IAEA-TECDOC-1072

Achieving Year 2000 Readiness: Basic Processes

The originator of this publication in the IAEA was:

Special Projects Unit , DIR-Office of NSNI
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

ACHIEVING YEAR 2000 READINESS: BASIC PROCESSES
IAEA, VIENNA, 1998
IAEA-TECDOC-1072
ISSN 1011–4289

Printed by the IAEA in Austria
March 1999

FOREWORD

This document provides an approach for addressing safety and operability concerns related to Year 2000 (Y2K). Although written for nuclear power stations, the methods herein are largely applicable to other nuclear installations and to many industrial concerns. Insights from ongoing, world-wide, industry Y2K Readiness programs were extensively used in preparing this document.

The primary goal of this document is to provide a brief, but comprehensive, approach that may be used to discover, understand, and correct Y2K related problems. It may be especially useful to facilities that are starting their Y2K Programme at a late date. The approach is applicable to the entire gamut of software items from very large mainframe programs to embedded chips and micro processors. Guidance is also included for nuclear regulatory authorities to assist them in their related function.

The document relies upon certain basic expectations of the facility that would apply to any programme: ownership, management, knowledgeable participants, thorough application of the approach, documentation of efforts, quality assurance of products, and compliance with all regulatory requirements.

This document is not a substitute for national requirements, nor should it be used without first understanding such requirements that are applicable to a facility.

The IAEA has and will continue to be involved with Member States to assist them in implementing this document and achieving Y2K Readiness.

The reports issued together are: Achieving Year 2000 Readiness: Basic Processes; Safety Measures to Address the Year 2000 Issue at Medical Facilities Which Use Radiation Generators and Radioactive Materials; and Safety Measures to Address the Year 2000 Issue at Radioactive Waste Management Facilities. This document addresses basic processes for achieving Year 2000 Readiness.

DISCLAIMER

It is the responsibility of each Member State to ensure that all its equipment is Y2K Compliant or Y2K 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.

EDITORIAL NOTE

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

Very few companies or government agencies, can satisfy their operating commitments without software. As the turn of the century approaches, they face a significant and complex task: to resolve the Year 2000 (Y2K) problem in their software.

The problem occurs in some software because two-digit date fields were used to represent the year and the algorithms used may not be able to recognize the change to the new millennium and may misread "00" for the year 1900 instead of the year 2000. Others do not correctly identify the year 2000 as a leap year and risk failure at 29 February 2000 or 31 December 2000 (the 366^{th} day). Date related problems can affect software in mainframes, desktop computers, local area networks (LAN), digital control systems, and is sometimes embedded in facility equipment. It can also affect information residing in data files, databases, and libraries.

The most important realisation must be that many failure modes are possible and some can render equipment inoperable. This can result in a challenge to safety or operability.

The deadline and the consequences cannot be avoided. Defining the exact severity and extent of Y2K problems at any given facility can be complicated by many factors:

- A diverse software inventory,
- Embedded systems that are difficult to detect and test,
- The potential need for regulatory review of resulting changes,
- Remediation costs that are a challenge to predict,
- Difficulties in obtaining information from vendors,
- Limited time to identify and correct the problem, and
- Significant staff requirements.

This document suggests a strategy for a facility Year 2000 Readiness Programme and is part of the assistance offered by the IAEA to address nuclear safety concerns related to this important issue. This strategy emphasises the essential elements, explains their importance, and provides guidance for accomplishing the Programme. The Programme consists of four principal phases:

- Initial Assessment,
- Detailed Assessment,
- Remediation, and
- Contingency Planning.

Figures 1 and 2 illustrate the sequence of events and the variety of activities that comprise the Programme.

2. Y2K PROGRAMME MANAGEMENT RESPONSIBILITY

The Programme Manager at each facility is responsible for the management of the Programme. They are responsible to the facility management, which is responsible for the safety and operability of the facility. The Programme Manager accomplishes the objectives of the Programme by implementing the steps identified in this document.

The Programme Manager:

- Creates or modifies the procedures and control measures that are required,
- Identifies those responsible for accomplishing activities,
- Schedules items in the various phases,
- Documents the major milestones.

The control measures (e.g. procedures) should be applied throughout the Programme to include all implementation activities. Existing measures such as work control systems, facility modification procedures and surveillance procedures may be employed as long as the Programme Manager determines that they are suitable. These measures should ensure that an appropriate level of oversight of the Programme is performed, which may take the form of planned periodic audits, inspections at documented hold points, or reviews of approved documents. The control measures are structured to make sure that the performance of essential activities is supported by objective evidence.

Common control measures that should be specifically invoked by the Programme are:

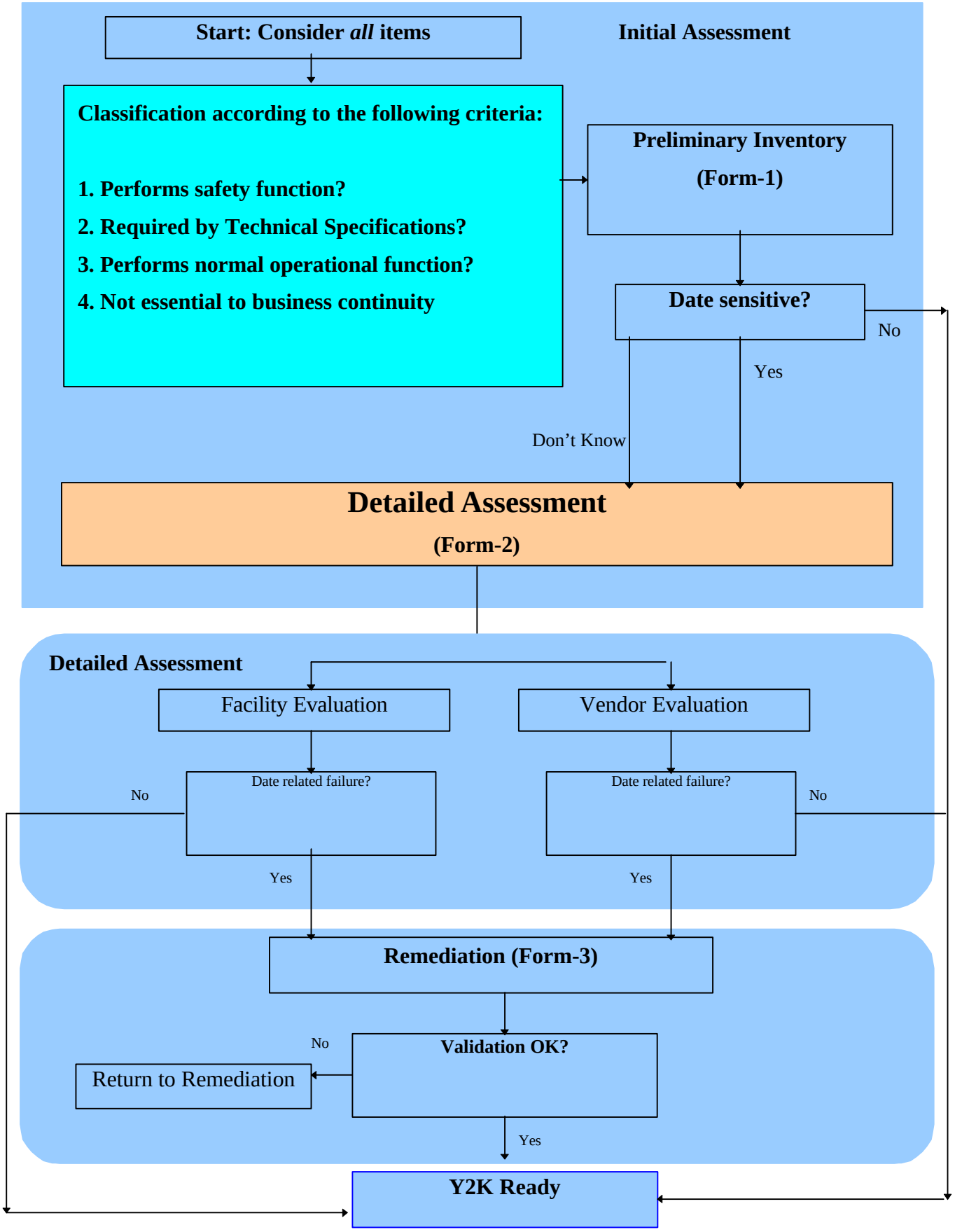
- Quality Assurance (or Oversight),
- Document Control, and
- Regulatory Compliance.

The measures should also ensure that the Programme:

- Activities are staffed reasonably and are achievable,
- Personnel are qualified,
- Decisions are based upon the facility priorities,
- Addresses all on-line and off-line systems,
- Includes equipment that does not pose a radiological hazard but is important to the operation of the facility,
- Is periodically reviewed by management and oversight authorities.

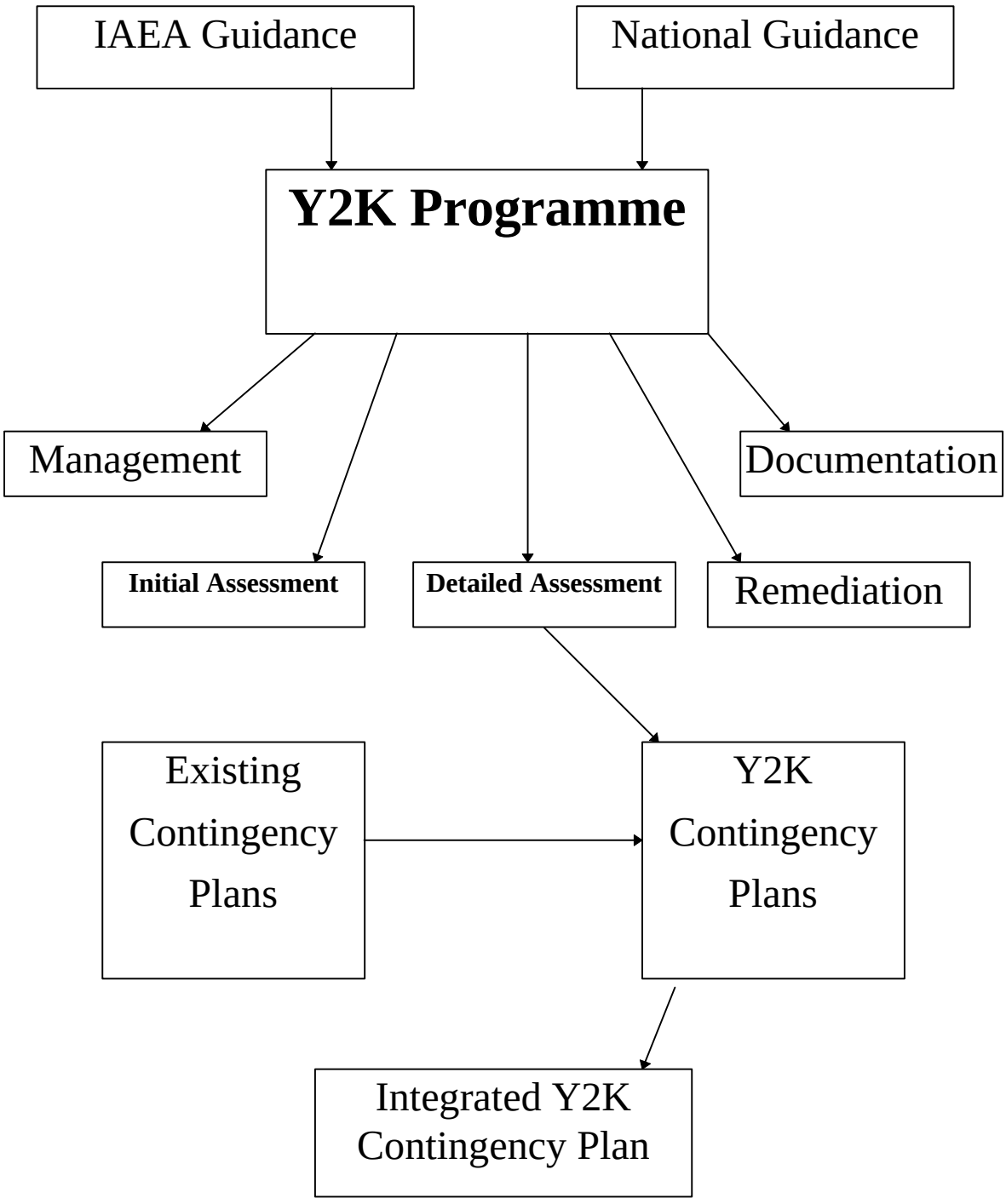
The Programme Manager will need to obtain resources from a sponsor. While this sponsor may be the facility management, a government ministry, design group, or some other benefactor to the Programme. To accomplish this it may be necessary to provide an awareness to the sponsor to enable them to appreciate the importance of the Programme.

The Programme Manager documents the progress of the Programme in status reports to the Programme Sponsor and appropriate members of the installation’s management. These reports should include details of Key Performance Indicators (KPIs) such as numbers of items addressed, expenditures, the current disposition of resources in the field, and schedule status.



Simplified Logic Diagram of Programme

Figure 1



Overview of Programme Contents

Figure 2

3. INITIAL ASSESSMENT (FORM-1)

The purpose of the Initial Assessment is to establish an inventory of the items that are required to be reviewed, determine the importance of each item to the facility, and schedule those items that require further analysis during Detailed Assessment. Initial Assessment is the first step towards accomplishing the Y2K Readiness of each item.

Initial Assessment, as described in this document, employs a method that takes a potentially large population of items and reduces it to the minimum appropriate population. The traceability of important devices is maintained. This is accomplished by judgements that should be fully within the discretion of the facility Programme Manager.

Initial Assessment is a phase that includes certain decisions. The first is Classification which determines whether an item is of sufficient importance to be included. Preliminary Inventory Analysis provides an objective means for excluding items from the inventory. Together these processes help to ensure that subsequent phases focus on items of importance to the Programme.

3.1. Classification

Each item to be processed within Initial Assessment is classified according to its importance to the facility. Classification should be done in parallel with the Inventory described below. The classification terms recommended and used elsewhere in this document by number are:

1. An item that performs part of a Safety Function.
2. An item that performs a function required by Technical Specifications, Operating Rules, or their equivalent (this is often related to but sub-tiered to Classification 1).
3. An item that performs a normal operational function or is relied upon to support operation (this may be also interpreted as an item that is important to the continuity of business but is sub-tiered to Classification 1 and 2).
4. Other (items that require the attention of the Programme, but are not essential to the continuity of business).

Should a facility desire to use a different classification method than the one recommended they should also understand that other elements of this document may need to be revised also (such as the forms).

3.2. Inventory

Inventory establishes a list of items relevant to the Programme. The inventory is the basis for all subsequent work and provides information essential to the Detailed Assessment. It also provides auditable trail regarding the conduct of the Programme.

Two inventories are created by Initial Assessment: the Preliminary Inventory and the Initial Assessment Inventory. Both are described in the following sections.

For sites that consist of multiple facilities (multi-unit nuclear or fossil power units), unique inventories should be created for each facility and another inventory for site or shared items. Furthermore, items that are used in multiple systems (i.e., different System Identification

codes) within a facility should each be listed uniquely in the inventory. If multiple quantity is used for the same system, only one inventory entry is necessary.

Items should be uniquely identified and the relevant information recorded. The investigator should use Form-1 and enter information into Part A. How the item was discovered should be entered into Part B. Classification should be performed by the investigator and entered into Part C.

The source of items in the Inventory will include plant operating equipment, support items, and emergency equipment. Types of items that will appear in the Inventory include:

- Equipment containing embedded processors,
- Microprocessors,
- Logic controllers,
- Instrumentation containing digital components,
- Standalone computer systems and associated applications programs, operating systems and device drivers.
- Data files and databases,
- Communications networks,
- Man/machine interfaces.

The information should also be transcribed into a database. This will allow the review of Programme information by staff and management and will also allow the Programme Manager to track progress.

The Inventory should be constantly updated as additional items are identified. New items may be discovered at any time during the Programme.

3.2.1. Preliminary Inventory

Preliminary Inventory must be a comprehensive process. It is the most important since every other activity will rely upon its completeness. The personnel used to perform this activity should be intimately familiar with the facility and its culture. Their efforts should receive independent review and Programme Manager approval.

The objective is to discover items of concern to the Programme. It is essential that all systems pertaining to the operation of the facility be reviewed. Clearly this includes all safety systems, however, it is also important to obtain information on normal operation systems, off-normal (emergency) systems, support systems, and management systems. The use of the guidance in Appendix B is suggested. It is suggested that the following be reviewed to discover date sensitive items for the Preliminary Inventory:

- System walkdowns,
- Safety cases/analyses,
- Technical specifications,
- License submittals,
- Procedures,
- Design basis documentation,
- Work orders,
- Task descriptions,
- Surveillance worksheets,

- Design documents,
- Facility descriptions,
- Interviews with experts, operators, and technicians.

Particular care should be taken to ensure that embedded items are included, as they are difficult to detect. Examples of plant items and equipment, which may contain embedded microprocessors are: cranes, circuit breakers, control systems, instruments, remotely operated or automated valves, lifts and vehicles.

All items may be examined immediately to determine whether they are date sensitive. This is a judgement that should only be made by sufficiently experienced personnel having the requisite training. Generally, any item having a microprocessor or computer should be included in the Preliminary Inventory and further analyzed in subsequent sections.

Items that clearly do not have date sensitivity need not be carried forward from the Preliminary Inventory to the Initial Assessment Inventory.

This provision is included in the Programme because some organizations have accumulated inventories approaching 30,000 items just because they found electricity coursing through a device. This resulted in a burden on Detailed Assessment to determine that a fax machine was unimportant and needed no evaluation under the Programme. Neither did the analogue relay.

Items that are not carried forward into the Preliminary Inventory are not considered further by the Programme.

This activity should be completed for the entire facility before proceeding on to 3.2.2.

3.2.2. Preliminary Inventory Analysis

If information becomes available during Initial Assessment, but subsequent to entering an item into the Preliminary Inventory, that an item has no possibility of date sensitivity, the item can be noted on the Inventory form as Y2K ready. A complete justification, including documentation for the reasoning should be included in Form-1 Part D by the investigator. The results are then transferred to Part E.

3.2.3. Initial Assessment Inventory Formation

Items not Y2K Ready in the Preliminary Inventory are moved to the Initial Assessment Inventory by using Form-2. This Initial Assessment Inventory serves as the initial input to Detailed Assessment.

Since Inventory (in general) is a continuing activity throughout the Programme, it is possible that additional items will be discovered later in the overall schedule. Those that are should be entered into the Preliminary Inventory process. As a result the Preliminary Inventory Analysis and Initial Assessment Inventory Formation may be repeated several times during the course of the Programme.

3.3. Planning Items for Detailed Assessment

A review of each completed Inventory forms should be performed by the facility Programme Manager. They will establish the plan, prioritisation and schedule to consider items in the Detailed Assessment. The planning should consider:

- The Classification of the system,
- Competing schedules such as equipment replacement projects and plant outages,
- Priority of the system relative to others,
- Availability of qualified personnel,
- Number of items of a given type,
- Available funding.

The facility Programme Manager establishes this schedule, by filling out Form-2, Parts A&B and recording the schedule onto Form-2 Part C for each item. Form-2 is then provided to the investigator performing Detailed Assessment. The schedule should include not only a date for completion, but the estimated resources required for the Detailed Assessment (financial support, equipment, staff, etc.).

4. DETAILED ASSESSMENT (FORM-2)

The purpose of the Detailed Assessment is to obtain or generate sufficient information about an item to determine its expected behavior on critical dates. Form-2 is provided to document the activities accomplished. Detailed Assessment results are used to make decisions regarding Remediation and/or Contingency Planning.

4.1. Vendor Evaluation (Part E)

For items originally supplied to the facility by a vendor, the vendor should be contacted and their willingness or ability to support the evaluation of an item should be evaluated. The ultimate purpose is to determine whether the vendor will participate in the evaluation and will provide certification of an item’s performance. The licensee retains the ultimate responsibility for vendor performance.

For vendor supplied items that are supported, the facility Programme Manager should determine the appropriate instrument to obtain their support (purchase order, license agreement, regulatory requirement, etc.). The support may result in relying upon the vendor or arrange for co-operative efforts.

Where use is made of suppliers' information, there should be a clear evidence that these statements refer to the specific hardware and software configuration of the facility. The vendor should specify the means used to arrive at any conclusions that an item is Y2K Ready. If a test program is used the Programme Manager should determine the completeness of the approach.

Items determined by Vendor Evaluation to have date related problems should be scheduled for Remediation. Form-2 should be completed by the investigator including appropriate vendor information.

If vendor evaluations are relied upon for an item the section 4.2 provisions are not applicable.

4.2. Facility Evaluation (Part F)

If a vendor evaluation is not available or appropriate to an item, then a formal evaluation by the facility is required. The objective is to determine the acceptability of the item under consideration. Two methods are identified in this document.

4.2.1. Inspection

Inspection is one acceptable means available to determine the acceptability of an item. Possible techniques that may reveal the presence or absence of date sensitivities include, but are not limited to:

- Review of schematics,
- Review of design documents,
- Review of source code.

If Inspection conclusively proves that an item lacks date sensitivity it may be marked Y2K Ready in Form-2.

4.2.2. Investigative Testing

The purpose of Investigative Testing is to provide an objective evaluation of an item's date sensitivity. Items not determined to be Y2K Ready under Vendor Evaluation or Inspection should be subjected to investigative testing.

Where the source code is available it is possible to determine the functions which are date sensitive by performing searches on the source code. Thus, strings that are known to be associated with date functions can be detected. Arguments can then be made to limit the testing to those functions.

There are a number of date related occurrences that can cause failure. These include:

- Rollover,
- Date related triggers,
- Date range calculations,
- Utilities that deal with historical information,
- Statistics that contain date arithmetic,
- Rates that use date arithmetic,
- Histories and data archives,
- Date-time stamped entries used for alarms or reminders.

For in service equipment Investigative Testing should only be carried out after carefully considering the implications of failure. Testing which compromises safety in any way should be only performed on equipment that is not in service. If carried out without sufficient planning, testing may actually introduce faults into the system, some of which may remain hidden and be very difficult to detect and/or cause unexpected hazardous events.

A plan for each test shall be prepared, or an appropriate existing plan used, in advance of actual testing according to the facility procedures. This test plan should identify means to limit failure occurrences, the means to recover from them, and changes required because of the effects of the testing related failure. When testing computer systems, the tests should deliberately encompass the crossover points, i.e., entry to the day and exit from the day at

midnight. The tests should not simply ascertain whether or not the system keeps running – many will continue to run, but will produce erroneous results. So comprehensive testing of functionality and data consistency is required at each point.

A test plan for an item should consider:

- Facilities required to support the test,
- Detail of tests to be carried out,
- Data to be logged during testing,
- Safety precautions required during testing,
- Facility configurations required during the tests,
- Expected duration of tests.

Testing Guidance is provided in Appendix C. It provides details of a variety of tests that may be applicable to an item. They may be supplemented by the facility as necessary.

Where the decision is made to test the item while out of service, the configuration should be sufficiently representative of an in-service item. This provides confidence that the test results accurately mimic the behavior of an in-service item.

The tests should be sufficiently comprehensive to detect any adverse effect of the item's functionality due to date sensitivity. The correct behavior of the item beyond the critical dates may be established from the previous test results or design documents.

Provisions in the tests should include cycling power to the item off and on. This sometimes reveals date-related flaws that are the result of the "boot up" sequence.

If the item stores data for later analysis then a simple date test may not be sufficient. The routines that use this date must be invoked. Where a radio clock is used to set the date and time it may be necessary to obtain a special simulator to enable different dates to be input to the item.

Some special precautions are required where an item communicates with other items. For a proper test, the dates must be synchronized. Also the correct sequence of events must be ensured when testing these inter-dependent items. Tests should be performed with the item in all modes of operation.

After completing Investigative Testing the item should be marked Y2K Ready on Form-2 by the investigator. For those items that are NOT Y2K Ready the investigator shall complete Form-2 and obtain the signatures of the Programme Manager. The Programme Manager will then enter the item into the Remediation process by filling out a Form-3, Parts A&B.

5. REMEDIATION (FORM-3)

The purpose of Remediation is to address the failure modes identified in the Detailed Assessment. During Remediation the Programme Manager should track the timeliness of purchased materiel delivery and the progress of conversions, replacements, deletions, retirements, and vendor efforts. Remediation efforts that are not timely require Programme Manager attention.

Form-3 should be used for Remediation. The Programme Manager should ensure the application of appropriate software quality assurance controls. Procedures that accomplish these goals shall be utilised and created for such purposes if necessary.

5.1. Schedule Remediation (Part C)

A review of the Remediation Forms should be performed by the facility Programme Manager who establishes the schedule for Remediation. The criteria for setting priorities should consider:

- The Classification system,
- Competing schedules such as equipment replacement projects and plant outages,
- Availability of qualified personnel,
- Number of items of a given type.

The facility Programme Manager establishes this schedule, records it onto Form-3 Part C for each item and provides Form-3 to those performing Remediation. The schedule should include not only a date for completion, but the estimated resources required for the Remediation (financial support, equipment, staff, etc.).

5.2. Select Remediation Strategy (Part D)

Once an item has been determined to be susceptible to Y2K failures or that there is a likelihood of failure, a Remediation Strategy should be selected. Strategies include:

- Retire. This strategy removes the item from service without providing a replacement.
- Replace. This strategy removes the item from service and provides an alternate means of satisfying the function performed by the item.
- Modify. This strategy alters the existing item thus removing the noted Y2K problem.
- Work-around. This strategy provides a means for satisfying the functional requirements without correcting the Y2K fault.

A Work-around is not a preferred Remediation Strategy. They are, however, a pragmatic reality. They should be subjected to an analysis to ensure that they are achievable and safe. Consideration should include failure modes, interaction effects, and the consequences of failure upon staff resources. The investigator identifies the selected strategy in Part D.

5.3. Perform Remediation

5.3.1. Retire

This strategy removes the item from service without providing a replacement. The process employed should include removing an item from the safety analysis, technical specifications, operating procedures, surveillance schedules and facility documentation.

5.3.2. Replace

This strategy removes an item from service and replaces it with another. The replacement should be completely reviewed for Y2K failure modes and be Y2K Ready or Compliant.

Furthermore the replacement item must fully satisfy all requirements and should be subject to appropriate integration tests with systems that it interacts with.

5.3.3. Modify

Modification should be accomplished using the applicable facility procedures. Such procedures include those for facility changes, safety evaluations, quality assurance, documentation, personnel training, etc. the preferred result of Modification is to accomplish Y2K Compliance. However, in some cases an item cannot be made fully Y2K compliant. In such cases Y2K Readiness is an acceptable result. It is within the discretion of the Programme Manager to approve such Modifications.

During Modification it is important to ensure that date related data held in any item is not lost or corrupted. Modification should not affect other items that are still in service. Careful consideration should be given to the most appropriate time to implement changes to items.

It is essential to co-ordinate the Modification of interfaces between the items internal to the facility or to external organizations.

5.3.4. Work-around

A Work-around accomplishes neither Y2K Compliance nor Readiness. It acknowledges the problem and accepts or implements a solution that is acceptable, but not desirable for the long-term. An example of a Work-around would be date roll-back on January 1, 2000 to January 1, 1972 (1972 begins on a Saturday and was a leap-year, as is 2000). This should include the human factor components and their effect on the safety or other activities. Shutting down a nuclear installation over the critical-date periods constitutes work-around that should be regarded as a last resort. Work-arounds are for known problems that will happen and should not be considered as risks that are treated under Contingency Planning.

5.3.5. Identify Remediation Risks

The Programme Manager should continuously scan the schedule of Remediation activities to determine those whose Key Performance Indicators (KPIs) indicate they will not be completed by the required date; these are sometimes termed remediation risks.

Remediation risks may arise because of the:

- Availability of replacement components,
- Concern over vendor support,
- Scarcity of resources.

Upon such a determination the Programme Manager shall select an alternate Remediation strategy or apply additional resources.

Remediations believed to be at risk should be acted upon promptly.

5.4. Validation (Part E)

The purpose of Validation is to test the item's functionality subsequent to Remediation and determine that:

- Remediation efforts have acceptably addressed the Y2K problems noted during Vendor or Facility Evaluations,
- Unintended functions do not exist or have not been introduced,

- Required functionality of the item is adequately performed.

Technical experts shall propose the type and extent of testing to be performed during Validation (Part E). The recommendations shall be reviewed and approved by the Programme Manager.

Validation may be performed at several levels:

- Unit Testing focuses on functional evaluations of the logic (software) of an item,
- Integration Testing evaluates the inter-related logic (software) of related items,
- System Testing evaluates the integrated performance of hardware and software components of items.

Upon satisfactory Validation, the Programme Manager obtains from those performing Validation certifications, signatures, and documentation consistent with the requirements of the Programme. The certification should clearly indicate on Form-3 whether the item is Y2K Ready or Y2K Compliant.

6. CONTINGENCY PLANNING (FORM-4)

Contingency Planning is an integral activity to the Y2K Programme. Contingency Planning is a process that may begin at any time subsequent to Initial Assessment and may continue throughout the program. Programme Contingency Plans may utilize existing plans created for other purposes, such as Station Blackout, site emergency plans, or emergency operating procedures. Existing contingency plans (CPs) should be reviewed to ensure that they adequately address the issues of common mode failure or multiple failures that could occur simultaneously.

The primary goal of this Section is the preparation of Contingency Plans and of a single Integrated Contingency Plan. Contingency Plans are developed for specific risks from internal or external sources. The Integrated Contingency Plan is developed from individual Contingency Plans.

The following are the recommended steps for developing Contingency Plans:

- Risk identification - determines risks to the facility from Y2K-induced events.
- Risk analysis - reviews the identified risks, determines potential failure modes and consequences, and documents pertinent information.
- Risk management - uses information from risk analysis to determine mitigation strategies. It should consider Y2K-induced risks and their interdependencies.
- Validation - reviews the results of risk management and provides confidence that the contingency plan will effectively mitigate the risk.

Contingency Plans should be subject to the same elements of the facility processes and programs discussed under Remediation and should be submitted to the Programme Manager when completed. Form-4 is used to document a Contingency Plan.

The Integrated Contingency Plan (ICP) provides facility management with a comprehensive perspective of the risks associated with Y2K-induced failures. The Programme Manager should ensure a facility-specific Integrated Contingency Plan is developed. The ICP allows the facility management to posture the facility in such a way as to most comprehensively deal with events.

6.1. Contingency Plans

6.1.1. Risk Identification (Part A)

This document identifies two types of Y2K related risks that a facility can be subjected to:

Internal Risks

The Initial and Detailed Assessments and the Remediation phases of the Y2K Programme are designed to provide identification and Remediation for items that could degrade, impair or prevent operability or safety of the facility. However, there remains some possibility that items could still be subject to Y2K-induced events that affect facility operations. The purpose of internal risk contingency planning is to provide a logical approach to anticipate and prepare for such events and reduce their impact on the facility. Internal risks may arise because of improper application of the Programme including undetected failure modes.

Internal risks may be found by reviewing inventory and assessment results for devices and software. Items to consider as risks include:

- Systems with multiple, integrated digital control devices or software subsystems,
- Systems that use digital input from other systems,
- Systems for which significant remediation effort was required.

The investigator should review appropriate items and histories and select those items or systems that are of concern. This is a somewhat subjective process that requires knowledge of the facility, its systems, history of performance, and capabilities.

External Risks

External risks result from circumstances, conditions, or events that are not under the direct control of facility management. The purpose of external risk contingency planning is to provide an awareness of such events and the means for mitigation of the consequences.

External Risks may be discovered using the Boundary Analysis technique which postulates a boundary surrounding the facility as Figure 3 shows. Items, signals, information, or data that cross the boundary are candidates for investigation. This technique may result in a detailed examination of facility supply chains for critical services and consumables.

There are many documents and existing contingency activities that may be used to identify external events that may be of concern to the Y2K project. Examples include existing plans such as those for:

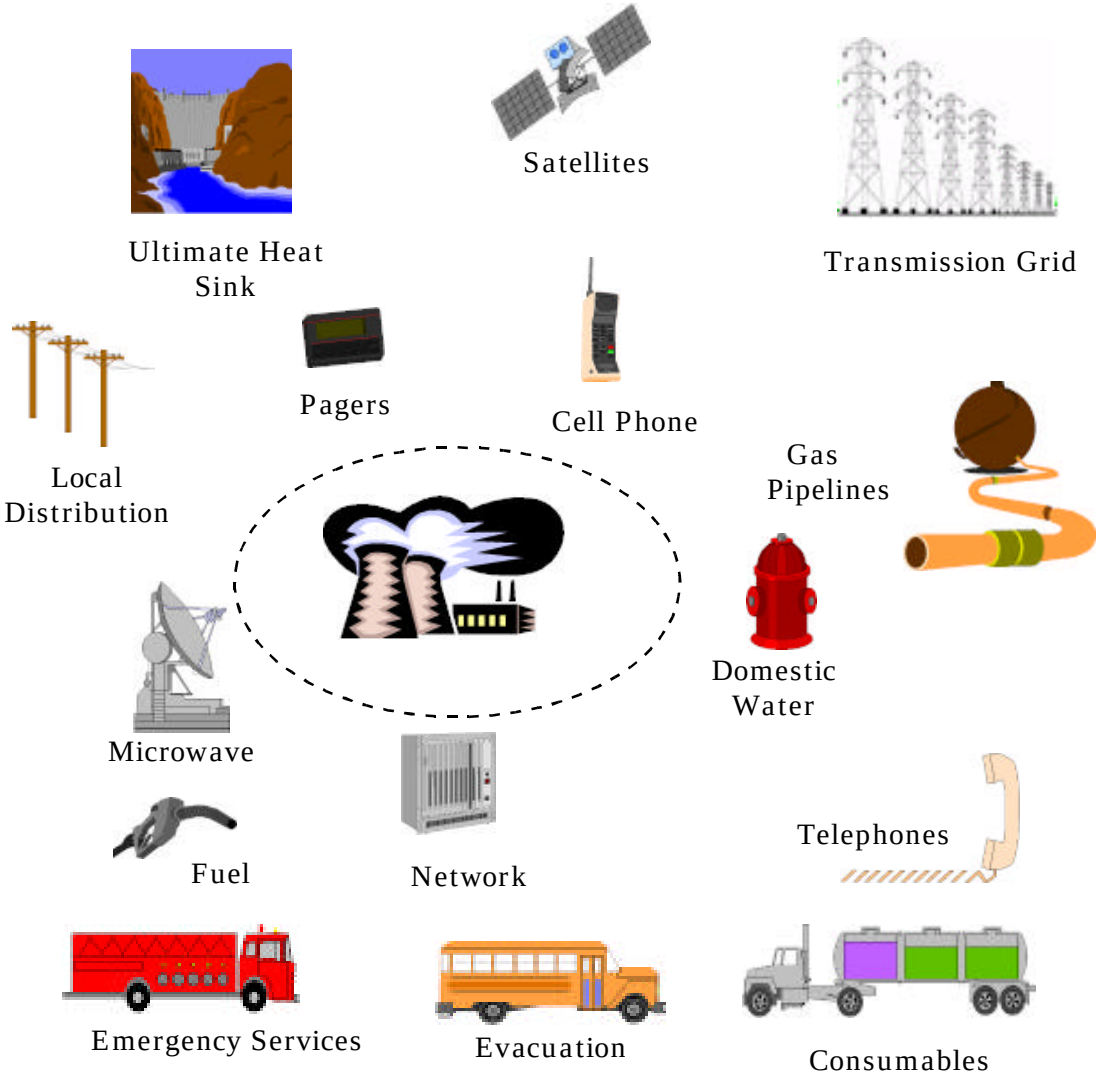
- Disaster recovery,
- Resumption of business,
- Station blackout,
- Grid restoration,
- Emergency preparedness,
- Storm restoration.

In addition investigators may consider it useful to review certain documents to assist them in identifying facility risks:

- Safety analyses,

- Facility descriptions,
- Design documentation,
- Maintenance records.

The investigators should document each identified risk on a Form-4, Parts A, B, C.



Boundary Analysis

Figure 3:

Boundary Analysis—Consideration of external events may be facilitated by the use of boundary analysis. This figure provides a graphic view to help visualize this process, along with items that may be considered. This is not meant to be a comprehensive list, nor is it required that each item indicated be addressed.

6.1.2. Risk Analysis (Part D)

The purpose of Risk Analysis is to understand and evaluate the implications of Y2K induced events to the facility. For each event, the responsible organization should consider the following:

- Consequence on safety or operability,
- Likelihood of occurrence,
- Potential for inducing other events, or changing the probability of their occurrence,
- Understanding when the facility is affected by an event - immediately, delayed, etc.,
- Determining the priority for resumption of service,
- Long-term effects of the events.

Risk Analysis should also consider the effect that complex supply or support chains may have on the mitigation strategy. A supplier may have a reliance on another supplier or service that is subject to Y2K-induced risks. A chain of failures in a complex supply chain may compromise more than is readily apparent.

6.1.3. Risk Management (Part E)

Risk management uses the information from Risk Analysis to determine the mitigation strategies that will reduce the risk to an acceptable level. Risk management may mitigate the risk or may extend the period of facility service pending resumption of the service or subsidence of the risk. This management function requires input from business and technical specialists. The two phases of risk management are Risk Notification and selection of the Mitigation Strategy.

6.1.3.1. Risk Notification

It is important to communicate to all involved organizations outside the facility the significance of a risk to the facility. These organizations may be requested to provide a description of their Programme elements that address the risk. The facility Programme should consider this information in determining the mitigation strategy. The evaluation should also consider the potential for the organization’s Y2K efforts to be successful.

6.1.3.2. Mitigation Strategy Selection

More than one mitigation strategy may be appropriate and employed. Some mitigation strategies that may be appropriate for consideration are:

- Facility alignment - Pre-set facility load or capacity to reduce the consequences to the facility of grid instability or voltage fluctuations. High-risk evolutions, such as refueling, reduced reactor coolant inventory operations or emergency diesel generator planned maintenance, should be scheduled to avoid Y2K critical dates, when possible.
- Minimize dependency - Stockpile consumables to support continued facility operation.
- Secure an alternate source - Most consumables are available from multiple sources.
- Employ an alternate process - Some services such as telecommunications may be accomplished using alternate methods.

- Rapid resumption of service - Where a proactive mitigation strategy is unobtainable or impractical, the management team may adopt rapid resumption of service as the recovery strategy.

6.1.4. Validation (Part F)

The risk management strategy should be validated. This process provides confidence that the strategy selected is capable of achieving the intended purpose, can be accomplished coincident with other strategies and includes personnel who are able to execute it. Methods that can be used for this evaluation may include management assessments, independent reviews, peer evaluations, external organization reviews, walk-throughs, drills or simulations.

6.1.5 Approval (Part G)

The Programme Manager and the appropriate facility management should approve all Contingency Plans. They should complete Part G.

6.2. Integrated Contingency Plan (Form-5)

The Integrated Contingency Plan (ICP) is a comprehensive document that will be used to manage the resources required to support the facility leading up to and during critical dates. Contingency plans are used to develop the ICP.

The Integrated Contingency Plan includes several items of information that are from the individual Form-4's submitted to the Programme Manager. There is one Form-5 for each facility and it is revised whenever a Form-4 is revised or created.

6.2.1. Integrated Contingency Plan Development

The Programme Manager is responsible for the development of the Integrated Contingency Plan. As Contingency Plans are developed, staffing requirements and actions are extracted and documented in Form-5. This matrix is then used to determine the overall resource requirements for the facility. Form-5 supports the generation of the ICP.

The final Integrated Contingency Plan should be reviewed and approved by facility management.

6.2.2. Integrated Contingency Plan Content

The Integrated Contingency Plan should include the following topics:

- Purpose and scope - includes the purpose and reasons for integrating the resources for a facility-wide approach to mitigate consequences. The scope establishes the boundaries for the plan.
- Integrated Contingency Plan Matrix provides the relationship between the Contingency Plans.
- Responsibilities - assigns responsibility for managing the implementation of the Integrated Contingency Plan.
- Resource scheduling - the plan coordinates timing and resources necessary for implementation of the elements of the ICP. This includes coordination between

departments, groups and outside agencies. Plans should specify items such as facilities, communications, status tracking and infrastructure support.

- Event response coordination - identifies the key decision-making processes for responding to events as they occur.
- Integrated action plan - summarizes the actions associated with the restoration of facility systems, components, and equipment.
- Integrated Y2K Contingency Plan training and awareness - identifies any specific training requirements.

6.3 Facility Posture

The facility management should carefully consider the status that they want the facility to be in on any critical date. This should consider the status of Remediation projects and guidance from the Integrated Contingency Plan.

Where possible, all invasive plant operations (e.g. on-line re-fuelling) should be avoided on critical dates. All required resources (e.g. fuel, communications, safety significant items) should be secured prior to each critical date.

The facilities' management should make sure that the staffing levels, staff competencies and levels of authority will be appropriate for the potential risk and consequences over each critical date. Staff should be adequately trained in all the facilities' Remediation changes (including work-arounds) prior to the critical dates. Staff should also be advised to be alert to potential system malfunction following each of the critical dates and should be aware of, and adequately trained in, the actions that should be taken in the event of the failure of any system.

7. REGULATORY CONSIDERATIONS

Nuclear regulatory authorities should ensure that their licensees are aware of the Y2K issues and are responding effectively to them; specifically, that each nuclear facility is pursuing a course of action similar to the Programme described in this document to ensure safety. Regulators also need to monitor the implementation of the Programme.

The approach proposed in this document forms a sound technical basis for an individual nuclear facility's Y2K Programme but does not restate or replace other requirements that also pertain (surveillances, safety evaluations, etc.) and are prescribed by the national regulatory bodies. Some additional considerations are included in Appendix D that regulators may use to assess a facility Programme. These requirements are somewhat specific to the language and terms used in the UK nuclear programme and may need to be reinterpreted to be applicable in another setting.

Regulators should also ensure that their own required items (particularly those systems required to monitor or react to nuclear incidents) are Y2K Ready. The regulatory bodies themselves will also need to be in an adequate state of alert during the critical periods.

REFERENCES

[1] “Effect of the Year 2000 Computer Problem on NRC Licensees and Certificate Holders”, U.S. Nuclear Regulatory Commission (NRC), Information Notice 98-30, August 12, 1998.

[2] “Nuclear Utility Year 2000 Readiness”, Nuclear Energy Institute (NEI) and Nuclear Utilities Software Management Group (NUSMG), Report NEI/NUSMG 97-07, Washington, D.C., October 1997.

[3] J. Henderson and G.I. Davidson: **“**Safety and the Year 2000”, Health and Safety Executive (HSE), Sheffield, U.K., 1998, ISBN 0 7176 1491 3.

[4] “Year 2000 Readiness of Computer Systems at Nuclear Power Plants”, U.S. Nuclear Regulatory Commission (NRC), Generic Letter No. 98-01, May 11, 1998.

[5] “Assessment of Licensees’ Safety Cases for the Year 2000 Computer Problem – NSD’s Y2K Assessment Principles”, Draft – For Trial Use, Revision 1, Nuclear Safety Directorate (NSD): Health and Safety Executive (HSE), UK, 23 September 1998.

[6] “Health and Safety and the Year 2000 Problem – Guidance on Year 2000 Issues as they Affect Safety-Related Control Systems”, Health and Safety Executive (HSE), U.K., INDG267 C1000 5/98.

[7] “A Definition of Year 2000 Conformity Requirements”, The British Standards Institution, BSI DISC PD2000-1.

[8] “Nuclear Utility Year 2000 Readiness Contingency Planning”, Nuclear Energy Institute (NEI) and Nuclear Utilities Software Management Group (NUSMG), Report NEI/NUSMG 98-07, Washington, D.C., August 1998.

[9] “Safety Assessment Principles for Nuclear Plant", Health and Safety Executive, 1992, ISBN 0 11 882043 5.

[10] "Embedded Systems and the Year 2000 Problem, Guidance Notes", IEE Technical Guidelines 9:1997, ISBN 0 85296 930 9.

[11] "Testing Safety-Related Control Systems for Year 2000 Compliance", Health and Safety Executive, 1998, ISBN 0 7176 1596 0.

[12] "Managing Year 2000 Conformity: a Code of Practice for Small and Medium Enterprises", BSI, DISC PD2000-2,1997, ISBN 0 5802 7445 4.

Preliminary Inventory

Form-1

INVENTORY ITEM Number: (Sequential numbers)	

PART A Item 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 organisation 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 Discovered by (circle appropriate items):			
Safety cases/analyses	☐Yes ☐No	Surveillance worksheets	☐Yes ☐No
Technical specifications	☐Yes ☐No	Design documents	☐Yes ☐No
License submittals	☐Yes ☐No	Facility descriptions	☐Yes ☐No
Procedures	☐Yes ☐No	System walkdowns	☐Yes ☐No
Documentation	☐Yes ☐No	Interviews	☐Yes ☐No
Work orders	☐Yes ☐No	Other, Specify:	☐Yes ☐No
Supporting Information (references, procedure checklists, etc.):			

PART C Item Classification	
Check one only (if more than one class is appropriate, select the lower number)	
The item performs part of a safety function	**1** ☐
The item performs function(s) required by technical specifications	**2** ☐
The item performs normal operational function(s) and is date sensitive	**3** ☐
The item performs other function(s) within the scope of the Programme	**4** ☐
If one of the above categories applies to the item, go to Part D. If none of the above categories applies to the item, disregard it. Go to Part F.	

Preliminary Inventory

Form-1

PART D Preliminary Inventory Analysis	
1 Is information about the date sensitivity of this item available? 2 Provide details, attach any relevant documentation (if available): **Vendor information:**……. ……. ……. **Facility Information:** …… ……. ……. …….	☐Yes ☐No
Is there sufficient data to conclude that the item is: Date sensitive or Unknown Not Date sensitive	Yes ☐ No ☐

PART E Information Regarding Y2K Readiness	
1 Based upon the activities in D, is the item Y2K Ready? 3 If No, this item will be carried forward to the **Initial Assessment Inventory.** Complete Form-2 for this item.	☐Yes ☐No

PART F Form Completed By:	
Name:	
Position:	
Date:	Signature:
Approval Signatures:	
Date:	Signature:

Detailed Assessment

Form-2

INVENTORY ITEM Number:	

PART A Item Identification (transcribed from Form-1)	
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 organisation 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 Item Classification (transcribed from Form-1)			
The classification (Preliminary Inventory) of this item is:			
1 ☐	**2** ☐	**3** ☐	**4** ☐

Detailed Assessment

Form-2

PART C
SCHEDULED FOR THE DETAILED ASSESSMENT **BY THE FACILITY Y2K PROGRAMME MANAGER:**
Name: Date: Signature:
Deadline for the completion of this Form: **Estimated resources required:**

PART D Further Information About This Item	
The following is to be completed by the owner of this item (Department):	
1 Is the item included in any modernization or maintenance programme? If the answer is yes: In which Programme?…… Person responsible for this programme (name): …….....……. Date of completion of the Programme:…….....	☐Yes ☐No
2 Are there more items of this type in the facility's inventory? If the answer is Yes, ensure that a Form-2 is processed and an inventory item number assigned to each such item.	☐Yes ☐No

Detailed Assessment

Form-2

PART E Vendor Evaluation	
1 Does the vendor certify the item to be Y2K ready for the purpose the item is used for in the facility AND is the vendor a trusted source of information? If Yes: go to Part-G and mark 1 Yes. If No: go to Part F	☐Yes ☐No

PART F Facility Evaluation	
Inspection:	
1 Review the source code, design documents, schematics, manuals, procedures, etc., that relate this item.	
2 Is there any evidence that the item contains a date sensitive feature? If yes: go to point 3 If the information available for Inspection is of sufficient quality and reveals no date related sensitivity go to Part G and mark point 1 as Yes. If don't know: go to point 3	☐Yes ☐No
Investigative Testing:	
3 Write or identify a test plan.	
4 Perform investigative testing. Consider affect on on-service equipment, the effect on safety, tech specs, operating requirements, and observe all precautions.	
5 Was there a Y2K problem related failure? If Yes: go to Part G and mark: Schedule for remediation If No, or if there is a failure that can be accepted (i.e., the remaining problems can be tolerated): go to Part G and mark: Item is Y2K Ready	☐Yes ☐No

Detailed Assessment

Form-2

PART G Result of The Detailed Assessment	
1 Item is Y2K Ready	☐ Yes ☐ No
2 If 1 is No, schedule for Remediation using Form-3	

PART H Form Completed By:	
Name:	
Position:	
Date:	Signature:
Approval Signatures	
Date:	Signature:

Remediation

Form-3

INVENTORY ITEM Number:	

PART A Item Identification (transcribed from Form-1)	
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 organisation 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 Item Classification (transcribed from Form-1)			
The classification (Preliminary Inventory) of this item is:			
1 ☐	**2** ☐	**3** ☐	**4** ☐

Remediation

Form-3

PART C
SCHEDULED FOR REMEDIATION **BY THE FACILITY Y2K PROGRAMME MANAGER:**
Name: Date: Signature:
Deadline for the completion of this Form: **Estimated resources required:**

PART D Perform Remediation	
1 Select Remediation strategy: ☐Retire ☐Replace ☐Modify ☐Work-around Provide details of Remediation and any potential affect on approved procedures, safety analyses, etc.: ……. …….. …….. ……..	

Remediation

Form-3

PART E Perform Validation	
1 Perform Validation and go to point 2. Provide details on the type (unit testing, integration testing or system testing) and the extent of testing. 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 Result Of Validation
Item is: ☐**Y2K Ready** ☐**Y2K Compliant**

PART G	
FORM COMPLETED BY:	
Name: Position: Date: Signature:	
Approval Signatures:	
Date: Signature:	

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 organisation 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** ☐

Contingency Plan

Form-4

PART C Risk Description:

PART D Risk Analysis:

Contingency Plan

Form-4

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:

Integrated Contingency Plan Matrix

Form-5

CP No.	Item, System, Component	Risk Description	Mitigation Strategy	Period of Vulnerability	Implementation Timing	Resources Requirements	Subject Matter Expert	Priority

Appendix A - Definitions

Contingency Plan - is a document that defines the necessary resources, actions and data for responding to the loss or degradation of a service or function due to a Y2K-induced event. The objective of the contingency plan is to provide a pre-defined response to mitigate the effects and allow recovery from a Y2K-induced event.

Contingency Plan Matrix - is a document that identifies individual Contingency Plan actions, critical information, documentation, timing, key contact personnel and staffing requirements that arise from the Integrated Contingency Plan.

Embedded Systems - or embedded software-based systems comprise of one or more microprocessor or digital electronics with a timer or real-time clock mechanism and are "embedded" ("built-into" a device without any visible indication of its presence) in many modern instruments, fire alarms, lifts, controllers and machinery. The software program held within embedded systems (often referred to as "firmware") is often not normally accessible for modification by the user.

Integrated Y2K contingency plan (ICP) - is a document that includes essential elements from all individual Contingency Plans for the site or facility. Its purpose is to ensure the continuity of safe power production in the event of a Y2K-induced event. The Integrated Y2K Contingency Plan is the final product of the contingency planning process.

Leap year - is a year which is divisible by 4 (e.g., 1972, 1996). If a year is divisible by 100 (e.g., 1800, 1900,…) it is not a leap year, unless the year is divisible by 400 (e.g., 1600, 2000, 2400,…), in which case it is a leap year.

Real-time events - are processed as they occur and the results are available immediately. These systems are used to plan, measure, and store information and control processes.

Remediation – is the process of using a work-around, retiring, replacing or modifying an item to achieve Y2K Ready or Y2K Compliant status.

Risk management - is an ongoing activity through which management:

(1) Identifies and tracks internal and external risks to the organization/facility and outside parties resulting from Y2K-related problems,

(2) Assesses Y2K project and programme effectiveness, and

(3) Develops contingency plans for mitigating the effect of potential Y2K-related failures.

Y2K Compliant - is defined [1] as a computer system or application that accurately processes date/time (meaning devices and systems are able to use a four-digit year input correctly) data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the years 1999 and 2000, and beyond, including leap-year calculations.

Y2K-induced event - is a date-related problem that is experienced by a software system, software application, or digital device at a critical date at which time the system or device fails to perform its intended function.

Y2K Problem, or **Year 2000 Problem** - is described as a set of date-related problems that may be experienced by a software system or application. These problems include: not representing the year properly, not recognizing that the year 2000 is a leap year [some systems are incorrectly programmed for this and risk failure at 29 February 2000 or 31 December 2000

(the 366th day)], and improper date calculations, also on other critical dates (see Appendix C for more information on the other critical dates).

Y2K Ready - is defined as a computer system or application that has been determined to be suitable for continued use (meaning that devices and systems will be able to function properly) into the year 2000, even though the computer system or application is not fully Y2K compliant.

Appendix B - Date-Sensitivity Search Suggestions

The following are some recommendations that may be useful in finding items that could have date-sensitive contents, and thus should be added to the inventory for further analysis.

	Does the item …	YES	NO	COMMENTS
F1	Display or print date or time			
F2	Implement a timed control sequence			
F3	Perform operations on a timed basis			
F4	Produce timed reports (hourly/daily/weekly, etc.)			
F5	Calculate timed-based totals, averages, rates or trends			
F6	Time-stamp its data, or use time-stamped data			
F7	Maintain historical records			
F8	Display or print data by time sequence			
F9	Generate alerts at pre-determined intervals (e.g., calibration)			
F10	Request the date on start up or allow user entry of date			
F11	Know which day of the week it is by date			
F12	Send or receive date and time information to and from other systems			
F13	Have date-based calibration/maintenance facilities			

Appendix B - Date-Sensitivity Search Suggestions

F1 Visible output of the date is a certain indication of date functionality. A two-digit year increases the chance of failure due to date comparison.

F2 Some timed control sequences are based on absolute calendar operation not just on elapsed time. Such systems are at risk of failure.

F3 Starting or finishing a sequence of actions on a date/time based schedule is a certain indication of date dependence.

F4 Any report whether printed, displayed or stored which contains a date indicates date dependence.

F5 Any calculation that uses an absolute date to calculate a rate, average or trend will use some degree of date arithmetic. This places it at risk of failure.

F6 Data stored by a system or products physically dated by it, indicates date dependency. Use of time-stamped data from electronic taps, bar-code look up tables or optical character recognition similarly indicates date dependence.

F7 Where a system stores data histories, storage efficiency is often maintained by date/time data vectoring techniques. These use date arithmetic to store only changed data by tagging them with their time of measurement.

F8 Lists of data such as alarms or timed events are often displayed or printed in date order (e.g., newest first). In order to generate such a list, date arithmetic is used.

F9 Some systems include monitoring/diagnostic functionality designed to warn the user when a set running period has been exceeded in order to allow regularly required maintenance to be carried out or because the system has a safe maximum run time. Although in many cases simple elapsed time indicators can carry out these functions, in some instances real-time clock/calendar system is used with associated date arithmetic.

F10 Some systems, which contain only a software clock, will request the time and date when started up or powered on and contain facilities to enter the date and time (e.g., for summer/winter time changes).

F11 Knowledge of the date (or at least the number of the day in the month) and the day of the week implies that some form of calendar functionality exists.

F12 If other systems remain in synchronism with this one or update their date/time when this one is adjusted, then there is a high probability that date/time synchronisation is being carried out by a data connection.

F13 Many systems require regular scheduled maintenance to continue to operate in a safe manner. Where maintenance scheduling is prompted by in-built diagnostics or scheduled by monitoring equipment, a Y2K problem in that equipment can mean that maintenance does not occur when required. Failure of a diagnostic system can also prevent essential equipment from operation.

Appendix C - Testing Reference Information

The Y2K problem revolves around the inability of some systems to handle not only the date 1 January 2000, but also the other critical dates listed below:

- **1 January 1999:** this date is a problem for computer systems that handle the year of a date with only two digits and that use the number 99 as a trigger or as an end-of–file marker (i.e., 99 is the last record in a file or list).
- **22 August 1999:** this date is a problem for systems, which interface with the Global Positioning System (GPS), for example, the transport of nuclear fuel where knowledge of its location is important. The original GPS design allocated a 10-bit register to handle the number of weeks which had elapsed since the base date (or GPS epoch date) of 6 January 1980. The 10-bit week counter will rollover from its maximum value to zero on 22 August 1999.
- **9 September 1999** (9/9/99)**:** as in the case of 1 January 1999, this date is a problem for computer systems that handle the year of a date with only two digits and that use the number 99 (or 9999) as an end-of–file marker or "STOP" code.
- **1 January 2000:** this date is a problem for computer systems that handle the year of a date with only two digits, because they may misread 00 as the year 1900 instead of the year 2000.
- **29 February 2000:** this date is a problem for computer systems that do not correctly identify the year 2000 as a **leap year** and risk failure at 29 February 2000, because it is a leap day.
- **1 March 2000:** this date is a problem for computer systems that do not correctly identify the year 2000 as a leap year and therefore do not recognize 29 February 2000 as a leap day. 1 March 2000 is the day after the leap day and these systems may carry erroneous data.
- **31 December 2000:** this date is a problem for computer systems that do not correctly identify the year 2000 as a leap year and risk failure at 31 December 2000, because it is the 366^{th} day.
- **1 January 2001:** this date is a problem for computer systems that do not correctly identify the year 2000 as a leap year and may carry erroneous data on 1 January 2001, because it is the day after the 366^{th} day (31 December 2000).

Appendix C - Testing Reference Information

The following are some suggested rules for handling date-related information.

- No value for current date should cause any interruption in operation.
- Date-based functionality should behave consistently for dates prior to, during and after year 2000.
- In all interfaces and data storage, the century in any date should be specified either explicitly or by unambiguous algorithms.
- Year 2000 should be recognized as a leap year.

The number of methods used to represent dates should be reduced to an absolute minimum. This is necessary to ensure that systems or operators cannot be either misled or left in doubt by an ambiguous representation. Systems should be implemented either based on a full 4-digit year representation or, where a 2-digit date is used, a single clear definition should be applied.

The following sections will cover some useful testing techniques and scenarios for Year 2000 testing. They are not meant to be all inclusive. Therefore, it is important that additional tests be tailored, as appropriate, for the application.

Attention: **By nature, Year 2000 exposures are time-sensitive and time-driven. Be cautious before resetting the system timer. Some system resources and functions are time-sensitive and may be activated or de-activated when the system clock is reset. Such effects can occur when the system clock is either set forward or backward. Without careful planning, you could cause the loss of these system resources and/or functions, some of which might contaminate the production system or production databases when running various test scenarios.**

Appendix C - Testing Reference Information

Basic Date Processing

Test	Compliant		
Applicable	Yes	No	Test
			1. Leap year - Ensure that year 2000 is processed as a leap year.
			- 1996/2/29 should pass (1996 is a leap year).
			- 2000/2/29 should pass (2000 is a leap year).
			- 2004/2/29 should pass (2004 is a leap year).
			2. Invalid Leap Year Test
			- 2/29/1999 non-leap year.
			- 2/29/2001 for non-leap year.
			3. Date Transaction Validation
			- (01/01/2000) Test processing for the first calendar day of the year.
			- (01/31/2000) Test and validate processing for the last business and calendar day of the month.
			4. Day-in-year calculation test
			- Does year 2000 have 366 days (not 365)?
			5. Day-of-the-week calculation test
			- 02/28/2000 should be a Monday.
			- 03/01/2000 should be a Wednesday.
			6. Week-of-the-year calculation test
			- The 11th week of the year 2000 is 3/5 to 3/11.
			7. End-of-Week Test
			- 01/08/2000 should be a Saturday.
			- 01/09/2000 should be a Sunday.
			8. Data Integrity
			- Are years 1800, 1900, 2000 distinguishable between one another?
			9. Date Related Sorts
			- Ensure sorts use dates properly in processing.
			- Validate and test sort parameters.
			- Review sorts internal to programs.
			10. Age Test
			- Use 12/31/1899 to verify age and date of birth calculations.
			- Validate processing for roll-over to 2001.

Appendix C - Testing Reference Information

Review Dates Manipulated

Test	Compliant		
Applicable	Yes	No	Test
			1. Validate data output records - data field following date field expansion.
			2. Validate data output records - data field in front of date field expansion.
			3. Validate on-line screen display field for error.
			4. Ensure all scheduling based on date return the same results before and after Y2K changes.
			5. Ensure conditions cover time zone differences.
			6. Ensure all extracting base date returns the same results before and after Y2K changes.
			7.Ensure all index processing based on date returns the same results before and after Y2K changes.
			8.Ensure all subscripting based on date returns the same results before and after Y2K changes.

Treatment of Date Input

Test	Compliant		
Applicable	Yes	No	Test
			1. Will program respond correctly if “00” or “2000” is entered.
			2. Is a 4-digit year accepted or is it truncated?
			3. Ensure xx/xx/xx date = xx/xx/xxxx after expansion or conversion for all databases and tables.

Error Handling

Test	Compliant		
Applicable	Yes	No	Test
			1. Normal error handling for current 4 digit year data entry when 2 digit data entry occurs.
			2. Normal error handling for current 2 digit year data entry when 4 digit data entry occurs.

Transferred Date Tests

Test	Compliant		
Applicable	Yes	No	Test
			1. Are proper parameters passed between applications?
			2. Is data transferred in the proper format to inter-system?
			3. Verify that the item can accept input from, and provide output to, other items with which it interfaces as interfaces change.

Appendix C - Testing Reference Information

Review Date Information in Output

Test	Compliant		
Applicable	Yes	No	Test
			1. Validation output report - Determine if data displays will be acceptable in Year 2000
			- Date fields.
			- Non-date fields.
			- Report headers.
			- Report footers.
			2. Validate on-line screens - Determine if data displays will be acceptable in Year 2000
			- Date fields.
			- Non-date fields.
			- Screen headers.
			- Screen footers.
			- On-line screen help.
			3. Validate that hard-coded dates or century indicators are ***not*** located in output records.
			4. Validate that hard-coded dates or century indicators are ***not*** located on output reports.
			5. Validate that hard-coded dates or century indicators are ***not*** located on screen displays.
			6. Validate output reports for zero suppression (i.e., year "00" would ***not*** display).
			7. Validate screen displays for zero suppression (i.e., year "00" would ***not*** display).
			8. Verify that the portion of the item that have *no* changes still runs properly as changes are made to other portions of the system.
			9. Verify that the program handles all its transactions correctly and remain stable for a defined period of time.
			10. Ensure that programs (or table subscripts) can handle date ranges that cross the millennium. - Some programs used dates as subscripts (i.e., September 1999 "999" my be considered as an end of file marker).

Appendix C - Testing Reference Information

Some PC Date Checks

Test	Compliant		
Applicable	Yes	No	Test
			1. Test if the system clock can be set beyond the year 2000.
			- Set the system clock to 01/01/2000, reboot PC and recheck the date.
			2. Test the system clock automatic update function.
			a.) Test the system clock automatic update function when the power is on. - Set clock to 12/31/1999, 23:58:00, keep power on, validate date when clock reaches the year 2000. - Power off PC and recheck the date.
			b.) Test the system clock automatic update function when the power is off. - Set system clock to 12/31/1999, 23:58:00, power off PC and wait until the clock reaches the year 2000. - Power on PC and recheck the date.
			3. Test time update by the operating system
			a.) Update After Suspension of a time-sensitive program: - Set system clock to 12/31/1999, 23:58:00; suspend a time display program without a "wake up" timer; keep power on; wait until the clock reaches the year 2000; resume time display program; and check the date.
			b.) Update After Suspension and Wake Up of time-sensitive program: - Set system clock to 12/31/1999, 23:58:00; suspend a time display program with a "wake up" timer set at 01/01/2000, 00:01:00; keep power on; wait until the time display program "wakes up"; check the date.
			4. Leap Year Test
			Change date 02/29/2000. If an error occurs, then BIOS is incorrect.
			5. Test CPU
			Use different machines (286/386, etc.) when executing tests to ensure processing time isn't impacted.

Appendix C - Testing Reference Information

Facility Defined Tests

Test	Compliant		
Applicable	Yes	No	Test

Appendix D - Regulator Assessment Principles

The following are some consideration taken from the UK references that provide some guidance that regulators may find useful to supplement their own requirements. Care should be exercised so that the facility management is aware of all requirements that are expected of them.

Dates

The licensee programme should clearly indicate all dates that are being investigated.

Project Management and Scope

A Y2K project is one of resource and record management; these should be seen to be properly and systematically managed. There should be a documented strategy[1], project plan and Quality Assurance (QA) plan. All activities should be covered by documented procedures and guidance to ensure completeness and consistency. The emphasis of all guidance should be that of positive demonstration with safety as the central focus.

Licensees should demonstrate that their projects have addressed not only all on-line plant systems but also all relevant off-line systems, including those at their headquarters, contractors' premises and elsewhere. For example, configuration management and software development systems may need to be considered since incorrect versions of the software might be incorporated into a new system build following the millennium change.

The project scope should include, in addition, the safety of all non-nuclear equipment on a nuclear licensed site, i.e. equipment that does not pose a radiological hazard but which might otherwise pose a risk to health and safety due to a computer-related, date problem. Evidence of an appropriate review process should be provided.

Licensees should demonstrate by means of a suitable document that their approach to the Y2K problem is properly controlled through the application of a strategy which broadly matches the following elements:

1. Project programme,
2. Quality Assurance plan/programme,
3. Prioritized inventory,
4. Investigation,
5. Solutions to problems found (system close-out),
6. Contingency plans,
7. Progress reports to the Regulatory Authority,
8. Justification(s) for continued operation.

All licensed nuclear sites, and any other locations associated with these sites which hold safety-significant computer systems, should be covered by appropriate strategy documents which should include QA plans and project programmes covering the critical dates.

The project programme should become more detailed once the inventory is developed and the problem-systems are identified. The updated programme should show when the tests will be carried out and should include the identification of any plant outages required. Because the

dates are immutable, the project programme should be supported by an analysis demonstrating that there are adequate resources to meet the programme's key dates.

Quality Assurance Plan/Programme

Quality Assurance plans/programmes should show all project responsibilities and demonstrate, by means of the status and competencies of the personnel involved, that the organization is committed to resolving the issues prior to the critical dates. Regular project reviews should also be included. There should be other evidence of effective quality control such as a system of peer reviews/checking and approval with appropriate signing off of all activities.

Justification for Continued Operation (JfCO)

Prior to each of the critical dates, the licensee should produce a justification for continued operation (JfCO) beyond each of the critical dates. This justification should show that the inventory was properly established; the investigation was comprehensive and thorough; the solutions are appropriate (and safe) and properly tested; and that the contingency plans (including supply chain management) are appropriate.

The JfCO should cover not only the continuous operation of the plant but all its modes of operation including shutting down and starting up after a critical date. Where the licensee opts to shut down a plant prior to a critical date with a view to restarting up again following that critical date, the JfCO(s) should demonstrate that the plant will be safe in the shutdown mode through the critical date and that it will be able to be operated safely in all proposed modes following the critical date. This equally applies to any operations which are not of a continuous nature, and irrespective of the frequency of their use.

The final solutions to the problem systems (close-outs) must be demonstrably safe, taking due account of any interactions between, or otherwise involving, proposed 'work-arounds' (both in normal operation and during fault conditions).

Where licensees wish to continue operation with a number of degraded safety-related systems, then the synergistic effect should be demonstrated to be safe. Any information, obtained from other sources and used in support of the plant's JfCO, should be sufficiently detailed and authenticated to enable the safety arguments to be evaluated without the need to seek further information held by others.

New equipment purchased prior to and during the periods of the critical dates should be subject to the JfCO process.

Prioritized Inventory

There should be appropriate inventory development and prioritisation procedures linked to suitable guidance. The procedures and guidance should ensure that the approach is sufficiently comprehensive to ensure that the inventory is complete and correct. The inventory should include all systems and these should be uniquely identified and their configurations recorded. Each system should be categorised according to its safety significance.

The completeness of the inventory should be kept under constant review to ensure that any date-dependant systems identified elsewhere, or subsequently, are included, as appropriate, in the inventory.

System aspects that the inventory needs to address include:

- embedded systems - these devices have one or more microprocessors embedded within them for the purpose of control or monitoring a plant item or machine (the software of these devices is often referred to as ‘firmware’ and employs a real-time clock - see ref. 10 for specific treatment of these devices);
- computer system and their software - applications’ programmes, operating systems and device drivers that use dates;
- data and databases - where dates are stored along with other information;
- communications/networks - where transmitted information is date stamped;
- human/machine interface - devices used for inputting and outputting dates.

Embedded, systems are of particular concern because it is less obvious that equipment and plant contain such devices. Examples of plant items and equipment which may contain embedded systems are: cranes, circuit breakers and associated supply system protection equipment, smart instruments (gas detectors, etc), smart valves, lifts and road transport vehicles. The inventory development process should be such as to ensure that such systems are captured - this may require questioning of the manufacturer or supplier.

Licensees' systems important to safety, and their systems which support safety (such as maintenance database systems and off-site systems), should be considered since degradation of any of these systems may have direct safety impacts on the plants involved, especially if there is a synergism between more than one failed system. The systems to be considered include (but are not limited to):

- Computer-based safety systems;
- Safety system support systems;
- Control and monitoring systems;
- Activity-in-air systems;
- Dosimetry systems;
- Maintenance support systems;
- Fire alarm systems;
- Building access/ security systems;
- Criticality detection and alarm systems;
- Communication systems;
- Emergency control centres;
- maintenance databases & tracking systems.

Prioritisation should be in terms of safety significance and required plant outages. Evidence should be available which demonstrates that systems are being investigated and solutions found, according to this prioritisation, so as to ensure that safety is being optimally secured prior to the critical dates.

Appendix D - Regulator Assessment Principles

Investigative Testing

The licensee should have adequate procedures and guidance for controlling the investigation. The guidance should describe how to identify systems with potential date dependency and how to test these systems for date-related problems. The guidance should show how the safety issues which might arise during testing should be addressed.

During any investigation, plant safety must be paramount. Where on-line testing is envisaged, plant investigations must be covered by the existing procedures for regulating experiments and modifications on the site. This may require safety submissions/risk assessments to be reviewed by the Regulatory Authority. Additionally, the on-line testing should be covered by an appropriate work instructions and permits to work. The potential for the system not to be able to recover from the test because of software and/or data corruption should be investigated and recorded as part of the documented demonstration of a safe testing regime. This should include consideration of the achievement of a safe plant state, or the ability to implement a recovery programme, following a test.

For systems important to safety, licensees have a duty to conduct their own investigations, including testing. It is not considered sufficient in this respect to rely solely on a supplier's statement of Year 2000 compliance (see ref. 6, Appendix C).

Where supporting use is made of suppliers' compliance statements, there should be a clear demonstration that these statements refer to the installed version of the software with the specific hardware and software configuration of the system under investigation. The statements of millennium compliance and other advice from manufacturers should be carefully reviewed.

During the investigation phase, an overarching principle should be one of prudence. The licensee should assume that systems and process with date dependencies will fail. They should not use probabilistic arguments to justify any lack of investigation.

Proposed desk-top software audits, and system tests, should be adequate (see ref. 10, Appendix E for suggestions for date strings to be used in searches of source code; also see ref. 12, Appendix A, which provides a more general discussion). The configurations of any systems used for off-line testing should be demonstrated to be sufficiently representative of the installed system so as to give a high degree of confidence that the test results accurately mimic the behaviour of the installed system. The coverage of any tests should be sufficient to detect any potentially adverse effects on the system's functionality due to the system's date dependency.

There should be evidence of a systematic approach to the investigation with justification for the recorded consequences, i.e. why a solution is required, or alternatively, the reasons (e.g., no computer in system, no use of date, use of date causes no safety concerns). Decisions should be peer reviewed.

Remediation

There should be procedures and guidance covering the full implementation of the remedial activity, including that of providing a documented demonstration of safety in relation to the critical dates. Where a change is required (either because of a software modification or replacement of the equipment), the site change control procedures should be used in the normal way including appropriate re-testing of the system and its interfaces following the change. Of particular importance is the maintenance of the plant's safety case. Hence, a comprehensive impact analysis should be undertaken for any such changes to ensure that all interactions are addressed - making one system safe may make another unsafe.

The remediation proposed to close-out a concern should be fully documented and demonstrated to be safe. For example: turning the clock back should be shown to be safe in the overall plant operating context; in particular, the impact on date-related records/activities should be systematically investigated and, where problems are identified, appropriate remedies implemented. Where a plant is to be restarted following a pre-critical-date shutdown that start-up must be shown to be safe.

Any software tools used to detect date information in source code and/or implement corrections must be demonstrated to be fit-for-purpose: and the solution offered must be subjected to all the site change control procedures.

Operations which are not of a continuous nature may be shut down over the critical date periods. Operators of such plant have a duty to carefully review, and where necessary rectify, date-discontinuity problems: taking no investigative/corrective action and assuming that shutting down over the critical periods constitutes an appropriate work-around should be regarded as unacceptable.

Work-arounds should be demonstrated to be safe. This should include the human factors aspects and their impact on the safety of other activities and work-arounds upon which the site depends for continued operation. Actual and potential operators' loading should be considered (as necessary) and demonstrated to be manageable.

Contingency Plans

Licensees should demonstrate that they have contingency plans appropriate to the consequences of major plant failure. These should recognise the possibility of widespread disruption of a licensees own internal infrastructure caused by multiple failures in seemingly non-safety related systems, or the possible disruption of the industrial infrastructure associated with the installation. Both of these events will place very high demands on staff in licensees organisations, with indirect detriment to safety. There should be adequate procedures and guidelines in place covering the production of contingency plans.

Licensees should demonstrate that their staffing levels, and staff competencies and levels of authority will be appropriate for the potential risk and consequences over each critical date associated with the millennium change. In each case this should be reviewed and the proposed arrangements shown to be adequate. Staff should be adequately trained in all the plant work-arounds (and changes) prior to the critical dates to which they apply. Staff should also be

advised to be alert to potential system malfunction following each of the critical dates and should be aware of, and adequately trained in, the actions that should be taken in the event of the failure of any system.

Evidence should be provided that all necessary external supplies have been secured prior to each critical date such that the need to re-order does not occur during the associated critical period. This may include the licensees establishing that their suppliers of safety significant items have made the appropriate securing provisions themselves.

There should be confirmation by the licensees that there are no plans to perform non-essential intrusive activities (such as re-fuelling) through the critical dates.

Licensees should demonstrate that the emergency arrangements for the critical dates have been reviewed which should include also the availability of the communication systems. In particular, both on-site and off-site equipment involved in the emergency arrangements should be checked and contingency plans laid. The review should include the need for specific manning of the licensee's emergency facilities over the critical dates.

List of Contributors

Ladislav Cocher	Dept. of Informatics, Slovenske Electranne A.S. Slovakia
Luis Lederman	International Atomic Energy Agency
Morgan D. Libby	Northeast Utilities, Berlin, CT, USA
Jose Martinez-Rico	International Atomic Energy Agency
Norman Wainwright	Health and Safety Executive, Nuclear Safety Directorate, United Kingdom
Nikolai Yakovlev	Dept. of Computers and Automatics, RDIPE, Russian Federation

Experts Meeting

on

The Evaluation of the Year 2000 (Y2K) Problem on Nuclear Installation Safety

Organized under Technical Co-operation Project RER/9/052

Vienna, Austria

9-13 November 1998