REPORT

RAPPORT
REPORT

Independent Verification in Operations at Nuclear Power Plants — Summaries of Site Visits

by

D.C. Donderi, A. Smiley
D.J. Ostry and N.P. Moray
Human Factors North Inc.

Prepared for the Atomic Energy Control Board under its Regulatory Research and Support Program
Ottawa, Canada

AECB Project No. 2.276.1

September 1995
TABLE OF CONTENTS

Visit to Darlington NGS
Visit to Pickering NGS
Visit to a Pressurized Water Reactor Nuclear Power Plant in the U.S.A.
Interviews at Illinois Power Clinton Nuclear Power Plant Concerning Verification of Operator and Technician Actions
Visit to U.S. NRC
Visit to Hartlepool Power Station, U.K.
Visit to Nuclear Installations Inspectorate, U.K.
Visit to Mihama Nuclear Power Station, Fukui, Japan
Visits to Direction de la Sûreté des Installation Nucléaires and Electricité de France
Visit with Technischen Überwachungs-Vereins Rheinland, Bundesamt fur Stralenschutz, and Gemeinschaftskernkraftwerk Neckerwestheim Representatives

APPENDIX A
APPENDIX B
APPENDIX C
APPENDIX D
APPENDIX E
APPENDIX F
APPENDIX G
APPENDIX H
APPENDIX I
APPENDIX J
Visit to Darlington NGS

Alison Smiley, PhD
Human Factors North Inc.

November, 1993

On Tuesday, November 16, 1993, I visited Darlington Nuclear station and spoke with AECB and Ontario Hydro personnel about independent verification in operations. My contact at Ontario Hydro was a representative of the Quality Assurance Department, who arranged appointments for me, and he or a nuclear shift supervisor accompanied me throughout the day. I spoke with the following people:

- A representative of the AECB
- Personnel in Laboratory Quality Assurance and Quality Control
- Personnel in Radiation Control
- A technical superintendent
- A Shift Supervisor (SS), an Authorized Nuclear Operator (ANO), a Supervising Nuclear Operator (SNO), a Nuclear Operator (NO), and a refuelling operator.

I collected a number of forms indicating procedures for verification of actions, independent or otherwise. A summary of the conversations follows.

Conversations with Nuclear Operators: ANO, SNO, NO, refuelling operator, SS, Unit Manager

ANOs and SNOs mainly check their own work, sometimes with checklists (when using OTPs [Operator Test Procedures], STRPs [System Safety Tests], OTOs [Order to Operate], AIM [Abnormal Incident Manual], sometimes when using work plans, for some callups), sometimes without checklists (routines, some work plans, OMPs [Operating Manual Procedures] and Operating Memos). SNOs are responsible for checking the work of NOs. How they do this is up to them and usually involves communication about how the job is going, rather than actually checking control settings or actions. The shift supervisor is responsible for checking the work of the operators. Actual time spent in the control room or field is fairly low, on the order of 5%. When large or complex jobs are done, involving employee safety, loss of production or environmental impact, the shift supervisor will assign someone to check the job.

With respect to the availability of procedures for each task, operators agree that the vast majority of tasks had some procedure. Nuclear operators carry out many tasks in the field routinely and carry written procedures relating to these tasks, called "routines", with them in the field. However, they do not generally refer to the routine book if they are very familiar with the task. There are no checklists associated with these routines. Nuclear operators occasionally find controls set incorrectly in the field and report these. This happens perhaps once or twice a year. Such errors are rarely found through checking by shift supervisors. This relates to the fact that
the shift supervisors are not trained in operations. They are aware of how the various processes are supposed to operate and detect problems at the process level, but are not trained in operations and so would not necessarily detect that a control setting was incorrect.

Callups and routines are regular tests. Callups refer to regular tests which are carried out more than a week apart. Routines refer to regular tests which are carried out once a week or more frequently. Routines are generally simple and do not have check lists associated with them. Callups are more complicated and can involve a written procedure. Both can involve checking particular variables without any action being taken, or manipulating controls. Panel checks are routines done every shift involving checks that controls are set correctly. The most critical controls are located in the control room, or, if seldom used, in the subsidiary control room. Few controls in the field are critical.

With respect to whether or not procedures are always followed, they are sometimes not. The major reasons for not following procedures is that the procedure is not up to date or is not clear. Operators are supposed to obtain permission of a shift supervisor before deviating from a procedure.

Operators do tasks for the first time without having their work checked. However, these tasks involve work plans generated and independently checked by the technical section. The work plan contains a section on which the operator can note any problems encountered, including deficiencies in the procedure.

Independent verification occurs in some settings and not in others. Many system safety tests are fully automated and run by the computer. The computer outputs a record of the test with yes/no indications which the operator checks to ensure the test has progressed as expected. Other system safety tests are not automated but have check sheets associated with them. These are completed by the operator. Whether the tests are automated or not, the paperwork (but not the control actions) is verified by the shift supervisor.

After an operator carries out isolation prior to maintenance, a field inspection is carried out by the operator and a maintenance supervisor or the maintainer who will be doing the work to ensure the isolation has been carried out correctly. In this case, independent verification seems primarily for the purpose of protecting workers from inadvertently working on live systems. If the isolation involves a safety system, then the shift supervisor must verify that the equipment can be taken out of service. Once maintenance is finished and a field operator returns the system to the operational state, there is no independent inspection of control settings to ensure the system is returned to a normal state. A checklist is completed and the paperwork is verified. Where safety and other important systems (e.g. the turbine) are involved, testing is carried out to ensure the system is functioning, wherever this is feasible.

For start-up, there is a start-up sheet listing tests to be done to check out the system. There is also a valve line up check and a tag check that applies to all systems regardless of whether they
have been worked on during the shutdown or not. For run-up, there is also a flow chart of work to be carried out. This is checked off by the operator, and the paperwork is verified.

Work plans are used for one time changes in the plant. During commissioning, many work plans are in use - during an outage, this is also the case. Work plans are seldom used during periods of normal operation. Work plans often involve verification points where a person from the technical section will be required to come and make an independent check.

When safety systems are tested, an operator may only test one of three channels. (There are three independent sensors associated with each shutdown system.) This is to prevent the same mistake being made in more than one channel, which would compromise the safety of operation.

For severe transients, the abnormal incident operating manual is used. The procedures themselves have been approved by the unit manager and by the AECB. The shift supervisor verifies both that the appropriate switches have been operated according to the procedure and that the effect is as desired. The shift supervisor does this at what he judges are key points in the procedure. During transients, the ANO is backed up by several other persons with operating experience or knowledge who perform an independent verification function. This independent checking in the control room is done on an informal basis rather than using checklists.

Operators were asked about errors which might have been avoided by independent inspection. One person commented that errors made by field operators seldom resulted in SERs and that independent checking would have a very slight impact on overall performance. In addition, operators expressed the opinion that the extra staffing that would be required for independent checking would make it impractical.

With respect to whether the greater automation at Darlington could allow more automated checks, this is already done in many system safety tests.

Refuelling Operators

The refuelling operator's task is more repetitive than the operator's task and involves controlling the manipulation of fuel bundles - removing spent fuel and fuelling empty channels on a 24-hour basis. At Darlington, much of this work is automated (this is less so at Bruce but very much less so at Pickering). The refuelling operation can be done in an automatic, a semi-automatic and a manual state. The last is rarely used. In the automatic and semi-automatic states, the computer carries out actions once the process has been initiated by the operator. The program will stop at certain points and wait for the operator's input to check if things are progressing correctly and continue the process. Depending on the process, this happens approximately every half hour.

Most SERs, and in particular the most serious SERs, have occurred at around 4:00 am, a time period known to be associated with sub-optimal human performance. It would be worth verifying that SERs tend to happen in this time period. If so, independent verification during this time
period might be given consideration since the nature of the job is such that hazardous or complex
tasks cannot be re-assigned to another time period.

Chemical Section

The chemical section looks after chemical testing of samples drawn from the plant. Four groups
are involved: quality assurance, environmental, on-line, and shift support. About half of the
technicians work on shift, to support operations. The other half work days. Most testing involves
drawing a sample and returning to the laboratory. Some testing is carried out online in the plant.
Approximately 95% of testing involves the running of reference solutions which contain a high
level and a low level of the substance being looked for. The reference solutions are run serially
along with the test solutions. Errors in test procedures show up as errors in values found for the
reference solutions. Where reference solutions are not available, as for example with free
chlorine, test procedures and analytical equipment are checked by means of samples with known
levels of the substance in question provided by various certifying organizations for this purpose.

When a sample is taken in the plant, control actions are made and these are not associated with
any checklist or verification procedure. However, in most cases, taking the sample involves
turning on a tap, and it is obvious whether the system has been put back in the same state after
the sample has been taken. One or twice a year, there are incidents where a control was not
placed back in the correct setting. These errors are usually caught from control room indications.

Certified reference solutions are obtained from certified organizations. These are used to make
a reference standard for the lab and to make working standards which are used routinely for
tests. The preparation of the reference standard involves independent verification of the process
step by step, by a second qualified technician. Preparation of the working standard involves
reanalysis by a second technician to ensure the standard was prepared correctly.

The chemical section has assessed field sampling practices to ensure technicians are carrying out
analyses correctly. Recently a system of job performance measures has been introduced to
evaluate an individual’s capability in in-laboratory testing. At the moment, both assessments are
a one-time certification process, but consideration is being given to a schedule of re-certification.

The chemical section is audited not only by the AECB, but also by three other certifying
organizations. CAEAL (the Canadian Association for Environmentally Accredited Laboratories)
does audits once every two years. COGIS (Candu Owners Group Information System) sends
samples related to chemicals in nuclear plants with known levels of substances to be tested so
that results can be checked. PET (Proficiency Environment Testing), like COGIS, also sends
samples to be checked, but these are related to pollutants in plant discharges.

According to laboratory personnel, there have been no SERs related to actions made by the
chemical group. SERs associated with this group relate to insufficient staffing and chemical spills
resulting from equipment malfunction but not to situations where independent verification would
have prevented an error.
Radiation Control

The Radiation Control section looks after radioactive sources, radiation protective equipment (clothing, respirators, etc.) and radiation measuring equipment (portable radiation instruments, bar code readers, monitoring stations).

Staff assist with waste handling, but are not directly involved with shipping. They give training in the use of radiation monitoring and measuring equipment, the Radiation Protection Procedures, and assist Technical section personnel in the preparation of work plans where radiation hazards are of concern.

They do radiation surveys either as part of regular monitoring queries or in response to a particular request.

Among other duties the Radiation Control Department independently verifies:

- on a random basis, area surveys done by other work groups
- that conditions in areas having radiation hazard signs correspond to the conditions posted on the sign
- that Radioactive Shipment Advice Forms are filled out correctly according to federal and provincial regulations
- that portable radiation instruments respond to accepted values of radioactivity
- unusual survey results arising from routine and non-routine surveys
- that numbers of protective equipment for the station use are adequate
- that all station personnel are following procedures.

Incorrect readings are occasionally made because the scale of an instrument is read wrongly. These are caught when they are compared to previous results from the area. All survey results are fed into a computer which contains a photo log of the plant. Technicians can have a surrogate photo from the area they wish to work in, in which radiological hazards are indicated.

General Comments

Some general themes which recurred during my visit were as follows:

- procedures and work plans are independently verified, but for the most part the actions to carry them out are not

- verification of actions when it does occur is for the most part paperwork verification rather than the observation of actions being taken or completed

- there is concern about the practicality and the usefulness of introducing more paperwork and more checking
- A6 -

- there is concern about watching over someone’s shoulder, which implies a mistrust of the other person’s competence
- there is concern about introducing more verification and duplication of effort unless it has a specific purpose
- there is concern that there is too much emphasis on assurance and not enough on quality.
Visit to Pickering NGS

Alison Smiley, PhD
Human Factors North Inc.

March 7, 1994

INTERVIEW WITH ANO (AUTHORIZED NUCLEAR OPERATOR)

Independent Verification

There is independent verification in work protection as two different operators write up the work protection plan. It is generally encouraged that the senior of the pair does the checking and the junior does the writing. Comparisons are made before a final work protection plan is arrived at. At Pickering, staff are starting to go to standard work protection plans for some jobs. These are stored on computer, printed out for a job and checked by a single individual.

There is a new process at Pickering, within the last 4 or 5 months, requiring independent verification before a safety system is brought back online. Before a permit is removed, two field operators must confirm the valve and tag states. The need to find a second operator for confirmation can slow work down. This practice arose from an incident at Bruce where a maintainer energized the correct piece of equipment but on the wrong unit where that particular piece of equipment was supposed to remain isolated for maintenance. This could have resulted in serious injury or death.

During abnormal events, the SOS (Shift Operating Supervisor) will check that the ANO is using the correct procedure, but does not verify specific control actions. Any changes from the design state (e.g. jumper records) are verified by a supervisor or by another operator. During normal operations, this might happen as frequently as twice per week.

During start up, both the SOS and SS are involved and check the flow sheet to ensure the process is progressing as planned. The ANO concerns himself with the equipment status, the SOS with the procedure and approval of power raises whereas the SS tends to take a larger view and is not directly involved in specific control actions or choice of specific procedures, but rather the general direction of the process.

Errors

The ANO thought most errors get caught because the unit trips. He felt panel errors where a control was left in the wrong setting were rare. Routine checks are made each shift of handswitches, panel meters, and process parameters (valve states are not included). Such checks amount to independent verification in that they are done by the incoming shift.
The ANO agreed with a statement made by an operator at Darlington that field operators seldom make serious errors because most of the critical controls are in the control room. He said that one of the most common errors involved personnel operating the correct device but on the wrong unit. This arises because of the similarity of the units. Colour coding of floors and large numbers indicating the unit have been introduced in an attempt to reduce this type of error. The operator noted that frequently this type of error does not result in a problem because the field operator often is doing a task which is harmless - e.g. topping up the oil in a pump.

With respect to being kept informed of errors made at other plants, the ANO said there is a CANDU owner's group publication, CANIT, which publishes SERs from around the world. He said the engineers may analyze errors, but he is not aware of the results of such analyses.

Consequences of Errors

When an error occurs, steps are taken to ensure it does not get repeated. It seems that the answer is always to introduce another step in a procedure or another procedure, although sometimes the problem is just incompetence.

Reducing Errors

Procedures could be written better. It seems to take a great deal of time to get procedures fixed - sometimes years. Operators who are new to a procedure may make an error because a step has been left out in the procedure, which other more experienced operators know about. Where errors are noted, a deficiency report (DR) can be written. However, the process of getting the DR acted upon is long and cumbersome.

The ANO expressed concern about workload during shutdowns. He felt the need to deal with many people requiring work authorizations, especially at the beginning of a shift made it very difficult to adequately monitor the panels. He cited an incident where an operator in such a situation had missed an alarm. He said this is not as much a problem on the day shift as it used to be, however the problem still occurs on night shifts. On the last outage, he phoned to get help. He felt there were many unusual problems that come up during a shutdown and it would be helpful to have a second operator, so that one operator could concentrate on the unit and the other on interacting with field personnel. In addition, it would be helpful to have a second operator with whom to discuss diagnosis and strategies.

INTERVIEW WITH SNO (SUPERVISING NUCLEAR OPERATOR)

According to the SNO, he spends a short time in the control room at the beginning of the shift and then goes into the field where he is responsible for getting the field operators to do what the ANO needs done and supervising their work. Routines are not supervised closely. However, depending on the training and experience of the field operator doing the job, the SNO may accompany him as he does the work, or check the work after or simply ask how the work went.
During checking, he may find things like leaks which were overlooked, and much less commonly (perhaps once per year), controls in the wrong state. This latter is most likely during shutdowns when controls are operated and left in a position inappropriate for start-up. He estimated that this might occur perhaps once a year.

Independent verification is always carried out when a permit is put in place and, as of a few months ago, when a permit is removed. The SNO will usually "walk the permit" with the member of the trade group doing the job or the maintenance foreman. There were initial concerns that the new requirements for independent verification would slow work down but in practice it has not been as difficult as people imagined it might be. Although it is sometimes difficult to find two operators to verify the isolation is correctly removed, the SNO felt this was a worthwhile practice.

Runups do not involve much independent verification. It would only occur in the sense that when a control is operated in the field, the control room operator will verify that the expected response occurs on the panel.

Efforts are being made to encourage personnel to do more self checking (stop, think (what am I doing, what do I expect will happen), act, confirm - look for expected consequences of the actions).

With respect to operating equipment on the wrong unit, the SNO said this occurs because people are used to working on a particular unit and when they are asked to work on another unit, for example during a shutdown, they will go by mistake back to their own unit. He thought there had been 5 such errors in the last 10 years at Pickering.

The SNO is made aware of errors from other plants at safety meetings which are held during supernumary days every 5 weeks.

**INTERVIEW WITH NO (NUCLEAR OPERATOR)**

The NO notices differences between SNOs in terms of their practices with regard to independent verification. Some do the tasks along with the NOs, other discuss the work but do not observe it, and others check. A lot of the differences in approach have to do with the experience of perceived competence of an NO with respect to a particular task.

The NO expressed a concern with independent verification that it resulted in people not being forced to think for themselves. If one person does the job and the other verifies it, then no one is really responsible.

Routine panel checks in the control room involve a check sheet. In the field, routines are done according to a guide, but check sheets are not used other than for specific cases involving the standby generators and emergency power generators.
INTERVIEW WITH FUELLING PANEL OPERATOR

Much of the fuelling panel operation is automated. The fuelling process involves the initiation of a series of programs to carry out the fuelling task. These can run for as long as 40 minutes before the operator is required to make any input. When fuel is sent to the bay, 3 separate programs are involved. The computer controls robotic operations which are carried out until a certain point at which the operator independently (of the computer) verifies that everything is progressing as planned and the operation should continue. The fuelling supervisor monitors the work of several fuelling operators. He can observe actions, and if there are problems, can repeat steps. If problems arise with respect to certain pieces of equipment, or if manual operations are required, the supervisor will be informed. If troubleshooting is required, the fuelling supervisor will ask that a procedure for doing it is written up so he can check it. Work involving checking the location of guarder springs to prevent tubes touching, and work involving checking for blisters in pressure tubes is always a two person job. The more senior reads the steps and checks the actions as they are performed by the junior.

I asked this operator if he had noticed that serious errors tend to occur in the early morning hours, as had been claimed by a fuelling operator at Darlington. He said he had not noticed such a pattern. He felt that errors were most likely to happen when operation was in manual mode, and logic and interlocks which guard against errors, were bypassed. In his opinion, fuelling errors were more due to equipment failures than to personnel errors. There are also errors due to missing a step in a procedure.

Prior to opening a fuel channel, the fuelling operator must verify that he is locked on the correct channel. He does this by using a camera, a periscope or x-y positions. Once he has verified the position, he reports this to the ANO. The ANO can verify which channel the fuelling operator is working on by observing a temperature drop in that channel as cooling water is put into the channel. When the fuelling operator moves fuel into the channel, the ANO monitors the changes in flux that should occur. Refuelling a channel takes about 40 minutes. During about 15 minutes of this time, the fuel is being moved. The ANO will stop any testing he is doing in order to monitor this process (i.e. temperature and flux changes).

At the start of each shift there are checks of all handswitch positions. Once a day, there is a bulb check (they do not have a lamp test, but have a second bulb instead). Checks are also carried out at the beginning of each shift in the field. Fuelling operators currently follow the same guidelines as the control room operators, in that when equipment is isolated or brought back into service there is independent verification. This operator did not see any need for more independent verification.

INTERVIEW WITH SHIFT SUPERINTENDENT

The shift superintendent supervises operations, fuel handling and maintenance.
The opinion of the shift superintendent interviewed was that independent verification was a valuable tool which should be used on a required basis, for example, when tasks were carried out where error has serious consequences. One example given was work involving the connectors feeding inputs into the control computer. Independent verification is used to ensure the control computer remains connected.

Independent verification is also used to check valves operated on safety systems, where the consequences of having the valve in an incorrect position would not be seen. The requirement for this verification is written into the procedure. Isolations done for operational, as opposed to maintenance, reasons require an OTO (Order to Operate) which has a check list associated with it.

The SS independently assesses the state of the unit and confers with the SOS to compare assessments. The SOS is more aware of being at critical steps in procedures, and does a little more checking of controls that the SS. The SS verifies key actions using procedures.

The SS interviewed felt that the new requirement to independently verify after de-isolation was appropriate and required.

When asked about feedback of operating experience, the SS said that he thought the feedback from other plants around the world was insufficiently filtered, and he doubted that many people read it.

The SS thought many errors arose from procedures not being followed. Although deficiency reports (DRs) are written, it can take a long time before a procedure is updated. He felt there was more attention paid to this issue two years ago.

He himself checks work protection permits, especially those involving electrical isolations, before approving an outage. He also looks at the overall quality of the permits being written. With respect to the preparation of permits, he prefers that the junior prepares the permit and the senior person checks it. This is essentially independent verification of the procedure.

During outages, he must severely curtail the checking of permits. However, it is not necessary to review every permit to get an idea of the quality of the work.

The consequences of an error depended on the severity of the error and the circumstances under which it was committed. Retraining may be required, however, discipline for operating errors is rare.

The shift superintendent’s opinion of the STAR (stop, think, act, review) approach was that it took years to integrate it into the workplace. He encourages and continually reinforces it and feels it has been a successful approach.
With respect to the negative consequences associated with independent verification, he believes it requires extra labour and slows work down. However, this is a small price to pay for the benefits. He feels the level of independent verification currently in use is sufficient. He did not feel that independent verification leads to people taking less responsibility for their work. In his view, most people take sufficient pride in their work that this should not be a concern.

INTERVIEW WITH AECB SITE INSPECTOR

Each plant reports about 200 SERs per year. These relate to nuclear and public safety. There are also ERs (Event Reports) or production manager reports. These are reviewed by the AECB inspector on site to ensure the incident is correctly rated. AECB does not use the International Nuclear Event Scale (INES) scale to assess incident seriousness, however Ontario Hydro does.

The major cause of SERs at Pickering is related to plant configuration (e.g. the right equipment being available). This is in contrast to the situation in the U.K., where parameters outside operational policy limits was a major concern. Where this had occurred in the past at Canadian plants, the AECB had requested backfits to install alarms to warn of this.

During operational isolations, the passive safety systems can change state. This causes indicators to change out in the field. If the control room operator verifies this with a field operator, this would be independent verification. However, this is not always done.

INTERVIEW WITH A HEALTH PHYSICIST

The Health Physics department does the following:

1) reviews and approves radiation protection aspects of documentation

2) carries out an independent assessment program which includes detailed assessments of radiation protection systems, e.g. effluent monitoring, access control systems, etc. and involves both surveys and observation of working procedures (workers are responsible for doing their own surveys - however these are verified on a sampling basis (less than 1%) by the health physics group). A second group, Radiation Control, has Radiation Control Technicians who verify 10 - 20% of the surveys done by operators. This can go as high as 40% during reactor shutdowns.

3) is responsible for dosimetry

4) gives technical advice and assistance

5) approves emergency response procedures relating to radiation protection
6) carries out investigation of radiation related incidents

7) reviews effluent results to ensure monitors are calibrated and working properly.

There are on the average about 20 SERs a year related to radiation issues. In about half the cases, the cause is either procedural compliance (not taking surveys, not wearing protective equipment, not doing the required up-front radiological work) or failure to perform the procedures adequately. This is not generally a case of missing a step in a procedure, but rather not doing surveys that they should have known were required, or not anticipating hazards that might be there.

A major focus of the Health Physics department’s work is plant tours and observation of behaviour. The Health Physics staff find it is productive to focus these tours on particular aspects of a system or particular behaviours (e.g. on one day checking that everyone is wearing a dosimetry badge).

INTERVIEW WITH PRODUCTION MANAGER

When he was part of the Reactor Safety Group at Head Office, the production manager had worked on a project at Darlington that concerned independent verification. This group determined that valves, if misplaced, might affect any of 5 areas of concern: worker safety, public safety, environmental protection, reliability and cost. Where public safety is a concern, protection against inadvertent operation of valves is generally designed in by using valves in series or by providing automatic annunciation of the valve position in the control room. No safety system valves were found to require independent verification. With respect to the other areas, these were not as adequately considered in the design. As a result, the process of deciding which valves required independent verification grew unwieldy.

At Pickering B, independent verification has been introduced where work is done in the field on safety systems and there is no direct indication of a misplaced valve or set point error, etc. in the control room.

Extra alarms and annunciations are installed and procedures changed in response to SERs. The production manager’s opinion was that this was a reactive approach. He felt it would be more productive to take a proactive approach.

As an example of the need for this, he cited the area of work protection. While there are SERs identifying deficiencies in the managed process, they probably are the "tip of the iceberg" and symptomatic of a much larger number of smaller violations. It would be helpful to determine problem areas and determine solutions before SERs result.
INTERVIEW WITH QUALITY ASSURANCE

Personnel in the quality assurance section have varied backgrounds so that a range of expertise is available. There is some performance monitoring during quality assurance audits. However, only a small proportion of an operator's job would be subject to such a performance audit. In making observations of an ANO for example, quality assurance may bring in observers from other plants. They have a mandatory topic list that they cover. They also get requests from supervisors to cover particular areas (e.g. adequate completion of work reports). This is very profitable in terms of finding problems. They also analyze SERs to determine which areas of performance should be checked.

An updated CSA standard which includes an expanded clarification of independent verification is about to be issued. A draft form of this section is available in an Ontario Hydro document on quality assurance, and is attached to this report. The standard gives supervisors guidance as to when independent verification should be required.

Work permits are independently developed by two operators and verified each time they are prepared. If there are differences of opinion about the permit, a first operator will be asked to resolve any conflict. Ontario Hydro is introducing some standard permits which will be verified the first time they are used but not thereafter.
NOTE: This Quality Principle encompasses a large scope of every job performed at Pickering NGS and therefore, requires meticulous attention to details from all procedures and information available in order to complete the job safely and efficiently.

3.9.2 Change Control

**PRINCIPLE:** CHANGES TO ACCEPTED ITEMS, PROCESSES AND PRACTICES WILL BE CONTROLLED.

Changes to accepted items, processes, and practices shall be controlled.

Permanent and temporary changes to accepted designs, items, computer software, processes shall be:

- reviewed, verified and approved before they are implemented;
- reviewed, verified and approved by persons who have full knowledge of the original intent and requirements;
- documented

A Station procedure shall be issued specifying the procedure for change control and the specific responsibilities for administering the program.

* SRP-0.4 Change Control - Systems and Equipment
* SRP-0.11 Repair, Replacement, On-Site Manufacturing and Disposal of Failed Equipment

3.10 Verification

**PRINCIPLE:** WORK WILL BE VERIFIED TO CONFIRM THAT IT IS CORRECT.

Quality work at Pickering NGS shall be accomplished by qualified personnel performing work following the quality principles. The quality will be confirmed through implementation of a verification program that consists of three parts;

- Worker performance requires attention to detail, worker self checks and is subject to an effective supervisory process;
- Field equipment is tested prior to return to service;
- Some work on equipment requires specific independent in-field inspection to confirm that results meet requirements.
Inspection and supervision are separate and distinct activities. Some examples which characterize the differences are as follows:

- All work is to be supervised; not all work requires inspection.
- Inspection is a planned, specific activity which is in sequence with the work; supervision is a continuous process.
- Work may not proceed until the specified inspection is performed.
- The results of inspections are recorded.

The method (supervision or inspection) and the extent of verification will be determined by considering the following:

(a) The degree to which the performance of work is dependent on the skill and attention of the performer;
(b) The potential impact of the work on system or equipment performance and plant safety;
(c) The complexity of the work, and the potential for error in the performance of the work;
(d) The degree to which pre-requisites such as equipment accuracy, set-up and cleanliness are important to the success of the work;
(e) The degree to which important characteristics, such as finish, clearances, dimensions, temperature, flow and pressure can be verified by test or operation;
(f) The degree to which the overall satisfactory performance of work can be verified by test or operation;
(g) The history of problems or failures;
(h) The degree to which the work is novel or routine; and
(i) The involvement of several groups, shifts, trades or organization.

Required inspection activities shall be planned prior to the start of work, including the identification of: what is to be inspected, when the inspection is to be performed, who is to conduct the inspection, method and acceptance criteria. Inspection activities shall be conducted by a person(s) who:

- have the skills and knowledge necessary to understand the objectives of the performance activity;
- can judge the acceptability of the results of the activities and can maintain objectivity.

Line management shall identify the individual responsible for ensuring that inspection activities are carried out and any resulting non conformances are resolved. In most cases this is the first line supervisor. The identity of the inspectors shall be recorded.

- **SRP-0.17** Verification
- **SRP-0.3** Preparation and Control of Maintenance Procedures
Visit to a Pressurized Water Reactor Nuclear Power Plant in the U.S.A.

Neville Moray, D.Phil.
Technosophy Inc.
1109 South Orchard
Urbana, Illinois 61801, U.S.A.

March 17, 1994

The B plant is a 2-unit Westinghouse pressurized water reactor power plant. It has been in service for more than a decade. It is also a centre for training and has several full scale simulators. Shifts are 8 hours. During the visit, I spoke to two Senior Reactor Operators (SROs), two Reactor Operators (ROs), and one person responsible for training chemical technicians and who had worked also as a radiation technician. SROs appear to be the equivalent of Shift Supervisor. All the relevant questions from the lists provided by Human Factors North Inc. were put to the personnel, omitting only those which are specific to computerized control rooms which are not present at this plant. The SROs and ROs were interviewed in pairs, since only limited time was available from their retraining program. In each interview, the definition of "verification" taken from the HFN report was read to those being interviewed, and the general purpose of the study was explained. They were then told that their answers would be kept anonymous and that no information would be made available to plant management.

The interviews took place in a Training Centre which was heavily decorated with slogans implying a dedication to excellence, to safety, and to high standards of performance. The training centre itself was very impressive and spotlessly clean. It was clear that the plant is intended to be a major player in safe and efficient performance.

REACTOR OPERATORS

Both operators interviewed had considerable experience in the nuclear industry in general, and as operators, in particular.

Procedures

1. Do all tasks you do have a written procedure associated with them?

Both A and B said that all their tasks had associated written procedures.

2. Do procedures call up independent verification procedures?
Both A and B replied "no" to this question. They stated that all tasks seen as safety related and important would tend to call for independent verification, but that many routine tasks did not.

2a. Are checks planned and specified in advance of work being done?

For tasks of sufficient importance, mainly safety related, the nature and timing of verification would be specified in the procedures. However, on the whole, who is to verify is not specified. The phrase used was "whoever is available", and this seemed to mean that it might be another RO, or the SRO. It would be another qualified person, but which one was left to an informal decision.

2b. Can such checks be by-passed?

In principle, it is possible to bypass such checks, but both operators stated that they had never seen it happen. On further reflection, they stated that in a sequence where the operators were very much in a hurry checks might be bypassed sometimes. It is not advisable to bypass checks unless there is a high radiation level, in which case verification might be bypassed if it called for exposing another person.

2c. Are hold-points established to perform checks?

This question seemed to be puzzling to the people being interviewed: it was apparent that the phrase "hold point" was not one which was in common use in their plant. In discussing this, they made it clear that verification would usually be performed at the end of an "evolution", that is, at the end of a sequence of operations which taken together constituted a procedure. In general, they seemed not to be thinking in terms of verifying steps but of verifying an entire sequence of operations. In theory, verification should be performed as soon as possible after the task is completed.

3. Who gives approval of permits to work, etc.?

The Senior Reactor Operator

Independent Verification

1. Who checks your work and how often during a shift is your work checked?

The Unit Supervisor or Shift Engineer at SRO rank performs the checks. The rate of checking depends very much on the person performing the checks. Some people constantly monitor what ROs are doing, others only check at the end of the shift. I believe that "checking" here is a mixture of two notions. One is looking over the shoulder from moment to moment, with no record being made, and the other is checking by signing off on the signatures made by the ROs when they have completed a task. It is the second of these which can be left to the end of the
shift. But these ROs were certainly indicating that there were very great differences in the rate of checking from person to person during a shift.

2. Does the frequency of checking depend on the type of job you do?

The answer was "yes". Moreover, they stated that this was independent of the person doing the checking. Safety critical tasks tended to be checked more than non-safety critical tasks. (See below under SRO for the classification of tasks and procedures.)

3. Have you ever done a task for the first time without having it checked?

RO A said "no". RO B said "yes". The latter noted that it had happened under the "old system", and he did not think it likely to happen under the new system. He was referring to the fact that early in the history of the station there had been a single Shift Supervisor for the two units. He remembered a time when, because the Supervisor was busy on the other unit, he (RO B) had had to perform an action without supervision for the first time. Furthermore, this was a supervisor who tended to check only at the end of the shift. One should probably take into account that it may be the case that ex-nuclear navy people with several years of reactor operation experience in submarines would be confident in their technical knowledge. On the other hand, they might also be expected to await orders and "go by the book" because of the navy tradition. Either way, he had performed a procedure for the first time without supervision. But in general, it happens rarely, and is much less likely to happen now when there is an SRO for each unit.

4. You are probably aware that an airline pilot has his actions independently verified by a second pilot. If your actions were to be independently verified, what would be the most practical way of doing this? (Who, when, how?)

The ROs stated that it would be impractical to have independent verification of all actions. This is because (a) there is such a range of actions, and they often occur very rapidly, and (b) the control room is so large that it would be difficult to follow a person around to verify everything.

5. Can independent verification be done by other techniques such as valve lineups, tagout checks, etc.? Are these adequate?

The answer to this was not clear. This was because it seemed that to these ROs the notion of checking was quite tightly tied to the notion of signing off formal procedure forms.

6. Can independent verification increase the likelihood of error?

Yes. Knowing that someone else was going to check your work to make sure it had been done well might reduce your concentration because you would think that were you to make a mistake the other person would catch it.
7. Is there any reason why increased verification might be undesirable?

It would slow down operations and take more time, it might expose people to extra radiation in certain emergencies, and it would cost more. In general it was felt to be undesirable.

8. Can you think of any case where had there been independent verification an error could have been prevented?

Both ROs stated that they could not think of any such case. They made the interesting assertion that independent verification could not prevent but only detect errors after the fact.

Attitudes Towards Human Error

1. When someone makes an error during operations, what happens? In particular, is follow-up action taken to ensure the mistake is not repeated?

Minor mistakes are reported and a note is circulated drawing people's attention to the possibility. For major errors (which are rare), everyone gets together and discusses the report. These meetings include management. There is a very open culture: "If anyone makes a mistake everyone knows about it". This is true even if the event is formally non-reportable to NRC. It will still be reported and discussed internally.

2. Are you aware of occasions where operators made errors which could have been avoided by having someone else check the work? If so, please describe.

There have been some in the past, and independent verification has been added. In particular, there were problems with tasks in the control logic and fuse boxes. There was a case where someone pulled the wrong fuse in the safety related logic, a "wrong train" problem.

3. What is the overall philosophy of "blame" for errors and "near misses" ("critical incidents")?

If someone deliberately violates a procedure, that is, if intention to violate is found, then the person will be "given days off". (This is a euphemism for "made to take days off without pay", that is "punished". This strikes me as a curious response to a mistake, as it may have implications for the integrity of teams, shift work schedules, etc.. But it seems to be the standard way things are done at this plant.) But for genuine errors, "It is better to be found out earlier than later", so it is as well to admit you have made a mistake.

The answer to this question was in marked contrast to the attitude which I reported from the other plant I visited. At the present plant, there was a distinct feeling of unease at discussing this question. The ROs went on to say that they felt that things went in cycles. At present,
there was a tendency to blame the operator for the error and give him "days off", whereas some
time ago there was much more of a tendency to emphasize that it is important to report errors
so that something can be done about training, improving procedures, etc.

Overall there is not much change in the use of independent verification, although there may be
currently a slight increase in its use.

Use is made of the slogan "STAR" in training. This stands for "Stop, Think, Act, Review". The
two ROs thought that this was a good idea as a general philosophy but that in practice you
did not have time to do that, and anyway, a good operator would tend to come to a state where
he did many of the procedures without having to go through such steps explicitly. It is more
part of the plant philosophy than an actual description of what to do.

SENIOR REACTOR OPERATORS

SRO A had entered the plant with an engineering degree and had 11 years of experience at the
operator or SRO level. SRO B had joined this plant also with a degree in computer engineering,
and had a total of 11 years at this plant, 5 as an SRO.

Procedures

1. Do all tasks you do have a written procedure associated with them?

The vast majority do, in particular all the safety related tasks. If an operator is walking around
the plant and comes across a leaking valve, he would tighten it without consulting anyone or any
procedure. But almost all control room activities have procedures, although there are different
classes of procedures which call for different degrees of stringency in following them.

2. What determines when a written procedure is used, and when it no longer needs to be
consulted or checked off as the task is completed? Are verification activities specified
in the procedure? Are procedures always followed - if not why not?

Procedures are classified into four types:

- Continuous use procedures - they must be open and in use and they call for
  independent verification

- Reference use procedures - they do not have to be open, but they must be
  followed (that is, memory can be used without reading).

- Information use procedures - they do not have to be open and give information
  rather than exact direction for action
Multiple use procedures - it was not made clear what these are.

In an emergency where no procedures are provided, the operator must do "what is needed to protect the plant". (This does not necessarily refer to a "real" emergency - normally EOPs [Emergency Operating Procedures] would be in the Continuous Use or Reference Use categories. But if situations arise for which there are no procedures provided, then the operator must do "whatever...".)

In those procedures which demand verification, it is so stated in the procedure. The probability of there being an explicit call for independent verification becomes lower as you get away from Continuous Use procedures. Furthermore, it seems that as you come down the hierarchy there is more freedom for the operator to act in ways not exactly in accord with the procedures. The critical thing is that the classification of procedures makes much clearer where some freedom exists. (It is interesting that no mention was made of this by the ROs.)

Procedures are not always followed exactly. Some very limited "creativity" is allowed, and if reported, can be reviewed by the Procedures group for potential inclusion in a revision of the procedures. At all times the "intent" of the procedures must be followed, whatever action is taken.

STAR is a philosophy, not a reference to a set of actions or a sequence of behaviour. It amounts to saying to people, "Before you do anything, make sure you know what the action is for".

Independent Verification

1. Do you check the work of the operators and how often during a shift do you do this?

During a shift, there is general "surveillance". Check-offs and independent verification are performed "as soon as possible after the action". During certain critical times such as start-up, there is very close surveillance and verification. During normal operating conditions, there is much less.

2. Does the frequency of checking depend on the type of job being done?

The answer was "yes". See also the answer to the previous question.

3. Do people ever do a task for the first time without having it checked?

See the classification of procedures as described earlier. The verification is not decided on the basis of the level of experience, but on which class of procedure is being used. It is certainly possible in some cases for people to avoid being checked in some classes of procedures. Part of training is aimed at inducing a sense of responsibility and sensitivity on the part of the
operator - he is expected to ask for assistance if uncertain of what to do. (Note that the answers to several of the other questions which were put to the ROs would seem different in the light of what the SROs are saying. It seems that the ROs were thinking mainly about the procedures which were by definition to be followed, not about Information Procedures, etc. Unfortunately, they were interviewed before the SROs, so it was not possible to check on this. If this is not true, there seems to be some contradiction in the data.)

4. You are probably aware that an airline pilot has his actions independently verified by a second pilot. If your actions were to be independently verified, what would be the most practical way of doing this? (Who, when, how?)

There are two kinds of independent verification.

1. "Part in action" - this kind of task requires verification to be performed before the action is taken. This seems to mean that for some tasks the operator must have someone check that the action he is about to take is correct. The SROs referred to this as "the new style".

2. "Part in time" - "the old style". Independent verification is done after the action has been taken.

More than what is done now is not needed. Independent verification is not done on balance of plant and similar actions. It is reserved for safety related actions, restoration after tests being the most frequent.

3. During or after which tasks would independent verification be most useful and practical? (a) isolation in preparation for maintenance, (b) removal of isolation in preparation for operation, (c) during or after system safety tasks, (d) prior to start-up, (e) prior to run-up, (f) during transients, (g) other.

The answer was that they did not think in that way. Verification and surveillance were thought of in relation to types of equipment or plant, not in connection with types of task. (Although note that what they said about classification of procedures to some extent contradicts this.) Independent verification is required where the equipment is safety related, and is not needed where the equipment is not safety related. (To get rid of the contradiction with earlier answers, one has to assume that the procedures are classified in a way which relates equipment to safety, not merely to task or function.)

Currently there is a tendency towards increasing the amount of independent verification. This may be related to some particular incidents, such as one where a person was sent to pull a fuse on a non-safety related piece of plant and instead pulled one which tripped the reactor on a safety system. This was similar to one of the "wrong unit/wrong train" kind of actions. Now two people are required for the task.
4. Can independent verification increase the likelihood of error?

Yes. Knowing that someone else was going to check your work to make sure it had been done well might reduce your concentration because you know that if you make a mistake the other person will catch it. The answer was almost exactly the same as that given by the ROs earlier. One of the SROs claimed to have seen this happen not in the control room but during Procedure reviews, where people became less careful and missed errors if they knew someone else was checking their output. It was also suggested that even with the "Part in Action" philosophy the effect of independent verification might be for one person to lead the other down the wrong path. "I think we should do this, don't you?...Well, yes - I suppose you must be right."

Independent verification makes the explicit assumption that the two (or more) people involved are truly independent in their perception, judgment, action, etc. If they are not, but can affect one another, then independent verification will give you less of a check than you think. And people can lose their independence.

5. Is there any reason why increased verification might be undesirable?

Cost, and exposure to hazard of an extra person.

Attitudes Towards Human Error

1. When someone makes an error during operations, what happens? In particular, is follow-up action taken to ensure the mistake is not repeated?

A case where an error led to a change in practice was the incident where the wrong fuse was pulled. This was changed to a task which now requires independent verification using two people. The pattern of work was changed in response to the error.

ROs feel that they are held to a higher standard of performance than other people in the plant, and this is probably true.

There is a document called the "PIF" (Problem Identification Form). The station is trying to encourage people to use these forms to self-report difficulties and errors. At present, there is a change going on towards a better information reporting and collecting system. Much more use is being made of PIFs and of incident reports to examine what problems happen and to try to see how to prevent them in the future.

TECHNICAL PERSONNEL

The person interviewed was originally trained as a chemist. He had 4 years experience in Radiation Protection, and 3 years in Chemical Protection. He is currently an instructor of
chemical technicians. Many of the questions did not seem relevant in the form they were asked of the other people. Late in the interview, it turned out that this was because there is a sense in which almost everything that is done by his section is implicitly independently verified (see below). The contents of his interview will be presented in a less structured way because of this.

1. Procedures

All the tasks of the chemical and radiation technicians have procedures. These procedures as such do not call for verification. If a piece of equipment is faulty, then an independent verification may be called out by marking the equipment, and by marking the step in the procedures checklist to call for that test to be repeated. There is a special sense in which this kind of work is "proceduralized": in almost all cases, the task involves writing down information such as calibration settings, followed by the readings taken. The "procedure" is inherent in the design of the form which has to be filled in: a form which has blanks is not a completed task. Putting this together amounts to saying that the design of the forms which are used to record data verify the fact that the procedures have been completely carried out, and hence whether data has been recorded which indicate that the plant is in a "normal" or "non-normal" state.

2. Are checks planned and specified in advance of work being done?

Yes

2b. Can such checks be by-passed?

No. If there is something special about the task which requires independent verification, then the technician will receive a special packet of sample bottles, equipment, etc. with a different pattern of check-off boxes, so that the task cannot be completed without the verification being performed and signed off. (The only possible way would seem to be for someone to forge a signature.)

Independent Verification

In normal conditions where samples are taken at regular intervals, for example of stack effluent gases, there is no hold point required. The technicians go about their jobs more or less independently of what is happening in the control room, and a normal permit to work is issued as a standard procedure unless there is something abnormal which calls out a special condition.

The whole question of checking is approached in a different way. The chemical and radiation technicians put data down on data sheets, and the data sheets are checked by the appropriate supervisory personnel such as the Radiation Foreman, Chemical Supervisor, or Health Physicist. The checking consists of signing off that the steps of the procedure have been carried out, that
the values of the isotopes in the calibration sample are as expected, etc.. What are checked are the results of the procedures, not the activity. This works because of the nature of the test - that it is usually a question of comparing a sample obtained from a part of the plant (such as stack effluent) against a sample of known chemical composition. Hence checking is built in. All results are checked.

There is another sense in which independent verification is done. If a chemical or radiation reading is required, then two people take samples independently within a specified time span. That is, they draw their equipment, go to the sample point independently at separate but reasonably close times, and each take a sample in the absence of the other. Each sample is analyzed independently, and the results are compared. In effect, this is an extremely thorough kind of independent verification. Any disagreement leads to resampling and re-analysis.

The person interviewed knew of one case where in the final signoff, which is the only place where only one person works unchecked, a technician had made an error by misreading 4500 for 450 when recording a sample size. He believed that had that step been independently verified it would probably have been caught and led to resampling. This was the only case he could think of. He did not believe that increasing the number of independent samples was worth doing.

It is unlikely that a newly qualified person would ever do a task for the first time alone, since their training consists entirely of doing these tasks of sampling and analysis. The most likely problem would be that some task might not have to be performed for several months after the person had qualified.

**Attitudes to Error**

The attitude of the management to errors had changed in the last two years. Earlier than that it was mainly a matter of urging the person to be more careful and not to do it again. Now increasingly errors are "rewarded" with "days off". Extensive meetings follow the occurrence of errors. Information is circulated. There is a feeling that the occurrence of one or two errors may herald the arrival of a wave of errors, which seem to come in batches. Every group will have a meeting to decide what they can best do to try to catch themselves so that the one error will not grow into a wave of errors. He would like to see more information more widely circulated so everyone can learn from it. Where errors are caught in his section, it usually leads to changes in training.

**SUMMARY**

There seems to be considerably more divergence of opinion at this plant than there was at the other U.S. plant visited. One gets an impression that to some extent people at the RO level look at the way they are doing their tasks in a way which is different from the SROs. Certainly the
question of the role of independent verification is quite different for the chemical and radiation technicians compared with the reactor staff.

What does come through is the almost universal belief that too much independent verification may lead to a loss of feeling of responsibility and increased carelessness. Whether this is true or not, of course, is an empirical question. Another point on which people agreed is that enforcing independent verification can, in certain circumstances, lead to more people receiving an undesirable dose of radiation.

There seems to be agreement that independent verification is useful for safety related operations, but that an increase in other areas is probably impractical. The notion of verification before the action vs. verification after the fact is interesting.
Interviews at Illinois Power Clinton Nuclear Power Plant Concerning Verification of Operator and Technician Actions

Neville Moray, D.Phil.
Technosophy Inc.
1109 South Orchard
Urbana, Illinois 61801, U.S.A.

February, 1994

The Clinton nuclear power plant is one of the more modern U.S. nuclear power plants (NPPs) having been completed only in the late 1980's. It has a control room which is based on computer displays with conventional hardwired displays and controls used only as backups. However, the plant is a General Electric Boiling Water Reactor (BWR) and is no more automated than other GE BWRs. That is, although the human-machine interface is more heavily computerized than most U.S. NPPs, the actual control of the plant is no more computerized than other BWRs, and far less than CANDU reactors. The term used for the verification of actions is "double verification", which implies that the person performing the action is expected to perform the first verification.

During the course of a one day tour of the plant, interviews were carried out using the set of questions received from Human Factors North Inc. The following personnel were interviewed:

- 1 Senior Reactor Operator
- 2 Reactor Operators
- 1 ALARA coordinator
- 1 Radiation Protection Supervisor
- 1 Director of Radiation Plant Protection Services.

1. Radiation Protection Technical Staff

   Supervisor - 8.5 years nuclear navy, 2.5 years supervisor at Clinton

   1.1 All tasks have a procedure associated with them. Some double verification is performed for special tasks, in particular valve line-ups and tag-outs.
1.2 It is company policy that all checks are planned in advance and procedures specified, and although this is currently not done in all cases, efforts are being made to improve practice so that everything will be pre-planned.

1.3 Procedures have checks associated with them which are normally performed by the person performing the task, but checks can always be by-passed by someone who is determined to do so.

1.4 Hold-points can be inserted in principle, but they are not used as much as they should be. In this respect also, practice is being upgraded.

1.5 Permission to begin tasks is given by the Radiation Protection Shift Supervisor, and for high risk operations the Director of Radiation Plant Protection may also be involved.

2. Attitude to Errors

2.1 The personnel stated very firmly that the company had a philosophy of encouraging self reporting of errors and minimizing a "blaming" attitude towards such reports. Rather, errors are seen as a chance for the company, plant and personnel to learn and improve its performance.

2.2 Errors are not penalized unless regulations insist on penalties. Errors are discussed in detail by colleagues involved, and every effort is made to understand why they happened and to invent ways to prevent their recurrence. Notices of the events are circulated throughout the department. All changes made as a result of discussing errors are circulated for all in the department to read. If a Notice of Violation results, procedure changes are circulated to all concerned.

2.3 Errors certainly have occurred which could have been prevented in principle by double verification. But it is impractical to verify all actions. The only rational way to choose a subset of actions which should always have double verification would be on the basis of a cost/benefit analysis. This should include a task analysis to discover where double verification would result in an unacceptable slowing down of the work sequence.

3. Practice of Verification

3.1 The practice of verification and checking is varied. Sometimes it is left to the person performing the task. Sometimes it is performed by the Nuclear Assessment Department (which seems to be responsible for overall quality control of the plant operations). Sometimes a second technician checks the work of the first technician. From time to time, audits are performed on the records of actions performed.
3.2 The frequency of checking (double verification) depends on the task. Verification by another member of the Radiation Protection Security System is increasingly being used rather than calling on other departments in the plant. (That is, another member of the same department does the check.)

3.3 Tasks are never performed by a person alone for the first time. This is because the final phase of training is essentially an apprentice format, in which the newly licensed person performs the task with an experienced member of the team (The British "Sitting by Nellie" method). But this is a matter of habit and practice - there is no formal procedure to guarantee it.

3.4 It is believed strongly that it is impractical to doubly verify everything. This is particularly true of jobs performed "out in the field" rather than in the control room or in the containment. Documentation is always checked and routine job evaluation checks are done, but these amount mainly to looking to see whether all steps in procedures have been signed off by the person performing them.

4. Computer checks

4.1 The computer system does provide some checking, although it was not designed to do so. The computer system is essentially a computer display system and is not deeply integrated into the control of the plant in the CANDU sense. It does perform logging and record keeping. Hence, by looking at the logs and records it is possible to see if some (but not all) jobs were completed and the plant left in the appropriate state.

5. Verification philosophy

5.1 If double verification were used correctly it would reduce errors.

5.2 Drawbacks of double verification:

1. It can cause more danger. If the area where the job is performed is one with high radiation levels, double verification will imply the exposure of a second worker to high levels of radiation, especially if the tasks are associated with radiation leaks. In some cases, such as certain valve line-ups, the amount of radiation will prevent the possibility of double verification. The person being interviewed contrasted this situation with a nuclear weapons manufacturing plant in which everything was checked regardless of the danger to the personnel - a case of cost/benefit analysis biased strongly in a direction unacceptable to civilian installations.
2. The interviewee raised a conceptual question. If double verification is desirable, why not triple or quadruple or n-tuple verification? If we regard each verification as being independent of the earlier ones, the probability of a fault remaining undetected will decline exponentially as shown in Figure 1. But the value of the exponent is critical. If one extra verification lowers the probability of an undetected fault substantially, then probably no more are needed. But if it is difficult for the verifier to be sure whether the job has been done well, then we need more verifications, as in Figure 2. But this leads to an unanswerable question - how many verifications are needed? To what level do we want to reduce the probability of an undetected imperfectly performed job? (This relates clearly to probabilistic risk analysis.) The interviewer believed that if the verification is performed by someone who really knows the plant well no more than one verification is needed.

2.0 ALARA Coordinator

ALARA Coordinator - Experience: has worked in 15 plants.

1. Double verification can be dangerous and undesirable due to the risk of exposure to high radiation in cases where there are radiation leaks, but may be necessary and have benefits in situations and tasks of high safety relevance.

2. The attitude towards human error of "blaming" is ineffective.

All revisions to procedures are checked by the Nuclear Assessment Department.

3. All safety-related operations have special procedures which are followed exactly. Non-safety-related tasks are left more to trust and the professionalism of the workers.

4. When exposure to high radiation levels is necessary to perform a task, the plant personnel involved are briefed concerning the procedures and carefully monitored.

5. The computer is mainly used to check the qualifications of a person chosen to perform a particular task. (This seemed not to be the same computer which runs the displays in the control room, but a computerized personnel management system. It is therefore not strictly comparable to the computer systems used in CANDUs).

6. No task is performed alone the first time. A "buddy system" is always used the first time that a person performs a task.

7. There is reason to be worried about the interaction between the "buddy system" and double verification due to the social dynamics. If someone thinks that his buddy is going to perform a check, he may be less careful because he knows that any error will be detected by the buddy. On the other hand, he may be more careful because he does not want his buddy to find that he has made a mistake. But the social dynamics are unpredictable with regard to the outcome.
Figure 1

Figure 2
3.0 **Control Room Operators**

(These interviews were conducted in the actual control room while the operators were on shift, and hence were less detailed than would have been desirable.) The senior operator had 7 years experience, the other 2 had about 1 year each. It was noticeable that the senior operator left many of the replies to one of the young ones who seemed to be, in many respects, a natural leader.

The control room is one of the more modern in the U.S.A. Although the plant is not run by the computers in the sense that CANDUs are, the human machine interface is very much a computer interface with fairly good computer graphics. There are eight 21" monitors with colour graphics at a desk where the operators sit. Behind them are three banks of conventional hardwired displays and controls for use as backups, and there are one or two more banks of hardwired instruments in other areas of the room. Most of the monitoring and control is done through the computer interface.

1. Over 95% of tasks have procedures.

2. Double verification is used "as required". An example cited was for the restoration of the plant after tests of safety systems.
   1. Verification is performed by "whoever is at hand" among the other operators.
   2. Checks cannot be falsified "unless signatures on the checkout sheets are falsified". That is, the nature of the verification is very much looking at the procedure checklist and ensuring that each step has been signed off as performed.
   3. There are no standard "hold-points". (I think there is some reason to doubt this, at least during startup.)

3. **Attitude to errors.**

   If an operator makes an error, there are discussions involving everyone who was involved in dealing with it. There is brainstorming on how to improve the procedures to prevent it happening again. Fact-finding about errors is regarded as very important. The attitude of management is to use errors as an opportunity for learning not an occasion for blame. Routing sheets make sure that the results of post-error inquiries are circulated to everyone.

4. The operators could think of no case where double verification would have prevented an error. In general, checking is done by each person on their own work and by other members of the team. There is no formal double verification. The frequency of checks depends on the nature of the task. It would be impractical to perform universal double verification because it would take too long and also it might undermine the sense of
responsibility of the individual if he believed that his errors would be picked up by someone else. In some cases, double verification is implied by the sequences of operations.

5. The computer is merely a system state display and does not give direct and immediate feedback of the identity and nature of the actions taken, hence it cannot play a direct role in verification.

6. The operators made the same point that was made by the ALARA director - double verification might be distracting, because of the feeling of someone "looking over your shoulder". The social dynamics are uncertain. If afraid that your supervisor might notice your error you might improve, but if you expected that any error you made would be picked up by the supervisor you might become careless. These effects plus the distraction effect would make the value of double verification very uncertain.

4. **Comment**

The management of the plant changed about 3 years ago. The previous manager had been very authoritarian and worked "by the book". He had been very unpopular. (Indeed one or two people actually used the word "hated".) The interviewees all remarked that there had been much more verification under his rule - even triple verification. Currently, verification is used less often and more verification procedures are less formal. But the new management is very popular. There is a feeling that the manager understands the workers and is dedicated to making the plant efficient and of high quality. He is clearly very popular, and in particular the attitude to human error is seen by the employees as being admirable. They are not afraid to report their errors, and they know that the result will be that the information will be used for the welfare of the plant as a whole. Morale is exceptionally high. It is clear that the manager has produced a situation where people will work very hard and conscientiously to repay the trust that is being put in them by management. Part of this results in the fact that less formal verification is used, but the plant has recently received a comment from NRC as to how much it has improved in the last year. The comments on the social dynamics of verification (distraction, motivation) are very interesting, as are the comments on the cost/benefit aspects of exposing people to high radiation (or high hazards in general) in order to carry out verification.

If further information is required about this plant, there is no problem arranging a return visit. Note that this is the plant which was visited by our Dr. Sanderson who spoke to the Shift Supervisors in late 1993.
APPENDIX E

Visit to U.S. NRC

Alison Smiley, PhD
Human Factors North Inc.

January, 1994

On Wednesday, January 12, 1994, I visited the U.S. NRC and spoke with personnel of the Human Factors Engineering Section and Quality Assurance. The Quality Assurance representative had spent 8 years as an on-site NRC inspector and 2 years as a Specialist Inspector.

The U.S. NRC "covenants" with its licensees to have programs in place to achieve various ends, for example, quality assurance. Quality assurance programs are required which will involve random checking of operator actions, as well as verification of programs and activities. The licensee may agree to have certain types of independent inspection in place, in which case this agreement is legally binding. However, how the licensee designs its quality assurance program is an individual plant matter, and not proscribed by the NRC. NRC resident inspectors carry out random checks of operations. This can involve spending time on a daily basis in the control room talking to and observing operators. Once a month, the inspector goes through the valve line-ups for a particular system safety test. NRC resident inspectors review log entries and observe start-up procedures. (Although they are not usually operators themselves, inspectors must pass an equivalent of an operator licensing exam.)

A number of types of independent verification in operations at American plants were identified. Independent verification is required when any safety critical system is operated, whether this is during a system safety test (surveillance test), or during an emergency. Verification occurs when elements of a safety system are isolated and when they are brought back on line. Independent verification occurs through checks of log entries and panel checks carried out by oncoming crews.

All utilities have a Shift Technical Advisor (STA). Most plants have an STA assigned to each shift. This individual is responsible for checking operator actions and is required to be within 10 minutes of the control room at all times. The STA monitors but is not a supervisor and thus is independent of the operators. All utilities have an STA.

Some, but not all, procedures have checklists associated with them. Emergency operating procedures have check points. At some plants, the use of emergency operating procedures involves independent verification. Because of the complexity of these procedures, one operator will read the procedure, another will carry it out, and a shift supervisor will verify the actions are correct. At other plants, the shift supervisor will read the procedure and the operator will carry it out. However, the shift supervisor does not verify the actions of the operator. Sometimes when such procedures are used, the operator verbally repeats back to the supervisor
what he is doing. However, this practice is sporadic and varies from utility to utility and crew to crew.

ANSI standards require independent verification of tag outs on safety critical systems. All such tag outs are approved by the shift supervisor, but carried out by an operator. During refuelling, there might be 10 to 15 tag outs per day whereas during normal operation there would only be 1 or 2. About 20% of tag outs relate to critical safety systems and require independent verification by an independent auxiliary operator. One per cent or less of such tag outs would lead to a reportable error. A root cause analysis approach would be used to investigate these errors. Errors which are repeated lead to stronger action by the NRC and can lead to civil penalties in the hundreds of thousands of dollars. Most plants have had at least one such fine levied.

When new work plans are carried out the system engineer may or may not be involved in checking the progress of the plan. This varies from plant to plant and from engineer to engineer.

Independent verification does not eliminate operator errors. Errors have occurred because the personnel who were required to do an independent check in fact did the check together. This may happen because of time pressure or because of the type of check required. It is particularly tempting to do this when a valve is difficult to locate or when a valve is to be operated in a radiation environment. In one incident, 6 operators reached their radiation exposure limit one after another trying to locate a valve in a radiation environment. Finally, it was determined that the valve had been removed from the area but the drawings had not been updated. Better diagrams, photos, or videos would assist in locating valves, especially in a radiation environment.

If a valve that is difficult to reach must be opened or closed, it is tempting for the independent verifier to look at and try to ascertain the position of the valve based on the stem’s height or a valve position indicator (VPI), rather than try to move it, and assume that the first person placed the valve in the desired position. The operator can be misled about the actual position of the valve because the position indication is not maintained. Even on a motorized valve with a dial, the closed and open indications can become shifted. False indications that valves are open or shut, as occurred with the pressure relief valve at Three Mile Island, can still occur. However, people are certainly wary of this problem. Also, acoustic devices have been installed to detect flow and therefore reduce the likelihood of a false indication.

Where independent verification is required, documents and managers should make clear that these mean independent in time and space. If it is determined that two persons responsible for independent verification worked together, this is considered cause for concern.

Independent verification can also fail because of poor human engineering design. In some cases, inspection was independent, but both operators operated the wrong valve because of poor labelling. Failures can also occur because of incorrect procedures. Finally, inattention can occur because the check was cursory, or the person involved was preoccupied. There was some
disagreement among the group of NRC personnel interviewed about the frequency of such errors of "inattention".

U.S. plants file approximately 2,000 significant event reports per year, or an average of about 20 per plant. Plants vary greatly in the likelihood of reporting an error. (Some just don’t describe the circumstances in sufficient detail to identify human factors implications.) Analysis of licensee event reports have shown that 52% of event reports involve human error. Of these, 73% involve procedural errors. There is some difficulty in defining why the procedural errors occurred - whether operators were trying to follow a procedure and missed a step or were taking a short cut.

Generally, the NRC personnel interviewed at this meeting were satisfied with the level of independent verification currently used at U.S. plants. Within each plant, a quality assurance group independently verifies programs and activities. Paperwork is checked and performance is sampled from time to time. Each shift does panel checks. Besides the plant’s own quality assurance group, there is a shift technical advisor who does independent verification on an ongoing, though not formal basis, as well as an NRC site inspector who samples performance of various activities. Lately, each facility management has been encouraging plants to have their supervisors check what plant and auxiliary operators are doing, and verify the quality of their work.
Visit to Hartlepool Power Station, U.K.

Alison Smiley, PhD
Human Factors North Inc.

January, 1994

Hartlepool Station is a 2 unit station, with each unit generating up to 660 MW. The plant design is an advanced gas cooled reactor, using CO$_2$ gas as the cooling agent. The plant is designed for on-line refuelling. However, this has not yet been achieved. Currently, refuelling is done with the plant in a shutdown state and occurs 3 times a year per unit, taking approximately 12 days each time. The plant has been in operation since 1983, but has only recently fully finished the commissioning process.

Staff complement is currently at 640. Over the next few years, it is anticipated that this will be reduced to 600. Hartlepool is one of 16 nuclear power plants in the U.K. which together produce approximately 20% of the electric power.

General Information re Plant Operation

The Shift Charge Engineer is in charge of operations. He sits outside the control room. Under him are two Assistant Charge Engineers, one who looks after plant operations and one who looks after the control room. The plant operators are divided into two groups, one looking after the reactor side, and the other, the conventional (turbine) side. Most maintenance is done during the week, Monday to Friday, between 0830 and 1630, starting 1 hour after the desk operators’ shift starts. There are also maintenance crews on shift.

There is much emphasis placed on self-checking - a recent training campaign encouraged people to Stop, Think, Act and Review (STAR). There are also safety campaigns where compliance with various targets (e.g. wearing of safety helmets) is posted. The degree of compliance determines the size of bonuses paid out to workers.

Interview with Desk Operator

The desk operator is equivalent to a first operator (ANO) in a Canadian nuclear power plant. The operator I spoke with had 4 years operating experience and had worked at the plant for 6 years. The desk operators have bachelor’s degrees in engineering or an equivalent qualification and go through a training period of 1-1½ years prior to starting desk operation. Their training period includes time on the plant floor, courses on advanced gas reactor physics, simulator training at Oldbury, operating the panel with an experienced desk operator ("sitting by Nellie"), and a final training period during which they operate the panel, but a fully qualified desk operator is working out in the plant, ready to back up the trainee should any serious situations develop.
The desk operators work 8-hour shifts on a 2-2-3 rotation. They spend 1 day out of 5 on average working out in the field. This is viewed as important for keeping in touch with the state of the plant and for providing some variety in the job.

The control panels have few annunciator panels - perhaps 2 dozen. These are general alarms backed up by a computer-based alarm system. The operator uses a conventional panel to operate and also has 6-8 video display terminals (VDTs). Two of these are dedicated to alarms (colour-coded and prioritized and only first out alarms and major causes alarm pages are displayed). The other VDTs can be used to monitor different systems at the operator's discretion. There is also a VDT on the operator's desk which can be used to call up trends of various parameters over various time periods.

*Verification Activities and Use of Procedures*

Most tasks (99%) have a specific written procedure associated with them. Sometimes, fault finding is required for which no written procedure exists. This occurs less than once per month.

With respect to verification activities specified in the procedure, during start-up, there are hold-points at which time the desk operator checks all standing alarms as being OK or investigated. These are rechecked by the Central Control Room supervisor, prior to the desk operator continuing. There is an informal system in place whereby an additional desk operator will assist with start-up. On shift changeovers, there are panel and alarm checks.

Also during start-up, there are hold points to check the guard lines. These are safety circuits that monitor trip parameters. There are four parallel systems. Two out of four are needed to trip the reactor. If certain protections have been vetoed, these are checked by maintainers in charge of instrumentation and control and by the shift assistant engineer prior to the desk operator continuing with start-up. Also, there is a requirements to double staff the operating desk for start-ups after refuelling. A specialist reactor physicist is also required to be present.

The Assistant Engineer Operations (equivalent to an ANO) commented that in his opinion it would be difficult to define any activity which would benefit from an independent verification process other than the application of major plant isolations to help ensure that all points of isolation covered all planned work and did not degrade nuclear safety. Isolations are applied by operations staff.

During shutdown, there is a hold-point at which the adequacy of core cooling is reassessed by the Assistant Engineer Operations together with the Assistant Shift Charge Engineer.

During normal operation, the only hold-points relate to refuelling. Prior to the plant being handed over to the fuelling team before a fuel stringer is removed, the gas flows are checked to be correct. The desk operator uses a checklist to do this and the fuel route team leader also has a copy of this. These are self checks, however, rather than independent verification.
For the most part, operation is alarm driven. Each alarm is associated with a SOI (station operating instruction), a procedure which is presented in flowchart form and which is supposed to be followed by the operator. Operators are explicitly told to use the written procedure and not to memorize it. Only a few SOIs, for example, those involving assessment of reactor power, have checksheets associated with them. These are filled in by the operator himself and not independently verified.

With respect to the handling of transients, alarms refer to SOIs, which rarely have hold-points associated with them. One Assistant Shift Charge Engineer said there are insufficient resources to allow an independent check.

At every shift change, there are routine checks made, for example, of valve states. These are checked by plant operators who communicate them back to the Assistant Shift Charge Engineer. There are also checks of plant availability by plant operators (equivalent to safety system tests). A schedule is used whereby different systems get checked with various frequencies and everything is checked at least once every 3 months.

When a procedure is used for the first time, there is a formal process whereby a supervisor witnesses the use of the procedure. Operators or maintainers have the opportunity to provide feedback about the adequacy of the procedure and suggest changes. The person responsible for writing the procedure (the owner) must record his decision on the maintainers' and operators' comments. For old procedures, there is a "document amendment proposal form" which can be submitted by anyone. This goes to the "owner" of the procedure who assesses it and may amend the procedure.

**Consequences of Error**

There is a "no blame" policy in effect. However, if safety operating rules are contravened, even inadvertently, then disciplinary action can be taken. A recent event involved an Assistant Shift Charge Engineer operating a transformer for number one unit when number two should have been operated. The two other panels relating to the transformer have unit one on the left and unit two on the right, however, this panel is reversed. Since there have been similar errors before, the switches have covers over them. The idea is that operators will stop and think before operating them. The engineer involved had just been working on unit one. Because of the seriousness of the error, he and the Control Room Supervisor were disciplined.

Recently, there have been a number of errors with commercial rather than safety implications. These have not resulted in disciplinary actions against those involved.

There is an abnormal event reporting system. Information on these is circulated throughout the plant. Twice a year, the desk operators meet with the Operational Feedback Engineer to discuss relevant incidents at their own and other nuclear plants. Currently, a near miss reporting system is being developed.
Interview with Shift Charge Engineer

The Assistant Shift Charge Engineer sits in the centre of the control room with his desk oriented so that he can observe the panels of each of the 2 units. Behind him are the common services and electrical grid panels. Several years ago, overview panels were installed on each of the 2 units so that the Assistant Shift Charge Engineer could better follow what was occurring to the units during normal and abnormal conditions (e.g. reactor trips).

The Assistant Shift Charge Engineer is responsible for ensuring the operators comply with regulations. He sanctions access to safety systems. He approves permits to work. He does most of the work dealing with phone calls to the control room. He communicates with the desk operators as to the isolations that are to be carried out on their units. He may offer advice on strategy in a transient. During transient conditions, operators rely to some degree on their operating experience and may not always go step by step through the SOIs (station operating instructions).

According to the Shift Charge Engineer, most reported incidents are rule transgressions, rather than operators inadvertently operating the wrong switch. Sometimes it is not obvious at the time of the incident that a rule (for example, about how high a pressure may rise) is being transgressed. This is particularly so where such rules are transgressed but no alarm is generated to warn of this.

With respect to independent verification, there are holdpoints related to safety systems only. After a safety system is isolated, maintainers carry out the required work. Once the system is brought back into service, the operators carry out function testing as well as a valve alignment check. This is signed by the Assistant Shift Charge Engineer. The safety system is not considered available until these checks have been made. These checks catch most errors which involve leaving controls in the wrong settings.

Independent verification has been introduced for checking that sufficient fire systems are available. To isolate these systems requires the operation of 30 to 40 switches. Twice it happened that everything was isolated when operating instructions required that some fire systems should be available at all times. There is no alarm to warn of this error. As a result of these errors, there is independent verification by other operational staff.

Interview with Fuelling Operators

A fuelling operation foreman (now called a team leader) was interviewed. He and his staff are responsible for refuelling. Nearly every fuelling job has a checklist associated with it. Prior to start-up, the foreman checks valves and gauges and communicates with the control room operator as to the state of the fuel route, plant and related equipment. These checks are also done routinely during normal operation. There are also routine weekly and monthly checks. However, 9 out of 10 times nothing changes, so errors of having valves in the wrong state are rare. If they occur, these are most likely due to contractors leaving the plant in an incorrect
state or, in the opinion of the foreman, to carelessness of workers. When asked about the consequences of error, the foreman said his response was to give the employee involved "a good dressing down".

Contractor errors and fuelling worker errors have been reduced greatly. This is thought to be due to greater experience on the part of the contractors as well as to the introduction of a bonus scheme. This bonus scheme is linked to commercial costs of errors and absenteeism. The bonus is substantial - $2,000 per person per year.

We observed the fuelling machine control panel. Valve position lights were poorly illuminated and the CRT displays were oriented so that one got a stiff neck looking at them. Several switches on the panel operated equipment which was rarely used and these switches were covered to prevent inadvertent operation. A perspex window under the operator’s seat was intended to allow a view of people moving about the fuelling machine below, however, the condition of the window was such that it was difficult to see through.

Interview with Operations Feedback Engineer

Most plants have two operations feedback engineers whose role is to 1) investigate (using a root cause analysis for serious events), 2) keep a database of incidents, 3) keep informed of incidents at sister plants and at plants of other types, both in the U.K. and internationally, and 4) keep operations staff informed about pertinent incidents at other plants. There are on the order of 4 or 5 abnormal events reported per week, and 3 incidents reported per month. Abnormal events are unexpected occurrences during operations or maintenance. The events are reported if they have or could have nuclear or industrial safety or commercial implications. About 30% of these are recorded formally as a site licence requirement and brought to the attention of the NII. The main reason for human factors problems is that procedures are not followed, either because the individual is unaware the procedure exists, or because the individual carries out the procedure from memory and a change has occurred of which the individual is unaware. A directed reading program exists to keep operators up to date on changes in procedures. However, they sometimes lag behind. The engineer we spoke with said that approximately 60% of incidents involved human error; of these, 23% were related to design, 31% of an inappropriate action (slips or mistakes), 35% to procedural faults (mistakes in the procedure, failure to follow procedure).

Interview with Health Physicists

The main work of the health physics group on an advanced gas reactor plant is to ensure compliance with statutes concerning radiation levels and to put into action systems for monitoring and controlling doses. In addition, this unit ensures monitors are calibrated and ensures adequate protective equipment is available. At Hartlepool, there are 8 professional health physicists and 15 support staff.
Most radiation surveys are concerned with the fuel route. Compliance with transportation regulations for fuel has to be assured. Surveys are done of every area on a weekly or fortnightly basis. Paper records are kept. Due to the nature of the shift schedules, surveys are usually carried out by a different person each time. Actual comparisons with previous surveys are not made unless radiation levels look different from normal. Most radiation levels are nil, therefore higher values are noticeable. Areas of the plant with non-zero radiation levels are discrete and well-defined. Thus, there is a fairly stable pattern of radiation and changes from it are easily detected. Bands of radiation are defined very narrowly (e.g. <7.5, 7.5-25, 25-500, >500 pC/s h⁻¹) and areas are seldom designated as "hot spots" as is the case in practice in other countries.

Portable radiation monitors are fully recalibrated annually and performance is checked quarterly. Health physicists interviewed were unaware of any occasions when mistakes were made due to the selection of a wrong scale. Most of their instruments use a single, full scale in any case.

A recent event which resulted in a reportable incident involved radiation protection rules not being followed on a maintenance job. The radiological section had assumed the maintainers knew what was required and had not posted the required warning signs.

With respect to contamination, in half of the events no clear reason can be found. There are approximately 2-3 contamination events per year. However, doses are low. Last year no one exceeded ½ mSv. In 10 years of operation, no one has exceed a dose of 1msv.

With respect to independent verification, there are two situations in which it occurs. The first is in the final checks on the fuel flasks before shipment. The survey involves 65 points, not all of which are clearly indicated. Two people carry out the survey together.

The second is in the making up of solutions for dosimetry. Solutions for developing film badges are made up by one health physicist while a second health physicist witnesses the procedure.

Up until the present, health physics has been responsible for monitoring radiation levels for individuals in the plant. There is a move towards having individuals do this for themselves - "self-monitoring".
Visit to Nuclear Installations Inspectorate, U.K.

Alison Smiley, PhD
Human Factors North Inc.

January, 1994


Conversation with Personnel in Quality Assurance

NII Regulatory Role

The principal concerns of the NII are policy, inspection and assessment in nuclear installations. The nuclear plants are like Canadian Crown corporations in that they are independent but government employees sit on the Board of Directors of each plant. Similar to the situation in the U.S., the NII sets requirements in a non-prescriptive form. It is up to the licensee to determine how to meet the requirements. The plan produced by the licensee becomes a part of the licence.

In the past, the quality assurance group has been mainly concerned with ensuring adequate documentation. Now, more emphasis is being placed on team inspections. These involve a multidisciplinary team usually consisting of 2 site inspectors and 2 subject matter experts. The site inspector for the plant will choose the area of plant operations that will be scrutinized. This will generally be associated with areas that have given rise to a number of concerns or incidents. Team inspections are normally led by the site inspector, however some inspections biased to Q.A. (audits) are led by the Q.A. group.

Modifications to the plant may require NII approval but not necessarily. For a major modification (category 1), the NII must give its approval. For modifications with fewer safety ramifications (category 2 and 3), the NII may be involved. Each plant type (e.g. magnox or advanced gas reactor plants) has a nuclear safety committee to advise station managers on safety. This committee is headed by an individual from the licensees’ Health and Safety Directorate. The committee also includes members from the licensee plants (i.e. station managers) as well as independent members, such as university professors.

When modifications are made or new equipment is installed, a number of inspections take place. The licensee itself (e.g. Nuclear Electric) inspects the installation or modification. The manufacturer inspects the installation and there may be a third independent inspection for or on behalf of the NII. When 3 such inspections are involved, there is concern about who is responsible for acceptance and who has responsibility for any problems found later. At a new plant, i.e. Sizewell B, the manufacturer, licensee and independent inspector (Lloyds Register)
are all involved. In addition, the Institute of Mechanical Engineers monitors certain critical ASME components.

**Licensing of Operators**

With respect to the safety of operations, the NII rely heavily on well trained operators and on the plant to provide adequate training. The licensee presents NII a training program, which the NII must approve. However, unlike the AECB, the NII does not license individual operators although some in the NII feel they should. (This is also the case in Germany and France. However, the Finnish regulators do license their operators.)

The station hierarchy comprises a station manager, a number of department heads, either 3 or 4, one of whom is responsible for production which includes plant operation. On a shift basis, there is a shift charge engineer, 2 assistant charge engineers, one in the control room and one supervising plant operations. There are also assistant engineering operators in the control room for each reactor unit (Desk Operations) and 2 or 3 others covering the turbine, reactor, and fuelling. These are supported by foremen who have responsibility for general workers.

Permits for Work (PFW) are intended to achieve safety from the system. This is usually achieved, where appropriate, by the use of isolations and precautions. The maintainer or foreman (known as the "competent person") signs to indicate that he accepts and understands the PFW. The maintainer can inspect the equipment before working on it but is not formally required to. Sometimes, the system is such that checking is impractical and impossible to carry out. Consequently, permits are usually signed without inspection. If something goes wrong regarding the safety of the isolation then it is the "authorized person" (i.e. the person who carried out the isolation) who is held responsible.

**Conversation with a Representative of the Health and Safety Executive**

In 1974, a Health and Safety Executive was formed, putting inspectors for most industries including the nuclear industry within one government department. The railway inspectorate joined after the Clapham Junction accident, and the oil rig inspectorate, after the Piper Alpha accident. With this structure, the Health and Safety Executive can draw on experience in a number of different industries in promoting health and safety policies. A current interest is in the measurement of health and safety performance within a safety management system. The Health and Safety Executive wants to promote the use of upstream measures rather than simply looking at injuries and accident safety after the fact.

The inspectors have found that they are much more effective in influencing health and safety for large numbers of workers if they approach the Boards of Directors of companies rather than individual company managers at site level.
The value of paperwork records as a basic method of ensuring jobs had been done, at a given
time, by authorized personnel and the drawbacks of depending on paperwork verification were
discussed. One example given involved an explosion at an explosives manufacturing plant.
Investigation after the accident showed that safety regulations were routinely flouted. The
explosion occurred at one point in time, yet records were found covering work 3 hours later.
Some auditors look mainly at records, and can miss unsafe practices and misrepresentation such
as occurred in this incident.

The Health & Safety Executive representative was not aware of much effort in the area of
independent verification. If anything, there are pressures against this. Currently, industry in the
U.K. as elsewhere, is "right-sizing". This means self-checking rather than independent
verification. It also means trends to multi-skilling of trades, where individuals do certain
maintenance on machines they use. This raises questions of adequate competence and, in the
long run, safety. There are also trends to automation to protect against worker errors such as
at Sizewell B where a computerized protection system guards against unsafe machine states being
selected.

Conversation with Personnel in Human Factors

Seven years ago, the human factors section was started at the NII. Most work until recently has
related to the design and operation of new plants rather than to ongoing operation and analysis
of errors. One representative had worked for Nuclear Electric for some years. In his experience
there, procedures occasionally had holdpoints for independent inspection, however, this was not
a standard approach. If anything, there were more holdpoints associated with the fuel route than
with operations. Carrying out on-line refuelling with advanced-gas reactors has proved difficult
despite the reactor being designed to allow this. Because of problems with the reliability of
computer control, there is more human operator involvement than originally anticipated.
Reliability of performance is critical. This has resulted in the introduction of independent
verification requirements for successive stages in the preparation and use of the fuelling
machine.

Start-up and power-up require paperwork verification only in that a second signature is required
to continue past certain holdpoints. No inspection group per se exists at the stations. However,
there is a yearly self-audit program, involving observation of various operations by quality
assurance people from the plant. This is independent verification of a sort, but on a sampling
rather than a routine basis.

With respect to the analysis of incidents to determine whether independent verification would
be helpful, the NII do not have access to incident details unless safety systems are involved.
Even then, the detail which would be needed to determine whether independent verification
would be of assistance is not available. Interviews with personnel involved in an incident would
only be carried out by NII for major incidents.
Nuclear Electric (the biggest utility) has adopted the Institute of Nuclear Power Operations (INPO) approach to human performance evaluation systems (HPES). This has worked well so far but there is still a lot of training to be accomplished for the individuals involved.

An attempt is being made to use information from incidents to improve human performance. Each plant has an operations feedback engineer, whose job it is to analyze incidents and feedback knowledge gained not only from incidents at the plant in question, but also from incidents at plants of similar design, and plants of other designs. The knowledge is used in modifying training and procedures to improve safety. The operations feedback engineer carries out root cause analyses on a number of incidents each year. He meets with the operations staff on a regular basis to provide them with feedback.

NII receives reports on 10's of incidents per plant per year. Each plant has its own incident registry which will contain 30 to 40 incidents per year. An attempt to start an anonymous reporting system for "near misses" was tried at one plant. The idea was to model this after the anonymous reporting system used in aviation. Unfortunately, this system was introduced just as the nuclear industry was starting staff reductions. There was a great deal of mistrust of management motivation and few reports were filed. We discussed the need for a clearly independent body (such as the Federal Aviation Authority [FAA] in the U.S.) to monitor and analyze reported incidents. (Within the Canadian nuclear industry, Atomic Energy of Canada Limited [AECL] was suggested as an appropriate body.)

Conversation with Personnel in Incident Analysis

Licence Condition 7 requires licensees to make arrangements for the notification, recording, investigation and reporting of incidents. As a result, licensees must have adequate arrangements for the analyzing of incidents from their own sites and for those from other sites. Nuclear Electric has documents (MCP 18 series) which specify requirements for identifying and reporting incidents.

The International Atomic Energy Agency (IAEA) International Nuclear Event Scale (INES) is an internationally agreed scale for rating the severity of incidents with respect to safety. Persons on nuclear power plant sites will classify an incident on this scale. A rating of 0 or 1 is a low level, which the licensee will investigate on site and report as required by MCP 18. An incident rated at INES level 2 or above is reported to the IAEA in Vienna; this is an IAEA requirement. The reporting is done by the NII who check the rating. In the U.K., there are about five incidents per year rated 2 or above, and one or two hundred at the 0 and 1 level (Chernobyl was rated 7). In the case of at least one licensee, there is a company bonus system dependent on the number of incidents occurring per year at the INES level 2 or above. This is likely to influence the rating of the severity of incidents.

If a breach of a Licence Condition occurs, the NII may take regulatory action, which in an extreme case could result in a prosecution and fines being levied on the licensee by the Courts.
Less extreme action the NII could take would be the issuing of an "improvement notice" on the licensee, requiring, for example, an improvement in procedures or training.

MCP 18/1 specifies what incidents should be reported to the NII and how soon they should be reported; generally within 24 hours, to be followed up by written confirmation. These are known by the NII as "Fast Stream" reports. There is also a system whereby the more severe, or politically sensitive incidents are reported to the Secretary of State (Department of Trade and Industry), so that he is appraised of the event if/before questions are raised in parliament or by the media.

Personnel in Incident Analysis are in the process of developing a data base of incidents for the reactor inspection branch of the NII. Currently, most of the information in this database is from one company, Nuclear Electric. NII is not yet involved in trend analysis of incidents but expects to start doing this, and also expects to use the incident data as an input to safety performance monitoring. The result of safety performance monitoring could help decide how NII inspection resources should be used - for example, more inspection resource might be allocated to plants with poorer safety performance. Under the current system, all plants receive the same basic inspection program. The data base is also likely to be most helpful in answering parliamentary questions.

Trend analysis, to varying degrees, is done at sites by the operational feedback engineers. In addition, there is a Central Feedback Unit at Barnwood (a part of Nuclear Electric, but also funded by Scottish Nuclear Ltd. and British Nuclear Fuels Ltd.). In some ways, it is a national equivalent of INPO in the U.S. Plants report not only safety-related but also production-related events. On the order of several hundreds of events per year are reported. Many are summarized and circulated to all plants in NUPER News, a nuclear industry newsletter. The operational feedback engineers at each plant ensure that this information is fed back to the appropriate personnel in their plant.
Visit to Mihama Nuclear Power Station, Fukui, Japan

D.J. Ostry, PhD
Human Factors North Inc.

February 2, 1994

On February 2, 1994, I visited the Mihama Nuclear Power Station, a 3 unit pressurized water reactor of Kansai Electric Power Company. The purpose was to obtain information about independent verification in nuclear power plant operation in Japan. My visit to Mihama consisted of a tour of the facility and a group meeting with the following representatives of Mihama:

- Assistant Superintendent
- Manager, Engineering Section
- Manager, Simulator and Operation Manual
- Assistant Manager, Nuclear Planning Group
- Fukui Prefecture, Quality Control Centre
- Engineering Section.

The meeting was also attended by a Senior Researcher from the Ministry of Science and Technology and a Conference Interpreter.

Subsequent to the meeting at Mihama, I interviewed a representative of the Human Factors Research Laboratory, Japan Atomic Energy Research Institute, Ibaraki Prefecture.

This report provides a summary of my discussions at Mihama. I describe the practices associated with verification of procedures and, for comparison purposes, those associated with the verification of maintenance. I have appended to the report, as Annex 1, a document given to me at Mihama which gives an overview of operations.

Verification of Procedures

There are written procedures and accompanying checklists for almost all operations at Mihama. The operators complete the checklists and the supervisor and/or technical advisor approve the work. I was told at Mihama that the check list is completed as the work is carried out. However, the Human Factors Research Laboratory representative said that check lists are not actually used in this way in the facilities he is familiar with. Procedures are memorized and check lists are completed afterwards. Written procedures may be used during start-up and power shifts but not during regular operations.

The role of the supervisor is to verify the actions of the operations staff but there are, in general, no explicit procedures for the verification of routine operations. For important items, I was told
that supervisors check the work and that for critical operations outside of the control room, the technical advisor goes to the site. Typically, the head of a section within the plant decides what needs verification.

During patrols, one person checks a patrol sheet, which is signed by the shift supervisor and technical advisor. The technical advisor sometimes accompanies the patrol and sometimes checks particular equipment. There is apparently a detailed patrol sheet for operations related to the emergency core cooling system and the auxiliary water pump.

Although there appears to be no independent verification of routine operations, I was told that there is independent verification during start-up and connecting to the grid. In these cases, the chief engineer verifies parameters in the control room. In general, working together during more critical procedures was emphasized.

Plans for monthly and periodic tests are submitted to the Ministry of International Trade and Industry (MITI) and after their completion a report is made to MITI. I was told that sometimes during critical tests MITI observes. However, as the Human Factors Research Laboratory representative pointed out, although MITI has a schedule for start-up they don’t check operators’ actions.

In a follow-up telephone interview with the Assistant Manager of the Nuclear Planning Group, I was told that there is no inspection by MITI after power fluctuations. However, an on-site MITI inspector is available and is informed when significant fluctuations occur. After stabilization, MITI may check parameters in the control room and in the field.

Verification of Maintenance

For comparison purposes, I inquired into the practices in Japan for verification of maintenance. I was told that the maintenance schedule is dependent on the type of component - valves monthly, pipes weekly. (In February 1991, a pipe inside the steam generator of the Mihama No. 2 reactor ruptured causing a loss of primary coolant. The emergency core cooling system was activated, apparently the first such incident in Japan.)

A data-base of part failures is maintained and maintenance is scheduled partly on this basis. There are three levels of maintenance verification: in-house verification, daily routine inspection by an on-site representative of MITI and annual inspection by a team of MITI inspectors.

Maintenance is not carried out by Mihama employees but is carried out by independent contractors. I was told that the maintainers work is checked by their supervisors. Mihama personnel verify that maintenance has been carried out correctly. In addition, sub-contractors provide maintenance specialists to observe critical work. Less critical work is verified by the superintendent for the contractor.
Contractors apparently prepare step by step work plans for both preventive and corrective maintenance. Written procedures are used for all maintenance.

I was also told that there is a daily meeting between the Kansai maintenance staff and the subcontractor. On the basis of a schedule submitted to Kansai Electric by the contractor, a decision is made concerning what to verify. This is not specified exactly.

I was told that, even in routine maintenance, the maintainer works from a check sheet and that supervisors go to the work site to verify the work of their subordinates. Verification points are apparently written into the maintenance procedure. There was a general consensus among the senior personnel that I talked with that this general account is essentially correct.
Annex 1 - Operation

1. Organization Chart of Plant Operation Section .............. H5
2. Working System ............................................. H6
3. Training Pattern of Operator (example) ................. H7
4. Qualification Grade and Assignment of Operators (for operation) ........................................ H8
5. Principle for Safe Operation .............................. H9
   Purpose of Guideline for Safe Operation ................. H11
   Prevention of Re-occurrence of Human Error .......... H12
6. Start-up curve for a PWR power station (example) ...... H13
   Shutdown curve for a PWR power station (example) .... H14
7. Standard for automation (Mihama Unit 3) ............... H15
8. Standard and Instructions System (operation room) .... H17
10. Organization of Accident Processing Rule given in Flow Chart ................................................. H19
11. Idea for Prevention of Human Error (picture) ........... H20
12. Periodic Function Test for Preventive Maintenance .... H27
13. Patrol ......................................................... H28
    Patrol Sheet (6, 4) ........................................ H29
14. Liaison Flow Chart of Work Orders (requested work) .. H31
    Liaison Flow Chart After Completion of General Works .. H32
As of March 31, 1992:
Total number of Operators : 138
Average age of Shift Supervisor : 49.7
Average age of Workers in Operation Section : 33.2
## Working System

<table>
<thead>
<tr>
<th>Arrangement</th>
<th>Shift system</th>
<th>Annual working hours</th>
<th>Annual nonwork days</th>
<th>Holidays</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-team, 3-shift system</td>
<td>45-day cycle: (1.1.1.1, 1.1.1, 2.2.2, 3.3, 3, off) + day-shift for 9 days</td>
<td>Workers under standard business hours: 1,919 hours</td>
<td>Workers under standard business hours: 120 days</td>
<td>Paid holidays: 20 days</td>
</tr>
<tr>
<td></td>
<td>Class 1: 8:00-16:10</td>
<td>Workers under three-shift system: 1,907 hours</td>
<td>Workers under three-shift system: 101 days</td>
<td>Summer holidays: 3 days</td>
</tr>
<tr>
<td>4 teams working under three-shift system, and 1 team working under day-shift system.</td>
<td>Class 2: 16:00-23:10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Class 3: 23:00-8:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Day-class: 8:40-17:10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Standard business hours: 8:40-17:30)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1-hour break for each class.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Shift rotation

| Date | Jan 1 | Jan 2 | Jan 3 | Jan 4 | Jan 5 | Jan 6 | Jan 7 | Jan 8 | Jan 9 | Jan 10 | Jan 11 | Jan 12 | Jan 13 | Jan 14 | Jan 15 | Jan 16 | Jan 17 | Jan 18 | Jan 19 | Jan 20 | Jan 21 | Jan 22 | Jan 23 | Jan 24 | Jan 25 | Jan 26 | Jan 27 | Jan 28 | Jan 29 | Jan 30 | Jan 31 |
|------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|

---

### Shift Rotation

**January**

- **January 1:** 8:00-16:10
- **January 2:** 16:00-23:10
- **January 3:** 23:00-8:00

**February**

- **February 1:** 8:00-16:10
- **February 2:** 8:40-17:10
- **February 3:** 8:40-17:30

*Day Class: 8:40-17:10*

*Day Off!*
## Training Pattern of Operator (Example)

<table>
<thead>
<tr>
<th>Classification</th>
<th>Induction Education</th>
<th>Practice Education of aux. machine</th>
<th>Education of aux. equipment operator</th>
<th>Education of Turbine-Generator operator</th>
<th>Education of reactor operator</th>
<th>Education of administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Pattern</td>
<td>1 year</td>
<td>1 year</td>
<td>3 years</td>
<td>3 years</td>
<td>6-7 years</td>
<td>This term of education is not defined because it may change personnel. So, it is difficult to clarify the term.</td>
</tr>
</tbody>
</table>

### Education System

- **Nuclear Training Center**
  - Education of nuclear training center—initial train course
  - Education of nuclear training center—retrain general course
  - Education of nuclear training center (retrain high class course)
  - Education of nuclear training center (retrain supervision course)

### Education in Nuclear Training Center

- Education in Nuclear Training Center (Tie-up train course of re-training member)
<table>
<thead>
<tr>
<th>Operator</th>
<th>Experience in Operation</th>
<th>Knowledges and Skills</th>
<th>Assignment (Operation)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shift Supervisor</strong></td>
<td>Not available</td>
<td>Must be well experienced and skilled in nuclear (including thermal power) operation and qualified for enhanced control and supervisory operation</td>
<td>During normal operation, must guide and supervise the operators of his shift on the handling of the operation, surveillance, recording and patrol check so as to perform in the operation task correctly and must patrol on the important areas in operation</td>
</tr>
<tr>
<td></td>
<td>(Vary depending on abilities of the operator, such as previous qualification and skills)</td>
<td>Must be extremely high level specialized knowledge and skills with ability to guide the personnel of his shift in view point of the safety control and the prevention against failures</td>
<td>In emergency must grasp the conditions of the accident and plant operation, guide and supervise the operators of his shift on quick and appropriate actions, report and notify other sections on the situation</td>
</tr>
<tr>
<td><strong>Shift Technical Advisor</strong></td>
<td>Not available</td>
<td>Must be adequately experienced in nuclear (including thermal power) operation and adequately qualified for control and supervisory operation</td>
<td>During normal operation, from a view point of safety management must assure the handling of operation and the appropriate procedures, patrol check, review on the emergency prevention measures, and educate with guidance for the operators of his shift</td>
</tr>
<tr>
<td></td>
<td>(Vary depending on abilities of the operator, such as previous qualification and skills)</td>
<td>Must be attained with very high level and specialized knowledge, and skills</td>
<td>In case of unusual event occurred, from a view point of safety management must support the shift supervisor on the emergency measures. In emergency, direct the personnel of his group to response quickly and properly according to the directions given by the shift supervisor</td>
</tr>
<tr>
<td><strong>Senior Reactor Operator</strong></td>
<td>Not available</td>
<td>Must be adequately experienced in nuclear (including thermal power) operation and reactor control operation with ability to supervise</td>
<td>During normal operation, must perform in the operation of facilities systems, handling and equipment, and grasp the operation condition so as to appropriately operate equipment and distribute the load according to the direction given by the shift supervisor. Also must direct the shift personnel to carry out surveillance tests and maintenance on each equipment as well as measurement.</td>
</tr>
<tr>
<td></td>
<td>(Vary depending on abilities of the operator, such as previous qualification and skills)</td>
<td>Must be attained with very high level and specialized knowledge, and skills</td>
<td>In case of unusual event occurred, perform secure and quick measures following the directions given by the shift supervisor</td>
</tr>
<tr>
<td>Operator</td>
<td>Experience In Operation</td>
<td>Knowledge and Skills</td>
<td>Assignment (Operation)</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Years</td>
<td>Range of Experience</td>
<td>Normal Operation</td>
</tr>
<tr>
<td>Reactor Operator</td>
<td>7 years (Approx.)</td>
<td>Must have experienced in the Turbine Generator operation or equivalent skills who received practical training on the reactor control</td>
<td>Must grasp and survey the operation condition and be engaged in the reactor facility operation in the main control room during normal and abnormal operation.</td>
</tr>
<tr>
<td>Turbine Generator Operator</td>
<td>4 years (Approx.)</td>
<td>Must have experienced in auxiliary equipment operation or equivalent skills who received practical training on the main equipment operation</td>
<td>Must grasp and survey the operation condition of the main equipment and be engaged in its operation in the main control room or in the site during normal and abnormal operation. Also, maintenance patrol for the main equipment.</td>
</tr>
<tr>
<td>Auxiliary Equipment Operator</td>
<td>1 year (Approx.)</td>
<td>Must have completed education in the school for a year and received training on the auxiliary equipment after schooling</td>
<td>Must grasp and survey the operation condition of the auxiliary equipment facility by maintenance patrol and be engaged in the operation of the auxiliary equipment in the site during normal and abnormal operation.</td>
</tr>
</tbody>
</table>

**Note:** The year of experience in operation is based on the criterion set on high school graduates; therefore, it will be modified according to the skills of the individual if his academic background is not applied to this criterion.
Principle for Safe Operation

Safety Operation

Prevention of accidents

Instructions

Confirmation

Report

Information

Countermeasures

Maintenance of equipment

Inspection

Maintenance

Early detection of accidents

Patrol

Repetition of instructions
Purpose of Guideline for Safe Operation

1. Accident-free operation can only be achieved by checking conditions all the time. That is, as soon as an erroneous condition is detected, details of the problem should be directly reported to the relevant personnel, and appropriate countermeasures should be taken according to the instructions given by the personnel.

2. When the instructions have been given, the director and the operator should repeat the instructions for confirmation, and after the instructions are observed, the operator should then report to the director so that the director can check the conditions.

Repeating the instructions is the foundation for maintaining order in the organization. Therefore, regardless of positions, all workers should readily and strictly make a habit of repeating instructions before following them. Any worker should draw attention to those who neglect the repeating of instructions so that all workers shall conform to the ruling that all instructions have to be repeated.

3. Careful inspection should be performed during the patrol in order to detect minor failures, and to prevent the occurrence of serious failures.

4. Safe operation relies on the proper repair and continuous maintenance of equipment.

5. Operation parameters should be checked in detail, evaluated, and analyzed to observe the conditions of station operation.

6. The training and education of operators should be fully arranged to maintain or to improve their technical level. Training and education are also important for taking appropriate measures when a failure or error is detected. The training and education of operators greatly contributes to safe operation.
Prevention of Re-occurrence of Human Error

Human errors management system

Purpose: Prevention of misoperation by operator

Outline: The data on human errors that occurred are collected and arranged for discussion at examination meeting or the study meeting held in each team, so that all operators are familiar with and can acknowledge error case studies.

| Occurrence of human error | (Sift supervisor of occurrence team) Inform chief manager of operation room of error situation. | (Each team) Organize examination meeting and study meeting in each team to acknowledge situation of occurred error, and discuss error prevention plan. | (Team in charge of human error) Propose and execute error prevention plan. |

[Example]

Worker X closed a wrong valve.

Human Error Report
Date: March 19, 1985
Description: A wrong valve was closed.
Cause of error: Communication between operators was not satisfactory.

Examination meeting and study meeting were organized in each team.

Operation rules were revised.

Installation of valve name plate
Identifier of pipe

[Result]
Human errors management is a most effective training system which considers errors familiar to operators.

(Human errors management system contributes to:

1. Avoid repeating the same type of mistakes. (Through acknowledgement of error situation, installation of warning sheets, etc.)
2. Review of the operation manual. (Establishment and revision of detailed regulations and check sheets)
3. Improving the ability of operators. (Substantial education and training, preparation of references, dissemination of operation techniques)
4. To improve or repair insufficient equipment. (Improvement of equipment, proposal to replace equipment, etc.)

The human errors prevention system has been effectively working, and the number of the human errors has decreased.
H13 -

- Rated power reached
- Feed water control and control rod control set to automatic control
- Turbine bypass control switched over to Tavg control
- Steam supply started (condenser vacuum secured)
- Main steam pipes warmed up
- Average no-load coolant temperature and pressure reached

- Residual heat removal system isolated
- Charging flow rate automatically controlled; normal letdown system secured
- Pressurizer water level set to no-load running water level
- Steam generation started in pressurizer

- Residual heat removal pump stopped
- Hydrogen blanket formed in volume control tank
- Primary coolant system water examination completed

- Primary coolant system water examination started; the examination covers oxygen concentration
- Primary coolant pumps started up
- All pressurizer heaters turned on; shut down rods withdrawn
- Charging pump started and letdown pressure set (at 3.2 kg/cm²)

- Inspection before start-up completed
Primary coolant pumps stopped

- Residual heat removing system started operating; turbine bypass valves (primary coolant pressure maintained)
- Let down pressure set 28.1 kgf/cm²
- Safety injection system manually blocked (up to 135 kgf/cm²)
- Pressure decreased by manually controlling pressurizer spray (cooling rate adjusted at 77.8 Centigrade/h)
- Turbine bypass flow rate increased
- One of coolant pumps stopped (another in operation)
- Reactor cooling started; all pressurizer heaters switched off
- Boric acid injected
- No-load running pressure reached by turbine bypass controlling
- Subcritical condition reached by adjusting control rods
- Generator disconnected from parallel running; turbine stopped
- Minimum generator loading reached
- Turbine bypass switched over to pressure control
- Control rod control switched over to manual control; feed water control valves switched over
- House lead switched over from house transformer to startup transformer
- Generator loading started decreasing
- Turbine bypass control set at Θavg
- Water feed automatically controlled
- Control rods automatically controlled
- Primary coolant system maintained at normal pressure and temperature
- Operating at rated power

Cooling stopped due to pressurizer vapor phase removal started

- Reactor cooling started; all pressurizer heaters switched off
- Boric acid injected
- No-load running pressure reached by turbine bypass controlling
- Subcritical condition reached by adjusting control rods
- Generator disconnected from parallel running; turbine stopped
- Minimum generator loading reached
- Turbine bypass switched over to pressure control
- Control rod control switched over to manual control; feed water control valves switched over
- House lead switched over from house transformer to startup transformer
- Generator loading started decreasing
- Turbine bypass control set at Θavg
- Water feed automatically controlled
- Control rods automatically controlled
- Primary coolant system maintained at normal pressure and temperature
- Operating at rated power
1. Already automated control of equipment (In main system)
   (1) Control of control rod
   (2) Control of pressure of pressurizer
      • Control of spray of pressurizer
      • Control of proportional heater and backup heater
   (3) Control of water level of pressurizer
      • Control of water flow for charging flow
   (4) Control of water level of volume controlling tank
      • Automatic make-up
      • Automatic diverting
   (5) Control of water level of steam generator
      • Control of main water supply
      • Control of by-passing of main water supply
   (6) Control of turbine by-pass valve
      • Control of average temperature of coolant
      • Control of pressure of main steam header
   (7) Control of turbine
      • E.H. governor
   (8) Control of heating steam of moisture content-separating heater
   (9) Automatic voltage regulator of generator
   (10) Automatic power switching of house power
   (11) Power supply for instrumentation (Automatically switched when error occurs.)
2. Automation of equipment in nuclear reactor safety protection system

(1) Automatic tripping of nuclear reactor (17 items)

Tripping occurs when:
- Source range neutron flux high
- Intermediate range neutron flux high
- Power range neutron flux high (with low set point)
- Power range neutron flux high (with high set point)
- Pressurizer pressure low
- Pressurizer pressure high
- Pressurizer water level high
- High temperature (ΔT) high
- High Power (ΔT) high
- Reactor coolant flow low
- High difference between main steam amount and feedwater and steam generator water level low
- Steam generator water level low-low
- Reactor coolant pump breaker trip
- Reactor coolant pump frequency low
- Turbine trip
- Earthquake trip
- Safety injection trip

(2) Automatic operation of emergency core cooling system (5 items)

Safety injection system operates when:
- Containment vessel pressure high
- Pressurizer pressure low and water level low
- Pressure of pressurizer low-low
- Pressure difference between main steam lines high
- Increase in flow in main steam line and decrease in pressure or excessive fall of average temperature of primary coolant occur concurrently.

(3) Automatic operation of containment vessel spray

(4) Permissive signal (Signal for activation or stopping of operation of control system and protection system)

(5) Isolation signal

- Isolation of containment vessel (A and B)
- Isolation of ventilation and air-conditioning of containment vessel
Standards and Instructions System (operation room)

Safety Regulation

Summary of essential points on nuclear power station operation

On-duty Shift supervisor transfer sheet writing instruction

For Unit No.1, 2 and 3 respectively
- Operation procedures manual (electricity)
- Operation procedures manual (turbine)
- Operation procedures manual (reactor)
- Manual for accidents (accident)
- Manual for accidents (alarm)
- Manual for accidents, Part two (severe accident)
- Periodical inspection manual (monthly inspection)
- Periodical inspection manual (annually inspection, annual examination, inspection while reactor is stopped)
- Patrol manual

Solid wastes disposal building
- Operation procedures manual (asphalt)
- Operation procedures manual (incinerator)
- Manual for accidents (accident)
- Manual for accidents (alarm)
- Periodical inspection manual
- Patrol manual

Cask storage building
- Operation procedures manual
- Manual for alarm
- Patrol manual

- Operation instruction unit manual
- Station computer capability registration manual
- Equipment lubrication oil management manual

- Manual for creating/storing operation record
Flowchart for Revising Operation Rules and Regulations

1. Improvement of operation method
2. Reflection of error case studies
3. Agreement of each team
4. Preparation of operation instructions
5. Agreement of leaders of concerned team
6. Decision of director
7. Issuance of operation instructions
8. Modification of data of original rules and regulations recorded on magnetic system by KRM
9. Distribution of operation instructions to all teams
10. Replacement of rules and regulations in all positions
11. Notification of operation instructions through TBM, education and circular notice
12. Preparation for circular notice of operation rules and regulations

(For important operation:)
Safety Management Committee
Organization of Accident Processing Rules given in Flow Chart

Occurrence of accident

Safety functions monitoring

Safety functions monitoring parameters are continuously monitored until the event becomes stable.

Station event-based operation rules
Manuals describing operations necessary to follow scenarios assumed for particular events (including several events not assumed in the plant design).
- Loss of external power supply
- Reactor trip
- Loss of coolant
- Loss of secondary containment piping
- Loss of coolant fluid inventory
- Abnormalities in containment
- Loss of cooling water supply
- Other issues

Are all safety function requirements met?

Yes
- Applying appropriate accident processing rules and carrying out necessary operations bring the situation under control
- Bringing event under control

No
- Are station event-based operation rules applicable?

Yes
- Bringing event under control
- Returning to normal operation rules and proceeding to low temperature shutdown

No
- Station safety function-based operation rules
Manuals describing necessary operations to ensure critical safety functions for plant safety regardless of types of causal events and evolution leading to failures. Manuals cover multiple failures that could not be assumed at the design stage.
- Ensuring reactor criticality
- Maintaining reactor core cooling
- Maintaining steam generator heat removal
- Ensuring and monitoring operation of safety injection system
- Maintaining water primary flow
- Preventing radiactivity release

Are all safety function requirements met?

Yes
- Applying appropriate accident processing rules and carrying out necessary operations bring the situation under control

No
- Bringing event under control
Main control room & CRT

Wireless paging equipment
CRT & Monitoring TV
To mark the value of gauges
Green: Normal value
Yellow: Alarm value
Red: Trip value
To enclose important gauges with a white line
To display which signal moves by and the current condition

P: Containment Spray Signal
T: Containment Isolation Signal
S: Safety Injection Signal
O: Light on in the normal condition
Δ: Light on in the accident
To enclose related switches with a white line

To display the set-up time of equipments that start automatically by SI and BO signals
Attachment of an attention card

Coloring important control switches
### Periodic Function Test for Preventive Maintenance

**Performed on Main Equipment of Hihama Unit 3, August 1989**

<table>
<thead>
<tr>
<th>Item</th>
<th>Freq.</th>
<th>Date of execution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CRDH operation test</td>
<td>1 1st</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>2. Operation changeover of charging/high pressure</td>
<td>3 1st</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>safety injection pump</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Residual heat removal pump start-up test</td>
<td>1 Daily</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>4. Diesel generator start-up test</td>
<td>2 Daily</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>5. Diesel generator load test</td>
<td>1 Daily</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>6. Battery voltage and specific gravity measurement</td>
<td>1 Daily</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>7. Operation changeover of boric acid pump</td>
<td>1 1st</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>8. Containment vessel spray pump start-up test</td>
<td>1 Daily</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>9. Annulus air cleanup fan start-up test</td>
<td>1 2nd</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>10. Motor driven auxiliary feedwater pump start-up test</td>
<td>1 Daily</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>11. Turbine driven auxiliary feedwater pump start-up test</td>
<td>1 Daily</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>12. Turbine safety device test</td>
<td>1 1st</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>13. Turbine valve stem-free test</td>
<td>1 1st</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>14. Safety injection system valve opening test</td>
<td>1 Daily</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
<tr>
<td>15. Reactor Protection system logic test</td>
<td>1 -</td>
<td>123456789101112131415161718192021222324252627282930</td>
</tr>
</tbody>
</table>
**Patrol**

Based on the patrol manual, the turbine generator operator, nuclear equipment operator, and T-G equipment operator shall perform patrol with the frequency indicated as follows.

The results of patrol shall be written in the patrol sheet, confirmed by shift supervisor on duty, and transferred to workers in the next shift.

Shift technical adviser on duty and shift supervisor on duty shall perform patrol to important equipment if necessary.

[1] Important equipment in safety system
   - Power supply for emergency, auxiliary water supply system, RHRS (Residual Heat Removal System), compressor for instrumentation, etc.
     - Once/day. Third shift shall perform patrol.
     - Patrol sheet (Patrol sheet for important equipment in safety system)

[2] Important equipment
   - Equipment mentioned in [1] above, equipment which may be the cause of trip, and equipment which may be the cause of radioactive contamination.
     - 3 times/day. Each shift shall perform patrol.
     - Patrol sheet.

   - Once/day. Third shift shall perform patrol.
     (As for outside buildings, day-duty worker shall perform patrol.)
     - Patrol sheet table.
<table>
<thead>
<tr>
<th>No.</th>
<th>Equipment Name</th>
<th>CS</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1A primary water pump</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>1B primary water pump</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>1C primary water pump</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>2A secondary water pump</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>2B secondary water pump</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>2C secondary water pump</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Patrol Sheet** (Inspection Sheet for Important Equipment in Safety Protection System)

*For Central Control Room*
# Patrol Sheet

(For Nuclear Reactor Auxiliary Building)

<table>
<thead>
<tr>
<th>No.</th>
<th>ポスト</th>
<th>天</th>
<th>図</th>
<th>項目</th>
<th>檔</th>
<th>1日</th>
<th>2日</th>
<th>3日</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ナンバー1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ナンバー2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ナンバー3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>ナンバー4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>ナンバー5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>ナンバー6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>ナンバー7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>ナンバー8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>ナンバー9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(continued...)

Page 4
<table>
<thead>
<tr>
<th>部 閣</th>
<th>担 当</th>
<th>任務遂行場所</th>
<th>任務</th>
</tr>
</thead>
<tbody>
<tr>
<td>均長</td>
<td>運転室長</td>
<td>事故発生中央制御室</td>
<td>①総合指揮  ②本部との連絡</td>
</tr>
<tr>
<td></td>
<td>業務係員 (中村・中川)</td>
<td>事故発生中央制御室</td>
<td>本部との連絡補佐 (室長の補佐)</td>
</tr>
<tr>
<td></td>
<td>副班長</td>
<td>担当ポジション</td>
<td>①信号による放送周知  ②事故処置  プラントの緊急停止処置  災害（事故）の拡大防止</td>
</tr>
<tr>
<td></td>
<td>本員 （発生側）</td>
<td>事故発生中央制御室 2名応援（主任と互換要員）</td>
<td>①本部以外への連絡対応  ②非常用電話、資料等の準備  ③CRTパソコン</td>
</tr>
<tr>
<td></td>
<td></td>
<td>担当ポジション</td>
<td>本置業務</td>
</tr>
<tr>
<td>[日勤直取]</td>
<td>当直係長</td>
<td>事故対策本部</td>
<td>①業務係長からの引き継ぎを受け方針決定  参画  ②中央制御室との連絡</td>
</tr>
<tr>
<td>副班長</td>
<td></td>
<td>担当ポジション</td>
<td>本置の応援</td>
</tr>
<tr>
<td></td>
<td>日勤直取</td>
<td>事故発生中央制御室 （1〜2名応援）</td>
<td>時系列（時刻）照合 引継簿とCPU</td>
</tr>
<tr>
<td></td>
<td>本員 （健全側）</td>
<td>日勤直取</td>
<td>要請があれば本置応援</td>
</tr>
<tr>
<td></td>
<td>（健全側）</td>
<td>故障監視</td>
<td></td>
</tr>
<tr>
<td>[特務掛]</td>
<td>業務係長</td>
<td>事故対策本部</td>
<td>①事故発生直後の本部での対応  ②係員の指揮</td>
</tr>
<tr>
<td>副班長</td>
<td>宮崎・川藤</td>
<td>事故対策本部</td>
<td>①中央制御室との連絡補佐  ②事故速報時系列の照合</td>
</tr>
<tr>
<td></td>
<td>資務係員</td>
<td>事故対策本部</td>
<td>特命事項の処遇</td>
</tr>
<tr>
<td></td>
<td>資務係長</td>
<td>事故対策本部</td>
<td>非常待出し</td>
</tr>
</tbody>
</table>
事故時における運転室不在者代行について

事故時における運転室の不在代行を下表の通り定め、運用する。
尚、運転員および特命員については、随時、業務係上席者から順番に

- 3.10.31
- 3.12.10
- 4.6.10

下表は、1．2号機側で事故発生の場合を示す。事故発生が、3号機の場合は 

<table>
<thead>
<tr>
<th>ケース</th>
<th>不在なし</th>
<th>室長不在</th>
<th>A日勤係長不在</th>
<th>B日勤係長不在</th>
<th>業務係長不在</th>
<th>A日勤係長不在</th>
<th>B日勤係長不在</th>
<th>業務係長不在</th>
<th>最低必要人数</th>
</tr>
</thead>
<tbody>
<tr>
<td>班長（中央）</td>
<td>運転室長</td>
<td>A日勤係長</td>
<td>B日勤係長</td>
<td>業務係長</td>
<td>運転室長</td>
<td>A日勤係長</td>
<td>B日勤係長</td>
<td>業務係長</td>
<td>1</td>
</tr>
<tr>
<td>（木御）</td>
<td>B日勤係長</td>
<td>B日勤係長</td>
<td>B日勤係長</td>
<td>業務係長</td>
<td>業務係長</td>
<td>宮崎家彦</td>
<td>宮崎家彦</td>
<td>中村和弘</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>A日勤係長</td>
<td>A日勤係長</td>
<td>A日勤係長</td>
<td>A日勤係長</td>
<td>A日勤係長</td>
<td>中川弘一</td>
<td>中川弘一</td>
<td>加茂嶋</td>
<td>3</td>
</tr>
<tr>
<td>運転部（中央）</td>
<td>中村和弘</td>
<td>中川弘一</td>
<td>富田光一</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>特命員（事務所）</td>
<td>宮崎家彦</td>
<td>田原伸吾</td>
<td>田原伸吾</td>
<td>田中亀井</td>
<td>井上浩</td>
<td>小谷伸治</td>
<td>小谷伸治</td>
<td>佐々雄次</td>
<td>4</td>
</tr>
</tbody>
</table>

注釈※1: 室長不在時の代行順位 
※2: B日勤係長不在時の代行順位 
※3: 業務係長不在時の代行順位 
※4: A日勤係長不在時の代行順位

- 934 -
Visits to Direction de la Sûreté des Installation Nucléaires and Electricité de France

D.C. Donderi, PhD
Human Factors North Inc.

February, 1994

On February 21, 1994, I met in the morning with the Chargé de Mission, International Affairs, of the Direction de la Sûreté des Installations Nucléaires (DSIN) of the French Ministry of Industry, Posts and Telecommunications, and External Commerce. In the afternoon, I met with two people from Electricité de France (EDF) - the Chief of the Human Factors Section of the Nuclear Power Plant Division, and the Assistant Manager for International Program Coordination of the same division.

Relationship between DSIN and EDF

EDF is the state industry which produces and distributes electrical power throughout France. DSIN is the agency responsible for all aspects of security in the French nuclear industry. The key to the relationship between these two institutions is "contrôle." EDF is responsible in the first instance for all of the plans relating to the security of its own installations. Security encompasses the siting, construction, commissioning, operation, maintenance and protection of all of EDF's installations.

DSIN reviews and approves or disapproves all of the EDF initiatives. Among the EDF products subject to DSIN approval are operational procedures and training requirements and programs.

DSIN and EDF Security Philosophy

The focus of our inquiry as set out in the Statement of Work was the use of independent verification in nuclear industry operating procedures. The intention was to investigate the extent to which independent verification was used in other nuclear industries and the extent to which it could be used in the Canadian industry to improve nuclear operations safety.

With respect to independent verification, our colleagues in the DSIN and EDF spoke with a common voice. All three people were equally convinced that little was to be gained by increasing the mandated level of independent verification in nuclear operations. This unanimity stems from a profound and consistent revision in the human factors philosophy guiding the quest for reliability and safety at both DSIN and EDF.
Professionalism and Individual Responsibility

Mechanical failures which in principle could have been easily controlled and contained by correct human intervention, have very often triggered serious nuclear system catastrophes like Three Mile Island (TMI), as well as many less damaging but economically disruptive events.

The DSIN-EDF attitude to human error is to change motivation rather than to monitor behaviour. DSIN-EDF reason that a passive mental attitude is induced by following step-by-step procedures "by the book" while someone else "signs off" the same procedure by the book. DSIN-EDF know and accept that many procedures are both so critical and so complex that routine, step-by-step instructions are essential. They have no intention of abandoning written procedures (all EDF written procedures are subject to DSIN approval). But rather than encourage either blind dependence on the procedure, or blind dependence on someone else to verify the procedure, DSIN-EDF encourage rather the adoption of an individually critical attitude towards the procedures and towards ones' own actions. They consider an individually responsible, professional attitude to be the key to reducing human error in both standard procedures and in the response to abnormal operating conditions.

According to the DSIN-EDF approach, every action in operating a nuclear power plant (NPP) should be based on a plan - formal or informal - and every plan should lead to an expected outcome. The route to successful control of human error, according to DSIN-EDF, is to inculcate in every NPP operator a critical, confirmation-seeking attitude towards both the individual control action and the plan on which it is based.

DSIN-EDF want to make everyone both feel and act with an autonomous sense of responsibility towards the safe and efficient operation of the NPP.

Autonomous Planning of "Safe" Manoeuvres

As a positive part of this policy, EDF encourages operators to formulate and carry out independently manoeuvres which when carried out normally will keep the plant well within the normal operating parameters. These manoeuvres can be formulated and carried out without reference to previously catalogued "step-by-step" written procedures. It must be emphasized that there are very strict limits on the applicability of this "new autonomy" and most procedures, including all maintenance verification, remain catalogued, step-by-step, and obligatory.

But even here, it is not DSIN-EDF's intention to multiply independent checks on operator actions. Instead, the intention is to encourage the development of an autonomous, critical, self-correcting attitude towards plans and outcomes.
Education for Autonomy

DSIN-EDF recognize three parts to the education of NPP operators and maintainers. The French expressions are: connaissances, savoir-faire, and savoir-être.

Connaissances

It is fundamental that operators have the knowledge necessary to do the job. EDF is responsible for assuring that operators have the necessary knowledge, and DSIN monitors both the training programs and the certifications which attest to the acquisition of that knowledge.

EDF operators and maintainers receive a series of certificates, or habilitations, which entitle them to work on more or less of the entire plant, under more or less supervision. The greater the level of responsibility, the more complete the habilitation. Habilitations are obtained through a combination of special courses taken on released time, supervised on-the-job training, and simulation training.

Savoir-faire

Operators must, of course, know their procedures as well as the scientific and engineering principles governing the operation of their plant. Simulation and on-the-job training are the means by which this is achieved.

In order to facilitate simulator training by reducing both travel costs and the costs of central simulation facilities, EDF plans the future installation of full-scale simulators at large power generation sites, to be used on a regional basis.

Savoir-être

This is the new approach that DSIN-EDF are taking to improve nuclear safety. Much in the footsteps of the late W.E. Deming, DSIN-EDF want to establish a "culture of quality" in which everyone participates, in a recognized and responsible way, to achieve the goals of safe and efficient operation.

I learned very little in detail about how DSIN-EDF hope to achieve this goal. It remains a goal - and all of our French colleagues accept for the moment that they do not have in place a concrete plan for achieving this goal. In the absence of a demonstrable successful method of teaching "savoir-être", the French nuclear industry has not abandoned written procedures and checklists, nor abandoned supervision and independent verification, but they do not favour the proliferation of external controls, including independent verification.
Visit with Technischen Überwachungs-Vereins Rheinland, Bundesamt fur Stralenschutz, and Gemeinschaftskernkraftwerk Neckerwestheim Representatives

Don C. Donderi, PhD
Human Factors North Inc.

February, 1994

The visit to Germany was organized by the BUNDESAMT fur Stralenschutz (BfS), or Federal Department of Radiation Protection, in cooperation with two other groups. The first group was the Technischen Überwachungs-Vereins Rheinland (TUV), the private German industry research and safety and product standards organization. TUV does much of the nuclear safety inspection work and standards setting in the human factors field, under contract to BfS. The other group was the Gemeinschaftskernkraftwerk Neckerwestheim (GKN), a two-reactor complex about 30 km from Stuttgart. My party, which included 2 BfS people, was the guest of the Station Manager of GKN II, which is a 1365 MW Siemens PWR, the third most powerful single reactor in the world according to their 1992 annual report.

The technical part of the visit consisted of a three-hour meeting with TUV and BfS representatives in Cologne on Wednesday, February 23rd, followed by a dinner meeting in Talheim with BfS and GKN representatives. The next day, from 9:00 a.m.-1:00 p.m., was dedicated to a combination of conference, and control room and reactor inspection of GKN II.

In order to understand the roles of these people, a brief explanation of the organization of the German nuclear industry is in order. There are about seven or eight separate operating authorities which cover the German territory. Germany is a federal state, and these authorities are responsible both to state governments and to the federal government through the BfS.

The BfS is a relatively small organization. It relies for both technical advice and for actual verification and oversight services on TUV. TUV is something more than a cross between a standards association and a research laboratory. It is an umbrella organization in which various profit-making consultancies are amalgamated under a not-for-profit industry technical association which deals with both production efficiency and safety, and consumer product standards. TUV began in the nineteenth century as an industry-wide standards organization for steam boiler construction. It came into existence, of course, as a result of several catastrophic boiler explosions. TUV has a human factors group which began, in 1977, to report to the German Government on human factors standards applicable to the German nuclear power industry. Their advice, some of which has been translated into English, covers materials, procedures and the preparation of manuals, including emergency operating procedure (EOP) manuals.

The particular focus of our inquiry was "independent verification." Apropos of this, the German TUV group is well acquainted with both the organizational structures and current practices of DSIN (the French Direction de la Sureté des Installations Nucléaires) and EDF (Electricité de
France, the French operating company), and the contact between EDF and German nuclear authorities is very close, taking place both commercially (German fuel is reprocessed by COGEMA, the French nuclear fuel company) and through European and worldwide committees of the Institute of Nuclear Power Operations (INPO) and the European Nuclear Authority.

The general tenor of our discussion can be very succinctly conveyed. It bears a surprising similarity to the French discussions. By itself, independent verification or "double-checking" as the Germans called it, without specific justification, would be considered a useless nuisance. However, there are clear situations where independent verification is essential and is never overlooked. The first of these situations is start-up after an outage, where specific, detailed work statements are prepared for the position of every manually-operated safety-related valve. During start-up, the operating manual is copied and used as a procedure checklist for the many interlocked manual procedures. Electronically opened valves are not included because their position (not their position command) is indicated in the control room. For manual valves, each valve position must be verified independently, and signed off, by two field operators, and then the whole procedure must be reviewed and signed off by the shift supervisor. Entering the completed procedure in the computer then unblocks permissions for the next procedures.

The second obligatory independent verification situation is during a transient or other unexpected condition. The control room staff for the single-unit GKN II is usually five people. During a transient, the staff splits in two. The deputy shift supervisor and one operator continually monitor 15 to 20 safety parameters, the location and display of which they must know perfectly. They can monitor these parameters either from individual displays in the control room, or from different banks of 8 visual display units (VDU). The screens in each VDU bank can be independently switchable to one of about 20 different comprehensive system status displays. All of the safety parameters can be viewed on one or more of these displays. The parameter states are checked by the operator, and double-checked by the deputy shift supervisor. The shift supervisor himself oversees the correction of the transient.

The specific attitude of the GKN staff towards independent verification is "Independent verification if necessary, but not necessarily independent verification." It is considered essential in any case where the consequences of an action cannot be immediately verified. A clear example of this is seen in the work plans for isolation and de-isolation of a system. Isolation is independently verified where the consequences are not immediately obvious. A computerized system prints out a work plan which indicates where and when isolation independent verification is necessary. But for de-isolation, system tests are always run immediately afterwards, and the results of the system test will confirm or not confirm the isolation. Therefore, independent verification is not used for de-isolation.

The Key Interlock System

A very ingenious control system for manual valves has been installed in GKN II. The system applies to all manual valves in any safety-related subsystem, like a primary or secondary cooling
circuit. All manual valves in these circuits are in a permanent safety-appropriate position. They can only be changed from that position by unlocking them. The keys necessary to unlock the valves are kept in a clearly marked order in the shift supervisor's office. Once a key has been inserted to unlock a valve, it cannot be released until the valve is turned back to the safety-appropriate position.

The lock pattern for each safety-related system is the same. There is at least one key for each safety-related system, so if any valve in that system is turned to the non-safety-appropriate position, the absence of a key will be observable.

As an additional source of information, the computer-generated work plan for every maintenance task also produces a series of red "lockout" cards. One part of the card contains the instructions related to the maintenance operation. Another part of the card goes to the shift supervisor. A third part goes on the valve or switch which has been modified. And if it is a question of a safety-related manual valve, another part goes on the key panel in place of the lockout key which is now in the valve.

GKN II Merits Close Study

GKN II has three features which should merit close study by all parts of the Canadian nuclear industry:

1) a completely computerized maintenance planning and scheduling system
2) a 6-part shift schedule with extensive provision for education and on-the-job training
3) the work verification philosophy described earlier, backed up by the key-lock and computer-based maintenance interlock control system.

Computerized Maintenance Control

My short visit did not provide me with the time necessary to thoroughly review this system, but its main features were described and demonstrated to me. In a conventional PWR, much maintenance work is done during the annual scheduled outage, and less is done on-line. But both scheduled and unscheduled maintenance are controlled by a very complete computer database system. The system has remote entry terminals throughout the plant so that field operators do not have to return to the control room to file maintenance reports. All operators have been trained to enter maintenance reports using conventional computer keyboards, and individual magnetic-stripe ID "signature" cards.

The reports are constructed on a German database system which operates on a mainframe computer. Data entry is constrained by menu selections, so that the system can be used to generate statistical analyses of maintenance incidents. Obviously, this requires that all possible
maintenance events be classified, and I cannot comment on the scope or adequacy of the classification.

When a maintenance report has been entered, it is tagged on the computer. At the beginning of each shift, the accumulated reports are reviewed by the shift supervisor and station manager. Additional data, including priority data, is entered by one or the other of these people. Their ID "signature" indicates approval.

The report is then automatically transmitted to the appropriate maintenance department, and logged for completion.

Up to this point, the entire maintenance report procedure is paperless. Not only is it paperless, but standard maintenance routines for standard problems are stored in the database and do not have to be entered or written out by the maintainers.

When a job has been scheduled to begin on a particular shift, an appropriate detailed work order is printed out by the computer. In addition, as described earlier, the appropriate lockout cards are printed out. If the isolation requires independent verification, then the work order is printed out to require independent verification. Where manual keylock isolation is required as described earlier, the appropriate key card (to replace the keys in the key cabinet) is also printed out.

The printed worksheet, appropriately checked off and signed, becomes the only archived paper maintenance record. The completion of the maintenance work is also signalled to the computer database, which incorporates the data in a standard statistical format which permits later summary statistics to be calculated and extracted.

The advantages of this system are: 1) elimination of handwritten maintenance records which because they are very hard to read and hard to understand, are important sources of error in maintenance procedures; 2) the generation of consistent work orders, including stepped, protective interlocks, which maintain the necessary safety redundancies or issue clear warnings when a redundancy has been compromised. This system works, as I understand it, by withholding succeeding work orders until previous orders have been completed, computer-logged, and computer-verified by the competent authority (station manager or shift supervisor); 3) the reduction of paper accumulation and 4) the collection of reliable and consistent maintenance statistics.

The mainframe computer maintains a current duplicated record of the state of every monitored parameter of the system. If the mainframe should go down, this backup "system state" record is immediately available on another computer so that maintenance and operating decisions based on state knowledge can be made in real time. I was told that the backup for the maintenance computer is off-site, but can be put on-line to the site terminals with a delay of several hours. On specific questioning, the plant authorities assured me that this was a fast enough backup, given the existence of a current, continually monitored system state record which is immediately available if the mainframe goes down.
Shift Schedule

GKN II uses a six-shift schedule. Each shift rotates through early, late, and night shifts, followed by a "training" day shift and then a day work shift. The early, late, night and "training" shifts are broken by one or two-day rest, the "training" to "day" shift is broken by a four-day rest, and the "day" shift is followed by an eight-day rest until the cycle begins again. I do not know about vacation schedules. Shift schedules similar to the actual schedule in practice at GKN II were discussed in a paper by W. Preuss (who I met) and G. Reinartz of TUV, titled "Auswirkungen des Schichtbetriebes in Theorie und Praxis", published in VGB Kraftwerkstechnik 65, Heft 2, February, 1985.

Work Verification Philosophy and Systems

Both the keylock system used at GKN and the computerized maintenance system would in my opinion repay very careful study by both the construction, regulatory and operating branches of the Canadian nuclear industry. In short, I think AECL, AECB, Ontario Hydro and the New Brunswick Light and Power Commission would all benefit by intensive study of GKN II.

Why? GKN is a new very large reactor with an excellent production record. Their 1992 Annual Report states they were on-line 92.2 percent of the time during the year, even including the annual inspection and outage. The annual report also states that GKN II produced the third-largest amount of power of any single reactor unit in the world in 1992. The station manager speaks excellent English, understands his plant well, and explains it well. At least one of his shift supervisors speaks good English. The plant was completed in 1989 and so is practically brand-new. The computerized maintenance system, if it is as good as it appears to be, is in my opinion a breakthrough by comparison to the other systems I have seen and previously reported on. They include: Point Lepreau, Pickering I, Maine Yankee, Cattenom(EDF) and Blayais (EDF).

The control room displays are well organized, and they have integrated VDU and conventional displays in an intelligent way. The maintenance system and manual keylock system are complementary and intelligent. The maintenance entry and display terminals are well placed both in the plant and in the control room. The printout and data recording aspects of the maintenance system reduce paper flow and increase retrospective system knowledge.

GKN II is independently operated. Unlike the French industry, GKN II is privately owned by an association of utilities and the German railway. Retrofits, updating and modernization are decisions made locally by the management, as in Canada, under the supervision of the regulatory authorities.
In short, from the Human Factors point of view, I saw a technically excellent nuclear reactor operation whose published statistics justify the impressions made onsite. The maintenance systems are of particular interest, and would repay intensive, careful study by all parts of the Canadian nuclear industry.