represent "generic" or family related data, thus the difference with general purpose reliability data bank is clear.

  Also, one can have a feel of the volume of data by multiplying the number of DED by the number of nodes in the plant breakdown: a few dozens DED actually mean a large database!

- there is no semantics attached to a particular depth or level of decomposition; thus, the identification coding of the subparts of the system relates only to a position in a tree.

  Moreover the model structure is completely independent on the depth level: for example any plant breakdown item can be associated to failure modes and maintenance task; this is not standard practice at EDF: the code of an item gives information on which subsystem the item belongs to and what kind of equipment is involved, also a failure mode or a maintenance task on the whole plant or on a subsystem are never considered.

3.2.2 Reliability data

The 1388 model defines four different values for a given reliability parameter, say a failure rate: *Compared, Allocated, Predicted* and *Measured* (CAPM). Despite the terseness of the norm on their meaning, we took:

- compared values as the results of operating feedback analysis on currently running equipments or installations, mapped to the current design;
- allocated values as the goals established in a top down direction;
- predicted values as the values expected in the project, possibly on the basis of compared values and incorporating, for example, expected improvements in technology or operating conditions pertaining to the design;
- measured values as values measured after the design is built.

We found this distinction very useful to clarify the scope of each study. For example, operational feedback analysts tend to compute directly predictions from observed data (sometimes combined with expertises). In the same time, the allocation process assigns objectives on the basis of what is currently possible and thus needs compared data.

We have to say, however, that when the item is a whole new design with no close running equivalent, the amount of interpretation required to produce a figure blurs the distinction between a compared and a predicted value.

3.2.3 Maintenance tasks

In order to be able to define the resources necessary to operations and maintenance, the 1388 model gives an "operational perspective" to maintenance tasks. A maintenance task must correspond to a unit of work actually performed by identified workers using identified tools.

This is in contrast with the highly abstracted "task" underlying a MTTR attached to a failure mode for the use of a reliability analyst. It is also quite different from a task selected by RCM which tends to abstract auxiliary and induced tasks like preliminary diagnostic or scaffolding erection.

Yet the three perspectives must coexist. We must say that, we have not established links in the model between, for example, a "reliability" MTTR and a maintenance task duration. Thus we only enforce a weak consistency on durations.

3.3 What we Added to the Model

To fulfill our goal of facilitating data exchange, we felt the need to add data elements to the model (pointed with a bold A label on figure 2).

First there are new data element that could not belong to a general model because they are specific to the system. In our case, for example, personnel exposure to radiation is an important design goal given in the form of a cumulative annual dose "for the plant". For health purposes, exposure data are currently collected on an individual worker basis, according to regulations. We determined that for design optimization the relevant data element should be the cumulative dose associated with each maintenance task. Thus our addition to the model. However, going from observed data on the personnel to data on tasks implies knowing *who did what*. Such knowledge is difficult to derive from the current data, for ethical and legal reasons, because they were not collected for that purpose.

On a broader perspective, we had to add CAPM values to failure mode dependent reliability figures. The 1388 model only provides for CAPM values attached to an plant breakdown item, or so to speak, "all failure modes being considered". One can interpret this as a stronger emphasis in reliability analysis in the CIDEM studies.

Finally, there is scarcely any provision in the model to justify the source of values obtained from operational feedback analysis. Nobody in the project would blindly use such figures. On the other hand, much care is taken by the feedback analyst to account for selected samples and provide, if need be, likelihood distributions. Therefore, we added for each item an *operating feedback sample code* that is a pointer to the feedback analysis conducted to produce all the "compared"

values related to the item. For the moment a qualitative examination is enough, no need was expressed for the use of numerical data like confidence intervals.

4 Feeding and Using the Information System

A demonstration scenario, linking the various CIDEM studies by the data flow was elaborated to demonstrate their integration through the sharing of key data.

This completed our static approach of building a data model and allowed a feedback on shaping the design for reliability and maintenance process. Furthermore, this was useful in avoiding the syndrome of defining an extensive model and being driven to collect useless data. Figure 2 is actually close to the result of an a posteriori filtering of the afore mentioned 80 or so data elements.

Detailing the scenario is not in the scope of this paper. However, in addition to showing inter-dependencies and proper sequencing of the studies mentioned at the beginning of this paper, the scenario underlined the need for an overlooked task: producing the plant break down along with the relevant failure modes.

The difficulty in this task is to elaborate this breakdown so that it is relevant to all studies and to do so before these studies are started.

If both conditions are not met, each study will use its own breakdown. As a consequence, the results will be related to slightly different plant subsystems or components. Then any global reasoning, trading, for example, availability against investment cost and maintenance policy, will be rendered impossible unless all results are "harmonized" meaning in effect rerunning the studies. If an inadequate breakdown is forced upon the studies, the results, if there are any, will be meaningless to their producers. When confronted to each other they will clearly be wrong and require a long and difficult tweaking.

We experienced both situations to a certain degree: there has been for long in EDF a standard plant breakdown system, it is not fully adequate to reliability studies nor to operations feedback analysis nor to maintenance optimization, as a consequence each domain uses a different breakdown.

However, we were able to reach an adequate consensus on the breakdown by focusing on the "right" depth level of the breakdown that we call the *functional groups level.* This level (which is not however met at a uniform depth in the breakdown) roughly addresses what are often called *components* in the safety and reliability literature.

At this level, we observe that we can quite easily link a piece of equipment with a basic function, then link this function to the behavior of the plant; we can quite easily measure failures on parts of this equipment and finally relate it to maintenance tasks.

Such a level has been identified and used in RCM studies. Its usefulness justified then the elaboration of a catalog by Saby (1995) of all the generic functional groups that are met in the thermo-hydraulic systems of a power plant. We relied

on this catalog and showed that its use can be extended to build reliability models. We claim that if all CIDEM studies use different breakdowns coinciding on this level, they will have a good level of consistency.

Unfortunately, the fuzziness of the preceding paragraphs is eloquent in showing the lack of an adequate theory that would give rules and principles on what is a functional group and what are its failure modes. We could only observe after using a catalog that it was adequate to our purpose.

5 Conclusions and Perspectives

The 1388 model is a useful and workable starting point for structuring reliability and maintenance information at the design stage. However, we had to augment it to suit our needs of integrating more closely availability studies and rigorous operations feedback justifications.

The quality of case studies is greatly improved. Firstly, data available in the central base curb shaky estimations of unavailable input data. Secondly, results output to the base are de facto submitted to a review process based on consistency with already present data and on overall rigor in common concepts definition.

Such a model must however be augmented with a system breakdown that will ensure a coincidence of the studies, at least at some kind of component level. Such a breakdown level must be finely determined and theoretical ways of describing it are still lacking.

Now that the CIDEM process is more settled, we wish to expand the scope of the information system to a larger set of studies conducted in the CIDEM project and that push the limits of our model framework.

First, we will have to embed our currently autonomous system into an overall CAD system. EDF is currently implementing a new CAD system (CAO 2000) that will manage the common technical description of the plant. It will be much more powerful and rigorous in the handling of libraries containing generic data that will make the studies much easier. Moreover, the CIDEM database currently gives an instant view on the data in the project, without accounting for history and interdependence of the studies. The study monitor of the CAD system should remedy to that.

Acknowledgments

The authors wish to thank C. Degrave, A. Lannoy, E. Bourgade, M. Bouissou, C. Meuwisse, D. Vasseur and C. Martin-Mattei for their comments on the drafts of this paper as well as for their contribution to the work described in it.

Références

Bouissou, M. and Bourgade, E. (1997). Unavailability evaluation and allocation at the design stage for electric power plants: methods and tools. In *Proc. ann. Reliability & Maintainability Symposium (RAMS97)*, pages 91–99, Philadelphia. IEEE.

Bourgade, E., Degrave, C., and Lannoy, A. (1996). Performance improvements for electrical power plants: designing-in the concept of availability. In Cacciabue, P. and Papazoglou, I., editors, *Probabilistic Safety Assessment and Management: ESREL 96 - PSAM III*, volume 1, pages 158–163. ESRA, IAPSAM, Springer Verlag.

Degrave, C. and Martin-Onraet, M. (1995). Integrating availability and maintenance objectives in plant design, EDF approach. In *Third International Conference on Nuclear Engineering (ICONE-3)*, volume 3, pages 1483–1488, Kyoto. ASME-JSME.

Degrave, C., Martin-Onraet, M., and Meuwisse, C. (1996). Integrated logistic support concept in the design of nuclear power plants. In *Fourth International Conference on Nuclear Engineering (ICONE-4)*, volume 4, pages 27–31, New-Orleans. ASME-JSME.

Degrave, C., Meuwisse, C., Hamon, L., and Martin-Mattei, C. (1997). Taking maintenance into account in the design of nuclear power plants. In *Fifth International Conference on Nuclear Engineering (ICONE-5)*, Nice. (to appear).

DOD (1991). DOD requirements for a logistic support analysis record. Military Standard MIL-STD-1388-2B, Department of Defense, United States of America.

Jacquot, J.-P. (1996). A survey of research projects in maintenance optimization for Electricité de France power plants. In *proc. 1996 ASME pressure vessels and piping conference*, volume 332, pages 83–88, Montreal.

Lannoy, A. and Procaccia, H. (1996). The EDF failure reporting system process, presentation and prospects. *Reliability Engineering and Safety*, 51(2):147–158.

Mazour, T. et al. (1996). Designing nuclear power plants for improved operation and maintenance. Technical Report IAEA-TEC-DOC-906, International Atomic Energy Agency.

Saby, P. (1995). Projet OMF, description générique des matériels et de leurs défaillances. note technique D4002.42.81-94/049 Indice 2, Électricité de France Production Transport, Exploitation du parc nucléaire, Département maintenance.