C-98—RELIABILITY OF SYSTEMS IMPORTANT TO SAFETY IN A NUCLEAR FACILITY

Philippe P. Hessel
Atomic Energy Control Board, Canada

ABSTRACT

Reliability targets, requiring that the risk from a nuclear power plant be less than that from other hazardous industrial activities, were set from the beginning of the nuclear era in Canada, [1]. Since demonstrating that a plant meets these requirements with the then available techniques was not possible, the AECB progressively introduced unavailability requirements for the Special Safety Systems (Shutdown, Emergency Core Cooling and Containment). Nevertheless, checking that the plant design was really was still not possible "balanced", i.e., that the different system designs and monitoring were commensurate with their contribution to plant safety was not possible.

The development of new methods and enhanced computing power has led to the generation of comprehensive reliability models for the Special Safety Systems and to the development of PSAs.

This document, C-98, has taken this progress in consideration. As a result, the new AECB policy requires that the licensees identify every system important for safety, determine its failure and success criteria, and that should be a reliability target set, monitored and maintained, commensurate with the contribution of the system to plant safety. Reporting the results is a part of that policy.

INTRODUCTION

NRX, was the first Canadian nuclear reactor. In 1952, it experienced a severe accident, leading to fuel damage. Further investigation showed that the accident was mainly due to the non separation between process and safety systems: A failure of one of the command systems disabled several safety systems. This accident led the AECB to require the following principles for the design of safety systems:

They must be simple,

They must be independent from the process systems,

They must be testable and periodically tested.

However, in these "pioneer ages," the risk due to radiations was not yet clearly identified and these requirements addressed mainly the notion that we should always avoid an accident.

THE FIRST SAFETY REQUIREMENTS

One had to wait till 1957 for the development of "real" safety requirements for nuclear reactors. It was then proposed by the AECB that the risk due to a nuclear reactor should not be higher than due to the other means for power production (i.e., coal, oil or hydro). This idea was applied with the first nuclear power plants. It was officially presented in June 1962 by G.C Lawrence, then president of the AECB, at the Washington Nuclear Congress (Reliability Requirements for Nuclear Power Station): "The risk due to the operation of a nuclear power plant must be lower to that due to other hazardous industries. The probability of a severe accident must be lower than 10^{-5} per annum." AECB 1010 made this target enforceable.

However, no means were available at the time to check conformance to the target. The complexity of nuclear plant was such that manual methods were not able to model the reliability of the whole plant. The AECB therefore developed a deterministic approach to reactor safety and required that deterministic criteria be met (e.g., single and dual failure criteria).

AECL then developed the "Safety Design Matrices" method to check the dual failure criterion.

During the 70's, the AECB issued several regulatory documents defining the requirements for the process systems and the Special Safety Systems (shutdown system, emergency core cooling system and containment).

- The frequency of Serious Process failures must be lower than one every three years.
- Special Safety Systems must show a probability of not meeting their design intent lower than 0.1% when required to do so.
- Periodic testing results must prove compliance with this requirement.

To be readily measurable, the requirement was expressed as follows: "The system must be designed and operated such that its unavailability period is less that 10^{-3} year per year."

The weakness of this method is that it does not allow to assess the impact of failures on the probability of meeting the design intent when required to do so. Also, one could interpret it as "the AECB allows the licensee to operate a plant without any safety system eight hours each year…" To alleviate these concerns, the licensees developed a classification of events according to their qualitative impact.

LIMITATIONS OF THE RESULTING POLICY

This regulatory approach, which relies on the protection given by the safety systems, was effective, since no severe accident has occurred in Canada.

It has, however, the following limitations:

- The predicted and measured availability are that of every system, considered as independent from the others. However, none of these systems is really independent. They need resources (power, water, compressed air, and so on) the failure of which is not considered when assessing the conformance to the requirements.
- Correlating the systems unavailability with the duration of events leading to their impairment, even using qualitative criteria, gives little information on the real degradation of the systems' performance. Assessing the criticality of the event is up to the AECB Project Officer. Some events can last long and be considered as non important. The AECB report would then state that system X was unavailable during 5400 hours last year (against a target of eight hours) and that this situation "needs improvement," but neither justifies a shutdown of the plant nor a revocation of the operating licence. We are in the situation where the licensee is formally at fault but where the AECB officers, have judged that the event is minor and do not object to plant operation.
- Accidents could occur even with all Special Safety Systems available, as shown by the present PSAs (DPSE for Darlington and PARA for Pickering A.) The main causes of accidents are these systems for which no reliability requirements exist.

THE BASIC IDEA OF C-98

C-98 tries to answer the following questions:

- What is important from a safety view point?
- Are the AECB resources focused where they are the most effective?
- Does the AECB focus its attention on the real safety issues?
- Is the AECB more demanding on issues that contribute for little to safety than on others that are high contributors to risk?

Present risk assessment tools can answer these questions. Why not use them …

The basic idea is that most of a nuclear plant systems contribute, in a way or another, to the plant safety. Some are designed to prevent accidents. Some have to mitigate any failure of the former ones and to keep the plant in a safe status. Others have to reduce the consequences of accidents. All of them are "important to safety" and must be included in the regulatory process. Thus all of them should have, like the Special Safety Systems, reliability and surveillance requirements. These requirements should be, of course, commensurate with the contribution of every system to the plant's safety. This requires that the importance of each system be identified, qualitatively as well as quantitatively, and that its failure criteria be defined. This process must be organized and audit able, thus the need for a reliability program and reporting requirements.

DEVELOPING C-98

The development of C-98 was different from that of the traditional regulatory documents. We have consulted licensees during the drafting phase. They have thus contributed to the setting up of the document before its release for public comments. The end of the drafting phase coincided with the release for public comments of R-99 "Reporting requirements for Nuclear Power Plants." That is why the section of R-99 on Reliability Reporting is strongly related to C-98 philosophy and specifications.

When she became President of the AECB, Dr Agnes Bishop noted that the Regulatory Documents system was not satisfactory, leading, for instance, to inconsistencies between documents, as and their content and application. She required a complete redesign of the regulatory documents and stopped any new publication as of January 1995. C-98 was the first document affected.

In 1996, AECL requested the AECB to conduct a preliminary assessment of the licence ability of its CANDU-9 design. C-98 was among the documents taken into account for this assessment. AECL comments on the practical application of C-98 highlighted some weaknesses, in particular a shift between the writer's intents and the strict application of the text. We noted and considered these comments for the rework of C-98.

The project on the new Regulatory Documents system is now finished: Regulatory documents are defined by their goal and the consequences of a noncompliance. Are so defined General Regulations, whose noncompliance leads to the Courts, AECB policy, AECB standards, AECB guides, and informative documents.

Thus, we have completely redesigned C-98 and issued three documents:

- P-98, stating the AECB policy on systems important to safety,
- S-98, stating what the AECB requires from the licensees,
- G-98, giving what the AECB expects from the licensees to show compliance with S-98.

P-98 AECB POLICY STATEMENT

A Regulatory Policy is a regulatory guidance document that describes the philosophy, principles or fundamental factors that the AECB uses to direct the actions of AECB staff and guide the conduct of persons subject to regulatory requirements, as well as others who interact with the Board's regulatory process.

The goal of this policy is to make sure that every system important to the safety of a nuclear power plant is reliable enough for meeting the safety goal of the plant. One has to note that definition of the safety goal is out of the scope of that policy.

To meet this goal, the AECB expects the licensees to set up a reliability program aiming at:

- Identifying these systems important to safety and defining safety targets apportioned to the plant safety goal,
- Assessing the reliability of every system important to safety to ensure that they are designed, built, operated and maintained to meet their targets,
- Maintaining the reliability of systems important to safety throughout the life of the plant.

Systems important to safety are these systems (including their components, structures and the associated procedures) which, when not meeting their intent, contribute to a radiological risk to the public.

P-98 requires from the AECB staff to make sure that the reliability program includes, at least:

- Identification of those systems important to safety,
- Allocating reliability targets,
- Preparation and maintenance of reliability assessments,
- Preparation of test, surveillance and maintenance procedures,
- Follow-up of the systems' reliability performances,
- Follow-up of components reliability,
- Reporting on reliability performances of the systems and components.

S-98 AECB STANDARD

A Regulatory Standard is a regulatory guidance document that describes detailed specifications, criteria or actions that can be objectively measured, are acceptable to the AECB as meeting regulatory requirement and are suitable for incorporation into AECB licences. According to the general AECB regulatory philosophy, the methods and procedures used to prove compliance are the responsibilities of the licensee.

S-98 states what are the issues that are mandatory in a reliability program. It develops what shall be the attributes and scope of the reliability program and the associated activities.

G-98 AECB GUIDE

A Regulatory Guide is a regulatory guidance document that describes criteria or actions that the AECB accepts and recommends as meeting regulatory requirements, but are not suitable for incorporation into AECB licences. The AECB can state preferred methods, but the licensee is free to use other methods, with the burden of proof that they are appropriate and validated.

G-98 is the document that describes the very intent of the AECB on systems important to safety. It explains what should be the scope of the actions, what methods are recommended, how thorough the actions should be, and what efforts should be allocated to meet the regulatory requirements.

We will only point out the major issues of G-98:

- A PSA is expected as the best way to assess the importance of every system to plant safety. However, a PSA is not yet required by the AECB. If no plant specific PSA is available, G-98 suggests an acceptable way of qualitatively assessing the importance of systems. When a PSA is available, G-98 recommends use of importance indices (Fussel-Vessely, RAW and RRW) to rank the systems.
- The efforts and resources to be allocated to a system should be in proportion to the contribution of the system to the plant's risk.
- For operating plants, the AECB does not intend to set safety targets. Reliability targets should be derived from the result of the plant PSA. If no PSA is available, then other methods can be accepted.
- Testing frequency, surveillance activities, maintenance procedures should be derived from the reliability analysis: Testing frequency should be such that the reliability targets are met. Surveillance must address the failure modes that can be so detected. Maintenance procedures should be such that every failure mode identified in the reliability assessment is addressed.
- The result of testing and maintenance activities should be used to update the reliability assessment. For instance, discovery of failure modes that are not modelled in the reliability assessment should result in a modification of the reliability model.
- Feeding the real events in the reliability model (and in the PSA if available) would give information to the plant operators on the importance of the event. It would be a useful information for planning the repairs.
- Monitoring reliability performance of the systems should allow assessing the effectiveness of maintenance, and detecting drifts in the failure frequencies. In that way, G-98 addresses the management of ageing.
- An effective monitoring and updating program supposes a sound configuration management program.
- Monitoring components reliability should result in more realistic and meaningful reliability assessments and PSA.
- G-98 also describes what reporting methods and data (required by R-99 [5]) would be the most informative and significant.

CONCLUSION

Introduction of P-98, S-98 and G-98 in the Canadian regulatory system marks an important step in the regulatory process.

The various requirements of S-98 address several issues that were not well controlled in the past.

Management of ageing has been for long a concern for the AECB, but no common ground has been found with the licensees after several years. Binding management of ageing with reliability assessing and monitoring gives a sound basis for regulatory enforcement.

The -98 sets also sets the basis for regulatory requirements and monitoring of maintenance definition and effectiveness.

ACKNOWLEDGEMENT

MM Ken Lafrenière and Tom Schaubel, from the AECB Reliability and Risk Assessment section, have been instrumental in the preparation of the -98 set.

REFERENCES

1. G.C. Lawrence, “Reliability Requirement for Nuclear Power Stations,” Nuclear Congress, New York, June 1962. (Also AECB 1010).
2. P-98, “Regulatory Policy - Reliability of Systems Important to Safety for Nuclear Reactor Facilities,” Issue for public comments. Fall 1997.
3. S-98, “Regulatory Standard - Reliability of Systems Important to Safety for Nuclear Reactor Facilities,” Issue for public comments. Fall 1997.
4. G-98, “Regulatory Guide - Reliability of Systems Important to Safety for Nuclear Reactor Facilities,” Issue for public comments. Fall 1997.
5. R-99, “Reporting Requirements for Operating Nuclear Power Facilities,” January 1, 1995.

KEY WORDS

Reliability, Nuclear Reactor, Systems, Policy, Maintenance, Test, Reporting.