THE NUCLEAR REGULATORY PROCESS IN CANADA EXPERIENCE AND POSSIBLE FUTURE DIRECTION

John D. Sainsbury - AECL/CO
Sheridan Park Research Community
Mississauga, Ont. Canada, L5K 1B2
416-823-9040

ABSTRACT

The underlying principle in the Canadian licensing process is that the licensee (owner/operator) bears the responsibility for safety while the regulatory authority sets safety objectives and audits their achievement. As a consequence, Canadian Regulatory Requirements emphasize numerical safety goals, and minimize specific design or operational rules.

This paper traces the evolution of this approach, and indicates direction for the future.

1. EVOLUTION OF A SAFETY PHILOSOPHY

Nuclear safety thinking in Canada was stimulated by the accident in the NRX research reactor in 1952. NRX was the first major experimental reactor at the Chalk River Nuclear Laboratories (CRNL). It was a heavy water moderated, light water cooled, natural uranium core, with fuel rods in vertical coolant tubes. The shutdown system was a designated part of the control rod system; in other words, there was no separation between the control and shutdown systems. In any such system (as in Chernobyl) the capability of the shutdown function is depended on the operating state of the reactor. In December of 1952, this lack of tolerance to operating state, combined with an operator error and mechanical fault, led to a power transient which failed fuel and released fission products. The accident was a psychological blow to the embryonic program and several senior technical staff at the laboratory thought hard about the lessons to be learned if there was going to be a successful power reactor program.

Dr. G.C. Laurence, who later became chairman of the Reactor Safety Advisory Committee (RSAC), was the first to clearly state the following safety design principles:

i) Process system (like control) and safety systems (like shutdown) must be independent of each other.

ii) Safety systems must be independent of each other and testable.

iii) Nuclear operators should be given an audit role thereby unloading them of the repetitive control tasks that lead to boredom and complacency.

These principles were applied in the CANDU prototype station (NPD) which started operating in 1962 and have become the foundation for the safety concepts of all subsequent CANDU plants.

When the Atomic Energy Control Board (AECB) appointed Dr. Laurence chairman of the RSAC in 1956, he developed the safety design principles into criteria to be used for licensing nuclear power plants[1]. The underlying objective was that the risk from nuclear power plants be lower than from alternative sources of electrical energy.

These criteria, last modified in 1972, set limits on the frequency of process failures and on the reliability of the safety systems[2]. They further state maximum values for the calculated radiation dose to the public for any process failure (single failure) and for any combination of a process failure and the unavailability of a safety system (dual failure). The dose limits are shown in Table 1. We also have public dose limits for normal operation which are essentially the same as those recommended by the International Commission on Radiological Protection, namely:

individual dose limits	5mSv/a	whole body
	30mSv/a	thyroid
population dose limits	100Sv/a	whole body
	00Sv/a	thyroid

Table 1. Operating Dose Limits and Reference Dose Limits for Accident Conditions

Situation	Assumed Maximum Frequency	Maximum Individual Dose Limits, mSv	Maximum Total Population Dose Limits, Sv
Normal Operation		5/a , whole body 30/a , thyroid	100/a , whole body 100/a , thyroid
Process Equipment Failure (single failure)	1 per 3 a	5, whole body 30, thyroid	100, whole body 100, thyroid
Process Equipment Failure plus failure of any safety system (dual failure)	1 per 3×10^{3} a	250, whole body 2500, thyroid	10^{4}, whole body 10^{4}, thyroid

The single process failure has a dose limit equal to the yearly operational limit and the dual failure has a limit about 100 times higher.

A corollary of this approach to safety is that the safety systems must be sufficiently separate and independent of the process systems and of each other that the likelihood of a cross-linked failure will be less than the likelihood of a dual failure.

This risk-based approach to reactor safety and licensing was developed in the early 60s and is still applied to current plants in Canada. This licensing approach requires the analysis of accidents assuming the impairment of any safety system. In particular, we assume that an entire shutdown system is unavailable. This analysis of power increases for which shutdown is not credited is difficult but has been done in the past. On recent plants, a second independent shutdown system has been added. This system is different in concept (liquid poison rather than rods) from the first system providing not only redundancy but diversity in our shutdown capability. At this level of protection, there is no practical purpose in analyzing reactor power increases without shutdown, nor is it required.

2. LICENSING PROCESS

The legislative foundation for the Canadian nuclear industry is the Atomic Energy Control Act, last amended in 1954; this act gave the mandate for research and promotion to a government-owned company, Atomic Energy of Canada Limited (AECL) and the mandate for regulation of the industry to the Atomic Energy Control Board (AECB).

The AECB has issued only procedural regulations leaving specific requirements to be imposed through the licensing process. It is only in the last few years that regulatory guides dealing with design of safety systems have been drafted - for most of our nuclear history in Canada we have licensed without detailed written requirements. It has often been stated that this is possible because we only have one nuclear vendor (AECL). Although a simple structure of nuclear industries has helped, the real reason we license without a lot of written requirements is a regulatory attitude or principle - the licensee is responsible for safety while the regulatory authority sets safety objectives and audits their achievement. This is a fundamentally different approach from that which is based on detailed rule making. It forces the licensee to understand the basic safety objectives and to strive for excellence during design, construction and operation. It can accommodate innovation and improvement rather than discouraging it with rigid rules. And finally, most important to a country wishing to develop an indigenous regulatory process, it can be applied to reactors of any type.

The Atomic Energy Control Act does not require public hearings and, to date, the AECB has not held a hearing for any aspect of its regulatory process. Licensing documents such as applications for licences, supporting documents, staff recommendations, and board decisions are available in a public reading room.

Although the regulations call for only two formal steps (construction approval and operating licence), in practice the process involves a prior step of site acceptance and many intermediate substeps. The licensing process is described in detail in Ref. 3.

2.1 Site Acceptance

The basic objectives at the site acceptance stage are to describe the conceptual design of the facility and to show that it is feasible to design, construct, and operate the facility on the proposed site in a way which meets the safety objectives of the AECB. The primary documentation required is a Site Evaluation Report providing a summary description of the proposed station and information on land use, present and predicted population, principal sources and movement of water, water usage, meteorology, seismology, and local geology.

During this phase the utility announces publicly its intentions to construct the facility and holds information meetings at which the public can express its views and question utility officials.

2.2 Construction Approval

Before granting construction approval, the AECB must be assured that the design will meet the safety objectives and that the plant will be built to appropriate quality standards. To do this, the design must be sufficiently advanced to enable preliminary safety analyses. The primary documentation required includes a Preliminary Safety Report (which combines the essential information of the Site Evaluation Report, a description of the reference design, and the preliminary safety analyses), an overall QA program for the project together with a specific program for construction QA and preliminary plans for operation.

2.3 Operating Licence

Before issuing an operating licence, the AECB must be assured that the constructed plant conforms to the approved design and that the plans for operation are satisfactory. The requirements include submission of a Final Safety Report, completion of a previously approved commissioning program, examination and authorization of senior personnel, approval of operating policies and principles, preparation of plans for dealing with radiation emergencies, and a specific program for operations QA.

Typically a provisional licence is issued to permit startup, and subject to AECB staff approval, increases in power to the design rating. A full operating licence is issued for a period not exceeding 5 years. Among the terms of an operating licence is the requirement that the licensee inform the AECB promptly of any occurrence or situation that could alter the safety of the plant.

Although the primary responsibility for the safe operation of the plant remains with the licensee, there is continued surveillance by the resident AECB inspectors, annual reviews of operation, and major reviews when the operating licence is renewed.

3. THE FUTURE

Currently the AECB is re-drafting the regulations primarily to formalize what has been common practice for many years. For instance, site approval will become a formal first step in the licensing process; the AECB will take on responsibility at the federal level for environmental control at nuclear sites; and there will be a formal approval of the design of components which are manufactured before issue of a construction licence. However the most significant change in the future will be in the licensing process. This new process has been developed jointly by the designer (AECL) and the regulator (AECB). We call it up-front licensing.

3.1 Reasons for Change

The Canadian plants started in the early 70s obtained construction permits with only a conceptual design in place. This was possible because these plants were very similar to previous plants and because there was respect and trust between the regulator, utility, and designer.

This did mean however that detailed design and analysis was going on in parallel with construction. In this situation, the construction schedule is vulnerable to design change and changes in licensing requirements—and both happened.

One of the largest changes initiated by the designer was from a low pressure to a high pressure emergency core cooling (ECC) system. When the construction licence was

issued for Gentilly-2 (a 600 MWe plant in the province of Quebec) the ECC system involved low head pumps drawing water from the dousing tank at the top of the reactor building and pumping it through the reactor core (Fig. 1A). In the mid 70s we made a major step forward in sophistication of our loss-of-coolant analysis codes. The new codes permitted analysis over the whole range of potential pipe break sizes and identified the possibility of small breaks which stagnate the coolant flow in the core.

These analyses led to a redesign of the ECC to a high pressure system using water accumulators pressurized from a gas tank (Fig. 1B). Once the high pressure tanks are emptied the system reverts to pumping from the dousing tank (as in the original system) for long term cooling. This change to a major safety system, coming midway through construction of the plant, led in turn to much more rigorous accident analysis, sensitivity analysis, questioning of assumptions, and demand for more experimental verification of analysis methods.

The other major change that came midway through construction of the 600MWe plants was caused by several forces - felt not only in Canada but throughout the western world. This was the period when the importance of designing for earthquakes was realized and also external events such as plane crashes were postulated as design basis events. Our response in Canada to these events was to provide additional power and water systems, qualified for earthquakes and located away from the conventional systems. All the safety systems were designated into two groups (each group capable of providing shutdown, core cooling, and monitoring after an accident) and the cabling and wiring for each group separated.

A second seismically qualified control area was provided, again well-separated from the main control room. These were major changes and had an effect on construction schedule. They also gave the regulatory staff new systems and analysis to review late in the project schedule.

Another type of problem was repetition of safety analysis. Much of the safety analysis was completed within the first few years of the project. Code development and associated experimental programs are continuous, and within a few years had produced better analytical tools. Although spot checks indicated no significant change

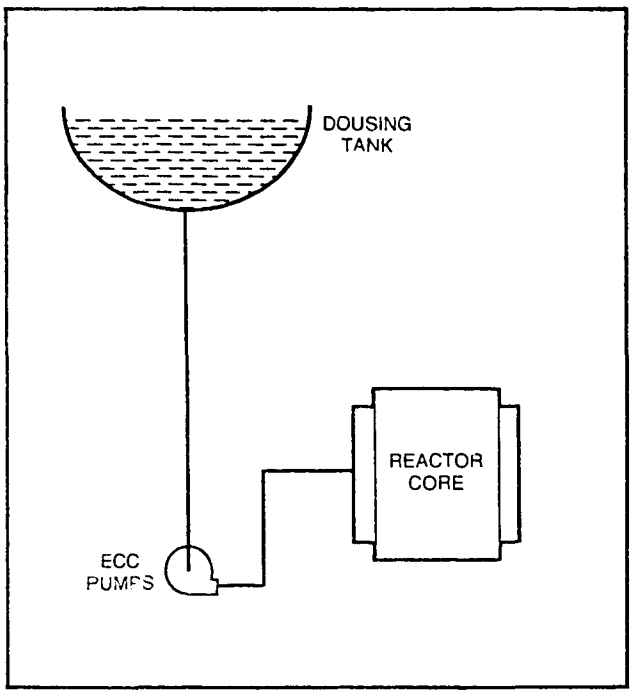

FIGURE 1A ORIGINAL LOW PRESSURE ECC SYSTEM

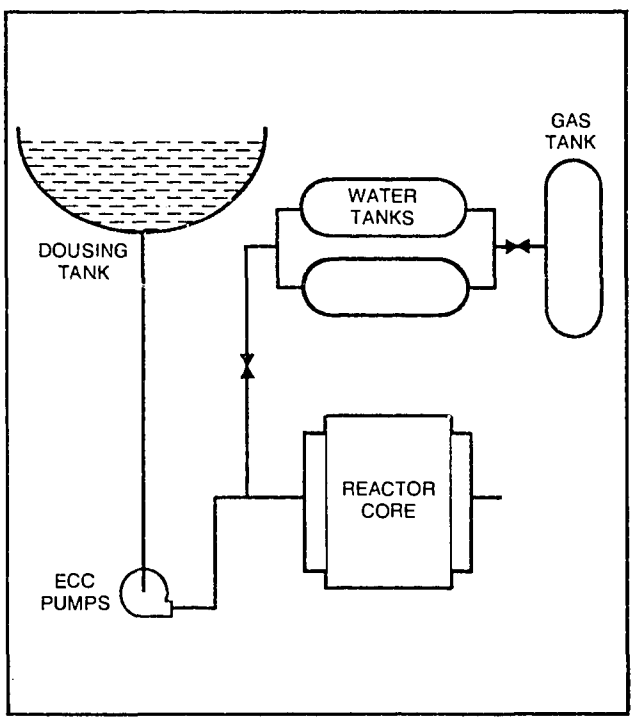

FIGURE 1B NEW HIGH PRESSURE ECC SYSTEM

using these better tools, the designer was requested to repeat a large fraction of the safety analysis within the last few years of the project. (This request may have come from a sensitivity created by the earlier ECC experience.) This request put a heavy work load on both the designer (during analysis) and the regulator (reviewing analysis) late in the project.

These are the major examples of problems which caused dissatisfaction with the licensing process on both sides. There was a common desire to find a better way for the future.

3.2 Up-front Licensing

The idea that has been developed over the last 4 years is to move all negotiation and agreements on licensing issues from the tail end of the project to the front end (Fig 2). In the future we will clearly define the design of major systems, code requirements to be applied, analysis methods and criteria etc., by the time of construction approval. A large fraction of the detail design and safety analysis will have to be done by this time. Ideally (no surprises) the analysis would be completed early in the construction phase and an operating licence would be issued when required without last minute disputes.

Both sides are giving up some freedoms in this approach; the designer must do a lot of engineering before construction starts and freeze the design, while the regulatory must freeze the licensing requirements. The current feeling is that the gains are worth the loss of freedom. The process of course needs a way to deal with surprise events. A TMI, Chernobyl, or major surprise from experiments will put a hold on the agreements until the significance to the project is evaluated. It is essential that there be a meaningful test of significance before a surprise event takes the project off on a different course - without this the process will degenerate to the old process that no one wants.

Over the last 4 years we have put a lot of effort into engineering our plants for faster construction because every month off the construction schedule is a saving of about $15M in financing costs. Shortening the schedule is accomplished by fabricating systems modules outside the reactor building and lifting into an open-topped building with a very heavy lift crane. We expect to build future CANDU 600 plants (limited use

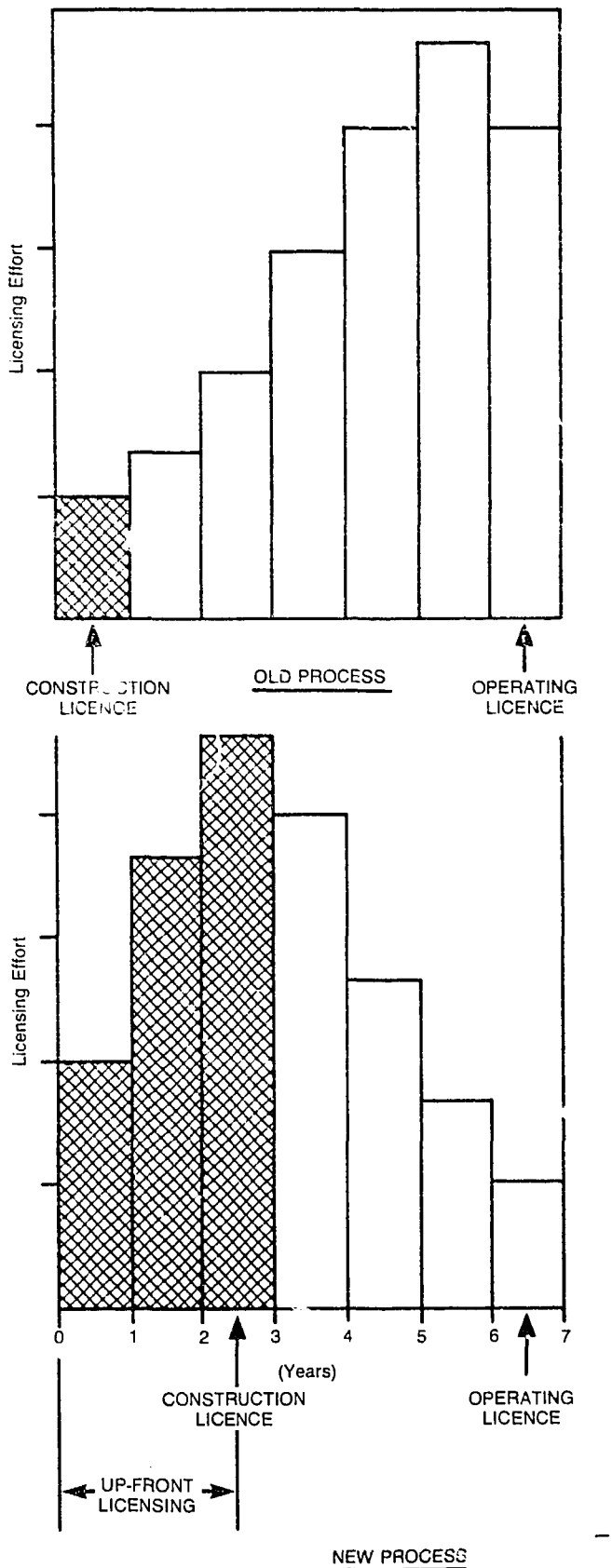

FIGURE 2

of modules) in 55 months and our CANDU 300 (extensive use of modules) in 42 months. These estimates are from first concrete to in-service. However, these short schedules demand that 30 to 40% of the engineering be complete before construction begins. Therefore our two initiatives - shorter construction time and up-front licensing are compatible; both require a shift of engineering and analysis to the early phase of a project.

4. CONCLUSION

The underlying principle in the Canadian licensing process is that the licensee (owner/operator) has the responsibility for safety, while the regulatory authority primarily sets safety objectives and audits their achievement. As a consequence, Canadian regulatory requirements emphasize numerical safety goals and minimize specific design or operating rules. The process is therefore generic and can be applied to any reactor type.

In the future we will be using an up-front licensing process which shifts licensing activities and negotiations to the early phase of a project. This is to minimize risks of licensing affecting construction schedules. This approach is compatible with the designer's desire to shorten construction schedules; both require that a significant fraction of engineering and analysis be complete before construction begins.

REFERENCES

1. G.C. Laurence, "Reactor Siting Criteria and Practice in Canada", ANS topical Mtg. on Nuclear Power Reactor Siting, Los Angeles, Feb. 18, 1965.

2. D.G. Hurst, and F.C. Boyd, "Reactor Licensing and Safety Requirements", AECB-1059, Atomic Energy Control Board, June 11, 1972.

3. M. Joyce, "The Licensing Process for Nuclear Power Reactors", AECB-1139/Rev.1, Atomic Energy Control Board, Nov. 21, 1979.