OPERATIONAL SAFETY MANAGEMENT AT POINT LEPREAU GENERATING STATION

D.F. WEEKS/D.J. WILSON

New Brunswick Electric Power Commission
Point Lepreau Generating Station
P.O. Box 10
Point Lepreau, N.B.
E0G 2H0

ABSTRACT

The objective of Operational Safety Management is to minimize the risks associated with Operation of the Station. This paper presents our views on what constitutes Safety, reviews the nature of problems faced by station operations staff and the tools available to deal with these problems. The dynamic nature of Safety problems and thus the methods required to manage them are explained. Examples are given of some recently experienced problems and the types of procedural changes being considered to better address operational problems in the future.

INTRODUCTION

The future of the Canadian Nuclear Industry depends on the effectiveness of Operational Safety Management at any Nuclear Power Plant.

As an Industry we enjoy, at best, a tolerance from the "Silent Majority", and the importance of our products to the economy of our Provinces and the Nation is generally ignored. The airlines, the railways, the oil industry, hospitals, hotels and car manufacturers; none of these face such wrath from the public. The seeming willingness of some to write us off due to a single major accident is unparalleled in other industries. Yet be assured that a major accident at Point Lepreau, whatever the cause, would indeed adversely affect the economic future of every Canadian, and the employment prospects of everyone in the Canadian Nuclear Industry, and every town and city associated with it.

This paper discusses Operational Safety Management at Point Lepreau and will cover four main areas;

(1) What is Safety?
(2) Nature of Operational Problems.
(3) Tools for the Job.
(4) Examples of the unexpected.

Each of these areas could easily form the topic for a paper, or indeed a whole session, so our coverage will, of necessity, be brief.

We will close by reviewing the Overall Safety Culture Philosophy as we feel it should be applied.

WHAT IS SAFETY

To obtain your appreciation of the scope of issues that must be addressed in Operational Safety Management, it may be necessary to challenge your current concepts of "Safety".

Dictionary definitions tend towards the view that Safety is freedom from danger and the absence of risk. Given that as Engineers and Scientists we know that in the real world there is no such thing as complete freedom from danger, and that nothing is nor can be risk free, we cannot be satisfied with this dictionary definition of Safety.

Safety is a concept that divides the world into three camps. The first camp comprises the reckless and ignorant who ignore or flaunt anything to do with safety, either yours or their own. The second camp contains those who hold that Safety is absolute, and that **only** zero risk is acceptable. These are the dreamers who believe that safety is their perception of living in a risk-free environment with zero danger. These people can only survive in the real world by drawing political or emotional curtains over everything they want to live with, and by pretending there is no problem. You cannot discuss safety with a group two person without being accused of being yourself a reckless group one ignoramus. In reality, group two is almost as much of a real danger to society as group one, as they fail to look for the real and often larger risks and costs in the alternatives to the things they oppose.

The third camp comprises those who know the nature of the real world and seek to define the real problems in life and to minimize the overall risk associated with these real problems. The third camp appreciates the problems, costs and risks associated with unemployment, poverty, the lack of adequate food, heating and housing, as well as both long term and short term risks to health and the environment.

In the latter half of the 1980s we have seen a gradual and necessary swing in society, as more and more people educate themselves regarding third camp issues. In the seventies and early eighties, the vast majority of activists people were in the second camp. They closed their eyes and minds to many serious health and safety issues and concentrated their efforts against a few high profile issues. These were the "Anti-s", and one of their major targets was the Nuclear Industry.

Public Safety from a Regulatory perspective can be achieved provided certain definable limits can be met. To second camp people, however, there is no such thing as a definable safe limit.

Public Safety from an ALARA perspective states that risk should be as low as reasonably achievable, taking into account economic and social factors. To second camp people, however, the only important social factors are themselves, economic factors are irrelevant unless they have to write the cheque on their own bank account, and the only reasonable thing to achieve is zero risk to themselves personally.

Indeed, **everyone** is a mix in some proportion of first, second and third camp attitudes, depending on the issue. Everyone has their own personal definition of "acceptably safe" and everyone is prejudiced. The risks that each one of us will accept or reject are not all based on definable or rational criteria. Test yourself! What risks do you accept individually or communally to avoid or defer expenditures of Effort, Time or Dollars? What criteria do you use on car repairs, seat belts, speed limits, weed killers, home heating, swimming pools and barbecues? How many of you use Safety Boots when mowing the lawn, or use Safety Glasses in your Home Workshop?

No Industry has ever been the subject of such detailed and continuous scrutiny on all aspects of risk and safety as the Nuclear Industry. Yet many of our problems are a result of our looking so closely. Because we have looked, an estimate can be made of the long term health effects of the Chernobyl accident. But has anyone looked at the alternatives? What are the widespread long term health effects of a Hydrogen Sulphide leak in Alberta, a Forest Fire in Northern Ontario, a fire at an Oil Refinery, a Chemical Warehouse, or indeed the building next door? A propane explosion demolished apartments and killed a number of people in New York, yet received only brief coverage on an inside page of a local newspaper. Were the future health effects on the people of Saint John any less from that fire in New York than they were from Chernobyl?

The basics of Nuclear Safety can be divided into four areas:

i) Design Safety
ii) Construction and Commissioning Safety
iii) Operational Safety
iv) Decommissioning and Disposal Safety

Today we are addressing Operational Safety, and our starting point is a Commissioned and Licensed Operational Plant, for which the granting of an Operating Licence assures that Design, Construction and Commissioning have been judged to be "acceptably safe".

Operational Safety encompasses Radiation Safety naturally, but perhaps more importantly, it covers Conventional Safety Areas such as Mechanical, Thermal, Chemical, Electrical and Fire Safety as well as First Aid and Medical Safety.

Operational Safety involves a procedural defence-in-depth approach. We realize that everyone makes mistakes. A program must therefore minimize the consequences of a single mistake, and maximize the chances that a mistake will be recognized and corrected before it is compounded.

NATURE OF OPERATIONAL PROBLEMS

Operational Safety is not a static business continually rehashing a fixed set of problems.

In Operational Safety Management we are dealing with two sets of variables which impact on the risks that must be minimized.

The first set are people; our staff, the public, politicians and regulators. For all of these groups we have to deal with ever changing perceptions of what constitute risks and safety issues. Changing perceptions, as well as new information and experience, continually impact on the way we view safety. Every major incident at any power plant, and even minor ones in-house require in-depth review for actual and potential safety implications.

For staff working at our plant, we have to consider not only Occupational Health and Safety Issues, including detailed work protection for every task, but also the potential impact of human error in the implementation of changes and in maintenance work. We also need to consider a variety of issues which are now becoming known as "Human Factors", as these issues too impact on safety. These include:

- balancing work loads so that the individual is challenged but not bored, avoiding continual overload which leads to stress, illness, fatigue and mistakes.

- presentation of information in clear, precise and unambiguous form, to ensure proper communication of plant status, work in progress, operating procedures and work plans, avoiding the misinterpretation that leads to problems.

At any level we have to ensure that information presentation is not so complex or specialized that it is difficult to understand, yet it is not so simple and familiar that it is ignored or overlooked. In a crisis requiring Emergency Response, relevant and accurate information must be presented in a useable form; it must not be lost in an overwhelming onslaught of alarms and indications occurring because every system in the plant has changed state. Accurate and appropriate response in a crisis also requires breadth and depth of individual expertise and experience in those in a position to respond.

The second set of variables impacting on Operational Safety is the equipment itself. All equipment deteriorates with time and use, some at its normal design rate, some at an accelerated rate due to erosion, corrosion, fretting, vibration or other adverse conditions. Equipment and component breakdowns are an unavoidable fact of life. Operational Safety Management involves not only ensuring that repairs are effected safely, but that the plant can continue to be operated safely until the repair is made. Often this is compounded by the non-availability of identical replacement parts, which can be as much a function of technological development over the 30 year plant life rendering the originals obsolete, as any warehousing or transportation problems. Ensuring safety with varying equipment configurations and component capabilities is part of the task.

Proving the continued availability and capability of Safety systems and safety support systems is another area which requires attention. As shown all too clearly at Chernobyl, design of some safety support systems can be such that proving their capability involves placing the plant in an unusual and often unnecessarily risky configuration.

One of the more significant areas for Operational Safety Management is that of Outage Planning. With systems designed to defend in-depth against incidents that may occur with the plant operating, we are faced with maintenance to a multitude of components; taking many systems out of service for inspection, yet still with the need to retain capability and backups for each essential function. All this work must be planned under the ever watchful eyes of those who tell us we are so valuable, that we are costing the people of New Brunswick $30,000 per hour in replacement energy costs alone, during an outage.

This is a brief summary of the operational problems impacting on safety. It is obvious from the scope and extent of the issues involved that Safety must be the concern of everyone at the plant; it cannot be delegated to a single individual or group.

TOOLS FOR THE JOB

The major tools required for the job of Operational Safety Management are Procedures, Training and Experience. They boil down to people.

At all times a licensed Shift Supervisor is in charge of the unit and has overall responsibility for safe plant operation. He must ensure that operation and maintenance of the plant is carried out in accordance with a heirachial set of procedures bounded by the Reactor Operating Licence and the Operating Policies and Principles (OP & P) of the Station. In particular, the OP & P document defines the bounds outside which the Station or any system must not be operated. OP & P overlay conditions imposed by Regulators on a well developed set of sound safe operating and management practices.

Within the procedural hierarchy are approved Operating Manuals (OMs) which incorporate the operating requirements of the design as well as related industry experience. These documents deal with regular and foreseeable tasks and include the experience and recommendations of a wide variety of experts in many technical fields. They also receive extensive in-house review and Operations feedback, so that there is every opportunity for input of lessons learned. Special sets of these manuals, Abnormal Plant Operating Procedures (APOPs) and Contingency Plans, are the topics of several papers to be presented at this conference.

Procedures are also in place to control permanent Engineering Changes to the original design of plant systems. Similarly procedures are in place to control the development and implementation of Work Plans needed to implement these Engineering Changes or to undertake any unusual tests on station systems, particularly safety or safety related systems.

All of these procedures are developed using a well tried defence-in-depth approach to identify and rectify problems. This approach includes but is not limited to the following:

i) Well trained and experienced initiating author.
ii) Experienced Technical and Management review.
iii) Safety and Regulatory review if Safety or Safety Support Systems or other high profile systems are involved.
iv) Operations review.
v) Final judgement of the Shift Supervisor regarding final implementation.

Implementation of Work Plans and non-routine tests on Safety systems, Safety Support systems and high profile process systems include a defence-in-depth approach to ensure that the steps are undertaken properly and in correct sequence. These generally include:

i) A well reviewed procedure, approved by Management, Regulators and the Shift Supervisor.
ii) Sign Offs at key steps.
iii) Independent verification of steps completed.
iv) Shift acceptance of the completed plan.
v) Testing of equipment prior to service.

If a temporary situation arises when a system must be operated in a manner different from that detailed in an OM, an Operating Instruction is developed (using the same process as for an OM).

If a work plan or operation is to be undertaken and the Shift Supervisor feels that the steps in the task are not sufficiently detailed, this detail can be covered in an Operating Order.

If an error is found in an approved Operating Procedure, or a situation arises that is inadequately covered, a **Jumper** can be raised, based on the Shifts training and experience, to temporarily resolve the problem. Jumpers can also be applied to temporarily resolve hardware problems, both in normal operation or for test situations. Installation of jumpers is strictly controlled. An approved jumper installation procedure details requirements for independent technical review, Management and Regulatory approval, clear field identification of the equipment involved in the jumper, clear documentation of the purpose and required duration of the jumper, and sign offs with independent verification for both installation and removal.

All field work, other than that of an operational nature, is governed by a Work Permit system. This ensures that adequate work protection (conventional and radiation safety) can be established for the job, that the Shift Supervisor and CRO are aware and approve of the equipment affected by the work, and that the status of the work can be tracked. All equipment affected by the job is clearly identified in the field and in the Control Room. Affected equipment is also subject to a release-for-service acceptance which involves suitable testing and repoising.

An additional aspect of the control of work is the requirement for planning and scheduling the necessary resources which is done through a central Planning Group.

An overall Daily Work Plan is produced which schedules work based on input from Operations, Work Groups and Management. In particular, major jobs or tests receive Management approval before proceeding.

A particular and effective feature of PLGS is the daily Planning Meeting, typically of 15 minutes duration, involving Management, Operations and Technical Unit supervisors and specialists. Overnight problems are presented and the proposed work for the day is discussed in an open forum where ideas can be freely exchanged, concerns raised and conflicts in schedule and requirements, which might have slipped through other procedural barriers, can be identified and resolved.

The volume of work, the opportunity for tests and the necessity of off-normal system configurations make the application of Operational Safety Management particularly significant for the planning and execution of maintenance outages.

At PLGS we assign a number of key staff to an Outage Coordination Group several weeks prior to each major outage to assist with the additional volume and complexity of work.

EXAMPLES OF THE UNEXPECTED

With thousands of jobs, involving tens or hundreds of thousands of components, undertaken in a single outage, a veritable mountain of paperwork must be processed in the form of Work Plans, Work Permits, Operating Orders, Jumper Records and Testing Requirements. Given the nature of people and the quantity of work, it is inevitable that mistakes will be made on some items and that some of the procedural barriers will be breached on occasion. Given the defence-in-depth approach, both procedurally and in equipment and system design, it is rare that a breach compounds itself through several barriers resulting in a Safety incident and casualties.

Operational Safety Management involves a detailed review of all incidents that involve a breach of one or more of the procedural or equipment barriers to create a safety hazard. On an individual basis, problems may be solved by procedural changes, design changes or further or restructured training. The objective is to both better communicate the way things must be done and the hazards involved in incorrect operation, and to make systems as invulnerable as possible to individual mistakes. Beyond the treatment of individual incidents, assessment of trends can require more generic changes to work practices.

All of the significant incidents that have occurred at Point Lepreau so far this year were related to the Annual Maintenance Outage. While we do not have the time to review each of these in detail, a few examples may be appropriate. We shall assume that the audience is familiar with the system designs and the additional Safety barriers which guard against any of these problems developing into a public safety concern.

During the outage, while the HTS was drained to header level for other work, a permit was issued to replace a valve in the HT Gland Seal Cooling system. After breaching the bottom joint of the valve and collecting about half a drum of heavy water, it was apparent that the line was not draining as expected as there was no lessening of the flow. The isolations for the work permit were checked and a direct path was found to the Heat Transport Storage Tank. If not for the job planning, training and experience of the maintainer involved, the error in the work permit might have resulted in an embarrasing heavy water spill.

After changing orifices in the HT Stability line, with the HTS refilled and pressurized, a series of tests were planned with only two of the four HTS pumps operating, to verify the expected reduction in vibration. During the test a small seal weld leak occurred at a HTS purification valve.

The Shift personnel were faced with an unexpected occurrence with probably minor consequences. The choices available were to continue the test for a further ten minutes or so to gather some very useful vibration data and to continue a multitude of unrelated maintenance work in the Reactor Building to meet the pressing, costly outage schedule. However the Shift Supervisor chose to act in the interests of Safety. The test was terminated, and all persons not involved with the test were asked to leave the reactor building until any contamination resulting from the leak were located and cleaned up.

A great deal of welding and subsequent radiography occurred in the turbine hall during the outage. At the end of one dosimetry period, a welder's TLD indicated an overexposure of 75 mSv deep dose. An immediate enquiry had to be held which determined that the confined space at one weld location had led the welder to take off his badge and place it nearby while he undertook his weld. For one break, during which his welds were radiographed, he forgot to retrieve his badge. Returning subsequently to retrieve the badge, he did not report the misplacement and obtain a new badge as required by procedures. While this incident may not have resulted in an overexposure or health risk to the welder, the increased stress imposed on AECB site officers and station Health Physics staff by revelation of such a TLD result, is not negligible.

There were two turbine related incidents; the first involved the inadvertent crossing of hydraulic power and trip system hoses to one of the intercept valves. The procedure required that only one hose be disconnected at a time. Nevertheless they ended up crossed, such that on any manoeuvre requiring power movement of the intercept valve, the pressure in the lower capacity trip system dropped, and a turbine trip occurred. There were no design barriers to identify the individual hoses and terminal points, and no barriers to prevent connection of either hose to either system. In the second incident, a jumper was installed to prevent movement of automated valves on the extraction steam lines while inspection and component replacement work was undertaken. The jumper paperwork was misplaced and consequently the jumper stayed in place after the outage, until it was discovered, subsequent to a turbine trip, that some valves were in the wrong position.

Beyond the obvious changes required to deal with each of these individual incidents, it is apparent that the paperwork mountain which occurs during an outage is imposing too great a work load on the current shift complement, such that tracking the status of individual jobs, and resolving the overall plant status is increasingly difficult.

In order to ease the load on the Shift Supervisor and CRO, we propose to expand and better define the role of the Shift Outage Coordination group in tracking and expediting work during future outages. The paper mountain imposed by our ability to superschedule our outage jobs with Computerized Work Scheduling, is a volume problem that we intend to resolve by developing an improved and computerized

data base system for tracking papertrails to resolve job status. This should reduce the chances of paperwork being mislaid, or necessary tests overlooked.

As one of our major areas of Safety concern, we intend to supplement the current status alarm monitoring system with a computerized Expert system to monitor critical safety parameters, equipment and backup system status, and to define such areas as heat sink status. This will not only rapidly diagnose problems, but display directly the procedural flow charts to be followed to resolve the problems or change to an Alternate Heat Sink.

We expect that the proper application of modern computer technology in these areas of Operational Safety Management will assist us in processing the volumes of data and information that are required to increase our efficiency and effectiveness.

REVIEW

The object of Operational Safety Management is to minimize the actual risks associated with real Safety hazards as they might impact on the operating staff and the public. Due to distortions implicit in evaluating risks, it is also necessary to apply these principles to minimizing additional perceived risks. A dilemma we occasionally face is being requested to reduce a perceived low level risk even where the only practical way to do this would actually increase real risk elsewhere.

Given that everyone makes mistakes, Operational Safety Management practices must ensure that there is a defence-in-depth approach in devising procedural barriers. This approach minimizes the consequences of a single mistake, and maximizes (by critical review) the chances that a mistake will be recognized and corrected before it is compounded. However, only by overlaying an effective system to adequately assess and rectify problems which lead to barriers being breached, can we minimize the frequency of barriers being breached. The process is itself dynamic, due to the nature of the people and equipment with which we work. We always welcome constructive criticism which can offer practical solutions to any problem we may face. We would like to open the floor to your questions and input.