The work on the Y2k issue in Sweden

Bo Liwång
Deputy Head
Department of Plant Safety Assessment
Swedish Nuclear Power Inspectorate
SE-106 58 Stockholm, SWEDEN
bo.liwang@ski.se
www.ski.se

Introduction

This paper will give a overview presentation of the work performed in Sweden on the Y2k issue. The paper will present the projects at the utilities, some lessons learned and the work performed by the regulatory body.

The layout and performance of the projects at the utilities

Summary of current status at Barsebäck nuclear power plant (BKAB)
2 Units (ABB-Atom BWR)

General

The work in securing year-2000 compliance has been underway for slightly more that a year. Since January 1, 1998, it has been carried out as a project with responsibility for all equipment at BKAB. Special procedures have been prepared for the project, as well as procedures governing the various phases of the work. The project reports directly to BKAB’s President.

The project is divided into a number of phases, beginning with Inventory and Classification and concluding with Verification and Start-up. The project’s objective was to ensure that all equipment that can affect safety or availability were made compliant by December 31, 1998. This objective has not been able to be reached but they are very close. All other equipment should be compliant by June 30, 1999.

Inventory

The purpose is to identify all systems and equipment that may contain components critical to the year-2000 transition. Components not owned by BKAB but which are important to BKAB’s organisation and operation are also being included in this process.
In an effort to attain structured methods and to ensure the quality of the work, inventory is taken in a number of different ways. A total of 40,000 components have been identified and approximately 700 of these are the component of further analysis. The others have been eliminated since they contain no processors.

Classification and setting priorities

The components that have not immediately been eliminated by the screening process have been divided into categories which form the basis for continued work and determine the quality requirements that will be set for further analysis and verification. Two definitions have been used: safety class and time class. The first category for classification is based on the component’s effect on safety and availability while the second is based on the point in time when possible tests and actions on the component can and must be taken. The safety classes have ten levels where class 1 defines a component with direct effect on reactor safety and class 2 contains components that have an indirect effect on reactor safety.

Analysis

An analysis is performed on those components not immediately screened out by the inventory process. The supplier of the equipment usually performs this analysis. The information requested must be in writing and contain an account of the analyses and tests the supplier has performed which form the basis for the information they have provided. The information is evaluated by the project and requirements for high quality work on the part of the supplier increase according to the component’s importance in terms of safety.

For class 1 components approved by the supplier, additional verifying tests, when possible, will be carried out in an operational environment as an added assurance of proper function. Other components of special interest will also be tested.

A general test procedure has been established, based on, among other things, a number of international standards. Component-specific tests are set up, based on these standards.

In cases where tests cannot be carried out on class 1 components, e.g., the date can not be entered, a more comprehensive analysis of the component may be called for.

Actions, Verification and Start-up

When it has been established that an component cannot cope with the year-2000 transition correctly, a decision is taken regarding further action. The choice of action is determined by the component’s safety class and by the effect the problem has on the component’s function. In cases where the equipment must be modified by replacing some form of hardware/software, this work will be carried out according to Barsebäck’s normal procedures for plant modifications.
Contingency plans

Since the Y2k problem is of the CCF (Common Cause Failure) type, and taking the point in time into account, a contingency plan will be drawn up for plant operation at the critical times. This plan is based on an analysis of the most critical systems in the plant, with the aim of determining which of these could in any way contain Y2k problems. This is followed by a study to determine the consequences of a malfunction in any of these systems and to establish a contingency plan for safely managing any possible disruptions in operation.

The plan will be developed during the autumn of 1998 so that it can, if necessary, be used as early as the end of 1998.

Project status

Work on the specific project has been underway since January 1, 1998. For the refuelling and maintenance outages during 1998, test procedures have been developed and tests have been carried out on some of the most important components and systems.

The comprehensive inventory and classification work is essentially finished. Only minor portions of the work remain to be completed. To ensure that no components that could affect reactor safety have been neglected, a function-oriented examination of safety systems is made as well as a comparison with the PSA model’s database.

During the refuelling and maintenance outage at Barsebäck 1 and 2, tests were carried out on ten different systems. An evaluation of the first five tests is currently being made and the preliminary results indicate no particular problems. One minor problem was identified in one of the five systems, which has no practical bearing on the system’s function from the standpoint of safety or operation.

A summary has been made of the plant-critical components, i.e., those that affect or may affect reactor safety, other safety/operating systems, as well as components in functions that can lead to transients or cause scrams. This basically corresponds to the previously mentioned class 1 and class 2 components. A total of approx. 100 such components have been identified. To date, all of these, except 3 or 4 components, have been certified as year-2000 compliant. The remaining components are technical approved but the final decision is not taken.

Summary of current status at the Forsmark power plant (FKA)
3 Units (ABB Atom BWR)

General

A comprehensive project called the Forsmark Millennium Project (FMP) is underway at the Forsmark power plant, intended to identify all equipment that may be affected by calendar events. Those components that are directly connected to reactor safety and/or production are handled separately in subprojects at the respective production units. This has been done in order to concentrate the work and to facilitate quick decisions in the event that faults or deficiencies are uncovered.
The production units have concentrated their work in an effort to categorise and rank the systems in the plant directly connected to safety or to production capacity.

Systems and functions to be followed up and inspected have been given priority according to the following: Safety systems according to "Final Safety Analysis Report (FSAR)" (electrical class 1E), other systems vital to safety (inspection group 1) and systems affecting operation and availability.

Up until now, most of the work has been devoted to identifying systems, subsystems and components that may be sensitive to the year-2000 transition. A number of criteria have been established to support the analysis work being done to identify equipment that may be sensitive to the year-2000 transition.

Currently, analyses, tests and definitions of necessary plant modifications are underway. As the inventory work and analyses are completed during the autumn of 1998, the work will be concentrated more on ensuring the quality and follow up of plant modifications that have already been decided and to ensure that all aspects regarding safety systems are taken into account.

According to the current schedule, the first two of the above mentioned priority areas should be thoroughly analysed by January 1, 1999. Any necessary actions may be carried out at a later date, depending on the type of action called for. All systems, including the above-mentioned systems that may affect operation or availability, must be analysed and any necessary action taken when the 1999 refuelling and maintenance outage has been completed. There is nothing at present to indicate that the schedule cannot be met.

A programme is currently being carried out to identify any possible built-in potentially sensitive systems, “embedded systems”. The main existing equipment groups, such as Combitrol and Combimatic will be examined at the circuit board level. Examinations of other product groups, e.g., relay equipment and controller measurement transducers, will also be performed.

Forsmark 3 has initiated joint work and an exchange of information with Oskarshamn 3, which for the most part has identical equipment. Forsmark 1 and 2 have, in the same way, begun collaborating with TVO in Finland.

To ensure the identification of all sensitive equipment, the selection of equipment is made using supplementary methods such as interviews, searches in the plant registers and product groups, as well as by system.

In the case of Forsmark 1 and 2, the principle applied to applications in the three priority groups mentioned above is that testing is the first alternative. Only when testing proves to be unfeasible should a decision be made as to whether the letters of exemption received should be considered valid.

Forsmark 1 and 2

The basic design of these reactors contains no microprocessor-based systems. For this reason, work to identify such systems can be focused on those modifications made to the plant since the systems were originally delivered.
Within the scope of Forsmarks millennium project, a total inventory has been taken, based on the accumulated knowledge of the various systems in the respective sections. This inventory is documented in a separate catalog. Aside from this inventory, all technical deliveries have been examined and assessed in regard to microprocessor-based systems. Information from this examination supplements the above mentioned catalog. These examinations are in turn supplemented by examinations of the circuit diagram of certain specific systems.

Project status indicates that two systems defined as safety systems according to FSAR (electrical class 1E) have been identified. Letters of exemption from the suppliers exist for both of these systems but tests under actual operating conditions will be carried out, checked and approved before the systems are declared year-2000 compliant.

A limited number of systems have been identified in other priority areas, and these are now being subjected to further testing independently of the actions that the manufacturer has taken. In certain cases, the equipment will be replaced.

Formark 3

The largest component group is the analogue electronic circuits and hardware-based logic systems, which has been examined at the circuit board level. The general system diagrams have been studied to identify possible CPU’s, memory or clocks. This component group can be found at approximately 1600 locations in the plant, for example in the original delivery of the central safety logic, and are, with some few exceptions, year-2000 compliant. With few exceptions, the equipment in these systems can be exempted completely, based on the fact that they contain no CPU’s, clock circuits or calendar functions.

Some systems according to FSAR (electrical class 1E) have been identified for further analysis. Most of them have been preliminarily exempted but additional analyses and tests must be carried out before they can be definitely exempted.

A limited number of systems have been identified in other priority areas. No problems are expected. Replacement is planned in certain cases for 1999 and a check for year-2000 problems will made as part of the delivery tests. In some cases, for example fuel loading machines during the refuelling and maintenance outage, plant modifications will be necessary. The suppliers have reported on the components that are not year-2000 compliant and have suggested upgrades.

Summary of current status at the Oskarshamm nuclear power plant (OKG AB)
3 Units ( ABB Atom BWR )

Background

The overall planning for year-2000 work within OKG started during the spring of 1997 as a part of the Sydkraft Group’s general Y2k project.

OKG’s own project, MILLE 2000, started in August 1997. The project was organised and staffed during September 1997. During the planning phase, all departments and units at OKG were informed of the impending work.
A Project handbook was written in the initial phase of the project. The purpose of the handbook was to serve as an aid in guiding and co-ordinating the subprojects and for activity managers in the project. The MILLE 2000 project has been divided into three main areas/subprojects; Process Systems, Technical Systems and Administrative Systems.

The subprojects were started in October 1997 and are managed by subproject managers from the technical department as well as group managers from the various specialist areas.

**Process systems**

The Process System subproject is responsible for ensuring that all systems/components linked to processes are dealt with.

Basic inventory was carried out in late 1997 according to the instructions that had been developed and documented in the Project Handbook. The inventory was carried out by the respective units’ operation and maintenance departments, through meetings and interviews with system managers to utilise their knowledge of the processes and familiarity with components. The inventory work has made use of a broad network of contacts, which has lead to an increased awareness of year-2000 concerns within OKG.

Additional checks will be carried out during autumn 1998 to ensure that the selected methods of taking inventory have identified all systems and components that can be affected by the millennium transition. These checks will be carried out by the technical department using the basic material produced during the PSA analyses of units 1, 2, and 3 as a starting point. The purpose is, through the use of supplementary methods, to specifically check those systems and components whose function, in connection with PSA work, was found to be safety related. The inventory work already carried out by the respective units and the function-oriented examination that is carried out with the PSA model’s database, is considered adequate to ensure that all components in safety systems containing processors are identified.

**Technical systems**

The subproject Technical Systems encompasses OKG’s computer infrastructure. It includes the PC network’s hardware and system software as well as technical application programmes. This group also includes the unit’s process computers, plant security computers, and dosimetry and chemical systems. The work associated with identifying year-2000 problems is underway, using the same methods as those utilised for process systems.

**Priorities**

Setting priorities for necessary corrective actions has been based on applicable functional classification of electrical equipment, in which systems/components with safety functions will be given highest priority in the continuing work.

**Analysis/examination/testing**

Work with continuing analysis and tests is carried out in accordance with instructions that were developed for the Project Handbook. The instructions describe the procedures for ensuring that identified components are year-2000 compliant as well as stipulating the way in
which the work is documented. In principle, the procedure includes making a test selection based on a component/design examination and to formulate the test itself. The work is concluded with a summary of test results, a decision is made as to the component’s millennium compliance and the work conducted is summarised in a report. The instructions provide ample guidance for the work and experience gained from a number of international documents has been used in formulating the instructions.

Summary and comments

OKG considers that the inventory work already carried out and the work now underway will identify all components in the various groups that contain technology that may be affected by the millennium transition.

The unit-specific account of the progress made by the project during August 1998 showed that the calendar events identified as being sensitive cannot have a direct effect on reactor safety.

Certain problems have been identified in, for example, power control systems. These are not safety systems but a fault would probably lead to a scram. A plan of action is now being formulated and in those cases where it is considered necessary, temporary solutions have been implemented.

Deficiencies have also been detected in certain information systems. Minor modifications and adaptations will be made during autumn 1998.

According the schedule for OKG’s millennium project, all actions on safety related systems should have been completed by December 31, 1998. Actions on other systems should be completed by June 30, 1999. There is nothing at present to indicate that the schedule cannot be met.

Summary of current status at the Ringhals nuclear power plant (Vattenfall)
4 Units ( 1 ABB Atom BWR, 3 Westinghouse PWR )

General

The Ringhals year-2000 project has been underway for over a year. The work is carried out according to methods documented in procedures, instructions and reports. The project is divided into three phases: phase 1 – pilot study, phase 2 – inventory, analysis and assessment, phase 3 – actions.

The project’s objective are; maintained reactor safety (documented and with no uncertainties), maintained personal safety, no disruptions in production and no other serious disruptions.

The project has progressed according to plan and phase 2 is completed, except for some minor areas. Phase 3 has been initiated to the extent that orders for actions have been placed at the departments that will implement these actions.
Phase 2 – inventory, analysis and assessment

A number of procedures and method descriptions have been developed to ensure high-quality work for the various stages. During inventory, the plant register has been searched for equipment containing process electronics, software and/or hardware. Components that may contain date fields, plus a number of details about the component, have been noted in a database. During the inventory process, system and component specialists have been interviewed and documentation from plant modifications has been examined.

In conjunction with the inventory process, all components have been placed in different risk classes, depending on if the component belongs to a system that can affect reactor, personal or operating safety.

In order to compile information on the identified components, suppliers have been requested to fill in a questionnaire. Their answers have been registered in a database.

When the submitted information has been compiled, it is dealt with in assessment groups comprised of people representing operation, maintenance, electronics, design, computers and quality. The first step in the assessment is to examine each component’s risk class, after which the component, based on the assembled documentation and knowledge of the component and its function, is judged to be safe or unsafe. Requirements regarding the scope of the documentation are dictated by the component’s risk class. All assessments are documented in minutes from meetings and are registered in the database.

To ensure that all equipment significant to safety is examined, an independent study of safety-related equipment is carried out as defined by the Technical Specifications and Final Safety Analysis Report. This study is performed by three people, representing operation, maintenance and technology. These people have not previously been involved in Y2k work and have thorough knowledge in their areas. As an additional measure, the spare parts warehouse is also examined.

Phase 3 – Actions

Responsibility for carrying out the actions necessary to ensure compliance of equipment found to be unsafe lies with the production units/system managers, as is the case with plant modifications. When these actions are carried out, the quality procedures for maintenance and plant modification work are observed. Certain supplements to normal procedures will, however, be drawn up. Implemented actions will be documented in reports and registered in the database.

Current status

Phase 3, Actions, has started. More than 200 inquiries have been made to suppliers, approximately 90% of which have been answered. Some responses concerning important systems have still not been received, which could result in a delay of the analysis. It may also be necessary to replace these systems due to a lack of information about them.

Phase 3 work has been initiated by planning actions according to normal routines to ensure the quality of their implementation.
No problems in major safety systems have been identified during the course of inventory and analysis. There are some measuring systems that have not yet been certified as being year-2000 compliant due to the fact that all information on these systems has not yet been submitted.

During the annual review of Ringhals 1, a number of tests were carried out. The preliminary results do not indicate any major problems.

*Emergency preparedness*

In response to the possible risk of disruptions in offsite power, water supply or other necessary systems due to the millennium transition, emergency plans will be drawn up.

*Lessons learned and typical types of problems found*

Of course there are a lot of small lessons learned but the main ones are;

It takes time, both in work hour but also in calendar time to perform identification, analysis and corrective actions.

The fault does not always occur at the time transition. The system can work as normal, but when a disturbance is introduced the system behave in a faulty way. That makes it very important that the test procedures are designed to take this into account.

It is important to identify and analyse equipment that is not a part of the plant but is used by contractors for maintenance of plant systems. This equipment is mostly not documented in the plant documentation system which can make them hard to find. One way is to interview the maintenance personnel.

The typical type of problems that have been seen is mostly not in the main function of the system. It is mostly the operators terminal and its communication that are the problem, not its safety function.

*The review of the regulatory body*

The legal situation in Sweden is clear. The utilities have the responsibility for the safety of the plants, and the Regulatory body has the responsibility to look after that the utilities takes their responsibility. What this means is the inspectorate has not the resources to review the solutions of the actual technical problem, the inspectorate concentrate on reviewing how the utilities work with the problem.

Once every half year the inspectorate formulates its conclusions, based on the reviews and inspections of the work performed by the utilities, of the situation in a report that is sent to the government.
In the report that was sent to the government in September 1998 the inspectorate made the following conclusions:

1. Problems encountered with the new millennium will not pose a threat to reactor safety.
2. Steps are being taken to minimise the risk of disruptions in operation.
3. The work carried out by the licensees is serious, well organised, with well-structured work methods.
4. The work performed is planned to allow adequate margins in the event of unexpected problems.
5. Steps are being taken to minimise the risk of external events affecting reactor safety or availability.
6. At present, no further directives to the licensees are necessary and work can proceed as planned.

In September 1999 there will be a detailed review of the situation especially on the safety systems at the plants as part of the final review and conclusions of the situation. If the inspectorate is not satisfied with the situation the actual utility can be forced to perform additional actions or to close the plant down during not safe time transitions.