IAEA-TECDOC-1111

Report of the International Workshop on Safety Measures to Address the Year 2000 Issue at Radioactive Waste Management and Nuclear Fuel Cycle Facilities, Vienna, 1–2 July 1999

(Supplement to IAEA-TECDOC-1073 and IAEA-TECDOC-1087)

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

August 1999

The originating Sections of this publication in the IAEA were:

Waste Safety Section
Nuclear Fuel Cycle and Materials Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

REPORT OF THE INTERNATIONAL WORKSHOP ON
SAFETY MEASURES TO ADDRESS THE YEAR 2000 ISSUE AT
RADIOACTIVE WASTE MANAGEMENT AND NUCLEAR FUEL CYCLE FACILITIES,
VIENNA, 1–2 JULY 1999

IAEA, VIENNA, 1999
IAEA-TECDOC-1111
ISSN 1011–4289

Printed by the IAEA in Austria
August 1999

FOREWORD

In resolution GC(42)/RES/11 on "Measures to address the Year 2000 (Y2K) issue", adopted on 25 September 1998, the General Conference of the International Atomic Energy Agency (IAEA) — inter alia — urged Member States "to share information with the Secretariat regarding diagnostic and corrective actions being planned or implemented by operating and regulatory organizations at … fuel cycle facilities … to make those facilities Year 2000 ready", encouraged the Secretariat, "within existing resources, to act as a clearing-house and central point of contact for Member States to exchange information regarding diagnostic and remediation actions being taken at … fuel cycle facilities … to make these facilities Year 2000 ready", urged the Secretariat "to handle the information provided by Member States carefully" and requested the Director General to report to it at its next (1999) regular session on the implementation of that resolution.

In response to resolution GC(42)/RES/11, the Secretariat convened:

— a group of consultants who met in Vienna from 20 to 22 January 1999 and produced a technical document (IAEA-TECDOC-1073) entitled *Safety Measures to Address the Year 2000 Issue at Radioactive Waste Management Facilities;* and

— a specialists meeting in Vienna from 24 to 26 March 1999, which produced a technical document (IAEA-TECDOC-1087) entitled *Potential Vulnerabilities of Nuclear Fuel Cycle Facilities to the Year 2000 (Y2K) Issue and Measures to Address Them*.

To foster information exchange and share existing experience the IAEA held an International Workshop on Safety Measures to Address the Year 2000 Issue at Radioactive Waste Management and Nuclear Fuel Cycle Facilities in Vienna on 1–2 July 1999. Whereas the focus of TECDOC-1073 and TECDOC-1087 had been on identifying relevant safety issues in relation to Y2K computer problems and on proposing methods to address them, the focus of the International Workshop was on sharing experience, setting priorities, developing work-around strategies and preparing contingency plans.

The results of the International Workshop are based on contributions by the participants (see the list of contributors to drafting and review). The International Workshop was chaired by R. Weh, Germany, and the Scientific Secretaries were E. Warnecke, Division of Radiation and Waste Safety, and R. Shani, Division of Nuclear Fuel Cycle and Waste Technology.

DISCLAIMER

It is the responsibility of each Member State to ensure that all its equipment is Y2K compliant or ready. In these circumstances, it is for each Member State to evaluate the information received from the IAEA and make its own independent judgement as to the value and applicability of that information with respect to Y2K compliance or Y2K readiness in that Member State. Accordingly, the IAEA cannot accept any responsibility or liability with respect to the use by a Member State of any information received from the IAEA relating to the Y2K issue.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. Background

In September 1998, the IAEA's General Conference adopted resolution GC(42)/RES/11 on "Measures to Address the Year 2000 (Y2K) Issue". In response to that resolution, the IAEA convened meetings on Y2K issues at — inter alia — radioactive waste management and nuclear fuel cycle facilities in order to assess such issues and provide assistance to Member States in dealing with them. The results of those meetings are summarized in two IAEA-TECDOCs [1, 2] which were widely distributed in order to alert and assist those responsible for dealing with Y2K issues on a national basis and to contribute to the safety of facilities by achieving Y2K readiness in time.

A major problem encountered in the assessment of Y2K issues at radioactive waste management and nuclear fuel cycle facilities is the great diversity of facilities, ranging from facilities managing high level waste to facilities dealing with decay waste, or from uranium mining and milling facilities to spent fuel reprocessing plants. The same diversity can be found as regards the Y2K issues and it is therefore important to clarify at the outset whether or not date sensitive computer based systems are involved in the operation of a facility. If a facility does not have any computer based equipment or if such equipment is not date sensitive, then the facility can be declared Y2K ready [1]. Facilities that cannot be declared Y2K ready should be examined in accordance with the basic process outlined in Ref. [3].

As a follow-up to earlier activities, the Secretariat convened a Technical Committee Meeting/International Workshop on Safety Measures to Address the Year 2000 Issue at Radioactive Waste Management and Nuclear Fuel Cycle Facilities (hereinafter referred to as "the workshop").

1.2. Objectives

The objectives of the workshop were: to provide a forum for the exchange of information on safety measures related to the Y2K issue at radioactive waste management and nuclear fuel cycle facilities, in particular recent information which could be used in updating the above two IAEA-TECDOCs [1, 2]; and, in view of the fact that only a few months remain until the year 2000, to set priorities for further actions, including the provision of support to those who have started late with the assessment of Y2K issues.

1.3. Scope

This report deals with Y2K issues related to radioactive waste management and nuclear fuel cycle facilities. It supplements and updates TECDOC-1073 [1] and TECDOC-1087 [2].

The focus is mainly on the experience gained, the prioritization of activities, "work-around" strategies and contingency plans.

2. EXISTING EXPERIENCE

2.1. Experience gained

During the workshop it became evident that some countries had embarked on Y2K assessment activities early, using carefully developed procedures and detailed instructions. In

a second group of countries, the respective work is still in progress. A third group of countries is about to commence their work in this area now. Although the knowledge of the Working Group was limited, the available information indicated that some countries have not commenced the necessary assessment at all. For this category of countries, the following information on the experience gained so far may provide support to set priorities and to establish contingency strategies in order to save time and to allocate resources in the most effective and efficient way.

2.2. Basis of study

The following information is based on a completed study of radioactive waste management and nuclear fuel cycle facilities including some 75 000 Y2K systems or items. These are actual results from a series of Y2K projects. Of these items, approximately 10 000 represent different items, and the rest are duplicates. The items examined include those which were known to be date dependent, those which might have been date dependent and all safety systems, regardless of their date dependencies. The results are provided from only one country but it is assumed that they may comply with those gathered in countries operating similar nuclear installations. The results also confirm that the issues identified in TECDOC-1073 and TECDOC-1087 are still valid and that no new issues have been identified.

In the reporting country, assessment and remediation activities started early, as a large number of systems were expected to be affected by the Y2K problem. In cases where time is limited, it might not be possible to conduct a study with the same level of detail. In these circumstances, it may be worth prioritizing the potentially date dependent safety systems.

2.3. Categorization of systems

In order to set priorities in case of an unexpected workload, the systems were categorized as Priority 1, 2 or 3 based on the potential impact they might have, should they fail.[1]

Priority 1: Includes systems whose failure might result in death, serious offsite environmental or radiological impact or serious legal implications. This automatically includes all primary safety systems (protection systems).

Priority 2: Includes systems whose failure might result in serious personal injury or contained environmental or radiological impact. This automatically includes all secondary safety systems.

Priority 3: Includes systems whose failure might result in a minor safety effect. This would also include support systems such as personnel and finance.

---

[1] Since operators need not only to take safety aspects into account but also the justified commercial interests of their customers, the categorization of systems also included the following commercial consideration:

Priority 1: significant commercial loss (>$5 million)
Priority 2: moderate commercial loss (>$1 million)
Priority 3: minor commercial loss (>$100 thousand).

These were the values chosen in an individual case. In other cases and other countries, differing monetary values may be appropriate due to differences in the overall economic situations.

The following table shows the number of systems tested and their breakdown into the above categories.

Category	Approximate number
Priority 1	10 000
Priority 2	55 000
Priority 3	10 000

The high number of Priority 2 items reflects the inclusion of a large number of safety systems that were ultimately not found to be date dependent. This relationship corresponds to results gained in another reporting country.

It should also be noted that supplier information was often found not to be accurate. Therefore, it is an important part of the Y2K methodology that two independent pieces of evidence are needed to certify the Y2K compliance of a system (such as testing or inspection and supplier information).

2.4. Overall failure rate

Virtually all of the Priority 1 safety systems contained no Y2K problems. This is a result of the deliberate design philosophy of excluding programmable devices from primary safety systems. Whether this applies to comparable systems in other countries remains to be assessed individually. However, safety systems which belong to the Priority 1 category are in general deliberately designed in such a way as to take into account any conceivable failure.

An overall failure rate of between two to three percent was found among the plant systems tested. Ninety per cent of all of the systems identified were plant systems, including control systems, instrumentation, and embedded systems. Failures ranged from trivial failures to serious failures.

A significantly higher failure rate was observed among the data processing or information technology systems tested. These amounted to ten per cent of all systems identified. While these systems tended to have no immediate effect on safety, some did have a secondary effect on safety (for example, dosimetry, nuclear accounting, scheduled maintenance).

While many of the above system failures might pose minimal safety problems when considered individually, the cumulative effect of many simultaneous failures can adversely affect the concentration of operators or the confidence in systems and/or instrumentations.

2.5. Date information

The following table provides information on the observed Y2K failures with respect to critical dates.

Dates	% Failures
1999-01-01	0*
1999-09-09	0**
2000-01-01	>90
2000-02-29	<10***

* Two systems exhibited minor failures.
** In addition to the data in the survey, very few "plant" systems outside the nuclear industry were found to fail on this date.
***Mostly leap year effects (29 February 2000) but a few failures were found to occur on other dates (2027, 2155).

It is worth noting that the vast majority of Y2K effects were observed at the rollover to the year 2000. This may be taken into account in the prioritization of work if time is becoming short and in the development of contingency plans.

2.6. Examples of failures

Failure modes are of a wide variety depending on the nature and design of the systems under consideration. It was not possible to derive a systematic failure behaviour or a generic approach to the Y2K issues based on the results presented. Therefore, the following examples cannot be considered typical or exhaustive. They are intended to serve as guidance on how to approach Y2K issues, on what types of failures can be expected and how failures may be handled. Further details of observed Y2K failures are presented in Appendix 1.

2.6.1. Example 1

Environmental monitoring system

The environmental monitoring system collects readings of radiation levels from monitors throughout the facility. The software records information on radiation levels and eventual alarms. Time and date are taken from the clock of the server computer and stamped onto events as they occur. Events are displayed and stored in order of occurrence. The environmental monitoring system has also the capability of calculating trends.

Failure mode

The system does not handle year 2000 rollover and leap year function correctly. The records would be corrupt.

Remediation

Upgrade of the time system needed to be installed and PC upgrade was necessary to achieve full compliance.

2.6.2. Example 2

Gas analyser

The gas analyser is used to monitor and control the gas composition of furnaces to prevent explosive gas/air mixtures.

Failure mode

The system failed to indicate that a new calibration of the gas analyser was required.

Remediation

In this instance the calibration feature was not used and no remediation was carried out. However, if this feature had been used, it could have resulted in a potentially dangerous situation.

2.7. Further work

With precautions taken on the basis of the analysis described above, it is expected that Y2K readiness will be achieved. Nonetheless, detailed contingency plans are being drawn up for backup purposes in order to avoid any remaining risks, in particular because some of the risks are associated with external factors.

3. PRIORITIZATION

The IAEA-TECDOCs [1–3] offer advice on how to implement a Y2K strategy. The following advice is to help those who are just beginning their Y2K programme and are limited by time or resource restraints. It suggests ways of simplifying the approach by prioritization, taking into account the experience gained in different countries and the available best practice.

The approach suggested is to sort or prioritize by considering primarily the risk or hazard presented by the process. The given proposal for an approach to the Y2K problems is divided into four steps or four levels of investigations, respectively, in order to consider the major hazards of the plant, the main functions for operability, the indirect risks of operational failures and any remaining or undetected lack in compliance.

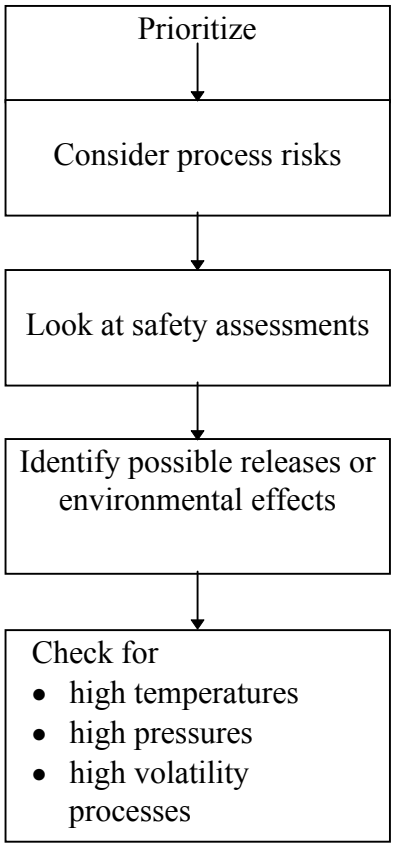
3.1. Major hazards

If there is no time to perform a detailed and complete analysis, the emphasis should be to focus on the main hazards that have severe or unacceptable consequences to the public or to the environment, in the following way:

Consider the major risks or hazards of each process. Examples of hazards are external releases and environmental effects. For all processes in enrichment, fuel fabrication, spent fuel

reprocessing, waste management or storage facilities and all related transports of hazardous materials a safety assessment is proposed by consulting existing documents. The major risks are evident in almost all cases, since safety assessments are carried out in the framework of the licensing process or for other purposes. These analyses should be taken into account as well as operational experience and known disturbances or incidents. The most vulnerable processes, as listed in the TECDOCs [1, 2], which pose major risks may be associated with high temperature, high pressure, high volatility processes, criticality, if applicable, or exothermal reactions.

A simple diagram depicts a stepwise approach together with individual decision elements, if time is of the essence:



3.2. Main functions for operations

If time permits, consider both operational and support functions or systems needed for continued operation and control of a facility. These functions and systems include, for example:

— security systems, including access control;
— health and safety systems, including radiation protection, criticality, explosion and fire protection systems;
— operational systems, including materials accounting and safeguards, if necessary;
— supplies of electricity, water, steam, gases and chemicals;

— quality management systems;
— communications (internal and external), particularly emergency arrangements, taking into account the extraordinary situation during the year 2000 rollover; and
— maintenance management systems.

3.3. Indirect hazards

Particular attention needs to be paid to indirect effects that can be caused by possible failure of the above functions or systems which may have no safety function primarily, but can lead to hazardous situations in the future (for example, loss of data associated with health and safety systems, security systems, material accounting and others).

3.4. Remaining or undetected compliance issues

Remaining or undetected compliance issues which could result from a lack of time or capacity for improvements or from incomplete investigations need to be covered by a contingency plan. Such a plan should be carefully designed and implemented individually for each identified potential source of risk. A special operating regime may be adopted to further minimize risks (see Section 4).

4. WORK-AROUND STRATEGIES

If countries or operators had a late start in investigating the Y2K issues it may not be possible to fully analyse and resolve all the issues. Even if the systems with the highest importance to safety are being addressed and probably made Y2K ready, a "work-around" strategy may have to be applied, in particular for systems that have not been addressed.

One example can possibly be changing the date to another leap year or, for example, to the year 1972, which computer programs treat as being identical to the year 2000. This strategy, which cannot be applied to embedded systems, may be limited to standalone computers, but not to computer networks, nor to situations where a system or process would otherwise depend on a date function. It should also be noted that newer systems may not run on the basis of the year 1972.

Another instance, for example, would be to stop production at critical dates or apply a special operating regime such as running a facility idle and not performing any transfer of radioactive material. The facility would be monitored during critical dates for any occurrences related to Y2K issues. If nothing happens, the facility could be brought back to full production. If date problems are encountered, the facility may need to be shut down, depending on the seriousness of the date problem. This may be done much more easily if a special operating regime is applied. As an alternative a contingency plan can be applied.

A third example could be to shut down a facility at critical dates if it is not Y2K ready. In such an approach it is of particular importance to ensure that the facility can be shut down safely, that it is in a safe state during shutdown and that safe operations without interference from date issues can be ensured upon restart. Restart is a very critical part because the date problems may continue to exist, because, for example, a two digit computer system may not be able to operate correctly with "00" for the year 2000. It is of utmost importance that the

regulators be involved in these matters. If there is any doubt about safety, they should decide that a plant must be kept shut down and not restarted until safety can be assured again.

It should also be noted that not all systems can be stopped or shut down, for example, the ventilation of buildings or the cooling of heat generating materials such as high level reprocessing waste or spent fuel. Contingency plans commensurate with the safety relevance of such systems should be in place at relevant dates, and emergency units or systems should be on alert. With respect to the year 2000 rollover it should be taken into consideration that telephone lines, independent of any Y2K issues, may not be available because of an overloading of the telephone lines by new year calls. Such situations should be discussed and resolved in co-operation with the respective telephone company.

5. CONTINGENCY PLANS

Even when the Y2K issues have successfully been managed in that all the hardware and software problems have been identified and resolved, or when an appropriate work-around strategy has been implemented, prudent plant management calls for contingency plans to be ready in case something has been overlooked or should go wrong. Contingency plans are even more important for facilities which had a late start into the Y2K compliance check and may not be fully Y2K ready. In such cases it might be more prudent to focus resources into work-around strategies and contingency planning rather than in assessing and testing computer systems for Y2K compatibility. Taking good account of the aforementioned precautions, such an approach can ensure that contingency plans are in place for the most critical systems so that any date failures will not cause unnecessary exposures and that incidents and accidents can be avoided.

Contingency plans should exist for nuclear facilities, independent of the Y2K issue. They should be reviewed and, as necessary, amended to cope with Y2K issues. It is essential that a contingency plan also covers the uncertainty of external supplies (electricity, water, etc.), regardless of how comprehensive a Y2K compliance programme has been. Predictions of infrastructure degradation or failure can only be dealt with by a contingency plan.

Guidance has been previously published to assist with the creation of this contingency plan [3]. A contingency plan should consider the following three items:

1. The contingency plan should define the systems that are needed to bring a plant in a pre-defined *safe state* in case of disturbances caused by failure of various internal systems or external supplies. Special attention should be given to the possibility of common mode failures.
2. The contingency plan must also define measures to keep a plant in a *safe state* regardless of the disturbances.
3. The contingency plan has also to define how and under what conditions a plant can be restarted.

The *safe state* will depend on the type of facility and can vary for performing idle operations with no movement of radioactive materials, stopping production and maintaining the facility in a quiescent state. Bringing a facility into a *safe state* can of course only be applied to facilities that do not carry out indispensable functions and, therefore, do not have to be fully operational over the critical date periods.

In terms of the aforementioned three points, the following items should be taken into account:

— Existing safety justifications should be consulted to determine the basis of how to bring a facility into a *safe state*. Existing shutdown procedures should also be consulted to bring a facility safely into a special operating regime, even if a facility should not need to be fully shut down. Existing contingency plans will not take into consideration the real possibility of common mode failures. An example of this is to replace a faulty monitor with an existing spare unit. The spare unit may also have the Y2K failure mode present.

— In a Y2K scenario, the identified external supplies such as electricity, water and emergency services, may be degraded or unavailable. Additional thoughts are required to ensure that a robust plan is in place which demonstrates alternatives to what can be normally expected.

— One advantage in restricting operations is that it is thus possible to better control eventual common mode failures. However, restricting operations is contingent on having a start-up plan available. If possible, processes must be started up in a controlled sequence allowing time to identify eventual failures and appropriate margins to react.

The overall extent of the contingency plan depends on the detail of the compliance work undertaken. However, as there is a possibility that external services and infrastructure will be degraded, the above three issues are of importance.

For any facility that will not be able to complete a Y2K compliance programme, it would be prudent to focus on producing contingency plans rather than on performing assessment and testing. This should ensure that the most critical systems are identified and safety is improved.

Generic guidance on contingency plans is available in Section 6 of Ref. [3]. This guidance outlines a framework to help achieve safe operations through all the critical dates but does not determine which safety systems are most at risk. Appendices 2 and 3 reproduce Form-4 and Form-5 of Ref. [3] which can be used to achieve safe operations through the development of contingency plans.

Form-4 is a contingency plan to be used to identify and document Y2K dependent systems or items. It includes information on risk identification and classification; risk description, analysis and management; and validation.

Form-5 is an Integrated Contingency Plan Matrix. This matrix assists with the management of resources required to support the critical dates. It is made up of individual contingency plans for key systems or items.

The contents of an integrated contingency plan, see Section 6.2.2 of Ref. [3], include:

— Purpose and scope
— Relationship between individual contingency plans
— Responsibilities
— Resource scheduling
— Event response co-ordination
— Integrated action plan
— Training and awareness.

Implementation of a Y2K contingency plan requires the availability of appropriate staff. It also requires that necessary consideration be given to the following points:

— Staffing levels
— Competencies
— Authority
— Training
— Cover in event of sickness
— Transport
— Communications.

In setting up contingency plans it should also be taken into account, as explained earlier, that external supplies could affect the safe operation of a facility. Systems should be in place to mitigate consequences in the case that external supplies should be interrupted.

6. SUMMARY

The items discussed and the results presented during the meeting clearly showed that the Y2K issues are relevant to radioactive waste management and nuclear fuel cycle facilities. Some countries, in particular those operating large industrial scale facilities, made tremendous efforts to solve all Y2K related problems as completely as possible and in a timely manner. There was insufficient information to allow a representative overview to be prepared for the evaluation of the situation in countries other than those represented in the workshop.

The majority of the results presented and discussed were based on experience gained at a wide variety of facilities in terms of types, throughput, inventory, process complexity and safety/security requirements. This is why the results are regarded as being valuable for other countries; they should be taken into account by those countries which are not in a position to achieve Y2K readiness prior to the critical dates.

The results presented are based on a completed study including some 75 000 systems or items. Of these, some 10 000 represent different cases and the rest are duplicates. The observed Y2K failures clearly indicate the areas of interest. More than 90% of the problems were found to be related to the year 2000 rollover and less than 10% were related to the leap year date (2000-02-29). No serious problems were found in relation to other dates (e.g. 1999-09-09).

It was found that the overall failure rate of all the plant systems tested was only between two to three per cent. It cannot be concluded from this finding that Y2K issues are marginal, since these failures ranged from trivial to serious, and thus could have serious consequences. The evaluation of data processing and information technology systems showed a significantly higher failure rate (ten per cent). These systems (for example, nuclear accounting or dosimetry) cannot be neglected although they normally do not directly affect safety. Attention needs to be given to cumulative effects of many simultaneous failures.

Several countries or institutions did not initiate actions related to Y2K issues in time. In the workshop it became evident that in several cases it could be too late to carry out a full Y2K assessment and remediation. In order to provide guidance to such countries or institutions, the meeting focused on “prioritization”, “work-around” strategies and contingency plans.

The figures on the failures, as given above, indicate that the year 2000 rollover must be considered to be the most critical date. Nevertheless, it is indispensable to set priorities in carrying out any Y2K related work. Such priorities should be determined from a safety point of view. A safety assessment, as it should be available as a part of a licensing process, should clearly indicate the most safety relevant processes which are associated with the highest risks for occupational and public exposures or for non-radiological hazards. Such processes may involve, for example, high temperatures, high pressure or high volatility processes. In addition to the safety relevant items, infrastructure systems, for example, safety and security systems, quality management as well as communications should also be addressed. Such systems are important for safe operations, although they may not have a direct impact on safety.

In cases where an individual Y2K problem cannot be eliminated in a timely manner, a work-around strategy may represent an adequate solution. One example can possibly be the change of date to another leap year or, for example, to the year 1972. This strategy, which cannot be applied to embedded systems, may be limited to standalone computers, but not to computer networks, and to situations where a system or process would not otherwise depend on a date function. It should also be noted that newer systems may not run on the basis of the year 1972.

Another work-around strategy could, for example, be to stop production or to shut down the facility at critical dates. In the latter approach it is of particular importance to ensure that the facility can be shut down safely, that it is in a safe state during shutdown and that safe operations can be ensured upon restart, without interference from date issues. If there is any doubt about safety, a plant must be kept shut and not be restarted until safety can be assured again. It should also be noted that not all the systems can be stopped or shut down, for example the ventilation of buildings or the cooling of heat generating materials such as high level reprocessing waste or spent fuel.

Even when the Y2K issues have successfully been managed in that all the hardware and software problems have been identified and resolved, or when an appropriate work-around strategy has been implemented, prudent plant management calls for contingency plans to be ready in case something has been overlooked or should go wrong. Contingency plans are even more important for facilities which had a late start into the Y2K compliance check and may not be fully Y2K ready. In such cases it might be more prudent to focus resources into work-around strategies and contingency planning rather than in assessing and testing computer systems for Y2K compatibility. Taking good account of the aforementioned precautions, such an approach could ensure that the most critical systems are identified and that any unnecessary exposures or incidents and accidents can be avoided.

Appendix 1

FURTHER EXAMPLES OF OBSERVED Y2K FAILURES

The following table shows examples of real systems that have failed various Y2K tests.

Description	Failure mode	Remediation
Pager management software	Unknown failure ~ Manufacturer advised upgrade.	Manufacturer upgrade applied to make PC fully compliant.
Fire database software. This is a Visual Basic (v3.0) program operated from a desktop PC in the control room. This displayed information on facility which had fire alarm in operation.	The system stopped functioning on the year 2000 rollover.	Updated code and recompiled on latest version of Visual Basic.
Weather and tide monitoring system This gives real time weather and tide information on computer network, essential for safety in a site emergency situation.	Access 2.0 code and 486DX100 PC's fail to rollover correctly. This could lead to incorrect information being displayed.	Upgraded computers and operating system.
Access control card reader system This system is used for personnel accountancy and to restrict access to authorized personnel.	Main system does not handle leap year correctly and communicates to local processors. This device could stop functioning or corrupt data.	Manufactures upgrade applied.
Data reduction and logging equipment	Fail to recognize year 2000 correctly, causing incorrect readings or incorrect data storage.	Upgraded to compliant version of firmware in data logger.
Stepper motor controller	Two digit date format rolls over to 1900. Day and number of days in year wrong.	Management procedure to add extra day in year 2000. The dates are not used by the PLC for any calculation or decision.
Personal integrated dose recording system	Software will fail to roll over if PC non-compliant. This will affect trending and previous record information.	Upgraded PC to compliant one.
Alpha and beta monitor	This monitor fails to recognize the leap year 2000. No effect on operation as dates not used in operation.	Management work-around to add extra day.
The **SCADA system** within the cementation plant provides monitoring and data logging of a drum as it travels through the various stages of the cementation process. The system also logs all the relevant data about the drum and the process. The system provides a graphical interface for operators and real time monitoring of alarms. The SCADA system has no control functions.	This system will not roll over to 2000 and will use the BIOS date default. The software used will only represent the year in two digits.	1. Do nothing and manage displayed date. 2. Clock back as date used only for QA. 3. Upgrade PC and operating system.
Effluent samples/flowmeters. System used to monitor and sample site discharge.	System locked up at 2000-01-01.	All affected systems were replaced with newer models.
Emergency Control Centre. Alarm monitoring system. System used to centrally announce remote alarm in silent hours.	Many parts of the system failed Y2K tests, but system would have operated.	Custom software upgraded by supplier. New PC purchased.
Distributed control system	Failed both 2000-01-01 and leap year. Unpredictable operation.	Upgraded by manufacturer.
Minicomputer measuring fission products in post-irradiated fuel.		Upgrade unavailable. Year unimportant, so clock being turned back to earlier year.

Appendix 2

CONTINGENCY PLAN
FORM-4

Contingency Plan Number	
Specify Internal or External	
INVENTORY ITEM Number: (if applicable)	

PART A Risk identification (fill in as applicable to risk):	
Risk identification:	
System identification:	**FACILITY INFORMATION**
Identification number:	Facility identification:
Quantity:	Unit number (if relevant):
Name of the item:	**OWNER IDENTIFICATION (Responsibility)**
Support group / Responsible individual:	Department name:
Description and use of the item:	Department organization number:
Spares held? ☐Yes ☐No If yes specify quantity here:	Head of the department:
Vendor information:	
Manufacturer:	Version or model:
Vendor name:	Serial number:
Support (provided?): ☐Yes ☐No	Warranty position:

PART B Risk classification:			
The classification of this risk is:			
1 ☐	**2** ☐	**3** ☐	**4** ☐

PART C Risk description:

PART D Risk analysis:

PART E Risk management:	
Period of vulnerability:	
Implementation timing:	
Resource requirements:	
Subject matter expert:	
Mitigation strategy:	
Training required:	
Exit strategy:	

PART F Validation:	
1 Perform validation of contingency plan. Attach all test plans and documentation of results: ……. . ……. . ……. . ……. .	
2 Was validation satisfactory? If yes: go to Part F If no: investigate reason, correct problem, perform necessary steps again.	☐Yes ☐No

PART F Form completed by:	
Name:	
Position:	
Date:	Signature:
Approval signatures	
Date:	Signature:

Appendix 3

INTEGRATED CONTINGENCY PLAN MATRIX
FORM-5

CP No.	Item, System, Component	Risk description	Mitigation strategy	Period of vulnerability	Implementation timing	Resource requirements	Subject matter expert	Priority

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Measures to Address the Year 2000 Issue at Radioactive Waste Management Facilities, IAEA-TECDOC-1073, Vienna (1999).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Potential Vulnerabilities of Nuclear Fuel Cycle Facilities to the Year 2000 (Y2K) Issue and Measures to Address Them, IAEA-TECDOC-1087, Vienna (1999).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Achieving Year 2000 Readiness: Basic Processes, IAEA-TECDOC-1072, Vienna (1998).

CONTRIBUTORS TO DRAFTING AND REVIEW

Grillenberger, T.	Company for Reactor Safety (GRS), Germany
Ibbott, G.	Department of Radiation Medicine, United States of America
Joppen, F.	Nuclear Energy Research Center (SCK/CEN), Belgium
Lechner, C.	Austrian Research Center Seibersdorf, Austria
Mackay, D.	United Kingdom Atomic Energy Authority (UKAEA), United Kingdom
Moore, B.	British Nuclear Fuels plc, United Kingdom
Pallmer, R.	Scientech Inc., United States of America
Plekhanov, V.	Federal Nuclear and Radiation Safety Authority of Russia (Gosatomnadzor), Russian Federation
Shani, R.	International Atomic Energy Agency
Warnecke, E.	International Atomic Energy Agency
Weh, R.	Company for Nuclear Service (GNS), Germany
Woods, B.	British Nuclear Fuels plc, United Kingdom
Zambardi, F.	National Agency for Environmental Protection (ANPA), Italy

Technical Committee Meeting/International Workshop
Vienna, Austria: 1–2 July 1999