Atomic Energy of Canada Limited

CONTROL AND SAFETY IN THE OPERATION OF THE NRX AND NRU REACTORS

by

D. G. BRECKON and J. H. COLLINS

Chalk River, Ontario

April, 1962

AECL-1486

ATOMIC ENERGY OF CANADA LIMITED

Control and Safety in the Operation of the NRX and NRU Reactors

by

D. G. Breckon and J. H. Collins

Paper to be presented at the International Atomic
Energy Agency Symposium on Reactor Safety and
Hazards Evaluation Techniques, Vienna, May 14 - 18, 1962

Chalk River, Ontario

CONTENTS

ABSTRACT

Safety in reactor operations is achieved through review and development of reactor control systems together with the exercise of sound administration controls.

At Chalk River, the control and safety systems of the NRX reactor have been developed over the 14 year history of the reactor to provide safer and more reliable operation. The original 18 boron carbide shut-off rods were replaced by 6 electrically operated rods of greater reliability. To augment this change an automatic dump of the heavy water moderator was included. Both devices function simultaneously but each is capable of shutting down the reactor independently.

Control of reactor power was initially maintained through two manually operated devices; a cadmium control rod and an overflow weir by which the moderator level was adjusted. Later, automatic control of the cadmium rod was possible during power operation. Now, automatic start-up and power control is achieved by adjustment of the moderator level, eliminating the control rod and the weir.

Incorporation of a two out of three coincidence system has further improved the safety of the reactor.

As reactor technology has advanced so have administrative controls. For safe reactor operation, it is essential to have well established responsibilities through a well-knit organization with personnel trained in sound policies and procedures. To assist in training, manuals

and policy instructions are used. These form the basis for the operation and are augmented by the control procedures. Field work is controlled by work permits, entry to limited access areas through interlock systems and operation of valves through valve slips and flowsheets. Where feasible check-off systems are used to verify field operations. Scheduled checks made possible at power by the two out of three coincidence system permit a continual assessment of the reactor systems. When associated with well established maintenance procedures, they enhance the reliability and safety of the reactor.

1. INTRODUCTION

In reactor operation safety must be maintained through the continual review of existing methods and the recognition of developments in all aspects of the field. Although original safety criteria are carefully considered before they are established, operators of reactors must always take advantage of advances in technology and improvements in technique to develop the best possible system. Development must not be confined to this aspect alone, however; sound administrative and organizational policies and procedures must also be developed.

An excellent example of technological advance is the development of the present NRX control and safety system. Since the original start-up of NRX in 1947 this reactor has been modified a number of times. The changes, based primarily on operating experiences and combined with advances in the field of reactor control, have been incorporated to improve safety and the reliability of control.

Despite such developments, the administrative and operational problems remain. Many people may be involved and the problems are those of organization and training, the preparation of reliable manuals and the establishment of satisfactory procedures. The NRU reactor, the largest of the Chalk River reactors, provides a fine example of the development of reactor safety through administrative control.

2. DEVELOPMENT OF THE PRESENT NRX CONTROL AND SAFETY SYSTEM

2.1 History of NRX Modification

Following the original start-up in July 1947 the NRX control and safety system was not changed except for minor revisions until after the major reactor accident in December 1952. Although this incident severely curtailed the experimental program at Chalk River it did provide time to assess the operation of the reactor from the standpoint of safety. The accident had clearly demonstrated that the primary shutdown device was unreliable. This investigation resulted in many recommendations to ensure safe operation and reliable control of the reactor. Major changes were proposed in three main components of the system, namely: shutdown devices, control devices and protective instrumentation. The improvements were introduced gradually over the period May 1956 to May 1958 when the change-over to the control system presently in use in NRX was completed.

2.2 Shutdown Devices

Rapid shutdown of NRX was originally achieved by the insertion of 18 air-cooled boron-carbide (shut-off) rods into the reactor core. These rods were air operated and air cooled, i. e. air was used to raise the rod out of the core where it was held by means of an electromagnet in the headgear. The 18 rods were raised in two banks of nine; a later modification reduced the total number of rods to 12 raised in six banks of 4, 3, 2, 1, 1 and 1 rods respectively. When a signal from a monitoring instrument indicated a condition unsafe for continued reactor operation, the electrical current through the magnet of each rod was broken and the absorber section was accelerated into the core by means of air pressure. The operation of the pneumatic rod is depicted schematically in Figure 1.

The boron-carbide rod was guided in its travel by a tube called a barrel. As the rods were pneumatically operated the clearance between the rod and its barrel was very small. This meant that any foreign material which entered the barrel could jam the absorber section and prevent it from becoming fully inserted in the core. Limit switches were used to indicate that the rod was fully inserted or fully withdrawn.

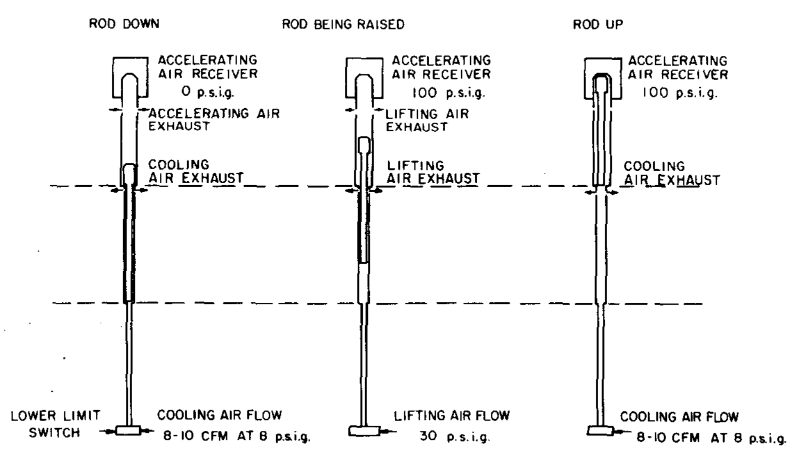

Figure 1

Pneumatic Shut-off Rod

Malfunction of these rods was not uncommon during the five years they were in service before the accident. During this time 62 rod failures occurred, representing a fault rate of about one per month. These were all due to absorber sections jamming in the barrel. Other faults mainly associated with the rod position instrumentation occurred at a rate of 18 per month. Investigation of the accident in December 1952 revealed that faulty performance of the shut-off rods had been a major contributing factor. At the time of the accident some of the rods which were withdrawn failed to drive fully into the reactor when released. Ultimately the power excursion was brought under control by a manual dump of the heavy water moderator.

The accident pointed out quite clearly that a reactor capable of operation but in a shutdown state is potentially more hazardous than when it is operating at full power, a fact which has been borne out by other reactor accidents throughout the world. With this in mind particular attention was paid to the type of shutdown device to be provided in the proposed new control system. This device must be very reliable. It was realized that the reliability would be increased if two independent means of shutdown were employed. Thus, if one device failed to operate the other would still shutdown the reactor.

The thinking regarding the position of shut-off rods during reactor shutdowns, when load changes were being made, changed radically at this time. Formerly all shut-off rods were fully inserted in the core under these conditions. Now it was proposed to have four of the rods in the raised position during load changes so that they would be availabe to stop the reactor should it be critical. This group of shut-off rods was termed the safety bank.

As a result of this proposal a decision was taken to alter the control system to provide two separate shutdown devices, viz. six reliable shut-off rods and an automatic moderator dump. Each device was to be independently capable of reactor shutdown.

Specifications for the new type of shut-off rod required that it be electrically operated, i. e. the boron-carbide absorber section would be retained but it would be connected by means of a cable to a motor driven drum. Insertion was to be under gravity on de-energization of an electro-magnetic clutch and the rod was to reach the full insertion point within two seconds. The removal speed was to be limited to that which would not result in a rate of increase of reactivity of more than 0. 3 milli-k per second (%rate $\Delta k = 0.03\%/\text{sec.}$).

It was realized that during the period when the new type of shut-off rod was being developed the reactor would have to be operated with the pneumatic shut-off rods as the primary shutdown device. A shut-down system comprising 18 rods was provided with each rod individually raised in sequence and the principal of the safety bank was adopted. In addition, whenever a shut-off rod failed to descend completely an auto-matic partial moderator dump resulted and a new operating instruction required that the offending rod be replaced with a spare.

During the two year period in which the reactor was operated under this system 23 shut-off rods were replaced due to failure of the rod to descend. By May 1956, the development and testing of the electrically operated shut-off rod had been completed and six of these rods were installed to replace the 18 pneumatic rods. A diagram of the new shut-off rod is shown in Figure 2.

Because there were fewer rods the total shutdown capacity of the new rods was less than that of the old ones. As a second system, automatic dumping of the moderator was included in the system.

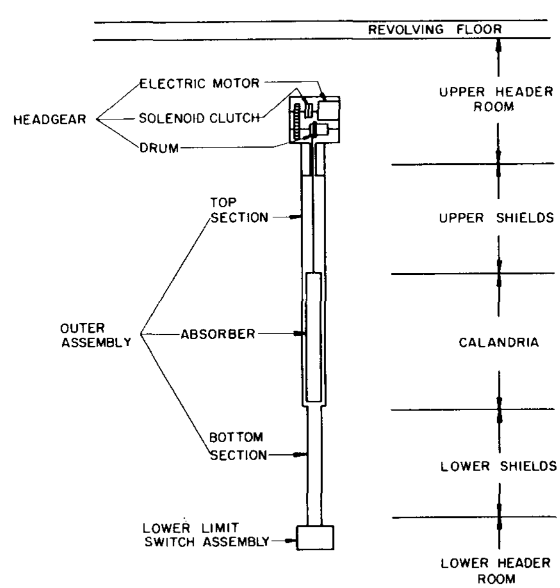

Figure 2

Electric Shut-off Rod

The rod control circuits were arranged so that the rods could only be raised one at a time and in a definite sequence. To guard against failure of a rod clutch to release, the electrical circuits were designed such that an automatic shutdown signal would apply full down drive to the motor of each rod that was not down regardless of any control settings.

The moderator was dumped through full opening of six valves below the reactor vessel at the same time that the shut-off rod clutches were de-energized. The moderator dump tank capacity was such that when the dump was completed the heavy water level in the reactor vessel was 140 centimeters, well below the level (180cm.) required to achieve criticality with a clean cold reactor.

As a further safeguard, to enforce maintenance and repair of faulty shut-off rods and dump valves, an electrical monitoring circuit alarmed if any one of the 12 units failed to perform its function within two seconds (i. e. full insertion for the rods and complete opening for the valves.) If a second unit failed to function within this time limit an absolute trip* prevented further operation of the reactor. This trip could only be cleared by using a key held by the reactor superintendent.

During the 5-1/2 years this system has been in operation it has performed very well. The dump valves have functioned flawlessly, there being no record of a failure of the valves to operate when required.

---

*An absolute trip requires that all means of reducing the reactivity of the reactor are initiated and maintained in action regardless of reactor power.

The performance of the new shut-off rods has been far superior to that of the pneumatic rods. There have been only four failures of a rod to descend completely, all detected during rod testing with the reactor shut down. In each case the defective rod was replaced with a spare unit. Frequent faults in the rod position indicating instrumentation continued to occur, most of them associated with the limit switches at the bottom of the rod. The bottom limit switches were removed in August, 1958 and replaced with limit switches in the headgear to indicate that the rod was fully down. This modification greatly reduced the frequency of this type of fault; in the first six months of 1961 seven limit switch failures were experienced.

A total of 10 rod assemblies were manufactured, four of which were available as spares. As all rod headgears were interchangeable it was possible to perform regular overhauls of these units. This maintenance, coupled with frequent cable inspection, ensured that the six operating rods were kept in good working order.

2.3 Control Devices

The original design of the reactor incorporated four water-cooled cadmium control rods each of which was manually operated. In the early days of operation three of these rods were removed from the system as experience had shown that only one rod was required for effective "fine" control. Additional "coarse" control was achieved through adjustment of the heavy water level in the reactor vessel by means of an overflow weir.

This device was also manually operated.

Operation of the reactor with these controls required that the supervisor in charge be in constant attendance at the control console to position the control rod and the overflow weir, particularly during the start-ups and until equilibrium operation was reached. It was not possible to hold the reactor power steady during normal operation as the control rod was continuously being adjusted to maintain the power at the desired level. This condition was alleviated by the introduction of a device that positioned the rod automatically. It was placed in operation by a manual switch when the reactor was operating at a definite power level, and was removed from service during periods of changing reactor power such as start-ups. This automatic control device was capable of maintaining the reactor power at a steady level. It received a signal from an ionization chamber monitoring the neutron flux in the reactor and moved the control rod to keep the signal output from the chamber at a constant value. This was the first step along the road to complete automation of power control. It did free the supervisor from the console to some extent, but he was still required to position the overflow weir until equilibrium power operation was reached and to adjust both controls during start-up.

The control devices remained unchanged until May, 1958 when a new concept of control was introduced. This involved automatic control of reactor power during start-up and at full power operation by adjustment of the moderator level in the reactor vessel. This method of control was proposed for NPD, Canada's first demonstration power reactor and it was felt that it would be advantageous to install such a system in NRX to obtain operating experience. This automatic system was installed in May, 1958 and the control rod and overflow weir were removed from service after a period of testing in which the new system proved to be very effective in control of reactor power. Incidentally, the elimination of the control rod permitted isotope load to be removed with the reactor in operation. This was not possible formerly as the control rod rack protruded through the top deck plate preventing movement of the rod removal flask over the reactor top.

The primary devices in this new system were three heavy water flow control valves located below the reactor vessel. These valves together with three additional dump valves opened to provide the automatic moderator dump on receipt of an automatic shutdown signal. During start-up and operation at power these valves were automatically positioned from fully closed to partially open on receipt of a signal from the electronic control equipment. The latter, in turn, received a signal from ionization chambers monitoring the neutron flux (reactor power) in the structure. The signal from the electronic control equipment was fed into electropneumatic valve positioners to move the valves. Thus, with a constant input of heavy water to the reactor vessel of 250 Igpm., the reactor power was controlled by the amount of spillage from the vessel through the three control valves. When the reactor power was changed, a proportional change was produced in the signal outputs from the ionization chambers measuring the neutron flux. These signals were amplified and processed in a function generator where the processed signal was compared with a fixed reference signal. Any disagreement produced an error signal which altered the position of the control valves thus changing the moderator level in the reactor vessel. The valve moved in a direction to cause the error signal to become zero when the demanded power level was reached.

The automatic power control circuit comprised three separate and identical circuits, called channels, extending from the ionization chambers through the electronic control equipment to the control valve. A diagram of one channel of the control system is shown in Figure 3.

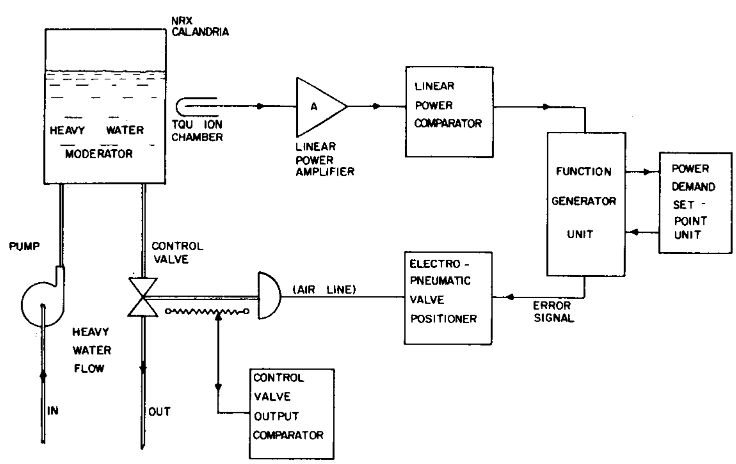

Figure 3

Single Channel Components in the Heavy Water Level Control System

Should any component in a single channel fail, the channel was automatically rejected and reactor power was adequately controlled by the remaining two channels. When two control channels were rejected, the reactor was automatically shut down. Provision was made for manual control of the valves but this was rarely used as automatic control was easier and smoother.

The start-up sequence for the reactor involved two deliberate manual operations, namely, resetting of the electrical trip circuits and raising of the shut-off rods. Once this was done, the dump and control valves closed automatically and the supervisor needed only to start the heavy water pumps and set the desired power level on the control console to achieve start-up. The automatic control system brought the reactor up to critical, to the demanded power level, and maintained it there without any further manual operations on the part of the supervisor. The entire start-up required about 15 minutes to complete. Sequence control circuits were provided to initiate automatic shutdown should the start-up sequence be contravened for any reason. In addition, the protective instrumentation system was in operation at all times and would shut down the reactor should an unsafe condition develop. Some trips such as rate-of-rise of power, mean power and overpower were actually built into the electronic equipment that controlled the reactor start-up. This meant that the supervisor, once he initiated start-up, was essentially free to observe instrumentation displayed in the control room and not required to operate the control console as he was previously.

The performance of this system has been extremely good. In the 3-1/2 years it has been in operation not a single control valve failure has occurred. Rate-of-rise-of-power trips were frequent during start-up under manual control; now this type of trip is rare. Reactor operation has been very stable with this method of control.

2.4 Protective Instrumentation

The original instrumentation system essentially comprised two separate electrical circuits; a parallel or "make" circuit and a series or "break" circuit as shown in Figure 4.

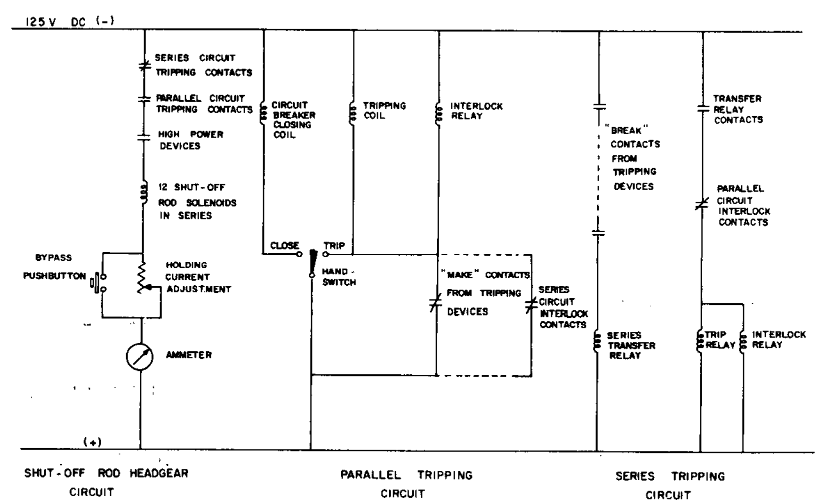

Figure 4

Original Electrical Trip System

Automatic reactor shutdown occurred on receipt of a signal from a monitoring device in either circuit indicating that a condition had developed that was unsafe for continued reactor operation. A shutdown (trip) would also result in the event of failure of a single instrument in either circuit.

In this scheme both the tripping devices and the parallel circuit were not "fail-safe", i. e. contacts closed and relays were energized to indicate a fault. On power failure the circuit was inoperative. A further disadvantage was the absence of positive identification of trips in the series circuit.

The reactor trip rate under these conditions was extremely high (275 per year). This was due in part to the fact that failure of a single instrument would cause a reactor shutdown even though the process being monitored was in a normal safe state.

Prior to the accident in 1952 an automatic reactor trip occurred on a signal from a monitor that an unsafe condition existed, regardless of the reactor power. On start-up in 1954 following the rehabilitation of the reactor, a new system was introduced whereby those reactor trip functions that were relatively unimportant at low power were conditioned such that they would not initiate a reactor shutdown below 1% of full power. Trips arranged in this fashion were designated "conditional" trips. The few remaining trips were considered sufficiently important to require that all means of reducing the reactivity of the reactor be used and maintained in action regardless of the reactor power. These functions were termed "absolute" trips. The electrical circuits were arranged as shown in Figure 5.

Under this arrangement the supervisor was permitted to make certain preparations for start-up and actually to bring the reactor to a low power stage with conditional trips actuated and indicating in the control room. Thus start-up could be initiated while the unsafe conditions causing the trips were being corrected. Once the trips were cleared, reactor start-up was continued to the high power stage.

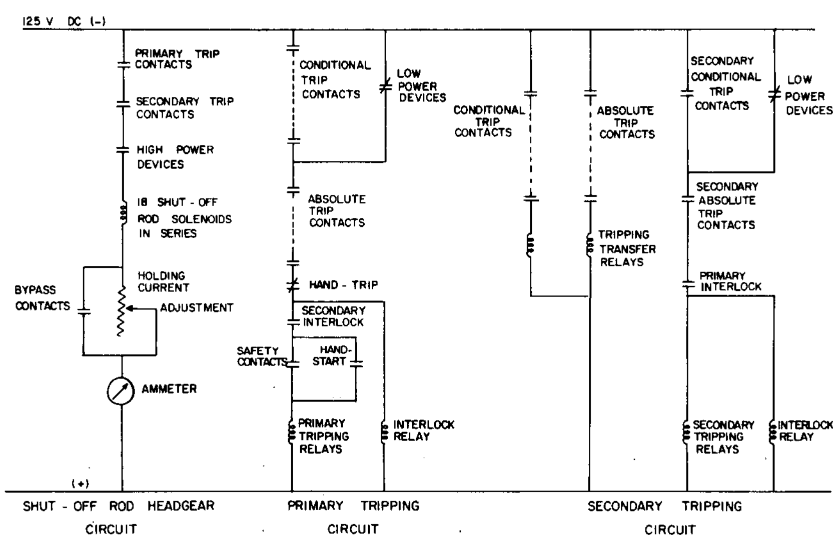

Figure 5

Electrical Trip System (1954-1956)

At the same time the "fail-safe" concept of electrical relays was adopted and the design of electrical circuits was kept as simple as possible. In the "fail-safe" arrangement all electrical relays were energized and contacts closed with the reactor operating normally at power. When the fault indicated, contacts opened and relays de-energized to initiate the trip. Although the primary and secondary trip circuits were "fail-safe" some of the trip devices were not and there still was no identification of individual faults in the secondary circuit.

This two stage start-up procedure improved operating efficiency in that potential poison shutdowns were prevented by minimizing the total down time of the reactor. However, reactor trips due to single instrument faults were still quite prevalent.

In 1956 when the electric shut-off rods were installed along with the moderator dump system the electrical circuits remained for the most part unchanged. The secondary circuit was modified to provide identification of individual faults. The electrical system was as shown in Figure 6. The dump valves were arranged in two banks of three for greater safety. Three control valves were installed at this time but were only used to dump the moderator. In addition all of the tripping devices were converted to a "fail-safe" type.

When full automatic power control was inaugurated in 1958, a new system of protective instrumentation was installed. Instruments monitoring processes in the reactor were triplicated and the electrical

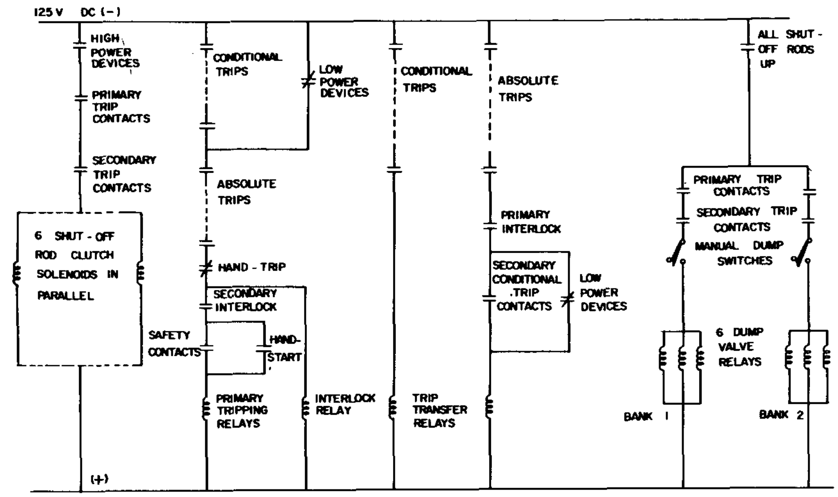

Figure 6

Electrical Trip System (1956-1958)

trip circuits were arranged in three separate identical channels. This system required that instrument contacts be opened in two of the three channels to initiate an automatic reactor shutdown. A danger signal indicating in only one channel produced an alarm. This arrangement of tripping functions was termed a two out of three coincidence system. The "fail-safe" arrangement of relays and the classification of trips into absolute and conditional, together with the two stage start-up system were features that were retained in the new system. The shut-off rod and dump valve circuits and one channel of the coincidence trip circuit are shown in Figure 7.

One basic advantage of this type of trip system was that any single channel could be removed from service to permit overhaul and repair of instruments and the components of a single channel could be subjected to a true functional test with the reactor operating. A further advantage lay in the fact that single faults in instruments or in the trip system would not trip the reactor. This greatly reduced the number of shutdowns caused by this type of fault.

The three channels of the power control system were tested daily with the reactor at power for a period of one year following installation of this system. These tests were designed to detect faults in the electronic control equipment and in the associated reactor power trip functions. Failures found in this test were so few in number that the test frequency for these circuits was reduced to once a week in 1959.

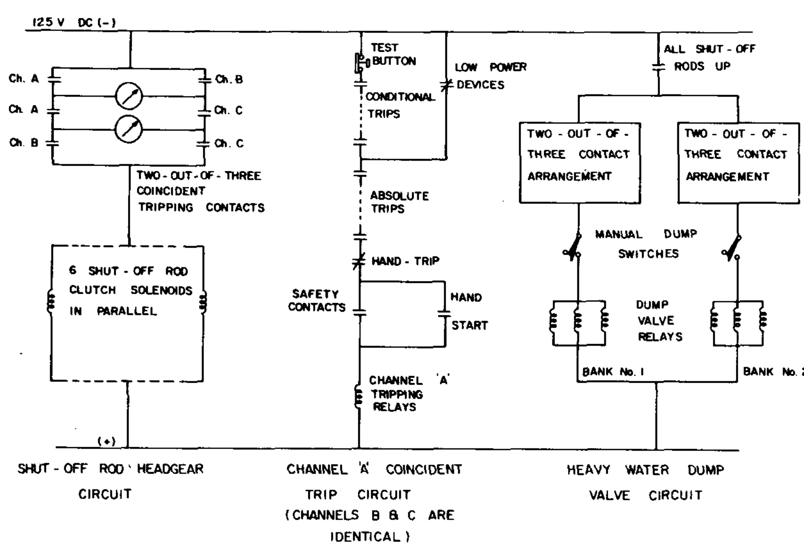

Figure 7

Present Electrical Trip System

These tests are still being conducted although a further reduction in frequency to once a month is under consideration owing to the small number of faults currently being detected.

Operating experience with this protective system has been most satisfactory. The overall trip rate of the reactor has been reduced to 63 stoppages per year (1961). This has been reflected in a slight improvement (from 75 to 79%) in reactor operating efficiency despite the fact that the scheduled monthly reactor shutdowns are of much longer duration because of the increased experimental load.

3. ORGANIZATION OF NRU REACTOR OPERATION

3.1 Historical Note on NRU

While many of the aforementioned NRX improvements were being realized the NRU reactor was being designed and built. In November 1957, approximately 10 years after the NRX start-up this reactor began operation. Being a 200 MW (Thermal) reactor, it was more complex than its Canadian predecessors, and in addition incorporated facilities for changing fuel rods under full power. Much valuable experience had been gained from the NRX operation and this experience was used not only in the design of NRU but in the establishment of safe operating techniques. Large complex reactors such as NRX and NRU require sound organizational controls. The larger the unit, the more complex they become. The organized responsibilities for the operation of the

NRU reactor demonstrate AECL's approach to reactor safety through administrative control.

3.2 Organization

To ensure satisfactory operation, the organization of personnel and the clear definition of their responsibilities must be well established. This applies both to the reactor branch itself and to the supporting organizations from other branches, on which the reactor branch is dependent for assistance.

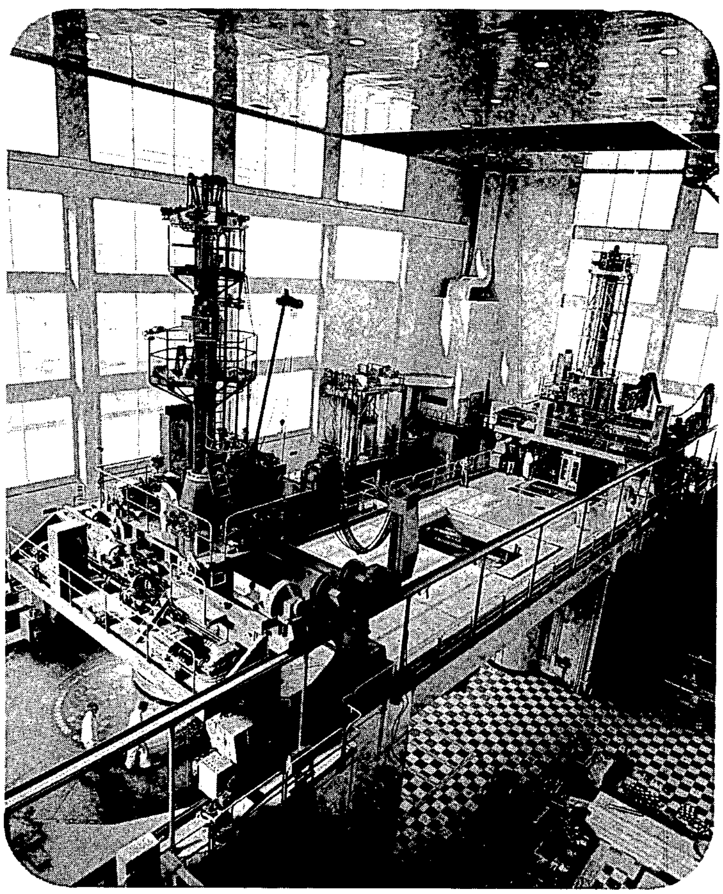

Figure 8

NRU Reactor

The organization established for NRU is typical. The responsibility for the reactor, and the building containing it rests with the superintendent and, through delegated authority, with the assistant superintendent and supervisors.

The reactor and its associated equipment are divided into six sections. A senior supervisor is assigned the responsibility for each of these sections under a policy laid down by the superintendent. Included in these responsibilities are the continual overall technical assessment of the operation of the section, its safety and efficiency, and the training of both supervisory and prevailing-rate personnel. The six areas of responsibility are:-

(1) Rod Work

(2) Control and Safety Systems

(3) Process and Service Systems

(4) Reactor Structure and Research

(5) Loops (High pressure, High Temperature, In-reactor, Engineering Test Rigs)

(6) Reactor Physics

The responsibility for carrying out the program on the reactor and its system is delegated to the supervisor in charge of each shift. A shift consists of the supervisor in charge, a rod supervisor, a loop supervisor, a supervisor of general operations, a process operator lead hand and eighteen process operators. In addition, there is normally one supervisor in training on each shift.

Two foremen are employed on day duty only; one is a rod foreman, the other a process foreman. These men work directly with the day crew of process operators and, through the shift organization have normal foreman responsibilities for the prevailing rate personnel on shift.

The reactor branch is dependent on a number of groups outside its own organization to assist in maintaining safe and efficient reactor operations. These are:-

Service Branches

All maintenance with the exception of the maintenance of rod parts is conducted by the plant maintenance forces. Established in the reactor building are sections of the Maintenance and Power Branch responsible for mechanical, process instrument and electronic maintenance as well as the installation of new equipment and modifications. All building maintenance is done as required on request to the Building Maintenance, and Construction Branch. The Workshop, Estimating and Planning Branch provide the normal machine shop service and are responsible for supplying sheathed uranium fuel for the reactor.

Engineering Design

On request of the reactor branch, the Engineering Design Branch is responsible for design work for the reactor. A design engineer is located in the reactor building to provide "on-the-spot-service" for the small day to day problems that arise in the field.

Engineering Development

On request of the reactor branch, the Applied Engineering Development Branch works on problems in the operation of equipment where no actual re-design may be required, but a change in material, for instance, may be the solution. This branch works as a service group to the Design Branch, developing and testing new design concepts.

Reactor Technology

Within the organization of the Operations Division, is the Reactor Technology Branch. This is an advisory group to the reactor superintendent and it reviews technical problems and safety aspects of reactor operations.

Radiation Hazards Control

The Radiation Hazards Control Branch assigns a group to each area on the project where radioactivity problems may arise. Such a group is established in each of the reactor buildings. This group contains personnel trained in radiation and contamination control. The supervision and radiation surveyors of the R.H.C. Branch act as advisors to the reactor branch on problems arising in their field. Two surveyors, one decontamination monitor and two decontamination operators are assigned to each shift to maintain contamination control and survey radiation hazards.

Research Branches

The research establishment at Chalk River is large and diversified. It is therefore possible when problems arise to call on the extensive knowledge of experts in many fields. The project policy is such that the reactor superintendent may call for assistance from these specialists when the need arises. Committees are established with representation from the research branches to review problems or proposed changes in operating policy as requested by the reactor superintendent and to make recommendations to him.

3.3 Training

As previously mentioned, the responsibility for training personnel on the various aspects of the reactor rests with the senior supervisors. In the case of process operators, the responsibility for carrying out the established training program is delegated to the rod foreman for rod work, and the process foreman for general operation. Ultimately, however, a considerable portion of the training responsibility must rest with the shift organization as the nature of the operation makes "on-the-job-training" mandatory.

The control and safety system, as the heart and nerve centre of the reactor, receives particular attention in regard to training. As in training on the other reactor systems, the senior supervisor responsible must satisfy himself that the supervisor in training is completely conversant with the equipment, drawings, and operation of the system. In order to maintain a consistent, safe and efficient mode of operation of the control console, shown in Figure 9, no one in training is permitted to operate the controls of the reactor, unless under the direct surveillance of the senior supervisor in charge of the control system. When a supervisor has satisfactorily completed his training on the control and safety system, he is authorized in writing by the superintendent to operate the reactor console.

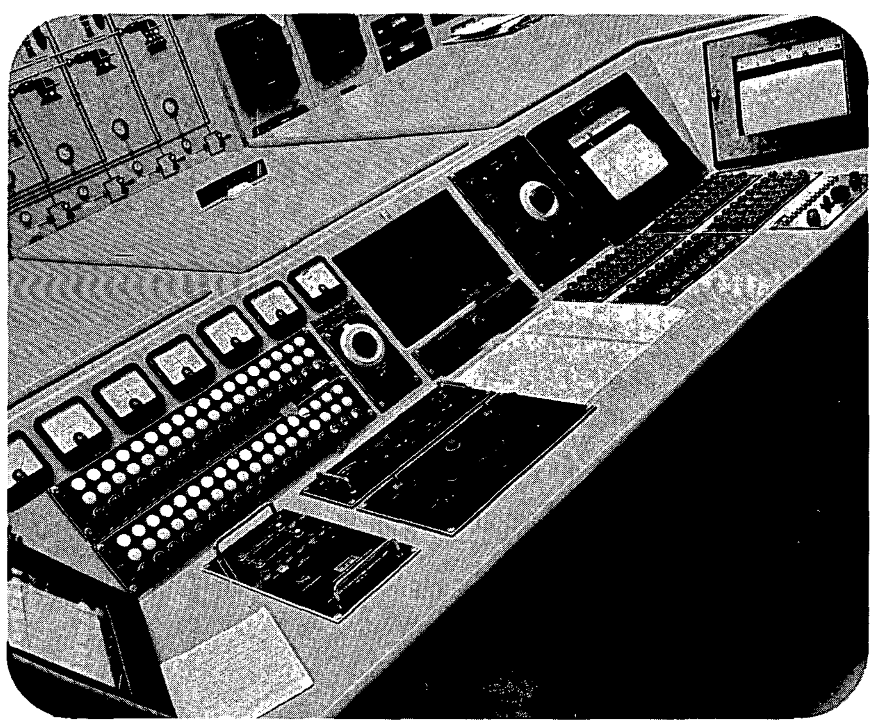

Figure 9

NRU Control Console

Reactor branch personnel are trained not only in the operation of the reactor and its auxiliary systems, but also in radiation hazards control. Although specialists from the Radiation Hazards Control Branch are always available, it is a well established policy in reactor branches that each supervisor, foreman and operator must be trained in radiation hazards control and must be capable of being his own radiation surveyor and contamination monitor. Under this policy a reactor branch employee should never have to jeopardize the health and safety of himself or his co-workers because a specialist does not happen to be present.

3.4 <u>Manuals</u>

The training of personnel is greatly assisted by the information outlined in the manuals for the reactor. In the case of the NRU reactor, there are over one thousand manuals which have been written and revised by reactor supervision throughout the history of the reactor.

The design manuals provide detailed information on the reactor and its auxiliaries. They provide, in fact, a complete handbook of the reactor.

The testing manuals primarily outline the test procedures that were used during the commissioning of the reactor.

The operating manuals detail the procedures to be followed in the operation of the reactor and its components. In addition they provide an outline of the philosophy for operating any particular system. They therefore form the basis for training personnel.

To augment the manuals, instruction entitled "Instructions to Supervisors" are issued as required, stipulating operating and administrative policies, detailing specific procedures for operating new equipment, and outlining the procedures to be followed to comply with new or modified operating policies. All supervisors are required to read and sign the control-room copy of each instruction.

3.5 Procedures

As indicated in the foregoing, for clarity and understanding, the established policy is that instructions must be in writing. This policy is maintained throughout. Examples of some of the procedures in force will be described to illustrate the method of control.

(1) Design Procedures

The procedure for completing design work may take a number of forms. For instance, minor modifications may be required for a quick solution to an immediate problem. In this case the Engineering Design Branch is consulted. The reactor branch authorizes the modifications by issuing a multi-copy, standard form memorandum to the maintenance group. The modifications are completed in the field and the drawings are brought up to date by the Engineering Design Branch.

The normal practice, however, is for the reactor branch to issue a request for design work to the Engineering Design Branch. A design proposal, either in the form of a design study for a large job or in the form of completed prints for a smaller job, is issued to the reactor branch for comments and approval.

As in many fields, it is expedient from time to time to grant concessions to the design in the manufacture of items for the reactor. As an example it may be necessary because of difficulties in operation, to incorporate a proposed laboratory-tested modification to a replacement part to assess the modification in actual service. Such a concession is approved by the reactor superintendent in writing, on a specified form. This approval is normally given after a consultation with advisors on the subject. The concession is filed and provides a record for identification and control of the modification, or manufacturing concession for the specific part.

It is essential that up-to-date information and correct blue prints on all systems are available at all times. No change to a system is permitted without written authorization.

(2) Work Permits

The control of field work is required in the interest of reactor operation, as well as the safety of personnel. The financial authorization and description of work for maintenance, modification or installation requirements is issued by the reactor branch in the form of a work order. This, however, does not authorize the maintenance personnel to proceed.

When the work is to be done, a work permit is issued. Authority for the issuance of work permits is delegated to the supervisor in charge of the shift, he being the man who is in direct control of the overall operation of the reactor. The life of a work permit is eight hours. If it is necessary to continue work after this period, authorization to proceed is required from the supervisor in charge of the relieving shift.

There are three copies of every work permit, each bearing at least two signatures, and where health hazards may be involved, three signatures. A surveyor of the Radiation Hazards Control Branch signs the clearance, and outlines in the space provided the health precautions to be taken and the protective equipment to be used. The reactor branch supervisor signs the clearance authorizing the work to proceed. Finally the maintenance representative signs the permit indicating that he understands the instructions given on the work permit.

A close record of the work permits is maintained in the control room at all times. At the end of the shift, the work permits are signed off by the maintenance and reactor branch personnel as either complete or incomplete and appropriate action is taken.

In the case where the work directly affects reaction operation, requiring the reactor to be shut down, the work permit is designated as APO (affecting pile operation). A board, shown in Figure 10, is maintained in the control room of the reactor, and on this board are numbered tags covering all the maintenance trades.

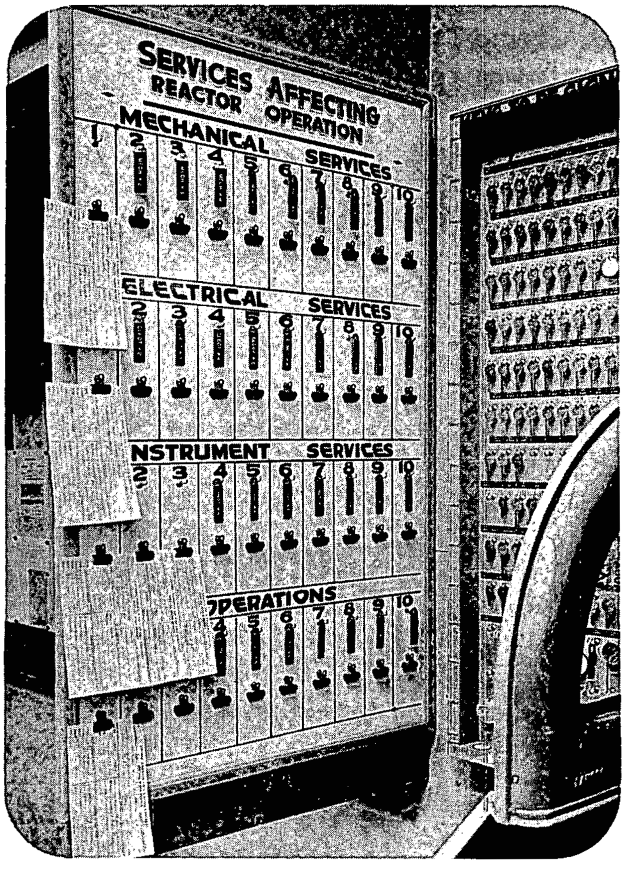

Figure 10

Board displaying Work Affecting Pile Operation

When an APO work permit is issued, the reactor is in a shut-down condition. A tag is removed from the board and replaced with the reactor branch copy of the work permit. The tag is issued to the maintenance man. Procedure dictates that the reactor will not be started up with a tag missing from the APO board.

(3) Door Interlocks

For further protection to personnel, a system of door interlocks is installed in the reactors. Much of the reactor equipment is located in areas that are not accessible during reactor operation due to high radiation fields. The access doors to such areas have locks that are electrically interlocked to a key panel, Figure 11, in the control room.

In order to gain entry to the area, the key for the door must be obtained from the control room panel. The removal of the key from the panel automatically imposes a shutdown condition on the reactor. Conversely the keys must be replaced to remove this automatic shutdown

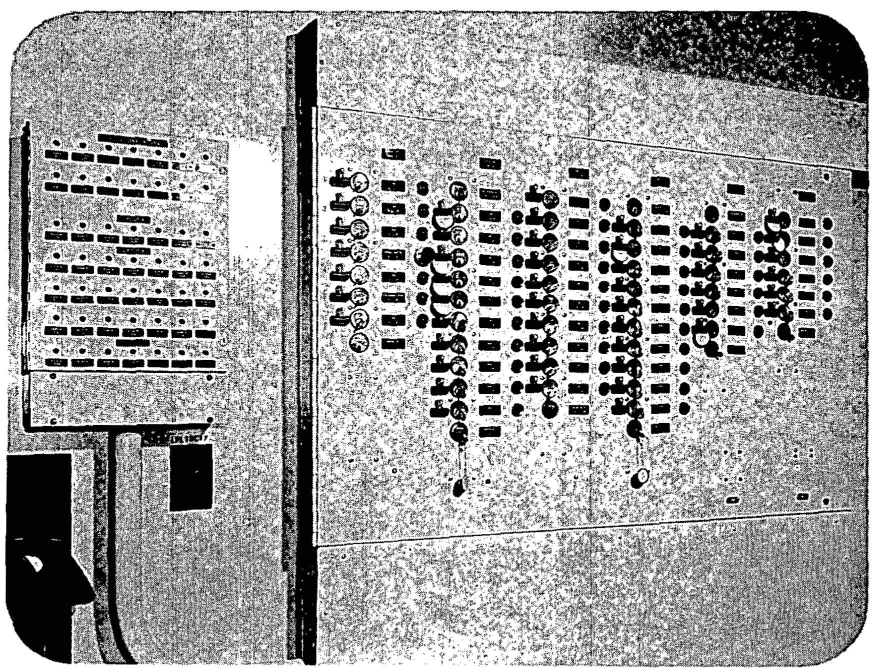

Figure 11

Door Interlock Panel

condition or trip from the reactor before the reactor can be started up. To minimize the possibility of locking the door with someone still in the area, a "door-closure-preventing" mechanism will not allow the door to close until an interlock circuit is closed by actuating a push button in the control room. Before a door can be closed the man at the door must obtain authorization from the control room. If the authorization is granted, the door can only be closed by the simultaneous actions of two people; the operation of the push button by the control room operator and the closing of the door by the operator in the field. The inadvertent closing of doors and replacement of keys in the interlock panel is thus prevented.

(5) Valve-Slip Procedures

A close control of the circulating systems must be maintained at all times, as the safety of the reactor is dependent to a large extent on the cooling systems. In a large reactor, these systems become quite involved. In the heavy water and helium systems of the NRU reactor, there are over 5000 valves, and there are many other systems as well. To ensure control, there is a precise flow sheet of each system maintained in the control room, and the status of each valve is shown by the use of coloured pins, (Figure 12). When a valve is to be manipulated, a written instruction in duplicate is issued by the supervisor to the process operator. This instruction is called a valve slip. One copy goes with the man who manipulates the valve and the duplicate stays in the

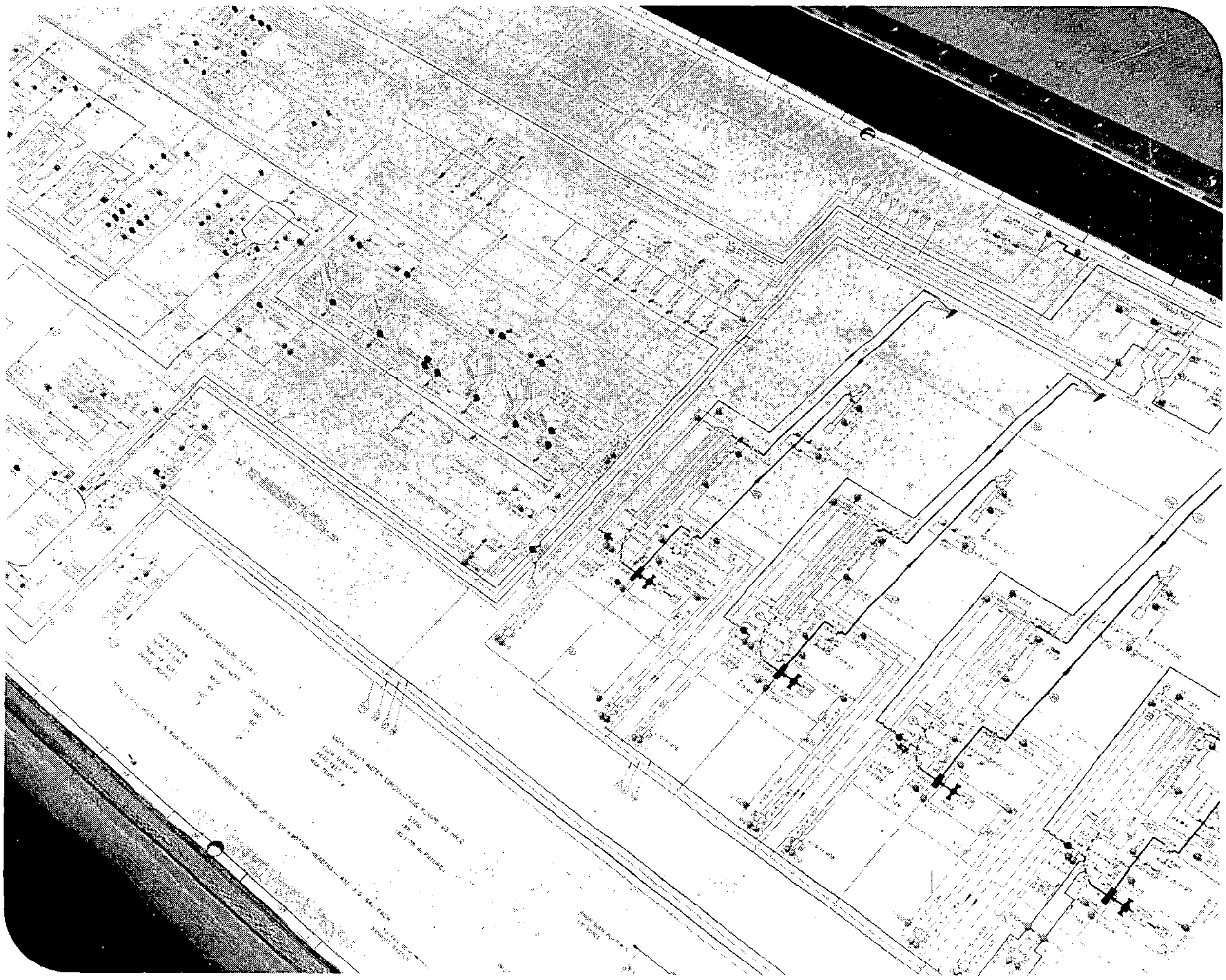

Figure 12

Recording the Positions of Valves

the master book in the control room When the manipulation is complete, the man completing the work informs the control room and the status of the valves on the flow sheet is brought up to date.

(6) Maintenance Procedure

Where possible, to ensure efficient operation as well as reliability of the system, back-up equipment is provided. For instance, parallel pumping units are installed where reactor shutdown would result from the loss of a single unit. A schedule for routine preventive maintenance is established to maintain equipment in top operating condition Parallel units are changed over on a routine basis to spread the wear over the units and to ensure that they will operate when required.

There are some areas in reactor systems however, where restrictions must be placed on routine maintenance An example is the pile-face amplifiers in the NRU reactor control system This is a four-channel system, so designed that any one channel can be rejected during reactor operation to permit maintenance. The reliability of the system is enhanced by the fact that the four channels are compared to one another. The only true proof of the individual unit is its response to the signal from the ion chambers seeing the reactor flux. This has been carefully calibrated throughout reactor operating experience. It is therefore safer to remove a unit for routine maintenance and install a replacement unit while the reactor is operating and the signal is known. The policy is thus established that no more than one pile-face amplifier.

can be removed for routine maintenance during any one reactor shut-down, if the units are reading below a reliable output level.

(7) Check-off Systems

Some reactor operations are quite complex and yet in their complexity they demand rapid, precise action. This requires trained personnel, well versed in the operation of the system so that procedures can be completed as expediently as possible. A typical example is the operation of the fuel rod flask which is used to replace fuel rods in the NRU reactor under full reactor power. To ensure the safety of this operation, a check-off system is employed. The rod crew conducts the operation without reference to procedure carrying out the routines as required. One man however, is established as an observer, with a precise written procedure on hand. This man is trained in the operation and checks off each item in the procedure as it is completed. He takes no active part in the operation unless a step is inadvertently missed at which time he will point out the error. In this manner, a precise procedure is always maintained, minimizing the chance of error and ensuring the required safety and efficiency of the operation.

(8) Equipment Checks

To obtain the maximum in efficiency and safety, the integrity of the safety system must be of the highest order. The philosophy of the safety system for the NRU reactor is based on the coincidence system. Thus, all units that will automatically shutdown or trip the reactor on fault are triplicated. The actuation of any two of the devices will cause a trip. This enables checks to be made on any one of the devices while the reactor is operating. Routines are established whereby each trip and alarm device as well as its actuating mechanism is checked on a regular basis.

Of course many of the safety devices cannot be checked except when the reactor is shut down. Procedures are therefore established and maximum advantage is taken of every reactor shutdown to complete these important checks. In some cases, this involves simulating power failures by pulling main power supply breakers to ensure that all the required safety devices operate, that the interlocks function and that emergency power supplies come into service in the prescribed manner.

4. SUMMARY

In review, experience at Chalk River has indicated that reactor operations must not remain static. The operating staff must always be receptive to possible improvements in safe operation.

As a result of experience and technical advances, the NRX reactor can now be operated much more safely and reliably than was possible with the original control and safety systems. Today, through adjustment of moderator level, start-up and control are fully automatic. The automatic protective trip system is designed in a two out of three coincidence arrangement in which two independent shutdown devices are actuated when an unsafe condition develops.

Concurrent with these advances have been developments in administrative control to enhance reactor safety. Some of the many procedures that have been established to maintain the safe and efficient operation of the NRU reactor have been outlined. AECL experience indicates that it is essential to have well established responsibilities. Once having these established, it is necessary to have a well-knit organization with personnel trained in sound policies and procedures.