OECD International Workshop
Hosted by
Atomic Energy Control Board of Canada
Ottawa 8 to 10 February 1999

Impact of the Year 2000 on the Nuclear Industry

The Year 2000

and the French nuclear facilities

J.-Y. HENRY
P. RÉGNIER
S. MANNERS
F. DAUMAS

Institut de Protection et de Sûreté Nucléaire
France

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 France and in other countries. In particular, the nuclear industry in France 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. In France, this programme is being examined by the Institute for Nuclear Safety and Protection (IPSN) in collaboration with the Safety Authority.

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 we are talking about the 19th century or the 20th. Therefore, the millennium bug could mean that one minute after midnight on 31 December 1999 some computers will think that it is the 1st 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 will delete records made at dates subsequent to (i.e. 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.

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 (i.e. DOS) or developed for applications (i.e. 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.

The difficulties in achieving millennium compliance

One estimation, made by the American Groups Gartner and Meta, states that on average one program (mainly management programs) processes the date every 50 lines of source code. For instance, it may be necessary to process the date in data recording formats, contents of computer files, data entry forms, processing logic, printing and display formats, maintenance and use procedures, etc.

Therefore, the first and main difficulty to be overcome in order to deal with potential millennium malfunctions is *to identify all the parts of the computer systems requiring correction*.

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 (i.e. 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. Nevertheless, 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.

The main worry is that one or more computer systems could fail at the same time, triggered by the millennium bug.

Determining an analysis strategy at the IPSN

The nuclear operators (EDF, COGEMA, etc.) are responsible for the actions which need to be taken to ensure that nuclear installations are safe during the millennium transition. In 1997, the IPSN worked out an approach to analyse the problems the millennium bug may present for computer systems. 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 computer and control systems, human factors, operation and accident management.

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

- a specific organisational system for analysing and dealing with the millennium bug problem,
- 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 the longer term, including the possible loss of national power supply,
- an organisation which ensures, by carrying out tests for example, that the modifications made to non millennium-compliant equipment are effective,
- a specific plan of action to implement the contingency measures necessary to obtain defence-in-depth, that is to say which make it possible to manage an abnormal situation caused by the millennium bug.

The IPSN's approach also tackles the specific cases of other dates which present the same type of risk to computers as the millennium bug, by encouraging operators to broaden their investigations as possible as they can.

A specific organisational system

An organisational system dedicated to the millennium problem must be set up to determine and supervise tasks to be carried out. Decisions regarding the co-ordination of the aspects of the different responsibilities within the organisation must be taken by top management. The use of the teams and standard resources of the organisation is preferable for actions associated with impact analysis. Different teams should check these tasks.

An analysis of installation sensitivity

The first step is to make a list of the computer systems and applications. The exhaustiveness of the list must be checked using other means (i.e. by functional analysis of the installation).

The second step is to make a list of the computer applications and systems actually affected by the millennium problem. An analysis of the functional consequences of potential failures of systems and applications can be used to make a study of contingency measures.

A study of resources

The installation must observe safety criteria in the event of internal failures due to the millennium bug. It is also necessary to study the impact that malfunctioning of external resources necessary for operation of the installation could have in the long-term. In this context, human and material resources, which are external to the installation (power supply, water make-up, fire brigades, etc.) must be taken into account.

An organisational system for tests

After the impact analysis and conversion decision, actions aimed at replacing a computer application or system or at correcting errors, must be followed by checks. In all cases, after a new or corrected computer application or system has been delivered to a facility, it is important that a series of tests be carried out to ensure that the solution adopted is compatible. This must be organised in such a way that the installation and the on-site acceptance of the different computer applications and systems comply with the availability of the systems required to maintain safety.

Contingency measures

The analysis of computer applications and systems cannot set out to detect all the sources of malfunctioning caused by the millennium bug. It is therefore necessary to implement specific measures capable of preventing this common mode failure. These measures are determined from the functional analyses and the ability to make the proposed solutions available to the installation after the conversion decision.

Conditions for correct analysis

The basic design principles of a nuclear installation are based on studies including safety margins considered to be sufficient. The latter must be revised in the event of a common mode failure liable to affect installation systems and not treated as such. For this reason, the millennium bug must be analysed taking the following two aspects into account.

The safety case of the installation must remain valid in the presence of the consequences of the millennium bug. In particular, the common mode failure caused by the bug must leave available, not only the actual systems which ensure the safety of the installation, but also the shared response resources in the short and long-term.

The consequences of malfunctions must be considered during the year 2000, whether they appear during the management of an accident or during normal operation.

In the latter case, resources important for safety, that have to be millennium-compliant, must be identified with the following two points in mind:

- avoiding all abnormal releases, and in all cases, limiting releases to those authorised for normal operation,
- maintaining a sufficient level of defence-in-depth.

Analysis of PWRs

The IPSN has paid particular attention to the more specific case of EDF pressurised water reactors (PWR) for two reasons. Firstly, because a PWR is a nuclear installation whose safety level must be maintained during the millennium transition. Secondly, it is important that the supply to the national grid be uninterrupted.

EDF has informed the Safety Authority of the method it has chosen to assess and deal with the risk to nuclear power plants stemming from the millennium bug. This method is being assessed by the IPSN, in particular on the basis of the points in the questionnaire which it has drawn up.

In addition to the assessment of the method, and with a view to ensuring the relevance of the approach taken by the operator, the IPSN has started a technical assessment of the detailed design work carried out by EDF. This technical assessment is based on:

1- a methodological approach, based on the analysis of the method adopted by the operator to ensure that the systems which may be affected by the bug are identified. EDF therefore divided these systems into seven packages (control systems, telecommunications, industrial computers etc.) and instituted a scale of priority for dealing with them. This scale shows the extent of the potential impact of failure of the systems, particularly in terms of security. Obviously, it is important that the operator is able to provide proof of an exhaustive record of the computer systems and their applications.

2- an organisational approach. The IPSN is kept informed, by three-monthly monitoring reports, of the progress of studies made by EDF and conversion solutions adopted for the systems affected by the bug.

3- A thorough assessment of certain files. These files either relate to the analysis of computer systems (impact study, conversion, tests, manufacturing) or to the contingency measures including operating aspects of the plant (operators and procedures), or to analyses specific to lack of external resources (i.e. loss of power supply on the national grid for a long period of time).

Analysis of other installations

Operators of other nuclear installations have addressed the millennium bug methodology and means that they have put in place for.

In the work frame of the evaluation, IPSN asked for dossiers corresponding to the phases of the operators approaches. For those of the licensees that did answer yet, IPSN has start a letter again asking for the demonstrative dossiers.

IPSN initiatives in support of its assessment

The IPSN has started working with other companies such as France Telecom, which have similar availability problems to those of EDF, in order to better assess, and increase its experience of, millennium bug related problems. The IPSN is going to carry out a conversion exercise on one of its computer systems. This exercise will provide information to judge the relevance of conversion scenarios, tests and manufacturing of computer systems.

IPSN's international actions

Actions are underway in many countries. Nuclear operators and national authorities have implemented plans to correct malfunctions due to the millennium bug and to manage situations where failures could occur despite the efforts made to prevent them.

The IPSN is holding on technical exchanges with American, Canadian and British safety organisations. It is actively participating in a number of technical workshops and international discussions organised by the International Atomic Energy Agency and the OECD.