

# **Y2K Safety Issues : How To Provide Confidence During The Millennium Roll Over Of The Nuclear Installations**

|                   |             |
|-------------------|-------------|
| <i>Henry</i>      | <i>IPSN</i> |
| <i>Heinsonn</i>   | <i>GRS</i>  |
| <i>Vandewalle</i> | <i>AVN</i>  |
| <i>Courtois</i>   | <i>AVN</i>  |

---

## **SUMMARY**

The millennium bug (or Y2K problem) could lead to a common cause failure of the Nuclear Power Plant computer based systems.

This international conference is the occasion to discuss Y2K related issues with respect to the safety of the nuclear power plants.

The consequences of failures must be estimated to assess the impact on the safety of the installation, taking into account that these installations were designed with due allowance for the possibility of failure of equipment or components.

The main objective of the work done by operators and licensees is aimed at ensuring the millennium bug could not cause failure or unavailability of equipment or components which are needed for the safety of the installation. The obvious solution is to correct the sensitive systems so that the potential failures could not occur.

Moreover, the risk of a loss of grid should be taken into account as the safety of nuclear power plants depends upon plant resources and consequently the delay necessary to recover external electrical sources.

Safety authorities have issued recommendations asking for reporting periodically the progress and results of the Y2K plan the licensees and operators have to implement for Y2K readiness.

Up to now, Belgium, Germany and France are on the tracks. If some works are still ahead, the results shown today are rather reflecting the readiness of the nuclear installations in due time.

## TABLE OF CONTENT

|   |    |
|---|----|
| 1. The Y2K problem identification .....                                       | 3  |
| 1.1 The millennium problem.....   | 3  |
| 1.2 The causes of the problem.....  | 3  |
| 1.3 Computer systems and safety of nuclear installations .....                | 4  |
| 2. Belgium section .....  | 5  |
| 2.1 Regulatory position .....   | 5  |
| 2.1.1 Issues and General guidance.....  | 5  |
| 2.1.2 Examination and Review : objectives and targets.....                    | 6  |
| 2.1.3 On site Inspection : objectives and targets.....                        | 6  |
| 2.2 Nuclear Power Reactor Licensee position.....                              | 6  |
| 2.2.1 Methodology (corrective, preventive, defensive phases).....             | 6  |
| 2.2.2 Achievements to date .....  | 7  |
| 2.2.3 Specific issues (General Loss of Grid, ...).....                        | 7  |
| 2.3 Main results reviewed to date.....  | 7  |
| 2.3.1 Corrective phase.....   | 7  |
| 2.3.2 Preventive phase.....   | 8  |
| 2.3.3 Defensive phase.....  | 8  |
| 2.4 Conclusions .....   | 8  |
| 3. German section .....   | 10 |
| 3.1 Regulatory position .....   | 10 |
| 3.1.1 Requirements for the Year-2000 demonstration procedures .....           | 10 |
| 3.1.2 Examination of the progress made within the Year-2000 projects .....    | 10 |
| 3.2 Nuclear Power Reactor Licensee position.....                              | 11 |
| 3.3 Main results reviewed to date.....  | 11 |
| 4. French section.....  | 13 |
| 4.1 Regulatory position .....   | 13 |
| 4.1.1 Issues and General guidance.....  | 13 |
| 4.1.2 Examination and Review : objectives and targets.....                    | 14 |
| 4.1.3 On site Inspection : objectives and targets.....                        | 14 |
| 4.2 Nuclear Power Reactor Licensee position.....                              | 14 |
| 4.2.1 Methodology (corrective, preventive, defensive phases).....             | 14 |
| 4.2.2 Achievements to date .....  | 15 |
| 4.2.3 Specific issues (General Loss of Grid, ...).....                        | 16 |
| 4.3 Main results reviewed to date.....  | 17 |
| 4.3.1 Corrective phase.....   | 17 |
| 4.3.2 Preventive phase.....   | 18 |
| 4.3.3 Defensive phase.....  | 19 |
| 4.4 General conclusion on French PWR readiness regarding the Y2K problem..... | 19 |

1.

## **2. The Y2K problem identification**

The transition to the year 2000 is a subject which worries the computer world and more generally those who use electronic equipment like automatic control devices. The processing of dates by computers or electronic devices is of common use in banks, administrations, non-stop industries, telecommunications, service companies, mass marketing, etc. Today, preparation for dealing with the millennium bug is underway. In particular, the nuclear industry has embarked on a millennium programme. This programme is based on an inventory of sensitive components, their impact on safety, their modification or replacement and their requalification.

### **2.1 The millennium problem**

The problem posed by the millennium bug for computer systems in particular relates to the use of dates which have been simplified so as to occupy a minimum of space in the computer's memory. For instance, the date 2 November 1976 is abbreviated to "02 11 76" and it is not strictly possible to know if the abbreviated date relates to the 19<sup>th</sup> century or the 20<sup>th</sup>. Therefore, the millennium bug could be generated by the fact that one minute after midnight on 31 December 1999 some computers will behave as it is the 1<sup>st</sup> January 1900!

The consequences of this could be disastrous for many companies. For example, databases are managed automatically by comparing the dates of files. If there is a discrepancy in these dates, the management program of the computer may delete records made at dates subsequent to (1999 abbreviated to 99) the current year (2000 abbreviated to 00). This would destroy all the databases up to the year 1999 at one fell swoop!

All the automatic management functions of computer files (archiving, storing, purging, transaction logging, etc.), data transmission over networks (PABXs, hubs, modems, servers, etc.), security of access to protected sites (validity dates of security cards, dates of birth of persons, etc.) and other areas may be affected by this problem.

### **2.2 The causes of the problem**

There are many causes as the problem is linked to:

- the way the date is represented, inside the computer, i.e. if abbreviated to optimise memory space,
- software processing operations, whether they are in the operating system (e.g. DOS) or developed for applications (e.g. Excel).

These solutions, which were developed in the 1960s when it was important to save memory space, are still used as they are included in:

- the optimised integrated circuits using these techniques (microprocessor, processors for computers, peripheral communication or internal clock circuits, etc.),
- software applications in which the corresponding programs are integrated in the form of library modules by the compiler,
- operating systems which were made by adding new functions to the original parts.

### **2.3 Computer systems and safety of nuclear installations**

As in all other types of industry, nuclear installations use computer systems and logic control systems to carry out the control and regulation functions required in the industrial process. Other computer systems carry out service or management functions (e.g. limiting access to controlled areas). For obvious reasons, some of these systems are sensitive to the millennium problem. The consequences of failures must be estimated to assess the impact on the safety of the installation. It must be borne in mind that these installations were designed with due allowance for the possibility of failure of equipment or components. The first step is to correct those sensitive systems so that the potential failures could not occur. As well, it is important to ensure that the millennium bug does not cause failure or unavailability of equipment or components which are not provided for in the installation design hypotheses. Moreover, the risk of a loss of grid should be taken into account as the safety of nuclear power plants depends upon plant resources and consequently the delay necessary to recover external electrical sources.

**3.**

## 4. Belgium section

### 4.1 Regulatory position

#### 4.1.1 Issues and General guidance

In the second semester of 1997, AVN, the Belgium nuclear regulatory body, sent to the NPP's in Doel and Tihange Y2K information on the Y2K problem (in particular [Wainwright and Hunns 1997] ), and drew their attention on the need for action.

In August 1998, a letter was sent to each site with copy of the Generic Letter 98-01 from the US Nuclear Regulatory Commission (Y2000 Readiness of Computer Systems at Nuclear Power Plants), and with additional references to technical information, most of it accessible on the internet. The AVN letter essentially was requesting the following:

- a description of the plans and time schedule needed to make a full inventory of the vulnerable computer based systems used in the plants, and to make these systems Y2K compliant or ready;
- the list of identified systems, and the corresponding actions that would be planned;
- confirmation of actions taken to get external suppliers involved;
- description of the planned or already completed verification and test programmes;
- confirmation of steps taken to define contingency plans in order to anticipate problems that may be caused by systems which, despite remediation, might not be compliant or ready as expected.

AVN primary concern was Y2K timely *readiness*. *Compliance* was not considered as the primary objective, the rationale being that, in certain conditions, it might be safer to leave the software unmodified and rely on other means to make the application ready. It was also recognised that not only systems important to safety, but *all* operational computer based systems in the plant should be investigated and be part of the initial inventory.

In November 1998, AVN insisted on the necessity of contingency measures to face both internal and external risks induced by the Y2K problem. Concerning the internal risks, it was made clear that, in many cases, it would be impossible to be certain of the compliance or the readiness of the software. Contingency measures had therefore to take into account, for every vulnerable system, the possibility that it might fail to deliver proper service on the critical dates, even if it had been successfully tested compliant or ready.

In February 1999, AVN notified the licensees that it wished to be informed at the latest before June 1999 of all Y2K problems that would still remain unsolved and could place the site or the reactor units in conditions outside their design basis. This date was chosen, among other reasons, to give the operators enough time to implement adequate solutions and to get acquainted with modifications and/or new procedures.

#### **4.1.2 Examination and Review : objectives and targets**

The documents describing the plans mentioned above, and the documents produced by these plans were being reviewed and commented by AVN. In particular the structure and the contents of the databases (see below) produced in the inventory phase was reviewed by AVN. For each plant, the database has an entry for every computer component, equipment and application in the plant, and keeps a record of the status of these items, together with the results of tests, of contacts with manufacturers, contingency measures, etc. .

#### **4.1.3 On site Inspection : objectives and targets**

AVN has been conducting on-site audits and inspections at Doel and Tihange to follow and discuss in detail the progress of the work. AVN inspectors and software specialists take part in these inspections. The objective is to see how well the Y2K plant readiness programme is being implemented, and how it will meet its objective of making the plant ready on schedule. Items that have been on the agenda of these inspections are:

- The Y2K program organisation, management, resources, schedule;
- The criteria used to establish the inventory, ensure its exhaustiveness and to prioritise the work;
- The verification methods and tools for assessing Y2K susceptibility, compliance and readiness;
- Methods and status of remediation;
- Test cases before and after remediation;
- Y2K non-compliance findings and technical issues (e.g. the maintenance of the consistency of date windows across different communicating systems).
- Contingency measures.

### **4.2 Nuclear Power Reactor Licensee position**

#### **4.2.1 Methodology (corrective, preventive, defensive phases)**

At the nuclear power plants in Doel and Tihange, the Y2K project was started in 1997. The objectives defined by the licensee were (i) the safe and reliable production of electricity, (ii) the avoidance of the loss of data, and (iii) the economic justification of all actions. In order to reach these objectives, two basic plans were scheduled: (1) making all equipment and computer programs Y2K *compliant or ready*, and (2) elaborating *contingency* measures for both internal and external potential causes of problems. As said earlier, these plans and their implementation were audited by AVN.

The Y2K compliance/readiness plan started with the inventory phase. All computer components, equipment and applications were identified - and recorded in a database - by different (bottom-up) search procedures. The results of these search procedures were also cross-checked by a top down approach, starting from the safety and production systems, and gradually decomposing and analysing them at component level. All components (like PLC's, controllers, embedded systems, computer hard and software systems, interfaces,...) were thus associated with equipments (e.g. steam generator level control systems, rod position control systems,..) or with applications (e.g. radiation monitoring, maintenance, access control,...). A priority status was assigned to every item in function of its impact on safety and availability.

Items were then tested for Y2K compliance and/or readiness, starting with those of highest priority, and with test plans and strategies based on the conformity requirements of the British Standard DISC PD 2000-1, and guidance from the US NRC, HSE UK and relevant technical literature. This testing phase was followed by a remediation and a new phase of non-regressive tests. Among the test tools used are NSTL's YMARK2000, TDTEST (for the Crouch-Echlin Effect) and Express 2000.

#### **4.2.2 Achievements to date**

The inventory phase was completed in the second half of 1998. More than 300 applications and equipment, composed of more than 2000 components were identified per site. Out of those 300 or more applications/equipment, about two thirds may have some impact on safety or availability (i.e. are not of the lowest priority). By the end of 1998, all safety systems had been tested and certified Y2K compliant except one which, because of a minor problem, was certified ready. In March 1999, about only 20% of all the applications/equipment that had been tested were found not ready. Most of these non ready items are software applications which rely on non-compliant operating systems and third party products. At the beginning of June 1999, approximately 95% of equipment and applications which may have some impact on safety or availability (i.e. which are not of the lowest priority) had undergone test and analysis, and 90% of those were considered as being compliant or ready.

The objective of both sites was to complete this compliance/readiness plan by the end of July 99, exceptions being made for a handful of applications which would undergo tests during outages before the end of the summer.

#### **4.2.3 Specific issues (General Loss of Grid, ...)**

A set of contingency plans is being designed to cover both the internal risks resulting from problems raised by systems used within the plant, and external risks resulting from problems originating outside the site:

*Internal risks:* For every Y2K sensitive equipment or application which may affect safety or production, a contingency plan is being implemented, on the assumptions that the item may remain not ready or not compliant following the inventory and remediation phases.

*External risks:* Scenarios and actions are envisaged with the essential objectives of sustaining instabilities on the grid, water and supply shortages and communications problems. The corresponding actions ensure extra provisions for fuel, consumables, communication links, human resources, as well as special training and general procedures.

For every internal or external risk, a contingency plan is being designed, basically following the guidance in [NEI/NUSMG 98-07]. The total number of such plans per site will approximately amount to 200 for the applications and equipments, plus one plan per external risk. Each plan is approved by four different responsible persons independent from the author. An integrated contingency plan matrix collects all contingency plans with their specific characteristics (description of risk, mitigation strategy, vulnerable periods, subject matter experts identification, implementation timing constraints, resources required, priority status). At the end of March, about 50% of the contingency plans had been provided in Doel. The completion of the definition of these contingency plans was scheduled for the end of August.

Instabilities on the national and international grids, loss of external supplies and loss of external communications are recognised as three major external risks. Plants aim at sustaining a 2-weeks period of unreliable grid with an external temperature below zero degrees Celsius.

### **4.3 Main results reviewed to date**

#### **4.3.1 Corrective phase**

Examples of systems for which remediation was needed are:

- A seismic monitoring system and a fuel container pressure monitoring system unable to perform correct calculations when entering 2000 dates.
- A battery test system converting 2000 dates into 1900 dates and producing incorrect trending curves.
- A primary coolant monitoring system unable to work with dates between 00 and 50.

- A tritium measurement system which confuses year 2000 with 1900, causing miscalculations in the decay scheme.
- An atomic emission & absorption spectrometer which dates calibration results, reports and application versions incorrectly beyond 2000.
- A nuclear waste vessel transport system which uses the date to make an itinerary reservation and fails to work beyond 2000.
- Full scope simulators which give no possibility to set dates in 2000, even not 00.

Some commercial off the shelf information systems had to be updated to achieve readiness. This was the case for a plant maintenance planning tool, a maintenance tracking system, and an archiving system. A frequent problem met with these applications was caused by the possibility of entering both 8-digit and 6-digit date formats, information being stored correctly in the first case, incorrectly in the other.

#### **4.3.2 Preventive phase**

Provisions are taken to ensure, among other measures:

- agreements with suppliers for spare parts;
- replacement of critical filters before the end of year;
- empty storage for liquid waste;
- extra testing of redundant communication equipment;
- avoidance of preventive maintenance at the end of year;
- avoidance of modifications of software during the last two months of 1999;

At this stage of the design of the contingency plan, no specific changes are being made to the technical operating specifications, nor to incident or accident operating principles.

#### **4.3.3 Defensive phase**

During the critical time periods, the plant should be capable of sustaining at least a 2week period of water shortage with a temperature of -10°C. Provisions will also be taken for:

- extra diesel and lubricates;
- extra fuel to keep operational the auxiliary steam system;
- extra reserves of consumables (gas, chemicals).
- avoidance of equipments being taken out of service.
- allocation of extra personnel in the control room, of Y2K project members, I&C personnel and IT specialists on site and on call, extra fire brigade; engineers on duty shall be on site;

On the critical dates, it is also planned to operate the nuclear plants in Belgium at a reduced level of their nominal power. This reduced level differs for units and varies from 50 to 70%. One nuclear unit and four classical units will be maintained on house load to facilitate restart procedures in case of incident. Specialised training of operators on simulator is planned.

The Electrabel department in charge of the co-ordination of the production and of the international grid exchanges is discussing means of facing the critical dates with international partners, under the auspices of the UCPTE.

Important industrial energy consumers have been approached to consider a planning of the reduction of their consumption on these dates.

#### **4.4 Conclusions**

In summary, one may conclude that at both sites in Doel and Tihange, there are no Y2K concerns that might affect the performance of safety systems, that licensees are following state-of-the-art industrial practices to achieve Y2K readiness, and that the schedules for the remaining few Y2K items will be completed before the transition from 1999 to 2000.

## References

[DISC PD2000-1] A definition of year 2000 conformity requirements. BSI, London.

[NEI/NUSMG 98-07] Nuclear Utility Year 2000 Readiness Contingency Planning. August 1998, Nuclear Energy Institute, Washington, D.C.

[NRC Generic Letter N° 98-01] Year 2000 Readiness of Computer Systems at Nuclear Power Plants. May 1998. USNRC, Washington, D.C.

[Wainwright N., Hunns D.M. 1997] The Y2000 Problem. The Nuclear Regulatory Perspective. Private communication published in Nuclear Engineering International in January 1998.

**5.**

## **6. German section**

At the time of the drafting of this text, the Year-2000-projects and their reviews by the expert organisations in Germany have not been finished yet. For this reason, essential statements on this topic have not been available.

### **6.1 Regulatory position**

In accordance with the federative system of government, the tasks of the authorities are separated and allocated to the nuclear supervisory authorities of the federal states, i.e. the *Bundesländer* and the Federal Government. The *Bundesländer* are responsible for the nuclear power plants located in their area, and the Federal Minister for the Environment, Nature Conservation and Nuclear Safety (BMU) exercises the so-called supervision on expediency towards the *Bundesländer* and takes care for the uniform implementation of the Atomic Energy Act. Both the *Bundesländer* and the BMU commissioned expert organisations for technical advice and assistance. The *Gesellschaft für Anlagen- und Reaktorsicherheit* (GRS) is the expert organisation of the BMU.

In spring 1998, GRS initiated measures for ensuring the Year-2000 conformity in the nuclear installations by means of GRS information notices (GRS-WL).

The GRS information notices inform the nuclear supervisory authorities of the *Bundesländer*, their experts and the operators of nuclear installations about events of general significance to the safety of nuclear installations and on the basis of which corresponding measures are recommended. Thereupon, the operators have to report to their competent authority in which way the recommendations of the information notices will be implemented at their plants.

In the middle of 1998, GRS initiated the drafting of the requirements for the procedure of demonstrating the Year-2000 conformity. Further, GRS was commissioned to survey the progress made, and to prepare a general final expert's assessment on the Year-2000 projects at the plants at the earliest possible date.

#### **6.1.1 Requirements for the Year-2000 demonstration procedures**

The requirements regarding the demonstration procedures for the Year-2000 conformity were laid down in the «Compilation of the information necessary for the safety-related assessment of the programmes provided by the German nuclear power plant operators to ensure Year-2000 software compatibility » (Year-2000 catalogue of requirements) [1]. The Year-2000 catalogue of requirements was drafted by GRS and approved by a working group of the RSK committees on "Electrical systems" and "Reactor operation". This Year-2000 catalogue of requirements sets the standards for the assessment of the Year-2000 conformity demonstrations by the German supervisory authorities. In December 1998, the *Bundesländer* concerned were recommended to apply the Year-2000 catalogue of requirements forwarded in an annex to the GRS information notice.

#### **6.1.2 Examination of the progress made within the Year-2000 projects**

Since the middle of 1998, the *Bundesländer* have been commissioning its experts to examine the Year-2000 projects of the nuclear power plants. Further, BMU asked the *Bundesländer* to make progress reports from all plants available to GRS by the end of January, middle of May and middle of August 1999 for a general assessment.

The experts of the nuclear supervisory authorities of the *Bundesländer* have surveyed the Year-2000 projects on site as an accompanying measure. GRS has made a general evaluation of the progress reports from the nuclear power plants for BMU.

## 6.2 Nuclear Power Reactor Licensee position

In the middle of 1998, all nuclear power plants operators have started Year-2000 projects. The project organisation, structure and proceeding have been laid down in accordance with international standards, e.g. of the NRC or the British Standards Institution (BSI) and the Year-2000 catalogue of requirements.

At the end of July, the registration, examination and upgradings of the systems to control incidents and processes of abnormal operation (Category S according to Year-2000 catalogue of requirements) as well as of the systems which upon failure demand short-term termination of power operation (Category V according to Year-2000 catalogue of requirements) was largely finished. For completion, an interim report had been drafted for each nuclear power plant.

For software-based components and systems of Category B (according to Year-2000 catalogue of requirements), that are components and systems with a limited safety-related significance not belonging to the Categories S and V (e.g. process computers, recorders, measuring systems, fire alarm systems, radioactivity monitoring systems, physical plant protection systems), the proofs are furnished when the projects in the plants will be finalised. The end of September is scheduled as deadline for delivering the final reports. The final expert opinion is expected by the end of October.

With regard to the contingency plan, in Germany distinction is made between the back-up measures of the utilities and the planned precautions of the operators of the power supply systems. The back-up measures are subject to nuclear supervision. For this reason, the requirements for the back-up measures are laid down in the Year-2000 catalogue of requirements. The planned precautionary measures of the operators of the power supply systems primarily have the aim, besides the preferred energy supply of the nuclear power plants, to ensure the public energy supply in case of power failure, which falls into the competence of the Federal Minister of Economics in Germany.

Presently, there are drafts for back-up measures concepts. The detailed planning of the back-up measures will be made after the system have been checked. The finalisation of the detailed planning of the back-up measures is expected for November 1999.

Back-up measures are to be provided for situations, in which there would be an inadmissible effect on safety if the available Year-2000 measures were to prove ineffective. Here, the procedure is to be as follows:

- assessment of possible effects of the malfunction of software-based systems or components with regard to possible impact on plant safety,
- check of the specified organisational measures (e.g. organisation manual, operating manual) in case of malfunctions of these systems or components,
- if necessary, provision of substitute measures, like e.g. supplementary shift instructions or measures on the failure of computerised fault reports, work execution or isolation procedures directed at a transition to manual activities,
- sensitisation of the control room personnel concerning the Year-2000 problem in the context of training,
- provisions for functions that may not be ensured and on which the power plant itself has no influence (e.g. integrated grid system, telephone, provision of supplementary means and petrol for diesel engines).

It is furthermore recommended to provide on-call personnel on the crucial days.

## 6.3 Main results reviewed to date

Based on the general assessment of GRS, the following findings can be stated.

The checks of the systems to control incidents and processes of abnormal operation have been completed in July 1999 (Category S).

Nation-wide, 15 software-based component types were identified in Category S. Only for the measuring system Sinuperm N of the nuclear instrumentation, which is installed in two plants, a date processing was identified. In all the other cases, a date processing could clearly be precluded. For none of the components, upgrading measures were required. For all components, absolute conformity, i.e. conformity stage 1 according to the Year-2000 catalogue of requirements, has been demonstrated.

The checks of systems which upon failure demand short-term termination of power operation (Category V) has largely been finished in July 1999.

Nation-wide, about 40 component types were identified in Category V. In none of the cases, components had to be upgraded. In one case, non-conformity had been identified for a component, for which replacement measures have been decided on site with the approval of the expert.

As a result of its general assessment and experience, GRS cannot preclude for the balance of plant systems (BOP systems) with any degree of certainty that some components of the Category V have been overlooked. For this reason, it is also taken into account in the safety-related assessment that initiating events may occur at the turn of the millennium.

Therefore, GRS roughly assessed the technical risk to estimate the possible consequences by means of precursor analyses. For this purpose, it was assumed hypothetically that, despite the Year-2000 check, the main heat sink, the main feed-water supply and the auxiliary power supply fail at the turn of the year. The assessment shows that the frequency of the system damage states with endangerment of the core cooling increases up to factor 7, but that it still stays clearly below the international standard value of  $10^{-4}$  per year for the frequency of core damage states. GRS takes the view that there is no reason for safety-related concerns although the components of Category V might not have been considered in the assessment completely.

## Reference

Zusammenstellung der erforderlichen Informationen zur sicherheitstechnischen Bewertung der von den deutschen Kernkraftwerksbetreibern vorgesehenen Programme zur Sicherstellung der Jahr-2000-Softwarekompatibilität (*Compilation of the information necessary for the safety-related assessment of the programmes provided by the German nuclear power plant operators to ensure Year-2000 software compatibility*) Bundesamt für Strahlenschutz (*Federal Office for Radiation Protection*), RSK-Geschäftsstelle 21.12.1998

## 7.

## **8. French section**

The nuclear industry in France has embarked on a millennium programme since beginning of 1996. This programme is based firstly on an inventory of sensitive components, their impact on safety, their modification or replacement and their requalification. Lines of defence in depth have been implemented by the licensees to secure this basis. The whole programmes are being assessed by the Institute for Nuclear Safety and Protection (IPSN) as the technical support of the safety authority (DSIN).

### **8.1 Regulatory position**

#### **8.1.1 Issues and General guidance**

Nuclear facilities and plants in France largely use computers to implement functions related to the control and the command of the processes, as well as to implement the important to safety systems.

Facing the millennium bug, the main worry is that one or more computerised systems could fail at the same time. Moreover, the risk of a large loss of grid in France should be taken into account as the safety of nuclear power plants depends upon plant resources and consequently the delay necessary to recover external electrical sources.

The nuclear operators (EDF, COGEMA, etc.) are responsible for the safety and in that case for the actions which need to be taken on its side, the IPSN worked out in 1997 an approach to analyse the problems the millennium bug may induce in the nuclear facilities and plants and to assess the provisions the operators have envisaged. This approach is based on the interdisciplinary nature of the IPSN's activities. All the specialists at the IPSN have contributed to the strategy, including site assessors, experts in nuclear facilities systems, in instrumentation and control systems, in human factors, in operation and accident management.

This approach led to issue a questionnaire to facilitate the assessment of actions and measures taken by the various operators. These should therefore include :

- a specific organisational system for analysing and dealing with the remediation of millennium bug impact on equipment, including an organisation which ensures that the Y2K modified equipment are effectively at site,
- an analysis of the sensitivity of the installation to the millennium phenomenon, which must include identifying the relevant equipment and the consequences of potential failures caused by the bug,
- a study of resources (energy, fluids, telecommunications, etc.) necessary to the installation in the short term and in a longer term, including the possible loss of national power supply grid,
- a specific plan of actions to implement the contingency measures necessary to obtain defence-in-depth, that is to say which make it possible to manage at least an abnormal situation caused by the millennium bug.

A specific group, inside the IPSN, has been set up to review and follow-up the progress of the licensees actions in due time, as well as the status of internal analyses. International nuclear and national other industries information relevant to Y2K problem is reported to that group.

Moreover, the IPSN has continuous exchanges with other international organisations (e. g. OECD, IAEA) on that millennium bug issues.

### **8.1.2 Examination and Review : objectives and targets**

Of course, the IPSN assessments cope with all the phases of the Y2K methodology the licensees adopted to achieve the Y2K plant or facility readiness. These phases are (1) the corrective phase, which is the baseline of the strategy, (2) the preventive phase, and (3) the defensive phase. Those three encompass, depending upon the strategy of the licensee :

- inventory of the systems that may be affected by the Y2K problem ;
- corrective measures (e. g. modifications or replacement of the affected systems, ...) ;
- preventives measures (for example, identification of outside dependencies, bypass of non corrected systems, plant safe postures regarding the Y2K possible failures, ...) ;
- defensive measures (i.e. crisis planing and staffing) ;
- restart measures, when the nuclear installation will be stopped at the end of this year (e. g. testing of safety systems, ...).

The follow up of the licensee's actions is done by quarterly periodic meetings. Moreover, technical meetings are held to deeply examine some of the concerns raised by the licensees files sent to the safety authority (DSIN).

It must be noted that nuclear installations are not all of the same type. Some as Nuclear Power Plants (NPP) or the EURODIF enrichment facility at Tricastin site are based on a continuous process. Some other are able to stop for a while. It is the case of the majority of the fuel cycle plants, the experimental reactors as well as the other types of nuclear facilities. Those will be stopped at the millennium roll over, but the licensee is required to provide the safety authority with the evidence of the Y2K readiness of these installations.

The large number of installations under examination and the available time of assessment have led the IPSN to develop a different strategy of assessment with regard of the type of installations, taking in account the process of the plant or the facilities, the associated potential risks, the centralised structure of the licensee of the installations.

### **8.1.3 On site Inspection : objectives and targets**

The main objective of the on site inspections, performed by the safety authority accompanied by the IPSN, is to provide inputs to the safety authority on the actual situation of the installations, regarding the implementation of the corrections of the systems as well as the preparedness of the teams that will be involved during the millennium roll over.

Inspections are being conducted on a representative sample of the different types of nuclear reactors in France (900 MWe, 1 300 MWe and 1 400 MWe PWRs) or large facilities (fuel manufacturing plant, reprocessing plant, ...). Technical meetings between site representatives and the IPSN are also conducted to assess the organisation and the means put in place to cope with the Y2K problem of the local items if those are not in the licensee national inventory.

## **8.2 Nuclear Power Reactor Licensee position**

Electricité de France is conducting its Y2K program with the objective to allow the 58 nuclear power water reactors to product safely and continuously electricity, as before the 1st of January 2000.

### **8.2.1 Methodology (corrective, preventive, defensive phases)**

To face the millennium bug, Electricité de France developed a phased methodology. These phases are :

- a corrective phase, to eliminate the millennium bug effect on computerised systems and software applications.
- a preventive phase, to independently validate the inventory made during the corrective phase, to rank the necessary plant systems to provide safe production of electricity, to

identify the plant postures and the contingency measures that would be needed for the roll over,  
- a defensive phase, to elaborate the corresponding crisis and staffing plans and to implement them.

EDF has put in place an organisation that have been increasingly staffed from 1997.

For the corrective phase, two levels of responsibility are defined : the national level, which take into account the computerised systems and software applications that are common to all plants of a series, and for all series (900 MWe, 1 300 MWe, 1 400 MWe) ; the local level, which have the responsibility for conducting all the phases of the national EDF strategy on computerised systems and software applications that are of local importance. The EDF national level Y2K program staff is involved in the Y2K site teams by means of planed common reporting sessions. The corrective phase includes three steps that are :

- inventory, the list of all computerised systems and software applications has been established on the base of the national level list validated by the 19 sites teams ; each site has made a list of the local items that are of computerised type ;
- impact analysis of the Y2K problem on each of the computerised systems and software applications identified ;
- remediation (if needed) including modification or replacement of obsolete items the functional impact of which is not acceptable, a series of tests in situ or in EDF premises to validate this remediation scenario, and the deployment of those remedied equipment.

The preventive phase is turned both to validate the corrective phase and to propose solutions for the defensive phase. A functional analysis has been made by an EDF specific Y2K team during that phase to verify the list issued from the inventory of the corrective phase. It led to rank the 535 NPP systems regarding their importance to the safety and the availability taking in account delay (day, week, month). This phase includes also studies of plant precautionary postures and outside dependencies (e. g. large scale loss of off site electrical power).

The defensive phase allows firstly for choosing the hypotheses to be the rational basis for the period of the millennium roll over and secondly for determining the operational provisions for the period beginning from the 1st December of 1999 to the 31st of March 2000.

### **8.2.2 Achievements to date**

The inventory was completed in the first quarter of 1999. Among the 962 computerised systems and software applications that were inventoried, 193 were found affected. In parallel, the impact analysis and the remediation choices were conducted. This led EDF to abandon some of the most obsolete ones (29), to declare acceptable the Y2K functional impact for 20 of the 193 and to correct the others. This position was stated for more than 70 % in April 1999. The rest was completed by the end of June. The deployment of the remedied equipment is mostly done (more than 95%) and will be done completely by the end of October. The complementary examination made by EDF on electronic boards that use real time clock chips has not led to any change in the status of the equipment (affected or not affected). Date forcing and windowing modifications are still to be made. EDF has to establish the list and the procedures to be followed for modifying theses equipment on site.

The preventive phase was conducted by EDF and ended in June. This phase included : (1) a functional analysis of the nuclear power plants of the three series (900 MWe, 1 300 MWe and 1 400 MWe PWRs), (2) a plant precautionary posture study and (3) an outside dependency study.

The functional analysis, made by EDF to validate its inventory and impact analyses, was ended in April. This analysis was done on the basis of the operational technical specifications of the plant series. This led to identify 9 computerised systems that need a deeper impact analysis to be sure of their Y2K compliance (for example the primary pump speed measurement system). One of the major conclusions of the EDF analysis is that the cross correlation between that study and the results of the corrective phase allow for some confidence in the absence of common mode failure risk on important systems.

The plant precautionary posture study was ended in June. Prescriptions were addressed to the sites that are : (1) to verify the availability of the necessary systems to face a loss of off site power (emergency diesels, water service station, ...), (2) to make the stock of the necessary materials for the reactors as great as possible (refill of fuel and water tanks ; lithia, boron, hydrogen, resin fully supplied ; ...), (3) to have stable production of electricity and restrict the power to 60 % for the reactors that will be near the core cycle end, (4) to limit during the week-end the programmed activities to the needed actions to allow the operators to be as much as possible available (no fuel handling, no periodic tests, ...) ; (5) to report to the headquarter any discrepancies during the periodic tests that will be done in the first quarter of year 2000, so that experience feed-back can be share between sites.

The outside dependency study focussed on the loss of off site power and was completed in August. It must be stressed that Y2K program led EDF to accelerate technical implementation of solutions decided before the beginning of the Y2K program.

It took in account the work done on this topic by EDF before the Y2K program. This work led to obtain derogations to the technical specifications from the safety authority (see below specific issues).

The first part of the defensive phase, which deals with the hypotheses to be taken into account for the roll over period (i.e. the Y2K team profiles, the number of inquiries from operators, the safe transmission between centres, the time period for having Y2K teams on duties ...), was achieved in August. The implementation of the crisis plan is quite achieved too and operator awareness and training plans are in place.

### **8.2.3 Specific issues (General Loss of Grid, ...)**

The Y2K problem raises the risk of disturbances that may impair the stability of grid. The loss of off site power could lead to weaken the safety of PWRs, if house load is not reached successfully.

The work done by EDF during the corrective phase and the preventive phase ended on the conclusion that no common mode failure could affect the plant systems that are necessary to provide continuously electricity on the grid, within the technical specifications.

On the other hand, the grid is monitored and operated from EDF centres that are able to quickly disconnect areas or regions that could be affected by instabilities of the voltage or the frequency.

Consequently, the hypothesis taken into account by EDF is the possibility of a regional loss of power, either due to customer problems or EDF plant problems. In such a case plans exist yet for repowering the French grid from hydro, fuel, and nuclear plants that would have been successfully on house load.

In co-operation with the EDF nuclear division, the EDF division in charge of the grid achieved the correction of the Y2K non compliant computerised systems, used for example in the switch yards, and the implementation of the remedied systems.

In the context of a possible loss of power in a region, EDF has developed a validation program on the basis of two scenarios of external repowering of a reactor (i. e. any off site power source from hydro plant, fuel/gas plant or turbine generators) and one scenario of internal repowering (i. e. from another reactor or the same site).

According to the EDF study, any reactor can be supplied within 12 hours maximum, wherever the site is, including the time to intervene on grid equipment if necessary.

### **8.3 Main results reviewed to date**

The IPSN was asked by the safety authority to conduct the technical assessment of the Y2K readiness of the nuclear power plants of EDF.

Quarterly meeting between EDF, the safety authority and the IPSN have been in place since 1998 to follow-up EDF nuclear division activities and their results.

A first meeting of the standing group of experts for reactors took place (April 22, 1999), the purpose of which was to inform that group with the Y2K strategy adopted by EDF and the main issues the IPSN has raised.

A second meeting (September 23, 1999) has reviewed the provisions proposed by EDF in the preventive phase and the defensive phase. Concerning the three phases (corrective, preventive, defensive) the main conclusions of the IPSN are drawn hereafter.

#### **8.3.1 Corrective phase**

The IPSN has reviewed the methodology and the means EDF applied to identify and correct the computerised systems and software applications shown Y2K non compliant. Sampling was done by the IPSN to verify the implementation of the methodology on different categories of the computerised systems and software applications (e. g. telecommunication systems, I&C systems, process computers, ...).

Examples of malfunctions identified by EDF analysis are : health measurements that can not be stored correctly due to a non compliant date management, fire detection centralised system the software of which is locked while year of the date is greater than 1999, ...

Early in the assessment, the IPSN stressed that EDF would have to identify precisely the version of the software and the hardware configurations within the list of equipment, to be sure that the corrected equipment or application software is the one installed on site. Moreover, the IPSN raised the question of real time clock integrated circuits (RTC) that could be Y2K non compliant. EDF has sorted a list of those and verify digital equipment against it to conclude there is no forgotten systems in the list of computerised systems and software applications.

The IPSN concluded that the corrective phase was acceptable in terms of methodology and results except for the telecommunication equipment that need to be more explicit, as EDF relies on manufacturer validation.

The IPSN noted that EDF has still to achieve some actions to be ready : (1) the date forcing or the windowing of some equipment (PCs essentially) that were not corrected due to the low impact of the Y2K problem, (2) the bypass of equipment that were forecasted to be corrected and finally were not on some sites, and (3) the advices to operators for equipment that presents malfunctions and were considered by EDF as having a Y2K minor impact (like displaying the year of the date as «00 » on screen or printed paper). EDF will issue specific procedures beginning of December.

Regarding the achievements on site, the IPSN has pointed out that national prescriptions and provisions are not fully implemented at the end of the first semester, especially concerning the training of the personnel.

### 8.3.2 Preventive phase

The IPSN agreed on the methodology of this phase that encompasses a systematic functional analysis to cross check the corrective phase results, and a sensitivity study to external resources to identify weaknesses (postures and dependencies) and to decide provisions in accordance to. Especially, this phase covered all the plant systems that are necessary for the safety demonstration during the millennium roll over, period where the risk of a common cause failure increases. The results did not show any discrepancies regarding the systems and application software identification made in the corrective phase, except for one system out of 535. It comforts the confidence in the corrective phase.

Two programmed changes, related to the operation of the diesels auxiliaries (emergency power) and the electrical protections of bus bars (condenser pumps), will be implemented in advance to increase the probability of successful house load and lower the risk of a loss of on site power.

Nevertheless, the IPSN has raised the question of the potential consequences in case of common mode on units of the same series. EDF has produced a study that shows no generic problem. This study identified the systems that are common to all plant functions (general purpose logic system, closed loop regulation, reactor control and protection) and those that are specific and contribute to production of electricity (turbine governing system, turbine protection system and turbine generator remote control system). Those that are of analogous technologies were examined to confirm the absence of any component that could be microprogrammed and the digital equipment were assessed to show evidence of Y2K compliance or the efficiency of the correction when needed. EDF concluded that there is no risk of common mode failure in the functionally important systems.

Regarding the periodic tests after the 1<sup>st</sup> of January, the IPSN has underlined that EDF has not changed the planning of that activity. The necessity to track potentially residual malfunctions that may prevent safety systems to correctly command the actuators requires an early experience feedback, e.g. during the first quarter of the year. EDF has to address that point and give the safety authority the list and the schedule of important periodic tests, together with the justification for that choice.

The major issue of that phase, i.e. a large loss of off site power, has been correctly assessed by EDF. EDF adopted deterministic hypotheses for designing the corresponding case study : (1) no general loss of grid, (2) a possible regional loss of off site power cumulated with a non systematic failure in a unit. EDF justified these hypotheses on the basis of the corrective phase and the functional analysis results, together with the provisions related to the precautionary postures and the repowering plans. In particular, EDF has specific provisions to manage the means that are common to units of the same site (rough water tanks, emergency mobile turbine). The IPSN noted that EDF excluded a loss of off site and on site power onto twin units of 900 MWe, the design of which imposes to share the high pressure pump used to maintain primary circuit integrity (primary pump seal injection). This situation has been shown of a very low probability due to the repowering strategy on site.

The final step is to implement the provisions that were decided consequently to the results of the preventive phase. This will be in place by the end of November. Information is required about the correctness and effectiveness of their implementation.

### **8.3.3 Defensive phase**

EDF achieved the first step of the defensive phase. This includes definition of the scenarios to be taken into account for the Y2K crisis plans and definitions of operator awareness and training plans.

The IPSN assessed the methodology and the results applied to define the Y2K crisis plans, against the principles adopted for an on site emergency plan. EDF has added Y2K teams to the nuclear crisis organisation, taking in account the variable level of risk from December the first to March the thirty-first. The sizing of the EDF local and national teams is based on the following hypotheses : (1) some non generic computer systems malfunctions on few units, (2) a regional loss of power on grid, (3) a degraded situation on two sites that need assistance from the national crisis centre, with only one site triggering the on site emergency plan. The IPSN has concluded that, in the context of EDF assumptions, the national teams are set up correctly. However, EDF has still to confirm that local teams profiles conform to the national prescriptions presented to the safety authority. The IPSN highlights the need for a working method (to be used by the national teams) that allows for the follow-up of all the PWR units, specifically in case of Y2K events without any on site emergency plan triggered.

Concerning the operator awareness and training plans, the IPSN noted that the sites staff and operators have been informed on the EDF Y2K national level actions. Especially, EDF has planned training on loss of off site power scenarios for operating teams that will be on duties for the millennium roll over period. It is considered necessary that sites staff and operators have the last release of the impacted system and software application list before the last training period planned in December. This list will provide relevant information on the Human Machine Interfaces modification due to corrections or minor impact of the Y2K problem. EDF has done a drill that simulates a crisis on two different sites (October 27th, 1999). The whole EDF site and national teams were acting in contact with the correspondent teams from the safety authority and the IPSN.

### **8.4 General conclusion on French PWR readiness regarding the Y2K problem**

The Y2K action plan is not yet completed. The French PWR units and the supporting organisation in EDF are on the way to be ready for the roll over. The IPSN assessments show acceptable methods and means put in place to deal with the Y2K problem satisfactorily and to be prepared to residual events that could occur during the millennium roll over period. An important effort was done by EDF to show evidence on the preparedness. During the second half of the 1999 year, EDF will make the readiness effective.