REACTOR SAFETY REVIEW OF PERMANENT CHANGES

K. F. Lam
Technical Supervisor
Operational Compliance Section, Nuclear Safety Department
Darlington Nuclear Generating Station, Bowmanville, Ontario

1.0 INTRODUCTION AND OVERVIEW

Operational Compliance engineers review all changes as part of a change control process. Each change, permanent or temporary, is required to undergo an intricate review process to ensure that the benefits associated with the change outweigh the risk. For permanent changes, it is necessary to ensure that the proposed design meets the nuclear safety requirements, conforms to the licensing requirements and complies with regulatory requirements. In addition, during installation of the permanent change and prior to in-service, a configuration management process is in place to align the change with operating and maintenance documents.

2.0 PURPOSE AND SCOPE

The purpose of this paper is to outline the reactor safety review process to ensure that regulatory, licensing and nuclear safety requirements are met. This paper describes the overall nuclear safety review process, the role an Operational Compliance engineer in the conduct of reactor safety review of Permanent Changes and the tools available to him/her to execute the review process.

The scope of reactor safety review primarily covers three main areas:

- Review by Systems
- Review by Locations
- Review at the Interfaces

These reviews are necessary to ensure compliance with nuclear safety, licensing and regulatory requirements.

3.0 WHAT IS A PERMANENT CHANGE?

A Permanent Change is loosely defined as a change in design requirement or a change in designer's intent. Design Requirements are generally well documented in the Design Manual and cover a wide range of topics, for example, functional and performance requirements imposed overall requirements on a system; interfacing requirements imposed requirements on other systems to ensure compatibility; environmental requirements and seismic requirements imposed on specific components qualifications. Only a few of the Permanent Changes encountered during the operational phase of a nuclear power plant result in changes in design requirements. Permanent Changes which result in changes in design requirements require rigorous review to ensure validity of the design documentation and that the impacts of changes of design requirements are addressed. On the other hand, designer's intents are generally implicit and not well documented. Very often, they are considered to be good design practices by designers. Changes in designer's intent are less profound than changes in design requirements. However, with passage of time and staff changes, designer's intent may become more and more difficult to recognize and to be confirmed. For conservatism, often changes to designer's intent and/or change in design requirements are classified as Permanent Changes to ensure that the project team implements the change process through a "managed" system.

4.0 THE ROLES OF REACTOR SAFETY REVIEW OF PERMANENT CHANGES

Reactor safety review of Permanent Changes is intended to fulfill a number of safety and licensing objectives that include, among others, three key areas:

- To comply with the legal requirements prescribed in the Power Reactor Operating Licence.
- To demonstrate reactor operation within safe operating envelope defined by the station's Operating Policies and

Principles. Where changes in safe operating envelope are necessary, such changes meet public safety criteria and are approved by the regulatory body.

- To ensure the documentation associated with the Permanent Changes that impact on nuclear safety is followed up through a "managed" process.

Another important role of the reactor safety review is to outline deficiencies in the Permanent Change if nuclear safety, licensing or regulatory requirements are not met, and to suggest design solutions, where appropriate, to meet these requirements.

4.1 To Comply With The Legal Requirements

The first key area is fulfilled by ensuring that all Permanent Changes which require regulatory approval are submitted to the AECB prior to implementation. The requirements for regulatory approval are explicitly defined in, but not limited to, the Power Reactor Operating Licence. For example, regulatory approvals of temporary and permanent changes are stipulated in the station's Operating Policies and Principles. In addition, regulatory approvals are sometimes required prior to design or procedural changes of certain equipment which are regulated federally or provincially. The requirements for regulatory approvals are described in applicable Codes and Standards which have been adopted as statues. Operational Compliance engineers must decide correctly the need for regulatory approval and the reasons for making that decision. It is undesirable to seek regulatory approval of changes that might require AECB approval as opposed to changes that shall require approval, although it may be a temptation to do so. To request regulatory approval of a Permanent Change that does not require AECB approval not only adds unnecessary work loads to the AECB staff, but also results in unnecessary delays in implementation as well. A tool that guides Operational Compliance engineers to make correct decisions is listed in Figure 1. Permanent Changes in areas that require AECB approvals are flagged.

Currently, Permanent Changes that require AECB approval can be loosely divided into three main types:

Protocol Approval. The requirement for prior AECB approval is specifically stated in the Power Reactor Operating Licence or stipulated in the Operating Policies and Principles. Permanent Changes in the following areas require AECB approval.

- Special Safety System
- Reactor Regulating System
- Fuel Design
- Nuclear Safeguards related to IAEA equipment
- Station's Physical Security
- Use of Land within the Station's Exclusion Zone

Jurisdictional Approval. The requirement for prior AECB approval is stipulated in the applicable Codes and Standards, for example, changes in System Code Classification (SCL). SCL is a tabulation of safety related systems describing their nuclear and non-nuclear code classes approved by the AECB. Code Class designation is generally based on the radioactivity content, pipe size and the consequences of failure. Since AECB is the primary jurisdictional body for nuclear power plants, certain jurisdictional approvals require concurrence from the AECB.

Regulatory Approval. AECB approval is required for Permanent Changes which could significantly and adversely affect the assessment of public risk as stated in the current licensing submissions. Operational Compliance engineers are required to exercise reasonable judgement, based on a cursory review of the impacts of Permanent Changes on nuclear safety, to decide whether additional safety assessment is required to demonstrate compliance.

4.2 To Demonstrate Reactor Operation Within Safe Operating Envelope

The second key area is satisfied by performing a safety assessment to demonstrate that the Permanent Change does not result in reactor operation outside of the Safe Operating Envelope (SOE). Safe Operating Envelope is that regime of station operation where the risk to the public resulting from station operation is considered by the AECB and Ontario Hydro to be acceptable. The boundary is defined by various licence conditions, operating limits resulting from safety analysis, with assessment from other sources. This assessment is executed through a step by step process which involves understanding the safety related function at the system/component level, nuclear safety design requirements of the system/component, and the impact of Permanent Change on safety analysis. In some cases, Permanent Changes are accompanied with changes in the SOE boundary. Deterministic and probabilistic risk assessment are required to redefine the SOE. AECB approval would be required.

4.3 To Ensure The Documentation Alignment Through A "Managed" Process

The last key area is to ensure the configuration management process is well in place for Permanent Changes that have nuclear safety implications. This step is important to ensure compliance prior to installation and in-service of the Permanent Change. A simplified checklist is provided in Appendix A to facilitate the review process. Additional assessment is required when a Permanent Change indicates certain nuclear safety, licensing and regulatory requirements have to be complied with.

5.0 THE REACTOR SAFETY REVIEW PROCESS

For administrative purpose, the reactor safety review can be loosely divided into three steps.

5.1 Step 1 - Subject Classification

All Permanent Changes are sorted by Subject Classification Index (SCI). SCI is a categorization of subjects and subsystems by numbers. Systems, components and the associated instrumentation and controls are provided with corresponding identification numbers to define the system boundary. The use of SCI allows all changes to the Special Safety Systems (SSS) and Reactor Regulating System (RRS) be readily identified so that these changes are flagged and submitted to the AECB for protocol approval in accordance with the licensing requirements and as required by the Operating Policies and Principles. In addition, Permanent Changes on other standby safety systems (see Appendix C), whose unavailability is monitored, receive a thorough review. Other safety-related systems can be reviewed based on the safety credits they were provided. A safety related system is one by virtue of its failure would result in radiological consequences to the public. Therefore, safety related systems constitute a very large group of systems in the nuclear power plant. Safety credits are design provisions, assumptions, initial conditions or operator actions which were assumed in the safety analysis or built into the accident scenarios. Deviation from these conditions may have significant effects on the frequency of initiating events or radiological consequences of postulated accidents. Non-safety related systems do not require a nuclear safety review related to its system design. However, all permanent changes are reviewed with respect to their locations and interfaces to confirm with safety assumptions employed in the safety analysis.

An additional advantage to use SCI to classify Permanent Changes allows Operational Compliance engineers to focus on changes on safety related systems and to decide on the need of AECB approval based on the work sub-packages within the scope of the Permanent Change.

5.2 Step 2 - Preliminary Review:

A preliminary review of each Permanent Change includes three parts:

5.2.1 Review The Impact Of The Permanent Change By System Requirements. The review focuses on the impact of the Permanent Change on the system level. Based on the system SCI in Step 1, an Operational Compliance engineer is able to ascertain the type of systems which the Permanent Change associates with.

For Special Safety System and Reactor Regulating System, the approval of Permanent Change is mandatory as stipulated in the station's Operating Policies and Principles. From a safety assessment perspective, it is imperative that the Permanent Change has no adverse effect on both the system's performance and reliability or the adverse effects were evaluated and found to be acceptable. A design requirement of the Special Safety System is that its unavailability requirement should be no greater than 0.001 yr./yr. This unavailability requirement is stipulated in R-7 [1], R-8 [2] and R-9 [3] and is assumed in the safety analysis. Therefore, any adverse effect on the system performance and unavailability as a result of the Permanent Change should be quantified to conform with safety analysis and licensing requirements.

For Standby Safety Systems other than the Special Safety Systems, it is necessary to demonstrate that the Permanent Change does not exceed their prescribed unavailability targets. It is important to note that the frequency of occurrence of postulated accidents coincident with Standby Safety System failure is a criterion for assigning dose class which forms the basis of acceptance by the regulatory body [4]. Therefore, Permanent Change that results in adverse effect on system performance or reduces the system reliability should be substantiated to ensure consistency with safety analysis.

For safety related systems other than the Standby Safety Systems, it is necessary to assess the impact of the Permanent Change on nuclear safety requirements. This require an Operational Compliance engineer to review the system's design manual and to scope the safety credits related to the change. Where a Permanent Change results in a change in Design Manuals or Operating Manuals, a detailed assessment would be required to ensure continued alignment of design and operating documentation.

Questions generally asked to guide an Operational Compliance engineer in the conduct of a reactor safety review of safety related systems focus around the impacts of the Permanent Change on reactor's ability to control reactivity, to cool fuel and to contain radioactivity. For example, does the Permanent Change has any adverse effects on:

- the shutdown capability of the reactor?
- the regulating function of the reactor?
- the Guaranteed Shutdown State?
- the primary, backup, shutdown or emergency heat sinks?
- the containment envelope?
- separation at division, system or group level?
- the claimed system availability?

For Permanent Changes in non-safety related systems, a review by system requirements is not needed because these systems do not have any safety related function. Reactor safety review is therefore, confined to outside, rather than inside, of the system boundary. However, reviews by location and at the interface are required to confirm that the safety credits claimed in the safety analysis continue to be provided.

5.2.2 Review The Impact Of The Permanent Change By Location. This review aims at the requirements generally at the component level as a result of certain design basis accidents postulated to occur by virtue of its location. Environmental qualification and seismic qualification are important considerations. For this reason, it should be noted that addition of a new component not qualified for the environmental or seismic requirements or modification of an existing qualified component in that area represents a new nuclear safety hazard. It is essential that environmental or seismic qualifications of components where credited in the safety analysis continue to be valid after they are modified, and new components added in a seismic qualified area must be assessed or requalified to preserve its safe operating envelope.

A list of design basis accidents related to environmental conditions are provided in Appendix B.

The following questions are prompted by an Operational Compliance engineer during review of Permanent Changes in certain locations. For example, does the Permanent Change has any adverse effects on:

- station's ability to cater for common mode events?
- system alarm/annunciation including beetles for leak detection, fixed area gamma/tritium monitors etc.?
- seismically qualified components?
- environmentally qualified components including flood and steam barriers?
- the accessibility of certain equipment whose operation is credited during abnormal incidents?

It is important to recognize that a change of pipe size or valve configuration may have profound implications to the postulation of design basis accidents in certain locations. For example, an increase in pipe size may result in larger break discharge exceeding the assumed values in the safety analysis. Change in valve configuration could result in different manual or automatic actions in response to different design basis accidents. Consideration should be given to locations where accessibility is restricted during normal power operation or following an accident.

5.2.3 Review The Impact Of The Permanent Change On Interfacing Components. This review ensures that the system and component interfacing requirements continue to be compatible with the Permanent Change. This is an important consideration when a Permanent Change results in a change in boundaries associated with Nuclear Code Class, containment or seismic qualification. Nuclear Code Class refers to the designation described in the ASME Boiler and Pressure Vessel Code Section III and CSA Standards N285.0 [5]. A change in system operating pressure, due to a change in pressure relief valve setting, a change in the pressurizing pump, or a change in the pump/valve controls could result in significant changes in a large number of interfacing components.

A review of the interfacing requirements of the system's design manual is an important step to scope the impact of a Permanent Change on its interfacing systems.

Generally, there are several interfacing conditions the project team and designers have to contend with during design execution of Permanent Changes.

Physical Interface. This is the interface through physical contact in which force and moment, electric current, conductive heat transfer etc. take place. Therefore, where Permanent Change results in significant changes in physical interface, a detailed assessment would be required to address the impact on reactor safety.

Questions generally asked by an Operational Compliance engineer focus around the effects of Permanent Changes on physical interface include the following: Does the Permanent Change result in:

- a significant increase in loads on floor or wall, particularly when drainage, curb or louvers are altered?
- a significant change in loads of the adjacent components?
- a change in the ASME service level?
- a change in operating/design temperature, pressure and mass flow? If so, what are the effects on piping flexibility analysis and equipment rating?
- a change in the operation of any of the heat sinks (primary, backup, shutdown or emergency)?
- a change in equipment loading of interfacing system components such as nozzles, expansion joints, supports etc.?

Instrumentation and Controls Interface. This is the interface in which a parameter is monitored or controlled for manual or automatic actions. Any change in instrumentation and controls interface should be addressed in the detailed assessment to ensure satisfactory operability.

An Operational Compliance engineer would ask:

- Do the instrumentation and controls requirements meet the (process) design intent?
- Do the instrumentation and controls meet the separation requirements outlined in the Nuclear Safety Design Guides?

Supporting Services. These are the services that support the operation of a system or equipment. Examples include: service water, instrument air, electrical power, heating, ventilation and air conditioning, drainage and venting etc. The requisitioner of the supporting services should communicate with the services provider to ensure the change in services can be accommodated by the supporting systems. Any significant change in the supporting services should be reviewed by the System Responsible Engineer of the services to ensure that such change does not result in a significant change in system performance and reliability. For example, a significant increase in service water demand may result in an overall pressure drop such that the water consumption in certain critical equipment may be cutback below its minimum requirement necessary to meet its safety function. The role of an Operational Compliance engineer is to confirm with the System Responsible Engineer that he/she has reviewed the change in supporting services, accepts the new requirements and that there is neither adverse effects on system performance nor degradation in system reliability. Questions generally asked by an Operational Compliance engineer include:

- Does the class of electrical power provided to the new equipment meet the nuclear safety requirements?
- Does the change have any adverse effect on the electrical load to a bus or cable tray carrying critical nuclear safety services ?
- Does the change necessitates any change in settings of electrical relay/switches to protect the associated equipment?
- Has the change supported by other plant services such as service water, instrument air, heating and ventilation, drainage and venting etc.?

Human Factors Interface. This is the interface between the operator/plant worker and the equipment. The following 4 types of Permanent Changes should be addressed in detailed assessment.

- Change in control panel or consoles
- Change that could be altered by improper operator action
- Change that could be altered by improper maintenance activities
- Change that accompanied with complicated operating procedures

5.3 Step 3 - Detailed Assessment

A reactor safety review of a Permanent Change requires a detailed assessment if the preliminary review shows that a more in-depth review is needed to ensure that AECB regulatory requirements, licensing requirements and nuclear safety design and operating requirements are met. This review process is normally performed in conjunction with the project leader and the designers, and is often supplemented by a field tour to familiarize with the field conditions. Additional analysis, where required, are requested to support the Permanent Change. When deficiencies in the Permanent Change are noted, design solutions, where appropriate, are suggested by an Operational Compliance engineer to the project team for consideration.

The following includes a list of items to be considered during a detailed assessment. This list is not exhaustive but intended only as a guide for Operational Compliance engineers in the conduct of a detailed assessment.

5.3.1 Changes Affecting Safety Analysis or Data Set. An Operational Compliance engineer has a role to ensure that Permanent Changes do not affect the safety analysis envelope generally covered in the Safety Report and licensing submission.

To facilitate this process, an Operational Compliance engineer has to review the safety related functions of the existing design, to compare with the Permanent Change and to identify changes, if any, in the analysis assumptions or data set so that the safe operating envelope is preserved.

To maintain the safe operating envelope, it is necessary to demonstrate that the Permanent Change does not result in hazards of a different nature not identified in the safety assessment, a higher frequency of failure than predicted in the safety assessment, or higher radiological consequences than previously predicted in the safety analysis.

To comply with these restrictions, an Operational Compliance engineer is required to review the safety related function of each system affected by the Permanent Change and to ensure that their safety credits demanded by the safety analysis are either not changed or diminished. This review process includes, among others, to confirm the safety parameter, system conditions or equipment involved; to confirm relevant design basis accidents; to confirm the limiting accidents and the appropriate safety criteria; and to ensure that the bounding values required to meet the safety criteria for limiting accidents are not affected. Any change in safety credits would result in a change in safe operating envelope and additional effort are needed to implement further changes in safety analysis and operating documents.

For Permanent Changes in Standby Safety Systems, it is necessary to ensure that:

- the replacement components have the same or better component reliability. Critical components such as pumps, heat exchangers and valves are provided with the same degree of redundancy or better unless a reliability assessment is provided to support that a lower component redundancy is acceptable.
- the quality assurance for the replacement or new components are compatible with the existing ones.
- failure indications to annunciate component failure, though not part of the control function, is not impaired by the Permanent Change.

Where Permanent Changes are made to alter the safe operating envelope, an assessment should be made in support of this change to demonstrate the change in safety analysis assumptions, safety credits and radiological consequences. Such change would normally accompanied with a change in licensing documentation and operating documents.

Apart from the deterministic assessment, an Operational Compliance engineer is required to refer to risk assessment documents to ensure that the licensing basis is preserved or additional risk assessment has been included to support the Permanent Change.

5.3.2 Changes In Nuclear Code Class System. A Permanent Change in a Nuclear Code Class System often results in a change in Code Class or boundary. There are three distinct situations for changes in a Code Class System:

- a shift in Code Class boundary while the Code Classes on either side of the boundary are not changed.
- a change in Code Classification while the Code Class boundary is not changed.
- An extension of or a deletion from a section of a system while the Code Class boundary is not changed.

In some cases, a Permanent Change involves more than one of the above cases or a combination of the cases above.

For Permanent Changes on Nuclear Code Class Systems, changes on the following three documents, if any, have to be ascertained.

- System Classification List (SCL)
- Consequences of Failure (CoF) statement
- Over-pressure Protection Report (OPPR)

An Operation Compliance engineer has to confirm with the system designer that a change in Code Class System is consistent with the SCL and that the CoF statement and OPPR continue to remain valid. Any change in SCL, CoF or OPPR would require a submission to the regulatory body to amend these documents and to substantiate that the changes are acceptable.

Where a Permanent Change results in a modification of an existing nuclear Code Class system, an assessment is needed to determine whether the change is considered "major" or "minor" [5] within the context of CSA N285.0. When a modification is accepted by the regulatory authority as "minor", it may be made to the same class as the original system and to the same or later issue of the Standards. For "major" modifications, the design and construction requirements are similar to a new system and is governed by the current issue of the Standards. Depending on the nature of changes, AECB concurrence may be required for Permanent Changes classified as "major" or "minor" modifications.

Where a Code Class boundary is associated with a containment or seismic qualification boundary, extra caution must be exercised to ensure that the component functions satisfy the seismic, containment and Code Class boundary requirements. These requirements are stipulated in Nuclear Safety Design Guides and AECB Regulatory Requirement R-7.

Where the change in Code Class boundary also results in a change in assured status of containment boundary valve, the operational flowsheets, operating manuals and the Valve Position Assurance Program database have to be updated to reflect this change.

5.3.3 Changes In Pressurized Systems. Pressurized systems for non-safety related systems are governed by the provincial body (i.e., Ontario Ministry of Consumers and Commercial Relations). For safety-related systems, both the provincial body and the AECB have jurisdictions on pressurized systems.

Where a Permanent Change results in a change in operating pressure or temperature or a change in pressure boundary, it is necessary to document these changes in both design and operating documents.

The role of an Operational Compliance engineer is to confirm with the system designer to ensure that the design is registered with, and approval granted by the regulatory body prior to implementation. In addition, since the change in one pressurized system may have effects on the interfacing systems outside the SCI boundary, Operational Compliance engineer has a role to review the interfacing systems and to confirm that accommodating actions are taken to align with the change.

5.3.4 Changes Involving Building Codes. Conformance to Building Codes is required for all architectural modifications. Examples include:

- change/deletion of fire door/wall
- change/addition/deletion of ladders or handrails
- addition of field office
- addition/deletion of entrance/exit
- addition of a new building or extension of an existing building

Power Reactor Operating Licence requires that all laws of general application in the Province of Ontario are applicable to and in respect of the nuclear facility and must be complied with, except to the extent that such laws are in conflict with any applicable federal statue, order, rule or regulation. Therefore, civil engineers or architects should be consulted to ensure conformance to applicable Building Codes.

As indicated previously, the layout of a nuclear power plant is governed by three levels of government. Building Codes and Fire Codes are administered by the province and the municipality. Physical Security Regulations and Radiation Protection Regulations are governed federally by the Atomic Energy Control Board. Operational Compliance engineers should ensure that where conflict arises in these jurisdictions are reconciled by the project leader.

Of particular interest is the access and exit requirements stipulated by these governing documents. By virtue of the nature of their intents, these documents are, in some cases, in conflict with one another. For example, to limit access to meet Physical Security Regulations may, in some cases, contravene the Fire Codes. The intent of Fire Codes is to allow rapid egress in the event of a fire while the Physical Security Regulations prohibit access, and therefore exit, of unauthorized personnel.

Another important consideration in change in station layout is partitioning in high Radiological Zone Areas. A role of Operational Compliance engineer is to prompt designers to assess the effects of partition on radiation protection and ventilation air flows. Alteration of station layout at or near radiological zone boundary has to be reviewed by Health Physics to ensure compliance with Radiation Protection Regulations. Ventilation flows as a result of change in layout or partitioning change have to be confirmed by a ventilation engineer to ensure compliance with Radiation Protection Regulations which prohibit normal air flow direction from high Radiological Zone Areas to low Radiological Zone Areas.

5.3.5 Changes Involving Reconciliation Of AECB Regulatory Documents. Power Reactor Operating Licence requires the operating requirements for the special safety systems to comply with AECB Regulatory Documents R-7 [1], R-8 [2] and R-9 [3]. In addition, the design of the nuclear power plant shall comply with the Nuclear Safety Design Guides. Where the design cannot comply with the Nuclear Safety Design Guides but the intents of these guides are complied, the designer is required to file a Design Guide Exception to document the rationale why such deviation is needed, for example, due to no viable alternatives.

Another area of important consideration is the Permanent Changes on Primary Heat Transport (PHT) Systems. AECB Regulatory Document R-77 [4] sets the service limit requirements for PHT systems during normal, abnormal or accident conditions including design basis accidents prior to and following shutdown system trips. Permanent Changes on PHT systems should be assessed to ensure continued compliance with this Regulatory Document.

Where the AECB Regulatory Documents impose unnecessary restrictions on the design and operation of a special safety system, containment boundary devices or PHT systems, prior approval should be obtained from the regulatory body before detail design is executed.

The role of Operational Compliance engineer is to confirm with the system designer that Permanent Changes that might be in conflict with AECB Regulatory Documents and Nuclear Safety Design Guides are reconciled and the basis for deviation from these documents are justified prior to station's approval of the Permanent Change.

In the reconciliation process, an Operational Compliance engineer has to ask two important questions:

- Does the Permanent Change meet the design requirements?
- Are the design requirements appropriate?

The first question addresses the Permanent Change to ensure that the established design requirements continue to remain valid after the Permanent Change. However, as a result of further understanding of the system requirements that give rise to the Permanent Change, it would also be appropriate to address the latter question, i.e., validity of the design requirements. Where a change in design requirement has emerged, it is necessary to capture the impact of these new requirements on the affected systems to ensure compliance with the new requirements.

5.3.6 <u>Changes That Result In Change In Environmental Qualification Functions</u>. When a Permanent Change affects the environmental qualification function of a system or component, it is necessary to understand the rationale of the change and the scope of change. Environmental Qualification function is the capability requirements of the system or component rather than the documented evidence of the device.

The parameters generally considered in the formulation of environmental qualification functions of safety related components include: temperature, pressure, humidity, radiation, immersion or water spray, vibration and corrosion. Therefore, Permanent Changes to rooms that are equipped with flood-proof or steam-proof barriers, special ventilation and cooling systems to provide the environmental qualifications of the equipment contained therein should be reviewed in detail to ensure this environmental qualification function continues to be met.

If a Permanent Change imposes a more harsh environment on a safety related system or component than its capability as evidenced in the qualification document, it would be questionable whether the system or component would be able to fulfill its safety roles to mitigate the radiological consequences.

Where a Permanent Change results in environmental conditions more harsh than the environmental qualification conditions, three approaches can be taken to put the design within the safe operating envelope:

- Improve the environmental conditions so that the test conditions in the qualification program would be conservative (i.e., more harsh). This approach requires a change in the proposed design or additional safety analysis to meet the environmental qualification requirements.
- Requalify the equipment so that the environmental conditions anticipated in the design is less harsh than the test conditions in the qualification program.
- Reanalyse the postulated accidents by removing conservative assumptions or refining the methodology of the safety analysis so that the environmental conditions following the accidents would be less harsh than the test conditions in the qualification program.

The role of Operational Compliance engineer is to confirm with the system designer that the environmental qualification requirements are less harsh than the qualification (i.e., documented evidence) of the system or components. Where the environmental qualification requirements exceed the capability of the system or component, at least one of the approach has been employed to reconcile the design and the qualification program. The Environmental Qualification of Safety Related Component List (EQSRCL) is an important tool to facilitate this review process.

5.3.7 Changes Requiring Seismic Assessment. When a Permanent Change involves an addition of a new equipment or a change in an existing seismically qualified component within a seismically qualified area, there is a need to review the effects of these changes to ensure continued compliance with the nuclear safety requirements.

For a seismically qualified system, it is essential that its safety related functions continue unimpeded by the Permanent Change. This requires that any modification that could affect the performance of an existing seismically qualified components has to be requalified. Depending on the extent of the Permanent Change, documented evidence is required to support this claim.

For non-safety related systems within a seismically qualified area, it is necessary to demonstrate that the new components added in the Permanent Change are securely anchored such that they do not fall down during or following a seismic event. This process requires the component to be seismically qualified by design. An alternative approach is to conduct a field tour to ensure that the non-seismically qualified, non-safety related components do not cause any damage to the safety related components below. Generally, a 1.7m (5 ft.) corridor and 0.35m (1 ft.) below seismically qualified components are considered adequate for this purpose. Failure of non-seismically qualified component is not expected to create a hazard to seismically qualified components beyond these distances.

5.3.8 Changes Requiring Additional Loading Analysis. Permanent Change may result in a change in either static or dynamic loading (or both) on adjacent components. Static loads may arise due to, for example, equipment dead weight, thermal expansion, pressure forces due to change in area (such as increaser or reducer) or change in direction (such as pipe elbows), loads due to natural elements etc. Dynamic loads may arise due to, for example, vibration, pump starts or trips, pipe flow, waterhammer, seismic loads, design basis accident conditions such as pipe breaks etc.

Operational Compliance engineers should confirm with designers that all loads arising from equipment or piping as a result of the Permanent Change are communicated and accepted by the equipment or piping engineers. Since all loads eventually are supported by floor and wall, it is therefore necessary that these loads are communicated and accepted by the civil engineers as well. Where a Permanent Change may result in a higher fluid integrated discharge or discharge rate, the resultant effects on wall and floor loads should be assessed to ensure structural integrity.

5.3.9 Changes Involving Stress Analysis. Permanent Change may require additional stress assessments if the assumptions employed in the stress analysis are altered. These assumptions include component geometry, material properties, operating temperature and pressure, stress concentration factor, fatigue usage, stress intensity etc.

Where a Permanent Change results in a change in the above parameters that would adversely affect the component performance, it is necessary that the project leader be apprised of the impacts on component durability. If there is significant doubt on component durability as a result of the Permanent Change, the applicable stress analysis document should be reviewed for clarification. Two approaches may be taken:

- Amend the stress analysis document to demonstrate component durability to suit the operating conditions of the Permanent Change.
- Revise the Permanent Change to preserve the assumptions of the stress analysis.

The role of Operational Compliance engineer is to confirm with the system designer that the Permanent Change is consistent with the assumptions employed in the stress analysis to ensure continued compliance and that the basis of deviations from the design conditions are justified.

5.3.10 Changes Involving Safety Report Update. Some Permanent Changes when implemented result in a change of the description or safety analysis stated in the Safety Report. An Operational Compliance engineer should review the extent of each Permanent Change by assessing the nuclear safety role of the system/component in the overall defense in depth strategy and by assessing the effect of the change, particularly on the safety credits the system/component contributes to specific postulated accidents.

Where a Permanent Change results in a change in the safety analysis, two approaches can be taken to maintain consistency:

- Recommend design provisions or procedural changes in the Permanent Change so that the safe operating envelope is preserved.
- Where Permanent Change results in a net change in Safe Operating Envelope, an Operational Compliance engineer should ensure that such change is communicated to the appropriate work groups for action to align with the Permanent Change.

Where the change in description or safety analysis is considered of minor nature with respect to the Safe Operating Envelope, the required change are recorded to facilitate future Safety Report updates.

6.0 CONCLUSION

Reactor safety review at Darlington Nuclear Generating Station is a well-managed process. The "thought process" includes a flowchart (Figure 1) and checklist (Appendix A) which assist Operational Compliance engineers to execute the review process. Operational Compliance engineers were trained in the overall station defense in depth design provisions, safety analysis interfacing process, safety credits that tie into the safe operating envelope as this Permanent Change review process was put in place. Since mid 1994, several hundreds of Permanent Changes had been processed. During the project design execution, Operational Compliance engineers provide guidance to project leaders and designers to assist them to comply with the nuclear safety, licensing and regulatory requirements. There has been no OP&P non-compliance due to inadequate Operational Compliance review since the reactor safety review process was implemented.

7.0 REFERENCES

[1] AECB Regulatory Document R-7: "Requirements for Containment Systems for CANDU Nuclear Power Plant", issued February 21, 1991.

[2] AECB Regulatory Document R-8: "Requirements for Shutdown Systems for CANDU Nuclear Power Plant", issued February 21, 1991.

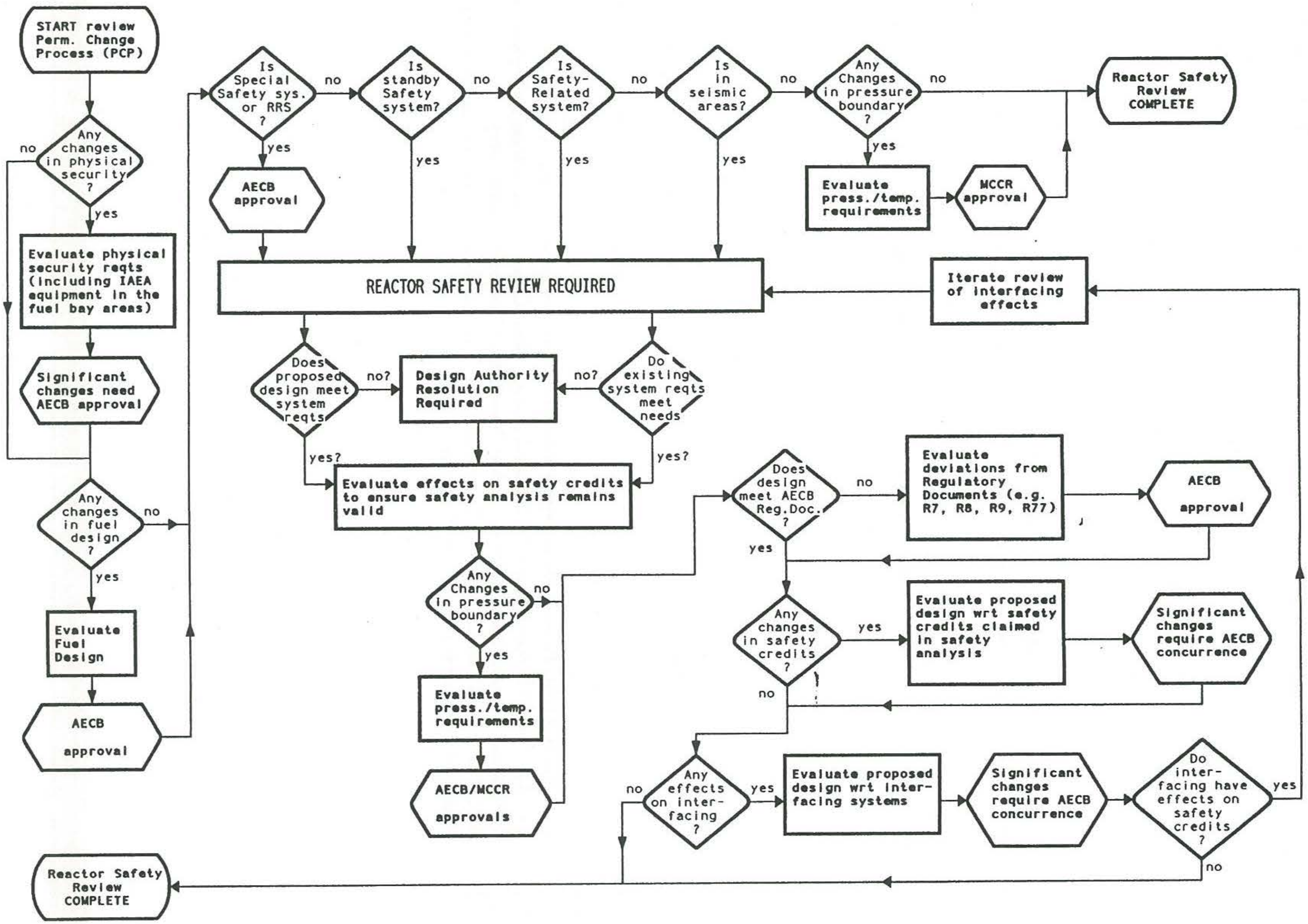
[3] AECB Regulatory Document R-9: "Requirements for Emergency Core Cooling System for CANDU Nuclear Power Plant", issued February 21, 1991.

[4] AECB Regulatory Document R-77: "Over-pressure Protection Requirements for Primary Heat Transport Systems in CANDU Power Reactors Fitted with Two Shutdown Systems", issued October 20, 1987.

[5] Canadian Standards Association CSA Standard N285.0-M95 "General Requirements for Pressure Retaining Systems and Components in CANDU Nuclear Power Plants" issued November 1995.

[6] AECB Consultative Document C-6: "Requirements for Safety Analysis of CANDU Nuclear Power Plant", (Proposed Regulatory Guide) issued for comment 1980.

Figure 1 Reactor Safety Review Process for Permanent Changes



APPENDIX A

Does this Permanent Change result in any of the following?

- ☐ Change to a Special Safety System or Reactor Regulating System.
- ☐ Change to a safety related system or major process system that might reduce its reliability or degrade its performance
- ☐ Change to components that might degrade its safety related function as defined in the Environmental Qualification of Safety Related Component List (EQSRCL).
- ☐ Change the description or analysis in the Safety Report.
- ☐ Change the fuel design or change that might degrade the safety related function of the fuel handling process functions.
- ☐ Change to station security (safeguard, access control, security barrier).
- ☐ Change to the Operating Policies and Principles.
- ☐ Change to a pressure, seismic or containment boundary (within a system) for which the system or component has been registered.
- ☐ Change or addition of equipment in a seismically qualified location.
- ☐ Introduction of combustible or hazardous materials or reduction in personnel/equipment accessibility.

APPENDIX B

Design Basis Accidents imposing environmental qualification requirements on system and components

Common Mode Events
Common Environment (Toxic Gas release)
Turbine Disintegration
External Explosion
Earthquake (DBE)
- only DBE qualified equipment survives.
- the effect of operation or failure of unqualified equipment are postulated on the basis of experience data

Earthquake (SDE)
- Earthquake (SDE) occurring 24 hours or more after LOCA.
- Only SDE or DBE qualified equipment survives.
- The effect of operation or failure of unqualified equipment are postulated on the basis of experience data.

Severe Atmospheric Conditions
Design Basis Tornado
Extreme Temperatures
Extreme Snow load
Hydrogen Explosion in the Tritium Removal Facility

Design Basis Accidents other than Common Mode Events
Loss of Coolant Accidents
- components inside reactor vaults as per environmental qualification envelope

Steam and Feedwater System Failure
- components inside the Powerhouse as per environmental qualification envelope

Random Pipe Failures
- including flooding caused by pipe ruptures

APPENDIX C

Standby Safety Systems are those systems specifically designed to minimize the risk of or to reduce the consequences of an "initiating event" or a reactor accident.

Standby Safety Systems include:

Special Safety Systems

	Function
Shutdown System I (SDS1)	Shuts down reactor using shutoff rods
Shutdown System II (SDS2)	Shuts down reactor using poison injection
Emergency Coolant Injection System (ECIS)	Cools reactor fuel following a loss of coolant accident
Negative Pressure Containment System (NPCS)	Contains radioactivity from releasing to the environs

and

	Function
Emergency Power Supply System (EPS)	provides electrical power to station services following a seismic event
Standby Class III Power Supply System (SBC3)	provides electrical power to station services following a loss of bulk electrical supply
Shutdown Cooling System (SDCS)	provides fuel cooling following reactor shutdown (without primary heat transport pumps)
Inter-Unit Feedwater Tie (IUFT)	provides feedwater supply to boilers from another unit's deaerator water tank
Emergency Steam Generator Cooling System (SGECS)	provides short term seismically qualified feedwater supply to boilers
Emergency Service Water (ESW)	provides a long term seismically qualified service water supply to station equipment
Powerhouse Steam Venting System (PSVS)	protects powerhouse equipment in the station from harsh environment following a steam or feedwater line break
Post Accident Monitoring System (PAMS)	provides instrumentation for monitoring the reactor status and critical parameters following an accident