

Reactor Safety Training for Decision Making

C. Keith Scott
Atlantic Nuclear Services Ltd.
P.O. Box 1268, Fredericton, NB, E3B 5C8

ABSTRACT

The purpose of this paper is to describe an approach to reactor safety training for technical staff working at an operating station. The concept being developed is that, when the engineer becomes a registered professional engineer, they have sufficient reactor safety knowledge to perform independent technical work without compromising the safety of the plant. This goal would be achieved with a focused training program while working as an engineer-in-training (four years in NB).

1. Introduction

The training of plant staff, other than operations staff, in reactor safety poses interesting challenges. Operations staff have a comprehensive approach to the plant and reactor safety is a part of their certification program. Technical staff are focused by discipline in their work and there are no certification requirements beyond their professional qualifications. Their knowledge of reactor safety is acquired, primarily, through work experience.

The bottom-up approach to reactor safety training through work experience has two drawbacks.

- It is a slow process and makes experience an important job qualification which may be difficult to meet; and,
- a comprehensive view is only developed after diverse work assignments ,delaying an understanding of important interfaces in the earlier years.

The management system and human resource plan can address these issues. However, with a changing demographic in the work force, a top-down training approach would have significant benefits.

The purpose of this paper is to describe an approach to reactor safety training for technical staff in an operating environment. It has three objectives.

1. To enable a person to make decisions in the course of their work that do not compromise safety. That is, to make conservative decisions.
2. To integrate the training with professional development so that objective # 1 can be met within five years of graduation from university. That is, to improve human resource planning.

3. To provide training that is generic and consistent with the time commitment for work and other training. That is, to have a cost effective training program.

Section 2 presents an analysis of the need for reactor safety training to meet the above objectives. The learning objectives for the first stage of training in a top-down approach are given in Section 3. Examples of material to be used in a classroom environment are given in Section 4.

2. Analysis

The technical support functions at an operating station are lead by graduate engineers and scientists. They work in diverse areas including: engineering, nuclear safety, system performance, maintenance, chemistry, reactor physics, fuel handling, heavy water management and procurement. Each area requires specialized knowledge and skills. New employees are assigned work in a particular area and begin developing their knowledge and competence.

The development of a professional engineer/scientist assumes the graduate brings technical knowledge to the job. Practical skills in applying the knowledge are acquired through work experience and mentoring. This professional development leads through a progression of levels of responsibility and independence in performing technical work. A standard model is summarized in Table 1. It is based on practices in New Brunswick where the P.Eng. designation is obtained after four years of supervised practical experience.

Table 1 includes a general description of each Experience Category in terms of the Job, Performance, Task Assignment and Supervision. Also, the nominal number of years to move through each category is included. The attributes form the basis for job performance measures.

In the first four years the supervisor takes responsibility for the accuracy of technical work done by the Engineer/Scientist-in-Training. Then the Specialist Engineer/Scientist 1 is expected to perform technically accurate work that is in conformance with policies and procedures subject to quality requirements. That is, the Specialist 1 is making decisions with respect to the direction and scope of work which have the potential to affect safety.

Examples of the types of decisions arising in the course of routine work that could impact safety include

- (a) A decision to request a safety review of a proposed design change because it does or does not have a potential impact on safety
- (b) A recommendation for a course of action from a technical operability evaluation.
- (c) Specifying an operating configuration for a maintenance procedure.
- (d) Establishing action criteria for an inspection procedure.

Beyond the Specialist 1 category (> 6 years experience) the technical responsibility grows with increasing independence within the management system. At higher levels of technical competence the Engineer/Scientist is functioning independently and obtaining additional technical guidance through interaction with colleagues in the external community.

The university graduate begins with limited to no knowledge of the practical aspects of reactor safety design and operation. Since the first four years of on-the-job experience are usually focused very narrowly, it is not possible to acquire an understanding of the overall safety requirements by experience alone. That is, to have the capability to answer the question, "Does this activity have any impact on plant safety?".

To give greater decision making capability at an earlier age formal training in safety is required to supplement the practical experience. Moreover, this training should occur early enough that it can be used in practical applications before moving to the Specialist 1 category.

The over-riding safety objective is to maintain the risk to the public from the operation of the plant as low as reasonably practical (the ALARP Principle). Following Reason's approach [Ref. 1] the selection of a course of action (a decision) is considered correct or incorrect according to its consequences for the public risk.

An action is considered a correct action (right decision) if it is taken on the basis of an accurate appraisal of its impact on the risk. An action is an incorrect action (wrong decision) if it is taken on the basis of an inaccurate assessment of the incremental risk.

From the above we conclude the training needs to provide knowledge of the overall safety case for the plant and how the implications of an action for the public risk can be appraised. The training should be introductory training for the Engineer/Scientist-in-Training. It should also be a foundation for focused in depth training in topical areas as the professional development continues.

The training need can be viewed as providing guidelines for individuals to apply self-checking in the course of performing technical work.

3. Design

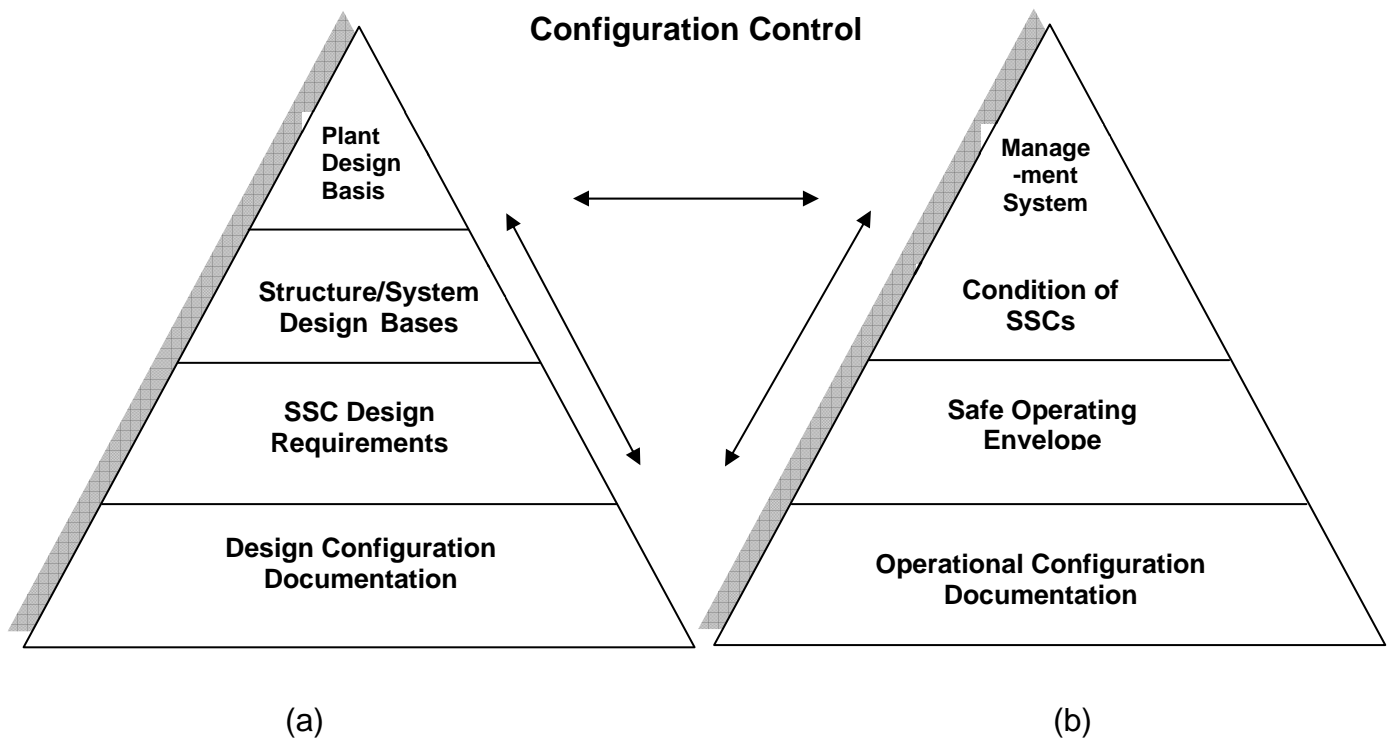
From the analysis of the need for reactor safety training, the goal is to design a course that will enable the trainee to take the correct course of action in performing work that has the potential to impact safety.

The training material should have the following features to fill the first level need and to be a foundation for more detailed development.

- (a) It does not presume extensive knowledge of the plant nor experience with the work processes.

- (b) It provides a top-down framework for knowledge of the reactor safety design that can be expanded over time with other focused training courses.
- (c) It explains the relationship between the design basis, design requirements and operational configuration.
- (d) It provides an overview of the interfaces and inter-relationships of the various work processes and programs with regard to safety.
- (e) It provides knowledge that can be used to accurately appraise the potential for an action to affect the public risk.

Given the above features, an overview of the configuration management requirements to assure safety would serve as the basis for the training. The high level elements of a configuration management program are summarized in Figure 1 [Ref. 2,3]. The pyramids indicate the increasing level of detailed knowledge that will be acquired through experience with the design and operating configurations. Configuration control is the means of assuring the public risk remains as intended according to the licensed design basis.



**Figure 1. The Essential Elements of the Facility Configuration Management Program:
(a) Design, and (b) Operation**

Based on the elements of configuration control listed in Figure 1, the training objectives are set as follows.

Objective 1 – DESCRIBE the safety design bases for the plant, structures and systems (SSCs) and how the design requirements are derived from them.

Objective 2 – EXPLAIN the safety significance of changes to design requirements and the design bases.

Objective 3 – EXPLAIN the importance of keeping the design configuration documentation up to date.

Objective 4 – EXPLAIN the importance of the Management System in ensuring quality and conformance among the elements of the configuration management program.

Objective 5 – EXPLAIN the safety significance of monitoring and surveillance of the physical condition of SSCs to ensure conformance between the physical configuration of the plant and the design requirements.

Objective 6 – EXPLAIN the safety importance of establishing the operational configuration in conformance with the design requirements.

Objective 7 – EXPLAIN how the Safe Operating Envelope is implemented to satisfy safety requirements and maximize production.

Objective 8 – DESCRIBE how safety principles and defense in depth can be used to make conservative decisions regarding risk.

4. Development

Examples of material that has been developed to meet the training Objectives 1,6,7 and 8 are presented here.

4.1 Objective 1 – Design Basis and Design Requirements

For Objective 1 the starting point is the four fundamental safety design approaches that form the licensed design basis for the plant.

1. Design to Protect the Public
2. Design for Common Cause Events
3. Design for Defence in Depth.
4. Design for Operational Configuration Control.

The linkage between the design basis and the design requirements is illustrated in the following approach to the design basis to limit public risk.

To protect the public the designer must apply two risk based design approaches:

A - the Siting Guidelines for design of the Special Safety Systems; and
 B - a probabilistic safety assessment approach for the design of the other safety related systems.

Design Basis ***A - The risk to the public from the operation of the station must be within the Siting Guidelines of the CNSC.***

The Siting Guidelines specify the single/dual failure design basis accident analysis that must be performed. The purpose is to show that the design of the four Special Safety Systems is such that in the event of an accident the radiation exposure to the public is within the prescribed limits. From this safety design basis statement the designer derives the performance requirements for the Special Safety Systems. That is, the design requirements for

- Performance capability; and
- Availability

To achieve the Siting Guideline objectives, the designer applies two design principles.

Design Principle **Only random initial failures are assumed to occur. That is, the design must be such that the initial failure does not cause other failures of process systems or Special Safety Systems.**

From this design principle, the designer derives the following functional design requirements:

- Systems must be environmentally qualified to perform under the accident conditions; and
- Systems must be separate and independent so there are no failures as a consequence of the initial event.

Design Principle **To meet the availability target there must be automatic initiation of the Special Safety systems in response to the initial accident event.**

From this design principle, the designer derives design requirements for

- Instrumentation and actuation

Design Basis ***B - A probabilistic safety assessment must demonstrate that the expected response of all systems to all credible upset transients leads to an acceptable public risk. At Point Lepreau these probabilistic safety assessments were called safety design matrices (SDMs).***

This design basis statement leads to the design requirements for

- Availability of standby safety related systems; and
- Performance requirements for safety related systems

To achieve the objective of the design basis statement the designer applies the following design principle.

Design Principle **In the probabilistic safety assessment the response of systems and equipment are based on their expected performance and reliability.**

From this design principle the designer derives the basis for abnormal plant operating procedures.

Following the design basis statements and the design principles given, the designer must specify how the derived requirements are going to be implemented in the overall plant design. The course then gives examples of how the different requirements are met. It covers

- performance capability
- separation and independence
- availability
- environmental qualification
- actuation and instrumentation

Work experience will add to the knowledge of the design requirements for structures and systems.

4.2 Objective 6 – Operational Configuration

The operational configuration is the state of the SSCs at a given time as determined by the operating and maintenance procedures. Objective 6 addresses the need to understand that for the safety design basis to be satisfied at all times, the operational configuration must be consistent with the design requirements.

To implement the operational configuration the design requirements must be identified for each 'operating state'. The corresponding procedures must then ensure the operational configuration meets the design requirements with conservative margins. Figure 2 illustrates this relationship in more detail for the configuration control elements given in Figure 1.

Design Basis	Operating States			Accident Conditions		
				beyond design basis		
Design Requirements	normal operation	anticipated transients	abnormal operation	design basis accidents	multiple system failures	severe accidents
	(a) (b)		(c)		(d)	
Operational Configuration	Operation & Maintenance Procedures			(e) APOP / EOP / Accident management plan		

- (a) Shutdown states
- (b) Operating modes other than shutdown states
- (c) Precursor accident conditions that are not serious process failures but are covered by DBA. For example, a boiler tube leak, off-normal flux shape, etc.
- (d) Beyond design basis accidents without significant core damage. For example, a loss of coolant accident coincident with a loss of Class IV power.
- (e) The accident management plan refers to station procedures for managing the accident situation after it has been brought to a controlled state via the abnormal operating procedures. This would include station management response to the accident as well.

Figure 2. Illustration of the Configuration Management Requirement for the Operational Configuration to be Consistent with the Design Requirements

4.3 Objective 7 – Safe Operating Envelope

To meet safety requirements the operational configuration must be within with the design requirements for each operating state. This limit for safe operation is the Safe Operating Envelope. Objective 7 addresses the need to implement the SOE so that both safety and production requirements are met.

Taking the SOE as the licence limit for operation, equipment impairments that take operation beyond the SOE result in lost production due to outages. To maximize production the maintenance strategy has to minimize the likelihood of operation going outside the SOE. This can be achieved by taking corrective actions before impairments challenge the SOE.

Figure 3 illustrates the maintenance strategy for impairments so the production is maintained together with a more conservative safety margin. The impairment levels are based on the levels of defence in depth.

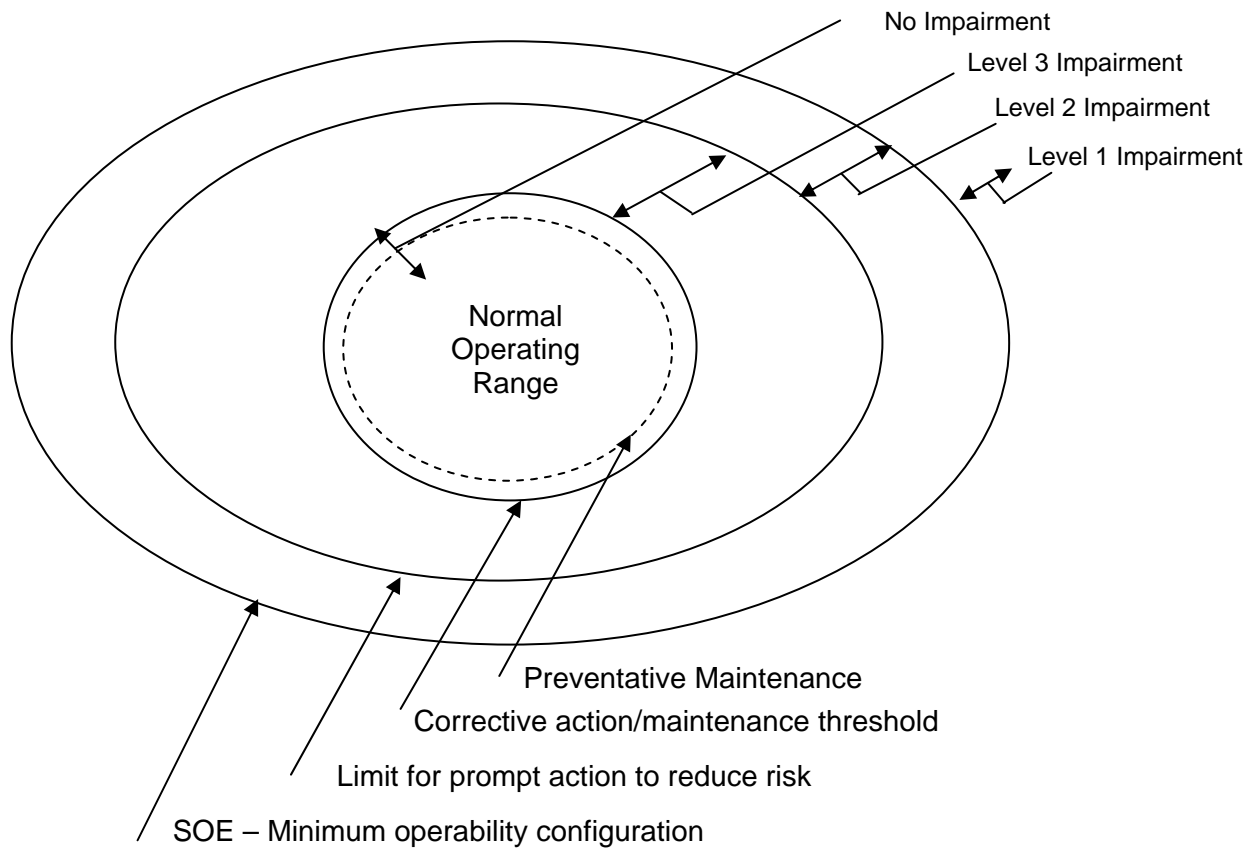


Figure 3 – Levels of Impairment and Their Operational Significance

4.4 Objective 8 – Defence in Depth

With limited knowledge it is not possible to assess the consequences of an action in terms of its impact on risk. However, it is possible to know if there is potential for the risk to be affected. Objective 8 addresses this need to assess the potential impact on risk.

The conservative approach to risk management is to maintain the five levels of defence in depth at all times. Figure 3 illustrates the levels in terms of the design requirements and the operational configuration. The trainee will develop skills in applying the defence in depth in operational scenarios through work experience.

Operating States			Accident States			Emergency Response
← 1 →	← 2 →		← 3 →	← 4 →		← 5 →
normal operation	anticipated transients	abnormal operation	design basis accidents	multiple system failures	beyond design basis accidents severe accidents	on-site off-site releases
Operation & Maintenance Procedures			APOP / EOP / Accident management plan			

Figure 4. Levels of Defence-in-Depth [labelled 1 through 5]

5. Conclusions

Course material has been used with operations staff in a classroom environment with success. The organization of design requirements as 'derivations' from the safety design basis gives them a rationale they would not have otherwise.

The same observation applies for technical staff. In the course of work, design requirements are encountered in isolation from their design basis. This makes it very difficult to assess the significance of the effect changes in one area may have in another. The top-down approach makes the linkages more apparent.

The configuration control process is an equivalent top-down approach to 'derive' the management system constraints on the conduct of technical work. It links plant ageing, safe operating envelope and design as a seamless view of safety.

6. References

1. James Reason, *Managing the Risks of Organizational Accidents*, page 73, Ashgate, 1997.
2. *Configuration Management in Nuclear Power Plants*, IAEA TECDOC 1335, January 2003.
3. *Configuration Control Process Description*, INPO AP-929, May 1998.

Table 1 - Task Assignments and Performance Expectations for Engineering/Scientific Staff by Experience Category.

<p>Engineer-in-Training / Junior Scientist 1 (<2 years experience)</p> <ul style="list-style-type: none"> • <i>Job:</i> review and summary reports, data analysis, run simulation codes, prepare design drawings and perform calculations that are not complex • <i>Performance:</i> Work is performed with direct technical supervision. • <i>Task assignments:</i> Specific work instructions are given with a description of the expected results. • <i>Supervision:</i> Technical supervisor checks work in progress and upon completion.
<p>Engineer-in-Training / Junior Scientist 2 (< 4 years experience)</p> <ul style="list-style-type: none"> • <i>Job:</i> Tasks of limited scope and complexity that require application of technical standards and the quality assurance program. • <i>Performance:</i> Work is performed independently with access to technical supervision to resolve more difficult issues and to select procedures for non-routine tasks. • <i>Task assignments:</i> Given detailed oral/written instructions as to the methods and procedures to be used. • <i>Supervision:</i> Technical Supervisor monitors progress of work and performs technical reviews of work upon completion.
<p>Specialist Engineer / Scientist 1 (4-6 years experience)</p> <ul style="list-style-type: none"> • <i>Job:</i> Tasks with specific objectives requiring investigation of a limited technical scope and addressing the interfaces with other work groups. • <i>Performance:</i> Work is performed independently to evaluate, select and apply standard engineering methods, procedures and criteria. Judgment is used to make minor adaptations and modifications to fit the task. • <i>Task assignments:</i> The statement of work is provided. The preparation of the work plan is an assigned task. • <i>Supervision:</i> Technical supervision reviews work for the soundness of approach and judgments made regarding trade-offs. The completed task would be accepted as being technically accurate and in conformance with policies and procedures subject to quality program requirements.
<p>Specialist Engineer / Scientist 2 (5-9 years experience)</p>

- *Job:* Development, planning, scheduling and coordination of the engineering work for part of a project of significant scope or a full project of limited scope. Work is conventional but includes the requirement to resolve technical issues.
- *Performance:* Work is performed independently with competence in the conventional technical aspects of the discipline/program. Broad knowledge of the work area and good knowledge of principles and practices of related disciplines / programs.
- *Tasks Assignments:* Tasks are assigned as general instructions about expected results. Required to plan, schedule and manage on time taking into account the plans of others.
- *Supervision:* Technical supervision reviews work for completeness in addressing issues and interfaces and the soundness of judgments in defining the scope of work, methods and approach.

Specialist Engineer / Scientist 3 (> 8 years experience)

- *Job:* Supervision of a work group or direction of a technical program requiring a comprehensive knowledge of the application area and a diversified knowledge of principles and practices in related work areas.
- *Performance:* Work requires detailed knowledge of a technical subject area using advanced techniques, theories or practices. Makes independent decisions regarding technical approach and methods to be used by supervised staff.
- *Task assignments:* In addition to supervisory role, tasks include modification of work processes, implementation of new approaches to address technical problems.
- *Management:* Supervisor monitors effectiveness in managing or applying technical resources to address on-going work and emergent issues.

Senior Engineer/Scientist (>10 years experience)

- *Job:* A technical expert for a particular discipline/process or program either to supervise work or to perform the work.
- *Performance:* Work requires independent complex technical work or supervision of complex projects with results of high quality. Maintains awareness of latest developments in field and uses network of peers for advice on solutions to difficult problems.
- *Task assignments:* Given responsibility for technical work packages including content, quality, cost, schedule, and interface with client.
- *Management:* Supervisor monitors technical results, cost and schedule performance in achieving management goals.

Principal Engineer/Scientist (>12 years experience)

- *Job:* Responsibility for the implementation and management of complex technical projects / programs.
- *Performance:* Work requires knowledge of international standards and best practices

for technical areas of responsibility. Maintains liaison with associations and organizations for establishing standards and addressing generic emergent technical issues.

- *Task assignments:* Project management for complex technical projects, develop management programs to address emergent design/operational issues.
- *Management:* Supervision addresses effectiveness in achieving business plan objectives.