IYNC 2008
Interlaken, Switzerland, 20 – 26 September 2008
Paper No. 408

Implementation of an Improved Safe Operating Envelope

Robyn Prime[1], Mark McIntyre[2], David Reeves[2],
[1]NB Power Nuclear, P.O. Box 600,Lepreau,NB,Canada;
[2]Atlantic Nuclear Services Ltd.,PO Box 1268 Fredericton, NB, Canada
rprime@nbpower.com

ABSTRACT

This paper is a continuation of the paper presented at IYNC 2004 on "The Definition of a Safe Operating Envelope". The current paper concentrates on the implementation process of the Safe Operating Envelope employed at the Point Lepreau Generating Station.

1 INTRODUCTION

The Safe Operating Envelope (SOE) refers to the set of limits and conditions within which the station must be operated to ensure conformance with the safety analysis upon which reactor operation is licensed and which can be monitored by or on behalf of the operator. Point Lepreau Generating Station (PLGS) has recognized that the safest nuclear plants are also the most economic (from a long-term investment point of view). This realization was the impetus for instituting the improved SOE process. A properly implemented SOE plays a key role in achieving the goal of safe and reliable operation by avoiding costly, unplanned outages due to unrecoverable threats to safety.

It has become apparent that the optimum time to implement the SOE is the period directly prior to a series of new safety analyses, such as prior to the Refurbishment of CANDU plants, as is the case with PLGS. This provides a consistent basis to ensure that safety analysis limits bound all normal operating characteristics.

2 TECHNICAL SPECIFICATIONS VERSUS THE CANADIAN APPROACH

The international approach to SOE is to use Technical Specifications (Tech Specs). At a benchmarking meeting with representatives from all utilities of the Canadian industry, a conscious decision was made to develop and adopt the "Principles and Guidelines for the Definition, Implementation and Maintenance of the Safe Operating Envelope at CANDU Nuclear Power Plants". This document was produced by the CANDU Owners Group (COG). The fundamental difference is that Tech Specs provide both the SOE definition and operational compliance framework. The Canadian industry has established a well defined and effective compliance framework and has taken credit for that framework in the Canadian approach to an improved SOE. Therefore, the Canadian approach has defined the SOE separately and the implementation phase is ensuring that the SOE limits are consistently and uniformly implemented into existing operational documentation.

Although there would have been some advantages in terms of international consistency, with adopting Tech Specs, the disadvantages were significant. The Candian industry has had 30 years of experience with the existing framework and it has served the industry well. A change at this time would not only be a costly undertaking but would also represent a significant change for Operations. This would introduce nuclear safety risk and a significant increase in training. The existing framework allows the flexibilty within the existing impairments structure to perform risk-based technical

assessments. This helps to eliminate unnecessary conservatisms which then impose limits to operation. Adopting the Tech Specs approach would have involved a solo venture for Point Lepreau and the benefit of experiences and knowledge gained by peers through the SOE process would be lost.

The Canadian Nuclear Safety Commission (CNSC) has endorsed the COG approach to SOE. A deviation from the accepted Canadian approach to SOE would require solid justification and subsequent approval from the Regulator.

3 OPERATING STATES

One of the overall purposes of the SOE process is to understand how performance requirements for systems, components and instrumentation are specified by design & safety analysis and translated into operating limits and conditions to assure plant operation is safe and reliable. This message of safe and reliable operation is consistent with the World Association of Nuclear Operators (WANO) Performance, Objectives and Criteria (Revision 3, January 2005). To achieve this objective it is necessary to understand the regime of plant operating states that are the basis of the reactor safety design and analysis.

Normal operating conditions (NOC) are defined as the operation within specified operational limits & conditions for configurations of systems, structures, & components (SSCs) which are designed to produce power, perform maintenance, or provide protection. This category is broken into full power (FP) operation and the “guaranteed shutdown state" (GSS).

Anticipated operational occurrences (AOO) are defined as an operational process deviating from normal operation or SSC degradation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

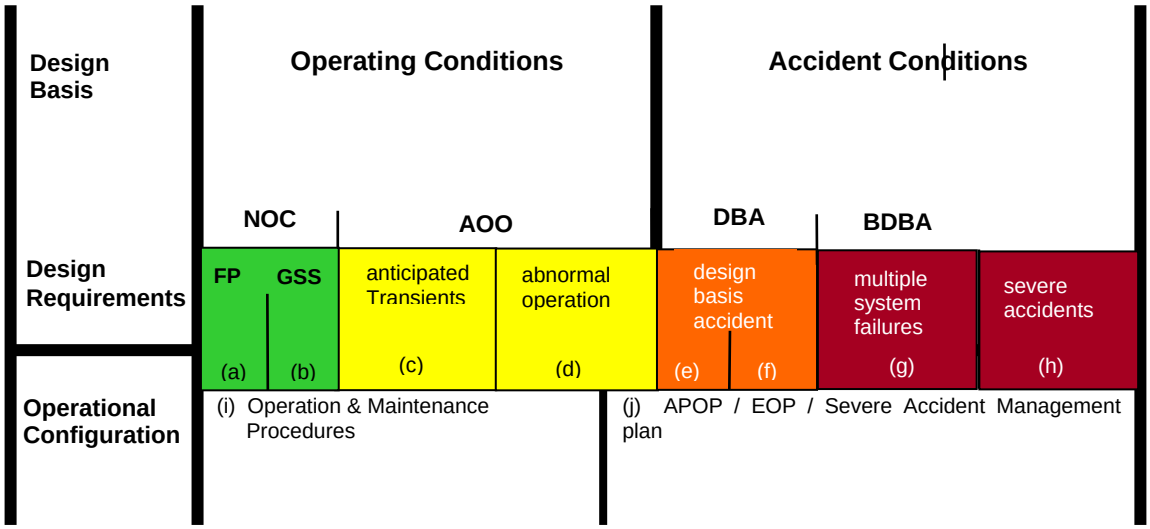
Design basis accidents (DBA) are defined as accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

Beyond design basis accidents (BDBA) are those less likely than a design basis accident and where accident conditions are more severe. The situation may or may not involve significant core degradation.

A severe accident is a type of beyond design basis accident that involves significant failures of fuel and damage to the core.

The operational states and operational configurations are summarized in Figure 1. Explanatory notes are found below the figure.

Figure 1: Graphical View of Operational States



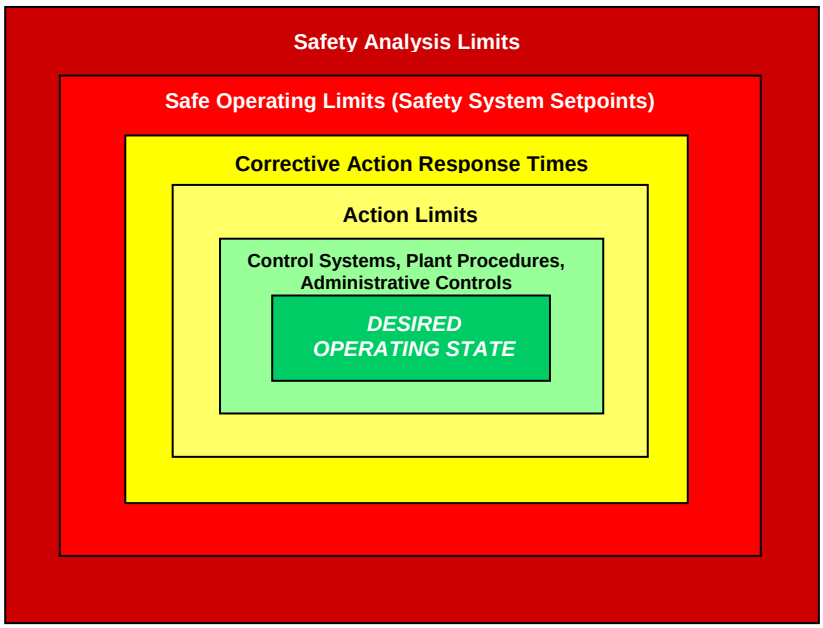
Notes for Figure 1

a) Normal operating configurations for producing power up to full power (FP).
b) Normal operating configurations when shutdown for maintenance in the Guaranteed Shutdown State.
c) Anticipated operational occurrences that are process transients or other conditions requiring corrective actions/maintenance.
d) Anticipated operational occurrences that are abnormal operating configurations with power production until corrective actions/maintenance can be performed.
e) Design basis accidents that are the basis for the design of the special safety systems.
f) Design basis common cause events for the design of emergency control/cool/contain requirements.
g) Beyond design basis accidents involving multiple system failures without significant core damage.
h) Beyond design basis accidents resulting in severe core damage.
i) O&M procedures for operating conditions with the process systems providing control/cool/contain.
j) Operating procedures for securing a safe shutdown state under accident conditions.

4 SAFETY MARGINS

The safe operating envelope can be viewed graphically. Figure 2 shows the operating ranges as a series of 'envelopes'. The safe operating goal is to stay within the normal operating range (green zone). The existence of a margin (the yellow zone) between the Normal Operating range and the Safe Operating Limit (red zone) does not mean the plant is to be operated in this range apart from transient conditions. This region is the 'safety margin' and part of risk management is to maintain safety margins. The attitude that '*safety margins can be used to improve production*' tolerates operation outside of the design basis. This increases both the financial risk and the safety risk.

Figure 2: Graphical Representation of the Safe Operating Envelope



The safety margin is provided by the design for 2 purposes:

- to provide the ability to correct anticipated transients before they challenge the safe operating limits and result in lost production, and
- to provide extra confidence the plant is not being operated unsafely due to errors and uncertainties

5 SAFETY, PRODUCTION and COST CONTROL

As an industry, the focus on station performance in achieving safe and reliable production of power has continued to improve. In 1992 Pate [1] recognized the need to control costs as well as pursuing operational excellence. The 3 elements of the unit electrical cost that are under the control of a station are: Operations and Maintenance (O&M) costs, forced outage losses and plant availability. Pate compared the O&M costs for plants to their INPO performance level. He found a wide variation in O&M costs with lower cost plants at all performance levels, BUT, only lower cost plants at high performance levels.

Pate provided the raw data in his 1992 “Excellence Versus Cost” speech to INPO executives. It showed the number of excellent plants tripled from 6 to 18 between 1986 and 1991 while average O&M costs for the excellent plants remained constant at 33% lower than the US industry as a whole. If significant additional O&M expenditures had been required to attain excellence, it would have been reflected in a convergence of O&M expenditures. This was not the case. This is evidence that the highest levels of safety, reliability and economic performance go hand in hand.

Mosey [2], in his book "Reactor Accidents", identifies the inter-related categories of institutional failures that lead to reactor accidents. They include priority of production, failure to recognize the importance of safety, and failure to provide adequate resources. Poorly maintained equipment and human performance can lead to lost production and at the same time increase the risk of exposing the environment and the public to radiation.

It is possible to promote production to the detriment of safety. Unknowing technical support personnel will recommend expanding the normal operating range by reducing the safety margin. This results in decreased defence-in-depth and an increase in financial risk because it is more likely that a transient could not be corrected before a shutdown would be required leading to lost production.

Point Lepreau Generating Station, through the implementation of the SOE, has undertaken a proactive pursuit of maximizing the operating goal where capacity factor and safety margins are optimized. For if nuclear electric generation is not competitive in the marketplace, excellent performance by environmental, safety or reliability measures will be a moot point.

6 THE IMPLEMENTATION PROCESS

A major goal of the SOE Implementation project is to ensure that all the station operations procedures are in agreement with the data presented in each of the SOE basis documents. On achieving this goal, the operator will be equipped with the appropriate limits to ensure that plant operation is within the Safety Analysis Limits (SAL) that define the SOE for the plant.

The SOE implementation requires a definition (technical basis) document associated with a particular safety related system. The definition systematically describes the characteristics of all process components that have a safety function and all safety related instrumentation loops. The SOE definition team creates a "gap" list that documents all deficiencies in design, operation or safety analysis as identified during the SOE definition. This list is then augmented by the SOE implementation team.

The gap list lays the foundation for the net safety benefit that the SOE implementation will achieve. The SOE Implementation Team has found that to convert skeptics, it is best to prioritize and document the resolution of gaps within existing station processes. These processes include corrective action programs, design change processes and configuration control programs dealing with operational documentation.

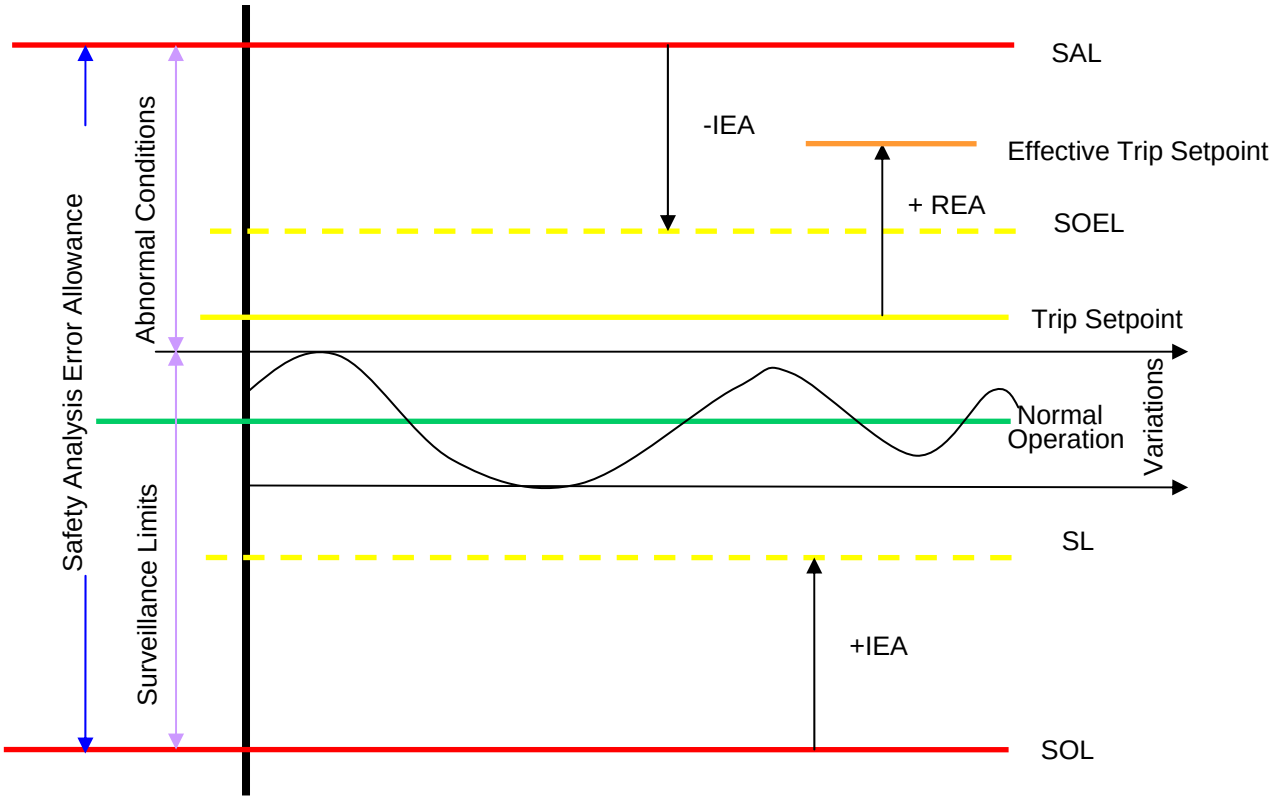
At Point Lepreau Generating Station, a large source of gaps is based on instrument uncertainties assumed in historical safety analyses. These differ from the instrument uncertainties calculated according to international standards in the latest SOE definition document. The uncertainties for the Instrumentation and Control (I&C) loops includes error allowances calculated for each trip parameter that consider the instrument loop uncertainties and biases for both normal operating and accident conditions. However, not all of the data presented in the basis documents are directly applicable to indications available to the operator in the Main Control Room (MCR). Since the operator observes instrument readings that already include the effects of instrument loop uncertainties additional data parameters are required for use by the operator than are defined within the SOE basis documents.

New terms were added to the Point Lepreau Generating Station lexicon for use in implementing the SOE for operations. The Safe Operating Envelope Limit (SOEL) is used during normal operating surveillance activities, such as when performing Operating Manual Tests. The SOEL is defined as the maximum allowable trip parameter value assumed in safety analysis (Safety Analysis Limit - SAL), less the uncertainty associated with the instrumentation (Instrument Error Allowance - IEA) during normal operation for high going trips. The SOEL is then a practical value to which the operator may compare trip parameter readings to ensure that the trip parameter remains within the licensing limits. Exceeding the SOEL is defined as a Level 1 Impairment of the trip channel.

The Effective Trip Setpoint (ETSP) is the Safety Analysis value which allows for all uncertainties and detrimental biases, refered to as the Required Error Allowance (REA). The ETSP, minus the REA, ensures the Trip Setpoint (TSP), as found in the control computers, is protected. The choice was made to include a REA of 2-sigma, which gives a 95% confidence level.

The Safe Operating Limit (SOL) represents the lower end of the allowable operating regime and is based on safety analysis. The Safety Limit (SL) is the monitored parameter which, with the addition of the IEA, ensures operation above the SOL, for a high going trip.

Figure 3: Safe Operating Envelope Applied to Instrumentation and Control Loops



7 MEASURE OF SUCCESS

An improved set of operational documentation will increase procedural compliance due to a consistent approach to implementation of operational limits and a reduction in conflicting instruction to the user. The focus of the operator will revert back to the routine, everyday tasks of running a nulcear facility, with fewer unusual plant evolutions.

8 CONCLUSIONS

Operating experience from nuclear power plants worldwide shows that middle-aged reactors must intensify their attention to configuration control issues. The direction of the industry is forcing newer employees to rely less on tribal knowledge and work-arounds and emphasis is placed on procedural documentation and compliance. An improved SOE offers the opportunity to eliminate gaps

and procedural inadequacies. This "modus operandi" contributes to world class operation and, through improved human performance, avoids unplanned outages.

REFERENCES

[1] Pate, Z.T., Excellence Versus Cost, Notes from speech to INPO 1992 CEO Conference, Atlanta, Georgia, November 4-6 1992.

[2] Mosey, D., Reactor Accidents, Nuclear Engineering International Special Publications, 1990.