NEI/NUSMG 98-07

NUCLEAR UTILITY YEAR 2000 READINESS CONTINGENCY PLANNING

August 1998

NEI/NUSMG 98-07

Nuclear Energy Institute
Nuclear Utilities Software Management Group

NUCLEAR UTILITY YEAR 2000 READINESS CONTINGENCY PLANNING

August 1998

Nuclear Energy Institute, 1776 I Street N.W., Suite 400, Washington D.C. 202.739.8000

ACKNOWLEDGMENTS

This document, *Nuclear Utility Year 2000 Readiness Contingency Planning,* NEI/NUSMG 98-07, was developed with the assistance of a task force of industry managers dealing with Year 2000 readiness issues. Timely development of this document was facilitated by use of the combined resources and expertise of the Nuclear Energy Institute and Nuclear Utilities Software Management Group. NEI and NUSMG wish to acknowledge the extensive efforts of the individuals who authored this document. Members of the industry's Contingency Planning Task Force include:

Terry Baxter	Union Electric
Doug Cremer	PECO Energy Company
James Davis	Nuclear Energy Institute
Wayne Glidden	Duquesne Light Company
Anne Houck	Duke Energy Corporation
Morgan Libby	Northeast Utilities
Don Lokker	Southern California Edison Company
Rich Lomax	Nebraska Public Power District
Bill Olsen	Nuclear Utilities Software Management Group
John Walderhaug	Southern California Edison Company

NOTICE

EXECUTIVE SUMMARY

Contingency planning for Year 2000-induced events has recently received a high level of attention from the government and in the press. A number of different, and often conflicting, approaches to contingency planning have been proposed. This document provides a focused approach to effective contingency planning that builds on the Year 2000 readiness program nuclear utilities already have in place. Insights from ongoing industry readiness programs were extensively used in preparing this manual.

The primary goal of this document is preparation of an integrated contingency plan that allows the plant operating staff to mitigate any Y2K-induced events that might occur at key rollover dates. The principal date will be the rollover to January 1, 2000. Each facility will need to evaluate whether there are other dates of concern. The assessment and remediation program elements provide many of the insights needed to identify and quantify the Year 2000 rollover date risks at a facility.

The integrated contingency plan is developed from individual contingency plans developed for specific risks from internal and external sources, as well as remediation program insights. Internal risks can be assessed from the complexity of a digital system and its importance to plant operations. External risks have the added factor of supplier readiness and evaluating readiness programs that are not under the facility's control. The integrated plan provides a comprehensive perspective of risks to the facility and the resources and staff required to implement mitigation strategies.

This document also recommends that during the remediation phase, where there is a significant risk that remediation cannot be completed in the time available, that alternate remediation strategies be identified to ensure the facility can achieve Year 2000 readiness before a key rollover date.

TABLE OF CONTENTS

Executive Summary i

1 INTRODUCTION 1

2 PURPOSE AND SCOPE 1

2.1 PURPOSE 1

2.2 SCOPE 1

3 DEFINITIONS 2

3.1 BUSINESS CONTINUITY 2

3.2 CONTINGENCY PLAN 2

3.3 CONTINGENCY PLAN MATRIX 2

3.4 INTEGRATED Y2K CONTINGENCY PLAN (ICP) 2

3.5 KEY ROLLOVER DATE 2

3.6 MITIGATION STRATEGY 3

3.7 REMEDIATION 3

3.8 RISK MANAGEMENT 3

3.9 Y2K COMPLIANT 3

3.10 Y2K-INDUCED EVENT 3

3.11 Y2K READY 3

4 Y2K CONTINGENCY PLANNING MANAGEMENT 3

4.1 CONTINGENCY PLAN COORDINATION 4

4.2 INDIVIDUAL CONTINGENCY PLANS 4

4.3 INTEGRATED CONTINGENCY PLAN 5

4.4 PROJECT REPORTS 5

5 REMEDIATION RISKS 5

5.1 RISK IDENTIFICATION 6

5.2 ANALYSIS 6

5.3 RISK MANAGEMENT 6

5.4 VERIFICATION 6

6 CONTINGENCY PLANNING FOR INTERNAL FACILITY RISKS 7

6.1 RISK IDENTIFICATION 7

6.2 EVENT ANALYSIS 7

6.3 RISK MANAGEMENT 8

6.4 VERIFICATION 8

7 CONTINGENCY PLANNING FOR EXTERNAL RISKS 8

7.1 RISK IDENTIFICATION 9

7.2 EVENT ANALYSIS 10

7.3 RISK MANAGEMENT 10
7.3.1 Risk Notification 10
7.3.2 Mitigation Strategy Selection 11

7.4 VERIFICATION 11

8 INTEGRATED Y2K CONTINGENCY PLAN 11

8.1 INTEGRATED Y2K CONTINGENCY PLAN DEVELOPMENT 12

8.2 INTEGRATED Y2K CONTINGENCY PLAN CONTENT 12

APPENDICES

A. PROGRAM INTEGRATION A-1

B. EXAMPLES OF REMEDIATION RISK PLANNING B-1

C. EXAMPLES OF INTERNAL CONTINGENCY PLANS C-1

D. EXAMPLES OF EXTERNAL CONTINGENCY PLANS D-1

E. INTEGRATED CONTINGENCY PLAN MATRIX E-1

F. BOUNDARY ANALYSIS AND SUPPLY CHAIN READINESS F-1

1 INTRODUCTION

The nuclear utility industry has embarked on a program to identify and remediate Year 2000 (Y2K) problems that could affect facility operations. Despite these efforts, there is some risk of Y2K-induced events. *Nuclear Utility Year 2000 Readiness* (NEI/NUSMG 97-07), which provided a programmatic approach for identifying and addressing Y2K problems, recognized this risk and included a recommendation for contingency planning.

Effective contingency planning provides a process for reducing the risks associated with Y2K-induced events. This document provides an acceptable method for nuclear utility contingency planning by addressing contingency plan management, development and integration. It divides contingency plan elements into three categories based on the source of the risk:

- **Remediation Risks**—Remediation risks result from circumstances, such as component availability, that challenge the preferred remediation strategy.
- **Internal Facility Risks**—Internal facility risks are associated with facility digital systems that, although remediated, may be subject to a Y2K-induced event at key rollover dates.
- **External Risks**—External risks result from circumstances, conditions, or events that are not under the direct control of station management.

An integrated contingency plan should be developed from individual contingency plans to provide a comprehensive action plan to mitigate Y2K-induced events that could occur on key rollover dates.

2 PURPOSE AND SCOPE

2.1 PURPOSE

This document provides guidance for establishing a contingency planning process. It recommends management controls, preparation of individual contingency plans and development of an integrated contingency plan that allows the utility to manage the risks associated with Y2K-induced events.

2.2 SCOPE

This document addresses Y2K contingency planning as applied to nuclear generating stations and includes generating facility systems, resources and external influences. This document assumes that the facility already has an effective Y2K management program similar to that outlined in NEI/NUSMG 97-07. Contingency plans should support enterprise business continuity efforts. Appendix A provides an example of one way to integrate the various program elements.

3 DEFINITIONS

The context of many of the terms used in discussing Year 2000 problems has shifted significantly over the past year. Different groups are using the same terms in discussing business continuity and contingency planning, but each group often applies significantly different meanings to key terms. In developing this document, the following definitions were used.

3.1 BUSINESS CONTINUITY

Business continuity is a high-level business strategy that provides senior management with an enterprise-wide overview of Year 2000 business risks and solutions. Business continuity is achieved through planning efforts that focus on reducing the risk of Y2K-induced business failures and addressing the organization's ability to provide the acceptable level of service in the event of Y2K-induced failure in internal or external systems.

3.2 CONTINGENCY PLAN

A contingency plan is a document that defines the necessary resources, actions and data for responding to the potential loss or degradation of a service or function due to a Y2K-induced event in a component or system. 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 in a system or component.

3.3 CONTINGENCY PLAN MATRIX

A contingency plan matrix is a document that identifies individual contingency plan actions, critical information, documentation, timing, key contact personnel and staffing requirements for inclusion in the integrated contingency plan.

3.4 INTEGRATED Y2K CONTINGENCY PLAN (ICP)

An integrated Y2K contingency plan is a document that includes essential elements from all 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.

3.5 KEY ROLLOVER DATE

A key rollover date is a date change on which digital systems may be susceptible to Y2K-induced events. These dates are identified from a facility detailed assessment. For example, December 31, 1999, to January 1, 2000, is a key rollover date.

February 28, 2000, to February 29, 2000, has also been identified as a key rollover date by some facilities.

3.6 MITIGATION STRATEGY

Mitigation strategy is a management process that results in documented instructions for reducing the effects of postulated or actual Y2K-induced events.

3.7 REMEDIATION

Remediation is the process of retiring, replacing or modifying software or devices that have been determined to be affected by the Y2K problem.

3.8 RISK MANAGEMENT

Risk management is an ongoing activity through which management: (1) identifies and tracks internal and external risks to the organization and outside parties resulting from Y2K-related problems, (2) assesses Y2K project and program effectiveness, and (3) develops contingency plans for mitigating the effect of potential Y2K-related failures.

3.9 Y2K COMPLIANT

Computer systems or applications that accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, the years 1999 and 2000, leap-year calculations and off-power on scenarios.

3.10 Y2K-INDUCED EVENT

A Y2K-induced event is a date-related problem that is experienced by a software system, software application, or digital device at a key rollover date at which time the system or device does not perform its intended function.

3.11 Y2K READY

A computer system or application that has been determined to be suitable for continued use into the year 2000 even though the computer system or application is not fully Y2K compliant.

4 Y2K CONTINGENCY PLANNING MANAGEMENT

The management of contingency planning requires coordination of a broad range of internal and external resources and interfaces. To meet this challenge, the Y2K project

manager should consider contingency planning as an integral activity to the Y2K project plan that implements NEI/NUSMG 97-07. Because of the importance and complexity of this task, the project manager should consider assigning an individual as the single point of contact for the contingency planning process.

Contingency planning is a process that begins during the Y2K detailed assessment phase and continues throughout the program. The following are the recommended steps in the process:

- **Risk identification**—determines which items present a critical risk to the facility from Y2K-induced events.
- **Event analysis**—reviews identified risks, determines potential failure modes and consequences, and documents pertinent information.
- **Risk management**—uses information from event analysis to determine mitigation strategies. It should consider Y2K-induced events and their interdependencies.
- **Verification**—reviews the risk management results and provides confidence that the contingency plan will effectively mitigate the risk.

Contingency plans should be documented, reviewed and approved by management.

4.1 CONTINGENCY PLAN COORDINATION

Y2K contingency plan coordination is a component of the facility Y2K project plan. Coordination activities ensure that each responsible organization develops individual contingency plans for identified risks. Recommended coordination activities include:

- contingency plan training
- assignment of appropriate resources
- development and coordination of individual contingency plans by responsible organizations
- tracking individual contingency plan status and progress
- assembling an integrated contingency plan
- reporting progress to the Y2K project sponsor

4.2 INDIVIDUAL CONTINGENCY PLANS

Individual contingency plans are prepared for items, systems or events. Plans should be identifiable and traceable to a risk. The following information should be included in individual contingency plans:

- inventory number or other unique identifier

- risk description
- subject matter expert identification
- event analysis
- period of vulnerability
- priority
- risk mitigation strategy and actions
- resources
- implementation timing and, if needed, an exit strategy
- training requirements
- any special Y2K procedures required
- identification and documentation of verification
- approval.

Individual contingency plans should be subject to appropriate elements of the facility Y2K readiness program such as quality assurance, management reviews and document retention. Individual contingency plans should be submitted to the Y2K project manager when completed.

4.3 INTEGRATED CONTINGENCY PLAN

The integrated contingency plan provides facility management with a comprehensive perspective of the risks associated with Y2K-induced events. The Y2K project manager should ensure a facility-specific integrated contingency plan is developed as described in Section 8 (see page 11).

4.4 PROJECT REPORTS

The Y2K project manager documents the progress of the contingency planning effort in status reports to the Y2K project sponsor and other appropriate management. Reports should include key performance indicators such as schedules, status, expenditures and any known issues with interfacing organizations, both internal and external.

5 REMEDIATION RISKS

Each facility's Y2K project will remediate those systems within the project scope prior to Year 2000. However, remediation efforts for some systems may involve challenges to completion. Under these situations, it is prudent to develop alternate remediation strategies as a contingency. These strategies are within the scope of the NEI/NUSMG 97-07 remediation process. This section provides a method that can be used to evaluate these

remediation challenges and determine whether development of alternate strategies is appropriate. Examples are provided in Appendix B.

5.1 RISK IDENTIFICATION

Remediation efforts may be challenged by a number of factors, including:

- availability of replacement components
- concern over vendor support
- scarcity of resources.

The Y2K project should identify those systems whose remediation strategies are subject to risk. These strategies will undergo further risk analysis.

5.2 ANALYSIS

Analysis is performed to understand the nature of the challenges to the selected remediation strategy. Alternative remediation strategies should be evaluated to determine their suitability and any further risks that their selection might introduce. For example, if replacement is the selected remediation strategy, the risk of late delivery should be considered. If the alternative remediation strategy is date rollback, then any risk posed by this alternative should also be evaluated.

Key performance indicators (KPIs) may be used to provide a mechanism for monitoring the progress of the remediation effort. In some cases this may be as simple as the component delivery date.

5.3 RISK MANAGEMENT

Using the results of the analysis phase, management should identify an alternate remediation strategy. Using the selected KPIs, management should select criteria for initiating the alternate remediation strategy. Schedule constraints and system complexity will be key factors in establishing the initiation date.

5.4 VERIFICATION

The selected risk management strategy should be verified. This process ensures that the strategy is capable of achieving the intended purpose, can be accomplished in the time available and identifies personnel necessary to execute it.

6 CONTINGENCY PLANNING FOR INTERNAL FACILITY RISKS

The inventory, assessment and remediation phases of the Y2K project are designed to provide identification and remediation for items that could degrade, impair or prevent operability of the nuclear facility. However, there remains some risk that digital systems could still be subject to a Y2K-induced event that affects 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 facility operations.

An example of an internal facility risk is a control system that relies upon process computer signals, embedded devices, and complex interfaces to other systems. These relationships become evident in the inventory and assessment process. Based on the importance of this system and its complexities, management may elect to develop an individual contingency plan for it. Contingency plans should identify failure modes and mitigation strategies. See Appendix C for samples.

Y2K contingency planning should also consider the potential that the problem results in a common cause failure that could potentially affect many systems or components, including essential infrastructure services.

6.1 RISK IDENTIFICATION

Risk identification for internal facility events includes a review of the Y2K inventory and assessment results for devices and software. The risk is a function of the short-term challenge to continued facility operation, the complexity of the system and the degree of remediation that may have been required. The following are examples of factors to consider:

- systems or components whose failure places the unit at short-term risk for continued operation
- 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

6.2 EVENT ANALYSIS

Event analysis is used to determine failure modes and their consequences. Analytical processes may include review of existing safety analyses and probability risk assessments (PRA). Simulations and experience-based judgments may be used to understand the implications of failure modes. For each event consider the following:

- consequence of the event on safety or operability, including safe shutdown operations

- likelihood of the occurrence of the event
- importance to the objectives of the facility
- when event consequences occur—immediate, delayed with a known or unknown time-to-occurrence
- long-term effect of the event.

6.3 RISK MANAGEMENT

Risk management uses the information from event analysis to determine the mitigation strategies that will reduce the effect of a Y2K-induced event. It may consider Y2K interdependencies. For internal facility risks, risk mitigation requires a wide range of technical and operations skills. Mitigation strategies to consider include:

- augmented staff
- implementing manual control
- placing backup or standby systems in service
- developing special procedures
- establishing specific training requirements
- monitoring systems to ensure proper operation following a key rollover date.

The facility should leverage existing procedures and practices when developing mitigation strategies.

6.4 VERIFICATION

Individual contingency plans should be verified. 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. The methods that may be used for this evaluation include management assessments, independent reviews, and peer evaluations.

7 CONTINGENCY PLANNING FOR 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 risks and the means for mitigation. Examples in this area are provided in Appendix D.

7.1 RISK IDENTIFICATION

Risk identification considers how external Y2K events could compromise the safety or continued operation of the facility due to Y2K-induced events. One technique that may be used is boundary analysis.

Boundary analysis postulates a boundary surrounding the facility. Items, signals, information, or data that cross the boundary are candidates for investigation. Examples include transmission lines, communications, consumables and services. This technique may result in a detailed examination of facility supply chains for a limited number of critical services and consumables for vulnerability to disruption by a Y2K-induced event. Particular attention should be given to facility services or equipment that are jointly administered, either in concert with the facility or by more than one external supplier. Further discussion is provided in Appendix F.

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.

The following list includes external events that a facility should consider for contingency planning:

- **transmission/distribution system events**—loss of off-site power, grid instability and voltage fluctuation, load fluctuations and loss of grid control systems
- **loss of ultimate heat sink**—river water level control
- **depletion of consumables**—bottled gasses, hydrogen, carbon dioxide, nitrogen, diesel fuel and demineralizer resins
- **loss of essential services**—telephones, microwave, domestic water, satellite, networks, select vendors, security, police and fire fighting
- **loss of emergency plan equipment and services**—pagers, radios, sirens and meteorology.

7.2 EVENT ANALYSIS

The purpose of external event analysis is to understand and evaluate the implications of external events to the facility. For each event, the responsible organization should consider the following:

- consequence of the event on safety or operability, including at-power or safe shutdown conditions
- likelihood of occurrence of the event
- potential for an event inducing other events, or changing the probability of their occurrence
- when event consequences occur—immediate, delayed with a known or unknown time-to-occurrence
- priority for resumption of the service
- long-term effect of the event.

Events should be investigated with consideration of 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 events. A chain of failures in a complex supply chain may compromise more than is readily apparent by looking only at the final source.

7.3 RISK MANAGEMENT

Risk management uses the information from event analysis to determine the mitigation strategies that will reduce the effect of a Y2K-induced event. It ensures that the risks posed by external Y2K-induced events are identified and are reduced 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 event. This management function requires input from business and technical specialists. The two phases of risk management are risk notification and selection of mitigation strategy.

7.3.1 Risk Notification

For external events, it is important to communicate to the responsible external organization the risk significance of an event to the facility. The external organization may be requested to provide a description of its Y2K project elements that address the event. The facility Y2K project should consider this information in determining the mitigation strategy. The evaluation should consider the potential for the external organization's Y2K remediation or contingency planning to be successful as a mitigation strategy.

7.3.2 Mitigation Strategy Selection

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

- **facility alignment—**Preset facility load or capacity to reduce the consequences to the facility of grid instability or voltage fluctuations. High-risk evaluations, such as reduced reactor coolant inventory operations or emergency diesel generator planned maintenance, should be scheduled to avoid Y2K key rollover dates, when possible.
- **minimized dependency—**Stockpile consumables to support continued facility operation.
- **an alternate source—**Most consumables are available from multiple sources.
- **an alternate process—**Some services such as telecommunications may be accomplished using alternate methods. For example, portable radios may be used to compensate for the loss of phone service.
- **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. An example might be a system that will be interrupted by the Y2K-induced event but is easily restarted with support of the external organization.

7.4 VERIFICATION

The risk management strategy should be verified. 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.

8 INTEGRATED Y2K CONTINGENCY PLAN

The integrated Y2K contingency plan is a compilation of individual Y2K contingency plans and includes any remediation actions planned during key rollover dates. It is a comprehensive document that will be used to manage the resources required to support the facility leading up to and during key rollover dates.

Using this information, facility management determines the resources required to properly staff for key rollover dates. Inputs required for development of the integrated plan include:

- organizational sponsorship and key contacts

- identification of required internal and external organizational support
- coordination with internal and external interfaces
- identification of conflicts among individual contingency plans
- identification of resources necessary to implement individual contingency plans.

8.1 INTEGRATED Y2K CONTINGENCY PLAN DEVELOPMENT

The Y2K project manager is responsible for the development of the integrated Y2K contingency plan. As individual contingency plans are developed, staffing requirements and actions are extracted and documented in the integrated contingency plan matrix. This matrix is then used to determine the overall resource requirements for the facility. This process begins during the assessment phase and continues throughout the Y2K program. A sample matrix is provided in Appendix E.

The final integrated Y2K contingency plan should be reviewed and approved by management.

8.2 INTEGRATED Y2K CONTINGENCY PLAN CONTENT

The integrated Y2K 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 Y2K-induced events. The scope establishes the boundaries for the plan.

integrated contingency plan matrix—provides the relationship between the individual contingency plans.

responsibilities—assigns responsibility for managing the implementation of the integrated contingency plan. This may include the following key responsibilities:

- integrated Y2K contingency plan coordinator—assembles teams and manages the implementation of the plan
- implementation teams—identifies personnel designated to carry out actions specified in individual contingency plans
- advisory teams—identifies personnel familiar with the technical content and details associated with mitigation strategies

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 Y2K-induced events as they occur.

integrated action plan—summarizes the actions associated with the restoration of facility systems, components, and equipment affected by Y2K-induced events.

integrated Y2K contingency plan training and awareness—identifies any specific Y2K-related training requirements. General facility awareness training on Y2K critical dates and associated contingencies should also be considered.

APPENDIX A

Program Integration

Contingency planning needs to be integrated with the other elements of the facility's overall Year 2000 readiness program. This appendix provides one way that these elements can be integrated to support the overall objective of reducing risk from Year 2000 problems.

NEI/NUSMG 97-07 *Nuclear Utility Y2K Readiness* provides guidance on managing the Y2K project, identifying contingency planning as one of management planning. Figure A-1 shows the relationship of contingency planning to the overall Y2K project.

As the figure shows, deliverables of the Y2K program assessment and remediation phases support developing Y2K contingency plans for the critical systems, devices and applications. This process involves the development of alternate remediation plans and contingency plans. Existing contingency plans may be used or augmented with Y2K event considerations.

Individual Y2K contingency plans are incorporated into an integrated contingency plan, which provides a comprehensive document to be used to manage risks at key rollover dates. The integrated contingency plan should support any enterprise level business continuity planning efforts.

Integration of the contingency planning effort into the overall Y2K readiness program time line is also important. Figure A-2 illustrates the overall time line for one facility. The timeline shows the relations of individual phases of the Y2K project. In this case, the project started in the fourth quarter of 1997. The relationship of one phase to another, not the absolute schedule, is what is important. For any given facility, actual time planned for each phase will depend on variables such as the number of operating units, available personnel and number of digital systems.

Development of the integrated Y2K contingency plan depends on completion of individual contingency plans for the identified risk categories. Contingency plan development for Y2K remediation activities and internal risks may be performed throughout the assessment and remediation phases of the Y2K project. This process is described in Sections 5 and 6. Assessing external risks as described in Section 7 involves cooperation of organizations outside of the control of the facility.

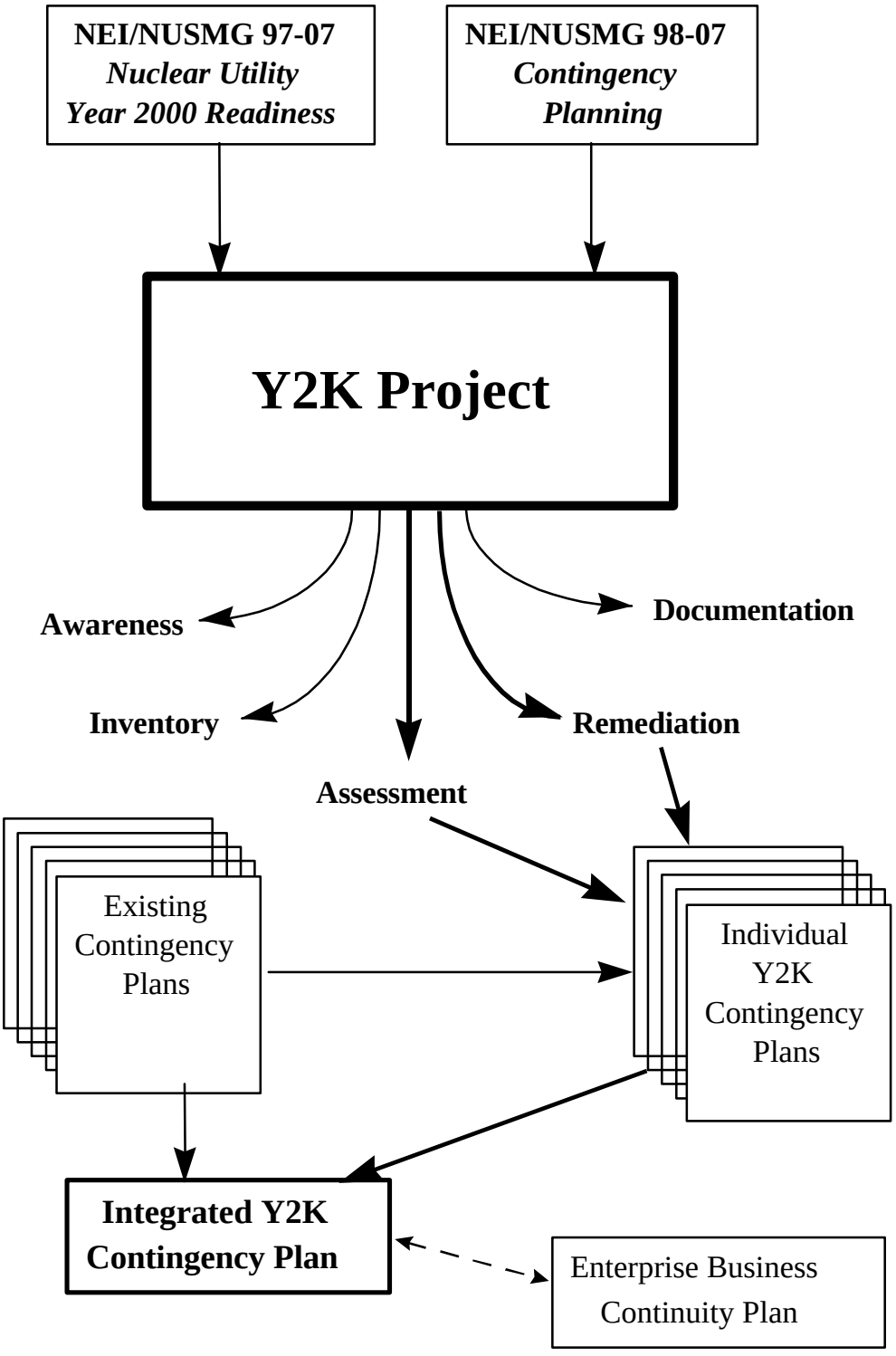

Figure A-1: Program Integration

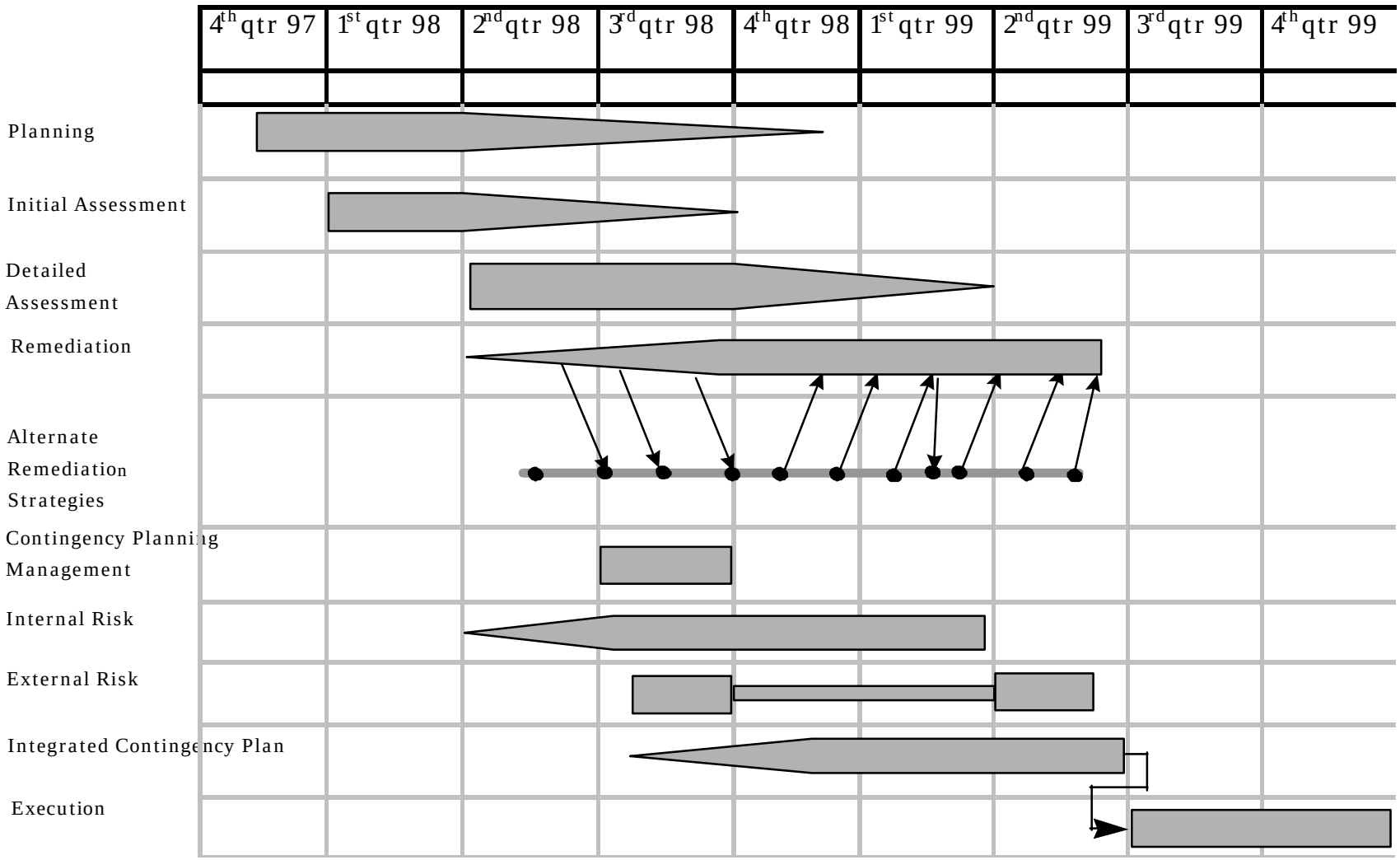

Figure A-2: Typical Year 2000 Project Time Line

APPENDIX B

Examples of Remediation Risk Planning

The information in this appendix illustrates the types of remediation risks, described in Section 5, to which planned Y2K remediation efforts may be exposed. These sample contingency plans demonstrate remediation risks from vendor concerns, resource limitations and scheduling difficulties. As for all of the sample contingency plans in these appendices, these plans are written for illustration purposes only to demonstrate the contingency planning process in different scenarios.

The first example, identified as B-1, demonstrates an alternative remediation plan based on a concern that a vendor may not successfully deliver and implement the primary remediation solution. The strategy recommended in this situation is to set the system clock back 28 years.

The second example, identified as B-18, demonstrates a situation where an enterprise-wide solution will ultimately replace a plant application that contains a Y2K weakness. In this case, the alternate remediation is to fix the software if the enterprise-wide solution does not meet the implementation schedule, even though the plant application will ultimately be replaced.

The third example, identified as B-179, documents a Y2K weakness with a database, where reports do not correctly render the four-digit year, even though all calculations and values are correct. This example represents a cosmetic problem only, therefore the accept-as-is alternate remediation option is specified.

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.: **B-1**	**Item/Component/System:** **Radiation Monitor**	**Priority** 3A

Risk Description:
There is concern over vendor support. The Radiation Monitor System Engineer has reported that the vendor cannot provide a firm schedule or price at this time. The vendor has a history of late project deliveries.

Risk Analysis Summary:

The uncertainties associated with this vendor indicate a significant risk that the current remediation plan may not achieve Y2K readiness; therefore, a secondary remediation plan must be provided.

Risk Mitigation Strategy:
The system has been analyzed to assure that it neither obtains nor provides dates to any other system. Consequently, as a stand-alone system the alternate remediation plan is to set the clock back 28 years. That will allow the days of the week and leap years to match.

Based on the desired completion date of July 1, 1999, and the estimated time required for verification of the contingency, November 1, 1998, has been set as the KPI that requires the vendor to demonstrate a factory tested upgrade. If this date is not met, the alternate remediation will be implemented.

Implementation:

Period of Vulnerability: N/A
Implementation Timing: Begin 11/1/98, to be completed by 12/31/98
Resource Requirement: Backups & System Clock change - 3 MNHRS
Procedure Reviews & Revisions - 10 MNHRS
Subject Matter Expert: R. M. Engineer
Training Required: N/A **Completed:** _____
Exit Strategy: N/A

Verification & Approval: Verify operability through use of facility surveillance procedure.

Verified By: _____ **Date:** _____

Approved By: _____ **Date:** _____

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.:	**Item/Component/System:**	**Priority**
B-18	Work Management and Maintenance Scheduling	3B

Risk Description:
The primary remediation strategy is the installation of an enterprise-wide work management system. The new system will replace a plant system that is currently maintained by plant computer personnel. Because of the broad scope of this project and the resources required, there is a concern that the target date of 12/31/1998 will not be met.

Risk Analysis Summary:
The present application will not schedule work and maintenance items past 1/1/2000. Some of these work items are required one year in advance and are used in support of technical specifications. Manual scheduling of these items is not feasible. An alternative to the primary remediation strategy is required.

Risk Mitigation Strategy:
The alternate remediation strategy is to correct the software problems in the current work management system. It is crucial that this work be completed by the end of 1998 so that year 2000 work items can be generated beginning in 1999. Because of this critical timing issue, the alternate remediation may have to be started before the status of the enterprise-wide solution is known.

Implementation:

Period of Vulnerability: 1/1/1999 until acceptance of enterprise-wide application
Implementation Timing: Must begin by 10/1/1998 to complete by 12/31/1998.
Resource Requirement: 4.5 man months application design, coding, implementation. 1 man month for administrative support.
Subject Matter Expert: J. L. Programmer
Training Required: N/A **Completed:** _____
Exit Strategy: N/A**:**

Verification & Approval: Verify operability of existing system by testing of added features and by an integration surveillance test using approved procedures.

Verified By: _____ **Date:** _____

Approved By: _____ **Date:** _____

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.:	**Item/Component/System:**	**Priority**
B-179	**HR Database(xxx)**	6

Risk Description:
Certain reports from the human resources database do not correctly display dates beyond 1999. Project XYZ has been initiated to correct this problem but, because of low priority, may not be completed by 1/1/2000.

Risk Analysis Summary:
The human resources applications provide reports to the fitness for duty and security access systems. Tests have shown that reports with dates beyond 1/1/2000 show up as "****". The only problem is in the reports. All stored and calculated data is correct.

Risk Mitigation Strategy:
The problem is cosmetic. The alternate remediation is to accept as is.

Implementation:

Period of Vulnerability: N/A
Implementation Timing: N/A
Resource Requirement: N/A
Subject Matter Expert: H. R. Manager
Training Required: N/A **Completed:** _____
Exit Strategy: N/A

Verification & Approval: Verification is N/A.

Verified By: _____ **Date:** _____

Approved By: _____ **Date:** _____

APPENDIX C

Examples of Internal Contingency Plans

The information provided in this appendix illustrates the types of risks that Y2K events may pose to systems under the control of the facility even after remediation has been accomplished. These were discussed in Chapter 6 of the basic document. Each example is followed by the related Year 2000 contingency planning form.

Example 1: Contingency Plan for the Facility Computer Network

Risk Identification - The information technology (IT) computer network and server farm is a system with multiple digital control devices and software subsystems that do not furnish diversity and cannot be operated manually. This system also uses digital input from other systems to perform its intended functions.

While this system has been individually evaluated, it has many complex interfaces and an enormous number of possible interactions and conditions that exist with any given transaction. A single failure in one of the components has the potential for impacting the entire data communications structure and therefore should receive additional attention in the form of contingency planning.

Event Analysis - Although each component and application has been assessed and no Y2K weaknesses were identified, the large number of interactions described above are of concern. Therefore, IT will augment staffing during the critical time periods to immediately respond to any abnormal conditions. The abnormal conditions could include hardware and/or software, so the augmented staff must include both programmers and technical support personnel.

Risk Management - The contingency plan for a Y2K event in the IT system includes the following mitigation strategies:

- Mitigation strategy from IT for potential failure of computer component(s). (IT will provide augmented staffing for the critical dates of 12/31/99 – 1/1/2000 and 2/28/2000 – 2/29/2000.)
- Each department has evaluated the impact and has developed mitigation strategies in the event of the loss of data communications capabilities. Those currently identified include:
    - Operations has developed a methodology to provide worker protection assurances (WPA) manually.
    - Maintenance has developed a mitigation strategy to obtain replacement parts manually.

- Stores has developed a mitigation strategy to access and distribute replacement parts manually.
- Emergency Preparedness has identified a mitigation strategy which is an alternate method for computer based notification and call out of personnel.
- Health Physics Operations will utilize manual methods for RCA entry as per existing procedure.
- Health Physics Technical Support's mitigation strategy is to use alternate radiation spectroscopy methods.

Each department has provided appropriate mitigation strategies for Y2K-induced events.

Verification - Examples of contingency plan verification of a few of the potentially impacted departments include:

Operations – The IT department has planned a computer outage for the platform on which the WPA application is located. Operations has developed a manual process to implement and track WPA. They will conduct a test of the process prior to the planned computer outage and implement during the outage to verify operability of the process.

Emergency Preparedness (EP) – EP will pre-stage emergency personnel, as listed on the attached list, for the key rollover dates as a contingency for this and other potential Y2K-induced events. As this does not require any new processes, no additional verification is required.

Health Physics Operations (HPOPS) – HPOPS has an existing procedure to manually control access to the RCA and track personnel dose. This procedure is a part of the training curriculum and has been successfully used by the current technical staff. Since implementation of this procedure has successfully been completed, no further verification is necessary.

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.: **EX-01**	**Item/Component/System: Facility Local Area Network File Server System**	**Priority:** **HIGH**

Risk Description: Possible loss of network communications and network based software applications.

Risk Analysis Summary: Individual network components have been assessed and determined to be Y2K ready; however, integrated testing could not simulate all possible combinations of software interaction. Any network anomalies are likely to manifest shortly after Y2K rollover. Restoration of the network may require software and hardware expertise.

Risk Mitigation Strategy: Augment IT staffing on Y2K rollover dates with network engineer and network hardware technician to perform restart of network servers, routers, and software applications as necessary. Perform full network backup on 12/31/1999.

- Mitigation strategy from IT for potential failure of computer component(s). (IT will provide augmented staffing for the critical dates of 12/31/99 – 1/1/2000 and 2/28/2000 – 2/29/2000.)
- Each department has evaluated the effect and has developed mitigation strategies in the event of the loss of data communications capabilities. Those currently identified include:
  - Operations has developed a mitigation strategy to provide worker protection assurances (WPA) manually.
  - Maintenance has developed a mitigation strategy to obtain replacement parts manually.
  - Stores mitigation strategy is to access and distribute replacement parts manually.
  - Emergency Preparedness mitigation strategy is an alternate method for computer based notification and call out of personnel.
  - Health Physics Operations will use manual methods for RCA entry as per existing procedure.
  - Health Physics Technical Support will use alternate radiation spectroscopy methods.

Each department has provided appropriate mitigation strategies for the potential Y2-induced events.

Plan No.: EX-01	Item/Component/System: Facility Local Area Network File Server System	Page 2

Implementation:

Periods of Vulnerability: 12/31/1999 – 01/01/2000, 2/28/2000 – 2/29/2000

Implementation Timing: Swing shift 12/31/1999, swing shift 2/28/2000

Resource Requirements: One network engineer, one network hardware technician

Subject Matter Expert: S. T. Trainer

Training Required: None **Completed:** _____

Exit Strategy: The exit strategy is to discontinue manual methods when automated system is restored and verified. The use of alternate methods will be discontinued when primary methods are restored and verified.

Verification & Approval: Adequate implementation of manual methods will be verified by supervisory oversight. Alternate methods usage will be verified by performing a calibration procedure.

Verified By: _____ **Date:** _____

Approved By: _____ **Date:** _____

Example 2: Contingency Plan for Condensate Polisher System

Risk Identification - The full flow condensate polisher (FFCP) system provides chemical conditioning of the condensate water while on line to enhance steam generator water chemistry control. The FFCP has a large number of integrated programmable logic controllers (PLC) and a known Y2K deficiency involving PLC halts when system time rolled over from 12/31/99 to 01/01/00. Remediation was accomplished with a firmware upgrade from the vendor for the PLC. Individual components were tested and validated for Y2K readiness.

Event Analysis - Failure of the FFCP system could cause transients in steam generator water level with possible reactor protective system activation and safety system activation if steam generator level control is lost. Extended loss of the FFCP will result in degraded steam generator water chemistry conditions.

If any Y2K-induced event were to occur, the control room annunciator alarm "FFCP TROUBLE" would be received indicating an abnormal operating condition. Automatic operation of the condensate polisher would halt with control valves failing “as-is.” Numerous process alarms would be received on the local control panel.

Risk Management – Several strategies will be used in the contingency plan to mitigate any unforeseen Y2K-induced event.

- Neutralize and discharge all FFCP sumps on 12/31/99 to ensure maximum sump capacity. Regenerate cation resin in the week prior to Y2K rollover.
- Operate FFCP in passive cleanup mode during Y2K rollover (no resin regeneration or sump neutralization operation).
- Post an additional operator to assist in restoring or bypassing FFCP.
- Train control room staff and FFCP operators in probable failure modes and alarms indicating Y2K-induced failure.
- Perform walkdown of FFCP following Y2K rollover to verify proper operation.

Implementation dates for contingency plan are:

- 12/25/99 - Perform feed and condensate water conditioning per operating procedure XXXXX. Secure clean-up when feed and condensate conductivity is XXX :mhos.
- 12/29/99 - Regenerate cation resin per operating procedure XXXXX.
- 12/30/99 - Perform acid neutralization of FFCD neutralization sump and discharge water to the outfall per operating procedure XXX.
- 12/31/99 - Station additional operator at FFCD control station on swing shift.
- 01/01/00 - Verify proper system operation by performing walkdown of system using special operating procedure XXXX.

Verification – All of the planned evolutions are currently part of plant procedures. Since no new process or procedure is required, no further verification is required.

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.: **EX-02**	**Item/Component/System: Full Flow Condensate Polisher System**	**Priority:** **MEDIUM**

Risk Description: Full flow condensate polisher system (FFCP) may experience Y2K related failure due to complex interaction of multiple programmable logic controllers in the FFCP automated control system.

Risk Analysis Summary: Failure of the FFCP may cause steam generator level transients due to flow perturbations in the feed and condensate system. Extended loss of the FFCP will result in degraded steam generator water chemistry conditions. Indications of FFCP failure will be "FFCP TROUBLE" annunciator in the main control room. Numerous process control alarms will be received on the local control panel.

Risk Mitigation Strategy: Neutralize and discharge all FFCP sumps on 12/31/99 to ensure maximum sump capacity in event of a process upset. Regenerate cation resin in the week prior to Y2K rollover. Operate FFCP in passive cleanup mode during Y2K rollover (no resin regeneration or sump neutralization operation). Post additional operators to assist in restoring or bypassing FFCP in event of Y2K failure. Train control room staff and FFCP operators in probable failure modes and alarms indicating Y2K related failure. Perform walkdown of FFCP following Y2K rollover to verify proper operation of control systems.

Trigger dates for implementation

12/25/99 - Perform feed and condensate water conditioning per operating procedure XXXXX. Secure clean-up when feed and condensate conductivity is XXX :mhos or less.

12/29/99 - Regenerate cation resin per operating procedure XXXXX.

12/30/99 - Perform acid neutralization of FFCD neutralization sump and discharge water to the outfall per operating procedure XXX. Ensure neutralization sump level is less than 5 percent by 12/31/99.

12/31/99 - Station additional operator at FFCD control station on swing shift.

01/01/00 - Verify proper system operation by performing walkdown of system using special operating procedure XXXX.

Plan No.: EX-02	Item/Component/System: : Full Flow Condensate Polisher System	Page 2

Implementation:

Periods of Vulnerability: 12/31/1999 – 01/01/2000, 02/28/2000 – 02/29/2000

Implementation Timing: See trigger dates in Risk Management section

Resource Requirements: One plant equipment operator

Subject Matter Expert: O. N. Engineer

Training Required: OPS - FFCP manual operation **Completed:** _____

Exit Strategy: N/A

Verification & Approval: Verification will be accomplished by a tabletop review by facility operations staff in conjunction with the training department and the Y2K project manager.

Verified By: N/A **Date:** _____

Approved By: _____ **Date:** _____

Example 3: Contingency Plan for Plant Monitoring System Computer

Risk Identification - The plant monitoring system computer is multiprocessor, multi-tasking, and real time redundant minicomputer system providing display, alarm, trending and reports of plant operating parameters. The core limits calculator system (CLCS) module is required for power operation greater than 80 percent reactor power. The operating system was upgraded by the computer manufacturer to achieve Y2K compliance. The real-time data acquisition and display software module was modified by a third-party vendor to be Y2K compliant. Trending software was modified in-house to be Y2K ready. Integrated testing of all components was accomplished using an off-line system and simulated field inputs.

A contingency plan is deemed appropriate due to potential facility forced power reduction if CLCS is unavailable and because of the complex real time interactions of multiple software applications.

Event Analysis - Any possible Y2K computer failure would be expected to occur within minutes of Y2K rollover. Possible problems include:

- Unexpected computer halt - Indication of a PMS computer failure would be the PMS watchdog timer alarm on main control room annunciator panel.

- Application stall or abort - Application modules such as TRENDS and CLCS may not complete execution within allocated task schedule. The task manager may abort individual tasks that do not respond to scheduled interrupts. Indication of application stall could be lack of response to user request to display trend data or failure of display information to update. Display of module status on system console would show tasks as INACTIVE.

- Invalid calculation results - RCS leak rate calculations may indicate extreme or illogical leak rates. Smooth reactor power averages may show a step change in value due to ring buffer errors.

- Loss of trend display continuity - Trend displays of plant data may appear inappropriate due to ring buffer errors.

Risk Management - Contingency plans to address potential Y2K problems include:

- Unexpected PMS computer halt - Switch CLCS display to backup computer system. System date for the backup computer system is to be set 28 years back from current date as a diverse remediation strategy.
- Application stall or halt - PMS computer system engineer or computer technician shall monitor the task scheduler for proper program execution. Reset or restart stalled

applications manually. For unresolved CLCS stall, follow same procedure for PMS computer halt.

- Invalid calculation result - Follow contingency plan for PMS computer halt if CLCS output contains an invalid calculation of process parameters. Perform RCS leak rate calculations manually.

- Loss of trend display continuity - Accept as is. Short-term trend display buffer will recycle after two hours. Long-term trend display recycles after 7 days.

Implementation dates for contingency plan are:

12/20/98 - Roll back system date 28 years on backup plant computer system.

12/31/99 - Perform RCS leak rate calculations manually per operating procedure XXXX.

12/31/99 - Augment swing shift staff with computer engineer/technician to monitor PMS computer performance during Y2K rollover.

01/01/00 - Verify CLCS operability post rollover date. Switch to backup computer system if CLCS is inoperable and cannot be restored on the PMS. Verify operability of trend display function, leak rate calculation, and smooth power display.

Verification – All of the activities are to be conducted as per procedure. Resource needs have been identified and will be available on key rollover dates.

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.: **EX-03**	**Item/Component/System: Plant Monitoring System Computer System**	**Priority:** **HIGH**

Risk Description: CLCS unavailability would result in a forced power reduction. The CLCS system incorporates complex real time interaction of multiple software applications that provides potential for a Y2K-induced event.

Risk Analysis Summary: Any possible Y2K computer failure would be expected to occur within minutes of Y2K rollover. Possible problems include the following:

- Computer halt - Indication of a PMS computer failure or halt would be the PMS watchdog timer alarm on main control room annunciator panel.
- Application stall or abort – Application modules such as TRENDS and CLCS may not complete execution within allocated task schedule. The task manager may abort individual tasks that do not respond to scheduled interrupts. Indication of application stall could be lack of response to user request to display trend data or failure of display information to update. Display of module status on system console would show tasks as INACTIVE.
- Invalid calculation results – CS leak rate calculations may indicate extreme or illogical leak rates. Smooth reactor power averages may show a step change in value due to ring buffer errors.
- Loss of trend display continuity – Trend displays of plant data may appear inappropriate due to ring buffer errors.

Risk Mitigation Strategy: Contingency plans to address potential Y2K problems are as follows:

- Unexpected PMS computer halt – Switch CLCS display to backup computer system. System date for the back-up computer system is to be set 28 years back from current date as a diverse remediation strategy.
- Application stall or halt – PMS computer system engineer or computer technician shall monitor the task scheduler for proper program execution. Reset or restart stalled applications manually. For unresolved CLCS stall, follow same procedure for PMS computer halt.

Plan No.: EX-03	Item/Component/System: Plant Monitoring System Computer System	Page 2

- Invalid calculation result – Follow contingency plans for PMS computer halt if CLCS output contains an invalid calculation of process parameters. Perform RCS leak rate calculations manually.

- Loss of trend display continuity – Accept as is. Short-term trend display buffer will recycle after two hours. Long-term trend display recycles after 7 days.

Trigger dates for contingency plan implementation:

12/20/98 – Roll back system date 28 years on backup plant computer system.

12/31/99 – Perform RCS leak rate calculations manually per operating procedure XXXX.

12/31/99 – Augment swing shift staff with computer engineer/technician to monitor PMS computer performance during Y2K rollover.

01/01/00 – Verify CLCS operability post rollover date. Switch to backup computer system if CLCS is inoperable and cannot be restored on the PMS. Verify operability of trend display function, leak rate calculation, and smooth power display.

Implementation:

Periods of Vulnerability: 12/31/1999 – 0101/2000
Implementation Timing: see trigger dates in Risk Mitigation section
Resource Requirements: One nuclear computer engineer, one I&C technician
Subject Matter Expert: I. R. Smart
Training Required: None **Completed:** _____
Exit Strategy: Once CLCS is restored, perform surveillances, then discontinue use of mitigation strategies.

Verification & Approval: Each of the activities is to be conducted as per procedure. Resource needs have been identified and will be available on key rollover dates.

Verified By: _____ **Date:** _____

Approved By: _____ **Date:** _____

Example 4: Contingency Plan for Work Control System Computer

Risk Identification - The work control system (WCS) is used to initiate, plan, coordinate and implement maintenance activities at the plant. Maintenance order preparation, review and approval is computerized. Hardcopy printout of the maintenance order is generated when the job is ready to be worked in the field. The WCS is classified as a "quality affecting" computer application. The WCS is a client/server application with a graphical user interface front end that provides access to a relational database over a wide area network. The system has several Y2K vulnerabilities including its complex integration of various computer platforms, network interface, and commercial and custom software programs with date/time stamp dependencies. Remediation has consisted of implementing vendor firmware and operating system upgrades and code inspection of custom software developed in house. Successful integrated testing was conducted using a mock up of the system off line. Failure of the WCS could result in significant delays in planning and implementing emergent repairs, some of which may be directly related to Y2K events.

Event Analysis - Any Y2K-induced failure of the WCS is expected to be discovered only after Y2K rollover during the first attempt to use or access the system. Failure modes could include inability to launch the application (network or server failure), inability to access or update the database, or incorrect calculation of future routine maintenance or surveillance dates based on faulty date arithmetic.

Risk Management - Prepare special procedure to allow the maintenance order process to be initiated, planned, approved and implemented manually for emergent work if the WCS is not available. Train maintenance planner and equipment control personnel expected to be on shift during Y2K rollover on WCS contingency plan. Minimize challenges to the WCS during Y2K rollover by deferring routine report generation and maintenance schedule preparation to next business day (if possible) or until proper system operation has been verified by IT. Perform full system backup prior to Y2K rollover.
Implementation dates for contingency plan are:

7/1/99 - Approve special procedure for manual work planning in event of WCS Y2K-induced failure.
12/1/99 - Train maintenance planners and equipment control personnel on contingency plan for WCS failure and special procedure on manual work processing.
12/31/99 - Perform full system backup of WCS.
01/01/00 - IT staff confirms proper operation of WCS.
02/29/00 - IT staff confirms proper operation of WCS.

Verification -The Training department will work with Maintenance and Operations to perform a walk-through of new WCS procedure and processes. The Training department will then develop and implement training for the identified personnel. These trained personnel will then perform the manual procedure in parallel with the computerized system to verify performance and end product.

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.: **EX-04**	**Item/Component/System: Work Control System (WCS) Computer System**	**Priority:** **MEDIUM**

Risk Description: The system has Y2K vulnerability because of its complex integration of various computer platforms, network interface, and commercial and custom software programs with date/time stamp dependencies. Remediation has consisted of implementing vendor firmware and operating system upgrades and code inspection of custom software developed in-house. Integrated testing was simulated using a mock-up of the system off line. Failure of the WCS could result in significant delays in planning and implementing emergent repairs, some of which may be directly related to Y2K events.

Risk Analysis Summary: Any unexpected failure of the WCS is expected to be discovered after Y2K rollover following the first attempt to use or access the system. Failure modes can be inability to launch the application (network or server failure), inability to access or update the database, or incorrect calculation of future routine maintenance or surveillance dates based on faulty date arithmetic.

Risk Mitigation Strategy: Prepare special procedure to allow the maintenance order process to be initiated, planned, approved and implemented manually for emergent work if the WCS is not available. Train maintenance planner and equipment control personnel expected to be on shift during Y2K rollover on WCS contingency plan. Minimize challenges to the WCS during Y2K rollover by deferring routine report generation and maintenance schedule preparation to next business day (if possible) or until proper system operation has been verified by IT. Perform full system backup prior to Y2K rollover.

Trigger dates for contingency plan implementation:

7/1/99 - Approve special procedure for manual work planning in event of unexpected WCS Y2K failure.

12/1/99 - Train maintenance planners and equipment control personnel on contingency plan for WCS failure and special procedure on manual work processing.

Plan No.: EX-04	Item/Component/System: Work Control System (WCS) Computer System	Page 2

12/31/99 - Perform full system back up of WCS.

01/01/00 - IT staff confirms proper operation of WCS.

02/29/00 - IT staff confirms proper operation of WCS.

Implementation:

Periods of Vulnerability: 12/31/1999 – 01/01/2000, 02/28/2000 – 02/29/2000

Implementation Timing: See trigger dates in Risk Mitigation section

Resource Requirements: One network engineer, one WCS application engineer

Subject Matter Expert: W. F. Olsen

Training Required: Operations/Equipment Control **Completed:** _____
Maintenance Planning

Exit Strategy: Discontinue manual process when WCS restored and surveilled.

Verification & Approval: The Training department will work with maintenance and Operations to perform a walk through of new WCS procedure and processes. The Training department will then develop and implement training for the identified personnel. These trained personnel will then perform the manual procedure in parallel with the computerized system to verify performance and end product.

Verified By: _____ **Date:** _____

Approved By: _____ **Date:** _____

Example 5: Contingency Plan for Loss of Station Emergency Plan Services (This Is the Emergency Plan Specific Portion of the Plant Process Computer Contingency Plan)

Risk Identification - The facility emergency response plan (EPlan) implements the requirements of NUREG 0654 and Regulatory Guide 1.23. One of the digital components used to implement the EPlan is the use of the plant process computer (PPC) to obtain and distribute information required by and produced by EPlan requirements.

Event Analysis - A review of the joint NRC-FEMA report on the "Effect of Hurricane Andrew on the Turkey Point Nuclear Generating Station" illustrated the need to anticipate multiple failures, common mode failures and interdependent failures. Furthermore, it documented the competition for restoration resources that sometimes occurs subsequent to events. The EPlan was modified significantly to implement improvements that mitigate such concerns. Y2K events may challenge the EPlan, but it is an EPlan that has already been tested and verified.

The PPC provides a common facility to gather information from the facility in general and EPlan equipment in particular. It maintains the integrity of the data, provides it in a useful format, and maintains it as a historical record. The information is continuously passed through the offsite information system (OFIS) to the Emergency Response Data System (ERDS). Both systems are used to distribute data to decision makers onsite, locally and nationally. Although the PPC has redundant processors, they provide no diverse means for assuring the performance of their intended function.

The EPlan features are technical specifications requirements. They are commitments of the licensing basis supporting the current operating license. The PPC is one of the identified components.

The PPC has undergone an exhaustive Y2K review. Detailed assessments were cross-compared with independent vendor results and those of other utilities. The assessments included all analog-to-digital converters (ADCs), data-gathering equipment cabinets, interconnected processors, intelligent instruments and traditional software. The detailed assessment included testing measures for all critical date conditions that pertain to the PPC. All identified failure modes were remediated fully and confirmed by validation testing.

All applicable reviews were performed. The commitments of the facility software quality assurance program were maintained, and the design basis documentation for the PPC was revised. No changes to the licensing basis were made. There were no changes made that required prior regulatory review.

However, the PPC remains a critical component to smooth operation of the facility in general and the EPlan in particular. Since the PPC is a very complex digital system of

interconnected components that receives information from other similarly complex components, the Y2K team elected to develop a contingency plan.

Risk Management - The risk identified is an *internal risk*. It poses a challenge to the performance of EPlan activities. The mitigation strategy selected to offset this risk is manual data collection and requires no augmentation of existing procedures.

Subsequent to the Hurricane Andrew report, several improvements were made to the EPlan. Among these improvements was the ability to perform required activities manually for an indefinite period of time. Regular EPlan drills are conducted to demonstrate the operability of the plan. During drills, additional personnel are stationed in the control room and the emergency operations facility. Their job is to gather information from analog indicators and communicate it via diverse means (telephone and VHF radio) to EPlan command personnel.

Verification - This contingency plan will be evaluated as a Y2K induced failure of the PPC during the next EPlan drill scheduled 4th quarter 1998. Conditions appropriate to Y2K will be simulated. Multiple and interdependent failures will be tested.

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.: **EX-05**	**Item/Component/System: Station Emergency Plan Services – Plant Process Computer**	**Priority:** **LOW**

Risk Description: The facility emergency response plan (EPlan) implements the requirements of NUREG 0654 and Regulatory Guide 1.23. One of the digital components used to implement the EPlan is the use of the plant process computer (PPC) to obtain and distribute information required by and produced by EPlan features.

The PPC provides a common facility to gather information from the facility in general and EPlan equipment in particular. It maintains the integrity of the data, provides it in a useful format, and maintains it as a historical record. The information is continuously passed through the offsite information system (OFIS) to the Emergency Response Data System (ERDS). Both systems are used to distribute data to decision makers onsite, locally and nationally. Although the PPC has redundant processors, they provide no diverse means for assuring the performance of their intended function.

Risk Analysis Summary: The PPC has undergone an exhaustive Y2K review. All failure modes were remediated fully and confirmed by validation testing. However, the PPC remains a critical component to smooth operation of the facility in general and the EPlan in particular. Since the PPC is a very complex system of interconnected components that receives information from other similarly complex components, it is prudent to postulate that some degradation from Y2K events may occur.

As a result of the Hurricane Andrew report, the ability to perform required EPlan activities manually for an indefinite period of time was retained. Regular EPlan drills are performed that demonstrate the acceptable use of both. During drills, additional personnel are stationed in the control room and the Emergency Operations Facility (EOF) whose job is to gather information from analog indicators and communicate it via diverse means (telephone and VHF radio) to EPlan command personnel.

Plan No.: EX-05	Item/Component/System: Station Emergency Plan Services – Plant Process Computer	Page 2

Risk Mitigation Strategy: The mitigation strategy selected to offset this risk is manual data collection.

If the emergency plan is activated, station additional personnel in the control room and the emergency operations facility (EOF) to gather information from analog indicators and communicate it via diverse means (telephone and VHF radio) to EPlan command personnel.

Implementation:

Periods of Vulnerability: 12/31/1999 – 01/01/2000, 02/28/2000 – 02/29/2000

Implementation Timing: 12/01/1999 – Designate and train additional EPlan personnel

Resource Requirements: Two station engineers

Subject Matter Expert: J. Pederson

Training Required: EPlan Personnel **Completed:** _____

Exit strategy: Discontinue manual methods once service is restored and surveillances are completed.

Verification & Approval: This contingency plan will be evaluated as a Y2K-induced failure of the PPC during the next EPlan drill scheduled 4th quarter 1998. Conditions appropriate to Y2K will be simulated. Multiple and interdependent failures will be tested.

Verified By: _____ **Date:** _____

Approved By: _____ **Date:** _____

Example 6: Contingency Plan for Rod Position Information System

Risk Identification - The rod position information system (RPIS) performs two major functions:

- It provides rod position information to the plant monitoring information system (PMIS) for control room graphical displays and calculation of core thermal values.
- It provides for the rod worth minimizer function by operating on pre-stored rod movement sequences.

While not a true safety system, RPIS is nevertheless an important system to plant operation. It is composed of a single PDP micro-11/23 processor.

Event Analysis - A failure of the RPIS would be obvious. The RPIS software has built-in error detection and reporting for most failures. Other failure modes would consist of the entire system going off-line, which would be immediately reported to the operators via PMIS. There is no hot standby for this system, but a warm standby is available. Less than one hour is required to bring the warm standby online. This standby provides redundancy, but not diversity, as it is identical architecture to the online system. The preferred remediation method is to obtain an upgrade to the current operating system version that is fully Y2K compliant.

Risk Management - The following strategy is proposed for minimizing the effects of an RPIS outage:

- Obtain rod positions from control room panels. These indications can be manually fed into PMIS so that core thermal calculations can continue. The capability to manually substitute values in PMIS already exists.
- Use existing procedures to perform rod sequence movements, if necessary, without the automation provided by RPIS. This includes additional verification steps by control room personnel to ensure that proper sequences were being followed.
- Prepare a procedure to change the date back 28 years. Since PMIS assigns all times to control rod information, the RPIS date/time is only cosmetically important.

Implementation dates for contingency plan are:

12/1/1998	Determine, by observation and documentation, whether rod position movements during startup could be successfully and safely achieved without RPIS online. This will be following the next refueling outage.

7/1/1999	Approve contingency plan for loss of RPIS during/after critical Y2K dates.
12/1/1999	Train operations and reactor engineering personnel on RPIS contingency plan.
12/30/1999	Obtain a full image backup of the RPIS system. Check operability of backup system.
01/01/2000	Nuclear Information Services assesses operational condition of RPIS.
02/29/2000	Nuclear Information Services assesses operational condition of RPIS.

VERIFICATION - Determine, by observation and documentation, whether rod position movements during startup, could be successfully and safely achieved without RPIS online. This test will be conducted following the next refueling outage.

NEI/NUSMG 98-07	*Year 2000 Contingency Plan*	
Plan No.: EX-06	**Item/Component/System: Rod Position Information System**	**Priority: HIGH**

Risk Description: The rod position information system (RPIS) performs two major functions:

- It provides rod position information to the plant monitoring information system (PMIS) for control room graphical displays and calculation of core thermal values.
- It provides for the rod worth minimizer function by operating on pre-stored rod movement sequences.

While not a true safety system, RPIS is nevertheless an important system to plant operation. It is hosted on a single PDP Micro-11/23 processor.

Event Analysis: A failure of the RPIS would probably be obvious. The RPIS software has built-in error detection and reporting for most failures. Other failure modes would probably consist of the entire system going off-line, which would be immediately reported to the operators via PMIS. There is no hot standby for this system, but a warm standby is available. Less than one hour is required to bring the warm standby online. This standby provides redundancy, but not diversity, as it is identical architecture to the online system. The intent is to obtain an upgrade to the current operating system version that is fully Y2K compliant.

Risk Mitigation Strategy: The following strategy is proposed for minimizing the effects of an RPIS outage:

- Obtain rod positions from the control room panels. These indications can be manually fed into PMIS so that core thermal calculations could continue. The capability to manually substitute values in PMIS already exists.
- Use existing procedures to perform rod sequence movements, if necessary, without the automation provided by RPIS. This includes additional verification steps by control room personnel to ensure that proper sequences were being followed.
- Prepare a procedure change to set the date back 28 years, at least until the operating system can be upgraded. Since PMIS assigns all times to control rod information, the RPIS date/time is only cosmetically important.

Trigger dates for contingency plan implementation:

12/1/1998	Determine, by observation and documentation, whether rod position movements during startup, could be successfully and safely achieved without RPIS online. This will be following the next refueling outage.
7/1/1999	Approve contingency plan for loss of RPIS during/after critical Y2K dates.
12/1/1999	Train operations and reactor engineering personnel on RPIS contingency plan .

Plan No.: EX-06	Item/Component/System: Rod Position Information System	Page 2

12/30/1999	Obtain a full image backup of the RPIS system. Check operability of backup system.	
01/01/2000	Nuclear Information Services assesses operational condition of RPIS.	
02/29/2000	Nuclear Information Services assesses operational condition of RPIS.	

Implementation:

Periods of Vulnerability: 12/31/1999 – 01/01/2000, 02/28/2000 – 02/29/2000

Implementation Timing: See trigger dates in Risk Mitigation section.

Resource Requirements: One NIS engineer**.**

Subject Matter Expert: T. I. Simple

Training Required: Operations Reactor Engineering **Completed:** _____

Exit Strategy: Discontinue manual methods once RPIS is restored and surveilled.

Verification & Approval: Determine, by observation and documentation, whether rod position movements during startup, could be successfully and safely achieved without RPIS online. This test will be conducted following the next refueling outage.

Verified By: _____ **Date:** _____

Approved By: _____ **Date:** _____

APPENDIX D

Examples of External Contingency Plans

As discussed in Section 7, external Y2K events are outside the direct control of the facility. Some external events are important enough to the safety of the facility that they were anticipated in design basis accident analyses. They have also been addressed exhaustively in existing contingency plans, probabilistic risk assessments (PRA), failure modes and events analysis (FMEA) and integrated plant evaluations (IPE). External events that the facility may elect to plan as part of their Y2K contingency planning process include:

- loss of offsite power
- grid instabilities
- interruption of consumable supplies such as bottled gases, domestic water, diesel fuel and telephones.
- loss of emergency plan equipment and services such as sirens, meteorology and communications equipment.

Three examples of individual contingency plans for external events are included.

Year 2000 Contingency Plan	Plan Number: 2000-01
Item/Component/System: Station Consumables	**Priority:** Medium

Risk Analysis: Consumable providers may not be able to provide a steady supply of consumables to the station as a result of Y2K-related interruptions

Risk Mitigation Strategy and Actions

1. Materials Management will review status of Y2K readiness for all consumable vendors and identify any vendors and their associated consumables that may be at risk on key rollover dates. Initiate a contract with an alternate, Y2K ready vendor for any critical plant consumable that is identified to be at risk from a primary vendor.
2. Maintain the following plant consumables at the 90% level or greater during the implementation timing periods below. At the end of these periods, return to nominal consumable stocking levels:
    - Main generator hydrogen storage farm
    - Containment atmosphere dilution (CAD) nitrogen tank level
    - Containment atmosphere control (CAC) nitrogen tank level
    - Reactor water chemistry chemical reagents
    - Auxiliary boiler fuel oil storage tank
    - Site vehicle gasoline storage tank
    - Emergency diesel fuel oil storage tanks
    - Emergency diesel fuel oil day storage tanks
    - Emergency diesel generator CARDOX CO2 storage tank
    - Lubricating oils and greases (operations storage area)
    - Turbine building CARDOX CO2 storage tank level
    - Sodium Hypochlorite tank for chlorine injection system
    - Pure water storage tank levels
    - Portable nitrogen bottles for plant use
    - Bottled gas bottles for welding and other maintenance

Implementation

Period of Vulnerability:	December 31, 1999 to January 1, 2000 February 28, 2000 to February 29, 2000
Implementation Timing:	08:00 December 20, 1999 to 08:00 January 7, 2000 08:00 February 17, 2000 to 08:00 March 6, 2000
Resource Requirements:	None
Subject Matter Expert:	John Smith x1234
Training Required:	None
Extra Strategy:	N/A

Verification: Review facility procedures for consumable vulnerabilities and compare against the list above.

Verified by: _____ **Date:** _____

Approved by: _____ **Date:** _____

Year 2000 Contingency Plan — Plan Number: 2000-02

Item/Component/System: Loss of external 500-kV grid system

Priority: High

Risk Analysis: There is a small potential for loss of the external 500-kV grid system due to a Y2K-induced failure at other sites connected to the grid system.

Risk Mitigation Strategy and Actions

1. Station an augmented operations crew on shift from 18:00 on December 31, 1999, until 18:00 January 1, 2000, and from 18:00 on February 28, 2000, until 18:00 on February 29, 2000. Additional personnel are listed on the attached modified shift lineup sheet.
2. Coordinate with the load dispatcher to reduce plant power on both units to 95% power from 23:00 on December 31, 1999, to 04:00 on January 1, 2000, and from 23:00 on February 28, 2000, to 04:00 on February 29, 2000, to provide additional operating margin in case of grid voltage fluctuations.
3. Station an additional plant reactor operator at the chief operator's station to monitor grid voltage and generator parameters.
4. In case of loss of grid, the station will execute the loss-of-grid casualty procedure using the additional operators to assist with dual-unit scram actions.

Implementation

Period of Vulnerability: December 31, 1999 to January 1, 2000
February 28, 2000 to February 29, 2000

Implementation Timing: 18:00 December 30, 1999 to 18:00 January 1, 2000
18:00 February 27, 2000 to 18:00 February 29, 2000

Resource Requirements: None

Subject Matter Expert: John Smith x1234

Training Required: Each operations crew will review the loss of offsite power procedure during the November-December 1999 training cycle. Principal crews scheduled to be on shift during the vulnerability period also will conduct a crew simulator session involving loss of offsite power in the week before the vulnerability period.

Exit Strategy: Follow guidance contained in approved facility procedures.

Verification: N/A covered by facility procedure approval process.

Verified by: _____ **Date:** _____

Approved by: _____ **Date:** _____

Contingency Plan 2000-3

Item/Component/System: Telecommunications

Risk Identification

Facility emergency plans and disaster recovery plans depend on the availability of telecommunications.

Event Analysis

Since the Y2K readiness of telecommunications companies does not assure continuity of service and many Y2K experts indicate that questions still exist concerning Y2K-related failures within the integrated telecommunications network, there is some risk of the plant experiencing some period of telecommunications service disruption.

The telephone company supplying services has been contacted and has indicated that they will be Y2K ready by the first quarter of 1999; but because of the complexity of the service, they cannot preclude possible service disruptions. The Y2K team has thus determined that a contingency plan is appropriate.

Risk Management

Each department will evaluate any operational impact from the loss of telecommunications. Departments will provide a list of license-based and business-critical activities that would be impacted by a loss of telecommunications and indicate the time required before the impact would be exhibited.

Each department will prioritize their impacted business processes and assess the need for a mitigation strategy. Examples include:

Emergency Preparedness

Callout of emergency plan personnel is dependent on telephones. Therefore, emergency facilities will be pre-staffed at a pre-determined level for the millennium turnover and leap year transition.

Communications with off-site city, county, state and federal agencies also depend on telephones. Portable radios will be issued to all agencies within radio range and text beepers will be issued to the remaining agencies. Alternate mitigation strategies can include Y2K-compliant direct link satellite mobile phones or relocation of personnel within radio range (This presumes you have found a supplier that is already Y2K ready).

Contingency Plan 2000-3 (Continued)

Operations

Fire department communications will be assured by providing the local fire station with a portable radio.

Law enforcement communications will be assured by providing the sheriff's department with a portable radio.

Medical emergency communication will be assured by providing the local hospital with a portable radio.

Implementation

Period of Vulnerability:	December 31, 1999 to January 1, 2000 February 28, 2000 to February 29, 2000
Implementation Timing:	January 1, 1999 for equipment purchase December 31, 1999 to January 1, 2000 February 28, 2000 to February 29, 2000
Resource Requirements:	Designated EP staff and designated departmental staff resources
Subject Matter Expert:	John Smith at x1234
Training Required:	None

Exit Strategy: Resumption of normal service will be accompanied by announcements over approved facility communications equipment that primary service has been restored.

Verification: Station procedures will be reviewed to ensure that no other related vulnerabilities exist.

Verified By: _____ Date: _____

Approved By: _____ Date: _____

APPENDIX E

Integrated Contingency Plan Matrix

This is an example of an integrated Y2K contingency plan matrix that is developed and used as part of the integrated contingency plan. This matrix is compiled as the remediation, internal risks and external risk individual contingency plans are submitted to the Y2K project manager. This matrix should be a controlled document that is frequently reviewed and updated for implementation timing and resources actions. The Y2K project manager should use this matrix to provide input to the project management scheduling program. Relationships and dependencies associated with the individual contingency plans should be identified and resolved based on the review of this matrix.

Plan No.	Item, System, Component	Risk Description	Mitigation Strategy	Vulnerable Period	Implementation Timing	Resources	Subject Matter Expert	PRI.
001	FULL FLOW CONDENSATE POLISHER (FFCP)	Risk may cause transients in S/G water level with possible safety system activation if S/G level control is lost. Extended loss will result in degraded S/G water quality.	Operate FFCP in passive cleanup mode during Y2K key rollover dates.	Key rollover dates between 12/31/99 to 01/01/00	12/25/99 perform OP XX, 12/29/99 regen. Per OP XX, 12/30/99 acid neut. Per OP XX, 12/31/99 station additional operator	Post one additional operator at FFCP control station	O. N. Engineer	High
002	WORK CONTROL SYSTEM COMPUTER (WCS)	Risk of inability to run application and access data base, and loss of ability to schedule and track surveillance	Prepare special procedure to manually perform work order process to be used for emergent work if WCS is not available. Perform full backup prior to key rollover dates.	12/3/99 to 01/01/00 02/28/00 to 03/01/00	07/1/99 Approve special procedure, 12/01/99 train maint. planners on procedure, 12/31/99 Full system backup of WCS. 01/01/00 IT staff verify operation of WCS.	Procedure prep 40 man hours, System backup IT 8 hours, Training 48 man hours.	W. F. Olsen	Medium
003	CONSUMABLE WATER TREATMENT CHEMICALS	Depletion of chemicals required for resin regeneration and water treatment. Risk is deterioration of water quality over time.	Stockpile supplies by topping off chemical tanks and having 60 day supply of bulk chemicals in the warehouse.	January 2000	12/20/99 Order sufficient chemicals to top off tanks. 12/20/99 Verify warehouse has 60-day supply of identified bulk chemicals. 01/03/00 Contact chemical suppliers and verify continuing supply chain.	Work performed as routine, 4 hours.	D. M. Johnson	Low

Figure E-1 Example Integrated Contingency Plan Matrix

APPENDIX F

Boundary Analysis and Supply Chain Readiness

Boundary Analysis—Consideration of external events may be facilitated by the use of boundary analysis. Figure F-1 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.

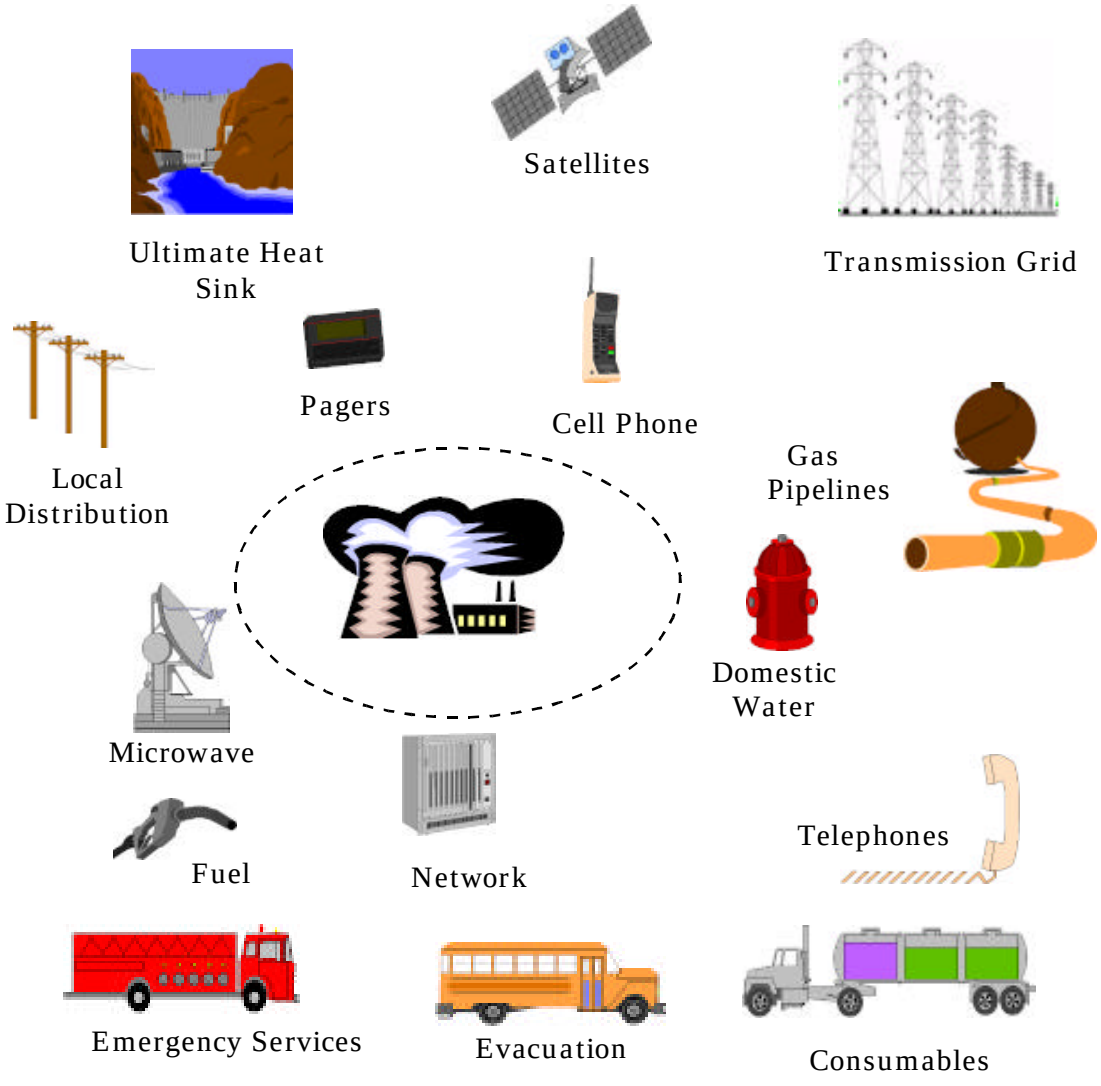

Figure F-1 External Event Boundary Analysis

An example that illustrates the use of the technique is: the ultimate heat sink for the facility is the level of water in the river. The water level is maintained by control of gates operated by another utility as part of its hydro-electric power generation division. There are technical specification requirements for river water level and temperature. Plant instrumentation indicating this information is transmitted to the hydro facility control room. The facility can also communicate with the hydro facility by phone.

Concerns regarding indication and communication have surfaced as part of the Y2K project detailed assessment. The external interface has been identified as a risk to the safe operation of the facility. To mitigate the risk, the facility has invested in suitable portable radios to provide a diverse means of communication.

Affected procedures have been revised at both facilities. Simulators have been upgraded to allow revised operator training. The radio system has been added to the appropriate surveillance procedures.

Supply Chain Readiness—The supply chain warrants special attention for critical consumables. A critical element of external event analysis is to understand the complete supply chain for critical systems and suppliers. Figure F-2 illustrates a process for assessing the Y2K risks that result from dependence on suppliers and their partners. The supply chain is only as strong as its weakest link. The weak links should be identified and analyzed. An appropriate mitigation strategy should be selected. The facility may place some reliance on the remediation program of the supplier.

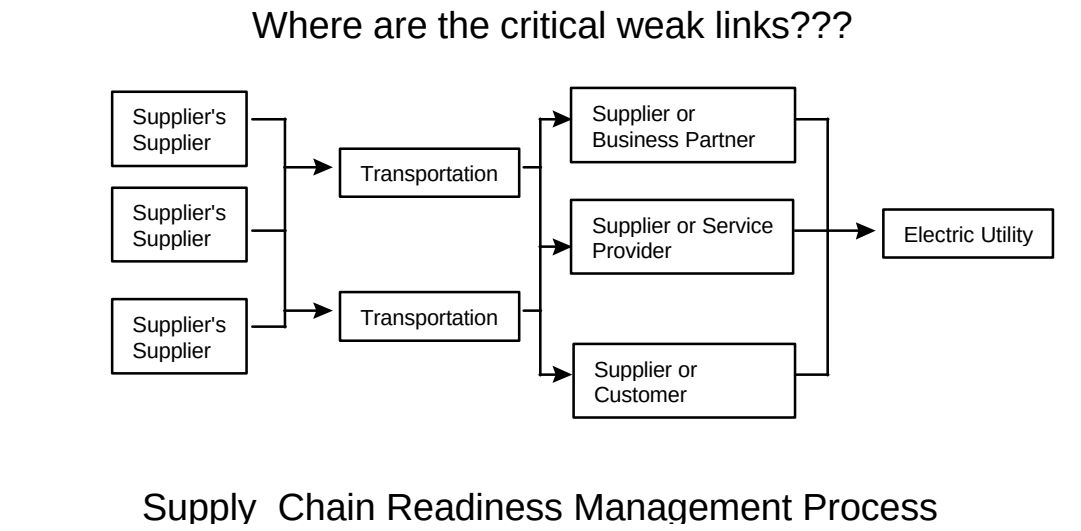

Figure F-2: Supply Chain Readiness Management