



Dow U.S.A.

The Dow Chemical Company
Midland, Michigan 48667

Director, Office of Nuclear Reactor Regulation
Attn: Document Control Desk
U. S. Nuclear Regulatory Commission
Washington DC 20555

DOCKET 50-264

Sir:

The Dow Chemical Company requests amendment of the Technical Specifications for the Dow TRIGA Research Reactor, facility operating license R-108. The changes introduced by the proposed amendment are for the purposes of

1. providing for the installation of a microprocessor-based instrumentation and control system, and
2. improving the assurance of compliance with surveillance activities by changing the timing of the required annual report to coincide with the majority of the annual surveillance tasks.

These amendments are described fully in the attachments; supporting documents are referenced or supplied.

A check to cover the filing fee of \$150.00 has been sent separately.

Very truly yours,

L. W. Rampy
Chair, Radiation Safety Committee
1803 Building
15 October 1990

9010260013 901015
PDR ADOCK 05000264
PDC

A020
11

DOW TRIGA RESEARCH REACTOR

- 1 -

1. MICROPROCESSOR-BASED INSTRUMENTATION AND CONTROL SYSTEM

The control console of the Dow TRIGA Mark I Research Reactor (previously used at the General Atomics Torrey Pines reactor facility) was installed at this site in 1967. Upgrades of the safety channels were performed in 1973 and 1974. Components of the system are no longer produced and spare parts are difficult to obtain. The Dow Chemical Company has made arrangements to install a microprocessor-based instrumentation and control system from General Atomics. This system is to be similar to those already installed at several locations, including the General Atomics 250 kW TRIGA Mark I pulsing reactor and the 1 MW TRIGA Mark F pulsing reactor at the Armed Forces Radiobiological Research Institute (AFRRI).

The control system for the Dow facility is to include one NM-1000 digital neutron channel, for both the wide-range linear channel and the wide-range log channel, and one independent NP-1000 analog neutron channel.

The installation includes a rebuild of the three control-rod drive units. The entire system will provide this facility with up-to-date capabilities commensurate with the recently-extended operating license.

The control system underwent extensive evaluation by General Atomics (SAFETY EVALUATION UNDER 10CFR50.59 MICROPROCESSOR BASED INSTRUMENTATION AND CONTROL SYSTEM FOR THE GENERAL ATOMICS TRIGA MARK I REACTOR, TRF-252, DECEMBER 1988). Further evaluation was performed for the AFRRI system, not under 10CFR50.59, and a Safety Evaluation Report was issued July 23, 1990, supporting the amendment of the operating license to allow the use of this control system.

The proposed amendment to the Dow operating license is intended to place a restriction on the safety channel instrumentation (requiring at least one analog safety channel) and to include an increase of safety surveillance (the additional scram capability of the watchdog circuit).

The new instrumentation is expected to provide more reliable and safer service than the current system, enabling the Dow Chemical Company to continue to utilize this powerful analytical tool.

DOW TRIGA RESEARCH REACTOR

- 2 -

All testing of the new system will take place following review and approval of the Reactor Operating Committee.

When the control system is delivered (expected late November 1990) the safety channels will be connected in parallel with the present system and the operation, particularly of the scram circuits, will be evaluated, with the present console maintaining complete control of the reactor. Following satisfactory completion of these tests the control rod drive motors will be removed and returned to General Atomics to be rebuilt. When the control rod drives are returned and installed the reactor will be tested with the new control system controlling the rod drives while the old system controls the safety and scram functions. Following successful testing in this mode, the old system will be completely disconnected and control of all of the reactor functions will rest with the new system.

The new console will be configured for 300 kilowatt operation but all of this testing will take place while operating under the 100-kilowatt limitation. Following successful completion of the testing of the control system the evaluation of operation at power levels up to the license maximum of 300 kilowatts will commence.

This portion of the amendment is concerned with pages 11, 12, 13, and 14 of the Technical Specifications. Explanatory pages, replacement pages, and a full replacement copy of the Technical Specifications are enclosed.

A copy of the Safety Evaluation supporting amendment 19 to the facility operating license R-84, Armed Forces Radiological Research Institute, is enclosed.

DOW TRIGA RESEARCH REACTOR

- 3 -

2. ANNUAL REPORT

The Technical Specifications (Amendment 5) require an annual report "...within 90 days of the anniversary of the license...", which is May 8. A number of annual tasks are performed in January of each year. Experience has shown that tasks may be performed more reliably when they are grouped. By deleting the phrase referring to the anniversary of the license and by performing all of the annual tasks at the same time the timely performance of the tasks becomes more reliable. It is proposed that the first such annual report be submitted in the first quarter of 1991 and annually thereafter.

DOW TRIGA RESEARCH REACTOR

Proposed changes. Additions are **bolded**, deletions are underlined. The additional paragraph on page 12 is not new but is carried over from the previous page, from which it was displaced by additions.

3.3. Reactor Control and Safety Systems

Applicability

These specifications apply to the reactor control and safety systems and safety-related instrumentation that must be operating when the reactor is in operation.

Objective

The objective of these specifications is to assure that all reactor control and safety systems and safety-related instrumentation are operable to minimum acceptable standards during operation of the reactor.

Specifications

There shall be a minimum of one scram-capable analog safety channel.

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

Each of the three control rods shall drop from the fully withdrawn position to the fully inserted position in a time not to exceed one second.

The reactor safety channels and the interlocks shall be operable in accordance with table 3.3A.

The reactor shall not be operated unless the measuring channels listed in Table 3.3B are operable.

Positive reactivity insertion rate by control rod motion shall not exceed \$.20 per second.

Bases

Safety channels with scram capability utilizing analog circuitry have been proven acceptable by more than thirty years of experience.

The requirement for three operable control rods ensures that the reactor can meet the shutdown specifications.

The control rod drop time specification assures that the reactor can be shutdown promptly when a scram signal is initiated. The value of the control rod drop time is adequate to assure safety of the reactor.

Use of the specified reactor safety channels, set points, and interlocks given in table 3.3A assures protection against operation of the reactor outside the safety limit.

The requirement for the specified measurement circuits provides assurance that important reactor operation parameters can be monitored during operation.

The specification of maximum positive reactivity insertion rate helps assure that the Safety Limit is not exceeded.

TABLE 3.3A.
MINIMUM REACTOR SAFETY CIRCUITS,
INTERLOCKS, AND SET POINTS

Scram Channels

<u>Scram Channel</u>	<u>Minimum Operable</u>	<u>Scram Setpoint</u>
Reactor Power Level	2	Not to exceed maximum licensed power
Reactor Period	1	Not less than 7 seconds
Wide-Range Linear/Log Channel Detector Power Supply	1	Failure of the detector high-voltage power supply
Percent Power Channel Detector Power Supply	1	Failure of the detector high-voltage power supply
Manual Scram	1	Not applicable
Watchdog (DAC to CSC)	1	Not applicable

Interlocks

<u>Interlock/Channel</u>	<u>Function</u>
Startup Count rate	Prevent control rod withdrawal when the neutron count rate is less than 2 cps
Rod Drive Control	Prevent simultaneous manual withdrawal of two control elements by the control rod drive motors

TABLE 3.3A

BASES FOR REACTOR SAFETY CHANNELS AND INTERLOCKS

Scram Channels

<u>Scram Channel</u>	<u>Bases</u>
Reactor Power Level	Provides assurance that the reactor will be shut down automatically before the safety limit can be exceeded
Reactor Period	Prevents operation in a regime in which transients could cause the safety limit to be exceeded
Reactor Power Channel Detector Power Supplies	Provides assurance that the reactor cannot be operated without power to the neutron detectors which provide input to the wide-range linear power channel and the wide-range log power channel
Manual Scram	Allows the operator to shut the reactor down at any indication of unsafe or abnormal conditions
Watchdog	Ensures adequate communications between the Data Acquisition Computer (DAC) and the Control System Computer (CSC) units.

Interlocks

<u>Interlock/Channel</u>	<u>Bases</u>
Startup Countrate	Provides assurance that the signal in the log power channel is adequate to allow reliable indication of the state of the neutron chain reaction
Rod Drive Control	Limits the maximum positive reactivity insertion rate

6.6. Reports

6.6.1. Operating Reports

A report shall be submitted annually, within 90 days of the anniversary of the license, starting with the first quarter 1991 performance of annual tasks, to the Radiation Safety Committee and to the Director, Office of Nuclear Reactor Regulation, US NRC, Washington, DC, with a copy to the Regional Administrator, US NRC Region III, which shall include the following:

- a) status of the facility staff, licenses, and training;
- b) a narrative summary of reactor operating experience, including the total megawatt-days of operation;
- c) tabulation of major changes in the reactor facility and procedures, and tabulation of new tests and experiments that are significantly different from those performed previously and are not described in the Safety Analysis Report, including a summary of the analyses leading to the conclusions that no unreviewed safety questions were involved and that 10 CFR 50.59 (a) was applicable;
- d) the unscheduled shutdowns and reasons for them including, where applicable, corrective action taken to preclude recurrence;
- e) tabulation of major preventive and corrective maintenance operations having safety significance;
- f) a summary of the nature and amount of radioactive effluents released or discharged to environs beyond the effective control of the owner-operator as determined at or before the point of such release or discharge (the summary shall include to the extent practicable an estimate of individual radionuclides present in the effluent; if the estimated average release after dilution or diffusion is less than 25% of the concentration allowed or recommended, only a statement to this effect is needed); and

DOW TRIGA RESEARCH REACTOR

Proposed changes. These pages are to be substituted for existing pages when the changes are approved.

3.3. Reactor Control and Safety Systems

Applicability

These specifications apply to the reactor control and safety systems and safety-related instrumentation that must be operating when the reactor is in operation.

Objective

The objective of these specifications is to assure that all reactor control and safety systems and safety-related instrumentation are operable to minimum acceptable standards during operation of the reactor.

Specifications

There shall be a minimum of one scram-capable analog safety channel.

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

Each of the three control rods shall drop from the fully withdrawn position to the fully inserted position in a time not to exceed one second.

The reactor safety channels and the interlocks shall be operable in accordance with table 3.3A.

The reactor shall not be operated unless the measuring channels listed in Table 3.3B are operable.

Positive reactivity insertion rate by control rod motion shall not exceed $\$.20$ per second.

Bases

Safety channels with scram capability utilizing analog circuitry have been proven acceptable by more than thirty years of experience.

The requirement for three operable control rods ensures that the reactor can meet the shutdown specifications.

The control rod drop time specification assures that the reactor can be shutdown promptly when a scram signal is initiated. The value of the control rod drop time is adequate to assure safety of the reactor.

Use of the specified reactor safety channels, set points, and interlocks given in table 3.3A assures protection against operation of the reactor outside the safety limit.

The requirement for the specified measurement circuits provides assurance that important reactor operation parameters can be monitored during operation.

The specification of maximum positive reactivity insertion rate helps assure that the Safety Limit is not exceeded.

TABLE 3.3A.

MINIMUM REACTOR SAFETY CIRCUITS,
INTERLOCKS, AND SET POINTS

Scram Channels

<u>Scram Channel</u>	<u>Minimum Operable</u>	<u>Scram Setpoint</u>
Reactor Power Level	2	Not to exceed maximum licensed power
Reactor Period	1	Not less than 7 seconds
Wide-Range Linear/Log Channel Detector Power Supply	1	Failure of the detector high-voltage power supply
Percent Power Channel Detector Power Supply	1	Failure of the detector high-voltage power supply
Manual Scram	1	Not applicable
Watchdog	1	Not applicable

Interlocks

<u>Interlock/Channel</u>	<u>Function</u>
Startup Count rate	Prevent control rod withdrawal when the neutron count rate is less than 2 cps
Rod Drive Control	Prevent simultaneous manual withdrawal of two control elements by the control rod drive motors

TABLE 3.3A

BASES FOR REACTOR SAFETY CHANNELS AND INTERLOCKS

Scram Channels

<u>Scram Channel</u>	<u>Bases</u>
Reactor Power Level	Provides assurance that the reactor will be shut down automatically before the safety limit can be exceeded
Reactor Period	Prevents operation in a regime in which transients could cause the safety limit to be exceeded
Reactor Power Channel Detector Power Supplies	Provides assurance that the reactor cannot be operated without power to the neutron detectors which provide input to the wide-range linear power channel and the wide-range log power channel
Manual Scram	Allows the operator to shut the reactor down at any indication of unsafe or abnormal conditions
Watchdog	Ensures adequate communications between the Data Acquisition Computer (DAC) and the Control System Computer (CSC) units.

Interlocks

<u>Interlock/Channel</u>	<u>Bases</u>
Startup Countrate	Provides assurance that the signal in the log power channel is adequate to allow reliable indication of the state of the neutron chain reaction
Rod Drive Control	Limits the maximum positive reactivity insertion rate

6.6. Reports

6.6.1. Operating Reports

A report shall be submitted annually, starting with the first quarter 1991 performance of annual tasks, to the Radiation Safety Committee and to the Director, Office of Nuclear Reactor Regulation, US NRC, Washington, DC, with a copy to the Regional Administrator, US NRC Region III, which shall include the following:

- a) status of the facility staff, licenses, and training;
- b) a narrative summary of reactor operating experience, including the total megawatt-days of operation;
- c) tabulation of major changes in the reactor facility and procedures, and tabulation of new tests and experiments that are significantly different from those performed previously and are not described in the Safety Analysis Report, including a summary of the analyses leading to the conclusions that no unreviewed safety questions were involved and that 10 CFR 50.59 (a) was applicable;
- d) the unscheduled shutdowns and reasons for them including, where applicable, corrective action taken to preclude recurrence;
- e) tabulation of major preventive and corrective maintenance operations having safety significance;
- f) a summary of the nature and amount of radioactive effluents released or discharged to environs beyond the effective control of the owner-operator as determined at or before the point of such release or discharge (the summary shall include to the extent practicable an estimate of individual radionuclides present in the effluent; if the estimated average release after dilution or diffusion is less than 25% of the concentration allowed or recommended, only a statement to this effect is needed); and



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

SUPPORTING AMENDMENT NO. 19 TO

FACILITY OPERATING LICENSE NO. R-84

ARMED FORCES RADIOBIOLOGY RESEARCH INSTITUTE

DOCKET NO. 50-170

1.0 INTRODUCTION

AFRRI has determined that due to the progressive obsolescence of their control console, a new reactor instrumentation and control system is needed to maintain reliable operations. On May 11, 1988 AFRRI published their safety analysis of the new reactor instrumentation and control system. In this report AFRRI concluded that the new system has equal or greater safety built-in than the existing system and therefore is an allowable change under 10 CFR 50.59. 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 a different type than any 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.

The staff concluded from its review of the AFRRI safety analysis report that since (1) the installation of the new reactor instrumentation and control system did present an unreviewed safety question because of the possibility of an accident or malfunction of a different type than any evaluated previously and (2) additional technical specifications were required, NRC review and approval were required of the replacement computerized control system.

Pursuant to 10 CFR 50.90, the licensee submitted by letter dated April 30, 1990, as supplemented on June 19, 1990 and July 13, 1990, a request to amend Appendix A of Facility Operating License No. R-84, "Technical Specifications for the AFRRI Reactor Facility." The licensee submittal of June 19, 1990 resubmitted the May 11, 1988 safety analyses. The requested amendment would allow installation of the microprocessor based instrument and control system and add the watchdog (DAC to CSC) scram to Table 2 of the Technical Specifications, "Minimum Reactor Safety System Scrams."

The licensee has temporarily installed, in parallel to their existing control console, the new digital microprocessor based instrumentation and control system provided by General Atomics. The transfer of control from the old to

9008030032
7PP

the new system (including scram) is via a series of gradual steps accompanied by tests which are expected by AFRRRI to demonstrate the reliability of the new equipment while maintaining the proven performance of the existing control system. Upon completion of all testing (described later in this SER), the new console will be used to control (except for the hardwired trip functions) both the safety and nonsafety aspects of operation of the TRIGA reactor and the old analog console will be disconnected. The new console will replace the old analog console in the control room. Included in this change is the installation of three new stepping-motor control rod drives.

The primary functions of the new system will remain the same as the old system; to monitor critical parameters and provide a scram signal when needed, to provide information to the operator and to provide control for the pulse and steady-state modes of operation.

2.0 HARDWARE AND SYSTEMS ASSESSMENT

This portion of the review focused on the areas of potential vulnerability or susceptibility of the new control console which might compromise its ability to present accurate information to the operator and to provide scram signals when required. No assessment was made of the reliability of the nonsafety-related operation controls. Issues investigated included single failure, environmental qualification, seismic qualification, surge withstand capability (SWC), electromagnetic interference (EMI), failure modes and effects, reliability, error detection, and independence.

The primary review criteria for instrument and control systems for research reactors are presented in ANSI/ANS 15.15 (1978) "Criteria for the Reactor Safety Systems of Research Reactors." The staff performed this evaluation also using criteria which apply to current vintage nuclear power plants. However, due to the inherent reactivity insertion safety feature of the TRIGA reactor design and minimal decay heat generation that cannot cause fuel damage, the staff has concluded that these power plant criteria may serve as guidelines and that strict adherence to the power plant criteria is generally not warranted. The exceptions are noted in the appropriate sections below.

During the review and audit, the licensee described the new system including licensing, engineering, testing and training aspects. The vendor also participated and provided additional information. The staff also had benefit of material from the U.S. Air Force, the University of Texas at Austin and the console owners group. The licensee also had an independent safety review performed by ORI, Inc. which concluded that the system was acceptable. This is the first system of this type provided by General Atomics which the staff has reviewed, therefore, there is no direct comparison that can be made to a previously licensed configuration.

At AFRRRI, the Safety System Scram Circuit consists of two analog nuclear power monitor channels (NP-1000, NPP-1000) and two fuel temperature channels which are hardwired. Also wired into the scram circuit are contacts for manual scram, pulse timer, low water level, key switch and watchdog timers. The NM-1000 microprocessor based nuclear power channel monitors reactor power, but is not wired to the scram circuit at AFRRRI.

2.1 Environmental and Seismic Qualification

The new control system will be installed in the control room and the reactor hall. The staff considers the reactor hall (excluding within the pool itself) to be a mild environment when compared to power plant requirements and therefore the entire system can be considered to be in a mild environment. The system has been constructed in standard commercial enclosures suitable for a mild environment. The testing that has been done to date has not revealed any problems related to temperature or humidity. The new system should not be unduly susceptible to temperature or humidity problems and is therefore acceptable to the staff.

Though there have been no requirements promulgated for seismic qualification testing of research reactor control equipment, the staff reviewed the equipment to determine general ruggedness. The equipment appears to be mounted in a good commercial quality fashion which should prevent any significant movement of components within the console and racks. In this TRIGA reactor, an inadvertent scram does not present a challenge to reactor safety systems because a scram consists of the removal of current to the control rod magnets allowing the control rods to drop into the core by gravity. No other equipment is required to maintain the reactor in a safe shutdown condition. The primary concern remaining would be relay contact chatter which could prevent a scram when required. The safety system scram circuits for this system are designed to scram on failure (which includes contact chatter) and therefore the staff concludes that any further testing is not warranted and the system is acceptable.

2.2 Electromagnetic Interference (EMI)

The staff reviewed the susceptibility of the new equipment to EMI due to the potential for common mode interference which could disable more than one system at a time. As discussed earlier, due to the design characteristics of the TRIGA reactor, an inadvertent scram does not present a similar challenge to safety systems that it would on a power reactor, though it might cause operational difficulties such as disrupting an experiment.

At AFRRRI, optical isolators are used which will prevent conducted EMI from being transmitted between the control and safety channels. The neutron flux signal cabling is shielded to reduce the impact of radiated EMI. Previous experience with similar equipment provided by several different vendors at other facilities has indicated that if EMI causes any perturbation in the system it will most likely cause a scram, which is acceptable to the staff for a TRIGA reactor. Based on the above, the staff concludes that EMI should not prevent a scram when required and the design is therefore acceptable.

2.3 Power Supplies

The power supplies for the system are buffered to reduce the possible impact of minor power line fluctuations. The scram circuits for the new system are designed to scram when power is lost to them. The NP-1000 and NPP-1000 are analog devices and will respond to power fluctuations similar to the existing analog equipment. The digital NM-1000 nuclear power channel uses a battery

backed-up random access memory (RAM) to store constant data during loss of power. In addition to self-diagnostics, the NM-1000 has a watchdog timer circuit which puts the NM-1000 in a tripped condition and scrams the reactor if power fluctuations prevent proper software operation. As described in the NM-1000 Software Functional Specification and Software Verification Program (March 1989), the NM-1000 is also tested to verify that the system returns to proper operation following restoration of power. The staff finds this acceptable.

2.4 Failure Modes and Effects

The May 11, 1988 safety analysis for AFRR1 included an April 22, 1988 Scram Circuit Safety Analysis performed by the University of Texas at Austin. This study identified the various ways in which the reactor safety system could fail. These include:

- 1) Physical System Failure (wire breaks, shorts, ground fault circuits)
- 2) Limiting Safety System Setting Failure (failure to detect)
- 3) System Operable Failure (loss of monitoring)
- 4) Computer/Manual Control Failure (automatic and manual scram)

This study was based on a fault tree approach which predicted failure to scram for various failure modes. The study concluded that a failure of all safety systems and therefore failure to scram was extremely unlikely. Failures attributable to the unique failure modes of the software of the NM-1000 were adequately considered and in addition, at AFRR1, the NM-1000 is not directly wired into the scram circuit. The staff concludes that the failure modes and effects of the new system were adequately considered and the design is therefore acceptable.

2.5 Independence, Redundancy and Diversity

The staff reviewed the data link between the safety channels and the nonsafety systems. The safety channels provide direct hard wired scram inputs and are also hardwired directly to independent indicators on the control console. In addition, the safety channels provide inputs to the Non-Class 1E Data Acquisition Computer (DAC) through optical isolators. The optical isolators used have not been tested for maximum credible faults which the staff requires for power plant use, but have been tested by the manufacturer to standard commercial criteria. The DAC is then connected via redundant high speed serial data trunks to the Non-Class 1E Control System Computer (CSC) which interfaces with the operator by controls, a keyboard and CRT displays. Since the CSC does communicate with the safety channels, this aspect of the system would not meet the independence requirements of a power plant. However, the staff has concluded that the level of independence which has been maintained is appropriate for the AFRR1 TRIGA reactor and is acceptable.

For the AFRR1 facility, redundant fuel temperature (Temp 1, Temp 2) inputs are provided to the scram circuit. Redundant power level inputs (NP-1000, NPP-1000) to the scram circuit are also provided. The staff finds this redundancy acceptable. Several additional scram signals are provided at the control

console (manual scram, system watchdog timers). At AFRRRI, the NM-1000 is not wired to the scram circuit but does provide inputs to the rod withdrawal prevent interlock system. The system as installed at AFRRRI meets most of the requirements of IEEE-279-1971 "Criteria for Protection Systems for Nuclear Power Generating Stations" and IEEE 379-1977 "Application of the Single-Failure Criteria to Nuclear Power Generating Station Class 1E Systems," and is therefore acceptable to the staff.

The operators are provided with information from both the analog NP monitors and the digital NM monitor. The information is displayed on both direct wired bar graphs and on a graphic CRT. The scram is provided with automatic and manual contacts and, with the exception of the computer watchdog scram contacts, is similar to the old system. The staff considers this system sufficiently diverse and therefore is acceptable.

2.6 Testing

Extensive testing of the new system has been done by both the vendor and the licensee. A significant number of design changes took place during the testing that AFRRRI performed during the phase-in of the new system. General Atomics has also reported no significant safety problems with their installation. The staff has reviewed the problems discovered during testing of the system and has concluded that the resolutions appear appropriate. The staff also agrees with the assessment by the licensee that long-term operability and safety is enhanced due to installation of equipment which has spare parts available and is capable of being properly maintained. An additional improvement is the self diagnostics feature which allows continuous on-line testing and reduces the possibility of undetected failures.

3.0 Software Assessment

3.1 Criteria

The staff requires an approved verification and validation (V&V) plan for software which performs a safety function or provides information to the operator. At AFRRRI, the NM-1000 provide inputs to the rod withdrawal prevent interlock system block function. The NM-1000 software development was reviewed by the staff to determine the acceptability of the V&V plan. The staff compared the General Atomics V&V plan to Regulatory Guide 1.152 "Criteria for Programmable Digital Computer Software in Safety-Related Systems at Nuclear Power Plants" which endorses ANSI.IEEE 7-4.3.2 - 1982 "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations." The staff has concluded that this standard is appropriate for use in reviewing research reactor software.

3.2 Verification and Validation Plan

The staff reviewed the verification and validation documentation provided by General Atomics. The staff also reviewed the additional validation which was performed by the AFRRRI staff. Since the safety scram circuits at AFRRRI are hardwired and do not require software to function the emphasis of the review was to ensure that potential software problems could not prevent a scram if required.

The hardwired scram circuit is wired so that a scram will occur even if the control software is requesting rod withdrawal. An additional important feature is included to prevent software errors from interfering with safety function. The Control System Computer (CSC) and Data Acquisition Computer (DAC) include watchdog timers which must be reset every 10 seconds by the software or they will trip and provide a scram signal to the rod magnet power. The watchdog timers provide a continuous check of proper software operation. The staff finds them acceptable. Though the software was not shown to be in full compliance with Reg. Guide 1.152, the software will not impede the safety systems and is therefore acceptable.

4.0 Technical Specifications

The scram circuit at AFRR1 will include watchdog timer contacts which will provide a scram upon software failure. The staff has concluded that the presentation of correct, timely information to the reactor operator contributes to the safe operation of the reactor. Therefore, the watchdog scram inputs are added to Table 2, Minimum Reactor Safety System Scrams of the technical specifications. The operability of the watchdog scram will be verified by Technical Specification 4.2.2 which requires a channel test weekly. The basis of Table 2 is also amended to add the watchdog scrams and safety chambers is changed to safety channels to more accurately describe the high voltage loss scram.

5.0 ENVIRONMENTAL CONSIDERATION

This amendment involves changes in the installation or use of facility components located within the restricted area as defined in 10 CFR Part 20. The staff has determined that the amendment involves no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and there is no significant increase in individual or cumulative occupational radiation exposure. Accordingly, this amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9). Pursuant to 10 CFR 51.22(b), no Environmental Impact Statement or Environmental Assessment need be prepared in connection with the issuance of this amendment.

6.0 CONCLUSION

The staff concludes that the hardware design of the new General Atomics console is acceptable for use in the AFRR1 TRIGA reactor. The Software design in the CSC, DAC and NM1000 will not prevent the safety functions of the hardwired scram circuit from performing and is therefore acceptable. The technical specifications are amended to include the watchdog scram inputs and surveillance requirements.

The staff has also concluded, based on the considerations discussed above, that: (1) because the amendment does not involve a significant increase in the probability or consequences of accidents previously evaluated, or create the possibility of a new or different kind of accident from any accident previously evaluated, and does not involve a significant reduction in a margin of safety, the amendment does not involve a significant hazards consideration, (2) there is reasonable assurance that the health and safety of the public will not be endangered by the proposed activities, and (3) such activities will be conducted

in compliance with the Commission's regulations and the issuance of this amendment will not be inimical to the common defense and security or the health and safety of the public.

Principal Contributor: James C. Stewart

Dated: July 23, 1990