Millennium Challenge: The Canadian Regulatory Strategy

Namir Anani, P.Eng., Head, Instrumentation Control and Electrical Group, AECB  
Tom Schaubel, P.Eng., Reliability and Probabilistic Risk Assessment Group, AECB  
Byron House, E.I.T., Instrumentation Control and Electrical Group, AECB

Keywords: regulator, nuclear, Y2K, millennium, contingency plans

Abstract

The Atomic Energy Control Board of Canada has viewed the "millennium bug" as a serious potential threat to the safety of nuclear plants. Public concerns for the millennium include the challenges that the Year 2000 or Y2K problem may present to nuclear safety. We have put a licensing process in place and requested the licensees to demonstrate that Year 2000 issues are being adequately addressed.

A graded approach methodology has been adopted with the purpose of dealing with the important safety systems first. This risk prioritization plan addresses our priority and mandate to ensure public safety and gives us confidence that the licensees have an appropriate program in place to meet the AECB’s June 30, 1999 date for Y2K readiness.

While we have not seen any serious Y2K problems that would directly impair safety system operation, we have found that certain tools used for the maintenance and calibration of these systems have Y2K problems. Our investigation challenged conventional thinking on Y2K dependencies by requesting arguments for the assumptions made and ensuring that they are based on sound scientific knowledge and engineering principles. The licensees were requested to provide complete and accurate documentation showing all places where date-dependent information flows within and between digital systems. For systems that were developed decades earlier, it is not always easy to produce such essential documents.

In addition to insisting on an open and auditable Y2K review process, we have required our licensees to present contingency plans. The plans must take into account that the Y2K problem must be viewed as a potential "common cause of failure" leading to simultaneous failures in several systems such as internal and external services.

This paper describes the process, and discusses a number of issues that have arisen as the work proceeds.
Introduction

Over the past few years the Year 2000 problem began receiving world-wide attention. Awareness of this issue has since increased considerably. The Atomic Energy Control Board of Canada viewed the "millennium bug" as a serious potential threat to the safety of nuclear plants.

The AECB realized that this may impact several layers that make up the real-time or the embedded component of digital systems, and include: system hardware, operating system software, application software, application data, and programming support tools. We then focussed our attention on licensees of major nuclear facilities: nuclear power reactors, research reactors, high energy particle accelerators, uranium mines and mills, nuclear fuel fabrication facilities, radioactive waste management facilities.

This paper will discuss some of the lessons learned so far and the experience gained in tackling the new challenge Y2K brings.

Contingency plans are an important element of the preparation necessary for the year 2000. The contingency plans have to deal with problems from both the internal and external risks of the year 2000 date transition. AECB’s policy on contingency plans will be presented in this paper.

Although, the AECB has adopted a strategy to deal with year 2000 and all its licensees, the scope of this paper will only focus on how this strategy has been applied to our nuclear power plant licensees.

AECB Y2K Strategy

Public concerns for the millennium include the challenges that the Y2K problem may present to nuclear safety. AECB’s position is that the Year 2000 and its impact dates shall not result in undue risk to health, safety, security and the environment, and more specifically shall not:

- result in any safety related transients;
- invalidate the requirements of the Atomic Energy Control Act and regulations;
- violate any license condition or assumptions made in the licensing basis.

Early in 1997, the AECB sent a letter to each licensee requesting to be informed of their intent. Concerned that the approach lacked formality, the AECB then sent further letters identifying the minimum expectations. The AECB required the licensees to examine, correct, and test all aspects of the plants which may be impacted by Y2K problems and could potentially increase the risk to health, safety, security, and environment before the millennium approaches.
A letter was sent to each licensee requesting:

- a list of all computer based systems important to safety
- details of risk assessment
- details of testing plans
- details of contingency plans
- details of Y2K project plan with a schedule

This resulted in formal plans submitted by all licensees to AECB staff. The AECB established a graded approach strategy to address various differences in priorities. Furthermore, a comprehensive strategy was developed to deal with the Y2K problem, and actions were taken to see that our own internal systems and those of our licensees are corrected, if required.

The graded approach strategy is essentially the treatment of Y2K issues based on risk significant basis, beginning with systems deemed the most critical. The development of this strategy followed with the development of a comprehensive review criteria which includes: planning and resources, inventory of Y2K dependent digital assets, impact assessment, remediation actions, and contingency plans.

The highest priority was to ensure that in the event of an incident, the plant would be able to shutdown, cool and contain. To do this the AECB’s first priority was the last line of defence in the accident sequence to prevent fuel damage, ie. assurance should be given that the four Special Safety Systems\(^1\) will not be affected by the Y2K problem.

After the four Special Safety Systems the next priority were those systems whose failure could challenge the Special Safety Systems. The priority was then focused on those systems involved in the sequence of events which could lead to a challenge of the special safety systems to reduce the probability of disturbances or initiating events and that the systems which are designed to mitigate these events have been reviewed.

Figure 1 shows the major project priorities and milestone dates for the nuclear power plants that were communicated to the licensees. The AECB required a remediation plan that had three major milestone dates: October 1, 1998; December 31, 1998; and June 30, 1999. The first date is significant for two reasons. First, it established a clear message that the Special Safety Systems were to be remediated first. Secondly, it provided an opportunity for the AECB to assess the licensees’ ability to meet our June 30, 1999 deadline.

---

\(^1\) CANDU designs have four Special Safety Systems which are - two shutdown systems, a containment system, and an emergency core cooling system.
Three major aspects of the AECB’s Y2K graded approach strategy are: Demonstration, Assurance, and Disclosure. Figure 2 illustrates where these aspects fit on the project process.

Many demonstration meetings have been held with the licensees. Some of these meetings involved a detailed guided walkthrough of targeted systems. It was apparent early that the licensees were taking the Year 2000 problem seriously. All power reactor licensees have demonstrated that as of October 1, 1998, their Special Safety Systems will not be impaired in any way by the passing of all impact dates including the transition from 1999 to 2000.

Furthermore, the licensees have recently demonstrated that the availability and operation of the Special Safety Systems will not be challenged by such systems as the online refuelling systems and the reactor regulating systems.

The licensees must now complete the Y2K remediation of all other assets that are necessary for the operation and maintenance of the reactor systems by June 30, 1999. The expected configuration is one which the plants and their operating staff will be ready to move into the year 2000. This will leave the rest of 1999 for plant staff to become familiar with new changes, new procedures, and contingency plans. The expectation of the AECB is that the nuclear power plants shall operate through the date transition as a normal “non-event”.

---

**October 1, 1998:**
All Special Safety Systems have been examined, corrected, tested, and declared as year 2000 ready. This will leave three months before the systems go into the year 1999.

**December 31, 1998:**
All reviews and corrective actions to be in place for those other control systems which, while not special safety systems, are nevertheless important and whose failure could challenge the Special Safety Systems.

**June 30, 1999:**

- All reviews, corrective actions or acceptable work-arounds are in place for those other systems, components and software toolsets, whose failure is not expected to directly affect the safety systems in carrying out their safety functions, but which, nevertheless, could impede the safe operation of the plant.

- The licensee is to provide assurances to the AECB that their Nuclear Power Plants are Year 2000 ready. The assurances should confirm that all necessary changes have been installed and tested, contingency plans are in place and that all adequate work-arounds and administrative changes are implemented and documented.

- The licensee is to disclose to the AECB the following:
  I. Any Y2K circumstances that has not been resolved and could potentially place the plant in a condition not previously analysed;
  II. Any work around to overcome such circumstances.
The licensees must show that their systems meet their defined specifications.

Inventory of non-compliant assets prioritized and based on the safety significance of the systems. List must include systems that directly and indirectly contribute to plant risk should they fail. List must also include embedded software and offline systems.

Risk assessment of all Y2K related failure modes and their impact on plant safety.

Modifications tested to ensure none of the original functionality of the systems are impaired and no new failure modes are introduced.

Contingency plans to overcome problems should systems not function as expected during the year 2000 date transition.

Confirm by June 30, 1999 all necessary changes have been installed & tested, contingency plans in place and all adequate work-arounds and administrative changes are implemented and documented.

By June 30, 1999 disclosure of any unresolved Y2K circumstance that could potentially place the plant in a condition not previously analyzed and any work-around to overcome such circumstances.

No unreasonable risk to public. No degradation in the capability of SSS.
If the licensee has not provided adequate assurances that remainder of their facilities are Y2K ready or has not provided adequate disclosure by June 30, 1999, licensing action may be necessary to see that there is no unreasonable risk to the public.

The AECB’s effort with respect to Y2K as previously detailed is considered to be Phase I of the project. The AECB is now in Phase II of the Y2K project. Phase II will enlarge the scope of our review to include the suppliers of embedded systems, programmable controllers, and other potentially date sensitive equipment. This will allow the AECB to acquire solid confidence, through independent confirmation, that the licensees are on track to achieve our primary objectives:

• operation into the new year shall not result in any safety related transients;
• the licensees shall not invalidate the requirements of the Atomic Energy Control Act and regulations;
• the licensees shall not violate any license condition or assumptions made in the licensing basis.

The AECB’s involvement in the power reactor Y2K project will continue into the year 2000. Phase III of this project will allow the AECB to assess the successful completion of the Y2K project and to perform a post mortem study to determine if there are lessons to be learned that will improve our ability to face any future challenges to safety.

Y2K Experience - Lessons Learned

As part of the demonstration phase, the AECB requested that the licensee walkthrough the processes used to ensure the readiness of digital assets for specific systems. These walkthroughs were used as a method to selectively ensure that the licensees were following their procedures correctly. The systems and components selected by AECB staff were demonstrated on site by the people who actually performed the work. These walkthroughs consisted of:

• description of the system and digital asset
• diagrams indicating boundaries and information flow
• investigation process (key word searches)
• identification of non-compliance
• method of correction
• testing strategy
• conclusions

The AECB expected to receive certification that each digital asset was investigated and all corrective actions have been taken and testing performed to make it Y2K ready. On the milestone dates, the licensees provided certification of the digital assets required to be “Y2K ready”.

We subsequently found that the terminology used with respect to describing Y2K status was not universal. For instance, the term “Y2K ready” was used extensively by both the AECB and the
licensees, however, each interpreted it differently. Terminology used throughout the world for Y2K status like “Y2K Ready”, “Y2K compliant”, and “Y2K certified” are not consistent.

Overall, there have been few surprises found in the assessment of digital assets at all of the plants. There has not been a single occurrence where a Y2K problem would have prevented a Special Safety System from performing its safety function.

In general most digital assets are not date aware. Some digital assets have internal clocks but are generally used as time counters that are continuously reset and are not aware of the date and time of day. We have found that Chameleon controllers have real time clocks which do track the day, month, and year but the selection of the year is arbitrary. Some were set at year zero when they were installed and now read year 8 or 10 and some were set at the current date when they were installed. If these were allowed to reach the millennium without repairs, the time would revert back to zero. Nevertheless, for these type of controllers, the licensees are proposing that the year will be rolled back to prevent them from experiencing such a change.

During one of the on-site walkthroughs, it was discovered that maintenance staff had developed a means of using a PC to load a calibration program for the off-line calibration of the PROM boards for the shutdown systems programmable digital comparators (PDCs). This PC was a 286 and definitely not Y2K compliant creating a concern about mis-calibrating a PROM board with corrupted data. This non-compliant PC was replaced by one which was Y2K compatible.

Demonstrations have shown that the digital control computers are date aware and there is a means of inputting the date into the computer via a keyboard. This device has been the most thoroughly examined of all of the digital assets at all of the plants and was considered the most likely system to experience problems as the programs were in generally written 1960s and 1970s. The AECB requested demonstrations and walkthroughs on the digital control computers from each of the licensees. In general the control programs were not adversely affected by any date transition. However, the date transition has been shown to cause erroneous date indications on alarm printouts and CRT alarm listings which are important to the running of the plant. In all cases, date dependencies were checked and corrections were made if they were found to be non-compliant. The digital control computers were then tested using an extra non-operational workstation available at each plant and then tested on the plant simulators.

Our investigation challenged conventional thinking on Y2K dependencies. We commonly requested arguments for the assumptions made and ensured that they were based on sound scientific knowledge and engineering principles. The licensees were requested to provide complete and accurate documentation showing all places where date-dependent information flows within and between digital systems. However, for systems that were developed decades earlier, it is not always easy to produce such essential documents.

**Contingency Planning**

Part of the AECB’s process for Y2K is to ensure that the licensee has plans to adequately compensate for unforeseen failures. In addition to insisting on an open and auditable Y2K review
process, we have required our licensees to present contingency plans. Our approach is to ensure that these plans include equipment and dependencies that, while not critical to safe and continued operation in the short term, long-term failures could reduce safety margins (eg. long-term unavailability of a wiring data-based program, communications).

Contingency planning is the attempt to ascertain the problems that are most likely to occur and preparations to deal with them. Typically based on risks deemed unacceptable or which require significant mitigation measures, the overall purpose of contingency planning is to recognize and address as many uncertainties and risks as possible so that plants can maintain control over their operations if a crisis strikes.

The contingency plans must take into account that the Y2K problem must be viewed as a potential "common cause of failure" leading to simultaneous failures in several systems. We have to review contingency plans for Y2K based events that may have some impact on safety. Since early 1998, discussions have been held with our licensees. We require them to prepare contingency plans by June 30, 1999. These plans must be constructed with two major areas in mind, risk identification and risk mitigation.

Risk identification and assessment will provide an insight to the possible safety concerns associated with the external risks. Close co-ordination has to occur between the utilities and their external dependencies such as the suppliers of fuel for the standby generators. Emphasis is placed on the external risks as the licensees do not have direct control over the external dependencies. The assessment should be able to provide as a minimum a description of the safety concerns such as severity of the safety concern and the likelihood of it happening based on knowledge, experience, expert judgement, etc.

Since Y2K is a new challenge, we are constantly developing a better understanding of it. For that reason, we believe that the emphasis in the development of contingency plans should not be placed on perceived probability of an event but rather the risk to safety.

Risk mitigation requires the licensees to perform and document the measures (technical, operational, maintenance) that have been and will be implemented to reduce the risk factor, and provide the rational behind the measures. Subsequently, a risk rating should be constructed after the corrective measures have been implemented. This should highlight any residual risk to safety present after all the corrective measures have been implemented. The AECB considers the importance of training for the successful execution of contingency plans and thus the licensee will have to show that training is part of the implementation process.

As a regulator, we need to develop contingency plans of our own. Our strategy is no different than what we require from our licensees: the contingency plan must contain risk identification and risk management. To perform our regulatory function during an emergency, we need to identify risks such as failure of power or failure of communications and make adequate preparations and contingency plans so that the residual risk to operation availability is a low as reasonably achievable.
Conclusion

We have passed two major milestone dates. To date our licensees have shown, that no serious problems have been found that would initiate an internal transient and if a problem did occur, the systems required for mitigation would remain functional.

The next milestone is June 30 at which time all Y2K issues internal to the plant will be resolved and the project will focus on contingency planning for the year 2000. The work is not yet finished and much remains to be done; but, based on our findings and that of our licensees, our expectations are that the transition into the new millennium will be business as usual.