APPENDIX A

Changes to Technical Specifications

1.0 Reactivity Insertion Rate

1.1 Proposed Change

Change specification 3.2.2 and its basis from its present form which reads:

"3.2.2 MANUAL AND AUTOMATIC CONTROL

Applicability

This specification applies to the maximum reactivity insertion rate associated with movement of a standard control rod.

Objective

The objective is to assure that adequate control of the reactor can be maintained during manual and automatic operation.

Specification

The maximum rate of reactivity insertion associated with movement of either the regulating, shim, or safety control rod shall be no greater than 0.12% Δk/k (~17¢) per second.

Basis

This limits the insertion of reactivity to a rate much less than that during a pulse insertion of 2.31% Δk/k reactivity. At a maximum insertion rate of 0.12% Δk/k/sec it takes almost 6 seconds to insert 0.007 Δk/k (~$1.0) of reactivity; the large negative temperature coefficient of the core (see page IX-29 of the SAR) limits the increase of the average core fuel temperature to 70°C due to the 0.007 Δk/k insertion. Thus, the core temperature will compensate for the rate of insertion of reactivity. In addition, the location of the maximum fuel temperature will be the same as that during constant power operation, i.e., near the position of the thermocouple. Hence, when either the linear, percent power, or temperature scram occurs, the maximum fuel temperature will be far below the 1150°C safety limit."

The proposed wording of specification 3.2.2 is as follows:

"3.2.2 MANUAL AND AUTOMATIC CONTROL

Applicability

This specification applies to the maximum reactivity insertion rate associated with movement of a standard control rod out of the core.

Objective

The objective is to assure that adequate control of the reactor can be maintained during manual and 1, 2, or 3 rod automatic control.

Specification

The rate of reactivity insertion associated with movement of either the regulating, shim, or safety control rod shall be no greater than 0.63% Δk/k (~90¢) per second when averaged over full travel. If the automatic control uses a combination of more than one rod, the sum of the reactivity of those rods shall be no greater than 0.63% Δk/k (~90¢) per second when averaged over full travel.

Basis

The ramp accident analysis (refer to Safety Evaluation, Chapter IX) indicates that the safety limit will not be exceeded if the reactivity addition rate is less than $2.50/second, when averaged over full travel. This specification of $0.90/second, when averaged over full travel, is well within that analysis."

This change is requested to be made effective at the time of the reactor console replacement.

1.2 Reason for the Change

The new control system allows automatic control with up to three control rods. The proposed change will give greater flexibility for three rod control.

1.3 Safety Evaluation of the Change

The analysis provided shows that the proposed specification gives the desired flexibility while maintaining a wide margin between the allowed reactivity insertion rate and that where the safety limit is met.

2.0 Overpower Scram Testing

2.1 Proposed Change

Change specifications 3.1.1.a and its basis and specifications 4.2.5 from their present form which reads:

"3.1.1 CONSTANT POWER AND SQUARE WAVE OPERATION

Applicability

This specification applies to the maximum power generated during manual, square wave, and automatic operation.

Objective

The objective is to assure that the safety limit (fuel temperature) will not be reached during manual, square wave, and automatic operation by providing a set point to automatically limit the maximum fuel temperature produced in the core and to limit the energy produced in any seven (7) consecutive days to that used in the LOCA analysis in the Safety Analysis Report.

Specification

a. The operating power level of the reactor shall not be intentionally raised above one megawatt except for pulse operation (see specification 3.1.4)."

"Basis

a. Thermal and hydraulic calcuations and operational experience indicate that a compact TRIGA reactor core can be safely operated up to power levels of at least 1.15 megawatts with natural convective cooling. Power operation at 1.15 megawatts will not produce fuel temepratures which exceed 600°C using any allowed core configuration giving a large safety measure when the power of operation is limited to 1 MW. Thus, small variations can occur about 1 MW during normal operation and still provide a large measure of safety in that the maximum fuel temperature remains well below the safety limit. This is true even if variations as high as 15% above 1 MW should occur. See Safety Analysis Report, section IX."

"4.2.5 Overpower Scram

Applicability

This specification applies to the high power and fuel temperature scram channels.

Objective

The objective is to verify that high power and fuel temperature scram channels perform the scram functions.

Specification

The high power and fuel temperature scrams shall be tested annually, not to exceed 15 months."

The proposed wording of specification 3.1.1.a and its' basis and specification 4.2.5 is as follows:

"3.1.1 CONSTANT POWER AND SQUARE WAVE OPERATION

Specification

a. The operating power level of the reactor shall not be intentionally raised above one megawatt except for the following two conditions:

1. During pulse mode operation, power may exceed 1 megawatt (see specification 3.1.4).

2. During overpower scram surveillance, power may not exceed 1.15 megawatts (see specification 4.2.5)."

"Basis

a. Thermal and hydraulic calculations and operational experience indicate that a compact TRIGA reactor core can be safely operated up to power levels of at least 1.15 megawatts with natural convective cooling. Power operation at 1.15 megawatts will not produce fuel temperatures which exceed 600°C, using any allowed core configuration. This gives a large safety margin since the LSSS is 700°C. Small variations in power can occur during nominal 1 megawatt operation and still provide a large margin of safety. This is true even if variations as high as 15% above 1 megawatt should occur (see Safety Analysis Report, section IX). During the short period of time that high power scrams are tested, the power may be raised to 1.15 megawatts without exceeding the safety limit."

"4.2.5 Overpower Scram

Applicability

This specification applies to the high power and fuel temperature a scram channels.

Objective

The objective is to verify that high power and fuel temperature scram channels perform the scram functions.

Specification

The high power and fuel temperature scrams shall be tested annually, not to exceed 15 months. During testing of the high power scrams, the operating power level may be raised to, but not exceed, 1.15 megawatts (see specification 3.1.1)."

2.2 Reason for Change

This change is not related to the reactor console replacement and is included in this submittal as a matter of convenience. As presently written, the reactor power cannot be intentionally increased above 1.0 megawatt. Scram devices set at 1.10 megawatts can, therefore, only be tested electronically. The change will allow the physical parameter, reactor power, to be raised to verify the scram setpoint.

2.3 Safety Evaluation of the Change

The accident analysis was performed at 1.15 megawatts, providing a basis for steady state operation at that power level. The proposed specification makes it clear, however, that exceeding 1.0 megawatt intentionally is restricted to overpower scram surveillance.

3.0 Replacement Pages

Attached are replacement pages 9, 14, 15, and 33 for the license R-2 technical specifications incorporating the proposed changes discussed above.

to reduce the amount of energy generated in the entire pulse transient, by cutting the "tail" of the power transient if the pulse rod remains stuck in the fully withdrawn position with enough reactivity to exceed the temperature-limiting safety system setting.

3.0 LIMITING CONDITIONS FOR OPERATION

The limiting conditions for operation as set forth in this section are applicable only when the reactor is operating. They need not be met when the reactor is shutdown unless specified otherwise.

3.1 REACTOR CORE PARAMETERS

3.1.1 CONSTANT POWER AND SQUARE WAVE OPERATION

Applicability

This specification applies to the maximum power generated during manual, square wave, and automatic operation.

Objective

The objective is to assure that the safety limit (fuel temperature) will not be reached during manual, square wave, and automatic operation by providing a set point to automatically limit the maximum fuel temperature produced in the core and to limit the energy produced in any seven (7) consecutive days to that used in the LOCA analysis in the Safety Analysis Report.

Specification

a. The operating power level of the reactor shall not be intentionally raised above one megawatt except for the following two conditions:

   1. During pulse mode operation, power may exceed 1 megawatt (see specification 3.1.4).

   2. During overpower scram surveillance, power may not exceed 1.15 megawatt (see specification 4.2.5).

b. The reactor shall not be operated to produce more than 70 megawatt hours of energy in any seven (7) consecutive days.

Basis

a. Thermal and hydraulic calculations and operational experience indicate that a compact TRIGA reactor core can be safely operated up to power levels of at least 1.15 megawatts with natural convective cooling. Power operation at 1.15 megawatts will not produce fuel temperatures which exceed 600°C, using any allowed core configuration. This gives a large safety margin since the LSSS is 700°C. Small variations in power can occur, about 1 megawatt, during normal operation and still provide a large margin of safety. This is true even if variations as high as 15% above 1 megawatt should occur (see Safety Analysis Report, section IX). During the short period of time that nigh power scrams are tested, the power may be raised to 1.15 megawatts without exceeding the safety limit.

3.2 CONTROL AND SAFETY SYSTEM

3.2.1 REACTOR CONTROL RODS

Applicability

This specification applies to the reactor control rods.

Objective

The objective is to assure that sufficient control rods are operable to maintain the reactor subcritical.

Specification

There shall be a minimum of three operable control rods in the reactor core.

Basis

The shutdown margin and excess reactivity specifications require that the reactor can be made subcritical with the most reactive control rod withdrawn. This specification helps assure it.

3.2.2 MANUAL AND AUTOMATIC CONTROL

Applicability

This specification applies to the maximum reactivity insertion rate associated with movement of a standard control rod out of the core.

Objective

The objective is to assure that adequate control of the reactor can be maintained during manual and 1, 2, or 3 rod automatic control.

Specification

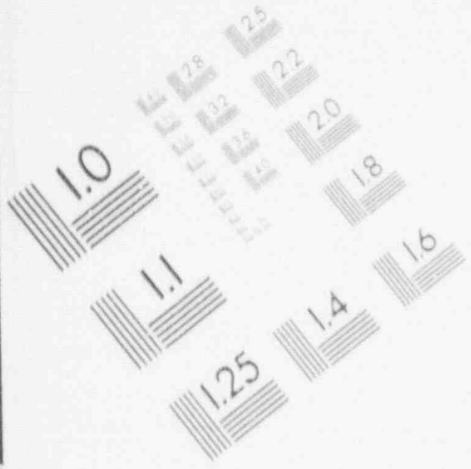
The rate of reactivity insertion associated with movement of either the regulating, shim, or safety control rod shall be not greater than 0.63% $\Delta k/k$ (~90¢) per second when averaged over full rod travel. If the automatic control uses a combination of more than one rod, the sum of the reactivity of those rods shall be not greater than 0.63% $\Delta k/k$ (~90¢) per second when averaged over full travel.

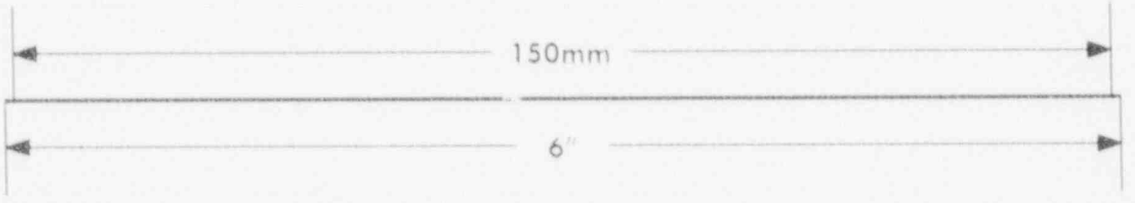
Basis

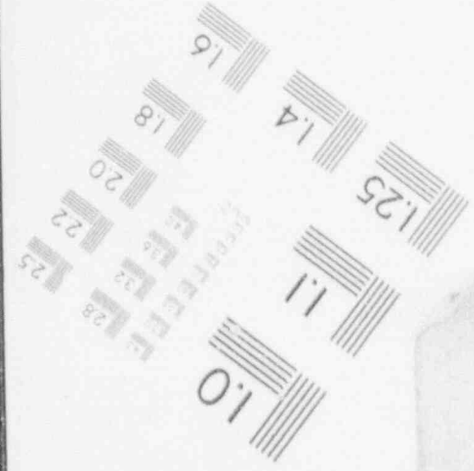
The ramp accident analysis (refer to Safety Evaluation, Chapter IX) indicates that the safety limit will not be exceeded if the reactivity addition rate is less than $2.50/second, when averaged over full travel. This specification of $0.90/second, when averaged over full travel, is well within that analysis.

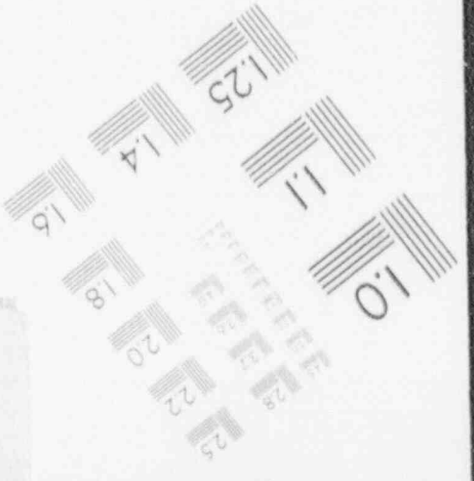
1

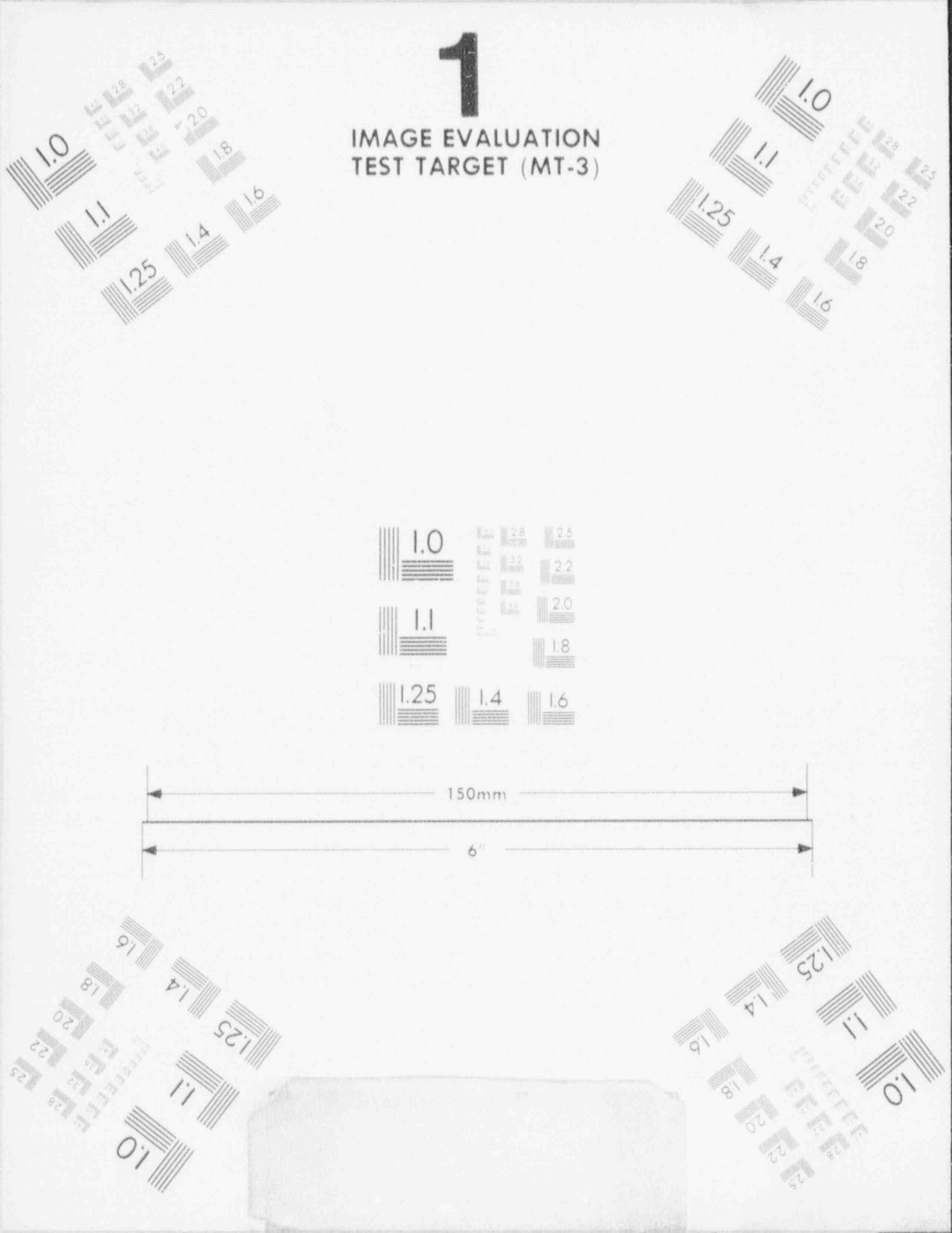
IMAGE EVALUATION TEST TARGET (MT-3)





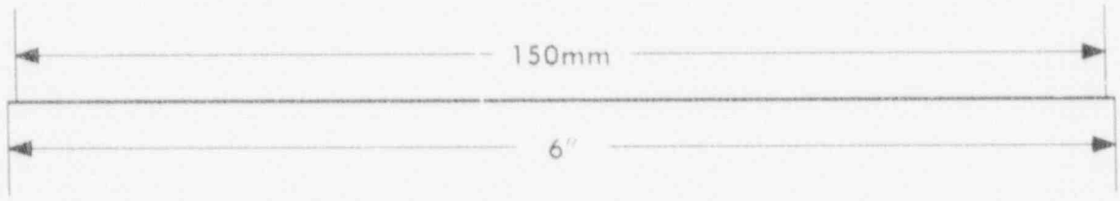





1
IMAGE EVALUATION
TEST TARGET (MT-3)
1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
150mm
6"

1

IMAGE EVALUATION
TEST TARGET (MT-3)



3.2.3 REACTOR CONTROL SYSTEM

Applicability

This specification applies to the information which must be available to the reactor operator during reactor operation.

Objective

The objective is to require that sufficient information is available to the operator to assure safe operation of the reactor.

Specification

The reactor shall not be operated unless the measuring channels listed in Table 1 are operable. (Note that MN, AU, and SW are abbreviations for manual, automatic and square wave, respectively).

Table 1

Measuring Channels

Measuring Channel	Min. No. Operable	Effective Mode		
		MN,AU	Pulse	SW
Fuel Element Temperature	1	X	X	X
Linear Power	1	X		X
Percent Power	1	X		X
Pulse Peak Power	1		X	
Count Rate	1	X		
Log Power	1	X		X
Reactor Period	1	X		

Basis

Fuel temperature displayed at the control console gives continuous information on this parameter which has a specified safety limit. The power level monitors assure that the reactor power level is adequately monitored for the manual, automatic, square wave and pulsing modes of operation. The specifications on reactor power level and reactor period indications are included in this section to provide assurance that the reactor is operated at all times within the limits allowed by these Technical Specifications.

c. A channel check shall be performed semi-annually, not to exceed $7\frac{1}{2}$ months, on the transient rod interlock which prevents application of air to the transient rod unless the cylinder is fully inserted.

d. A channel check shall be performed semi-annually, not to exceed $7\frac{1}{2}$ months, on the rod drive interlock which prevents movement of any rod except the transient rod in pulse mode.

e. A channel check shall be performed semi-annually, not to exceed $7\frac{1}{2}$ months, on the rod drive interlock which prevents simultaneous manual withdrawal of more than one rod.

Basis

The channel test and checks will verify operation of the rector interlock system. Experience at the PSBR indicates that the prescribed frequency is adequate to insure operability.

4.2.5 Overpower Scram

Applicability

This specification applies to the high power and fuel temperature scram channels.

Objective

The objective is to verify that high power and fuel temperature scram channels perform the scram functions.

Specification

The high power and fuel temperature scrams shall be tested annually, not to exceed 15 months. During testing of the high power scrams, the operating power level may be raised to, but not exceed, 1.15 megawatts (see specification 3.1.1).

Basis

Experience with the Penn State TRIGA for more than a decade, as recorded in the operation log books, indicates that this interval is adequate to assure operability.

4.2.6 Transient Rod Test

Applicability

This specification applies to surveillance of the transient rod mechanism.

Objective

The objective is to assure that the transient rod drive mechanism is maintained in an operable condition.

Appendix B

Safety Evaluation of the Reactor Console Change

It is PSBRs intention to license the reactor console change by the amendment route because of some technical specification changes. The following is a review of the reactor console change to assure that no unreviewed safety questions exist as a result of the change. The criteria of 10 CFR 50.59 is utilized to test the review.

10 CFR 50.59 permits licensees to make changes in the facility as described in the safety analysis report without prior Commission approval unless the proposed change, test or experiment involves a change in the technical specifications incorporated in the license or an unreviewed safety question. A proposed change, test or experiment shall be deemed to involve an unreviewed safety question (1) if the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the safety analysis report may be increased; or (2) if a possibility for an accident or malfunction (of equipment important to safety) of a different type than evaluated previously in the safety analysis report may be created; or (3) if the margin of safety as defined in the basis for any technical specification is reduced [4].

- **Duplication of Old Safety Functions Plus Redundancy and Additions**

  Figure 1 illustrates the division of the various components of the console into the functional parts; Reactor Safety System (RSS) and Protection, Control, and Monitoring System (PCMS). Functionally the DCC-Z is part of the PCMS but it performs no control or protection functions and it is isolated from the rest of the system with a one way data link. DCC-Z is not necessary to operate the reactor. For more detailled information see Chapter VII of the Safety Analysis Report [9] or the Design Manual [23].

- **Original *TRIGA* Console SCRAMs**

  Figure 2 lists all of the SCRAMs that existed on the original ***TRIGA*** console. All of the ones shown on the left are the SCRAMs that are

required by the technical specifications [9] and are reactor safety related. The individual rod manual SCRAMs exist for experimental convenience. The key switch SCRAMs the reactor for security reasons. It prevents unauthorized persons operating the reactor. The SCRAM with loss of AC power is a desirable feature and eliminates the need for emergency power. The external SCRAMs are available to experimenters to prevent or mitigate a potential unsafe condition.

- **New Console RSS SCRAMs**

  Figure 3 shows the new console RSS SCRAMs. Again those on the left are the required reactor safety related SCRAMs. All of the other SCRAMs of the old console also exist as well as two additions. The two additional SCRAMs are the PCMS SCRAM request and the PCMS Watchdog. These SCRAMs are not required by the technical specifications [9], nor are they safety related but SCRAM the reactor if nonconservative conditions occur.

  The PCMS Watchdog SCRAM occurs if the timer on the independent watchdog board is not reset by the PCMS for any reason. It occurs in less than 2 seconds if the reset does not occur within that interval. The PCMS does not reset the timer if the system fails for any reason, if a self test that is considered essential fails, if the hardware fails or if power fails.

- **PCMS SCRAMs**

  The PCMS SCRAM request occurs when any condition being checked by the DCC-X software logic becomes unsafe or nonconservative. Figure 4 illustrates all of the conditions that will cause a PCMS SCRAM request.

  The reactor bay truck door closed and at least one of two exhaust fans operating are two limiting conditions of operation (LCO). The PCMS SCRAM request assures that those LCOs are not violated.

  The east and west bay radiation and air particulate monitors, neutron beam laboratory radiation monitor and the evacuation pushbutton are required to activate the evacuation alarm by the technical specifications [9] but a SCRAM is not required. However, it is conservative and therefore desirable to SCRAM the reactor if an evacuation alarm occurs. That

SCRAM is initiated by the PCMS SCRAM request. The Co-60 laboratory radiation monitor is not required to activate the evacuation alarm or SCRAM the reactor by technical specifications [9] but the alarm is required by the Co-60 facility license and if an evacuation occurs it is desirable to SCRAM the reactor. The two fuel temperature high, the wide range power high, the power range power high and the pulse time out SCRAMs are duplications of the hardwired RSS reactor safety related SCRAMs. The operational interlock validation failure SCRAM occurs if there is a validation failure between the PCMS interlocks and the hardwired interlocks.

The velocity signal analog outputs from DCC-X to the motor controllers of the four rods is validated. This is accomplished by feeding the speed request analog output to the controllers back as an analog input to the computer (see figure 9). The software continuously compares the feedback signal to the requested output value. Validation failure results in a Rod velocity Signal Validation Failure PCMS SCRAM request.

The analog speed signal from the motor controllers is read by computer and a SCRAM occurs if the motor overspeed trip point is exceeded (see figure 9). An overspeed trip results in a Rod Motor Overspeed PCMS SCRAM request.

The 1 of 4 remote SCRAM buttons are available to experimenters to prevent or mitigate a potential unsafe condition of which they alone are aware. They are not required by the technical specifications.

The Square Wave Terminate PCMS SCRAM request is included for operational convenience. The operator can set a software timer to terminate a square wave operation with a SCRAM after a fixed interval.

All technical specification [9] required SCRAMs are hardwired in the new console as they were in the original ***TRIGA*** console.

- **New Console Hardwired Operational Interlocks**

  Figure 5 lists the new console hardwired relay logic operational interlocks. These interlocks are those required by the technical specifications [9] and identical to those of the original ***TRIGA*** console. The operational mode is communicated to the interlock logic by the PCMS and rod motion is prevented by closing the clockwise limit switches (CLS) or the counter clockwise limit switches (CCLS) to the motor controllers.

  The CLS contact closure stops the motor from moving in the clockwise direction. This input is controlled by the hardwired operational interlock logic for the up drive disable function. The CCLS stops the motor from moving in the counter clockwise direction while the contact is closed. This input is controlled by the hardwired operational interlock logic for the down drive disable function.

- **New Console PCMS Operational Interlocks**

  Figure 5 also lists the new console PCMS operational interlocks. The logic is implemented with PROTROL block language software. All of the technical specification required operational interlocks are duplicated by the PCMS. If there is a validation failure between the PCMS operational interlock and the hardwired operational interlock a PCMS SCRAM request is issued to the RSS.

  If the extensive PCMS self tests indicate a fatal failure of the DCC-X control rod withdrawal is prevented.

  If the reactor period is short control rod withdrawal is prevented. This interlock and the DCC-X failure interlock operate in all operational modes and are implemented by the closure of the CLS.

  The duplication of the hardwired operational interlocks, interlock validation SCRAM, the DCC-X failure interlock and the short period interlock are implemented by the PCMS and are redundant or not required by the technical specifications [9].

❑ **PCMS Stepbacks**

Figure 6 illustrates the PCMS stepbacks. The stepbacks are described elsewhere and are not required by the technical specifications. The original ***TRIGA*** console does not have stepbacks.

❑ **Explanation of Safety, Protection, Control and Monitoring Structure**

Safety in depth was a basis of design of the PSBR console. Figure 7 is a diagram of the new safety, protection and control system. It was decided that analog electronics, with its established reliability, would be used for the reactor safety system, RSS. The analog RSS is the safety related envelope within which the reactor operates. The PCMS computer, DCC-X, with its flexibility and versatility, provides a software protection envelope which continuously verifies the analog RSS with redundant and additional scrams and interlocks. Of course, inside the analog safety related envelope is the core design safety envelope based on the inherent safety of the ***TRIGA*** fuel system. The final envelope of protection is provided by a licensed and highly trained operator using her/his educated judgement and properly written procedures. Any control loops will operate outside the safety and protection envelopes which means that control cannot degrade reactor safety.

The primary indicators of the reactor state are the analog display devices which are hardwired directly from the analog reactor power and temperature instrumentation. In addition, the operator has consolidated information about the reactor state available from the CRT parameter display of the DCC-X computer. As always, the operator will have the final check of the validity of the information by periodically comparing the the analog display devices with the CRT parameter display. Figure 8 is a diagram of the old safety, protection and control system. If figure 7 and figure 8 are compared, the only significant change between the old and the new systems is the addition of the redundant software protection envelope and a CRT parameter display.

❑ **PCMS Is Not A Safety Related System**

In the Regulatory Guide 1.152 [8] methods are described that, if used, promote high functional reliability for safety related systems using programmable digital controller systems in the operation of nuclear power

plants. The methods are applicable for developing software, verifying software, implementing software and validating the system. As defined by the Regulatory Guide, safety related systems are those systems that must "...remain functional during and following a Design Basis Event (DBE) to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shutdown the reactor and maintain it in a safe condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential off site exposures comparable to the 10 CFR Part 100 guidelines." This is essentially same criteria used by the ANSI/ANS 15.15 [1] to define a negligible risk reactor. Using the criteria of the Regulatory Guide 1.152, the PCMS is not a safety related system. Irregardless, the software of the PCMS was developed using an extensive assurance plan (see the section in this appendix, Quality Assurance and Verification and Validation)

- **Present Safety Analysis**

The first accident that was analyzed was the LOCA [see section D, Chpt. IX of reference 9]. The proposed console change will not increase the consequences, the probability of occurrence or decrease the margin of safety of a LOCA.

The second accident that was evaluated was the Maximum Hypothetical Accident (MHA) [see section E, Chpt. IX of reference 9]. This accident assumes that a fuel element ruptures in an air cooled core. The MHA is defined as a postulated accident with potential consequences greater than those from any event that can be mechanistically postulated. The proposed console change will not increase the consequences, probability of occurrence or decrease the margin of safety of the MHA.

The third accident that was analyzed was the Reactivity Accident [see section F, Chpt. IX of reference 9]. In this accident, it is assumed that the reactor is taken to 1.15 MW power level with the transient rod at the lower limit and that the reactor is pulsed with a $3 reactivity insertion. A violation of the PSBR Standard Operating Procedures, a failure of the overpower SCRAMs, a failure of the fuel temperature SCRAM and a failure of the interlocks must all occur simultaneously for this accident scenario to

happen. The conclusion of this analysis is that the final maximum fuel temperature will be less than the safety limit of 1150 ^{o}C.

- **Negligible Risk Reactor**

  The ***TRIGA*** reactor is considered a negligible risk research reactor. A negligible risk research reactor is a "...reactor for which, in the postulated event of the complete failure of the reactor safety system coincident with the occurrence of the most adverse Design Basis Event (DBE), the radiological consequences would be negligible"[1]. A reactor with this classification does not need to meet the single failure design criteria for interlocks and automatic safety shutdowns of the RSS. In any of the accidents analyzed for the PSBR the radiological consequences would be negligible. None of the accidents analyzed, in chapter IX of reference [9], take credit for any safety trips or interlocks; therefore the PSBR can be considered as a negligible risk reactor.

- **Pulse Reactor**

  The ***TRIGA*** reactor is also a pulse reactor which has specially designed fuel elements that allow the reactor to accept large reactivity insertions without exceeding any safety limit. The negative temperature coefficient of the ***TRIGA*** is large and prompt, providing an inherent shutdown mechanism. General Atomics has inserted step positive reactivities of $5.00 without exceeding the fuel temperature limits of the fuel [5].

  The PSBR is a negligible risk reactor but the RSS of the new console is more conservative than ANSI/ANS 15.15 because it meets the single failure design criteria with its operational interlocks and automatic safety shutdowns. PSBR is also a pulse reactor. The staff at the PSBR have performed, over a period of 25 years, more than 6060 pulses of step insertions greater than $1.00 and some as high as $2.75, without exceeding a safety limit or rupturing a single fuel element. By analysis and technical specifications the PSBR is allowed pulses of $3.30.

- **Operations Envelope**

  The operations envelope defines the limits on reactor state. The reactivity accident analysis (see chapter IX of the Safety Analysis Report) shows

there is no credible accident that can exceed the safety limit as long as the accident is initiated while the reactor state is within the operations envelope. The operations envelope is adequately defined by the LCOs , the Limiting Safety System Setting (LSSS) and the High Power Trips, all of which are listed in the technical specifications [9]. The most important function of the PSBR RSS is to assure that the reactor SCRAMs if the reactor state goes outside the operations envelope.

- **Control Rod Motors and Interface**

  The original rod drive motors are single speed, single phase motors. Capacitors are used to obtain the phase shift and the direction of rotation is determined by the phase relation in the stator coils. One failure mode of this type motor is that it drives out at a speed predetermined by the frequency of the supply (60 Hz) and the number of poles in the motor. Also there is no single failure that could cause more than one control rod to drive out at the same time. The speed of the motors and the ratios of the drives were designed such that the maximum up drive rate is ≈ 0.425 in/sec for the transient rod (≈ 35 seconds from full in to full out). This speed, combined with the rod worth, gives a maximum reactivity addition rate of ≈ 14¢/sec for the old control system when the transient rod is in the middle of travel. This value is below the present technical specification limit of 17¢/sec [9].

  It was desirable to make changes to the rod drive motors along with the upgrade of the console for several reasons. In the original system there are three different motors for the four rods which required the stocking of three different motors for spares. The regulating rod motor is no longer being made which causes difficulties in obtaining replacement parts. Variable speed motors with both velocity and position control provides many more options for control. The ability to control several control rods as a bank was considered desirable for normal automatic control and necessary for a useful square wave mode.

  The maximum speed of the motors, in either direction, is set by jumper position (a choice between 1.5 rps and 4.5 rps). The actual speed is controlled by an analog velocity demand signal from the DCC-X. This

voltage signal can vary from -10 Vdc to +10 Vdc with the extremes demanding the maximum speed in either direction. The control system is tuned to place limits on the maximum up drive speed when moving individual rods. Those limits are restricted further when banked rod control is used to reduce the reactivity addition rate by the appropriate factor.

As is usually the case, an increase in versatility also increases the complexity of the system and the number of modes of failure. The motors are not part of the safety system (they are not required to function during or after a DBE) but they introduce a failure mode that must be analyzed to ensure that there is not an unreviewed safety question. Since the motors are variable speed there is a remote possibility that there could be a failure such that a control rod is driven out at maximum speed. There even may be a remote possibility that more than one control rod may be driven out at maximum speed. This would be a ramp accident.

A ramp accident would not render the RSS nonfunctional since the RSS does not depend on the motors being operational. The analysis must show that if the RSS is functional and a ramp accident occurs there is no unreviewed safety question.

Due to the design of the system, both hardware and software, it is not credible that one motor will fail in a nonconservative manner let alone more than one. In figure 9 a typical motor interface is illustrated. There is only one DCC-X computer and two I/O chassis but there are four separate controller/motor combinations, each with their own DOs, AIs, AO and serial link. The signals for each motor are distributed between the two I/O chassis and the many I/O cards so that no one failure in a chassis or single card will disable all of the signals.

The design manual [23] fully describes the motor interface. Before the motor provides torque, the MRDY (motor ready) and SVON (servo on) inputs to the controller must both be true (closed contacts). These two inputs are wired directly to DCC-X digital outputs. Both DOs are set true if DCC-X is healthy, its watchdog is energized and motor trouble is not detected. Otherwise, motor torque will be lost and rods connected to the

rack and pinion type drives will likely fail. Motor trouble is detected if any of the following conditions becomes true:

- a drive alarm occurs (AL01 or AL02)
- drive ready (DRDY) is false
- An error in serial link communications between the motor and
- DCC-X is detected.

The velocity signal analog outputs from DCC-X to the motor controllers of the four rods is validated. This is accomplished by feeding the speed request analog output to the controllers back as an analog input to the computer (see figure 9). The software continuously compares the feedback signal to the requested output value. Validation failure results in a PCMS SCRAM request.

The analog speed signal from the motor controllers is read by the DCC-X computer and a SCRAM occurs if the motor overspeed trip point is exceeded (see figure 4). An overspeed trip results in a PCMS SCRAM request.

A representative of NSK/ Motornetics Corporation [24] indicated that if the motor/controller does fail it will probably fail in one of two modes. Either all 3 phases would lose power, causing a loss of torque to the motor, or 1 or 2 phases would lose power and cause the motor to lock up. In the first mode of failure, if the motor is connected to the safety, shim or the regulating rod, the rod will drift into the core by gravity. The transient rod with its ball nut/threaded cylinder drive would remain stationary. In the second mode of failure the control rod would be locked in position. Both of these failure modes are conservative. If the motor/controller did fail in a third mode that caused it to drive the control rod out at maximum speed, the overspeed trip would cause a SCRAM (if the velocity signal out of the controller was valid). It would not be credible for more than one motor/controller to fail in this third mode concurrently.

It may be theorized that the PCMS could fail in such a way that:

1. More than one rod is demanded to drive out at maximum speed (which is greater than the set point in the software),

2. The demand validation software logic fails in exactly the way necessary such that there is no validation failure SCRAM,
3. The overspeed trip software fails in exactly the way necessary such that there is no trip and
4. These failures of software do not cause a failure of software self checks and subsequent PCMS SCRAM or watchdog SCRAM.

Due to the modular structure of the software logic (the velocity demand module is separate from the validation module which is separate from the overspeed trip module) and extensive self checks (which is in a separate module from the others), it is not credible that all of the above failures would happen concurrently.

However, even if an accident were to occur causing three control rods to drive out at maximum speed, the RSS and the design safety of the ***TRIGA*** fuel will limit and terminate the ramp before the safety limit is reached.

- **$5 Ramp Analysis**

The $5 ramp analysis was performed for AFRRI by General Atomics [7]. It indicated that even with a reactivity addition rate of $2.50/second, averaged over full control rod travel, the safety limit (1150 °C) was not reached. The rod withdrawal was terminated with a high power scram less than 1 second into the event. A reactivity of $1.86 was added after criticality was achieved and before the SCRAM occurred. The maximum power in the transient was 330 MW with a maximum fuel temperature of 330 °C. Compared to the maximum licensed pulse this excursion is inconsequential. It should be noted that the amount of reactivity available in the ramping rods does not impact on the final result as long as the reactivity addition rate does not exceed the $2.50/second rate, averaged over full control rod travel, and the SCRAM time is consistent with that analyzed. There are several factors that would come into play with the new console which may further reduce the effect of a similar transient at PSBR.

- **SCRAM Time**

  The SCRAM time is defined as the time interval from the time that the safety channel sees the parameter reach the trip set point until the control rods are fully in the core from fully out of the core. General Atomics used a one second SCRAM time in their analysis. The technical specifications [9] allo[illegible] maximum SCRAM time of one second but typically the maximum measured SCRAM time is ≈500 msec. A shorter SCRAM time would help reduce the energy produced in the event.

- **Scram Activity**

  The present technical specifications [9] allows a maximum core excess of $7.00. With that amount of core excess the critical control rod positions are at $5.65 withdrawn. If this transient were to occur at the PSBR, the total scram activity would be greater ($7.51 vs. $5.87 (reference 7) assuming that the same withdrawal beyond criticality ($1.86 as in reference 7) occurs) than that of the analyzed case. This would reduce power more rapidly after the scram occurs and lower the energy and subsequent fuel temperature peak.

- **Maximum Reactivity Addition Rate**

  The minimum withdrawal time of the safety, shim and regulating rod is full withdrawal in 4.77 seconds (set by jumper to 1.5 rps) with any hypothetical DCC-X hardware or software failure (The software limit is tunable but is typically set for a minimum withdrawal time of ≈ 20 seconds). Since the PCMS can be configured in 1, 2 or 3 rod automatic mode using these three control rods (the maximum speed is further reduced by software limits to account for the additive rod worths), and if a ramp accident did occur with more than one control rod, it would most likely be a combination of those three control rods. With these three rods the maximum average reactivity addition rate, with rod worths at the maximum allowed by technical specifications [9], would be less than $2.00/ second. The $5 ramp accident was analyzed using typical rod worth curves but the $2.50/sec reactivity addition rate was the average value during the duration of the accident. A lower average reactivity addition rate would reduce the consequences of the accident.

❑ **Environmental Qualification**

The RSS and PCMS components are located in the reactor bay and control room which is air conditioned to control temperature and humidity. The cooling air supplied to the console equipment is pulled from the reactor bay after further filtering. All of the equipment is designed to function in this type or harsher environment. The environment will not cause accelerated failure of equipment.

❑ **Seismic Considerations**

All of the equipment is mounted in high quality industrial racks and console. There should not be any significant movement if a seismic event occurs of the magnitude expected in this location. With a ***TRIGA*** reactor a SCRAM occurs with the removal of power to the rod magnets in the case of the safety, shim and regulating rods and solenoid valve in the case of the transient rod. The rods drop to their most negative reactive state by gravity and do not require any other equipment to maintain the reactor in the shutdown state. The RSS SCRAM circuits are designed to SCRAM on failure (which includes relay chatter) therefore a seismic event will not cause an unsafe failure of the RSS.

❑ **Surge Withstand Capability (SWC)**

Surge protectors are on exclusive electrical power feeds to console. Surge protectors are on the individual power distribution supplies within the console. In addition there is surge protection on individual components of the console. There is also surge protection on the individual I/O boards (see EMI section).

❑ **Electromagnetic Interference (EMI)**

All signal cabling is shielded and where possible the signal cabling is separated from power supply cabling or any other cabling which may induce EMI into the instrumentation or equipment. The power supply is filtered for high frequency EMI.

The DCC-X I/O card arrangement has been chosen to minimize signal noise by separating the digital outputs from the analog inputs. The analog

inputs and outputs are all voltage signals using a 10 V range, where possible, to minimize the effect of signal noise pick up.

Two types of analog input signal conditioning (gate) cards are used: transformer coupled and solid-state each providing 8 differential voltage inputs. The card selection is based on meeting appropriate filtering, sampling rate and SWC for the input signals.

The solid state gate card is unfiltered at its input and is used only for the gamma ion chamber pulse range signal. The pulse range signal is sampled at approximately 3000 samples per second during a pulse which is well within the card and analog to digital converter capability. This card can withstand a maximum of +/- 11 Vdc differential plus +/- 11 Vdc common mode on the input signals. This should be adequate considering that the pulse range signal is only routed within the console.

The transformer coupled cards are used for all inputs other than the pulse range gamma ion chamber signal. All inputs have a double pole filter (-6 db @ 14 Hz). The maximum sampling rate used for the transformer coupled signals is about 10 Hz. This card can withstand a maximum of +/- 25 Vdc differential plus +/- 400 Vdc common mode on the input signals.

The digital input card used provides for 16 optically isolated inputs. The card is jumper configured to sense the state of contacts wired across the input terminals with a closed contact being read as "true" in software. An external 24 Vdc power supply is used for contact sensing, resulting in a current of 4.4 mA through the contact when closed. A current level below 0.95 mA will read as an open contact. The 24 Vdc power is supplied to terminals on each I/O chassis which then supplies the digital input cards via the backplane. A maximum of 38 V is tolerable on the input terminals. The input signals are filtered with a 5 msec time constant.

The digital output card provides for 16 relay outputs. The relay contacts are mercury wetted having maximum ratings of 2 A, 200 V and 50 W. The contacts close within 2 msec. An external power supply of 12 Vdc is

required for the relay coils. This is supplied through the front edge connectors of the cards.

All analog outputs from the Wide Range Monitor and the Power Range Monitor are isolated with analog optical isolators. The digital outputs are all relay contacts.

The design and the construction of the console and equipment minimize the susceptibility of the system to EMI. The effect of EMI, at worst, will cause a SCRAM, which is a safe failure.

- **Loss of Power**

  A loss of power will cause the control rods to drop into the core in their most negative reactive state by gravity. DCC-X and DCC-Z will automatically reboot in ***DOS*** and will require operator action to restart the PCMS software. The control rod motor controllers have essential parameter information protected by battery backed RAM and they will automatically reboot when power is regained. If the battery fails there will be a motor trouble signal issued. This will cause a validation failure during operation or when the PCMS is restarted after a loss of power and the motor cannot provide torque. A loss of power to any motor controller will cause a motor trouble signal, a validation failure and a loss of motor torque.

  A loss of power to Wide Range Monitor and Power Range Monitor instruments will cause a loss of an operative signal and an immediate RSS SCRAM. A loss of HV detector bias to either instrument will also cause a loss of an operative signal and an immediate RSS SCRAM. If one of the calibration pushbuttons is pushed (inserting a calibration source) the operative signal is lost and an immediate RSS SCRAM occurs. The PCMS also monitors the operative signals and will request a SCRAM if the operative signal goes low.

- **Failure Modes and Effects**

  A Failure Mode and Effects Analysis, FMEA, of the RSS was performed by AECL as part of the contract to construct the new console [6]. The FMEA

was actually performed by R. Henderson of AECL, Montreal Operations which is independent of the AECL, Mississauga Operations and Gamma Metrics, San Diego, CA the constructors of the PCMS and RSS respectively. It was independently reviewed by D. Burjourjee of AECL, Mississauga Operations and approved by G. Raiskums of AECL, Mississauga Operations and D. Hughes of the Pennsylvania State University.

The conclusion of the FMEA is that "*...no single failure will prevent a reactor SCRAM or desirable interlock. Although, certain failures may impair a particular trip there is always an alternative trip parameter available to initiate a SCRAM*" [reference 6, page 17].

In any of the accidents analyzed for the PSBR, the radiological consequences would be negligible. None of the accidents analyzed take credit for any safety trips or interlocks; therefore, the PSBR can be considered as a negligible risk reactor. PSBR is a negligible risk reactor but the RSS is more conservative than the standard [1] because it meets the single failure design criteria with its operational interlocks and automatic safety shutdowns.

- **Reliability**

  The equipment used is commercial or higher quality and has a high degree of reliability. The RSS equipment quality is at least as good as that of the original TRIGA console and should be as safe and reliable. The operation of the PSBR is not so critical that shutdown for repair cannot be tolerated, however critical spare parts are being obtained to reduce the down time if a failure occurs.

- **Error Detection**

  The error detection of the new system greatly exceeds that of the old system. The PCMS utilizes extensive startup and continuous self checks on the computers. In addition, the PCMS performs validation checks on the SCRAMs of the RSS and operational interlocks, and issues SCRAMs for conditions other than those required by the technical specifications [9]. The PCMS also performs a power spread check between the Wide Range FC

and the Power Range GIC and will request a DCC-X SCRAM on failure. Even though failure of the PCMS will not cause an unsafe condition it is desirable that a SCRAM occur and repair initiated. To that end a watchdog circuit was incorporated in DCC-X. At most ≈1.7 seconds will pass before a SCRAM occurs if any condition prevents resetting the watchdog timer. In some cases the time before SCRAM will be much less. If the DCC-X detects a fatal failure in its self checks it will request a SCRAM immediately rather than wait for the time out. A watchdog SCRAM cannot be reset unless the failure is corrected and the software is rebooted by an authorized operator.

- **Independence of the RSS from PCMS**

  Figure 10 illustrates the communication that does exist from the PCMS to the RSS. This communication is necessary because the PCMS determines the mode of operation and that must be sent to the RSS to bypass the High Power SCRAMs during pulse mode and reinstated them after the completion of pulse mode. The hardwired operational interlocks that are in effect is also determined by the mode communicated from the PCMS.

  The interface is designed to reduce the probability that a single failure will allow operation in a mode other than pulse without high power SCRAMs. The DOs that signal the RSS to bypass and the DIs that feedback the status of the high power SCRAMs are located on separate I/O cards. (The Wide Range Monitor communications is with I/O chassis #1 and Power Range Monitor communications is with I/O chassis #2.) If only one chassis fails, only one bypass will fail. In addition, if one card fails the validation will fail. All of these failures will cause a self check failure and subsequent PCMS SCRAM and/or watchdog SCRAM of the reactor. If the DCC-X computer fails such that both DO contacts close, both high power SCRAMs will be bypassed (the high fuel temperature SCRAM will still be functional). The RSS causes a hardwired light on the Console SCRAM and Alarm Panel to light indicating "High Power SCRAMs Bypassed". Such a failure of the DCC-X would cause a self check failure and subsequent PCMS SCRAM and/or watchdog SCRAM of the reactor.

It would require more than one failure as well as reactor operator error to operate the reactor with the high power SCRAMs bypassed on the new console. This is no different than on the original ***TRIGA*** console where a single failure plus an operator error could allow operation of the reactor. Even though the PCMS does communicate with the RSS there is sufficient redundancy, diversity and independence to protect the public.

- **Independence of DCC-X from DCC-Z**

  The communication between the DCC-X and DCC-Z is one way. The data link has no handshaking. A error checking system called CRC is used to maintain the integrity of the data. It is not possible to compromise the DCC-X through DCC-Z.

- **Redundancy and Diversity**

  The High Power SCRAMs are provided by the Wide Range and the Power Range instruments. The former is a FC system and the latter is a GIC system. Neither system has embedded microprocessors. These two instruments provide the redundancy and diversity required for safe operation. This arrangement is similar to the original ***TRIGA*** console which used the Linear CIC system and the Percent Power GIC system to provide the High Power SCRAMs. In the RSS only one fuel TC is monitored to provide a High Fuel Temperature SCRAM. The PCMS monitors two TCs to provide a DCC-X SCRAM request if the setpoints are exceeded. The RSS is no different from the original ***TRIGA*** console which also monitored only one TC to provide the LSS SCRAM. The High Power SCRAMs are considered to provide redundancy and diversity for the High Fuel Temperature SCRAM and vise versa.

- **Software Assessment**

  The health and safety of the public is protected by hardwired systems in the new console in the same way it was accomplished in the original ***TRIGA*** console. Failure of the software of the PCMS is not an unsafe failure by the safety related definition in reference [8]. Reliable and precise operation is desirable and extensive verification and validation was used to assure it. The quality assurance, verification and validation,

maintenance and control measures that have been or will be implemented will assure that the new console is a safe and reliable system.

- **Quality Assurance and Verification and Validation**

The specification, design, construction, installation and testing of the new console is an elaborate process that is not yet complete.

The bid specifications [10] for the new console were written by the staff of PSBR utilizing public information about the General Atomics digital console, AFRRI new console specifications, an AECL proposal, PSBR technical specifications and conversations with personnel in the nonpower reactor community. The bid specification was utilized by the bidders to propose designs and bids that were evaluated by committee of PSBR personnel and Penn State faculty. AECL Technologies, Rockville, MD, was the successful bidder.

The next step was a meeting to negotiate a contract which specified any changes (additions and exceptions) to the bid specifications.

AECL then documented the design requirements [11] [12] & [13] which were approved by PSBR staff. Any changes to the design requirements, however initiated were approved by AECL and PSBR. Design drawings were also reviewed by PSBR.

A final acceptance test (FAT) was outlined by AECL and approved by PSBR. The FAT was written by AECL, approved by PSBR and performed by PSBR and AECL staff with the review of AECL quality assurance personnel. The FAT tested all hardware and software for functionality and compliance with all previously approved documentation. Any discrepancies or changes were recorded. In particular, software bugs or changes were recorded on software change request (SCR) forms which are part of AECL's QA accounting system. After the FAT the disposition of the changes were recorded. Any software tests were done according to AECL's test procedure, again tested by PSBR and the software version was frozen.

After the system was delivered, PSBR performed a site acceptance test (SAT) to assure that the delivered system was functional. In addition, tests were performed in the SAT that were not possible at AECL (ie tracking reactor power with the Wide Range and Power Range Monitors). Any discrepancies discovered were recorded on SCR forms and sent to AECL to be changed, tested and implemented.

For this project the AECL QA and V&V was integrated with PSBR review and testing. The process has assured a very well designed and reliable system.

- **Software Maintenance and Control**

  Maintenance Plan

  The new Console is an advanced system composed of both hardware and software components. Although the system is highly reliable because of the design and exhaustive testing it may periodically require some modification to repair a deficiency or enhance system performance. This repair, whether it is mechanical, electrical or software, must be performed in a methodical and reliable manner. PSBR will have a maintenance plan to provide the operating staff with a means by which system maintenance will be performed.

  A detailed maintenance manual [14] written by the original contractor, AECL, was provided as part of the original documentation. This manual details all mechanical and electrical maintenance that the contractor considered advisable. Additionally, it covers system I/O calibration and diagnostic maintenance that needs to be performed. This diagnostic/calibration maintenance will be performed by qualified personnel utilizing a software package that runs off line and will be performed at an appropriate frequency. This manual and other equipment maintenance manuals [16, 18, 19, & 22] will be used as a guideline and will be incorporated, as needed, into any procedures that are presently in effect that will be used with the new console.

Software Assurance/Maintenance Plan

Due to the complexity and criticality of the protection, control and monitoring software in DCC-X and the monitoring and historical data storage software used in DCC-Z, it is imperative that a Software Assurance/Maintenance Plan, SA/M, be implemented to ensure system software integrity. A SA/M will be designed and implemented not only to ensure system integrity but also to repair any software deficiencies that were not detected nor corrected during the initial testing of the system. In addition, it will cover any changes or enhancements that may be desirable to compensate for environmental changes or tc improve system performance. The SA/M Plan will be implemented through Administrative Procedures designed to identify, track and verify any software changes. Additionally, concerns about software security will be addressed.

Software Code Control

Software version control initially will be controlled by the contractor, AECL. This is due to their unique capability to generate the executable files and the I/O files necessary to run a PROTROL control system. This capability was not part of the original contract though it may be purchased at a later date. Until a PROTROL SYSGEN package is purchased and PSBR version control is implemented, it is desirable for AECL to maintain version control through the use of a software package that they presently employ in all their software revisions.

Physical Media Control

The software media (diskettes) that AECL provides to the reactor facility will be housed in a secured office or a vault located in the facility. Media backups will be provided by AECL in the eventuality of a diskette failure.

Access Authorization and Control

Access control is provided by two levels of password protection in the control system software. The first level is utilized by the system manager in controlling the level one password which allows only authorized personnel access to the maintenance/tuning level. The second level allows an authorized individual to change tuning parameters in each control block. Personnel having senior reactor operator licenses will have access to the

maintenance and tuning level. Only the Director, Operations Supervisor and the Engineering Manager will have access to level one. Both password protection levels have a timeout feature to prevent inadvertent access to unauthorized persons. Although SROs will have access to the tuning menu in the control system only authorized changes to tuning parameters will be permitted. This will be implemented through administrative procedure and controlled with a software change request (SCR) similar to those used by the manufacturer. Additional hardware safeguards will be installed to prevent system use for anything but reactor control (ie. disk locks). This will also protect the system from viruses that sometimes can cause severe consequences if not detected immediately.

Software Change Request

This form will allow management to track all software changes from its origination to completion in a reliable and consistent manner. The request will have the following information:

1. Description of the problem and a proposed corrective action,
2. Authorization to implement the change,
3. Listing of all items and systems expected to be affected by this change,
4. Estimate of the resources needed to complete the change,
5. Identification of personnel involved in the origination and disposition of the change,
6. Identification number and date initiated,
7. Date resolved and personnel completing the change and
8. Means of testing the change.

This information will allow management to resolve all change requests and verify that each was completed in a concise and accurate manner, that all appropriate documentation was updated and testing was completed.

Software Maintenance

Periodically maintenance will be performed on the system software to verify the correct version of software is installed and that all tuning parameters are correct. This will be implemented at an appropriate frequency with a Checks and Calibration Procedure. This procedure will also be implemented if unexpected system failures occur. A log of all

software changes will be maintained by the system manager. This log will be a written or electronic log and will help maintain system integrity through proper documentation.

Self Checks

Extensive self testing by the PCMS as described in the design manual [23] further assures a safe and reliable system.

References

[1] ANSI/ANS-15.15-1978, *American National Standard Criteria for the Reactor Safety Systems of Research Reactors*, American Nuclear Society.

[2] ANSI/IEEE-ANS-7-4.3.2-1982, *Application Criteria for Programmable Digital Computer Systems of Nuclear Power Generating Stations*, American Nuclear Society, 1982.

[3] Bryant, J. L., Wilburn, N. P., *Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry*, NUREG/CR-4640, U.S. Nuclear Regulatory Commission, p 2.1, Aug 1987.

[4] Code of Federal Regulations10 Part 50.59, U. S. Government Printing Office, Nov 30, 1988.

[5] Coffer, C. O., Shoptaugh, JR., J. R., and Whittemore, W. L., *Stability of U-ZrH$_{1.7}$ TRIGA Fuel Subjected to Large Reactivity Insertions*, General Atomics Publication GA-6874, Jan 1966.

[6] *Failure Mode and Effects Analysis*, prepared by R. Henderson, reviewed by D. Burjorjee, and approved by G. Raiskums and D. Hughes, AECL Document FMA-17-60501-001, Rev. 0

[7] General Atomics, *Analysis of 5 Dollar Ramp Insertion over 2 Second I nterval in AFRRI TRIGA™ Reactor*,General Atomics Publication of work performed for Armed Forces Radiobiological Research Institute, Bethesda, Maryland, April, 1988.

[8] Regulatory Guide 1.152, *Criteria for Programmable Digital System Software in Safety-Related Systems of Nuclear Power Plants*, U. S. Nuclear Regulatory Commission, Nov 1985.

[9] Safety Analysis Report for the Pennsylvania State University Breazeale Reactor, Facility Operating License R-2, Docket No. 50-005, Amendment No. 23, March 1985.

[10] PSBR Console Specifications, Printed by PSU 88 Oct 27.

[11] DR-17-60501-001, Design Requirements, Reactor Safety System.

[12] DR-17-60501-002, Design Requirements, Control and Monitoring System.

[13] DR-17-60501-003, Design Requirements, Console Layout and Operator Interface.

[14] MM-17-60501-001, Maintenance Manual, PSBR CSS Upgrade, Control and Monitoring System.

[15] NUREG-0700, Guidelines for Control Room Design Reviews, 1981 September.

[16] MM-17-60501-004, Maintenance Manual, Gamma-Metrics Instruction Manual (#158), Reactor Control Console for Penn State University.

[17] OM-17-60501-001, Operating Manual, Control and Safety System.

[18] MM-17-60501-002, Maintenance Manual, Transduction Computers.

[19] MM-17-60501-005, Maintenance Manual, NSK ***Megatorque*** Motor System User's Manual.

[20] RM-17-69020-001, Reference Manual, ***PROTROL*** Advanced Control Block Language: Control Designer's Reference Manual.

[21] TR-17-60501-001, Test Report, Reactor Safety System (Filled-Out copy of G-M Dwg #040264).

[22] MM-17-60501-003, Maintenance Manual, Computer Products I/O Hardware.

[23] DM-17-60501-001, Design Manual, Control and Safety System.

[24] Telephone Communications with Mr. Long of NSK/Motornetics Corporation, March 8, 1991.

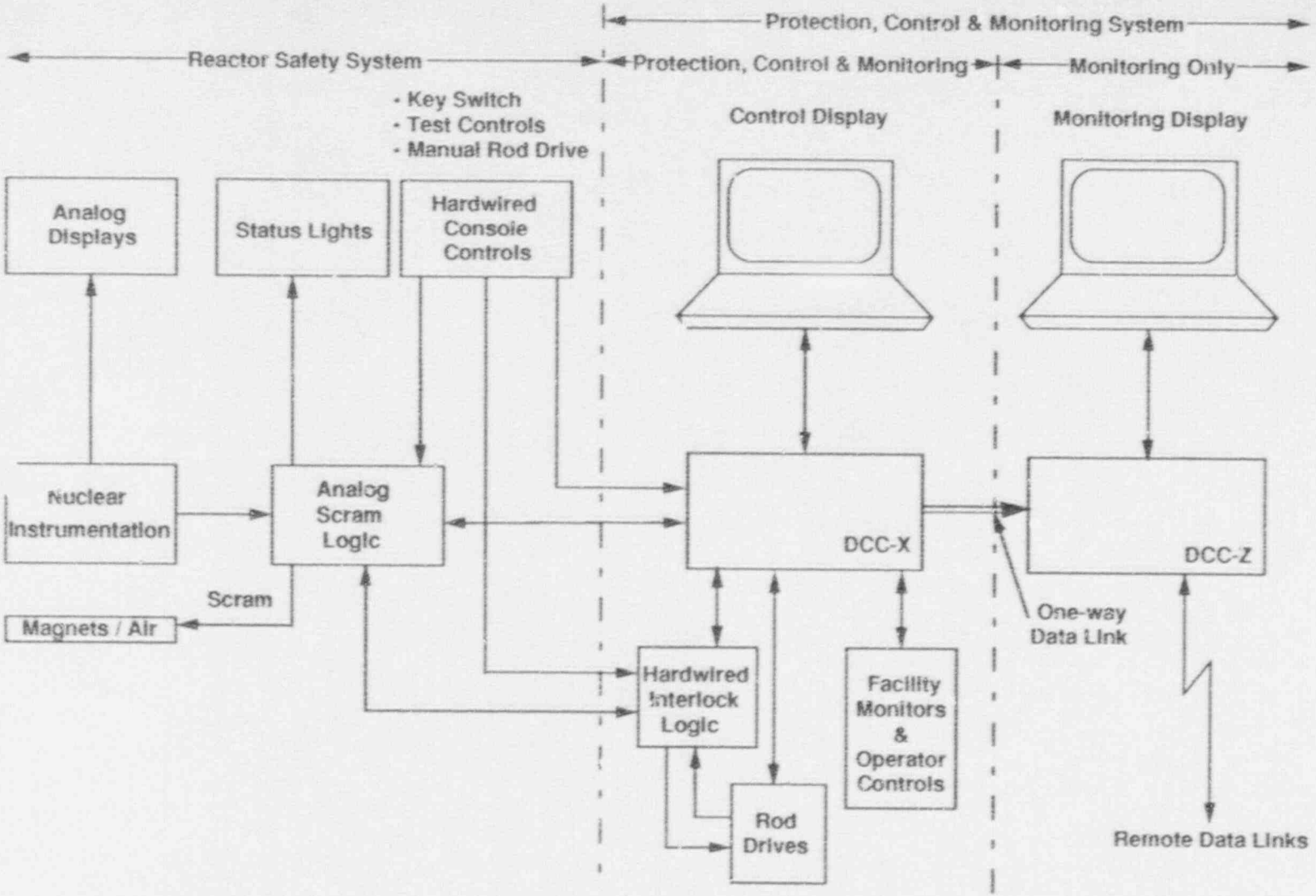


Figure 1 RSS & PCMS

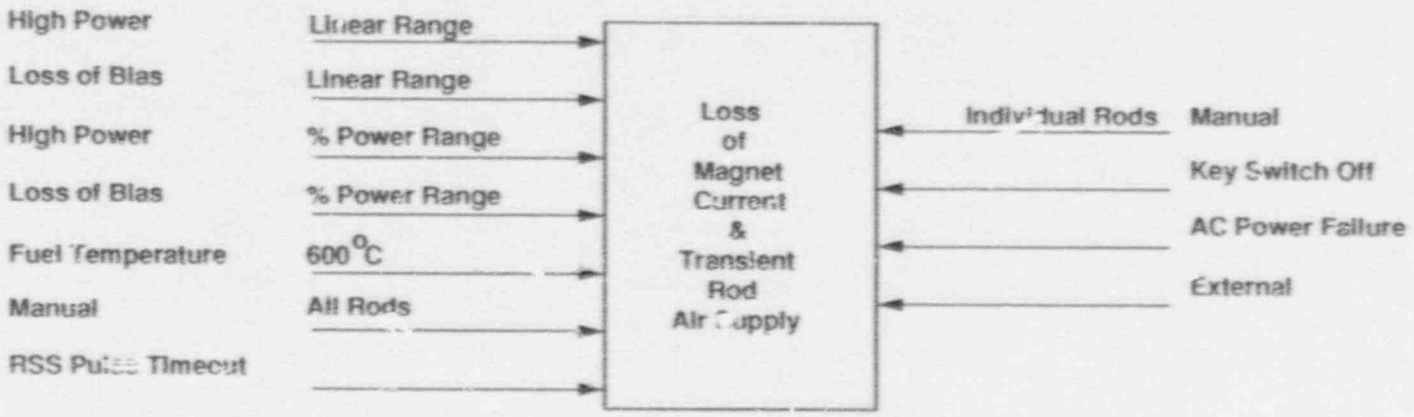


Figure 2 Old Console SCRAMs

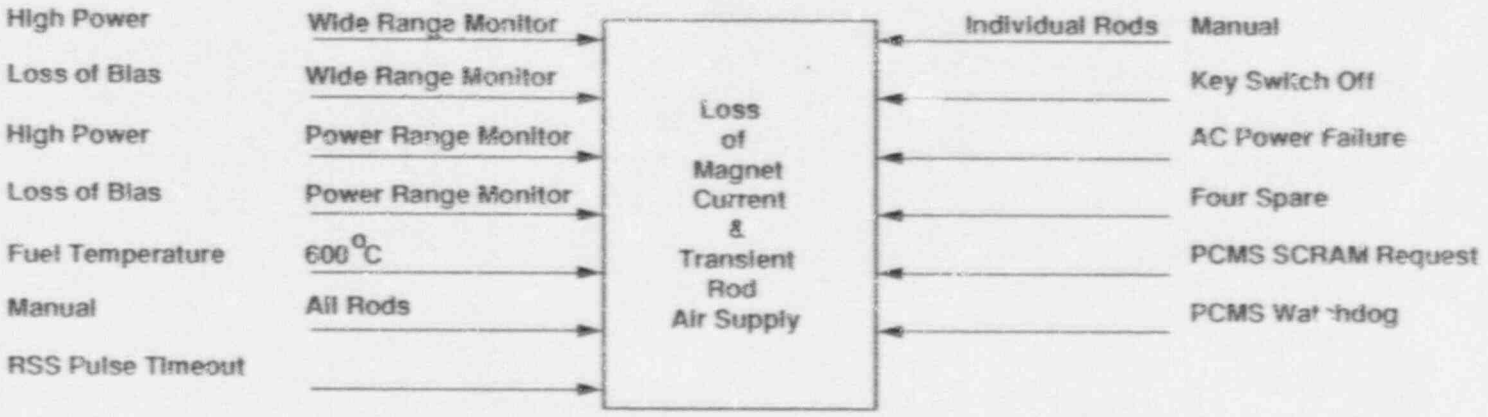


Figure 3 New Console SCRAMs

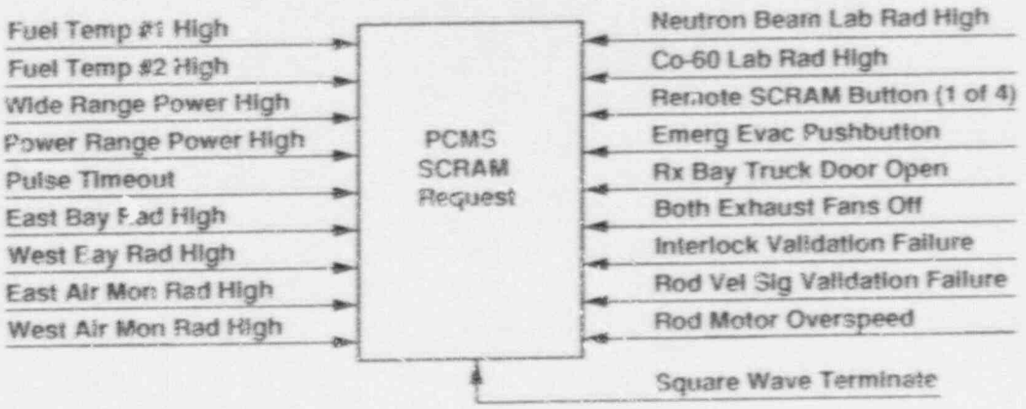


Figure 4 PCMS SCRAMs

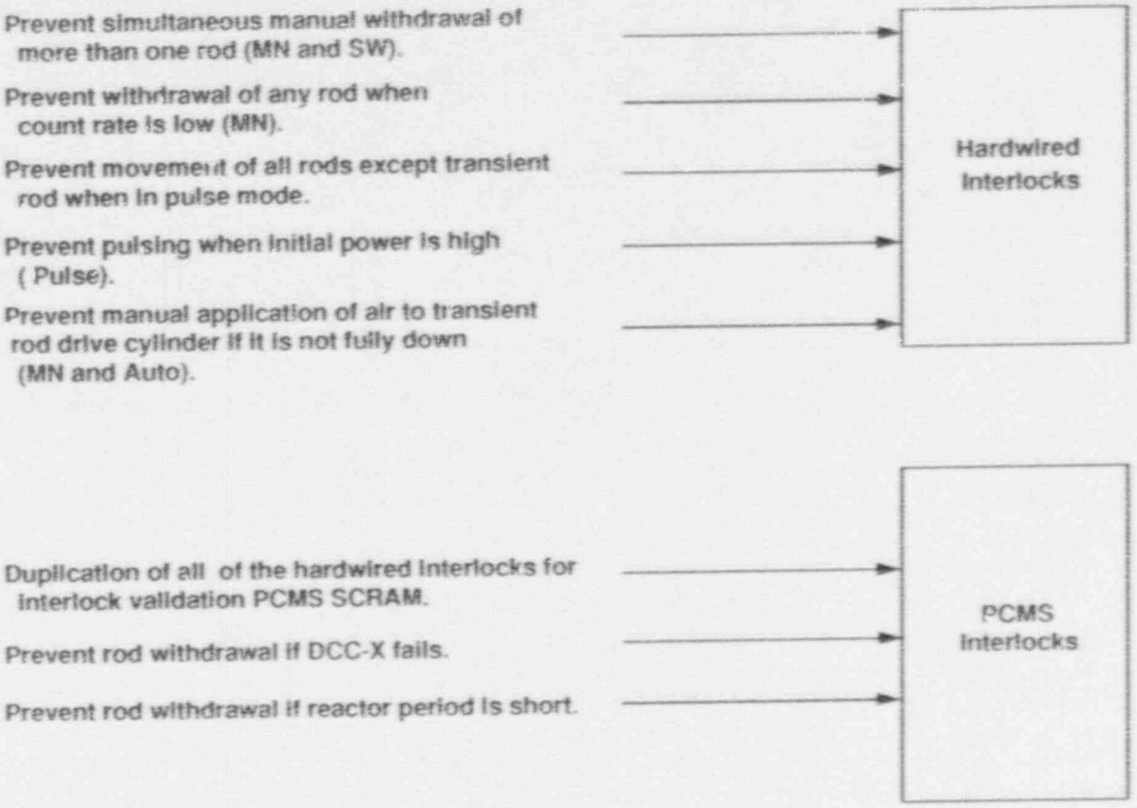


Figure 5 New Console Interlocks

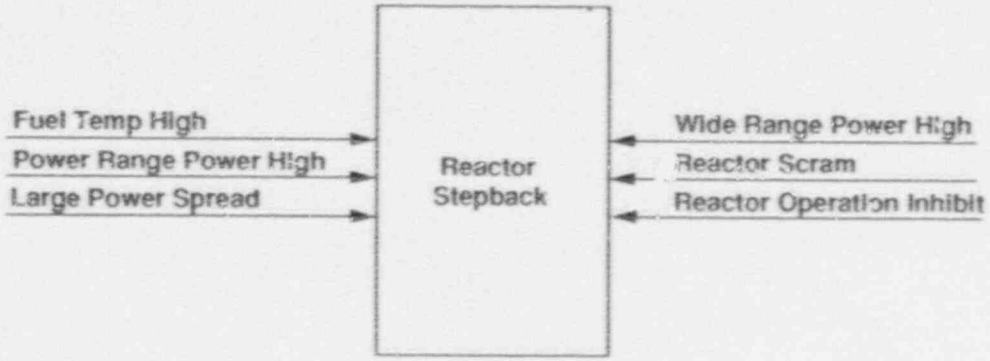


Figure 6 PCMS Stepbacks

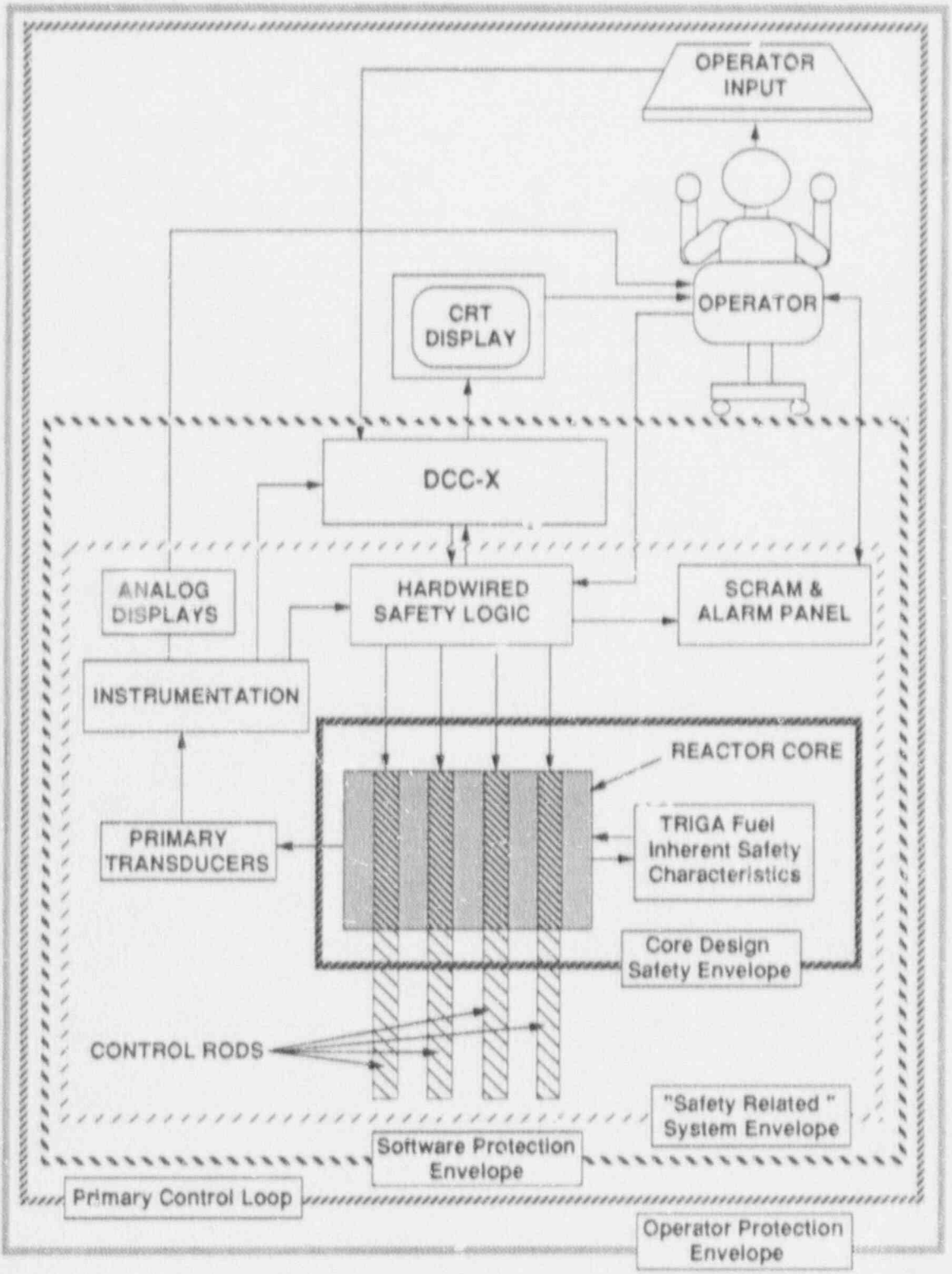


Figure 7 New PSBR Safety, Protection and Control System

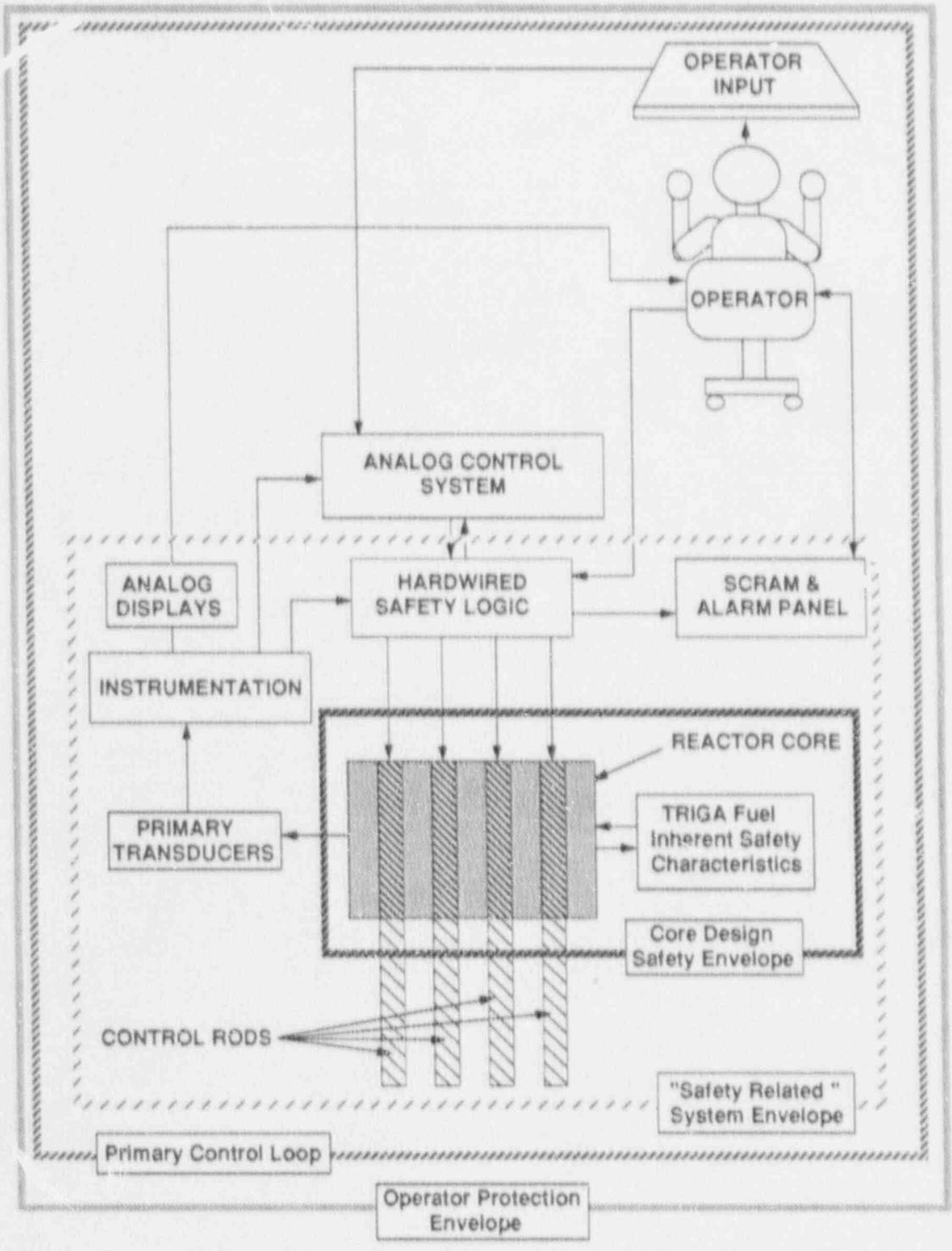


Figure 8 Old PSBR Safety, Protection and Control System

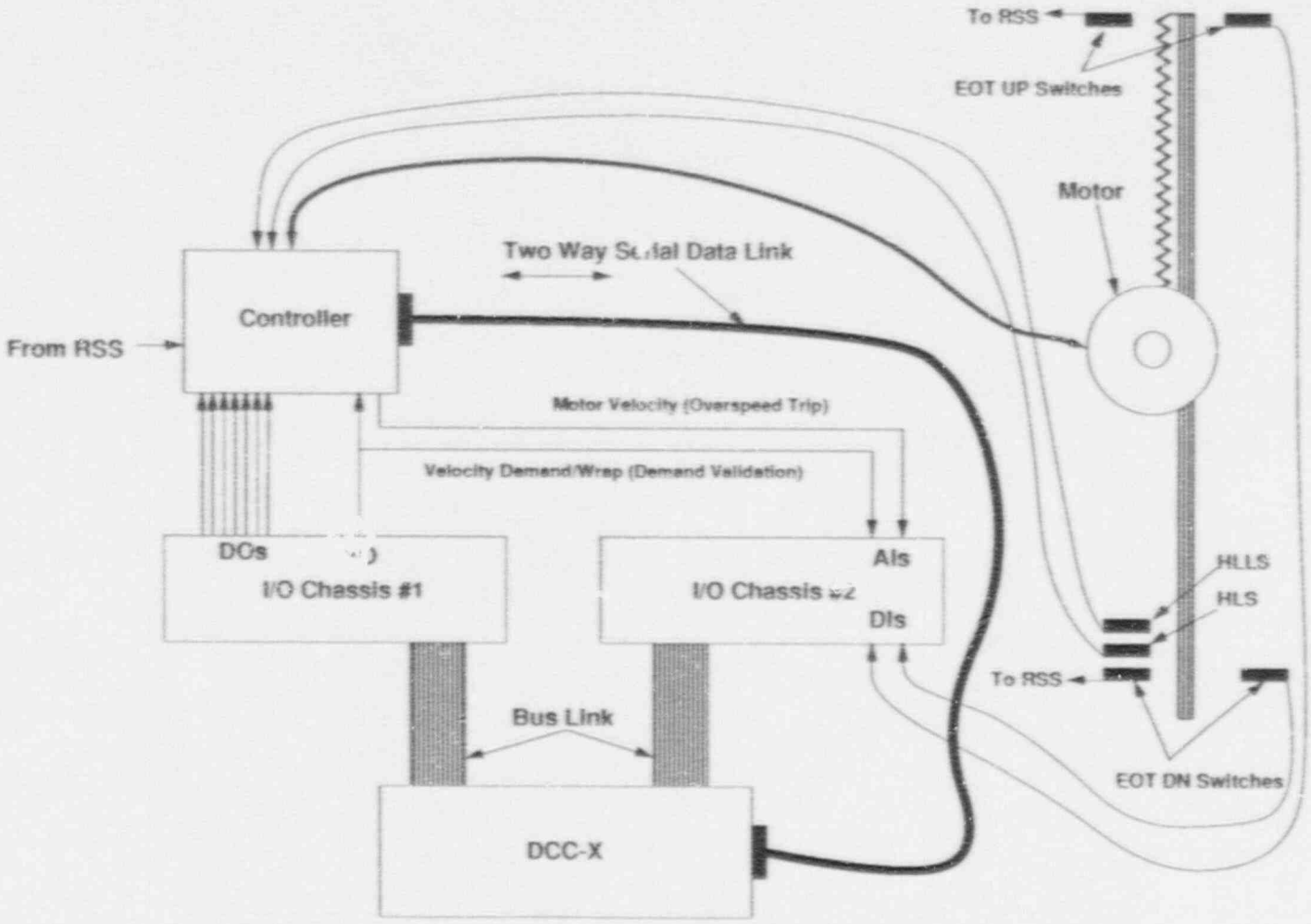


Figure 9 Typical Motor Interface

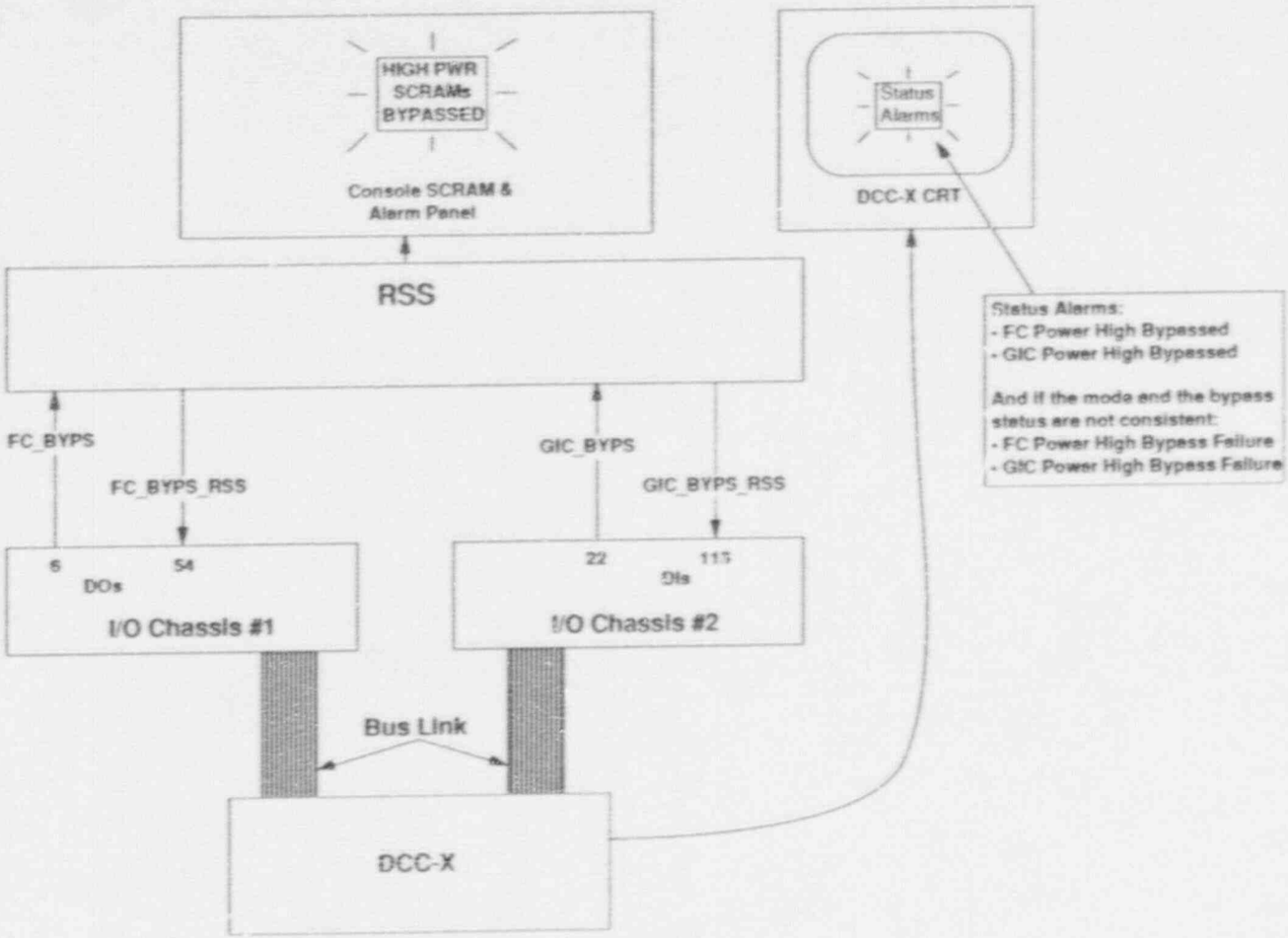


Figure 10 DCC-X to RSS Interface

Appendix C

INSTALLATION PLAN

This plan is written in order that the installation of the new console will be as efficient as possible. It will be coordinated with the biennial fuel inspection which is due in the spring. The following is the proposed sequence of events. The installation will take place utilizing an approved procedure which will be much more detailed than this plan which only covers the major steps.

It is assumed that certain tasks have already been completed. The first is that the amendment has been approved by the NRC and that the Penn State Safeguards Committee has approved the installation. Second the training of the staff must be on schedule to ensure that there will be qualified ROs and SROs to operate the console after the installation. Third the documentation, maintenance procedures, checks and calibration procedures, CCPs and standard operation procedures, SOPs, must be completed to the point that the installation, testing and operation can proceed safely.

- ❑ **INITIAL THERMAL POWER CALIBRATION**
  The initial thermal power calibration must be done to assure that the installation starts from a known calibration. Use CCP-3, CCP-7 and CCP-2 as appropriate to complete this task.

- ❑ **INSTALL AND CALIBRATE REFERENCE POWER INSTRUMENTS**
  The reference instruments can be the present fission chamber for count rate indication and the linear CIC for the wide range indication. In addition the fission chamber from the new console Wide Range Monitor should be permanently attached on the tower, if possible, and calibrated for reference. Determine the critical rod positions, CRP, by measuring the absolute rod positions while the reactor is critical at a low power (i.e. 50 watts).

- ❑ **UNLOAD THE CORE**
  Use SOP-3 to unload the core to allow the removal of the control rods. The fuel inspection, using CCP-16, may be performed after this unloading is complete. Some elements may have to remain in the core to prevent disturbing the reference power instruments. They can be inspected after the installation is complete.

- ❑ **REMOVE AND ADAPT THE CONTROL ROD DRIVES**
  This task will be performed by engineering st[illegible]s much of this as possible should be completed prior to the beginning of the installation.

- ❑ **REMOVE THE CONTROL RODS**
  CCP-17 may be used to inspect the control rods after they are removed.

- ❑ **REMO[illegible] OLD CONSOLE**
  This t[illegible]o involve the transfer of the radiation monitors to their new location, [illegible]xiliary instrumentation rack. The window and part of the wall will also have to be removed.

- ❑ **INSTALL THE NEW CONSOLE**
  This task involves the placing of the console, mounting of auxiliary equipment, installing the forced ventilation, running wiring, installing sensors or hooking up the existing sensors and providing power to the equipment.

- ❑ **INSTALL THE CONTROL RODS**

- ❑ **INSTALL THE DRIVES WITH THE NEW MOTORS**

- ❑ **TEST THE NEW CONSOLE AND DRIVES**
  This task consists of the testing of all wiring and sensors, powering up of all equipment, testing of all I/O, calibration of instrumentation, and performance of a modified SAT to assure that all is working as expected. The motors should also be tested at this time. CCP-1, CCP-3, CCP-4 and SOP-2 shall be performed.

- ❑ **READINESS REVIEW**
  Readiness review shall be performed by a subcommittee appointed by Safeguards Committee. The review is to assure the Safeguards Committee that all is ready to proceed with the loading of the core and begin post installation testing.

- ❑ **LOAD THE CORE WITH AN APPROACH TO CRITICAL**
  This approach will provide verification that the instrumentation and the system is operation properly as the core is loaded. At the critical point a determination must be recorded that the system is operating properly before proceeding to the full loading. Utilize SOP-3 during this task.

- ❑ **LOW POWER TESTING**
  Perform low power manual and automatic operation to assure that the system is operating properly. CCP-1, CCP-3 and CCP-4 shall be performed.

- ❑ **CALIBRATE NEW INSTRUMENTATION**
  Calibrate the new console instrumentation based on the reference instrumentation.

- ❑ **ROD WORTH AND CORE REACTIVITY EVALUATION**
  CCP-15 and CCP-11 shall be used for this task.

- ❑ **THERMAL POWER CALIBRATION**
  Perform this task with CCP-2.

- ❑ **MISCELLANEOUS CHECKS AND CALIBRATIONS**
  CCP-5 (Fuel Temperature Versus Power), CCP-6 (High Power and Fuel Temperature SCRAM Checks), CCP-13 (Semi-Annual Pulse Comparison), CCP-26 (Power Supply-SCRAM Channel Test) and CCP-30 (Transient Rod Worth, Pulse and Square Wave Prediction Curves) should be performed. Remove the reference power instruments and complete the inspection of those elements which were not inspected previously.

- ❑ **COMPLETE OPERATIONAL TRAINING**
  This is formal operational testing to complete the training of all of the operators.

- ❑ **REVIEW AND UPDATE AS INSTALLED DRAWINGS**

- ❑ **REVIEW AND UPDATE ALL PROCEDURES AND TRAINING MATERIALS**

- ❑ **REPORT TO THE SAFEGUARDS COMMITTEE, INSTALLATION COMPLETED**

- ❑ **REPORT TO THE NRC, INSTALLATION COMPLETED**

Appendix D

Safety Analysis Report Revisions

Instructions for updating the existing (March 1, 1985) Safety Analysis Report:

Remove Old Pages	Insert New Pages
	Title Page
Table of Contents (3 pages)	Table of Contents (4 pages)
List of Figures (2 pages)	List of Figures (2 pages)
	List of Effective Pages (1 page)
Pages III-1 thru III-23	Pages III-1 thru III-23
Pages IV-1 thru IV-9	Pages IV-1 thru IV-8
Pages V-5 / V-6	Page V-5 / V-6
Pages VI-9 thru VI-12	Pages VI-9 thru VI-12
Pages VII-1 thru VII-14	VII-1 thru VII-55
Pages VIII-1 thru VIII-4	Pages VIII-1 thru VIII-4
Page IX-29 / IX-30	Page IX-29 / IX-30
Pages IX-49 thru IX-52	Pages IX-49 thru IX-53

Safety Analysis Report

for the

Penn State Breazeale Reactor

License Number R-2
Docket Number 50-05

The Pennsylvania State University
University Park, PA 16802

April 19, 1991

SAFETY ANALYSIS REPORT

TABLE OF CONTENTS

Safety Analysis Report

List of Figures

Safety Analysis Report

LIST OF EFFECTIVE PAGES

SAR-I Introduction

Pages 1-2	March 1, 1985

SAR-II Site Characteristics

Pages 1-10	March 1, 1985

SAR-III Reactor Design

Pages 1-23	April 19, 1991

SAR-IV Reactor Pool and Water System

Pages 1-8	April 19, 1991

SAR-V Facility Construction

Pages 1-4	March 1, 1985
Pages 5-6	April 19, 1991
Pages 7-10	March 1, 1985

SAR-VI Facilities and Experimenters

Pages 1-8	March 1, 1985
Pages 9-12	April 19, 1991
Pages 13-14	March 1, 1985

SAR-VII Reactor Safety, Protection, Control and Monitoring System

Pages 1-55	April 19, 1991

SAR-VIII Conduct of Operation

Pages 1-4	April 19, 1991

SAR-IX Safety Evaluation

Pages 1-28	March 1, 1985
Pages 29-30	April 19, 1991
Pages 31-48	March 1, 1985
Pages 49-53	April 19, 1991

III REACTOR DESIGN

A. Introduction

As the original Pennsylvania State University (PSU) 200 KW reactor, with its MTR type fuel elements, approached its tenth year of operation, it became apparent that the replacement of certain basic components was desirable. To fulfill that desire and to increase research, instruction, and continuing education capabilities, The Pennsylvania State University purchased from Gulf General Atomic the components for converting to a TRIGA MARK III Reactor.

Dismantling of the 200 KW MTR reactor began on 26 November 1965 and five weeks later at 1237 hours on 31 December 1965 the 1 MW Penn State Breazeale Reactor (PSBR) achieved criticality.

B. Mechanical Design

1. Reactor Bridge

The angle aluminum suspension tower, four control rod drive motors two area monitor ion chambers, a fuel handling tool, the diffuser pump, the central thimble oscillator, a jib crane, an accumulator tank for transient rod air, bulk pool temperature sensors, pool lights, a nitrogen gas bottle, and a TV receiver are all items supported by a bridge assembly which spans the pool as shown in Figure 3-1. The bridge is mounted on four wheels and can be moved on rails that are bolted to the top surface of the pool walls. Movement of the bridge assembly is controlled by hand and the speed of the movement is limited by a high gear ratio hand wheel. Two vises clamp the bridge to the rails and the hand wheel is chained and padlocked so that the bridge assembly cannot be moved during operation. Electrical power and control circuit wiring are supplied to the bridge by a cable arrangement. The slack cable, which allows reactor bridge movement, is stored in a floor trough which runs parallel to the pool wall.

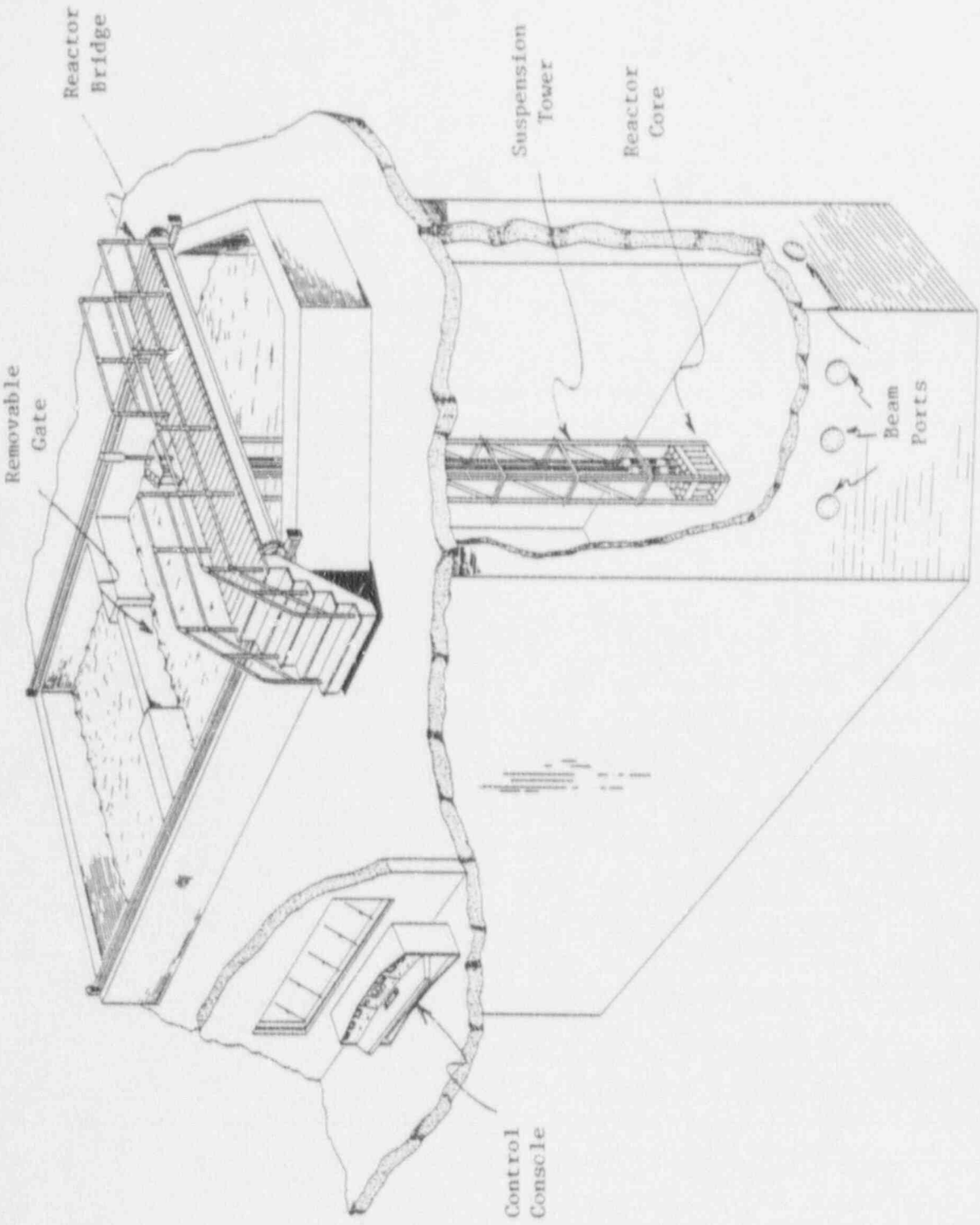


Figure 3-1 The Location of the PSBR Core, Bridge, and Control Console

2. Reactor Suspension Tower

The suspension tower is a welded assembly of 2 x 2 x $\frac{1}{4}$ inch angle aluminum. The upper end of the tower is bolted to the reactor bridge I-beams and extends 22'8" below the bridge floor. The lower end of the tower has a 19 x 29 x 3 inch grid plate bolted to it. A partial list of equipment supported by the suspension tower follows: the core assembly and grid plates, a central thimble, a GIC detector for the Power Range Monitor, a fission chamber for the Wide Range Monitor, the N-16 diffuser system plumbing and spray nozzle, an external neutron source, two pneumatic transfer system termini, vertical access tubes, and core lights.

3. Reactor Grid Plates

The grid plate arrangement is shown in Figure 3-2. The fuel element positioning holes are arranged in a hexagonal pattern. The bottom grid plate is an aluminum plate approximately 19 x 29 x 3 inches and is bolted to the vertical aluminum angles of the suspension tower structure. The bottom grid plate supports the weight of the fuel and has fuel element locating holes over its entire surface. The top grid plate is $\frac{5}{8}$ inch thick, made of aluminum but covers only a portion of the available area so that experiments can be conveniently mounted on the bottom grid plate immediately adjacent to the active core. Holes approx. $1\frac{1}{2}$ inch in diameter in the top aluminum grid plate position the fuel elements and control rods. A 12 x 16 x $1\frac{1}{4}$ inch aluminum safety plate is suspended approximately 12 $\frac{3}{4}$ inch below the bottom grid plate to prevent the control rods from dropping out of the core should their mechanical connections fail (see Figure 3-3). Small holes at various positions in the top grid plate permit insertion of wires and other small devices into the reactor for in-core measuring purposes. The following special in-core experimental facilities are available in the top grid plate (see Figure 3-2):

a. A central thimble 1.33" inside diameter
b. A central removable section of top grid plate provides a 4.12" diameter hole (15.85 sq.in. cross section).
c. Two removable triangular sections of the top grid plate provide circular openings with 2.4" inside diameters.
d. A large removable side section of the top grid plate.

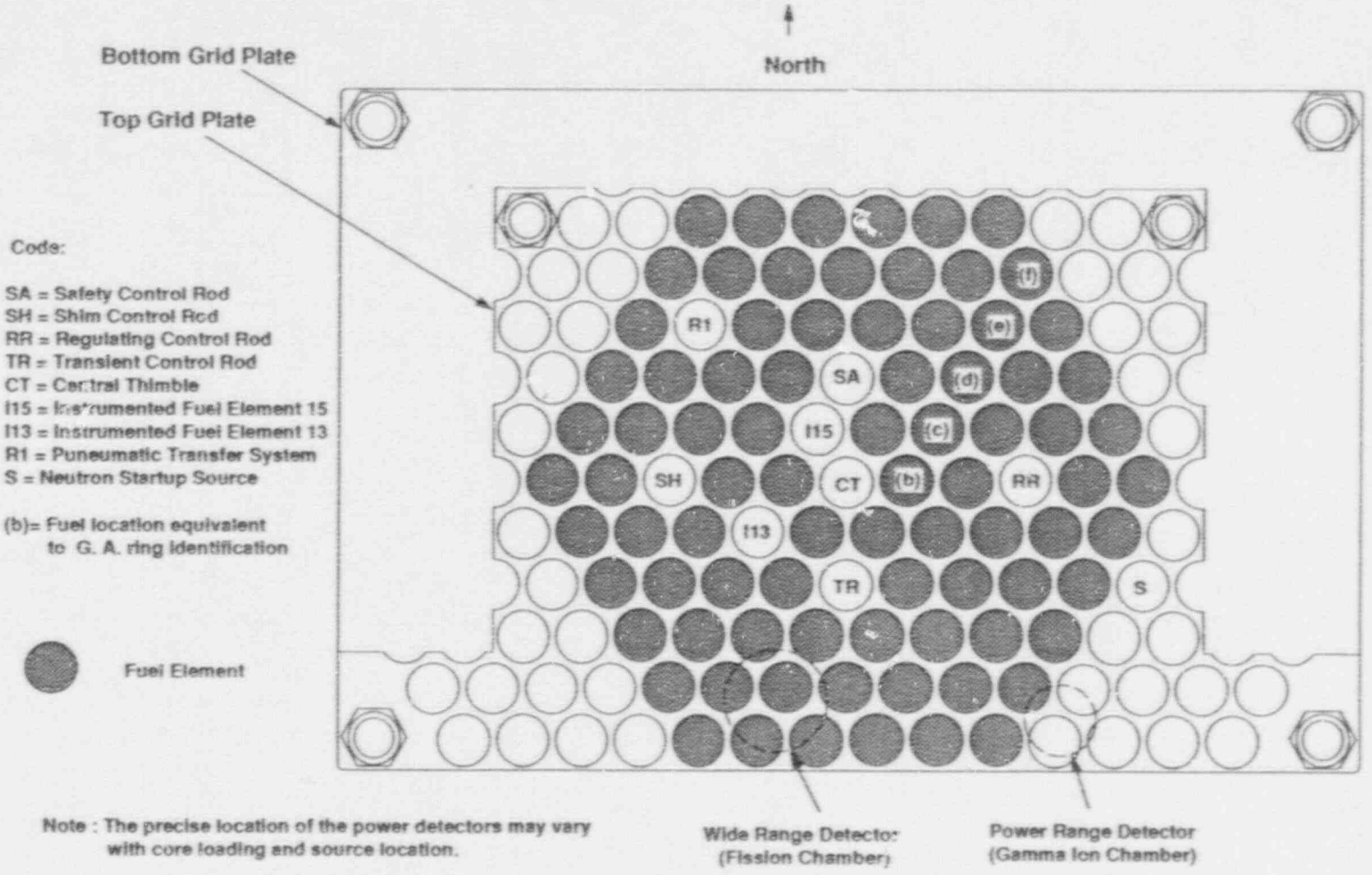


Figure 3-2 The Layout of the PSBR Grid Plates

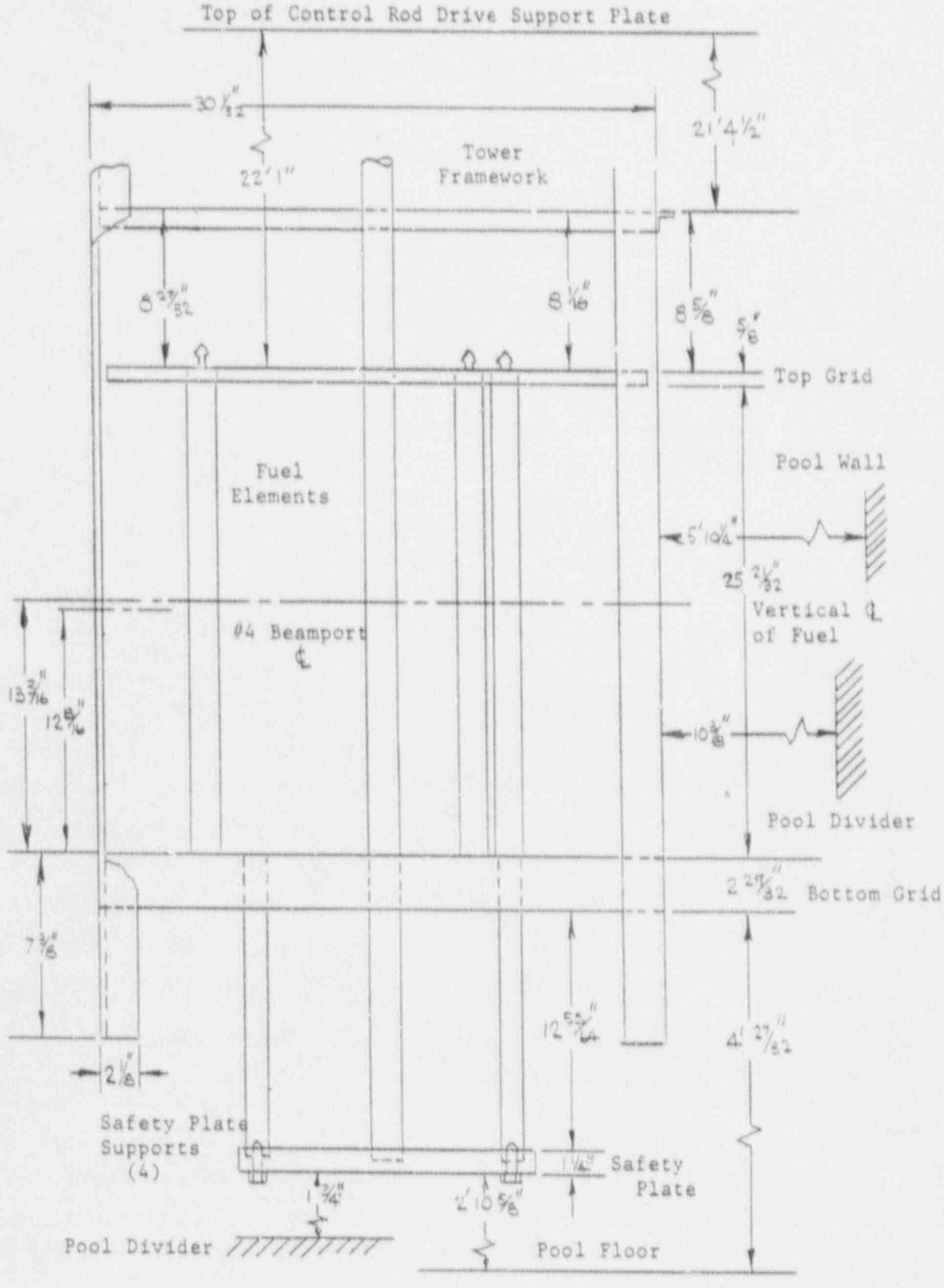


Figure 3-3 The Arrangement of the PSBR Grid Plates and Safety Plate

4. Fuel-Moderator Elements

The PSBR utilizes fuel-moderator elements in which zirconium hydride moderator is homogeneously combined with partially enriched uranium fuel. The fueled section of these elements is 15" long, 1.43" in diameter, and contains uranium in 2 different weight percentages enriched to slightly less than 20% in U-235. Part of the elements are 8.5 weight % uranium in zirconium hydride and the remainder are 12 weight %. The hydrogen to zirconium atom ratio of the fuel-moderator material for the original 8.5 weight % fuel is 1.7 to 1.0 and 1.65 to 1.0 for the 12 weight % fuel. To facilitate hydriding, a 0.18" diameter hole was drilled through the center of the active fuel section. A zirconium rod was inserted in this hole after hydriding was completed. Figure 3-4 shows a standard fuel element.

The weight of a fuel element is about $7\frac{1}{2}$ pounds with the U-235 content between 36 and 39 grams in the 8.5 weight % elements and between 53 and 56 grams in the case of 12 weight % elements. Serial numbers scribed on the top end fixtures are used to identify individual fuel elements. Each element is clad with 0.02" thick stainless steel.

To measure fuel temperature during reactor operation, instrumented fuel elements are fabricated similar to standard elements but with three thermocouples embedded in the fuel region. One thermocouple is at the vertical centerline of the element and the other two are located 1" above and 1" below center. All three thermocouples are located 0.27" radially from the center of the fuel element. Figure 3-5 shows an instrumented fuel element. The thermocouple lead wire passes through a water tight seal contained in a $\frac{3}{4}$" outside diameter stainless steel tube welded to the upper end-fixture. This stainless steel tube is extended to provide a watertight conduit carrying the lead wires above the water surface of the pool. Additionally, the stainless steel tube provides a means of handling the element.

5. Control Rods

Three standard, motor-driven control rods: one safety, one shim, one regulating rod; and one electro-pneumatic transient rod control reactor power during steady state operation. These control rods pass through and are

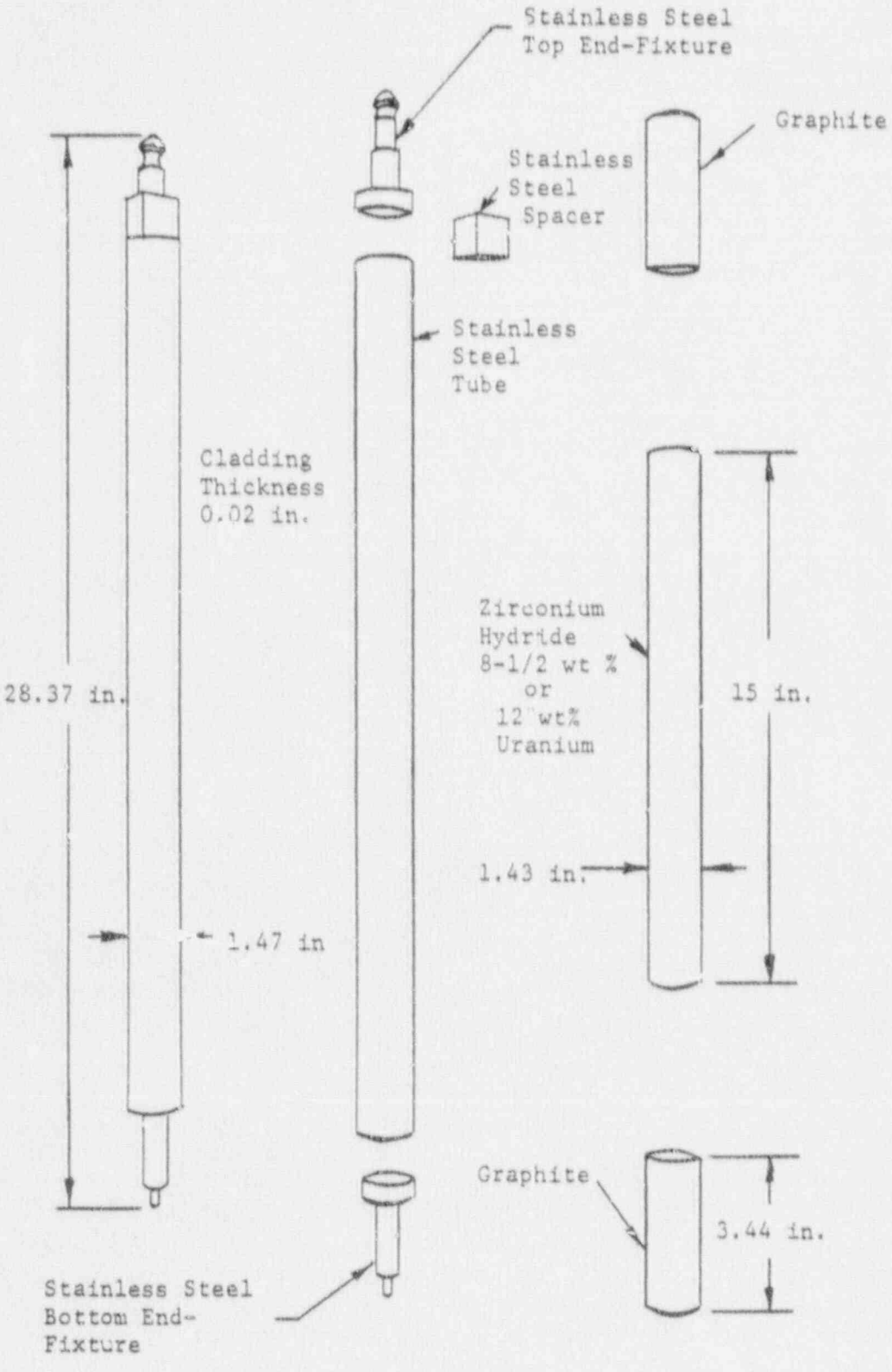


Figure 3-4 A Standard TRIGA Fuel-Moderator Element

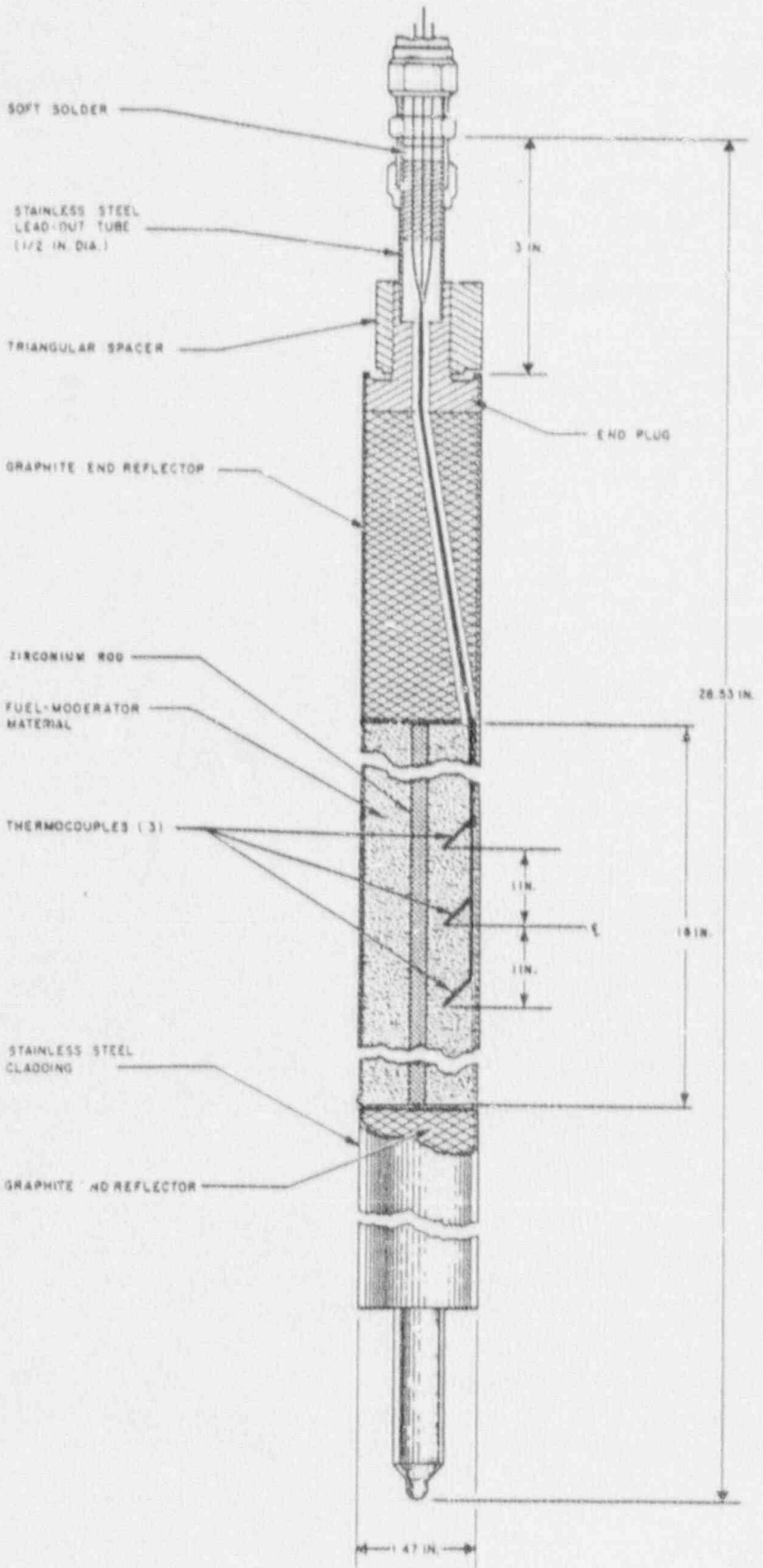


Figure 3-5 An Instrumented TRIGA Fuel Element

guided by the top and bottom grid plates. The rod locations are shown in Figure 3-2. The stainless steel clad control rods are 43" long and $1\frac{3}{8}$" in diameter. A standard control rod is shown in the withdrawn and inserted positions in Figure 3-6.

The upper section of a standard rod is graphite; the next 15" is graphite impregnated with powdered boron carbide which provides neutron absorption; the follower section consists of 15" of uranium zirconium hydride fuel (about 31 grams of U-235); the bottom section is $6\frac{1}{2}$" of graphite.

The fourth control rod, shown in Figure 3-7, is the transient rod. It has two functions; (1) it acts as a safety and/or control rod in the steady state mode of operation and (2) it is pneumatically driven from the core for the square wave and pulse modes of operation. The transient rod is 37" long and is contained in a $1\frac{1}{4}$" diameter aluminum tube. The borated graphite section is 15" long. Unlike the standard control rods, the transient rod has an air filled follower that is 21" long. The transient rod is guided laterally in the core by a thin walled aluminum guide tube that passes through the upper and lower grid plates and screws into the safety plate. All four control rods have a stroke of approximately 15".

6. Control Rod Drives

Rack-and-pinion drives are used to position the shim rod, the regulating rod, and the safety rod. Each drive consists of a variable speed, reversible servo motor/resolver; a magnetic rod-coupler; and a rack-and-pinion gear system (see Figure 3-8). The pinion gear engages a rack attached to a draw tube supporting an electromagnet. The magnet engages an iron armature attached above the water level to the end of a long connecting rod that terminates at the lower end in the poison rod. The magnet, its draw tube, the armature, and the upper portion of the connecting rod are housed in a tubular barrel. The barrel extends below the pool water level with the lower end of the barrel serving as a mechanical stop to limit the downward travel of the control rod assembly. Part way down the upper portion of the connecting rod, i.e., just below the armature, there is a piston that travels within the barrel assembly. Because the upper portion of the barrel is well ventilated by large slotted openings, the piston moves freely in this range; but when the piston is within 2

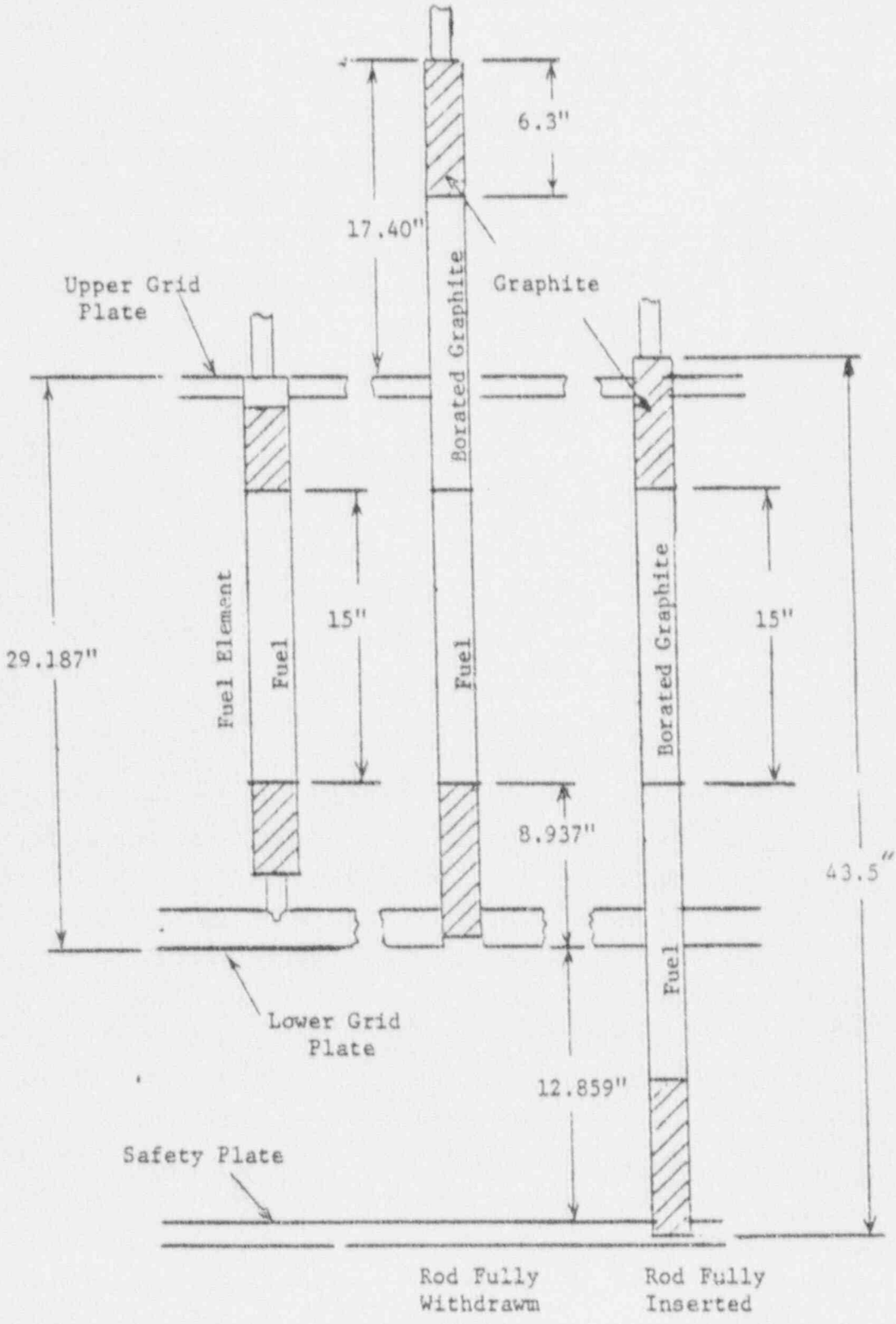


Figure 3-6 A Fueled Follower Control Rod with Respect to the PSBR Core

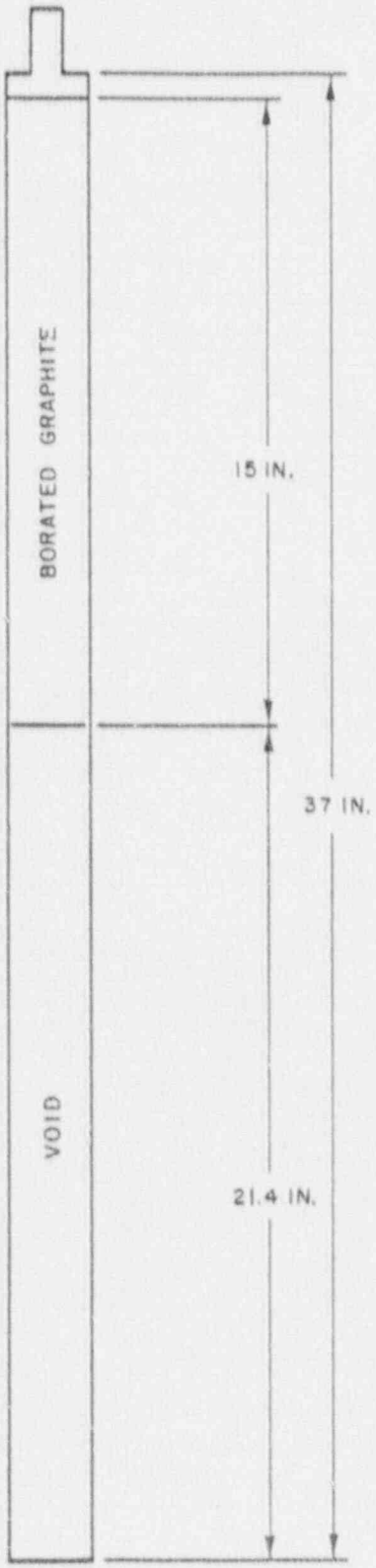


Figure 3-7 A Transient Control Rod

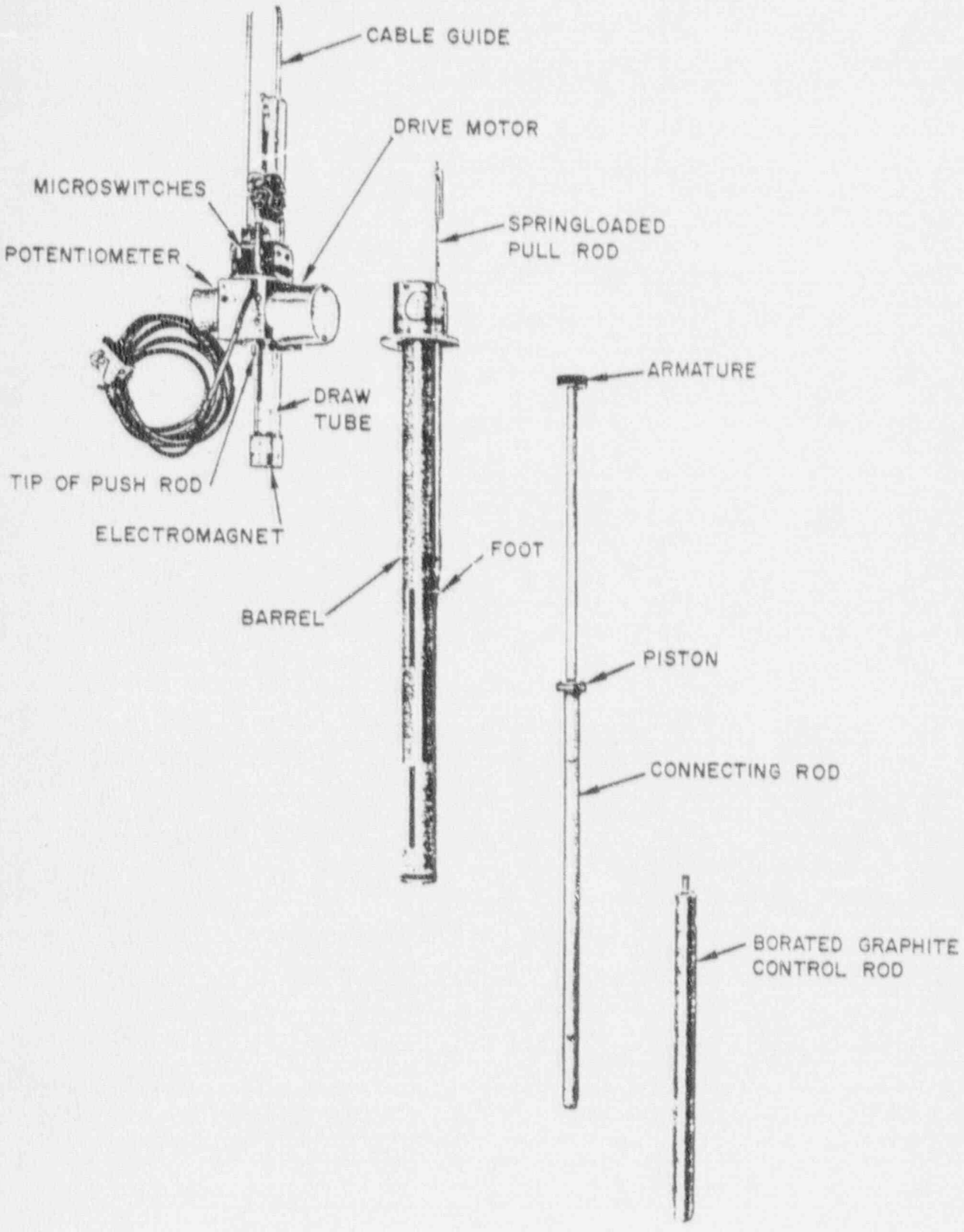


Figure 3-8 A Rack-and-Pinion Control Rod Drive

inches of the bottom, its movement is restrained by the dashpot action provided by the graduated vents in the lower end of the barrel. This dashpot action reduces bottoming impact when the rods are dropped by a scramming action.The control rod is withdrawn from the core by the rotation of the motor shaft when the electromagnet is energized. When the reactor is scrammed, the electromagnet is de-energized and the control rod drops into the core by gravitational force.

The drive motors for all of the control rods are variable speed, reversible servo motor/resolver/controller systems. The speed of the motors is determined by the jumper positions within the controller and the analog velocity signal to the controller from the PCMS of the new console (see chapter VII). The maximum speed of each drive is tunable such that the maximum reactivity addition rate of the technical specifications is not exceeded.

The control rod position and the drive position are mimicked on the operator display of the PCMS. The positions are determined by the PCMS from the resolver signal from the motor, the state of the drive end of travel switches and the state of the control rod down switchs. The rod drives may be "homed" under certain conditions to a known position. That position is determined by the use of home low speed limit switches (HLLS) and home limit switches (HLS) (see chapter VII).

To allow transient operation with the fourth control rod, use was made of a pneumatic-electro-mechanical drive system to eject a predetermined amount of the transient rod from the core (see Figure 3-9).

The pneumatic portion of the pneumatic-electro-mechanical drive, referred to herein as the "transient rod drive," is basically a single-acting pneumatic cylinder. A piston within the cylinder is attached to the transient rod by means of a connecting rod. The piston rod passes through an air seal at the lower end of the cylinder. Compressed air is admitted at the lower end of the cylinder to drive the piston upward. As the piston rises, the air being compressed above the piston is forced out through vents at the upper end of the cylinder. At the end of its stroke, the piston strikes the anvil of a shock absorber. This piston is thus decelerated at a controlled rate during its final inch of travel. This action minimizes rod vibration when the piston reaches its upper limit stop.

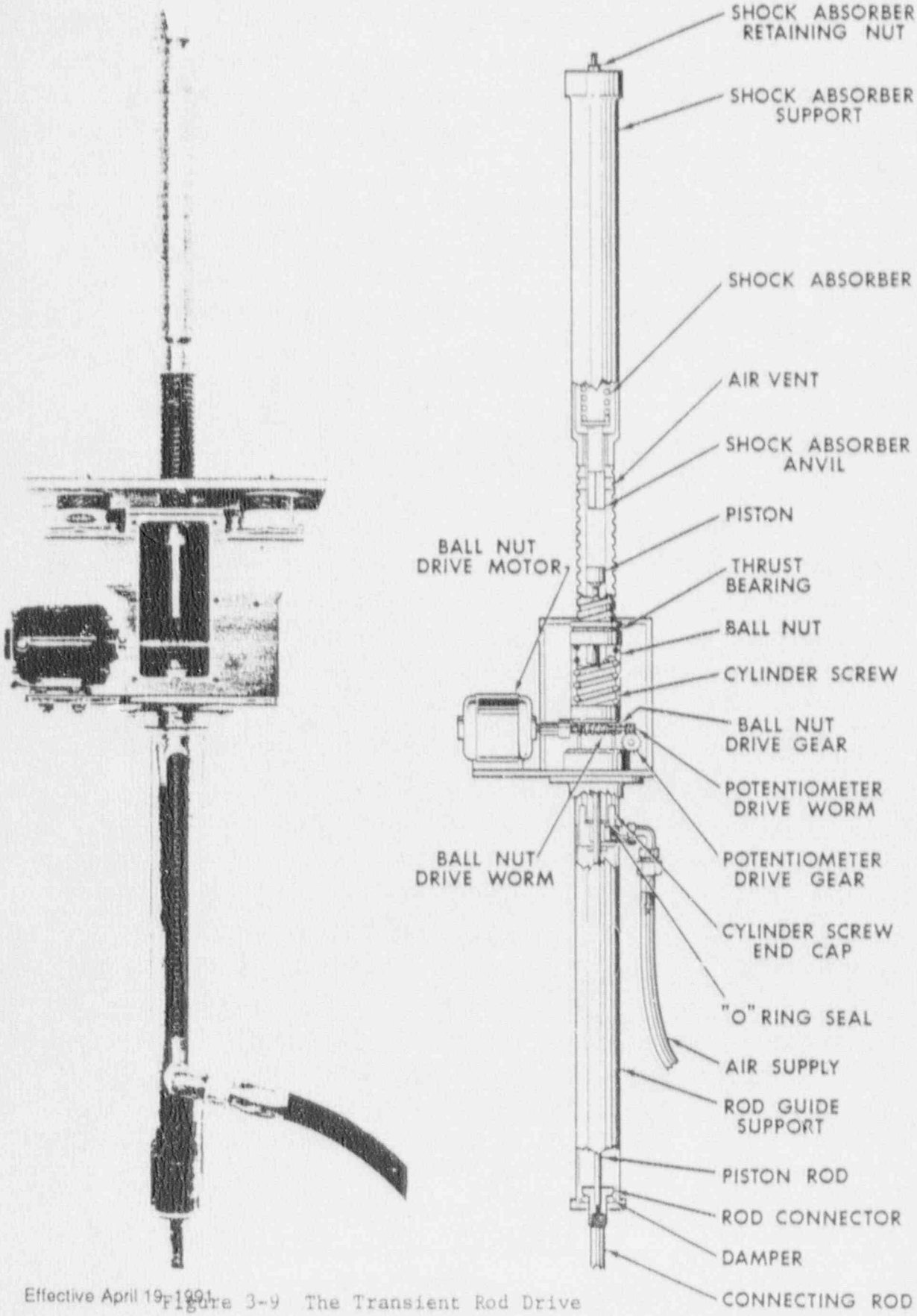


Figure 3-9 The Transient Rod Drive

An accumulator tank mounted on the movable reactor bridge stores the compressed air that operates the pneumatic portion of the transient rod drive. A three-way solenoid valve, located in the piping between the accumulator tank and the cylinder, controls the air supplied to the pneumatic cylinder. De-energizing the solenoid valve interrupts the air supply and relieves the pressure in the cylinder so that the piston drops to its lower limit by gravity. With this operating feature, the transient rod is inserted in the core except when air is supplied to the cylinder. Applying air to the transient rod cylinder by depressing the TRANSIENT ROD FIRE button prior to moving the cylinder allows the transient rod to be used as an ordinary control rod. Pre-positioning the transient rod cylinder and then applying air in accordance with PSBR Standard Operating Procedures allows the transient rod to be used for square wave and pulse operation.

The electromechanical portion of the transient rod drive consists of a servo motor, a ball-nut drive assembly, and the externally threaded air cylinder. During electromechanical operation of the transient rod, the threaded section of the air cylinder acts as a screw in the ball-nut assembly. These threads engage a series of balls contained in a ball-nut assembly in the drive housing. The ball-nut assembly is in turn connected through a worm gear drive to an electric motor. The cylinder may be raised or lowered independently of the piston and control rod by means of the servo drive. Adjustments of the position of the cylinder controls the upper limit of the piston travel, and hence controls the amount of reactivity inserted for a pulse or square wave.

A system of limit switches similar to that used with the standard control rod drives is used to indicate the position of the air cylinder and the transient rod. Two of these switches, the Drive Up and DriveDown, are actuated by the cylinder. A third limit switch, the Rod Down switch, is actuated when the piston reaches its lower limit of travel.

7. Graphite Reflector Elements

Graphite reflector elements may occupy the grid positions not filled by fuel-moderator elements and other core components. The graphite reflector elements are canned in aluminum and have aluminum end fixtures and spacer blocks. These elements are of the same dimensions as the fuel-moderator elements, but are filled entirely with graphite. Each graphite reflector element weighs 2.8 pounds and is anodized after assembly. The spacer blocks have a blue anodized finish to make the graphite dummy elements easily distinguishable from fuel-moderator elements. When properly installed in the core, the top of the triangular spacer block of the fuel and graphite elements are level with the top of the top grid plate.

C. Nuclear Design

1. Standard TRIGA Core

The design and operating characteristics of standard TRIGA cores are well known as is the inherent safety characteristic of this class of reactor. The first PSBR standard TRIGA core loading reached criticality in December 1965 (see Figure 3-10). Table 3-1 lists operating characteristics that were observed for core loading #4, one of the first, widely used, PSBR configurations of standard 8.5 wt % TRIGA elements (see Figure 3-11). Most of the fuel in core loading #4 received little burnup during this period of the PSBR operation. Table 3-1 also lists the core characteristics for the present loading #36, a core composed of a mixture of 8.5 wt % and 12 wt % fuel elements.

64 Elements = 2443 gm U-235
3 Rods = 94 gms U-235

Critical Rod Positions

Safety	816 units
Shim	817 units
Regulating	679 units
Transient	1014 units

Excess Reactivity = $0.15

(1)— Fuel Element Identification number

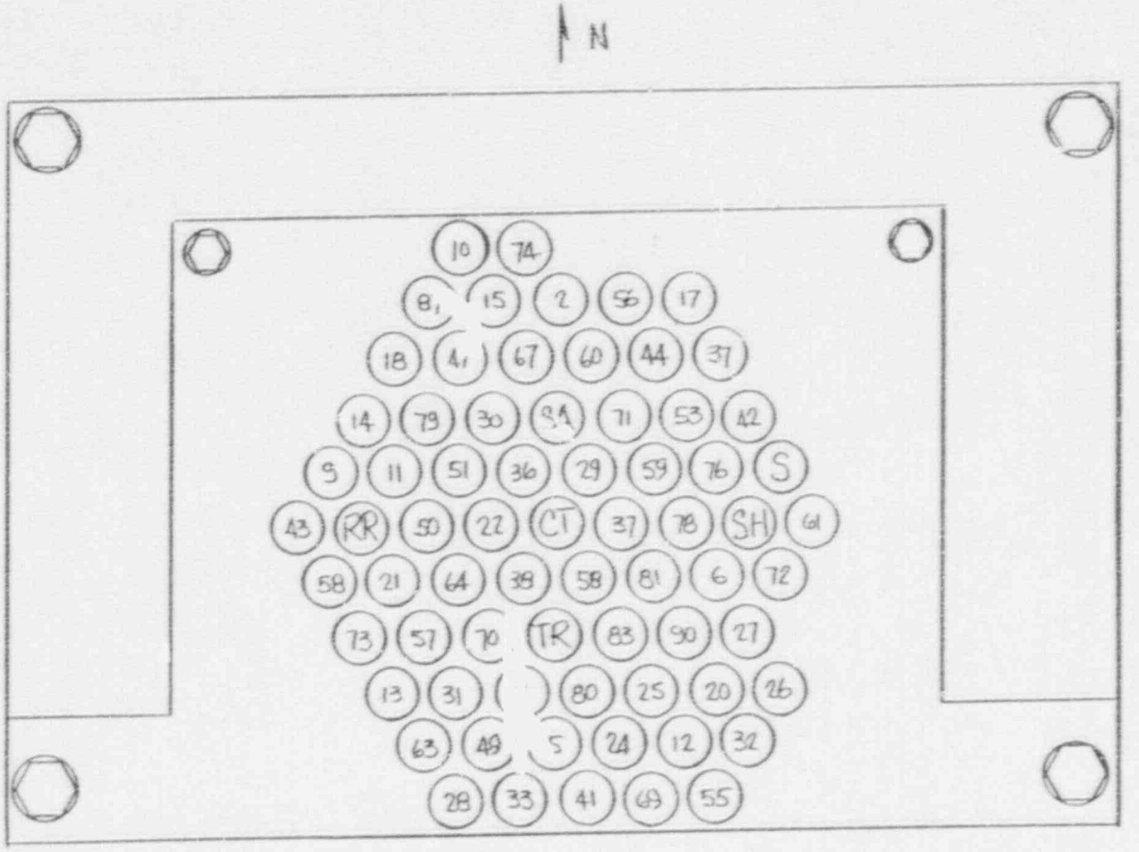


Figure 3-10 A Layout of Core Loading #1

82 Elements 3125 gm U-235
3 Rods 94 gm U-235

Control Rod Positions

Safety	769 units
Shim	49 units
Regulating	51 units
Transient	567 units

Excess Reactivity $6.64

(1) ← Fuel Element Identification number

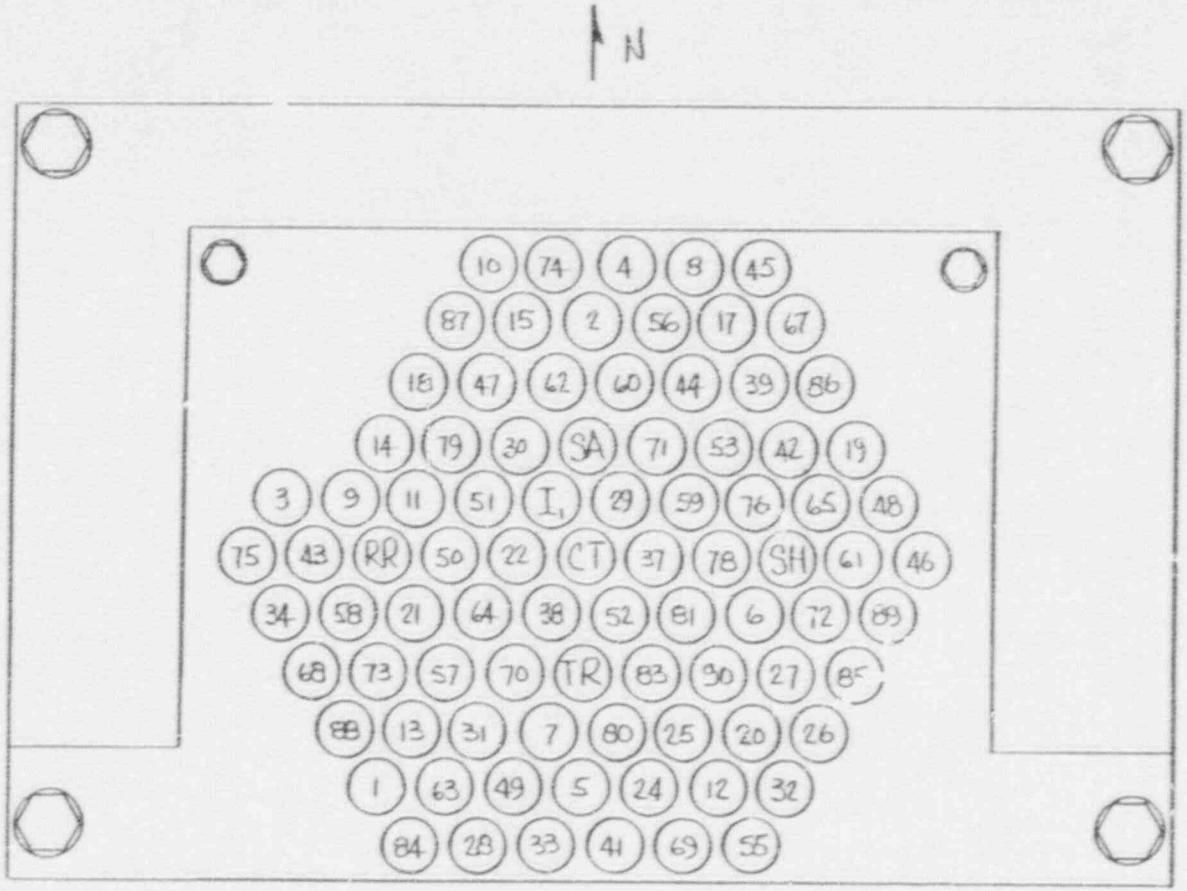


Figure 3-11 A Layout of Core Loading #4

Table 3-1

Operating Characteristics of PSBR Loading Core #4

Steady State Power Level	1 MW
Core Mass	3219 grams U-235
Minimum Critical Mass (Core #1)	2537 grams U-235
Total Control Rod Worth	$11.63
Excess Reactivity	$6.64
Power Defect (1MW)	$3.50
Prompt Negative Temperature Coefficient	-1.4×10^{-4} $\Delta k/k/C$
Maximum Pulse Temperature	912°C
Maximum Pulse Reactivity Insertion	$3.40

Operating Characteristics of PSBR Loading Core #36

Steady State Power Level	1 MW
Core Mass	3190 grams U-235
Minimum Critical Mass (Core #1)	---
Total Control Rod Worth	$11.14
Excess Reactivity	$6.39
Power Defect (1MW)	$4.00
Prompt Negative Temperature Coefficient	-1.4×10^{-4} $\Delta k/k/C$
Maximum Pulse Temperature	1067°C
Maximum Pulse Reactivity Insertion	$3.40

The Safety Evaluation section in this document will show that pulsing to $3.40 will not exceed the Limiting Safety System Setting (LSSS) of 700°C. The temperature and power characteristics during the first 19 pulses of core loading #4 are shown in Figures 3-12 and 3-13. Greater than 50% of the prompt negative temperature coefficient of a standard TRIGA core comes from the "cell effect" or temperature dependent disadvantage factor, and approximately 20% each from Doppler broadening of the U-235 resonances and temperature dependent leakage from the core. The current loading that is being used routinely at the PSBR is a mixture of 12 wt % and 8.5 wt % fuel

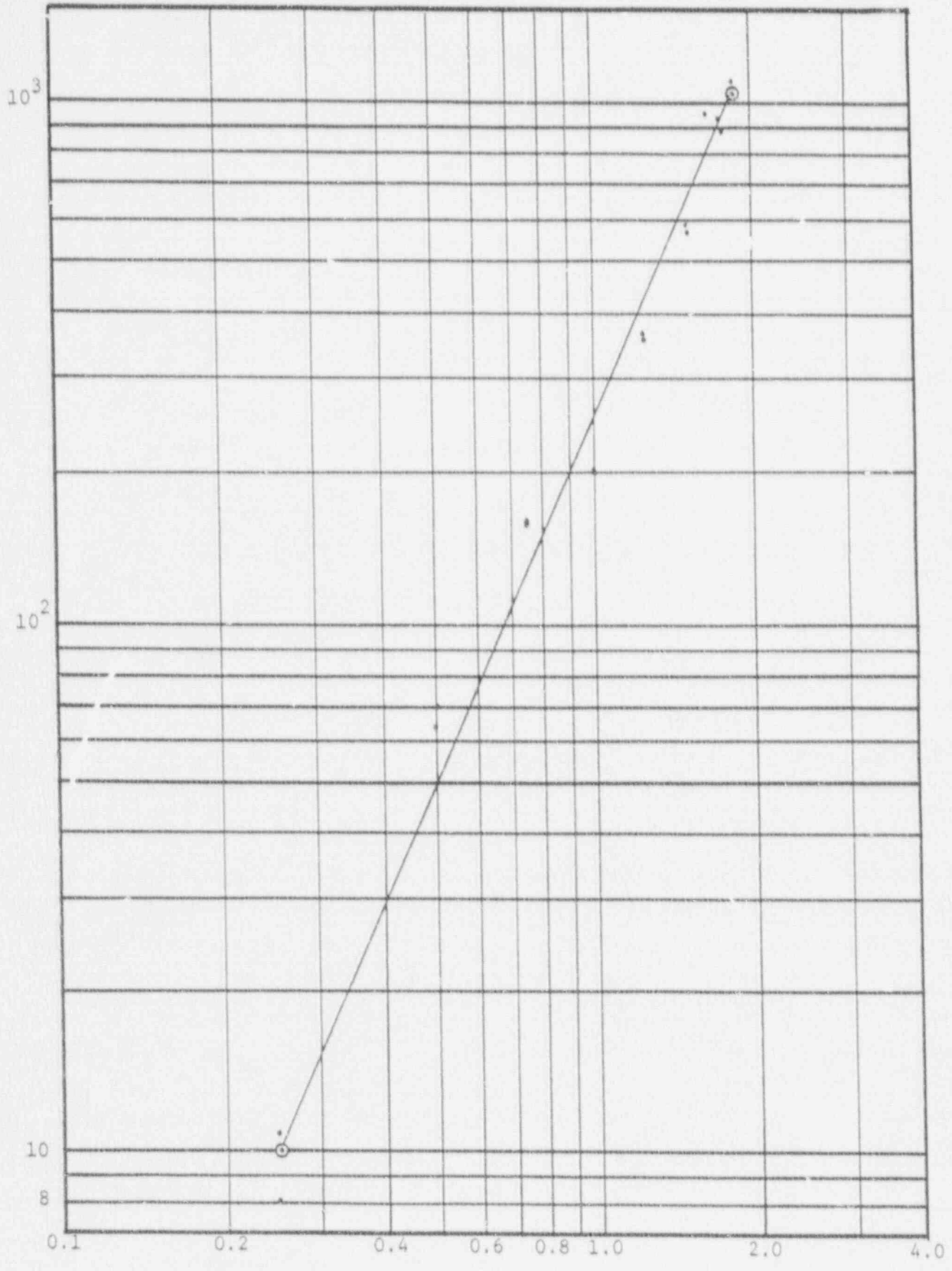


Figure 3-12 Peak Power versus Prompt Reactivity for the First Nineteen Pulses with Core Loading #4

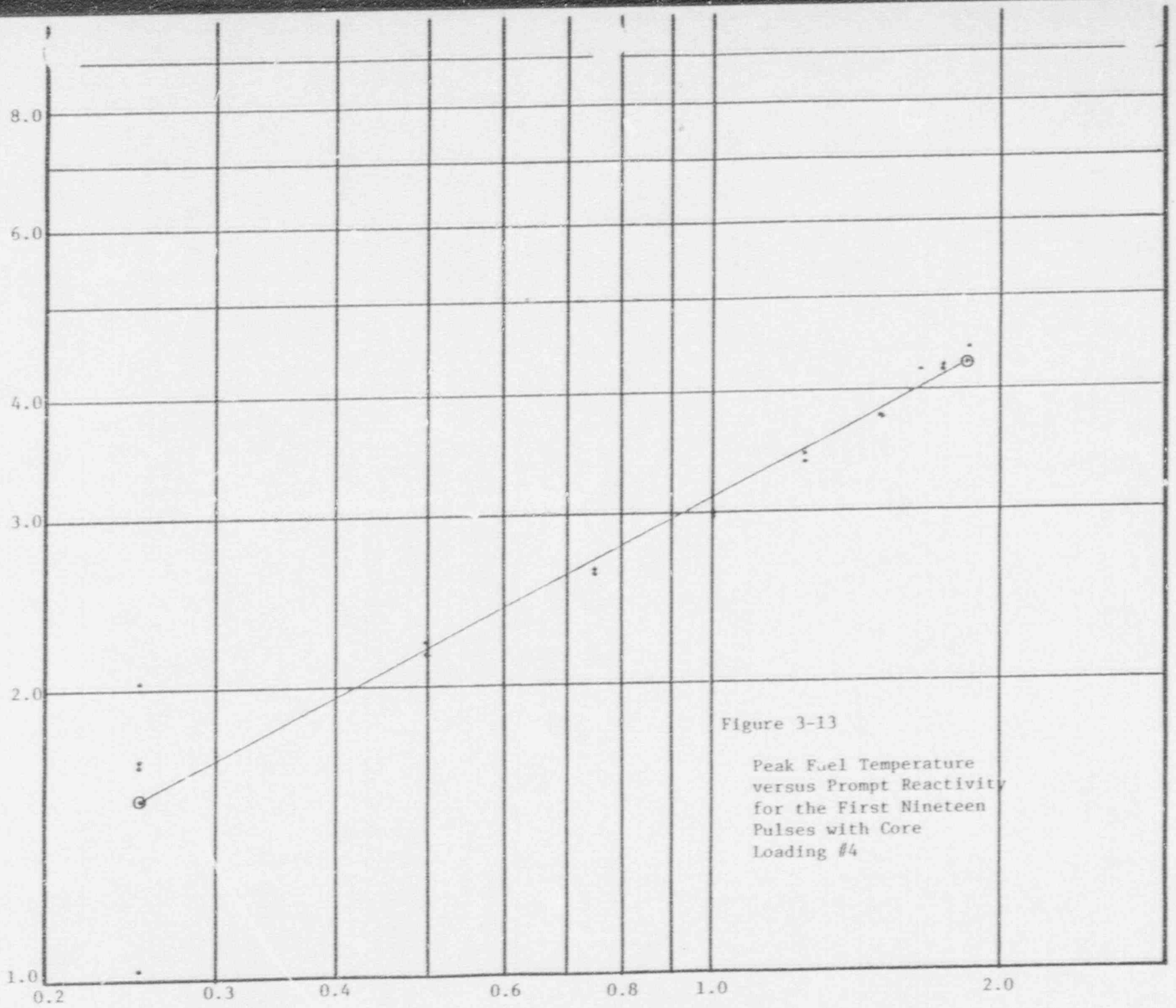


Figure 3-13

Peak Fuel Temperature versus Prompt Reactivity for the First Nineteen Pulses with Core Loading #4

92 Elements

(2xx) 14-12.0 wt%

(X XXX XX) 78-8.5 wt%

3 Fueled Rods

Control Rod Positions

(SA)	SAFETY	377 Units
(SH)	SHIM	370 Units
(RR)	REGULATING	311 Units
(TR)	TRANSIENT	448 Units

Excess Reactivity $6.39

(T) Central Thimble

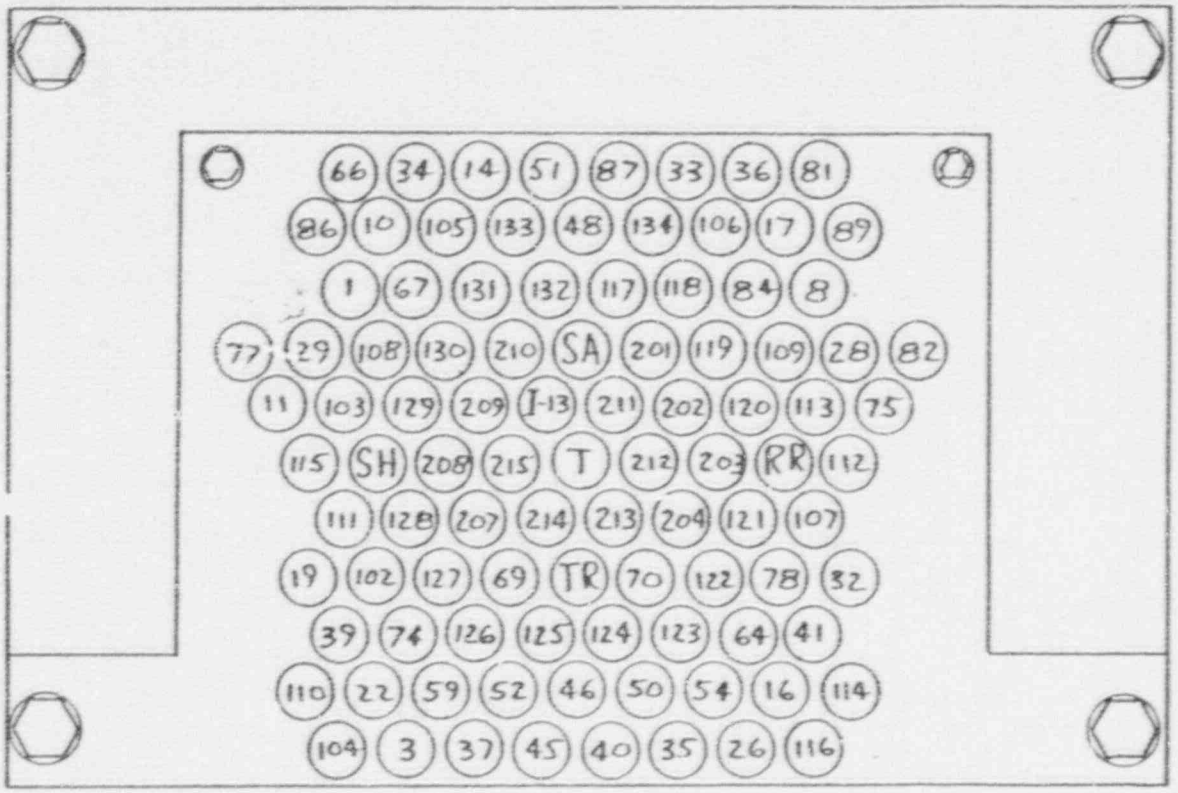


Figure 3-14 A Layout of Core Loading #36

(mixed core) as shown in Figure 3-14. Loading #36 exhibits many of the characteristics of Loading #4, i.e., similar excess reactivity, similar operating temperatures, etc. (see Table 3-1 for comparison), which indicates that mixed cores behave in a manner very similar to cores loaded with only 8.5 wt% fuel. The section on Safety Evaluation gives a detailed analysis of TRIGA core characteristics.

2. External Neutron Source

The start-up source used in the PSBR is a 3 curie americium-beryllium (Am-Be) neutron source doubly encapsulated in type 304L stainless steel. The source is contained in an aluminum source holder which has outside dimensions similar to standard fuel-moderator elements so that the holder can be positioned in any fuel element position in the core. Movement is accomplished manually by a cable attached to the top of the source holder.

Another external source available for use at the PSBR is a 0.235mg Californium-252 neutron source. The Californium oxide source in its platinum matrix is doubly encapsulated in zircaloy-2. It was fabricated at Savannah River Laboratories and is on loan to the University from the Department of Energy.

D. Thermal Design

The PSBR operates at 1 MW thermal steady state and is cooled by natural convection. Cooling water enters the core from the perimeter of the core region immediately above the bottom grid plate and to a smaller extent through holes provided in the bottom grid plate. The triangular shaped spacer blocks on the upper end of the fuel elements are used for positioning as well as providing a means for water to flow up through the core and out the top grid plate. Because of the natural convection cooling, the PSBR can be operated in a water filled pool with no direct coupling between the core and the heat removal system in the pool. Since no connection to a forced circulation system is required, the reactor can be operated at any position in the pool.

IV. REACTOR POOL AND WATER SYSTEMS

A. Reactor Pool

The reactor pool is approximately 30 feet long, 14 feet wide, and 24 feet deep. The pool is constructed of steel reinforced concrete. The pool walls are $1\frac{1}{2}$ feet thick below the level of the reactor bay floor and one foot thick above the reactor bay floor. The inside of the pool wall is coated with epoxy to form an epoxy pool liner. The pool is surrounded by earth fill with the exception of the south side. A room (Beam Hole Laboratory) exists outside the south side of the pool at the elevation of the reactor core. Additional shielding is provided by $3\frac{1}{2}$ feet of high density concrete on the outside of the pool wall in this room.

The total pool volume is approximately 71,000 gallons. The pool can be divided in two by a removable gate which permits draining either part of the pool while maintaining the reactor under water in the other part of the pool.

Seven beam ports penetrate the pool wall from the Beam Hole Laboratory to provide access to reactor radiation. The pool is equipped with two floor drains; one for each side of the pool when it is divided with the removable gate. Four other pool wall penetrations exist, two located approximately 10 feet above the pool floor to serve the pool recirculation loop and two located approximately 17 feet above the pool floor for the heat exchanger.

Several sources of water are available for adding water to the pool they are: (a) the distillate from the waste evaporator, which is stored in an underground tank, can be pumped into the recirculation loop for normal pool water make-up; (b) water from the University water system can be added to the pool through the demineralizer; (c) water from the University water system can be added to the pool at a high flow rate through the pool drain lines, after connecting a fire hose that is maintained in location for this purpose; (d) water from the secondary side of the heat exchanger can be diverted directly to the pool through a fire hose for emergency make-up water.

B. PSBR Water Handling System

1. General

For the proper and safe operation of the reactor and related equipment, certain properties of the water such as temperature and mineral content must be controlled. Figure 4-1 shows all of the water handling systems for the PSBR facility and in the following sections the individual systems are discussed in detail.

2. Pool Recirculation Loop

The recirculation loop normally recirculates pool water continuously through filters and a demineralizer to maintain water quality.

The flow rate through the system is about 40 gallons per minute. Water enters the system through a skimmer arrangement at the south end of the pool, flows through the recirculation pump, a filter, a mixed bed demineralizer and then flows back into the pool. In addition, a small portion of the water is diverted through a fission product monitor..

3. (THIS SECTION IS DELETED)

4. Transfer of Pool Water

Occasionally, for maintenance purposes, it is necessary to drain the reactor pool. In order to provide shielding for the reactor core and any stored fuel elements, only one half of the pool is drained at a time. The pool is divided into two parts by inserting an aluminum structure, or gate, into the gate support structures.

The water from either half of the pool can be stored in a 48,000 gallon aluminum hold-up tank located behind the facility. The water leaves the pool via large drains located in the pool floor along the west pool wall near the partial concrete divider. The storage tank transfer pump (capacity ≈300 gal/min) located in the beam hole laboratory is used to pump the water. Water can be returned to the pool from the storage tank using the same pump and floor drains (see Figure 4-1).

By opening the valves on either of the pool drain lines one could release pool water to the storm sewer. However, to minimize the release of radioactivity and to conserve the demineralized pool water, the pool water is transferred to the storage tank when it is necessary to drain the pool. To

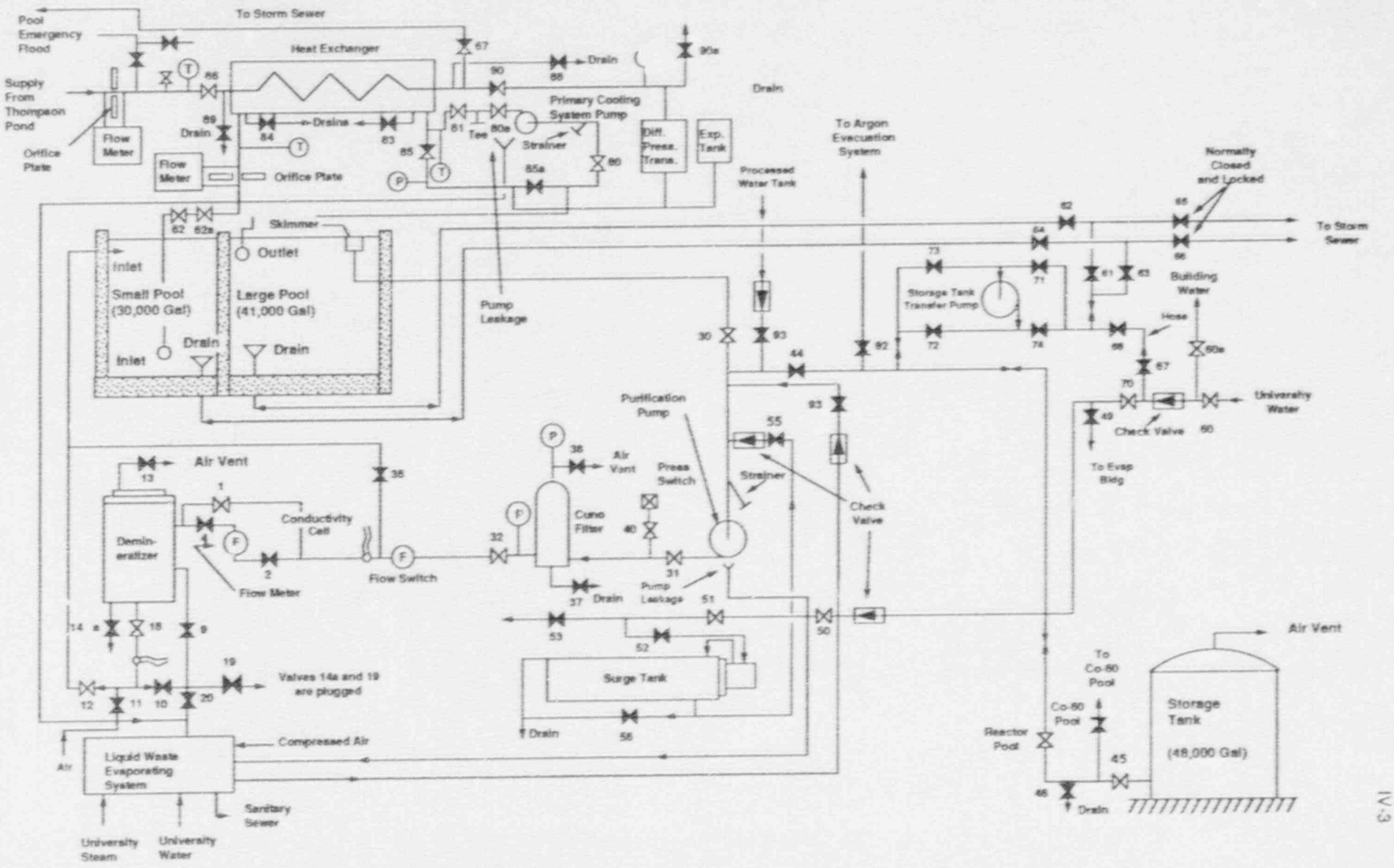


Figure 4-1 The PSBR Water Handling System

Figure 4-2 (This Figure is Deleted)

prevent any accidental release, valves #65 and #66 are secured with a padlock (see Figure 4-1). Keys to the lock are issued only to those with an NRC Senior Reactor Operator License.

5. Heat Exchanger

The PSBR heat exchanger limits the temperature of the PSBR pool water (see Figure 4-3). Maintaining lower pool temperatures decreases pool water evaporation losses and temperatures below 110°F are needed to prevent damage to the demineralizer anion resins.

The system is composed of two loops. In the primary loop, pool water is pumped through the baffled shell side of two double pass heat exchangers connected in series. In the secondary loop, cooling water is pumped from Thompson Pond, a spring fed pond located approximately 650 yards southeast of the PSBR, through the tube bundle side of the two heat exchangers and then to a storm sewer which returns the water to Thompson Pond. The lower quality secondary side water is passed through the tube bundles since by removing the ends of the two heat exchangers, the tube bundles can be cleaned more easily than the baffled shell side.

When the measured pressure difference shows the secondary outlet pressure to be less than 1.5 psig greater than the primary inlet pressure, a HEAT EXCHANGER SECONDARY PRESSURE LOW signal is activated to the PCMS.

Since the source of cooling water is Thompson Pond, which is fed by a 3 million gallon per day spring, relatively small year round variations in cooling water temperature are noted (55°F ± 2°F).

6. Liquid Waste Evaporator

Radioactive liquid waste is collected in either an underground holding tank just outside the evaporator building or in a holding tank below floor level inside the evaporator building. Liquid waste from either of these tanks (see Figure 4-4), can be pumped to the evaporator feed tank. This feed tank supplies the liquid to the evaporator during evaporator operation. The evaporator is a low pressure, low temperature unit which uses hot water as a heat source. The distillate from the evaporator is collected in a distillate tank.

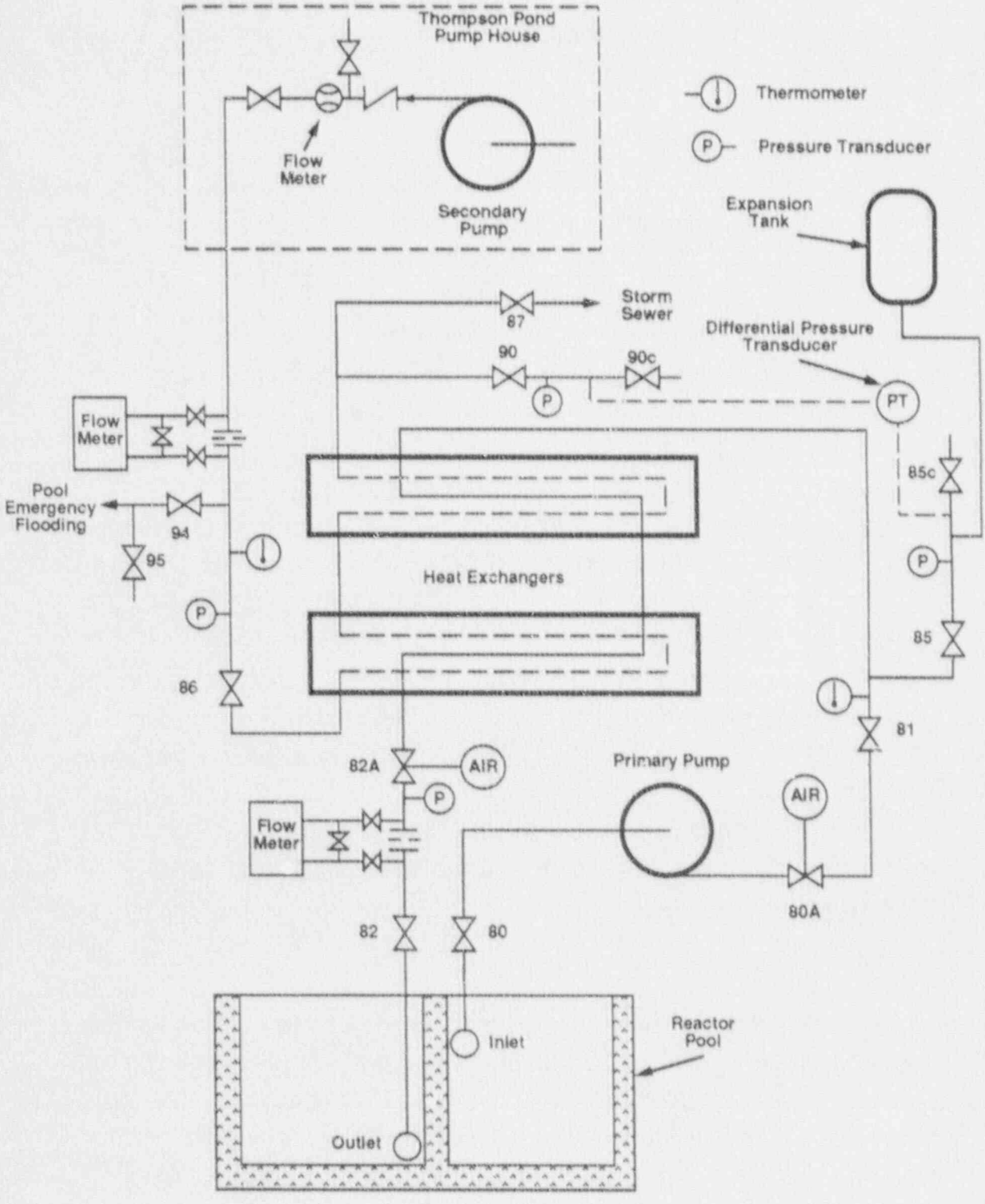


Figure 4-3 The PSBR Heat Exchanger

An overflow line installed in this tank directs the distillate to an underground holding tank where it is stored for later use as pool make-up water. The residue from the evaporation operation is removed from the evaporator, solidified and disposed by the Health Physics Office.

C. Water Quality Monitoring and Maintenance

Specific conductivity, pH and gross radioactivity are used as a measure of water quality. Conductivity is monitored by conductivity cells in the pool water recirculation loop (see Figure 4-1). pH and gross radioactivity are measured in the laboratory using a grab sample of pool water.

All three parameters: conductivity, pH, and gross radioactivity are controlled by filters and a demineralizer in the pool water recirculation loop. Abnormal levels in any of these parameters may indicate that this system is in need of service.

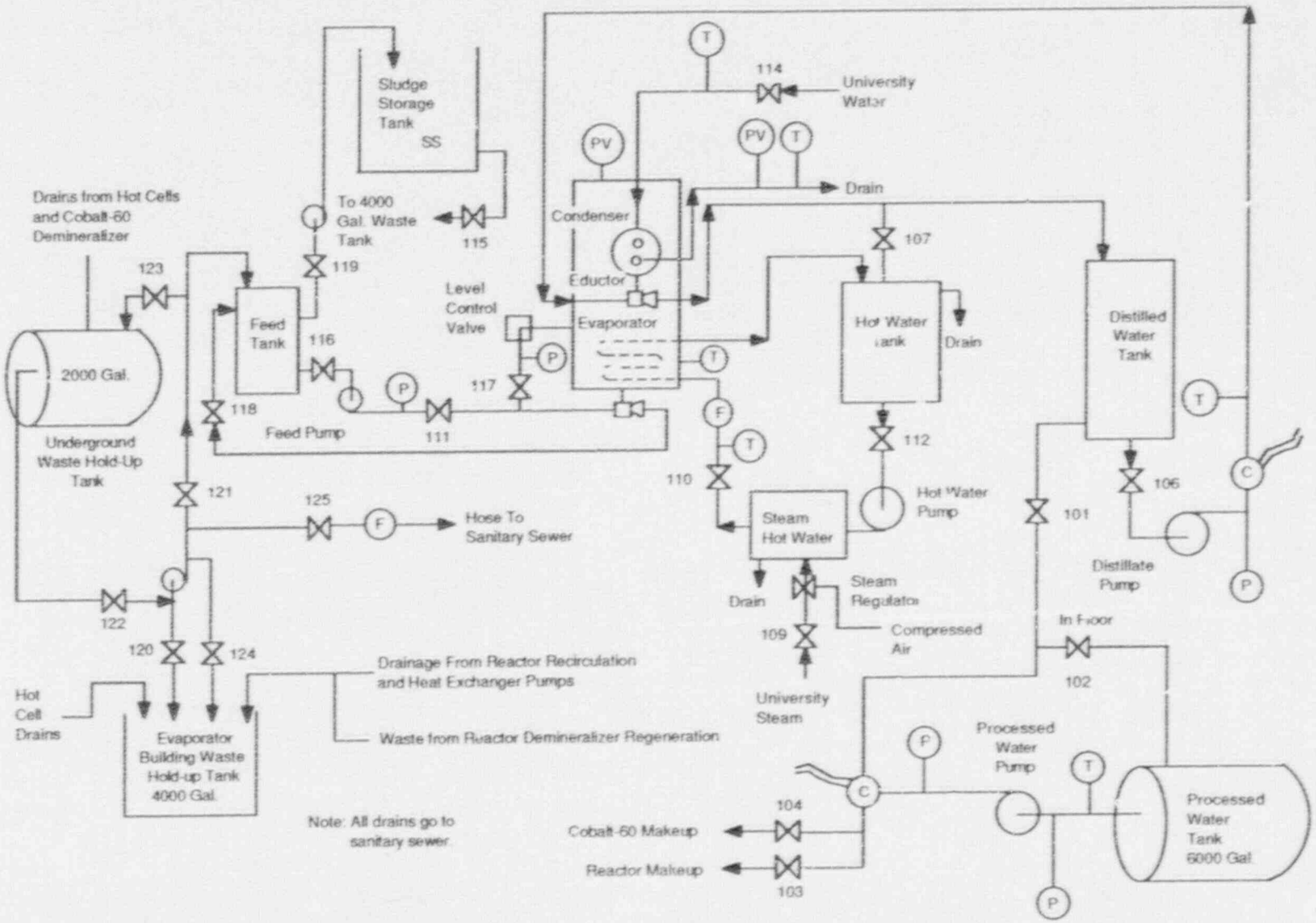


Figure 4-4. The PSBR Liquid Waste Evaporator System (APR 1991)

secured automatically when a building evacuation alarm is sounded. The second system, an emergency exhaust system, is automatically started when the building evacuation alarm is sounded. This emergency system exhausts the reactor bay through roughing filters, absolute filters and charcoal filters all in series before discharging to the atmosphere three feet above the reactor bay roof.

A control/status panel for the emergency exhaust system is located in the reception area for the cobalt-60 facility. This area is designated RECEPT A in Figure 5-2. This instrument panel is located such that the instruments on it could, in an emergency, be read from outside the building. Instruments on the panel consist of four differential pressure gauges, three of which indicate pressure drop across, the prefilter, the absolute filter and the charcoal filter. The fourth differential pressure gauge indicates the velocity pressure in the stack. Also located on the panel are two pilot lights; one indicates that the system is energized, the other indicates that there is air flow in the system. The second light gets a signal from a flow switch in the duct. A switch on this panel permits manual activation of the system. This switch does not permit defeating the automatic start upon receipt of an evacuation alarm.

The air in the reactor bay and control room is heated and cooled by a dedicated reactor bay air conditioner. This unit recirculates, heats, cools or dehumidifies reactor bay air as required. No air is interchanged with any other part of the building or outside of the building by this unit. Heating is supplemented by steam unit heaters as needed. The condensate from the reactor bay air conditioner is piped into the reactor pool as makeup water to help compensate for pool water evaporation. A typical evaporation rate is 25.5 gal/day for the period November 1983 through April 1984. The beam hole laboratory (room 17) has a separate air conditioner to provide cooling to that area. Heat is supplied to this room by steam unit heaters located near the ceiling. No heating or cooling is provided for the demineralizer room (room 9). Steam for the heating system is supplied from University power plants located at the east and west ends of the campus (see Figure 5-1).

C. Utilities

Electric power is supplied to the facility through a dedicated three phase transformer located inside the reactor site boundary fence (see Figure 5-3). The power is supplied by the West Penn Power Company. An uninterruptable power supply (UPS) system is maintained in the reactor bay as a backup power supply to the building intrusion alarm system.

In the event of a power failure, emergency lighting is provided in twelve places throughout the PSBR building by individual battery packs.

Water is supplied to the facility from the University's water supply from University owned wells located on University property.

Liquid propane gas is supplied to the laboratories from a tank located outside of the building adjacent to storage room 12.

Compressed air is supplied by two air compressors. A $1\frac{1}{2}$ horsepower compressor is dedicated to supply compressed air to the reactor transient rod drive. A 20 horsepower compressor supplies compressed air for general use throughout the building.

Both of these compressors are located in an equipment room (room 18) located under the loading dock adjacent to room 8.

D. Fire Protection

The reactor building is equipped with an internal (local alarm only) fire alarm system. Fire extinguishers of either the CO_2 type or compressed air and water type are located at strategic locations throughout the

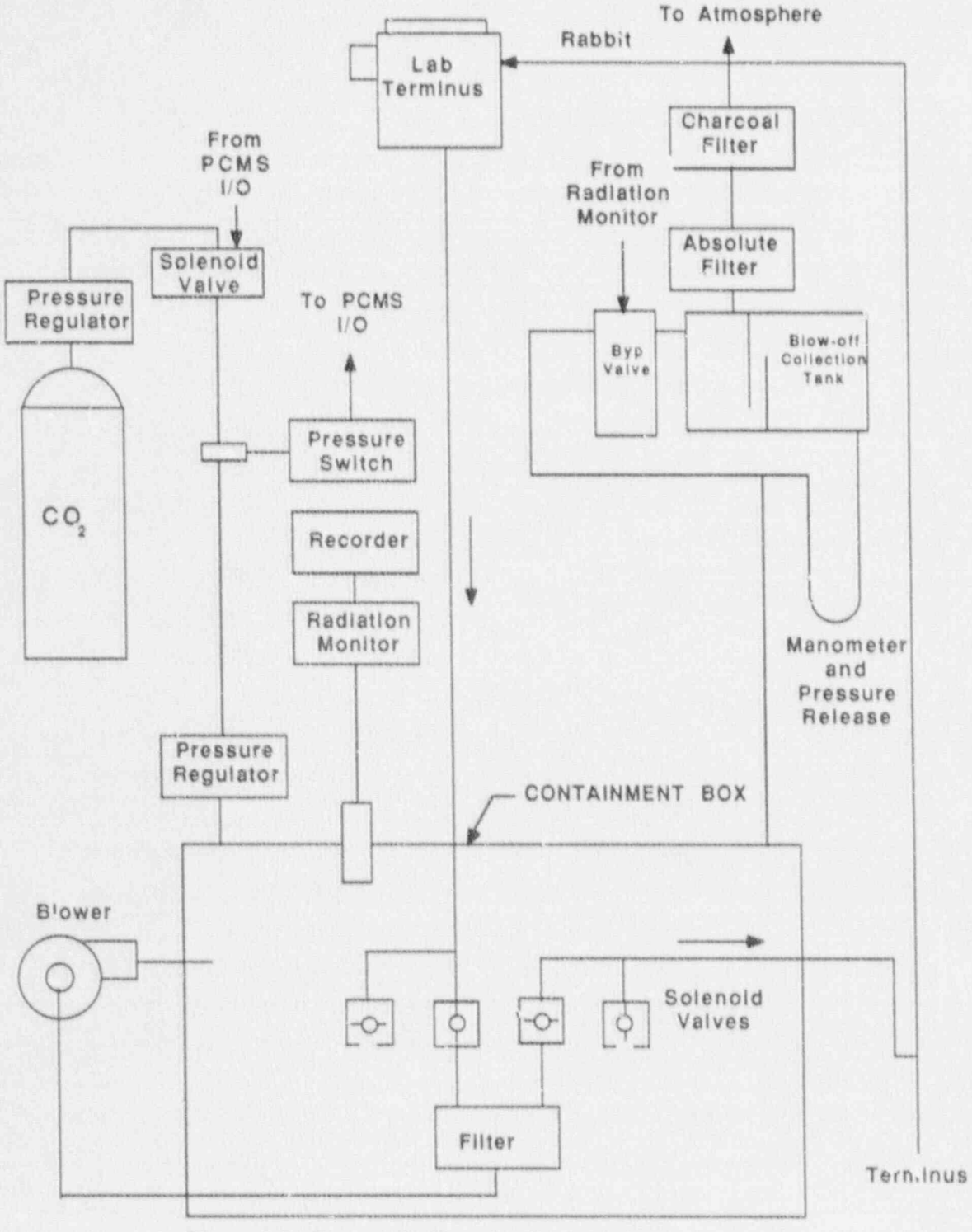


Figure 6-5 Pneumatic Transfer System I

The carbon dioxide working fluid is supplied from a high pressure cylinder through a standard two-stage regulator at about 20 psig to a fixed output regulator mounted on the containment box which further reduces the pressure to a few inches of water. When a pressure sensor between these two regulators senses a pressure less than 15 psig, a LOW GAS PRESSURE light is lit on the reactor console.

With a closed carbon dioxide system, contamination with atmospheric air would lead to argon radioactivity in the system. The laboratory terminus is designed to minimize the entry of air into the system. The terminus is cylindrical and uses "O" ring seals on a sliding internal piston to minimize gas leakage (see Figure 6.6).

Measurements indicate that about one liter of gas per minute is lost through leaks in the system. Concentration of radioactivity in this gas, with the reactor operating at one megawatt, has been measured to be 1.5×10^{-3} μCi/ml resulting in approximately 1.5 μCi/min escaping from the system during its operation.

The DCC-X computer of the PCMS (see Chapter VII) allows operation of the pneumatic transfer system from the keyboard when the operator controls screen is displayed. Master I (on or off) controls the power (through the I/O) to the master relay which in turn permits the transfer fan to be operated by the "Fan On" control. The master relay opens an electrically operated valve which supplies CO_2 to the system, and turns on a chart recorder that records the output of the radiation monitor. The audio is also controlled by the master relay which allows the operator to hear when a sample enters and leaves the core via microphones attached to the system tubing near the core terminus. Verbal communication between the experimenter and the reactor operator is via an intercommunication system.

The experimenter in the laboratory selects either MANUAL or AUTO mode of operation. In automatic mode, a preset timer controls the length of time the sample remains in the core.

A G-M tube in the containment box is connected to a monitor located on the Rabbit I panel in the reactor bay. An alarm on this radiation monitor will send a signal to the PCMS which initiates the following action: (a) prevent blower operation and (b) open an electrically operated valve to bypass the pressure relief manometer so that any pressure in the system is relieved

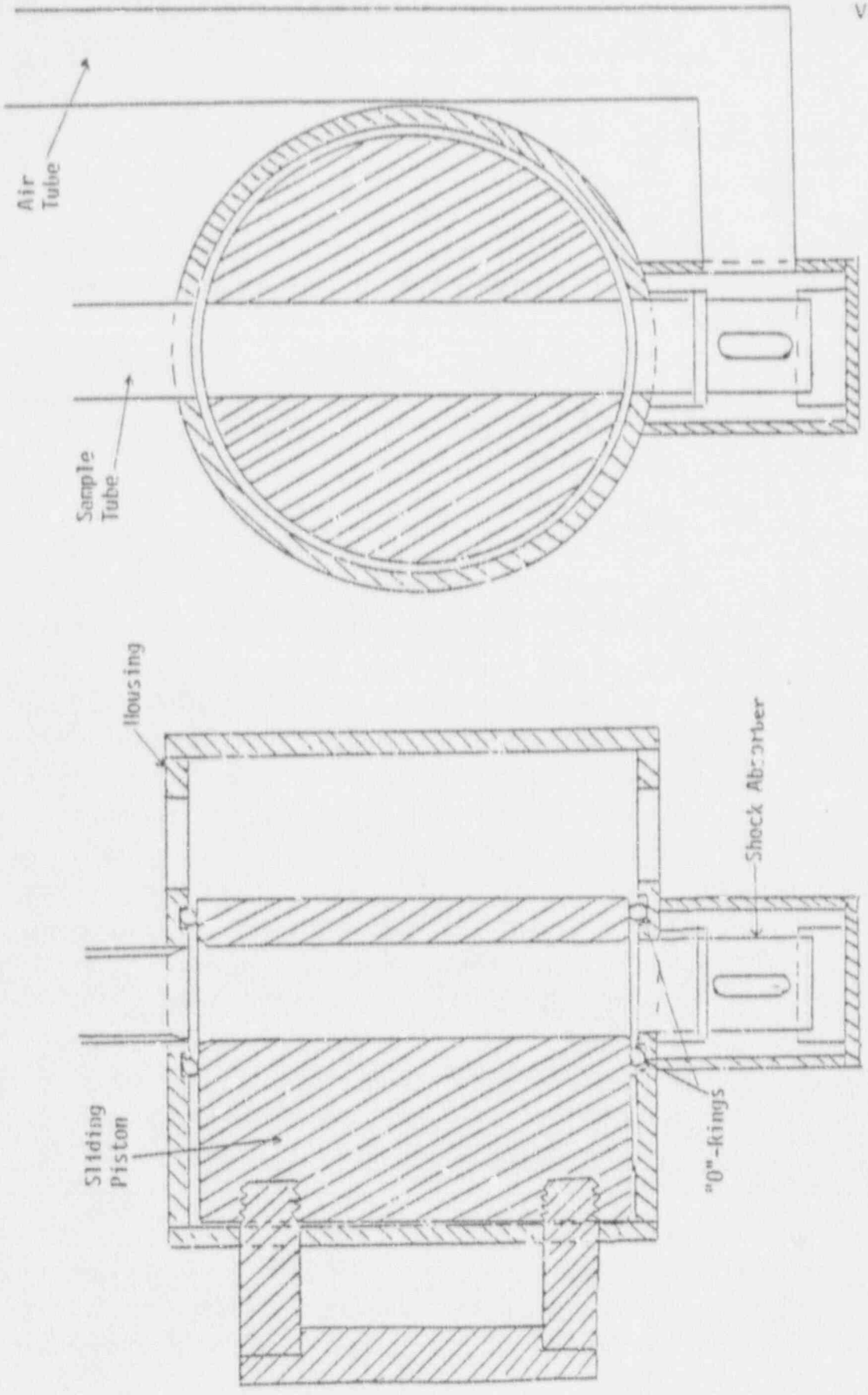


Figure 6-6 Pneumatic Transfer System I Laboratory Terminus

thus minimizing leakage to the building. An ALARM OVER-RIDE control on the DCC-X allows operation of the fan with a radiation alarm.

2. Pneumatic Transfer System II

This pneumatic transfer system provides a means of rapidly transferring samples between the ventilated hood in the reactor bay southeast annex and the reactor core or D_2O tank.

Electro-pneumatic valves control the flow of nitrogen gas in the system to push samples to and from the core (see Figure 6-7). A high pressure cylinder supplies nitrogen through a regulator to a surge tank providing gas to the "sample in" side of the system. Another high pressure cylinder supplies nitrogen through a regulator to a second surge tank providing gas to the "sample out" side of the system.

Irradiation termini consist of a stainless steel reactor core terminus, a cadmium lined aluminum reactor core terminus and an aluminum terminus that fits into the D_2O tank thimble.

The DCC-X computer of the PCMS allows operation of the pneumatic transfer system II from the keyboard when the operator control screen is displayed. Master II supplies power to all the system components. A delay relay prohibits operating for 10 minutes after energizing this switch so the recirculation blower can cool the core terminus before system use begins. The cooling provided by this blower is necessary to prevent softening of the polyethylene capsules when using the stainless steel core terminus at higher power levels. After the 10 minute delay, the reactor operator can operate the FIRE PERMIT control on DCC-X to allow the experimenter to send the samples. The master control also powers the audio which will allow the operator to hear (via microphones attached to the system tubing near each terminus) when the sample enters and leaves a core terminus. Verbal communication between the experimenter and the reactor operator is via an intercommunication system.

The send station, the receive station,and all valves which release gas from the system are housed in hoods equipped with a ventilating system which exhausts to the outside through an absolute filter in the reactor bay.

VII. Reactor Safety, Protection, Control and Monitoring System

A. System Summary

The reactor console described in the following sections (see Figure 7-1) was designed to provide the PSBR with safe and reliable operation in four different modes, Manual, Automatic, Square Wave or Pulse. This system is an upgrade for the original ***TRIGA*** console. This new console utilizes a reliable hardwired analog system for safety related functions. All nonsafety related functions are implemented with computer technology. In this use a safety related function or system is defined as that system or function that must remain operational "....during and following a Design Basis Event (DBE) to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shutdown the reactor and maintain it in a safe condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the 10 CFR Part 100 guidelines"[16].

In specifying the design of the console it was desirable to utilize state-of-the-art digital equipment to improve reliability, increase the flexibility of upgrading and reduce life-cycle costs. In addition, we desired a man-machine interface that would closely parallel that which the students would see in industry. It was also desirable to reduce the duplication of instrumentation by allowing isolated data extraction from the reactor equipment for experimental and laboratory use. In changing the system the goal was to duplicate every existing safety function with hardwired analog equipment.

Two independent systems are provided for the safety, protection, control and monitoring functions. The first, the reactor safety system (RSS) , provides all of the SCRAM and operational interlock functions required by the technical specifications [1]. The RSS is completely hardwired without making use of any software programmable equipment or devices containing embedded microprocessors. The second system, the protection, control and monitoring (PCMS), is fully computerized employing state-of-the-art digital control and monitoring features.

The PCMS consists of two computers, Digital Control Computer X (DCC-X) and its interface equipment and Digital Control Computer Z (DCC-Z). All of the non safety related functions necessary for operation are provided by DCC-X. The DCC-Z is strictly an monitoring computer in "read only" communication

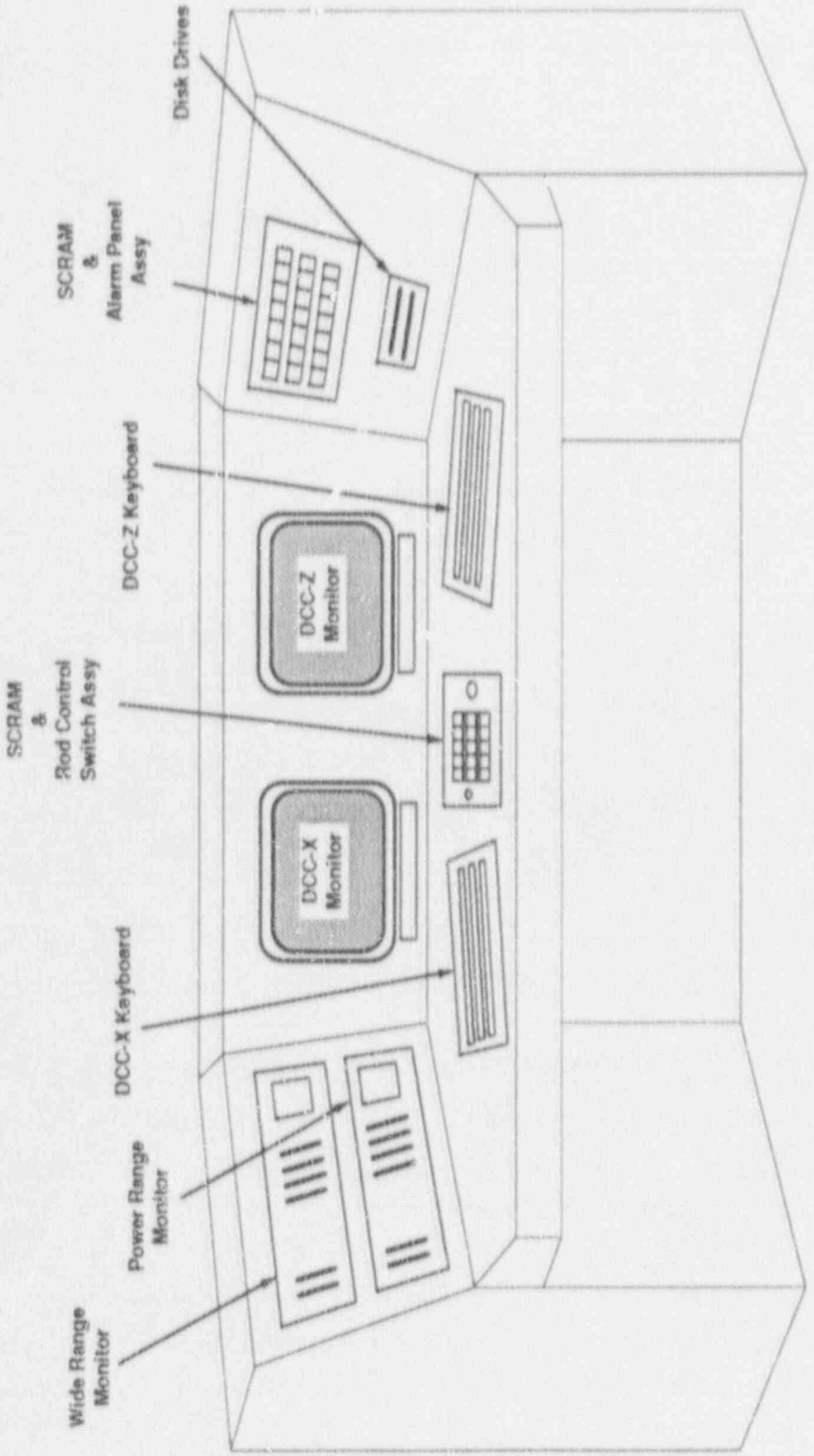


Figure 7-1 PSBR Console Layout

with DCC-X. DCC-Z performs data logging, data display and data broadcast to a local area network. DCC-Z is not required for reactor operation.

The console (see Figure 7-1) houses both the RSS and PCMS with the exception of field transducers and actuator devices.

Safety in depth was a basis of design of the PSBR console. Figure 7-2 is a diagram of the new safety, protection and control system. It was decided that analog electronics, with it's established reliability, would be used for the reactor safety system, RSS. The analog RSS would be the safety related envelope within which the reactor operates. The PCMS computer, DCC-X, with its flexibility and versatility, provides a software protection envelope which continuously verifies the analog RSS with redundant and additional scrams and interlocks. Of course, inside the analog safety related envelope is the core design safety envelope based on the inherent safety of the ***TRIGA*** fuel system. The final envelope of protection is provided by a licensed and highly trained operator using her/his educated judgement and properly written procedures. Any control loops will operate outside the safety and protection envelopes which means that control cannot degrade reactor safety.

The primary indicators of the reactor state are the analog display devices which are wired directly from the analog reactor power and temperature instrumentation. In addition the operator has consolidated information about the reactor state available from the CRT parameter display of the DCC-X computer. As always, the operator will have the final check of the validity of the information by periodically comparing the the analog display devices with the CRT parameter display. Figure 7-3 is a diagram of the old safety, protection and control system. If figure 7-2 and figure 7-3 are compared, the only significant change between the old and the new systems is the addition of the redundant software protection envelope and a CRT parameter display.

There are two power level instruments in the new PSBR digital control system. The wide range power monitor uses a fission detector and covers 10^{-8} % to 200% of 1 MW. The second detector, a GIC, is the input to the power range monitor with a range of 1 to 120% and to the pulse power monitor to a maximum of 2000 MW. In addition, there are two TC inputs from the instrumented fuel element.

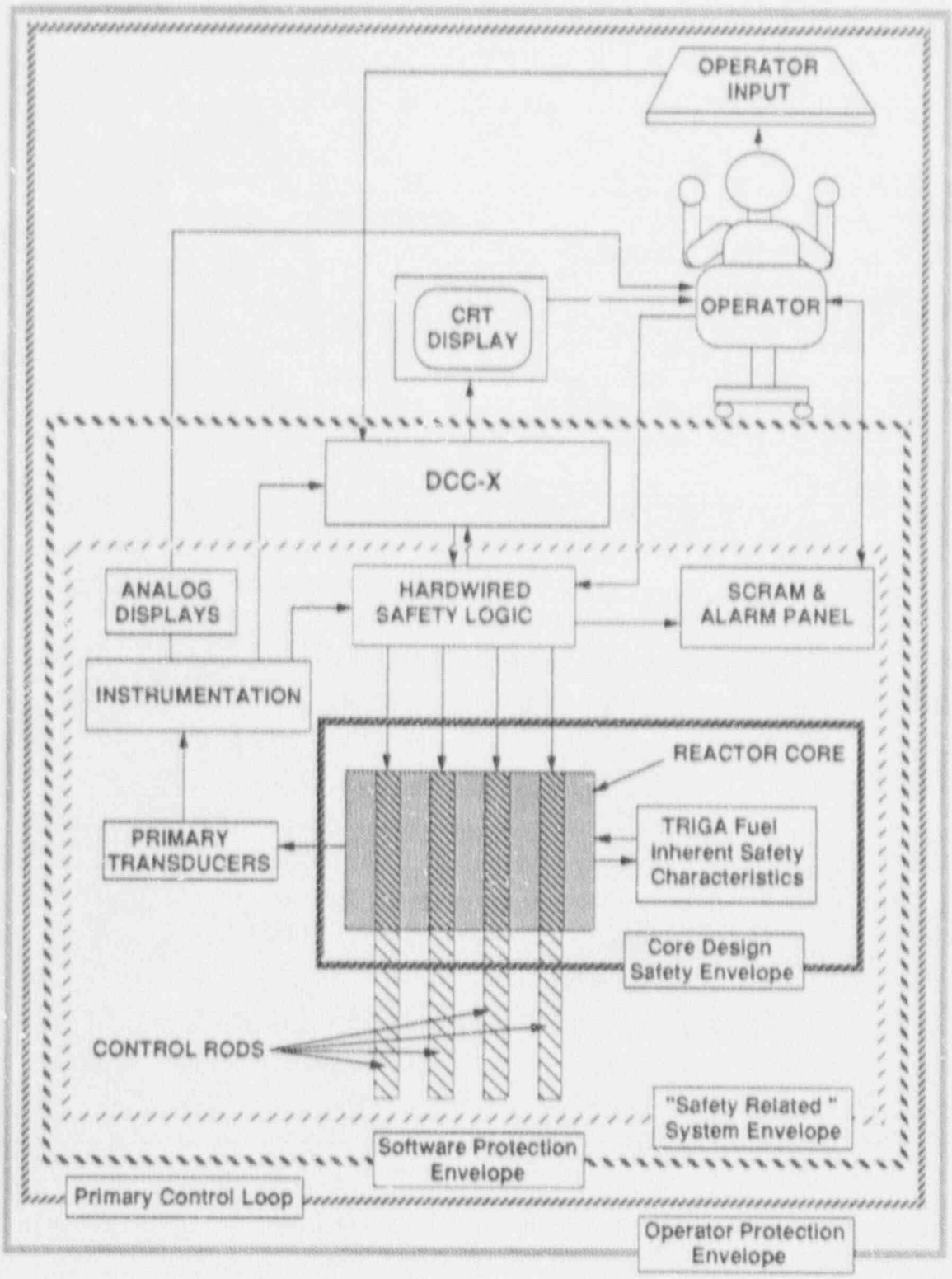


Figure 7-2 New PSBR Safety, Protection and Control System

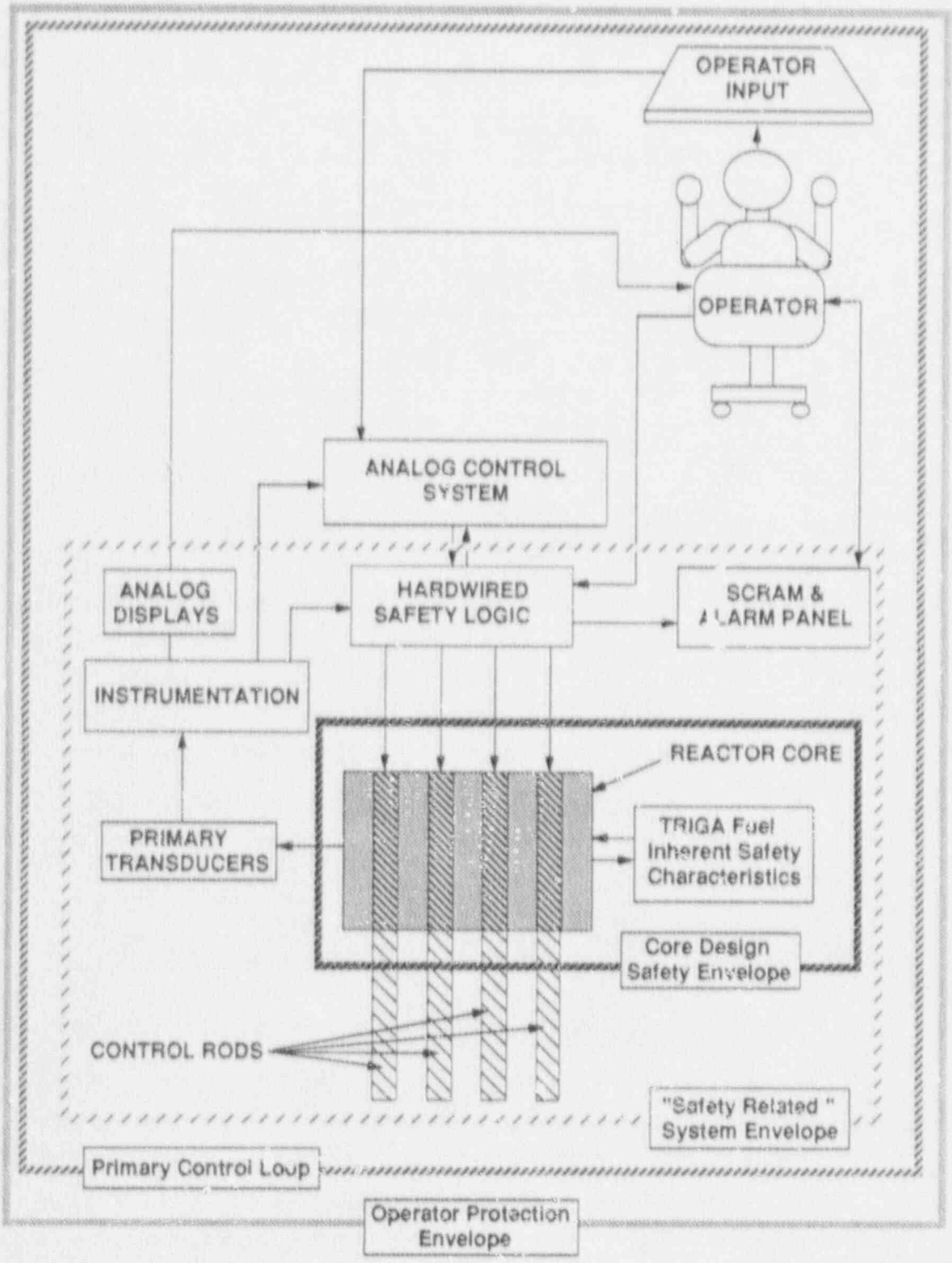


Figure 7-3 Old PSBR Safety, Protection and Control System

B. System Design Philosophy

The following are the basic design principles and philosophy used in configuring and design of the various systems.

(1) The RSS is separated from the control and monitoring system through use of buffered devices and by physical separation to the extent possible within the console.

(2) The RSS is completely hardwired and does not contain any software programmable devices with embedded microprocessors for signal processing or actuation functions.

(3) The RSS logic is designed to fail safe on loss of power.

(4) The functional design of the RSS is unchanged from the present R-2 Technical Specifications. Any enhancements, such as redundancy, to the safety functions or reactor protection functions are done through the PCMS via a DCC-X SCRAM input.

(5) The safety functions are designed to meet the single failure criterion for failures in the RSS crediting both the operable portions of the RSS and the PCMS to mitigate the failure consequences (see section G.2.c.).

(6) The PCMS, consisting of the DCC-X and its interface equipment and DCC-Z, is designed to fail conservative through use of extensive self tests and a watchdog.

(7) DCC-Z, the monitoring computer does not perform any control actions and is buffered from the control computer by use of one way data communications. All connections to external monitoring computer systems are via DCC-Z and hence these systems are also buffered from the PCMS DCC-X computer.

(8) DCC-X is designed to provide all reactor protection, control and monitoring functions necessary for safe operation.

(9) Where practical, design of human interfaces employ consistency in operation methodologies, equipment organization, labelling schemes, etc. to maintain an ergonomic interface for operation and maintenance.

C. Console Function Summary

The console provides the following functions:

- house all equipment associated with the RSS and PCMS with exception of the field devices.

- provide an ergonomic operator interface to control and display devices. Reference [7] was used as a human factors guide.
- serve as a desk with sufficient room for two operators.
- provide EMI shielding and heat removal for the enclosed equipment.

D. RSS Function Summary

The RSS performs the SCRAM and operational interlock functions.

D.1. SCRAM Functions

There are presently four control rods used in the PSBR and can be SCRAMed individually and all together by dedicated manual switches. A SCRAM of all four rods together shall occur automatically under the following conditions:

- Fuel Temperature High (LSS).
- Reactor Power High (Fission Chamber).
- Reactor Power High (Gamma Ion Chamber).
- Loss of Detector Bias Voltage (Fission Chamber).
- Loss of Detector Bias Voltage (Gamma Ion Chamber).
- Pulse Timer timed-out.
- DCC-X Watchdog tripped.
- DCC-X SCRAM request.
- Manual SCRAM pushbutton.
- Reactor Operation Keyswitch Off.

D.2. Interlock Functions

The operational interlocks prevent driving of each rod and applying air to the transient rod under various circumstances. The intent of the interlocks is to prevent unintentional insertions of reactivity through improper operation of the controls governing the rod drives. The following are the interlock functions:

- prevent manual withdrawal of more than one rod when in manual or square wave modes of operation.
- prevent manual withdrawal of any rod when fission chamber count rate is very low or reactor period is short.
- prevent movement of all rods except the transient rod when in pulse mode.
- prevent application of air to the transient if the drive is not fully down when in manual mode.

- prevent application of air to the transient rod in pulse mode if initial power is high.

All interlocks are validated by DCC-X and alarm on failure. The reactor is SCRAMed if a failure is detected.

E. RSS Description

The RSS, which includes the instrumentation, is equipment provided by ***GAMMA-METRICS*** and is designed to provide to the operator:

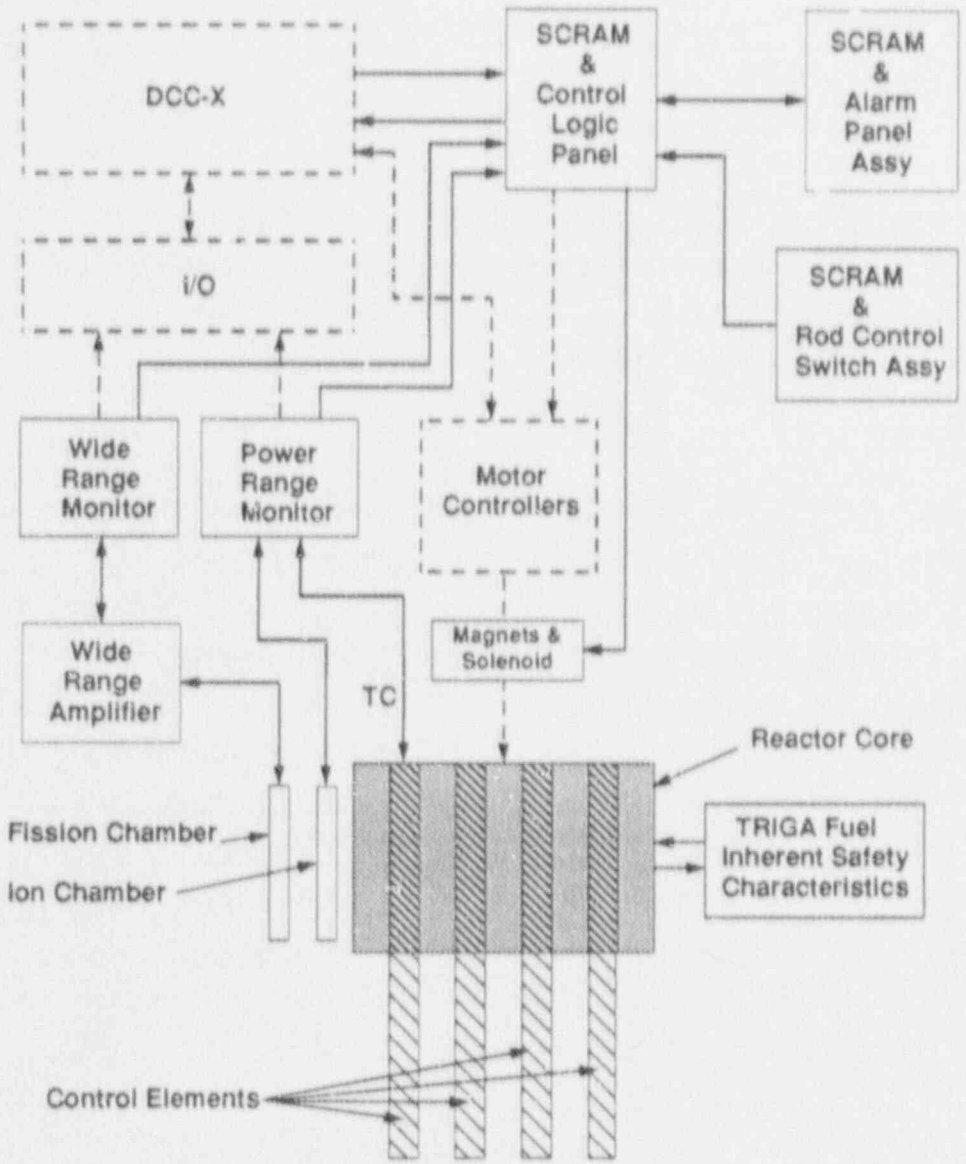
- a measure of the flux level and rate at the Wide Range Detector Assembly from source level (shutdown) to 200% of full power reactor operation.
- a measure of the pulse power at the gamma ion chamber from 0 to 2000 MW.
- a measure of the linear power at the gamma ion chamber from 0 to 120% of full power.
- a measure fuel temperature in degrees Celsius.
- the capability to operate control rods.
- all required safety trips and operational rod interlocks.

The equipment is designed to provide reliable neutron flux measurement from reactor shutdown to reactor full power level (10 decades) in a harsh environment. It is designed to measure neutron flux with the detector in a high gamma radiation and electrical noise environment, to measure the fuel temperature, and to provide controls and annunciators for rod movement. The RSS is entirely hardwired analog equipment and has no embedded microprocessors. It is designed to operate for 40 years under normal conditions.

Figure 7-4 contains a functional block diagram of the RSS. The following paragraphs contain a general description at the block diagram level.

The RSS is divided into four functional subsystems:

- the Wide Range Channel, consisting of the Wide Range Detector Assembly, Wide Range Amplifier, and Wide Range Monitor,



Note: The dashed components are not part of the RSS

Figure 7-4 Functional Block Diagram of RSS

- the Power Range Channel, consisting of a gamma ion chamber, in-core thermocouples, and the Power Range Monitor,
- the Control and Alarm Subsystem, consisting of the SCRAM and Rod Control Switch Assembly, and SCRAM and Alarm Panel Assembly, and
- the Power Distribution System consisting of AC power distribution panels and a DC power supply.

E.1. Wide Range Monitor Description

The wide range signals originate from the fission chamber of the Wide Range Detector Assembly located near the reactor core. This produces a series of pulses representing the power being generated in the reactor. These pulses are applied to the Wide Range Amplifier, located on the reactor bridge, which processes and amplifies the pulses; it then applies them to the Wide Range Monitor, installed in the Console Assembly. The Wide Range Monitor further processes the signal pulses to produce a front panel visual indication of the percent power (on a square root scale), fraction of full power (on a logarithmic scale, 10^0 corresponds to 1 MW), and the rate of change of reactor power. The Wide Range Monitor has built in test and calibrate capability and provides safety trip and operational interlock signals to the control and alarm subsystem when preset trip level setpoints are exceeded.

The Wide Range Monitor measures the number of pulses per unit time from the Wide Range Detector Assembly over the range from source level to the level where the error from the countrate loss due to coincident pulses becomes unacceptable. From about two decades below the upper end of the countrate range to full power, the Wide Range Monitor measures the mean square value of the time variant signal from the detector. This mean square value is proportional to the average rate of neutron pulses and is not dependent on the pulses being individually identifiable. It also provides good discrimination against alpha and gamma signals.

The derivative of the logarithm of reactor power provides a measurement that is proportional to the change in reactor power per unit time. The signals are displayed on the Rate bargraph in decades per minute.

The meters on the front panel of the Wide Range Monitor provide a display of the following signals:

Display	Signal
Power Range	Square Root Percent Power
Wide Range Log	Log Percent Power
Wide Range Rate	Rate of Change, DPM

Three dual bargraphs in the Wide Range display the measured variables and the trip setpoints. The left bargraph shows the magnitude of the measured variable in orange. The right bargraph shows the trip setpoints in red. Two trip set points are provided for each measured variable. The first setpoint is normally displayed. The second setpoint can be displayed by pressing the Trip 2 switch. The measured variable is in an alarm condition when the endpoint of the orange bargraph is within the range of the red, lighted portion of the alarm bargraph and/or the voltage to the input of the card exceeds the alarm setpoint voltage. The rate bargraph will flash when its display exceeds either of the two setpoints.

Output signals from the Wide Range Monitor are input to the digital PCMS, supplied by ***AECL Technologies*** in the Console Assembly. The digital PCMS provides redundant protection trip commands and reactor rod position control signals to the Control and Alarm Subsystem.

E.2. Power Range Monitor Description

The Power Range Monitor receives a power signal from a gamma ion chamber to provide a linear power output of 0 to 120 percent power and a pulse power output of 0 to 2000 MW. It also provides fuel temperature displays in degrees Celsius, the signals come from two out of three available Type K in-core fuel thermocouples. There is a trip select switch on the front panel to select which of the two fuel temperatures will provide the trip signal to the SCRAM and Control Logic Assembly. The Power Range Monitor has built in test and calibrate capability and generates reactor safety trip signals to the control and alarm subsystem when preset trip level setpoints are exceeded.

The meters on the front panel of the Wide Range Monitor provide a display of the following signals:

Display Signal	
Power Range	Linear Percent Power
Fuel Temperature 1	No. 1, Degrees C
Fuel Temperature 2	No. 2, Degrees C

Three dual bargraphs in the Power Range Monitor display the measured variables and the trip setpoints. The left bargraph shows the magnitude of the measured variable in orange. The right bargraph shows the trip setpoints in red. Two trip set points are provided for each measured variable. The first setpoint is normally displayed. The second setpoint can be displayed by pressing the Trip 2 switch. The measured variable is in an alarm condition when the endpoint of the orange bargraph is within the range of the red, lighted portion of the alarm bargraph and/or the voltage to the input of the card exceeds the alarm setpoint voltage. The rate (period or DPM) bargraph will flash when its display exceeds either of the two setpoints.

Output signals from the Power Range Monitor are input to the digital PCMS supplied by ***AECL Technologies*** in the Console Assembly. The digital PCMS provides redundant protection trip commands and reactor rod position control signals to the Control and Alarm Subsystem.

E.3. Control and Alarm Subsystem Description

The Control and Alarm Subsystem consists of the SCRAM and Control Logic Assembly, SCRAM and Rod Control Switch Assembly, and SCRAM and Alarm Panel Assembly.

E.3.a. SCRAM and Control Logic Assembly Description

The SCRAM and Control Logic Assembly contains all the relays necessary for safety trips from the Wide and Power Range Channels, from manual SCRAMs and from automatic SCRAM functions provided by the PCMS. The SCRAM and Control Logic Assembly also contains relays necessary for reactor rod movement operation, both manually and automatically.

E.3.b. SCRAM and Rod Control Switch Assembly Description

The SCRAM and Rod Control Switch Assembly also contains the Manual SCRAM switch which removes power from the magnetic couplers on the Safety, Shim and Regulating control rods and from the solenoid valve, dumping air from the Transient control rod. The SCRAM and Rod Control

Switch Assembly also contains the rod control UP and DOWN manual control switches and the individual SCRAM switches for each control rod. The SCRAM and Rod Control Switch Assembly, contains a keylock switch which provides the functions of OFF, OPERATE, and RESET for reactor operation.

E.3.c. SCRAM and Alarm Panel Assembly Description

The SCRAM and Alarm Panel Assembly, contains annunciator lamps for display of the trip status of each control rod, for the DCC-X Watchdog SCRAM and for visual indication of trip status from individual spare inputs. The panel contains indicator lamps for display of EVACUATION INITIATED, HIGH POWER SCRAMs BYPASSED and of POWER ON. The panel also contains pushbutton switches for LAMP TEST, LOW COUNTRATE DEFEAT and EVACUATION INITIATE.

E.4. The Power Distribution System

The 24 Volt Power Supply Assembly contains the 24 Vdc source which powers all indicator lamps, all relays in the Scram and Control Logic Assembly and provides power to actuate the control rod electromagnets and to operate the transient rod air solenoid. The 24 Volt Power Supply Assembly also contains a relay which provides contact outputs for an external evacuation alarm.

F. PCMS Function Summary

The PCMS consists of the following basic equipment:

- a control computer (DCC-X) system with hardware I/O and CRT / keyboard operator interface.
- a redundant monitoring computer (DCC-Z) system with a CRT / keyboard operator interface, printer, hard disk and serial and LAN communications.
- motor and associated controller for each of the four control rod drives.

Figure 7-5 shows the hardware configuration of the PCMS and interfaces to other systems. All signal interfaces to the PCMS shall be through the hardware I/O of DCC-X. DCC-Z shall receive all its signal data from DCC-X via a "one way" serial link using a broadcast type protocol. The "one way" serial link means that DCC-X cannot physically receive any communications from DCC-Z hence DCC-X is buffered from the effects of failures in DCC-Z or connected systems. It is intended that reactor operation is permissible with the DCC-X and with or without DCC-Z.

Basic summaries of the functions for DCC-X and DCC-Z are given in the sub-sections below.

F.1. DCC-X Functions

The PCMS is designed so that all technical specification [9] required functions are performed by DCC-X without reliance on the DCC-Z computer system. In the case of failure of DCC-X, DCC-Z can be used to replace DCC-X and continue operation. The replacement can only be done by physically and electrically changing computers.

The following functions are performed by DCC-X:

F.1.a Reactor Control and Regulation

There are four modes of operation:

Manual: all rods are controlled manually with the up and down pushbuttons.

Auto: various combinations of the rods are controlled automatically with manual control provided for the rods that are not being used for automatic control functions. Three combinations of rods are available for automatic control. The transient rod is never under automatic control.

1 Rod Auto -Regulating rod controlled with the shim and the safety "shimmed".

2 Rod Auto - Regulating and shim rods banked for automatic control and the safety rod "shimmed".

3 Rod Auto - Regulating , shim and safety rods banked for automatic control and no "shimming" rod.

Square Wave: a square shaped power trend is initiated by firing the transient rod to provide a step increase in power. This is followed by auto control of power at a fixed setpoint for a pre-selected time. The power trend is then automatically or manually terminated by a reactor SCRAM.

Pulse: a power pulse is produced by firing the transient rod to give a super critical step increase of reactivity. All other rods are frozen in position. A pulse profile is developed due to the prompt negative temperature reactivity from the fuel as it heats up.

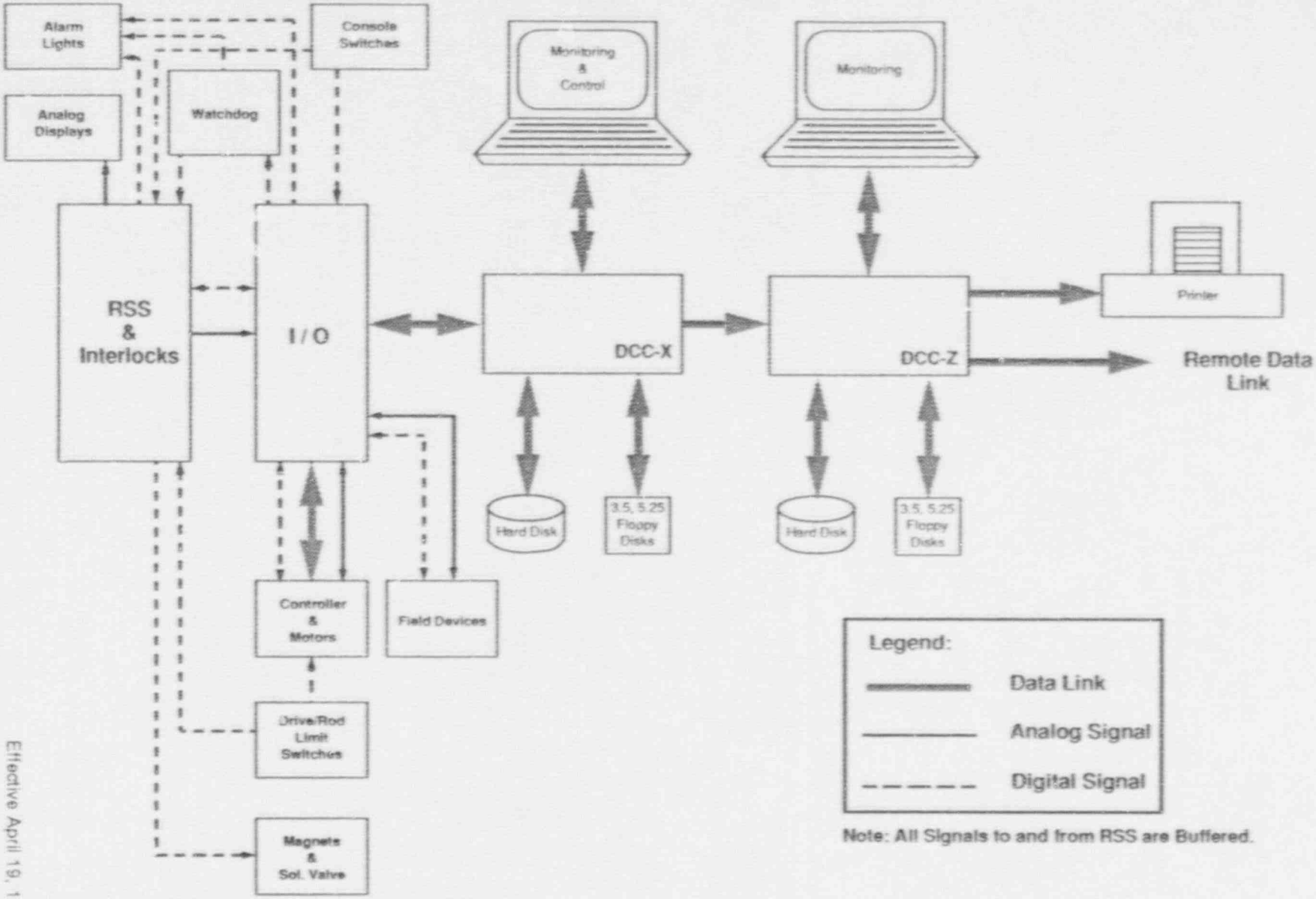


Figure 7-5 PCMS and Interfaces to Other Systems

DCC-X shall control the rod drive velocities for all manual and automatic control functions.

F.1.b. Reactor Protection

All of the operational interlocks and safety trips, that are required by the technical specifications [1], are performed by the hardwired RSS. The PCMS computer, DCC-X, validates the operation of the RSS by performing the same logic as the RSS. If there is a failure of that validation a DCC-X SCRAM request is issued to the RSS, causing a SCRAM. This is redundancy beyond the original RSS and is not required by the technical specifications [1]. In addition, the PCMS initiates SCRAMs, by the DCC-X SCRAM request, for conditions other than reactor safety, i.e. radiation alarms. In these cases the functions initiated by the PCMS are not appropriately classified as part of the safety system so it is more correct to designate them as protection functions.

(a). Reactor Stepback

A reactor stepback function is used to mitigate events that may lead to a RSS Trip or diminished control. The stepback is performed by driving all rods except the transient rod at high speed into the core. The stepback not only prevents operation, but also shuts down the reactor if it is already in operation. The following conditions initiate a stepback:

- Fuel Temperature High.
- Reactor Power High (Fission Chamber).
- Reactor Power High (Gamma Ion Chamber).
- Excessive Power Spread (between the Fission Chamber and the Gamma Ion Chamber).
- Reactor Operation Inhibit.

A bypass is provided to allow testing the RSS SCRAMs without causing a stepback. The bypass is allowed only in manual mode and has an automatic time out feature.

The inhibit condition is imposed in various operational situations (see section F.1.b.d.ii.).

(b) Reactor SCRAMs

A DCC-X SCRAM request will be given to the RSS in the following conditions:

- Fuel Temperature #1 or #2 High.
- Reactor Power High (Fission Chamber).
- Reactor Power High (Gamma Ion Chamber).
- Pulse Timer timed-out.

Radiation High from one of the following:

- East Bay Monitor.
- West Bay Monitor.
- East Air Monitor.
- West Air Monitor.
- Neutron Beam Lab Monitor.
- Co-60 Lab Monitor.

- Emergency Evacuation Button.
- Remote Pushbutton (1 of 4).
- Reactor Bay Truck Door Open.
- Both East and West Facility Exhaust Fans Off.
- Interlock Validation Failure.
- Rod Velocity Signal Failure.
- Rod Motor Overspeed.
- Square Wave Termination Request.

To allow testing of the RSS logic, a testing bypass is provided for the DCC-X SCRAMs as specified for the stepback function (see above).

(c) Reactor Interlocks

All of the operational interlock logic in the RSS is validated by DCC-X. DCC-X monitors all of the inputs and outputs of the hardware logic and performs the identical logic in software. If a validation failure is detected, a SCRAM is requested.

The DCC-X control logic is designed to avoid signal outputs that are in violation with the RSS interlocks.

(d) Facilities Systems Support

The following functions are performed for control and monitoring of various systems in the reactor facility:

(i) Emergency Evacuation

An emergency evacuation is initiated on high radiation or manually from a switch on the console. Following initiation these listed actions occur:

- evacuation horn is energized.
- emergency exhaust system is turned on.
- alarm light on console is lighted.
- alarm is sent to police services.
- facility exhaust system is secured.

(ii) Reactor Operation Inhibit

Reactor operation is inhibited by initiating a reactor stepback when an inhibit condition exists. The inhibit conditions cover the following situations:

- keyswitch is off.
- a radiation hazard from the neutron beam ports exists.
- both east and west bay or air radiation trips are defeated.
- pool temperature is high.
- reactor bay truck door is open.

(iii) Manual Controls

Manual control of the following devices is provided:

- east and west facility exhaust fans.
- N-16 diffusion pump.
- neutron beam lab CCTV camera and monitor.
- rabbit system controls.

(iv) Operating History Records

The following parameters are continually updated:

- integrated power.
- total time that the reactor was critical.
- total operating time (i.e. time that the keyswitch was in the operate position).

(v) Police Services Notification

The following operational conditions will initiate a signal of notification to Penn State University Police Services:

- evacuation initiate.
- reactor pool level #1 low.
- reactor pool level #2 low.
- reactor pool level high.
- intrusion alarm.
- intrusion tamper alarm.
- UPS-1 low battery.
- UPS-2 low battery (spare).
- waste tank level high.
- Co 60 pool level low.

(e) Alarms

Two types of alarms are provided, status alarms and state transition alarms. Status alarms are like traditional hardwired window alarms. Summary displays of alarm points are given to indicate the present state of these alarms. State transition alarms are chronological lists of alarm messages which are issued whenever an alarm point changes state.

(f) Operator Interface

The operator interface is through the analog instrumentation displays, DCC-X CRT display, the DCC-X keyboard and hardwired control switches. All operator inputs are performed with the keyboard except for the following:

- manual SCRAM switches.
- rod drive up and down switches.
- operation keyswitch.
- emergency evacuation switch.
- low count rate interlock defeat switch (provided to allow rod movement with a subcritical core).

Special operator displays are provided to give reactor status information as required for the various operator tasks.

The generic ***PROTROL*** maintenance display system are also provided with the following features:

- system utilities.
- time trends.
- bar charts.
- message log.
- tuning interface.

(g) Self Testing

The following standard ***PROTROL*** self tests are performed:

- control functions executed twice on startup.
- I/O checks.
- check watchdog contact open on startup before resetting the watchdog timer.
- disk operation error handling.
- serial port operation error handling.

In addition to the standard checks, continuous analog feedback checks of the velocity signals to the motor controllers are performed.

F.2. DCC-Z Functions

DCC-Z provides redundant monitoring capability plus enhanced monitoring features not available on DCC-X. Reactor control functions are not available from DCC-Z.

DCC-Z contains the same operator displays as DCC-X modified as necessary to exclude the control functions. The operator displays of pulse trends also include the capability to retrieve up to 10 most recent historical pulse trends.

DCC-Z has available the same standard ***PROTROL*** maintenance displays as DCC-X plus the additional historical trends. The message log includes all messages from DCC-X as well as DCC-Z.

DCC-Z transmits selected signals periodically onto the local area network for use by other machines connected to the LAN.

G. Systems Operation Description

Three operational subsystems are provided to perform the functions of the original console.

(a) Reactor Safety System composed of the following hardware:

- A fission chamber, a pre-amp and a signal processor measures power over a 10 decade range with log of ffp, linear (linear on the PCMS CRT displays, percent full power on a square root scale bargraph on the Wide Range Monitor front panel) and log-rate signal outputs.
- A gamma ion chamber with its amplifier and a fuel temperature signal processor provides linear power, pulse range power and two fuel temperature signal outputs.

- A hardwired reactor safety system which uses relay logic to perform SCRAM and operational interlock functions.

(b) PCMS:

PCMS availability is not of paramount concern and hence a single protection and control computer configuration is provided with a separate and redundant monitoring computer (see figure 7-5). The PCMS computer is designed with extensive self testing and employs a fail conservative watchdog for high reliability against nonconservative failures.

The monitoring computer is buffered from the PCMS computer by receiving all signal data from the PCMS computer via a one way serial link. (A CRC protocol is used to reduce errors in transmission.) No failure in the monitoring computer can propagate back to the PCMS computer. The monitoring computer also employs extensive self testing to assure high reliability of information display. Bad data is highlighted through status annunciation.

The monitoring computer is provided with hardware and software for connection to a local area network (LAN). This allows remote computers on the LAN to access signal data from the buffered monitoring computer without the possibility of affecting PCMS computer operations.

The PCMS configuration is designed to make the most of the enhanced protection, control and monitoring features provided by digital technology. Such features include graphic operator displays, an advanced control algorithm, historical data storage and secure network communication of data to remote computers.

(c) Console:

Figure 7-1 shows the front view of the console. The console is composed of left wing, center and right wing sections with the wings angled in to aid in reading their displays.

The RSS analog bargraph displays and testing controls are located in the left wing section. The center section contains the DCC-X and DCC-Z CRT/ keyboard interfaces and the rod control switches. The right wing section contains the hardwired alarm lights, infrequently used switches and floppy drives.

Figure 7-6 shows the back view of the console and arrangement of the major components. Looking from the back, the three sets of racks contain the control and monitoring system equipment. The right set of racks contain the RSS equipment.

A matching free standing rack contains the radiation monitoring equipment in the control room.

G.1. Reactor Safety System Description

The reactor safety system (RSS) shuts down the reactor (SCRAM) and inhibits movement of the rods when required by operational interlocks. The RSS is a completely hardwired system with no software programmable components or embedded microprocessors. All signal connections between the RSS and the PCMS are buffered through relays (for digital signals) or isolators (for analog signals).

A SCRAM is carried out by decoupling the control rods from their drive mechanisms allowing them to drop under gravity to their position of largest negative reactivity. The Regulating, Shim and Safety rods are coupled to their drives by electromagnets. The transient rod is coupled to its drive by air pressure applied to its cylinder via a solenoid valve. The SCRAM logic opens relay contacts to deenergize the electromagnets and the solenoid valve.

The control rod operational interlocks are implemented through contacts to the motor controllers and transient rod solenoid valve logic. These signals are controlled through relay logic, to prevent conditions which may lead to unintentional operation. The interlock logic is validated by DCC-X which will SCRAM the reactor on detecting a failure.

The RSS equipment occupies the entire left wing of the console (viewed from the front) and uses its own dedicated 120 Vac and 24 Vdc power supplies. Some of the switch inputs are located in other portions of the console for human factors reasons.

G.2. RSS Relay Logic Design

There are six separately fused circuits to divide the current load. The SCRAM and operational interlock functions are on separate fuses.

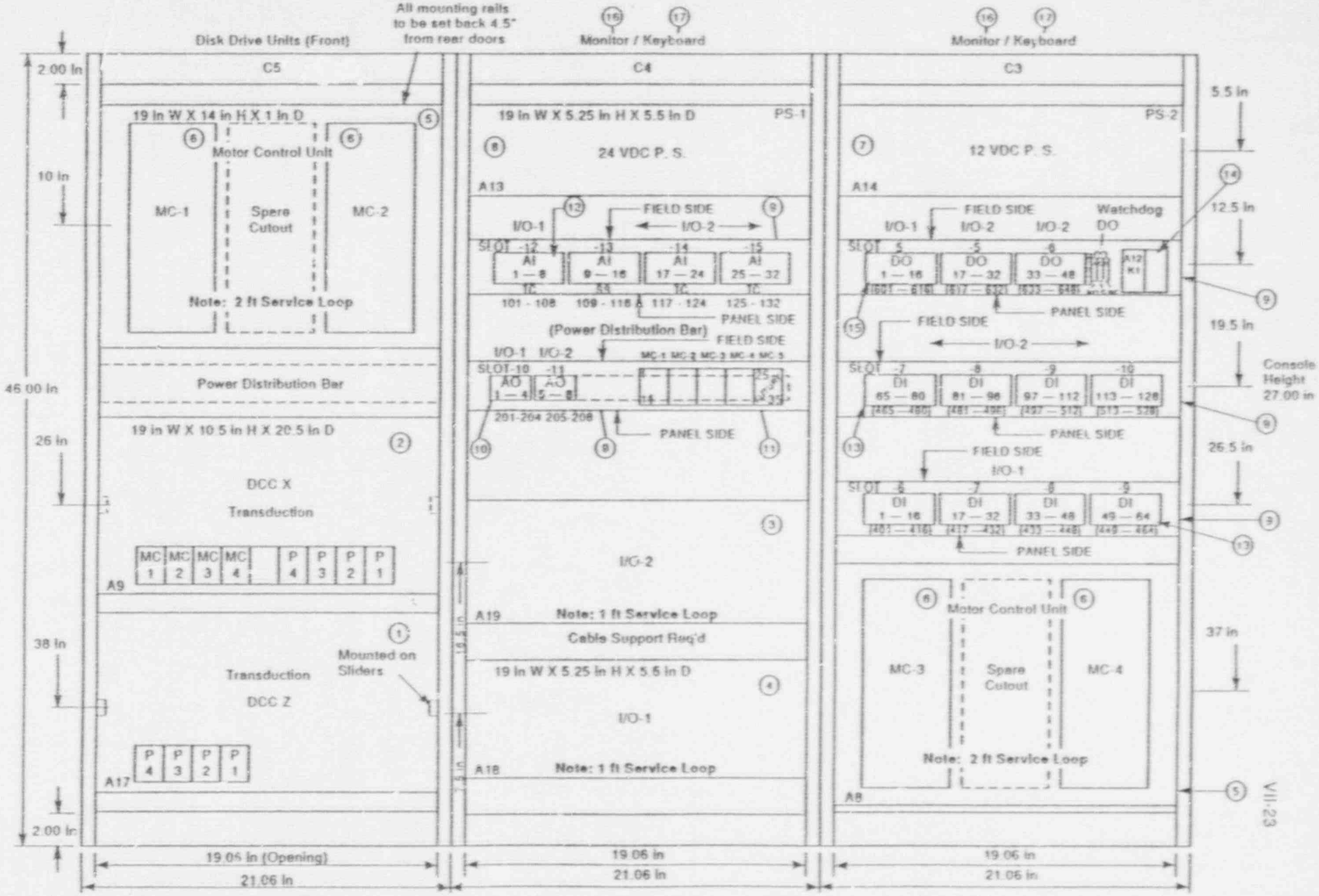


FIGURE 7-6 CMS EQUIPMENT LAYOUT (CONSOLE REAR VIEW)

(BILL OF MATERIAL 17-60501-01-001-BM-A)

901379

All lights on the alarm panel (right wing of the console) are driven from the RSS logic. A lamp test button tests all lights. Two blocking diodes are incorporated in the lamp test circuit. One is to prevent the logic for individual lamps driving other lamps through the test circuit and the other provides added insurance in preventing lamp test operation from back feeding into other logic.

A number of trip functions in the RSS logic employ latches requiring manual action to reset. Many logic states are also latched in DCC-X software. The reactor operate keyswitch resets all latches in the RSS and DCC-X software. The switch should generally be held in the reset position for 2 seconds to ensure that the slower DCC-X read and reset command tasks.

G.2.a. SCRAM Logic

The SCRAM logic is designed to meet the single failure criterion. The SCRAM logic fails safe on loss of power or open circuit. The voting logic for redundant parameters (including the DCC-X SCRAM) is separated into two circuits so that any single short between two points in the system can affect only one of the redundant parameters. The arrangement of parameters into the two circuits is as follows:

SCRAM Circuit #1	SCRAM Circuit #2
DCC-X Watchdog Trip	DCC-X SCRAM
FC Power High	GIC Power High
FC Bias Voltage Low	GIC Bias Voltage Low
Manual SCRAM	Keyswitch Off
Fuel Temperature High	2 Spare SCRAMs
Pulse Timer SCRAM	
2 Spare SCRAMs	

The DCC-X watchdog trip is a combination of a digital output and two watchdog relay contacts, all wired in series ("OR" configuration for trip) for enhanced reliability. The digital output allows the software to provide a quick trip signal independent of the watchdog relay. The watchdog relay covers software failures as well as hardware failures, but may take ≈ 2 seconds to issue the trip signal after a fault occurs.

The pulse timer SCRAM and watchdog trip employ latching logic so that the initiating condition is not needed to maintain the tripped state. The hardware latch for the watchdog eliminates dependence on the software for the latching function. DCC-X software must be re-started following a watchdog trip before it will resume updating the watchdog.

The pulse timer latch ensures that once started, the timer will time out independent of the the initiating signal from DCC-X or the keyswitch reset. This feature is used during testing to distinguished between the pulse timer SCRAM from DCC-X and RSS. The logic is tested by initiating a zero reactivity pulse. The DCC-X pulse timer SCRAM times out first. The DCC-X SCRAM can then be reset without resetting the RSS timer, allowing a subsequent check of the RSS logic when it times out later.

There is logic to bypass both high power SCRAMs in pulse mode. The bypass is performed by DCC-X which drives separate digital outputs to bypass each high power trip. A hardwired alarm light provides continuous indication of the bypass. DCC-X validates the bypass logic of both trips by reading back the bypass state through digital inputs. A failure generates a status alarm on the CRT.

There are two fuel temperature measurement channels provided for the RSS logic; however only one is used for the RSS SCRAM. A latching switch on the front panel of the console (power range chassis) selects 1 of 2 temperature measurement channels .

The SCRAM final voting logic is similar for each rod. The voting is an OR gate of the circuit #1 and #2 SCRAMs, individual rod SCRAM button and the latching logic. The individual manual SCRAM button is wired into the final voting directly from the pushbutton contacts to maximize reliability. The rod SCRAM latch cannot be reset unless the initiating conditions have cleared.

The final SCRAM voting logic deenergizes the electromagnets for the Reg, Shim and Safety rods directly. For the transient rod, the final SCRAM voting provides a signal to the air permissive logic. A contact from the air permissive relay is wired in the solenoid valve circuit to execute the transient rod SCRAM.

The state of all SCRAM parameters and final voted logic is fed back to DCC-X via digital inputs for annunciation purposes. The hardwired alarm windows indicate the final SCRAMed state of the individual rods.

G.2.b. Transient Rod Air Interlock Logic

The transient rod air interlock logic drives the air permissive relay. The transient rod SCRAM overrides all other permissives by unconditionally deenergizing the permissive relay. The logic is designed to fail safe on loss of power. Contacts must close to allow application of air to the transient rod.

The permissive conditions for applying air are as follows:

- in pulse mode AND initial power low.
- transient rod drive is at its bottom end of travel.
- in square wave mode.
- air has previously been applied (permissive latch).

The permissive latch is required to allow continued application of air following a pulse, and during manual driving of the transient rod. In both cases, the permissive conditions would otherwise be lost and the transient rod would drop. If air is initially applied in accordance with the permissives, continued application of air is allowed regardless of the state of the permissives.

DCC-X drives the contact requesting air to the transient rod. The above air permissive logic is also duplicated in software for the air request signal. In addition, the hardware logic is validated through a separate task in DCC-X which will SCRAM the reactor on validation failure.

G.2.c. Rod Drive Interlocks

The rod drive interlocks are shown on sheets 005..008 of reference [15]. The logic for the Regulating, Shim and Safety rods is similar. The logic for the Transient rod differs slightly from the others.

The rod drive interlock logic is not totally designed to fail safe on loss of power since power must be applied to the motor controller digital inputs to perform the inhibit function. The logic is thus a combination of negative (open contact is true) and positive (closed contact is true) logic. The lower reliability of this arrangement is compensated by the interlock validation in DCC-X and by the use of redundant software interlocks for the demand velocity signal. The reactor is SCRAMed on interlock validation failure. The software interlocks in DCC-X make use of separate end-of-travel (EOT) switch contacts that are configured to fail safe on loss of power.

The rod drive pushbuttons provide independent contacts for the RSS interlock functions and manual drive via DCC-X software. Normally closed contacts are used for the interlock functions so that the interlocks fail safe. Normally open contacts are used for the inputs to DCC-X so that power supply failure will not give a spurious drive request. For the Regulating, Shim and Safety rods, up and down drive are inhibited under the following conditions:

Up Drive Interlocks:

- "up" EOT is reached (drive limit switch)
- watchdog trip
- more than one "up" pushbutton is pressed
- low count rate (and not defeated by pushbutton)
- short reactor period
- in pulse mode

Down Drive Interlocks:

- down EOT is reached (drive limit switch)
- in pulse mode

If more than one "up" pushbutton (third "up interlock" above) is pressed, the logic blocks manual up drive of all rods regardless of whether or not the rods are being used for automatic control. Rods being driven under automatic control are not affected.

Up and down drive inhibits for the transient rod are the same as above except there is no interlock on pulse mode and the transient rod is not driven under automatic control.

Rod drive interlock validation is performed for the up drive interlocks of each rod. The pulse mode signal is also validated separately. A failure of any of these validations will result in a DCC-X SCRAM request.

H. PCMS Hardware Description

Figure 7-5 shows a block diagram of the PCMS hardware and interfaces to the other systems. The PCMS is composed of two computer subsystems called DCC-X and DCC-Z and the motor controllers for the four rod drives.

DCC-X is the control computer which handles all control logic and the input/output (I/O) interface signals to the field, rod drive motor controllers and RSS. The DCC-X computer system provides all the functions necessary for safe control and monitoring operation of the reactor.

DCC-Z is the monitoring computer receiving its signal information from DCC-X via a one-way serial data link. DCC-Z broadcasts signal information onto a local area network for use by other computer systems. DCC-Z buffers the other computer systems from DCC-X ensuring that failures in DCC-Z or the other systems cannot affect reactor operation.

H.1 Computers

The central element in each DCC is an ***IBM*** PC/***AT*** compatible allowing use of the many special purpose plug-in cards available for this type of

computer. The computer has a modular design and a passive back plane for easy "board swap" or module replacement repair. All cards including the processor are plugged into the passive ***AT*** bus back plane.

Each computer system is equipped with an ***AT*** 101 enhanced style keyboard, 40 Mbyte hard disk drive and two floppy disk drives (1.2 M byte 5.25" and 1.44 Mbyte 3.5" floppy drives). The 5.25" floppy disk drive is mounted in the console. The keyboard has a software programmable key repeat rate and delay. The repeat rate is slowed down by ***PROTROL*** software as a precaution to prevent inadvertent repeated operator inputs from the keyboard (e.g. book lying on key).

The following plug-in circuit boards are supplied with each computer (note: common board types between the two computers are the same manufacturer and model):

DCC-X:

- CPU board
- disk controller board
- display generator board
- serial port board
- I/O bus converter board

DCC-Z:

- CPU board
- disk controller board
- display generator board
- serial port board
- Local Area Network (LAN) board
- multi-function (serial/parallel port) board

The CPU board is running an 80386 processor at a clock frequency of 20 MHz. The board is supplied with 4 MBytes of RAM. This board is also equipped with an 80387 math coprocessor. The CPU board has six logic circuit layers implemented with CMOS circuitry and advanced low power SCHOTTKY gate arrays for low power consumption.

The disk controller board controls the hard disk and two floppy disk drives.

The display generator board drives the CRT monitor with a pixel resolution of 640 x 480 in 256 colors (similar to super VGA display generators). The advantage of the display generator board is that it has its own on board

processor and firmware to generate and position the display images using high level software commands. This reduces the loading of the computer CPU which would be necessarily greater with VGA displays. It also has its own memory to store many different displays for instant retrieval. Each computer is supplied with a compatible CRT monitor.

The serial port board provides the multiple serial connections required and unloads the main CPU from the overhead of serial communications. The board is connected to a board mounted on the back of the DCC which contains 8 serial port s.

The I/O bus converter provides the interface to I/O equipment for DCC-X.

The LAN board provides the interface between DCC-Z and remote computers connected to the LAN running at 2 Mbps. The board unloads the main CPU of network traffic handling by use of its own network coprocessor and memory. It is fully ***NETBIOS*** compatible allowing use of most popular network operating systems.

The multi-function board is used in DCC-Z for the parallel port connection to the printer (see reference [10]).

For more details on the above equipment, refer to the associated manufacturer's manual.

H.2. Input/Output Hardware

H.2.a. Chassis Arrangement and Watchdog/Test Cards

DCC-X is equipped with 2 chassis containing the following types of I/O:

- analog inputs (8 differential inputs per card)
- analog outputs (4 differential outputs per card)
- digital inputs (16 contact sense inputs per card)
- digital outputs (16 contact outputs per card)
- watchdog contact outputs

The I/O points provide the computer signal interfaces to the analog hardware equipment. Serial data links are also used for interfaces to digital equipment (e.g. motor controllers and DCC-Z). Usage of the I/O points can be summarized as follows:

- field interface signals to components throughout the reactor facility.
- interface signals to the RSS, motor controllers and internal controls of the console.

- digital and analog circuits output to input feedback (wrap around) self test of the I/O hardware (see figure 7-7).

The watchdog provides the function of testing both hardware and software integrity. The watchdog is composed of a relay and timer circuit that must be reset at a high enough frequency (period of 1.7 s) to maintain the relay energized. The software is scheduled to generate these pulses through the I/O hardware cyclically each time after passing all of the computer self tests every 0.7 s. If a self test fails or the software "freezes" for any reason, the watchdog will time out and its contacts will open.

H.2.b. Analog Signal I/O Cards

The analog inputs and outputs are all voltage signals using a 10 V range where possible to minimize the effect of signal noise pick-up. The following paragraphs describe the types of cards used to process the analog I/O signals.

Two types of analog input signal conditioning (gate) cards are used: transformer coupled and solid-state, each providing 8 differential voltage inputs. The card selection is based on meeting appropriate filtering, sampling rate and surge withstand capability for the input signals.

The solid state gate card is unfiltered at its input and is used only for the gamma ion chamber pulse range signal. The pulse range signal is sampled at approximately 3000 samples per second during a pulse which is well within the card and ADC capability. This card can withstand a maximum of +/- 11 Vdc differential plus +/- 11 Vdc common mode on the input signals which should be adequate considering that the pulse range signal is only routed within the console.

The transformer coupled cards are used for all inputs other than the pulse range gamma ion chamber signal. All inputs have a double-pole filter (-6 db @ 14 Hz). The maximum sampling rate used for the transformer coupled signals is about 10 Hz. This card can withstand a maximum of +/- 25 Vdc differential plus +/- 400 Vdc common mode on the input signals.

The analog output cards are all the same type each having 4 differential bipolar voltage outputs with a fixed range of +/-10.24 V. Each output channel has a 12 bit digital to analog converter (DAC) providing maximum output current of +/- 5 mA (short circuit protected). The output signal can change at a

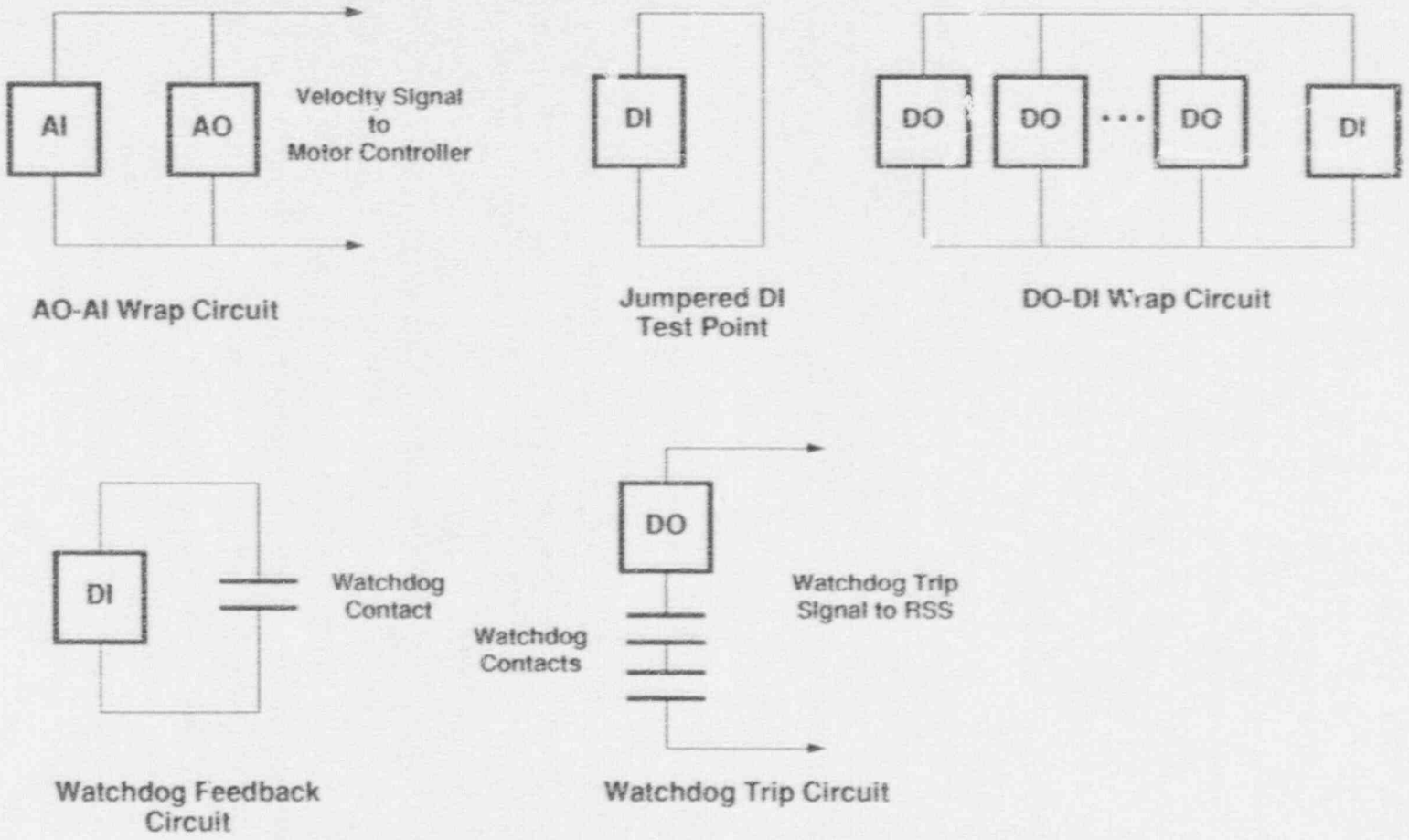


Figure 7-7 Watchdog and I/O Self Test Circuits

maximum slew rate of 1 V/microsecond and has a setting time of 50 microseconds.

H.2.c. Digital Signal I/O Cards

The digital input card used provides for 16 optically isolated inputs. The card is jumper configured to sense the state of contacts wired across the input terminals with a closed contact being read as "true" in software. An external 24 Vdc power supply is used for contact sensing, resulting in a current of 4.4 mA through the contact when closed. A current level below 0.95 mA will read as an open contact. The 24 Vdc power is supplied to terminals on each I/O chassis which then supplies the digital input cards via the back plane. A maximum of 38 V is tolerable on the input terminals. The input signals are filtered with a 5 msec time constant.

The digital output card provides for 16 relay outputs. The relay contacts are mercury wetted having maximum ratings of 2 A, 200 V and 50 W. The contacts close within 2 msec. An external power supply of 12 Vdc is required for the relay coils. This is supplied through the front edge connectors of the cards.

H.2.d. Watchdog and I/O Self Test Circuits

PROTROL caters to a number of generic self tests of the analog and digital I/O. These tests are defined in section I.4. This section describes the hardware circuits required for the self tests and the watchdog trip and feedback circuits. Typical circuits are shown in figure 7-7.

The watchdog trip circuit is wired to the reactor safety system. This circuit is composed of a digital output and two contacts from the watchdog relay wired in series (contacts open to trip). The use of two watchdog contacts provides increased reliability. When the DCC-X software detects a failure requiring a watchdog trip, the watchdog is no longer updated and the digital output is opened. The digital output is opened immediately. The watchdog contacts will open after the timer delay. "Killing" the watch dog means that the digital output opens immediately and the watchdog timer is no longer reset. "Kicking" the watchdog means that the timer is reset. If the watchdog is not " kicked" before the watchdog timer "drops out" the watchdog contacts open causing a trip.

The analog wrap around circuit is used to test the analog velocity signal to the motor controllers (one wrap around circuit for each motor) (see figure 7-7). When DCC-X starts up the wrap around circuits are tested by the CHK

task before allowing DCC-X to go into controlling mode. There after, the RRS task continually performs the velocity signal validation.

The first point of each digital input card is jumpered closed. This point is continually monitored by the CHK task to ensure that the point always reads in the closed state. Test failure results in a watchdog trip.

For the DO-DI wrap around test, the last point (contact) of each digital output card is wired in parallel to a digital input point (see figure 7-7). The CHK task continually toggles the digital outputs and checks for the correct response at the digital input. Test failure results in a watchdog trip.

The watchdog is continually tested for the proper state by the CHK task through the feedback circuit. Test failure results in a watchdog trip. If the test fails during start up, DCC-X will not be allowed to go into controlling mode.

H.3. Motors and Associated Controllers

The motors supplied for the rod drives are NSK ***Megatorque*** Motors, model AS0408 (flange mount), with mating EE style controller (interface option 05). The same motor/controller type is supplied for all drives, however the controller is configured differently for the transient rod. For a detailed description of the design features of the motor and controller, see reference [11] as specified for interface option 05. The motor has high torque and very smooth operation at low speeds.

The NSK ***Megatorque*** motors are servo controlled with selectable closed loop control modes of velocity, position or torque (not used in this application). Position and velocity feedback is provided by a resolver on the motor shaft. The motor controller (or driver) supplies the required current to the 3 phases of the motor, performs the closed loop servo control and motion interlock functions and handles the serial communications and I/O signal interfaces. All serial communications are with DCC-X over separate dedicated RS232C serial data links for each motor controller. Each motor's I/O interface handles an analog input signal for demanded velocity (from DCC-X), an analog output signal of measured velocity (to DCC-X) and various digital inputs for interlocking motor movement. The motor controller is very versatile, having the capability to easily switch between the various control modes "on the fly", provides the ability to input a velocity demand with an analog signal and provides an analog output to monitor speed.

The NSK motors were picked for the following reasons:

- smooth operation at low speed

- limited maximum speed (1.5 or 4.5 rps)
- rugged design with long life expectancy
- versatile controller and signal interface
- reasonable comparative cost.

The main negative feature of the NSK controller is that its digital inputs for interlocking motion require a closed contact to perform the interlocks. Redundant software interlocks on the demand signal have been provided to compensate so that loss of power will not violate an interlock. Software EOT interlocks are based on both fail safe configured limit switches and the resolver position indication.

H.3.a. Motor Control

The motor controllers make use of the following signals for control of rod drive position and velocity (see reference [11] for a description of their functions):

Digital Contact Inputs:

- counter clockwise limit switch (CCLS).
- clockwise limit switch (CLS).
- home limit switch (HLS).
- home low speed limit switch (HLLS).
- emergency stop switch (EMST).
- machine ready (MRDY).
- servo on (SVON).

Analog Voltage Signals:

- velocity demand (input).
- measured velocity (output).

Serial Data Link:

Controller to DCC-X:

- motor position (resolver counts).
- state of controller digital inputs: MRDY, SVON, CCLS.
- controller status:
  - drive ready (DRDY).
  - alarm 01 (AL01).
  - alarm 02 (AL02).
  - at home (HOME).

DCC-X to Controller:

- requests for the above data.
- commands to switch to velocity mode, position mode or give a homing request.

Before the motor provides torque, the MRDY and SVON inputs must both be true (closed contacts). These two inputs are wired directly to DCC-X digital outputs. Both DOs are set true if DCC-X is healthy, its watchdog is energized and motor trouble is not detected. Otherwise, motor torque will be lost and rods connected to the rack and pinion type drives will likely fall. When torque is not applied the motors can be easily turned by hand, facilitating setup during commissioning.

Motor trouble is detected if any of the following conditions becomes true:

- a drive alarm occurs (AL01 or AL02)
- drive ready (DRDY) is false
- An error in serial link communications between the motor and DCC-X is detected.

The interlocks listed below will provide torque to stop the motor, overriding all other controls (provided MRDY and SVON are true): NOTE: In all cases the input contact must remain closed to maintain the interlock.

EMST - stops the motor while the input contact is closed. This input is wired to the terminal blocks for use during commissioning.

CCLS - stops the motor from moving in the counter clockwise direction while the contact is closed. This input is controlled by RSS for the down drive disable function.

CLS - stops the motor from moving in the clockwise direction while the contact is closed. This input is controlled by RSS for the up drive disable function.

Under normal circumstances, the motors perform servo control of either velocity or position. Velocity mode is used for all operations to position the rod. The velocity control setpoint is provided by the analog voltage signal to the controller from DCC-X. Position mode is used only when the rods are stopped and when a homing operation is requested. This approach was used because it was found that some motors would drift very slowly when the rods are stopped in velocity mode. When holding the rods in position mode,

the setpoint is always the position value at the time of switching into position mode.

A homing operation is performed to move the drive down to a preset position relative to the home limit switch. This position is intended to be just above the bottom drive end of travel limit switch yet close enough for the magnets to pick up the rod. For the transient rod, the home position is low enough to so that the connected rod would have negligible reactivity insertion.

There are two reasons to home a rod:

- following a SCRAM to bring the drive into a position to allow reconnection of the rod when the SCRAM condition is reset. All rods home automatically following a SCRAM except for the transient rod.
- reset the resolver turns counter if power is lost to the controller. The resolver position measurement is only absolute over one turn.

To home a drive, the rod must first be SCRAMed and the drive must be above the HLS and HLLS switch positions. After the home request from DCC-X, the drive will move down at homing speed. When the HLLS contact closes, the drive will slow down to a creeping speed (both speeds are software tunable in the controller). Once the HLS contact opens the drive will continue moving at slow speed for a fixed homing offset (software tunable in the controller). When home is reached, the position measurement is set to zero counts in the controller and the HOME serial output flag goes true until the motor is moved from the home position. The home position value in DCC-X software can be set to any required value through tuning.

A homing request will be rejected under any of the following conditions:

- the rod is not SCRAMed first
- the CCLS input is true
- motor trouble is detected
- the drive is already homing

A homing operation will be aborted under any of the following conditions:

- the CCLS input goes true while homing
- the motor does not move
- motor trouble is detected

An analog voltage output signal from the controller provides a measurement of the motor velocity for monitoring purposes. This signal is used by DCC-X to SCRAM the reactor if the speed in the upwards direction is too high.

H.4. Power Supplies

All equipment in the console is powered from single phase 120 Vac. The AC power for the control and monitoring system equipment is distributed by two power bars each containing 8 surge protected outlets.

H.5. I/O Assignment

The philosophy used for assignment of cards to chassis and signals to I/O points is to minimize the consequences of single card or chassis failures where possible. First consideration must be given to the signal requirements and the self check points. Wherever there is flexibility in choice of point assignment, signals that have some level of redundancy are chosen to be on separate cards/chassis if possible.

The cards are organized as shown in drawing -05-009-DD-A of reference [15]. The AO, DO and DI cards are split between the two chassis, half in each. Chassis I/O-1 contains a bipolar ADC card and I/O-2 contains a unipolar ADC card which determines the splitting of AI cards between the chassis.

The following convention was adopted for the assignment of I/O points:

(1) The watchdog feedback DI is in I/O-1 providing maximal separation from the watchdog test card in I/O-2.

(2) The first point on each DI card is jumpered for self tests.

(3) The last point on each DO card is wired into the DO-DI wrap circuit for self-testing (see figure 7-7).

(4) The DI point for the DO-DI wrap is on the last DI card of I/O-2. Being the farthest point in daisy chain has a marginal reliability benefit.

(5) The AOs for rod velocity are in a separate chassis from the AIs used for AO-AI wrap testing (see figure 7-7). The AIs from

the motor controllers for the overspeed trip are also on a separate chassis from the rod velocity AOs.

(6) The redundant signals for the DCC-X SCRAM function are on separate AI cards.

(7) The DIs associated with controlling and monitoring functions of the rods are grouped together on a separate card for each rod. Two rod DI cards are in one chassis and two are in the other chassis.

(8) The DIs used to monitor the status of redundant SCRAM parameters are in separate chassis.

(9) The DOs used for the following functions are in separate chassis:

- bypass the redundant high power SCRAMs
- control the two lines to police services
- control the two Rabbits
- control the two exhaust fans

(10) The DOs for control of each rod drive are grouped on separate cards where possible (there are 3 DO cards yet 4 motors).

I. *PROTROL* Generic Software Description

The ***PROTROL*** operating system, with the exception of a very small segment, is written entirely in Pascal. The control application programs are designed entirely in a very high level control block language. These blocks are also written in Pascal, so there is a high degree of uniformity across the system.

Very intensive and extensive testing of the PROTROL operating system and service utilities (bar charts, trends, tuning) as well as the control language blocks have been performed to ensure the reliability and robustness of the system.

I.1 Control Language

A functional description of the block language is given in reference [12]. The major features of the control language used in PROTROL are:

- each control function or loop (e.g. reactor regulation or protection system trips) forms a separate unit within the computer system, in a structure analogous to using separate instrument racks for installing separate analog control systems. This provides "separation and independence" of different functions within the software. An added advantage is that testing of later changes or additions to the software is reduced in scope and very straight forward.
- there are provisions for separate control loops to send signals to one another, internally within the computer, without using physical I/O.
- control design is done in a "block" language, in which blocks correspond to conventional analog devices, or more advanced operations derived from AECL's experience in digital control.
- the "blocks" may input and output two kinds of control signals (with corresponding I/O for each) within the control programs: analog and boolean. The former corresponds to currents or voltages (e.g. 0..10V) and the latter to relay states (i.e. on/off or true/false).
- the signals are identified by self-documenting 12-character names or "tags".
- the set of "blocks" that can be used is very extensive: it includes all commonly used analog devices (e.g. PID, rate-limiter, etc.) plus a number of blocks with no simple analog world counterpart (e.g. SPREAD, SELECT, LEVEL-COMP, etc.).

- new or custom blocks can be added to the language for special applications: such as the MOTOR block created to provide the serial link interface to the NSK motor controllers.
- identical data structures are used in the control (DCC-X) and monitoring (DCC-Z) computers. This ensures that software signals have a common tag throughout the control and monitoring portions of the system.

I.2. The Operating System

The PROTROL operating system is a real-time, multi-tasking operating system.

The term "multi-tasking" means that a number of different functions can be performed, apparently (to the human) simultaneously. The kinds of functions performed include self-checks (diagnostics), control functions (e.g. reactor regulation) message display, tuning of setpoints or gains, etc., and display on the CRT of values of signals in bar chart or trend format. Each such function is performed by a separate "task", and the operating system kernel is responsible for scheduling each task (i.e. making it run at intervals) to meet system requirements.

The term "real time" means that the system runs identified critical tasks on time. Here "on time" means that, whether interrupt driven or periodically scheduled, the function is executed adequately fast to control the process to meet dynamic performance specifications (e.g. power overshoot). In practice, this means that all tasks are assigned a priority and the lower priority tasks are suspended when a high priority task "needs" to run.

For maximum software simplicity and predictability of response to all operating conditions, the PROTROL system is timer driven (sometimes this is described as "polling"). This means that hardware interrupts in the system, from the keyboard, disc drive, etc. are lower priority than the tasks performing self diagnosis and control. Moreover, no process driven interrupts are implemented. This design philosophy ensures maximal determinism in system response (i.e. predictability of loading and response time), and therefore, maximal system robustness.

The task scheduling function (called the dispatcher) is run off the real time clock interrupt. The interrupt interval is programmed at system boot time to approximately 27 ms, so this is the system's fundamental period. All tasks run at intervals which are multiples of the fundamental period.

The multi-tasking operating system will support many individual and separate tasks, each operating at its own period and relative priority. Each task is self contained, having its own database, block parameters, and access to the I/O.

The operating system schedules the execution of a number of tasks, representing the self test (CHK), and TASK-1, . . . , TASK-n, which are the individual generic and application tasks. The data structures of each task are private to the task.

Interfaces to a task are via blocks in the control block language library:

- I/O blocks (AI, AO, DI, DO) to physical I/O hardware.
- pseudo I/O blocks (SI, SO, BI, BO) to a shared data region called the ILDB.

Each task does its own process I/O. In addition, there are a number of signals exchanged between tasks using the pseudo I/O.

I.3. Generic Tasks Running in the *PROTROL* System

As described in the previous section, the heart of the ***PROTROL*** system is the multi-tasking operating system. The operating system schedules a number of periodic tasks in accordance with their defined intervals and priority.

At the bottom of all ***PROTROL*** CRT maintenance displays is a list in dark grey, of all the tasks in the system. As they are dispatched, the tasks labels are displayed in white (of underlined in white on some screens). By observing the continuous flashing of these indicators, the operator has an immediate view into the operating system's activity.

The generic tasks that are dispatched by the operating system are described below. The tasks exist on both DCC-X and DCC-Z unless noted (by "X" or "Z" beside task label).

LOAD Calculates the percentage of time the computer is busy executing either generic or application software.

CHK This task performs the self diagnostic tests and periodically "kicks" the watchdog to keep it from signalling a SCRAM if all critical self tests pass.

BCST X Broadcasts signals to DCC-Z via the "one way" serial link.

HDS Z Scans the tasks' data bases and stores selected signal values to disk at the one of 5 frequencies.

KBD This task processes the keystrokes from the operator keyboard in accordance with the displayed menu in

maintenance displays. It passes the keystrokes on to the appropriate task for processing in operator displays.

DSK Handles all access to hard and floppy disk drives.

BAR Barchart Display. This task displays and updates barcharts of up to 8 variables in a format like horizontal edgemeters. The sets of variables and update period are tunable on-line.

TRND Trend Diagram. This task plots an image of up to 4 variables on a real-time high resolution display in a format similar to a (very fast moving) strip chart recorder. The sets of variables and update period are tunable on-line.

HTND Z Retrieves the historical data stored by the HDS task.

HCPY Responds to a hardcopy request to save a screen image and sends it to the printer (DCC-Z) or hard disk (DCC-X).

KLOK Updates the clock display in the upper right corner of all displays.

MSG The message task prints messages to a screen from a queue. The latest message is always displayed at the bottom of the screen. A maintenance display menu allows browsing through the last 250 messages.

STAT This task periodically updates the maintenance display status of the operating system and tasks.

BRCV Z Receives all signal data broadcast through the "one way" serial link from DCC-X to DCC-Z. It puts the data into the appropriate task record for use in DCC-Z.

BLN Z Broadcasts signal data to the Local Area Network.

IDLE This is a dummy task which is run when the CPU is ready, but no other task is required to run.

I.4 System Self Checks and Defenses

The principles employed in the design of the system are to:

- keep it simple and robust,
- try to keep the DCC running for non-fatal conditions,
- fail the DCC for fatal conditions (i.e. drop the watchdog).

The types of failures which could challenge the system are:

- failure of critical field sensors,
- loss of power,
- failure of communications with the process I/O,

- failure of the arithmetic processing,
- program corruption faults.

I.4.a. Defenses Against Loss of Field Sensor

This type of failure is external to the DCC system, and the level of redundancy in the sensors and the actions to be taken are application specific, so defenses here are the responsibility of the control programs. The operating system does, however, provide assistance through the "quality" flag returned by each analog input block -- this flag warns the control program that the input is out of range.

I.4.b. Defenses Against Loss of Power

Loss of AC power will immediately drop the DCC's watchdog.

Partial loss of power, e.g. to the DI power supply or to an I/O chassis, is detected by the CHK program (which checks one point on each DI card, and "kills" the watchdog if a failure is detected) or through the "quality" flag returned to the control program by the AI block. I/O chassis failures (e.g. +5 V) which affect the operation of the test card cause an immediate dropout of the watchdog.

I.4.c. Defenses Against I/O Failure

Several layers of defense are provided here, most of which are performed by the CHK program, and some of which are the responsibility of the control program(s).

The first level of defense is the periodic check that data sent to the I/O chassis is correctly received, and can be returned intact. This is done by writing data to, then reading the registers on the test card in each I/O chassis. Any detected failure is first re-tried once after a short delay; a second immediate failure results in dropping the watchdog (if it has not already dropped out since it had not been correctly "kicked").

The next layer of defense is wrap around tests of representative I/O points (see figure 7-7). One representative point from each DO card is wired in parallel with one DI point. These DOs are then driven in turn to test that they are accessible and functional. These DO-DI wrap around tests are done within the operating system by the CHK program.

Analog wrap tests are also performed to check critical AOs. During system startup, the critical AOs (i.e. rod velocity signals) are "borrowed" and

tested by the CHK program. Thereafter, they are tested as part of the application logic.

The control designer maximizes the system availability and minimizes the effects of failure by assigning control signals for the control drives to separate cards when possible.

I.4.d. Defenses Against Computational Faults

The first line of defense is hardware integrity. This is verified on line every execution of the CHK program. This task (or program) tests every type of calculation performed by the floating point processor. An error in computed multiply or square root, etc. results "killing" the watchdog.

The second line of defense is software integrity. This implies that no module should output bad data nor fail because of bad data. Consequently, every module in the system which provides floating point outputs for other modules, calls a library routine to clamp values to within the "legal" range. Similarly every routine using data defends itself against illegal data. The "legal" range is defined so that no combination of "legal" values can produce a result that causes hardware problems.

I.4.e. Defenses Against Program Corruption Faults

The major software line of defense is the CHK program and the way it is executed. This is a periodic task, which must run on time or the watchdog will drop out since it is the only program which can "kick" the watchdog. Since CHK is a periodic program, it can only be executed provided that the dispatcher is working correctly. This means that virtually the whole used set of the CPU instructions must work correctly and that large segments of RAM must also be uncorrupted.

The CHK program and the dispatcher together perform the following checks:

- they trip "stuck" functions that are taking too long to execute:
  Any stuck function is terminated and a message is issued. If it is non-critical, the rest of the system continues to operate. If it is a critical function the watchdog is "killed".
- they check that each control program executes the correct number of times between passes of CHK:
  The watchdog is "killed" if this condition is not satisfied.

I.5. DCC-X/DCC-Z Self Tests and Robustness Functions

The following three features are incorporated into ***PROTROL*** to detect the level of faults or degradation of the computer and its I/O:

- self tests on start up
- self tests while on line
- built in protection functions

These features include many generic tests and functions for the various ***PROTROL*** computer configurations (e.g. single control computer, dual control computer, monitoring computer, etc.). This section lists those functions used in DCC-X and DCC-Z for the PSBR application.

The results of the self tests are logically combined to drive the state of two flags which give the level of capability for control and monitoring "healthy" and "fit". Under normal circumstances, both flags are true. For DCC-X, the watchdog is kicked as long as the "fit" flag is true. If unfit, the watchdog will drop out resulting in a SCRAM and DCC-X will switch to "inactive" mode. If either flag is false, an alarm message is issued. DCC-Z follows the same logic except that it does not have a watchdog.

The states of the DCC resulting from the tests are indicated in the upper right corner of the CRT displays. The possible states are as follows:

Initializing -	state when DCC is started up and performs initializing functions and initial self-tests.
Controlling (DCC-X) -	state after successful initialization.
Monitoring (DCC-Z) -	state after successful initialization.
Inactive -	state after failing a self-test performed by the CHK task.

The PROTROL tests configured for the DCC-X and DCC-Z are given below. The tests which affect fitness are indicated by [F]. Otherwise, only health is affected by the test result.

I.5.a. Self Tests on Start Up

The self tests on start-up are listed below. If a DCC-X fitness test fails, it will switch from "initializing" to "inactive" (instead of "controlling") mode and drop its watchdog before ever allowing control task I/O operations. Failure of a fitness test in DCC-Z will switch modes from "initializing" to "inactive".

COMPUTER CHECKS:

-[F] Floating point processor test (X and Z).

-[F] Serial link reception error (Z). A red banner will be placed across the DCC-Z CRT to highlight serial link failure.

- Serial link transmission error (X).
- Disk failures (X and Z).

SOFTWARE FUNCTION CHECKS (X AND Z):

-[F] all critical tasks executed twice to completion at defined frequency.

-[F] memory allocation OK.

I/O CHECKS (X):

-[F] Test for excessive I/O retrys.

-[F] DI cards jumpered point closed test.

-[F] DO-DI wrap test.

-[F] borrowed AO-AI wrap test.

-[F] Watchdog/Test card communications test.

-[F] Watchdog contact wrap test.

I.5.b. Self Tests While On Line

The on line self tests are listed below. If a fitness test fails, the associated computer will switch to "inactive" mode and DCC-X will "kill" its watchdog. This mode change seals in until the computer is restarted for all cases except serial link communication failure on DCC-Z. DCC-Z will resume monitoring once proper communications is restored.

COMPUTER CHECKS:

-[F] Floating point processor test (X and Z).

-[F] Serial link reception error (Z). A red banner will be placed across the DCC-Z CRT to highlight serial link failure.

- Serial link transmission error (X).
- Disk failures (X and Z).

SOFTWARE FUNCTION CHECKS (X AND Z):

-[F] all critical tasks execute to completion at defined frequency.

-[F] memory allocation OK.

-[F] manual shutdown request.

I/O CHECKS (X):

-[F] Test for excessive I/O retrys.

-[F] DI cards jumpered point closed test.

-[F] DO-DI wrap test.

-[F] Watchdog/Test card communications test.

-[F] Watchdog contact wrap test.

The built in protection functions are not tests per se, but rather functions in software that prevent anomalous system operation failure or provide early warning of software problems in the verification and validation phases of design. For example, ***PROTROL*** system software disables keys used by the disk operating system (DOS) that influence software operation. Other functions are those to prevent catastrophic failure if a software function becomes stuck, memory overflow occurs or there are illegal uses of internal hardware (e.g. floating point processor). The protection functions provided for DCC-X and DCC-Z are listed below.

PROTECTION FUNCTIONS (X AND Z):

- keyboard typo-matic rate slowed down to minimum.
- keyboard buffer size reduced to minimum for immediate recovery from string of anomalous key strokes.
- DOS keyboard buffer overflow prevented to eliminate possibility of "beep" function.
- DOS system keys disabled such as:
  - CRTL-ALT-DEL
  - CTRL-ALT-S
  - PRINT SCRN
  - SYSRQ
  - CTRL BREAK/C
  - PAUSE
- stuck functions shut down.
- warning for sequence of events message buffer overflow.
- floating point processor exceptions retried after processor reset or offending function shut down.
- tasks shutdown if their remaining stack space is low.
- display driver error buffer cleared frequently to prevent its use of RAM.
- display changes delayed to ensure that the display driver command list buffer doesn't overflow flowing a quick sequence of display change requests.

J. Application Software

The application software is composed of a number of independent tasks, listed below. The tasks concerned with control logic are ***PROTROL*** block language tasks. The other tasks are written in PASCAL code.

J.1. Block Language Tasks

RRS - This is the reactor regulating system task which performs functions related to controlling reactor power on DCC-X. On DCC-Z, this task contains only records of signals broadcast from the DCC-X RRS task via the "one way" serial link for display purposes (i.e. no control logic).

SSS - This is the safety support slow task. On DCC-X, it performs the slow portion of the RSS support functions (e.g. air interlock validation). On DCC-Z, it contains only records of signals broadcast from the DCC-X SSS task similar to the RRS task above.

SSF - This is the safety support fast task. On DCC-X, it performs the fast portion of the RSS support functions (e.g. DCC-X SCRAM and rod movement interlock validation). On DCC-Z, it contains only records of signals broadcast from the DCC-X SSF task similar to the RRS task above.

FAC - This task performs functions related to control and monitoring of the reactor facility (e.g. facility interlocks for reactor operation and police services alarms). On DCC-Z, it contains only records of signals broadcast from the DCC-X FAC task similar to the RRS task above.

J.2. Non-Block Language Tasks

OPR - This is the operator controls interface task. It processes all operator keyboard inputs for display navigation and functions that are controlled through menus. On DCC-X, it drives I/O directly related to keyboard input (e.g. manual control of bay exhaust fans).

DSP - This task handles updating of the CRT displays.

PULS - This task runs on a periodic basis to control the digital output to request air to the transient rod. When a reactor pulse is requested this task will read and process the GIC pulse range analog input signal and generate both the pulse data file and

display driver command list for display of the pulse. This task exists only on DCC-X and thus its internal variables cannot be accessed on DCC-Z.

In the ***PROTROL*** operating environment, tasks have the following attributes:

- independent scheduling frequency.
- definable scheduling priority relative to other tasks.
- independent module of code with controlled interfaces to other tasks.
- critical/non-critical attribute to determine whether or not failure will drop the watchdog.

The principles used for the task structure outlined above, are as follows:

[1] The independent safety system support functions are separated into different tasks from control system functions.

[2] Hardware I/O operations for safety support and control functions are performed independently in the associated task. This means that common I/O signals related to safety are <u>not</u> read from the hardware in one task and then passed to the other task in software (even though this would reduce CPU loading).

[3] Functions that do not have a high execution frequency requirement are placed into separate slower tasks so that CPU loading is not made unnecessarily high. For this reason there are both fast and slow safety support tasks (SSF & SSS) and control tasks (RRS & FAC).

[4] Related functions are grouped into common tasks to minimize task interfaces (even though they may have varying execution frequency requirements).

[5] Functions related to control of the operator interface are implemented in non-block language tasks allowing use of conditionally executed code. For example, dynamic portions of CRT displays are updated only when needed (i.e. a change has occurred). Much of the code must execute only when a key is pressed. This minimizes CPU loading without peak loading concerns since the operator cannot physically generate requests fast enough to cause a high peak load. The operator interface has been slowed down to provide additional assurance.

[6] Special purpose functions where the block language is mostly unusable, are implemented in non-block language tasks (e.g. PULS).

The design details of the various application software tasks as they apply to DCC-X and DCC-Z are provided in the design manual (reference [15]).

K. Control Room

K.1. General Description

The console assembly is located in the control room. All of the equipment described above is located in the console assembly with the exception of the FC and GIC Detector Assemblies, the in core fuel temperature TCs, the Wide Range Amplifier and the field sensors. A window is provided between the control room and the reactor bay such that an operator seated at the console can observe personnel movement in the reactor bay. A CCTV system is also provided in the control room so that the operator can observe personnel movement in the beam hole laboratory.

Three internal communication systems and a commercial telephone are available to the reactor operator in the control room. The internal communication systems allow: 1) two way conversation with anyone on the reactor bridge and the experimenters using the pneumatic transfer systems at any of the sending stations; 2) two way conversation between offices and offices within the building; and 3) the use of a page system that has speakers in all parts of the building.

A window between the control room and a public corridor allows visitors to conveniently view the reactor controls; it allows Police Services to observe any unusual indications on their inspection tours; and it allows the reactor staff to observe instrumentation from outside the reactor bay.

K.2. Monitor Indications in the Control Room

There is an instrumentation pedestal located at one end of the console in the control room. Figure 7-8 shows some of the equipment that is mounted in the pedestals. Table 7-1 lists the monitors that are equipped with alarms, their detectors, settings and ranges. An alert (as used in Table 7-1) results in an amber warning light on the monitor, and a status alarm and an alarm message is issued by the PCMS. An alarm (as used in Table 7-1) results in an red alarm light on the monitor, and a status alarm, an alarm message and an evactuation

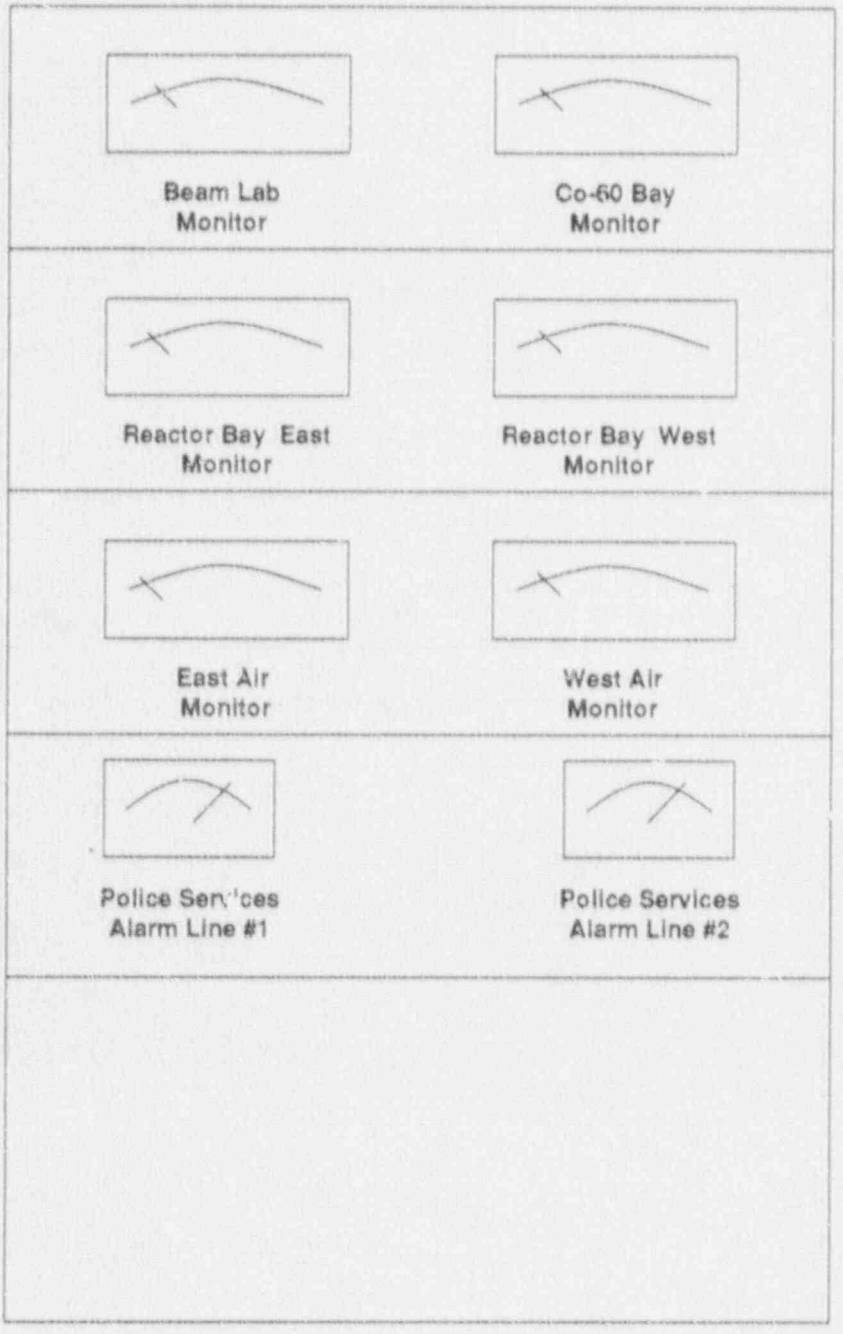


Figure 7-8 Instrumentation Pedestal

Table 7-1
Control Room *Alarmed Radiation Monitors

Monitor	Detector	Range	Setting**
Reactor Bridge East	Ionization Chamber	0.1 to $2x10^3$ mR/hr	Alert: 15 mR/hr Alarm: 30 mR/hr
Reactor Bridge West	Ionization Chamber	0.1 to $2x10^3$ mR/hr	Alert: 50 mR/hr Alarm: 200 mR/hr
Reactor Bay Air East	Thin End G-M Tube	10 to 10^5 c/m	Alert: 6000 c/m Alarm: 10000 c/m
Reactor Bay Air West	Thin End G-M Tube	10 to 10^5 c/m	Alert: 6000 c/m Alarm: 10000 c/m
Co-60 Bay	G-M Tube	0.1 to 10^4 mR/hr	Alarm: 6 mR/hr
Beam Laboratory	G-M Tube	0.1 to 10^4 mR/hr	Alarm: 6 mR/hr

*Alarmed is defined as lighting a red light on the monitor. An analog output from the monitors is an input to the PCMS. When that signal exceeds the setpoint a status alarm is issued, an alarm message is issued and an Evacuation is initiated (see section 7.5.1.2.e.).
**Setting is determined internally and established by PSBR procedure.

initiation is issued by the PCMS. Monitor #1 and Monitor #2 indicate the status of the phone lines to University Police Services. The alarmed monitors are calibrated at least annually according to internal Checks and Calibration Procedures. Figure 7-9 diagrams the radiation monitoring system.

L. Minimum Safety SCRAMS and Interlocks

Tables 2a and 2b in the Technical Specifications section list the minimum safety circuits and the minimum operational interlocks for the PSBR.

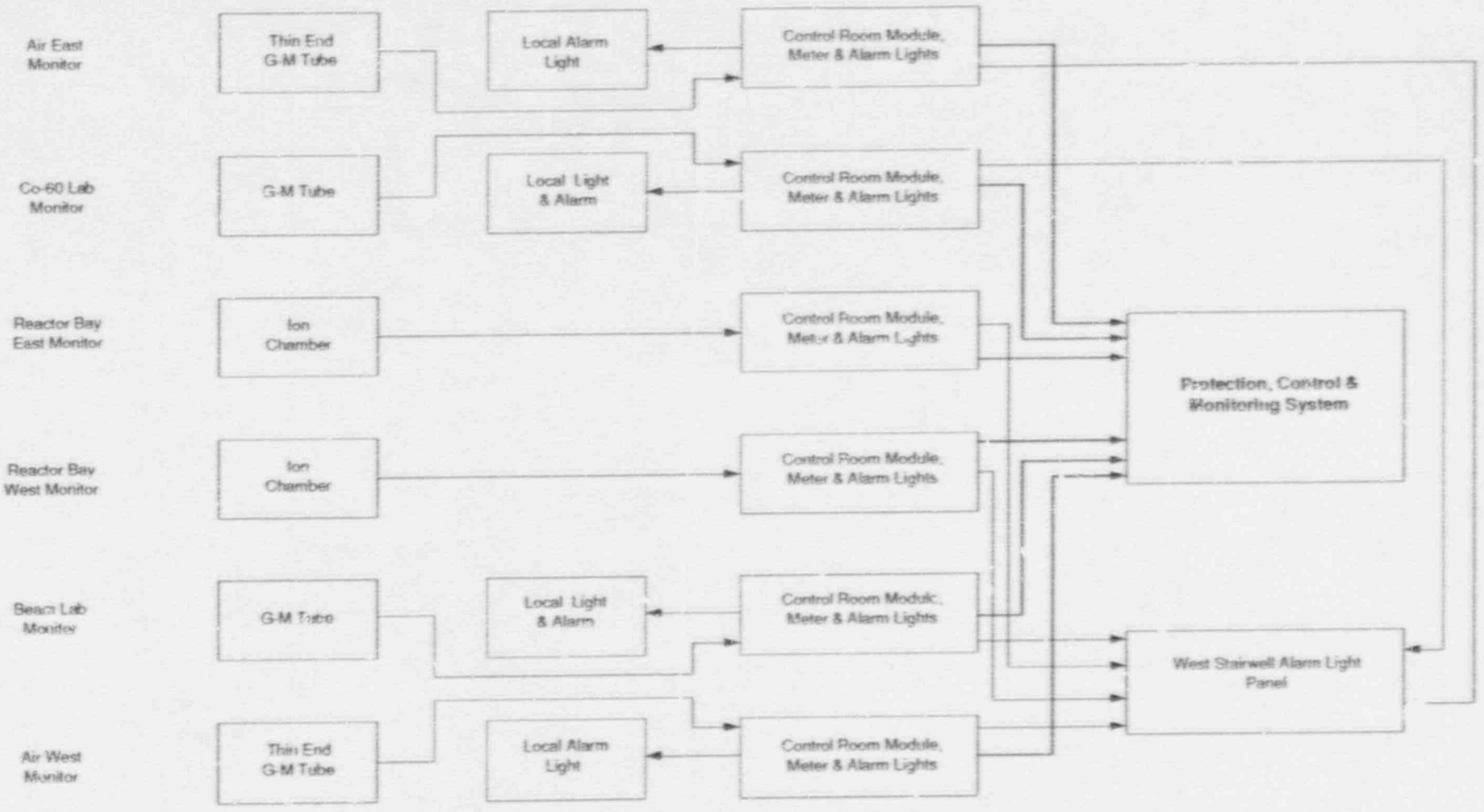


Figure 7-9 Radiation Monitoring System

M. References

[1] Docket No. 50-005, Facility Operating License R-2, Technical Specification for PSBR, 1986 January.

[2] PSBR Console Specifications, Printed by PSU 88 Oct 27.

[3] DR-17-60501-001, Design Requirements, Reactor Safety System.

[4] DR-17-60501-002, Design Requirements, Control and Monitoring System.

[5] DR-17-60501-003, Design Requirements, Console Layout and Operator Interface.

[6] MM-17-60501-001, Maintenance Manual, PSBR CSS Upgrade, Control and Monitoring System.

[7] NUREG-0700, Guidelines for Control Room Design Reviews, 1981 September.

[8] MM-17-60501-004, Maintenance Manual, Gamma-Metrics Instruction Manual (#158), Reactor Control Console for Penn State University.

[9] OM-17-60501-001, Operating Manual, Control and Safety System.

[10] MM-17-60501-002, Maintenance Manual, Transduction Computers.

[11] MM-17-60501-005, Maintenance Manual, NSK ***Megatorque*** Motor System User's Manual.

[12] RM-17-69020-001, Reference Manual, ***PROTROL*** Advanced Control Block Language: Control Designer's Reference Manual.

[13] TR-17-60501-001, Test Report, Reactor Safety System (Filled-Out copy of G-M Dwg #040264).

[14] MM-17-60501-003, Maintenance Manual, Computer Products I/O Hardware.

[15] DM-17-60501-001, Design Manual, Control and Safety System.

[16] Regulatory Guide 1.152, *Criteria for Programmable Digital System Software in Safety-Related Systems of Nuclear Power Plants*, U. S. Nuclear Regulatory Commission, Nov 1985.

VIII. CONDUCT OF OPERATION

A. Organization and Responsibility

The Director of the Penn State Breazeale Reactor (PSBR) reports to the Head of the Nuclear Engineering Department who reports to the President of the University through the Dean of the College of Engineering and, for matters related to reactor operations, the Senior Vice President for Research and Dean of the Graduate School. The directorship of the PSBR is a subset of broader responsibilities assigned to the Director of the Radiation Science and Engineering Center. An organization chart is presented in Figure 8-1.

Responsibility for the safe operation of the PSBR lies with the Director and the operations staff which is composed of permanent University employees. The permanent staff has extensive cumulative experience operating the PSBR.

The Penn State Reactor Safeguards Committee, an independent group with technically experienced members from both within and outside the University, advises the Director on all matters or policy pertaining to safety. Members are appointed by the Dean or the College of Engineering, acting for the Senior Vice President for Research and Dean of the Graduate School.

The University Health Physics staff, also independent of the reactor administration, provides "onsite" advice concerning personnel and radiological safety and provides technical assistance and review in the area of radiation protection. The Health Physcis office is one of the Intercollege Research Programs and reports to the office of the Senior Vice President for Research and Dean of the Graduate School.

B. Reactor Operating Safety Philosophy

All operations involving the PSBR shall be conducted in compliance with pertinent existing local, state, and federal regulations. The reactor shall be operated within the limits established by the operating license and the technical specifications. An ALARA program (as low as reasonably achievable) will be in effect

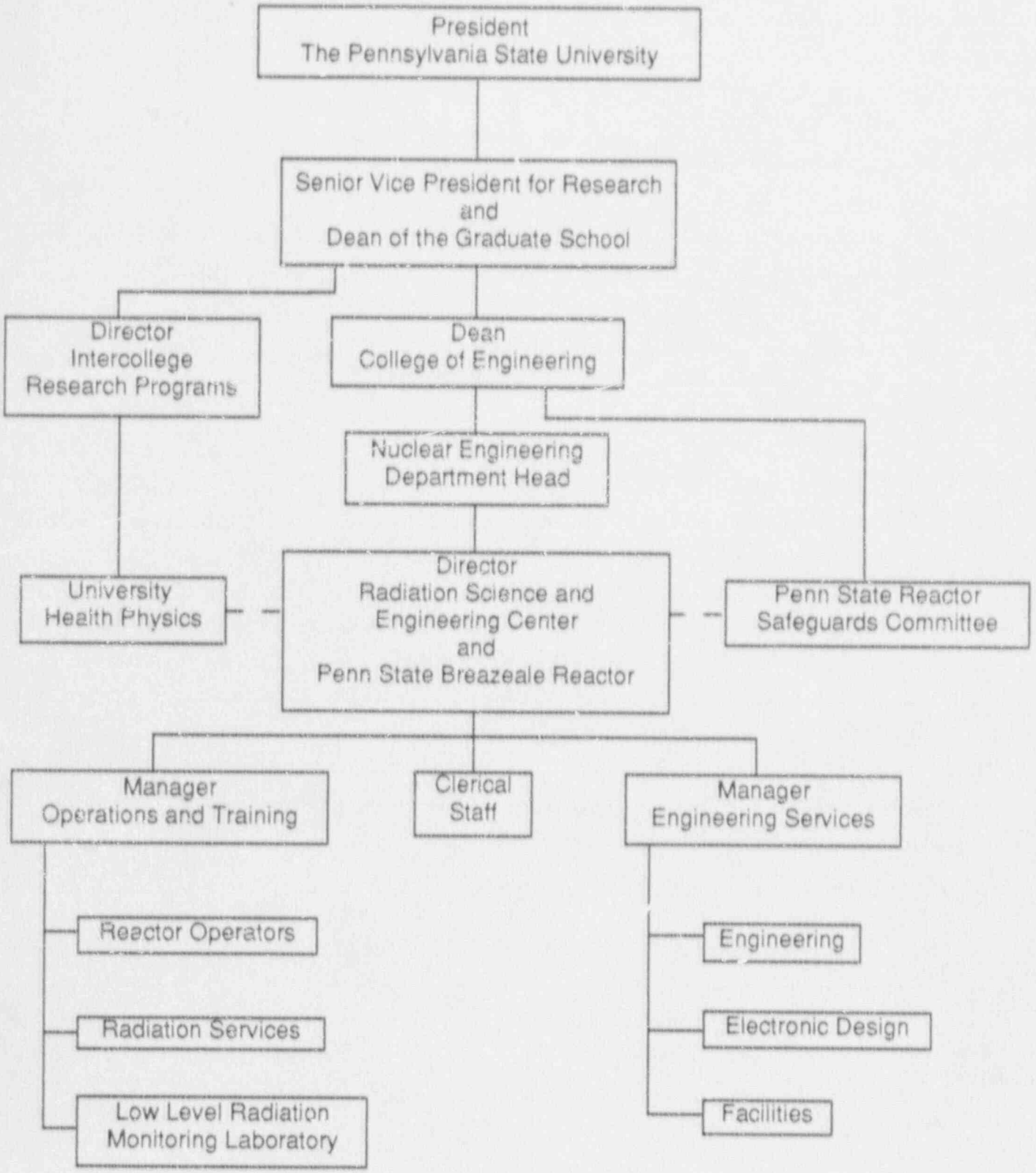


Figure 8-1
ORGANIZATION CHART

to minimize radiation exposures to the public, the staff, and the environment.

C. Training

The competence of the PSBR operators and senior operators is maintained by the PSBR requalification program. This program keeps the reactor staff cognizant of features of facility design, reactor principles and operating characteristics, reactor instrumentation and control, safety and emergency systems, emergency and standard operating procedures, administrative and special procedures, radiation control and safety, and other facility information necessary for a licensed individual to perform his or her duty.

Competency of licensed individuals to respond appropriately to the emergency plan is maintained by an annual review of the emergency plan for the reactor staff by the Emergency Director, and by participation of licensed individuals in drills required by the emergency plan.

D. Written Procedures

The practical application of the philosophy of safe reactor operation set forth in section B above is augmented by detailed written procedures. These procedures fall into four general categories, Emergency Procedures (fire, civil disorder, loss of pool water, etc.); Standard Operating Procedures (operation of the reactor, instrumentation checkout, fuel handling, etc.); Special Procedures (beamport utilization, cooling systems, etc.); Administrative Policies (personnel requirements for operation, facility keys, reactor safeguards committee procedures, etc.).

The written procedures are approved by either the Director or Deputy Director of the PSBR. Further, these procedures govern the activity of all staff personnel, experimenters, and visitors while in the PSBR. The procedures are reviewed annually and the review is documented.

E. Records

A daily reactor operations log is maintained by reactor operating personnel and contains such information as core loading and changes, experiments in the reactor including time in and out, power level, startup and shutdown times, control rod positions, and calibrations and maintenance notations.

Separate and more complete files are kept on reactor instrumentation readings, checkouts, calibrations, maintenance and other items concerned with operational aspects of the facility. All unscheduled shutdowns are reviewed and any corrective action necessary is performed before restart.

Records are maintained which indicate the review, approval, and conditions necessary for the production of radioisotopes and/or the performance of irradiation experiments.

F. Review and Audit of Records

The Penn State Reactor Safeguards Committee (PSRSC) acts as a review panel for any reactor experiments which, by their unusual nature and/or potential hazard or unprecendented complexity, could endanger health, life, and property in and about the PSBR.

The PSRSC also provides for an annual outside, independent audit of the operation of the PSBR facility.

depleted fuel element compensates for its being closer to the average core fuel temperature.

C. Evaluation of the Limiting Safety System Setting (LSSS)

The limiting safety system setting is a measured fuel temperature of 700°C as defined in the Technical Specifications.

If the core power were at 1.15 MW (15% over power) steady state, the measured fuel temperature using Eq. 32 is 552°C for the hottest fuel element in the core, i.e., N^P=2.2 and P=26.7 KW per fuel element for loading 36. The measured 552°C fuel temperature is close to the maximum fuel temperature (within approximately 10%) due to the radial temperature distribution. A sudden insertion of reactivity, close to but less than $1, into the core will initially increase the reactor power exponentially at a period faster than one second. Using a negative temperature coefficient of 1×10^{-4} dk/°C*, the increase in average core fuel temperature is less than,

$$\frac{.007\ \delta k/k}{1 \times 10^{-4}\ \delta k/k\ °C} = 70°C$$

and for an NP = 2.2, the maximum fuel temperature increase is 154°C (2.2 x 70°C = 154°C). Adding this increased fuel temperature in the hottest fuel element to the 552°C steady state temperature results in 706°C, much less than the maximum limit of 1150°C. For this to occur at power levels above the power level scram set point will require that both power level scrams fail. The temperature scram will be initiated when the measured temperature exceeds its set point. The equilibrium temperature of 706°C will be achieved at least within two to three periods (seconds) after reactivity insertion. A control rod drop time less than one second assures an early decrease in reactivity and fuel temperature. At this point, the control rods moving into the core will begin to decrease the reactor power in less than a second after the scram. Control rods are checked semiannually to assure their rod drop time is less than one second. The kinetics

* The temperature coefficient during a fast period is slightly less than the prompt temperature coefficient.

of the reactor cause the reactor power to decrease as soon as the control rods move a few inches into the core. Thus, the maximum fuel temperature will remain well below 1150°C since the measured fuel temperature is close to the maximum fuel temperature for these quasi-static conditions.

The maximum allowed pulse reactivity of $3.40 is established to prevent the measured fuel temperature from exceeding the LSSS. When the core produces a $3.40 pulse, the maximum measured temperature is, using Eq. (34) and NP = 2.2 for loading 36, 667°C. This corresponds to a maximum fuel temperature of 1067°C. The temperature scram will not lower the maximum fuel temperature attained during a pulse once the pulse is initiated; however, it does protect the core from high temperatures during steady state operation.

D. Loss of Coolant Accident

The PSBR pool contains 71,000 gallons of water. For a loss of coolant accident to occur, a break in the pool wall or break in a connecting pipe must occur below the bottom of the core. A series of alarms will occur as the water level drops more than 26 cm. Just below 26 cm, alarms will notify the reactor operator in the control room and the University Police Services. If the reactor is operating at 1.0 MW the area radiation alarms will sound and initiate a scram of the control rods and activate the evacuation alarm. It will also provide information to operating personnel that high levels of radiation exist in the reactor bay before the water drops another 100 cm. In case of a leak, there exists a moveable gate that can be used to isolate either side of the pool within hour after the leak is noticed. PSBR Emergency procedures call for moving the reactor to the non-leaking side of the pool and isolating that side of the pool with the gate to prevent the water level from dropping below the reactor core.

If a leak occurs, it will take time for the pool level to drop below the bottom of the fuel. With the reactor cooled by water for at least two minutes after the scram, which is produced by radiation monitors or operator, the maximum fuel temperature will drop more than 350°C,(17) and three minutes after the scram the maximum fuel temperature is within 20°C of the water temperature.(17)

If the reactor power is accidently raised to 1.25 MW, the excess reactivity available for pulsing will be less than $3. As a consequence the maximum fuel temperature attainable remains less than 1150°C. Hence, the reactivity accident will not violate the safety limit.

The $5 ramp analysis was performed for AFRRI by General Atomics [24]. It indicated that even with a reactivity addition rate of $2.50/second (averaged over the full rod travel) the safety limit (1150°C) was not reached. The rod withdrawal was terminated with a high power scram less than 1 second into the event. A reactivity of $1.86 was added after criticality was achieved and before the SCRAM occurred. The maximum power in the transient was 330 MW with a maximum fuel temperature of 330°C. Compared to the above analyzed reactivity accident this excursion is inconsequential. It should be noted that the amount of reactivity available in the ramping rods does not impact on the final result as long as the reactivity addition rate does not exceed the $2.50/second rate and the SCRAM time is not significantly longer than that analyzed.

G. Conclusion

There are two limits which, if not exceeded, will prevent rupture of the cladding of a TRIGA fuel element. They are:

(1) Limit the fuel temperature to a maximum 1150°C when the cladding temperature remains below 500°C, i.e., when the fuel is covered with water.

(2) Limit the fuel temperature to a maximum 900°C when the cladding temperature is above 500°C, i.e., during a LOCA.

TheTechnical Specifications for the PSBR are established to prevent reaching these two limits. The 1150°C temperature limit is not reached as the fuel temperatures are limited during pulse mode operations. Eq. (34) provides a direct method for determining the maximum fuel temperature based on the measured fuel temperature during a pulse. Using this equation and the maximum possible NP = 2.2 and core loading 36, the following limits are established:

(1) The maximum allowed reactivity insertion for the pulse mode is $3.40 and corresponds to a maximum peak fuel temperature of 1067°C and a measured peak temeprature of 667°C.

(2) The maximum allowed worth of the pulse rod is $3.70. A sudden insertion of $3.70 excess reactivity results in a maximum peak fuel temperature of 1150 C and a measured peak fuel temperature of 20°C.

(3) The maximum allowed excess reactivity of the core is $7. Thus, when the core is operating at 1.15 MW steady state, only $3 of excess reactivity is available for pulsing, $4 of excess reactivity is needed to reach 1.15 MW. A pulse insertion of $3 temperature to 1150°C.

(4) Core configuration limitations are also established to prevent a fuel element from producing too much power relative to the other fuel elements. An NP = 2.2 cannot be attained by any allowed core configuration limiting the maximum power of a fuel element in core loading 36 to 23.2 KW. Setting NP = 2.2 establishes a fuel temperature upper limit attainable during a pulse.

Limits set for steady state operation prevent the maximum fuel temperatures from coming close to 1150°C. Limits imposed here prevent the fuel temperature during a LOCA from reaching 900°C. If operated at 1 MW for 70 hrs. during each week, a single fuel element could operate above its max power level of 23.2 KW, as high as 24.2 KW, and still not have its fuel temperature exceed 900°C during any conceived LOCA. In addition, these same limitations on steady state operation limit the release of fission products to the environment to very low values if the cladding ruptures.

The maximum hypothetic accident (MHA) analyzes the effect of a fuel element cladding rupture in air at the end of 70 hours of reactor operation at 1 MW. In addition, the reactor was assumed to have operated for 70 hours each week during the previous year. Under these extreme conditions, the maximum exposure to a person in the unrestricted area is 23.3 mrem to the thyroid after 1 hr. and 26.3 mrem to the thyroid after 24 hrs.

In conclusion, the analysis described in this section shows that under no possible accident conditions will the regulations in either 10CFR20 or 10CFR100 be violated. Thus, the PSBR can be operated without exposing the public to any significant radiation risk, i.e., the PSBR can continue to operate safely without adverse environmental impact and without undue risk to the public.

H. References

1. Naughton, W.F., Cenko, M.J., Levine, S.H., and Witzig, W.F., "TRIGA Core Management Model," Nucl. Technology, vol. 23, p. 256 (Sept. 1974).
2. Naughton, W.F., Cenko, M.J., Levine, S.H., and Witzig, W.F., Increasing TRIGA Fuel Lifetime with 12 wt% U TRIGA Fuel, TOC-5, TRIGA Owner's Conference III (February 1974).
3. Haag, J.A., and Levine, S.H, "Thermal Analysis of The Pennsylvania State University Breazeale Nuclear Reactor," Nucl. Technology, vol. 19, p. 6 (July 1973).
4. Levine, S.H., Geisler, G.C., and Totenbier, R.E., Temperature Behavior of 12 wt% U TRIGA Fuel, TOC-5, TRIGA Owners' Conference III (February 1974).
5. Levine, S.H., Totenbier, R.E. (Penn State Univ.), and Ahmad T. Ali (PPAT Ismail - Malysia), Fourteen Years of Fuel Management of the Penn State TRIGA Breazeale Reactor (PSBR), ANS Trans, vol. 33 (November 1979).
6. Levine, S.H. and H. Ocampo, "The k_∞-Meter Concept Verified via Subcritical/Critcal TRIGA Experiments," Proceedings of the International Symposium on the Use and Development of Low and Medium Flux Research Reactors, MIT, Cambridge, MA (October 1983).
7. Kim, S.S. and S.H. Levine, "Verifying the Asymmetric Multiple Position Neutron Source (AMPNS) Method Using the TRIGA Reactor," Ninth TRIGA User's Conference, Anaheim, CA (March 1984).
8. Levine, S.H., "Module 5 - In-core Fuel Management," Nuclear Fuel Cycle Educational Module Series, N.D. Eckhoff, gen.ed., Kansas State University (July 1980).
9. Fowler, T.B., et.al., "EXTERMINATOR-II: A FORTRAN IV Code for Solving Multigroup Neutron Diffusion Equations in Two Dimensions," ORNL-4078, Oak Ridge National Laboratory (April 1967).
10. Huang, H.Y. and S.H. Levine, "An Automated Multiple-Cycle PWR Fuel Management Code," ANS Trans. (November 1978).
11. Cenko, M.J., "Comparison of PSBR Operation's History with the TRIGA Core Management Model," M.S. Thesis, The Pennsylvania State University (1972).
12. Barry, R.F., "LEOPARD - A Spectrum Dependent Non-Spatial Depletion Code for IBM-7094," WCAP-3269-26, Westinghouse Electric Corporation (September 1963).

13. Simnad, M. T., F. C. Foushie, and G. B. West, "Fuel Elements for Pulsed Reactors," GA Report E-117-393 (January 1975).
14. El-Wakil, M.M., "Nuclear Heat Transport," ANS (May 1978).
15. Goodwin, W.A., "The Measurement of Radial Power Distribution in a TRIGA Fuel Element During Reactor Excursion," Ph.D. Thesis, University of Illionis (1967). 16. Kim, S. S., "Development of an Asymmetric Multiple Position Neutron Source (AMPNS) Method for Monitoring the Criticality of the Degraded Reactor Core," Ph.D. Thesis, The Pennsylvania State University (1984).
17. PSBR Log Book 37, page 265 (November 21, 1984).
18. Shoptaugh, J. R., Jr., "Simulated Loss-of-Coolant Accident for TRIGA Reactors," GA-6596 (August 1965).
19. West, G. B., "Safety Analysis Report for the Torrey Pines TRIGA Mark III Reactor," GA-9064 (January 5, 1970).
20. Katcoff and Seymour, Nucleonics, vol. 18, p. 201 (November 1960).
21. Foushee and R. H. Peters "Summary of TRIGA Fuel Fission Product Release Experiments," GULF-EES-A10801 (September 1971).
22. Regulatory Guide 1.109, "Calculation of Annual Doses to Man From Routine Releases of Reactor Effluents for the Purpose of Evaluating Compliance With 10CFR Part 50, Appendix I."
23. International Commission on Radiation Protection Report #23.
24 General Atomics, *Analysis of 5 Dollar Ramp Insertion over 2 Second Interval in AFRRI TRIGA™ Reactor,* General Atomics Publication of work performed for Armed Forces Radiobiological Research Institute, Bethesda, Maryland, April, 1988.