NUCLEAR SAFETY AND RELIABILITY

WEEK 11

TABLE OF CONTENTS - WEEK 11

1. Safety Goals

It is obvious that both the public and the operating staff must be protected against the harmful effects of ionizing radiation. These are the first two goals of nuclear safety. The third goal is of a different kind and is not often recognized; it is protection of the plant against damage.

Plant protection is a useful safety goal for an operating utility because it leads directly to a more definite set of operating rules which can be seen to be in the utility's interest. While the regulatory rules defined by the AECB may satisfy the first two safety goals, they are externally imposed and so often draw negative reactions from utility staff and management. The third goal obviously contributes directly to achievement of the first two, but is internal, and so can act as a more positive force. This goal has not, as far as I know, been implemented explicitly at any nuclear utility. Many of the day to day actions are, however, based implicitly on plant protection principles. Unfortunately these ideas rarely extend to consideration of accident conditions.

The principles of plant protection were developed as part of the Darlington Probabilistic Safety Evaluation (DPSE), following the ideas presented by Chauncey Starr (Nuclear Safety 23,1, 1982). Ernie Siddall (AECL-7404, 1981) also has developed a rationale on which a

quantitative set of safety goals can be based - it is less direct than the simple "economic loss" criterion used in DPSE but much more general in application. Siddall argues that a limited quantity of money is available for use in enhancing safety; it follows (as a familiar utilitarian goal) that safety money should be allocated by the society so as to achieve the maximum health protection per dollar. On this basis he concludes that nuclear plant safety systems installed to meet the first two safety goals go well beyond the optimum allocation of resources. He does not address the third goal.

2. Economics of Safety

Starr presents an argument for plant protection goals based on the Rasmussen study, the USNRC draft safety goals, and the record of outage frequency and length for US light water reactors. Based on this analysis the average LWR owner in the US faces a financial risk exposure of $20 million per year simply by operating a nuclear plant. The results are summarized in Table 11.1.

Table 11.1 – Utility Risks vs Public Risks

This table assumes accident probabilities and consequences from WASH 1400, life value of $1,000,000, and outage rates and durations from US LWR data.

EXPECTED VALUE PER REACTOR YEAR

PUBLIC	
Early Fatalities	$150
Latent Fatalities	$700
Property Damage	$40,000
UTILITY	
With $300,000,000 Insurance	$3,000,000
No Insurance	$24,000,000

By comparison with the public risk exposure, the financial risk is much larger. Given the fact that the public risk figures are based on extremely pessimistic health effect estimates for major accidents, the dominance of financial risk is likely even greater than that indicated. The CANDU financial risk exposure is quite different, - as indicated in the DPSE summary report (handed out in class).

3. Distinction between licensing and achievement of safety goals

In the literature, the word "safety" is often used synonymously with the rules and regulations that are defined for the purpose of licensing the plant for operation. It is presumed that, provided all these rules are followed and equipment is in working order, the plant will be "safe". In reality a distinction needs to be made. If we assume that none of these rules act

contrary to the interest of safety in operation - a very real possibility in the real world - then they must be considered as a necessary but not sufficient set. Even this assumption is not a very safe one, because it presumes that the people who defined the rules and who designed the plant and procedures to satisfy the rules had a perfect understanding of the plant's characteristics and of the way in which the plant should be operated to achieve safety. The other reason for continued questioning of these rules is that it is unlikely that all of the unique situations that arise during a lifetime of operation of the plant could have been foreseen at the outset in formulating such a set of rules. Real safety requires continued vigilance and critical examination by the people who are running the plant.

It is not the purpose of the above comments to imply that safety rules and regulations are wrong; the purpose is to ensure that we routinely examine their relevance and correctness, and modify them when appropriate. The responsibility for doing so rests with the organization that holds the prime responsibility for nuclear plant safety - the operating company.

4. The safety management system

The following is based on a simple premise: that a nuclear plant is perfectly safe in the sense of radiological hazard until it begins to operate. A useful corollary is that there is no such thing as a safe nuclear plant, but there are plants that can be operated safely. At the end of 1990, about 480 nuclear plants were operating in the world with an accumulated total operating time of 6000 reactor-years. To date there have been no deaths nor serious injuries attributable radiation from the operation of these plants. This safety record is bound to be broken eventually, but already far surpasses those of equivalent industries. [This statement was written in 1985. It is obvious that Chernobyl-IV has broken the perfect record; nevertheless, the world safety performance of nuclear plants still far surpasses the record of equivalent industries].

The above statements place the Operating Company in the central position of responsibility. Figure 11.1 indicates the proper relationship between Operating Company and the other major participants. The prime reporting relationship is to the Public . Supporting roles are played by the technocrats on one side - the Designer/Builder and the Scientific/Technical Community, and the bureaucrats on the other - the Safety Standards Authority and the Regulatory Staff.

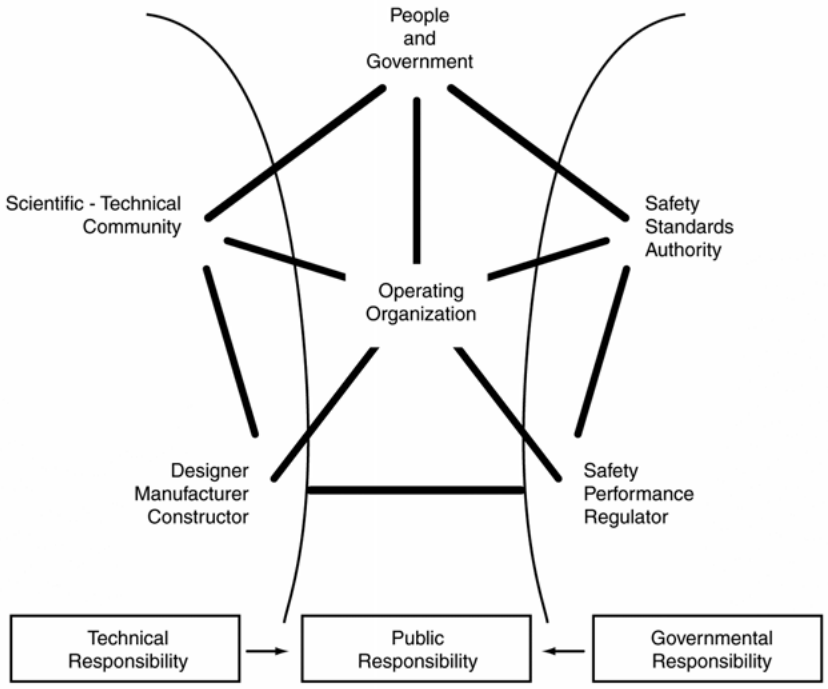


FIGURE 11.1
THE SAFETY MANAGEMENT SYSTEM

5. The role of the Designer-Manufacturer-Constructor

The newness of the technology, the dominant place of the Designer/Builder in development of the system, and the extended process of plant design and construction before the first license is issued tend to leave the impression that the central safety role is played by this group. However, it must be recognized that the Designer/Builder leaves the site shortly after first operation and has (at least in Canadian practice) no further responsibility for the plant. The Canadian exception is Ontario Hydro, but even in this case the plant responsibility transfers from one major organizational unit to the other. This can be considered nearly equivalent to handover from a vendor to an operating utility. Consider a unit twenty years into its operating life. The Designer/Builder organization is either disbanded or is committed to other projects, the Designer/Builder staff has forgotten the specific details of the unit, and even the drawings are out of date unless they have been kept up by the Operating Company. This is particularly true because changes are introduced into each unit by the Operating Company. Each unit becomes slightly different than its cousins, even if they were originally identical.

The central role of the Designer/Builder is to innovate on new plants so as to make them better performers at lower cost, so as to serve new customers and to stay competitive with other vendors. Their responsibility for safety is to deliver a plant to the Operating Company that not only meets regulatory requirements but meets the plant protection safety goal, as well as being economical to operate. During the operating phase, particularly in the early years, the

Designer/Builder might perform support services to the Operating Company. These services must eventually be taken over by either the Operating Company or a related organization whose only commitment is to support of operating stations.

The Operating Company has a return responsibility to the Designer/Builder. They must inform Designer/Builder staff of the design features that are most useful during operation, both from the point of view of performance and that of safety.

6. The Safety Performance Regulator role as auditor

The regulatory staff are assigned the auditor's role by the Safety Standards Authority. They review design features, operating procedures, and training to determine the acceptability of the plant for initial and continued operation. They have no role in design or operation. Furthermore, they cannot take any such role without compromising their position as impartial auditor.

The auditor's role involves a great deal of questioning of the Operating Company and Designer/Builder on details of design and operation. This role is never a popular one, particularly when approval to proceed with some action is held up, apparently to satisfy curiosity. There is, no doubt, some unnecessary holdup caused by lack of understanding or by personal factors. On the whole, the process is useful to the Operating Company because this is the only external and independent (not to say hostile) review of proposals. Internal reviews are valuable but sometimes miss important issues due also to lack of understanding or to personal factors.

One of the most valuable early decisions of the AECB was to assign staff at each station site. These people get to know a particular plant as well as the Operating Company supervisory staff, and often much better than the Designer/Builder or central office staff. They are therefore able to make reasoned judgements of the quality of safety-related aspects of plant operation on a regular basis. Knowing both the equipment and the people, they are better able to evaluate special situations which arise than are central office staff. Central office staff may be useful as technical backup, but the site staff must carry the main regulatory responsibility.

The Operating Company has an obligation to report matters of safety interest to the Regulatory Staff on a regular basis as well as to report any unusual occurrences. Questions posed by the Regulatory Staff in their auditor's role must be answered by the Operating Company to the satisfaction of the Regulatory Staff.

7. The role of the Safety Standards Authority

The Safety Standards Authority - in our case the Atomic Energy Control Board - carries the authority delegated from the government (and ultimately from the people) to administer the Atomic Energy Control Act. This Act grants very broad powers to make regulations for the administration of the Act. Up until recently, the Board chose to write only general regulations; specific regulatory requirements were applied through the licensing process - and so were largely

determined by the Regulatory Staff. In recent years the regulations have tended to become more prescriptive and inflexible. Nonetheless, authority and responsibility for all regulatory decisions rest ultimately with the Board, and until recently could be appealed to that body on an equitable basis.

In general, the role of the Safety Standards Authority is to determine the rules under which radioactive materials and processes must be managed in Canada. With regard to any activity involving ionizing radiation, they sanction the game; that is, they permit the activity to proceed provided that the rules are followed. Their ultimate power is to stop the activity if the rules are violated.

8. The role of the Scientific/Technical Community

This group is defined in terms of professional standing. As such, some of its members may be employed by the Operating Company while others report to organizations such as governments, engineering companies, research laboratories, and universities. Their common goal is to establish and maintain the scientific and technical information necessary to carry on the nuclear enterprise. In addition, it is their responsibility to carry on their activities within the bounds of high professional and ethical standards. On occasion, these goals come into conflict with some of the goals of the organizations in which these professionals are employed; particularly in matters of judgment on the importance of particular technical facts. In such cases their employer must recognize the requirements of professional conduct under which the Scientific/Technical group operates.

The Scientific/Technical group assists the Designer/Builder and the Operating Company in defining the equipment and procedures necessary to achieve safe operation. This group also deals directly with the Public in explaining the details of nuclear power technology and answering any concerns which they express. In our society, the Scientific/Technical group has a very high rating of credibility with the public. This trust rests, of course, on their continued adherence to the high professional and ethical standards noted above. Once this credibility is lost it can be very difficult to recover. This is one reason that employers must recognize their need to speak openly and honestly in areas of their own professional competence. The Scientific/Technical group must also recognize their special position as trusted interpreters of technology to the public. In recent years there have been many cases in which members of this group misused this trust by making unsubstantiated claims on one side or the other of the nuclear power controversy. The overall effect has been a reduction in the credibility of this group with the public.

In summary, the major roles of the Scientific/Technical group are (a) to provide reliable technical data for design, operation, and licensing, and (b) to inform the public of the realities of nuclear energy technology.

9. The role of the Public and Government

In the Canadian political system the public ultimately decides what is to be done and what is to be stopped. In this sense the whole of the nuclear enterprise reports to them. Officially, this reporting is done through government agencies and elected officials. In recent years, however, the public has become much more directly involved - the system has become more participatory and less representative. We all can recall cases in which public discussion has directly influenced the decisions made by both the Operating Company and the Safety Standards Authority. The safety management system has become a political system rather than a purely technical one.

In this climate, consider the position of the Operating Company when faced with a regulatory staff proposal with which they disagree, either on the basis of potential negative effect on safety or due to unfavorable cost-effectiveness. They can appeal this proposal to the Safety Standards Authority in hopes that reason will prevail. The Safety Standards Authority may rule against the Operating Company because of their heavy reliance on the regulatory staff for technical advice; in the present system there is no effective technical appeal.

The Operating Company cannot carry the argument into public discussion with any hope of winning the case. The reason is that the people have decided, right or wrong, that more safety is better for them. They do not count the cost. Many members of the public place a low credibility on the statements of the Operating Company. Opinion surveys show that only about half of the people are in favor of the nuclear enterprise; very little political support can be expected in this situation. The key participant group which the Operating Company must deal with in trying to maintain a rational licensing environment is the Regulatory Staff; very little can be done by the Operating Company without their agreement. They have become, in effect, the Safety Standards Authority.

The role of the public, it seems, is to force the Operating Company into an active public information campaign, virtually a political campaign, to gain acceptance of nuclear power technology. This is likely the most important task facing the Operating Company over the next 20 years.

10. The Operating Organization

Referring back to Figure 11.1, the Operating Company may be considered either to be at the center of the action or to be surrounded on all sides. The one indisputable fact is that the Operating Company is in the nuclear energy business for the long run. Since the station is already committed and running, the capital is spent, and a return on investment can be obtained only by operating the plant for a number of years, the Operating Company has no way out but straight ahead.

The key element for success of the enterprise is for the Operating Company to earn the confidence of the People in their ability to run the plant safely and efficiently.

The Canadian Regulatory Framework

11. Development of Canadian approach to nuclear plant safety regulation

The serious study of public safety issues in Canada began with the NRX accident in 1952. This apparent misfortune may have been the most helpful event in our history with respect to subsequent developments in the field of safety. It occurrence at a time when there were no CANDU plants in existence, so there was no established practice or tradition which had to be altered. Subsequent to this accident, E. Siddall developed a system of logic for judging the adequacy of power reactor safety. The system that Siddall devised was based on the principle of constant risk (taken as the product of accident probability and radiological consequence) for the whole spectrum of probabilities. The target was a frequency of 10^{-5} /yr for serious accidents, based on an overall risk of 1 statistical death per 100 reactor years. This method of establishing acceptance criteria was applied to NPD licensing with reasonable success. The weaknesses of the system lay in the fact that the failure probabilities were not well known, in the question of completeness of the accident sequences analyzed, and in the difficulty of judging the acceptability of a particular design feature for licensing purposes.

Concurrent with Siddall's work George C. Laurence also proposed, on the basis of risk arguments, that the frequency of a major accident in a power reactor should be less than 10^{-5} per year. He proposed that this goal was achievable by establishing independence between the operating equipment and the special safety systems (shutdown and emergency core cooling). Containment was later included as a Special Safety System. These concepts were formalized in 1965 into a set of criteria that became known as the Siting Guide. This simple set of basic safety criteria is still in effect.

Just after startup of the first units of Pickering A, Hurst and Boyd published the last revision of the Siting Guide (Table 11.2). This system retained the probabilistic concepts developed earlier but added deterministic requirements (single-dual failure logic, independence of safety and process systems, safety system unavailability limits, etc.). We are still using this system, albeit with many embellishments and added detail. A brief history of Canadian regulatory development is presented by Atchison, Boyd, and Domaratzki in a publication in Nuclear Safety (24,4 1983). What is not shown in that publication is the degree to which the interpretation of a nominally fixed set of rules has made the process of licensing in Canada extremely complex and stringent.

TABLE 11.2 – AECB SITING GUIDE

Situation	Assumed maximum frequency	Meteorology to be used in calculation	Maximum individual dose limits, mSv	Maximum total population dose limits, Sv
Normal operation		Weighted according to effect, i.e. frequency times dose for unit release	5/yr, whole body 30/year, thyroid	100/yr, whole body 100/yr, thyroid
Serious process equipment failure (single failure)*	1 per 3 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	5, whole body 30, thyroid	100, whole body 100, thyroid
Process equipment failure plus failure of any special safety system (dual failure)	1 per 3000 years	Either worst weather existing at most 10% of time or Pasquill F condition if local data incomplete	250, whole body 2500, thyroid	10,000, whole body 10,000, thyroid

* A serious process failure is defined as any failure of process equipment or procedure that requires action of a special safety system to prevent significant fuel failure or significant radioactive material releases from the station.

The reference dose limits during normal operation coincide with the recommendations of the International Commission on Radiation Protection (ICRP). The limits for single failures were set equal to the same values. The individual dose limits for dual failures were chosen to be within the range judged tolerable for a once-in-a-lifetime emergency dose; it is below the expected threshold for observation of early clinical radiation effects. Population reference dose limits for dual failures were chosen so that the incremental lifetime cancer rate expected following a dual failure would be very small - less than 0.1% increase in a population of 1 million people. A caution is necessary concerning the definition of single failure - this is a very different concept than that used in the US, where it applies to failure of components in redundant mitigating systems. Also, the Siting Guide is completely silent on "triple" failures. A number of additional criteria have been added to this basic framework. These additions are discussed in the following sections.

12. The US licensing system

The background of the licensing system developed in the United States is important to us because of its pervasive influence on the rest of the world, including Canada. Even though (fortunately) the Canadian system has been developed with a fair degree of independence, the ideas fostered within the US system have a strong influence on the way in which the Canadian regulations are interpreted in practice.

Most people in the industry think of the US system in terms of massive documents listing detailed requirements, enforced by bureaucrats with keen, legalistic minds. It was not this way in the beginning. In 1953 Edward Teller, addressing the Joint Committee on Atomic Energy of the US Congress, made a very interesting summary of the state of reactor safety at that time. He concluded:

"It would seem reasonable to extend the AEC (Atomic Energy Commission) procedures on reviewing planned reactors and supervising functioning reactors to nuclear plants under the control of private enterprise. To what extent these functions should be advisory or regulatory is a difficult question. I feel that the ultimate responsibility for safe operation will have to be placed on the shoulders of the men and the organizations most closely connected with the construction and the operation of the reactor".

This appears to be a reasonable statement by anyone's standards. At about the time this statement was made, containment was introduced as a protective feature on US plants. This addition was made to allow reduction of the then-existing requirement for exclusion radius ("exclusion radius" is the term used for the radius around the plant within which no permanent habitation is allowed). A reactor without containment would require a 17.3 mile exclusion radius if the power were 3,000 thermal megawatts. This was clearly unacceptable for commercial installations.

The emphasis in safety reviews at that time was on loss of shutdown action and potential reactivity increase with increasing power. As David Okrent notes, "Considering the weapons background of many of the committee members, and the characteristics of some of the reactors then reviewed, this emphasis is not surprising". The long-term result of this approach was overemphasis on some aspects of plant safety and neglect of others.

Following introduction of containment as a design requirement the situation was fairly stable until 1966, when meltdown and containment failure were linked by the "China Syndrome" and other mechanisms. Prevention of core melt by emergency coolant injection became a major topic. The formidable legal machinery of the US became involved in the process at a time when anti-nuclear interveners were appearing, ready to use whatever means were available to stop nuclear plant construction and operation. Poor workmanship and design errors showed up on a number of projects. The natural consequence of the now very complex licensing process, schedule delay and cost overrun, are now being used as further "proof" that the technology is not appropriate. It is unlikely that any US utility will order an LWR plant until the situation changes. Nevertheless, a number of US plants have been completed on time and within reasonable costs.

The impact of the US situation on Canadian utilities has been mainly through its indirect negative effect on public opinion. People who do not make distinctions between power reactors and nuclear bombs cannot be expected to recognize the fine points of difference between CANDU and the LWR, or between the Canadian regulations and those south of the border.

The impact of US practice on Canadian licensing has been mainly in adoption of practices quite similar to those in the US (e.g. formal Quality Assurance) and in transfer of issues being discussed by the USNRC. Much of this "technology transfer" has been useful, but it has brought with it some of the negative aspects of the regulatory process in the US.

The US reactor safety situation should be followed closely by Canadian designers and utility staff. The matter of fission product behavior inside containment is particularly important at the present time. In view of the fact that core meltdown is precluded in CANDU, there is a good possibility of completely eliminating the "disaster" scenario from consideration. This could have a considerable impact on public acceptance in the long term.

13. Standards, Codes, and Quality Assurance

A formal criterion has been established that "The design, construction, and operation of all components, systems, and structures essential to the safety of the reactor will follow the best applicable codes, standards, or practice and be confirmed by an independent audit". This rule has led to a massive system of quality assurance procedures, with more or less importance to real safety depending on the degree to which the particular process is made bureaucratic or focused on real safety issues.

14. Radioactive materials release during normal operation

In 1974 the Canadian Atomic Energy Control Board established design and operational targets for radioactive releases during normal operation such that the dose to individual members of the public would not exceed 1 percent of the statutory limits. These "targets" are now virtually requirements.

Recently, the International Commission on Radiation Protection (ICRP) has recommended reductions in operational staff doses to about 40 percent of their prior recommendations. The basis for these new recommendations is not clear; nevertheless, they probably will be adopted into Canadian law.

15. Independence between process and safety systems

The original formulation suggested by Laurence recognized that the level of public safety expected would require establishment of a very small recurrence frequency for major releases of radioactive material to the environment. He also recognized that a single system providing that defense would have to be so reliable that it would be difficult to establish its real reliability in any credible fashion. For this reason the independence and separation between process and safety systems became a basic part of the licensing system. This idea is probably traceable to the NRX accident, in which the use of safety rods in process functions contributed strongly to the failure

sequence. Specifically, prior to the accident, some of the shutoff rods were disconnected from their drive systems and left in the reactor in order to overcome the unusually high reactivity level necessary for a specific experiment.

The independence principle has been formalized as "The special safety systems will be physically and functionally separate from the process systems and from each other". The special safety systems (those which have no function other than accident mitigation) are shutdown, emergency core cooling, and containment. The special 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 that calculated for dual failure. The formal statement is clear in the case of shutdown. It is not so clear in the case of emergency core cooling or containment - is it intended that the performance of emergency injection should be functionally independent of shutdown? The two-shutdown-system rule, discussed in Section 11.16, resolves this question.

Independence from process systems has been interpreted to mean that no credit may be claimed for beneficial action of process systems in doing the licensing analysis. If process system action tends to increase accident consequences, however, then they must be credited.

16. The two-shutdown-system rule

Within the single-dual failure logic of the Siting Guide, it is stated that serious process failures must be analyzed assuming complete failure of any special safety system - including shutdown. No mitigating action could be claimed for process systems. This meant that uncontrolled TOP events had to be analyzed - a difficult process at best. After considerable effort in this area, particular in the context of Gentilly 1 licensing, the designers decided to install a second shutdown system in Bruce A and all subsequent plants. (Pickering A has a partial capability for independent shutdown by rods or moderator dump). The initial intent was to make the second system fully capable of mitigating major LOC sequences. The Board subsequently determined that the second shutdown system should be fully capable; that is, it must be shown that all requirements of the Siting Guide can be met by either SDS1 or SDS2 acting alone.

Furthermore, each of these systems must have two effective independent trip parameters for each accident sequence "where practicable". There has been much discussion of the meaning of the word practicable; in this case it seems to mean "possible" independent of cost or effect on normal operation reliability. Some compromises have, however, been accepted. The two shutdown systems are required to be conceptually different and sufficiently separate and independent of each other so that the criterion for cross-linked failures will be met.

Within the Siting Guide logic the result of having SDS2 is that there are no dual failure sequences without prompt shutdown. No special modification of the basic requirements was necessary to accommodate this major change in design. The major implication of AECB acceptance, however, was that the Siting Guide was recognized by the Board as a probabilistic regulation.

In retrospect, addition of the second shutdown system was a very beneficial development. Aside from its obvious benefits in avoiding problems in licensing and public acceptance, in purely pragmatic terms the second system is probably cheaper than the analysis that would have been required had the second system not been installed. There are still operational difficulties to be resolved in the area of in-service testing.

Currently, the AECB is exerting pressure on the Pickering A licensee to backfit a second fully capable shutdown system into the Pickering A station. Such a system would be extremely expensive and difficult to install; at this point the owner may choose to decommission the station.

17. Regional overpower protection

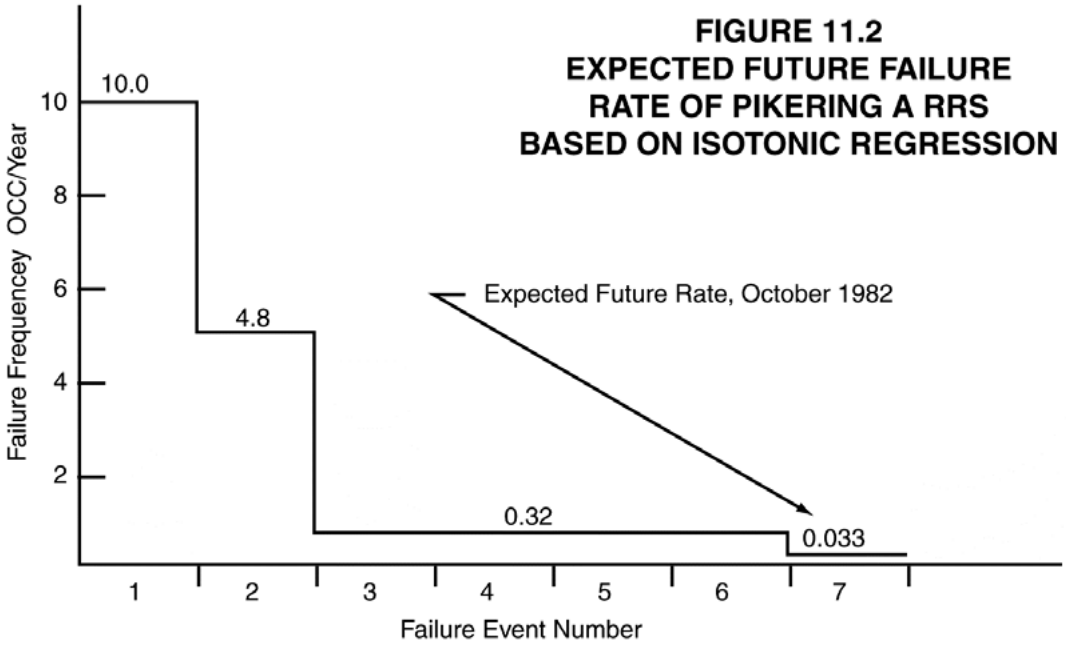
The fact that CANDU fuel bundles are immediately adjacent to the pressure boundary gives rise to concern about the potential for either dryout failure or fuel melting failure of sheaths to cause consequent pressure tube/calandria tube failure - and possible propagation to other channels. Steadily increasing fuel bundle powers in later designs (driven by the high cost of heavy water) increased this concern. A solution was proposed for Bruce A which consisted of a distributed array of flux detectors in the core, identified as the regional overpower protection (ROP) system. This system, of course, was required to be independent of the detection system used for plant operation. When SDS2 was introduced it had to have a second ROP system in order to be independent of SDS1.

A great deal of discussion has taken place, and expensive experiments conducted, on the subject of the setpoints on ROP system detectors. The AECB staff have insisted on generous error allowances on channel power relative to the expected onset of dryout in the "worst" channel, on the presumption that dryout can be equated to a potential for pressure tube failure.

18. Frequency of serious process failures

In 1980, Z. Domaratzki reviewed the then-existing experience of serious process failures (those in which shutdown system action was required to prevent fuel failures). He concluded that "-- (a) the frequency of serious process failures was roughly consistent with the assumption made for licensing purposes and (b) there were no resultant fuel failures or release of radioactive material from the stations. Nevertheless, both the Board and the plant operators considered that it was practical to reduce further the frequency of serious process failures and that it was prudent to do so". The last statement is a slight overstatement of the degree of concurrence by the plant operators.

With regard to the reactor regulating system (RRS), the original design intent was that the failure frequency should be in the range of one per 100 operating years - a rather stringent standard given the level of knowledge at that time. Review of Pickering A RRS revealed several deficiencies that were subsequently scheduled for correction. (One of these corrections slipped through the cracks and was not implemented - and caused an LOR in the early 1980's). The subsequent performance of RRS at Pickering has been steadily improving, as reported by Basu and Sharma (IEEE Conf., 1984). Figure 11.2 indicates the expected future unavailability based on isotonic regression analysis of past events.



Domaratzki states in his 1980 paper that "It is a requirement that reactor regulating systems be designed so that the expected frequency of loss of regulation accidents will be one per hundred reactor years. A thorough analysis is required to give reasonable assurance that this target will be met." It is notable that no credit is given for this requirement in licensing analysis - it must be assumed that the RRS acts in an unfavorable direction when analyzing accident sequences. If RRS action decreases accident consequences it must be presumed to fail to act; if RRS action increases accident consequences it must be presumed to function normally.

Operating experience at Douglas Point and Pickering had shown that loss of Class IV power (specifically, the loss of forced circulation by the HT pumps) represented a significant fraction of the total allowable frequency of serious process failures - or, more precisely, the rate of demand on shutdown action to restore the heat production/removal balance. Designers proposed addition of partial or complete power stepback by the RRS using separate solid control absorbers and installed this feature in all plants beginning with Bruce A. This feature was also adopted by the AECB as a rule. Stepback now "-- is required to ensure that the frequency of serious process failures is kept as low as reasonably achievable." Again, no credit can be claimed for stepback action in licensing analysis.

The last revision noted by Domaratzki in his 1980 paper was with respect to feedwater system reliability. The stated rule requires "Redundancy in the feedwater system itself to ensure that failures of single components do not interrupt feedwater flow, and establishment of and adherence to clear operating procedures". Subsequent to this paper, reactor trip on steam generator feedline low pressure has been made mandatory on all new plants.

19. Availability of special safety systems

In order to meet the frequency limit stated in the Siting Guide for dual failures, it is required that each special safety system meet an unavailability of 10^{-3} at the design stage and be testable in-service to ensure that the limit is met. The smallest unavailability that can be claimed for any special safety system is set at 10^{-3} to account for unknown cross-linked and common cause failure sequences. In his 1980 paper, Domaratzki noted that the unavailability performance of shutdown and containment had generally met the licensing requirements. An exception occurred in early operation of SDS2 at Bruce - a normal situation for the first system of its kind. This weakness was later corrected. During the past three years, Ontario Hydro plants have reported some high shutdown systems unavailability figures - this problem is currently under investigation.

The high unavailability (determined by testing) of emergency coolant injection systems showed that Siting Guide requirements were not being met in most years. A number of minor deficiencies were corrected in the Bruce A system. It was concluded by Domaratzki that the complexity of ECI would make it difficult for even those designs with redundant components to meet the AECB unavailability requirement, and that non-redundant systems such as the one installed in Pickering A were unlikely to meet the requirement. (Historical note - the Pickering ECI originally was targeted for 10^{-2} unavailability by the designers; AECB pressure in the later stages of the project led to the owner accepting a lower target of $3x10^{-3}$, too late for incorporation of redundant components. Also, the Pickering A design was established before the last revision of the Siting Guide which required complete independence and separation between the ECI system and process systems).

Basu and Sharma have analyzed the historical data using isotonic regression; their results are shown in Figure 11.3. It can be seen that the unavailability has been erratic, and generally above the unavailability target. The trend reversals are thought to have resulted from changes to maintenance procedures, particularly on the injection valve actuators.

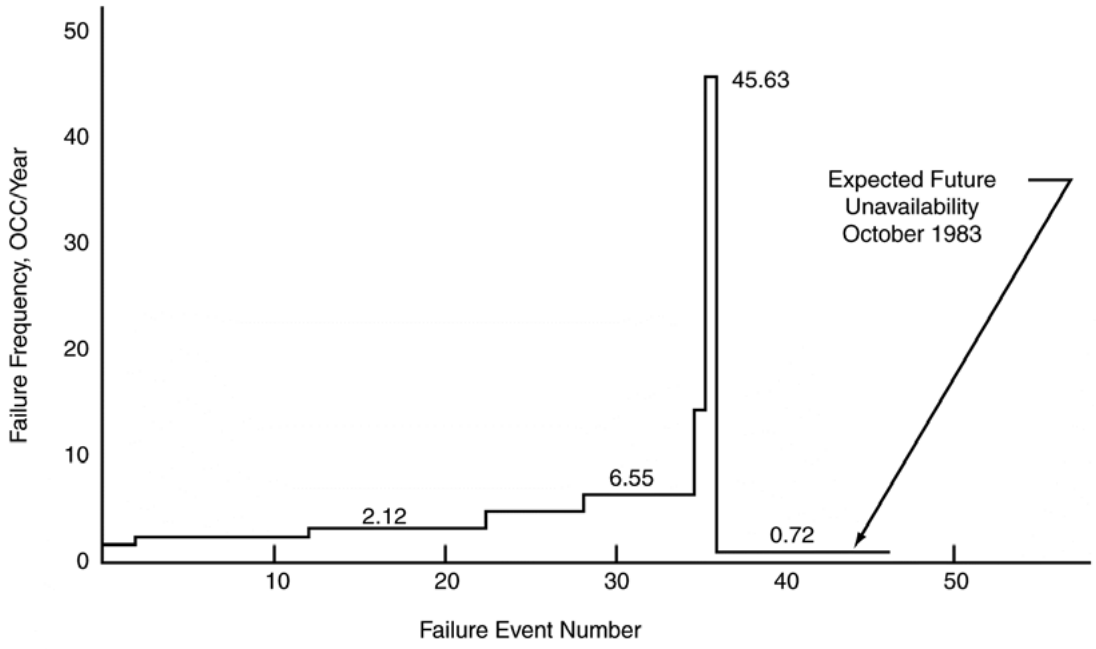


FIGURE 11.3
EXPECTED FUTURE UNAVAILABILITY OF PICKERING ECI SYSTEM BASED ON ISOTONIC REGRESSION

The Pickering A emergency coolant injection system has been upgraded by incorporation of redundant valving and by addition of a high-pressure injection.

There is still an open question as to the meaning of "unavailability" in this context, in relation to mission reliability. The duration of the shutdown system mission is only a couple of seconds, so the two can be considered the same. However, the emergency core cooling function must continue for months, and the containment function must be maintained for years in the most extreme cases. This issue is still being discussed; it seems that the most satisfactory approach would be to consider late failure of these safety systems as a "post-accident accident"; that is, to calculate the failure sequence from the desired initial post-accident state and introduce the safety system failures as new events. This exercise should be revealing as to the time available for corrective action, the effectiveness of backup systems, etc.

20. Effectiveness of safety systems

The major "revelation" referred to in the 1980 paper by Domaratzki was that ECI systems then in existence could not prevent fuel failures following a LOC sequence as claimed in Safety Reports. This claim was, in fact, a direct result of pressure on the applicant by the RSAC during the Pickering A licensing proceedings - presumably so that there would always be "two lines of defense" available to prevent fission product release. Earlier, during the Douglas Point

proceedings, W.G. Morison had concluded that it would likely prove impossible to prevent fuel failures for the "stagnation" break in which pressures are so balanced that water is rapidly ejected from both ends of a channel. In spite of this realization (which subsequent experiments and analysis have shown to be accurate) the AECB staff continued to insist on "no significant fuel failures".

High-pressure emergency coolant injection systems have been backfitted in Pickering A and Bruce A.

21. Containment impairments and testing

The original Siting Guide stated that containment failure was to be considered in dual failure analysis, but did not define "failure". Opinions ranged far and wide - even to a suggestion that it should be assumed that the containment had disappeared after the accident. Cooler heads prevailed, and in the end a number of impairments to active systems were defined for analysis as dual failure events. The revelation of the possibility of fission product release to containment during a LOC sequence (which was no revelation at all) has led to much greater emphasis on analysis of extreme impairments such as open airlocks, as well as extensive analysis of the operability of the plant systems following a LOC sequence. The AECB has specifically excluded three extreme containment impairments from consideration within the dual failure logic - open airlocks, total failure of dousing in single-unit containment systems, and complete failure of pressure relief valves in vacuum containment systems. Periodic full pressure testing of containment envelopes is a recently imposed rule.

22. Common cause and external events

Since about 1974, licensing proceedings have included the requirement to consider a large group of events such as earthquake, fire, aircraft crash, flooding, external explosions, etc. Designers have responded with physical separation and the "two-group" approach of redundant systems each capable of accomplishing shutdown and heat removal after such an event. (The concept has not yet been extended to containment.)

23. Summary

The sequence of development of these requirements has followed a more or less logical pattern of steady tightening of the rules and establishment of a large block of "Common Law" which now constitutes the licensing system in Canada. Some level of documentation of these rules would be useful to all concerned, and this is now in progress. On the other hand, establishing a set of prescriptive rules which define what is, and what is not, sufficiently safe would be counterproductive to real safety.

What is not clear is whether or not there is a state of nuclear plant safety which can be identified as "good enough"; that is, do we still have a risk-acceptance criterion or can we look forward only to a progression of new rules independent of either risk level or operational safety performance? The jury is still out.