NUCLEAR SAFETY: REPORT TO THE ONTARIO NUCLEAR SAFETY REVIEW

Ben Barkow, Ph.D., Behavioural Team, Toronto

1987

CONTENTS

DESIGN QUALITY ASSURANCE IN NUCLEAR GENERATING STATIONS

.c.Executive Summary

1. The results of errors committed at the design stage and the conditions leading to design errors are similar among the general construction industry and the powerplant industry. The Quality Assurance procedures in place for powerplants are not perceived as resulting in better outcomes as compared to general construction.

2. Quality Assurance guidelines tend to be treated as logical and compelling hedges against design defects in nuclear powerplants (discussed as the “Sacred Cow” theory below). This outlook may be contrasted with a behavioural or “Burglar Alarm” model which subjects the QA rules to tests of sensitivity in detecting flaws.

3. It would bring QA implementation closer to recommended practice if the following were considered.

a. The independence of those implementing the procedures within Ontario Hydro (and within AECB vis à vis Ontario Hydro) should be more critically preserved.

b. QA functions should be made staff not line; thus the organizational imperative behind QA would be more obvious and reporting channels more direct.

c. Professional specialty qualifications of QA staff should be assured by more objective means.

d. the AECB should decide whether its role is to be regulator or colleague.

.c.Introduction and Purpose

Errors appear in the texts I enter into my computer. Fortunately, in this office we are usually conscientious in subjecting texts to a computer-based “spelling checker” program. This program (a) highlights errors, (b) suggests better spelling, and (c) accepts some guidance from its human operators. Does this ensure that errors never show up in our reports?

Alas, errors do occur in our final reports despite efforts to apply the checker program. Why?

It may happen that

· the checker does not realize we meant “whether” not “weather,”

· being foreign in manufacture, the checker may have different standards for words,
· errors may have been introduced after the checker was last applied,
· the checker may have modestly accepted guidance from a person whose spelling gifts were less than the checker's own, and
· not rare at all, the checker's dictionary code may have contained its own errors.

Checking spelling is a pretty straightforward task compared to building error-free billion-dollar nuclear generating stations. Spelling goodness is judged in errors per unit of text and the errors tend not to interact or cumulate, nor do they form a pattern which can result in total negation of the value of the text. Readers do not come to a spelling mistake, "turn off" the reading process, and return the report for corrections before reading it through to the end.

An error in a nuclear generating stations, by contrast, is at best, confidence impairing and at worst, catastrophic. Curiously, if you look again closely at the weaknesses of our spelling checker, you may note some parallels with the weaknesses of Quality Assurance systems for nuclear powerplants….

The main purpose of this report is to distill information developed in a previous, more extensive review of the human-factors underlying civil and structural engineering design errors in Canada. That review compared Canadian experiences with design errors in general construction practice with those experienced in the construction of powerplants. Sponsored by the National Research Council of Canada and conducted by Behavioural Team, the publication is referenced as,

Darian Wallis and Ben Barkow:
Human Factors Underlying Building Failures.

This report, issued January 19, 1984, 110 pages, is archived in the library of the Institute for Research in Construction.

It is useful to review the history of this report. Dr. David E. Allen of the NRC had been interested in the topic of building design errors in the building industry for some time. In October, 1983, he asked Behavioural Team to examine the past twenty years of published reports on building design errors and to survey by phone a small sample of Canadians professionally engaged in design.

Behavioural Team welcomed this important and life-saving work. But it was pointed out that nothing improves the trustworthiness of a human-factors survey as much as a baseline or control group. In this context, it seemed wise to compare the commercial and pragmatic approaches of the construction industry to a branch of design deemed superior to all others — but still useful as a comparison — the designers of powerplants. Dr. Allen accepted this suggestion.

The research was conducted during the last quarter of 1983. The report was issued in early 1984. This study relates to building design errors which, if not caught in time, result in collapsing roofs, falling walls, and cracked floors. Most often, however, design errors are caught at some point before dramatic failure occurs. Often they are caught before construction begins but sometimes it is construction or, later, operations staff who detect the problem.

For the purposes of the Ontario Nuclear Safety Review and to update the material of the report, some additional literature was consulted and interviews were held with two key informants at the AECB and Ontario Hydro. These specialists are responsible for Quality Assurance in powerplant design.

.c."Human Error"

Human-factors psychologists try to reduce the impact of errors by —

(a) inhibiting or counter-acting them at their source and

(b) devising properly human-factored procedures for detecting them prior to their expression.

Human error is not viewed in a moral light as something which arises from a person's will. Psychologists are never content to hear, "Well, it was just human error." As with any other sort of human behaviour, the statistical incidence of errors can be controlled.

A great range of techniques are available for influencing the frequency of errors. At one extreme, engineers can be encouraged to get a good night's sleep before work days. Their conditions of work — acoustic, light, and interior climate environments — can be adjusted as can their personnel-related conditions of employment and motivation. At the other extreme, complex cognitive checking procedures can be put in place for review of work.

.c. Published Reports

The study of errors and faults is inherently statistical because so many error processes follow stochastic (as opposed to deterministic) causality. Moreover, many factors operate to intentionally and unintentionally obscure the true cause of failures and thus academic studies seeking to understand these events can rarely be definitive.

Of all building failures, about 60% to 70% are caused by people at the design or construction phase. Other failures arise from materials deficiencies,

statistically infrequent natural events, and, of course, human error in other phases.

In Canadian construction, of known errors, half appear to arise at the design stage and half in construction. Construction-stage errors may be inherently more detectable and thus the percentage occurring during the design-stage — and which lie dormant in our buildings — may be larger by an unknown degree.

The fine procedures established for industrial and construction quality control are not found in civil engineering design practice. That is because it is relatively straightforward to assess the quality of materials and workpersonship on a shaft bearing as compared to a complex roof truss. Moreover, sampling shaft bearings and exposing the sampled unit to destructive testing is rather more feasible than destructive or even non-destructive testing of roof trusses.

Obstacles to better quality control at the civil engineering design stage include:

- lack of à priori criteria of performance,
- professionals come from a variety of disciplines,
- insufficient statistical information on likelihood of errors,
- kinds of errors likely to occur are not well known.

But of all areas of construction design, nuclear power design teams could suffer from these individual weaknesses less than the general run of design offices. That is because they are (or could be) integrated in their approach, unanimous in their performance criteria, and, most important of all, rigourous in documenting and highlighting statistically-frequent past weaknesses.

There are many sound approaches to counter-acting design errors. These are outlined in the original report. Reduction in design errors can be brought about by the following procedures reviewed in the original NRC report.

1. Teamwork

There should be improved teamwork, whereby peers check the work of their co-workers as a matter of standard procedure. Each person in the building process should be aware how his task fits in with the successful completion of the project.

2. Supervisory Control

Precautionary measures against unintentional human errors and negligence include peer review (as above) and careful and regular supervisory control should be instituted.

3. Checking, Inspection, and Review Procedures

New or unusual features should reviewed externally by qualified experts. Checking and inspecting procedures should be incorporated into each stage of planning, design, and construction for the presence of errors. There should also be independent (external) assessment of the design, as for example the municipal authority. Checking and design reviews were the ways most commonly cited by our interview respondents to prevent design errors.

4. New or Unusual Features - Extra Care

Additional precautions are required in the case of new design or construction methods for which little prior experience exists. In such cases, it is wise to focus responsibility on one senior design professional and be alert to the consequences of changes in personnel.

5. Responsibilities

The responsibilities of all members of the planning, design and construction teams should be clearly defined orally and in writing. Tasks, responsibilities and duties of the owner, project manager, site manager and specialists must be clearly defined and the names of different persons fulfilling different functions should be drawn up on an organizational chart for easy reference.

6. Feedback from Failures

Failure reports on causes, types and consequences of building failures should be collected for categorization and analysis. This information would be used to identify problem areas and to improve Quality Assurance procedures. Such information, in our view, has not been given sufficient emphasis among design professionals over the years. “Human error” should never be considered an explanation. The antecedents and necessary corrective procedures to counter “human error” should be thoroughly reviewed by qualified professional psychologists and the corrective procedures implemented.

7. Training of Staff

There should be better education and training of staff through technical upgrading seminars. All staff, especially supervisory staff, should be trained in interpersonal skills to improve effective communication and working relations because communications was identified as a special problem by powerplant personnel. Examinations to certify operators and technicians should be of proven validity and should meet conventional standards of test-retest reliability

8. Communications

Communication should be improved by ensuring that all phases of the project are fully and clearly documented. Special care should be taken to communicate clearly at the interfaces of the project where information at one stage is

passed on to the staff of another stage. Effective communications is especially important when there is a change, apparent error, or disagreement.

9. Improved Supervision

Supervisors should be educated in interpersonal skills so that they will be able to better handle instances of individual failures and so they will be able to recognize signs of impending failure before they occur. Behaviour problems can be reduced by educating supervisors to make them aware of past indicators so they can recognize them if they occur again. They should also be skilled in how to handle apparent errors or disagreements that arise. There should be regular job performance reviews to highlight personnel problems.

10. Motivation

It is important that all those involved in the design and construction of powerplants have adequate motivation to do a good job. Motivation refers to an internal state of the worker, his attitudes and willingness to work well, in addition to external reinforcements such as pay which activate the individual to do a good job. Adequate worker motivation can be related to a sense of expertise and job performance. There should be good working morale among employees, activated by good working conditions and teamwork.

.c.Interview Results from the NRC Study, 1984

As an important part of the 1984 NRC study, members of the general building construction industry were interviewed. As a comparison to them and, it was expected, as a measure of excellence to hold up to general construction practice, designers of electricity generating plants — largely nuclear — were interviewed. Our previous work for the Atomic Energy Control Board, led us to feel that such error-fighting concepts of Quality Assurance, materials acceptance testing, fault trees, and other respected human-factors procedures have their highest likelihood of appearance and finest expression there. Some of these procedures and their Canadian Standards Association reference are discussed below.

Two sets of professionals were interviewed: 10 professionals from general building design and 10 engaged in the production of powerplants. The study did not seek to compare rates of errors because an “exposure incidence” would be needed in order to establish an “error rate.”

It should be noted, the samples were small, the interview was brief, and the project was not primarily designed to analyze the effectiveness of nuclear

generating station design Quality Assurance. On the other hand, clear results arising from studies which have low "sensitivity" (in the research sense), can have as much validity as similar findings arising from larger studies – and they do have much more emotional impact! For full details of sampling and procedures, please see the original report.

Respondents were asked how serious a concern design errors represent (on a scale of 1 to 7). The groups averaged 2.9 for general construction and 3.0 for powerplants indicating quite similar levels of concern.

Individuals in the two groups were then asked to tell us of three case histories of design errors. This may be viewed as a quasi behavioural approach because respondents have to relate specific incidents with which they are familiar… as opposed to relating their attitudes or reactions to hypothetical issues.

Some flavour of the cases studied can be gathered from the following instances:

· a numbering system for parts, modified to be unique for each project, resulted in wrong parts being ordered,

· pre-cast concrete panels were not properly fastened to a building because the designer incorrectly assumed how the contractor performed the work,

· the compatibility of materials on tube sheet welding in water heaters was wrong resulting in brittle welds,

· D.C.-powered cooling fans (instead of A.C.) were installed for a turbine generator; they failed to cool the generator….

On a three-point scale, how serious did they feel [each] of these to be? The two groups averaged 1.9 and 1.9 ("somewhat serious" was defined for respondents as a response of "2"). Thus, upon reflecting back on errors which had surfaced, the average degree of seriousness of recalled events was judged to be the same in the two groups.

The consequences of the design errors were explored with respondents. Both groups indicated that financial loss with the major consequence of the error.

When during the course of development was the design error detected? The earlier a defect is detected the better it is because the cost of corrective action is related to promptness of identification. Expressed otherwise, pencil erasers are cheaper than pneumatic drills. Respondents were asked, "In what phase was the error [which the respondent had just specifically described] detected: (a) planning, (b) design, (c) construction, (d) use (production)?"

Of the 30 general construction errors, 50% were not detected until use or occupancy. Among powerplants, 43% of the errors went undetected until power production was underway. Thus both areas show what appear be, in our judgment, “leaky” error-detection sieves. Despite the QA structure imposed on powerplant designers, the powerplant designers are not much more capable of combatting errors upstream as compared to general construction designers.

Respondents were asked specifically about QA systems which were in place. Among the general construction industry, 53% of incidents would have been prevented and among powerplant personnel, 60% would have been prevented.

It is difficult to evaluate this item of data. Why didn’t the QA plans do what they are designed to do? Are the powerplant personnel showing greater confidence in their QA plan or are they saying, “Had it been implemented better, 60% of errors would have been caught”? In any case, the similarity of the commercial builders and the powerplant builders is cause for concern.

A list of 18 factors which can contribute to errors was presented in a consistent but randomized order. These range from “inadequate checking” (a common problem) to “poor working conditions” (seen as a rather rare contributing factor). The list, arranged in descending order of significance as seen by participants, is shown below. The ratings were as follows:

1 = somewhat common,
2 = not common, and
3 = entirely rare.

COMMON FACTORS CONTRIBUTING TO ERRORS

	Building	Powerplant
inadequate checking by members of design team	1.3	1.9
errors in design drawings or specifications	1.4	2.0
inadequate oral communication	1.4	2.0
political (eg. governmental or financial pressures)	1.4	2.3
gaps in information (eg. insufficient knowledge)	1.8	1.9
poor teamwork	1.8	2.1
inadequate documentation	1.9	2.3
errors in design assumptions	1.9	2.2
inadequate checking by others	2.0	1.7
error in design concept	2.1	2.4
unclear definition of responsibilities	2.2	2.0
forgetfulness	2.2	2.3
errors in design calculations	2.3	1.9
lack of Quality Assurance plan	2.4	2.5

insufficient knowledge	2.4	2.3
negligence	2.6	2.9
impaired job performance	2.7	2.7
poor working conditions	3.0	2.8
mean score	2.0	2.2

In an absolute sense, the powerplant group perceive fewer error-generating conditions in the course of their work as shown in the means of the table. Both means reflect a perception that such problems are “not common.”

Examining specific causes of errors, the most frequent to be expected in nuclear generating stations would be (in decreasing order of frequency):

1. inadequate checking by others,
2. gaps in information or insufficient knowledge,
3. errors in design calculations, and
4. inadequate checking by members of the design team.

Two questions may be raised from these data. First, do or should current QA systems account for these perceived conditions leading to errors; are they addressed in current plans and are they being implemented? Second, if they are not currently addressed and/or implemented, are they in principle or in practice incorporatable into better QA systems for the future?

The correlation of the two sets of judgments using a Pearson product-moment correlation was .68 with a probability below .002. For 20 respondents, most observers would say that .68 (with $p<.002$) represents highly similar agreement. In short, when given a free choice of ratings, the powerplant group indicate that the relative appearance of error-causing conditions is similar to the general construction group.

How do the two groups differ as to the general characteristics of error-engendering conditions? In the chart below,

· technical procedures relate to errors such as not knowing the materials which are compatible with a specific caulk substance,

· organizational/management relates to problems such as of communications, and

· behavioural relate to pressures to leave work at 5:00 PM or various career concerns.

The chart suggests that the two groups are similar in their ascription of root causes. However, the powerplant group are more dismayed by organizational and managerial concerns and less by behavioural and individual concerns.

It may be observed, that there is strong similarity between the perceptions of the general construction personnel and the powerplant personnel. Depending on your outlook and on your domestic proximity to a nuclear generating station, this information would make you proud of Canadian general construction practices or concerned about nuclear powerplant construction practices. This research does not resolve that choice.

.c.Present AECB and Ontario Hydro Practices

In order to learn the current approaches of the AECB and Ontario Hydro, interviews were conducted with two staff who head the QA organizational pyramids at their respective organizations:

J. M. Massicotte
Scientific Advisor - Quality Assurance
Atomic Energy Control Board

and

Robert Jeppesen
Manager - Quality Assurance
Engineering and Construction
Ontario Hydro.

Current approaches to QA in design tend to be referenced to CSA Preliminary Standard N286.2, Design Quality Assurance for Nuclear Power Plants, May 1979. N286.2 was created by a committee of seven (advised by four others) all of whom had direct Canadian nuclear industry affiliations. Thus it was created by experienced but self-interested individuals.

N286.2 was used in the Darlington development, seven or so years ago. But there was little formal QA thinking during the Douglas Point development period.

QA rules define such matters as -

- designer's log books,

- design review panels,
- alternative calculation routes,
- supervision of calculations,
- internal audits and verifications,
- etc.

The document outlines management functions, performance functions, design verification, audits, and recording procedures. In practice, Ontario Hydro realizes these recommendations in mammoth multi-volume rulebooks which are submitted to the AECB at the time that a new construction licence is sought. It is not clear how directive or controlling the AECB react when they review and respond to these rulebooks. Do they encourage improvements to these submissions? Do they insist on improvements?

The AECB, in keeping with general policy, do not visit sites unannounced ("midnight raids" in the USNRC manner) to verify that QA rules are being applied. However, AECB site officers do have certain random verification prerogatives which they may or may not exercise and, if they do, they may or may not be able to competently evaluate the outcomes of these inquiries.

Implementation of the procedures with Ontario Hydro rests with a small group of engineers assigned to a unit whose work extends into other quality control and error follow-up realms. They work in a cordial manner with those whose possible failures they exist to eradicate. Unlike some of their American counterparts, they are "line" not "staff" in the Hydro hierarchy. Thus they are lateral to those they oversee rather than responsive to upper management directly. However a broadly-based and high-level committee meets twice a year to consider QA issues.

The job of overseeing the design quality of some of the biggest construction endeavours in Canada is daunting. There are literally thousands of construction drawings for a nuclear generating station. Some of these drawings, QA practitioners believe, will show errors. (For a Sudbury hospital, the oxygen pipes got connected to nitrogen sources and a number of patients died.) In the view of the QA unit, it is not practically possible to review all of them to check for mistakes.

In addition to reviews and audits, this unit takes an active view of their role. They offer training in QA to interested engineers and encourage good practices. They maintain a positive attitude towards safety. On the other hand, and perhaps inherently incompatibly, they do not conduct "midnight raids" or other paranoid (but appropriate) unscheduled audits against those whose cooperation they seek.

For the AECB and for Ontario Hydro, the QA concept is held as a “Sacred Cow.” That is, it is accepted as a necessary logical approach to checking and re-checking development. As such, it can not be critiqued and re-evaluated. Thus it is held in an esteem which is beyond criticism or even empirical test.

By contrast, one need not view the complex and weighty strictures as inviolable writ. Instead a concept of QA as a kind of “Burglar Alarm” system might be appropriate. Burglar alarms are installed by fallible people to detect other, more fallible and unwholesome, people. For burglar alarms, it is well known that they will react to false impingements and, occasionally, fail to react to burglars.

Burglar alarm systems are regularly checked for loop integrity, sensitivity, discrimination of false- from true-alarms, and faulty components replaced. Likewise, elaborate QA systems and computer spelling checkers can be tested and improved or replaced.

A certain amount of post hoc serious event study does take place within the Ontario nuclear establishment. But it tends to be rather theoretical, computer-based, and not quite in touch with the human realities of the world of work. Thus it can not easily critique specific human-factors of errors and error-reduction.

The Ontario Hydro QA group do not study the effectiveness of QA. That is, neither Ontario Hydro nor the AECB have data indicating the number of errors which are detected or which go undetected in work units adhering closely to QA rules or, should any be known, in units which pay minimum attention to these procedures. As a consequence, they can not identify those elements of the QA plan which should be strengthened and those which serve little purpose and dilute the efforts needed in other areas.

Among those responsible for QA in the Ontario nuclear establishment, there are few formal credentials. Today, university courses specifically designed for QA professionals are being offered. However, while an American Association for Quality Control exists, there is no comparable organization whose members are QA per se or Canadian.

While credentials should not be taken as certifying skill or their lack as suggesting absence of skill, credentials are a form of “audit trail” which allow the contents of a person’s mind to be traced back to certain educational exposures and perhaps some knowledge gained. Excepting those with highest responsibilities, it is not established that those who practice QA within the Ontario nuclear community have (or lack) the training which might be expected.

With some areas of specialization and within some firms, organizational backwaters — Siberia’s — may exist. It is all too easy for QA to be viewed in

that light by those who are mainline development oriented. This can happen to a QA department unless it is imbued by its organization with appropriate importance and corresponding power.

.c.Recommendations

1. It is recommended that greater empirical effort be devoted to testing the efficacy of the QA procedures now in place. Using the “burglar alarm” model may help reveal unsuspected strengths and weaknesses of current rules.

2. The independence of those implementing the procedures should be preserved with a more critical eye. In the best of cases, organizations have difficulty producing legitimate self-criticism. The problem is especially acute within Ontario Hydro. That is because Ontario Hydro has the (otherwise) favourable condition of long-term, mutually supportive personnel. Moreover, the AECB practices a “distant” style of regulation with its licencees which is combined with historical close relationships among individuals,

3. QA functions should be made staff not line; thus the organizational imperative behind QA would be more obvious and reporting channels more direct. It represents a difficult conflict of interest when an engineering group chief must balance the progress of design with the requirements of QA. By moving QA into a staff function, much of that conflict is removed or, at least, moved to a higher level within the management.

4. Professional specialty qualifications of QA staff should be assured by more objective means. This will serve to ensure that QA not become a backwater into which “surplus” or dishonoured engineers get pigeon-holed. (There is no implication that this is currently the case at Ontario Hydro.) Moreover, such an action will help defend Ontario Hydro (and the AECB) against criticism in the future.

5. The AECB should decide whether its role is to be regulator or colleague. The peculiar status of the AECB vis à vis the licencees should be resolved. It is not clear whether the AECB views its role as one of advising, controlling, overseeing, regulating, or staunchest critic.

 Quality Assurance or "QA" as used in this report relates to procedures for reducing design errors.

 Until recently, this unit was known as the Division of Building Research.

 Please see the original NRC report for references.

 “His” should be taken without specific gender connotation.

 A similar correlation coefficient arises from the Spearman Rank -Order, r=.63, and Kendal’s, t=.48.

Thanks are due for the helpful cooperation of the AECB and Ontario Hydro.

 It is outside the scope of this report to endorse or to criticize the skills of those performing QA within Ontario Hydro or the AECB. Certainly Mssrs. Massicotte and Jeppesen have years of relevant experience behind their work.

1. The term "Quality Assurance" or "QA") should be understood as relating only to procedures for detecting errors in the
of nuclear power plants.