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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

SUPPORTING AMENDMENT NO. 6 TO

FACILITY LICENSE NO. R-115

DOCKET NO. 50-151

THE UNIVERSITY OF ILLINOIS

1.0 INTRODUCTION

By letter dated June 9, 1992, as supplemented on October 8, 1992, December 1, 1992, January 5, 1993, and January 11, 1993, the University of Illinois at Urbana-Champaign (UIUC or the licensee) requested changes to the Technical Specifications (TS) for the UIUC Advanced TRIGA Research Reactor (ATRR). The changes would allow the installation of a microprocessor based instrumentation and control system on the ATRR and make some minor corrections to the TS.

2.0 EVALUATION

2.1 Introduction

UIUC has determined that due to the obsolescence and progressive deterioration of their control console, a new reactor instrumentation and control system is needed to maintain reliable operations. The licensee has proposed installing a new General Atomics (GA) digital microprocessor based instrumentation and control system.

The primary functions of the new system 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.

2.2 Hardware and Systems Assessment

The staff evaluated the new control console to determine if it had vulnerabilities that might compromise its ability to present accurate information to the operator and to provide scram signals when required. The staff did not assess the reliability of the nonsafety-related controls. Issues investigated include single failure, environmental qualification, seismic qualification, power supplies, 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 that apply to current nuclear power plants. However, the TRIGA design has an inherent reactivity insertion safety feature and generates minimal decay heat, thus reducing the probability of fuel damage to a minimal amount. The staff has concluded that these power plant criteria are guidelines and need not be strictly followed.

During the review, the licensee described the new system including licensing, engineering, testing, and training aspects. The staff also had benefit of material from the U.S. Air Force, the University of Texas at Austin and the console owners group, as well as an independent safety review performed by ORI, Inc. which concluded that the system was acceptable. The system for the UIUC ATRR is a similar system to that reviewed and approved in the "Issuance of Amendment No. 19 to Facility Operating License No. R-84 - Armed Forces Radiobiology Research Institute (AFRRI)," "Issuance of Amendment No. 29 to Facility Operating License No. R-38 - General Atomics," " Issuance of Amendment No. 6 to Facility Operating License No. R-108 - Dow Chemical Company," "Issuance of Amendment No. 6 to Facility License No. R-113 - U.S. Geological Survey (RIGA Research Reactor Facility (GSTR)," and "Issuance of Facility Operating License" for the University of Texas at Austin.

The UIUC Safety System Scram Circuit required by the Technical Specifications consists of two fuel temperature channels, two analog (NP-1000 and NPP-1000) nuclear power monitor channels (for all modes of operation), of which one must be capable of causing a reactor scram, two reactor tank water level channels, a watchdog scram and a manual scram button which are hardwired. Also wired into the scram circuit but not required by the Technical Specifications are scrams for short period (provided by the NM-1000), loss of high voltage to the NP-1000 and NPP-1000, the console key switch, two external scrams, low primary flow with power above 1 MW, high tank water level and high primary outlet water temperature. There are also Technical Specification required rod blocks on transient rod withdrawal when reactor power is above 250 kW(t) (provided by the NM-1000), on control rod withdrawal when the neutron count rate is less than one count per second (provided by the NM-1000 and control system computer software), and a block to prevent withdrawal of the transient rod when the control rods are not fully inserted (provided by the control system computer software). Interlocks provided by the control system computer but not required by the Technical Specifications is an interlock to prevent manual withdrawal of more than one control rod at a time and interlocks to prevent withdrawal of control rods if all scrams are not reset, and if control rod magnet current is not enabled.

2.2.1 Environmental and Seismic Qualification

The new control system is installed in the control room and the reactor room. The staff considers the reactor room to be a mild environment when compared to power plant requirements. 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 and operations of the other systems installed have not revealed any problems regarding temperature or humidity. The new system should not be unduly susceptible to temperature or humidity and is therefore acceptable to the staff.

Although the NRC has not promulgated requirements for the seismic qualification testing of research reactor control equipment, the staff evaluated the equipment to determine general ruggedness. The equipment is mounted in a commercial quality fashion which should prevent the components from moving significantly within the console and racks. In this TRIGA reactor, an inadvertent scram does not present a significant 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 that the chatter of relay contacts could prevent a scram when required. The safety system scram circuits for this system are designed to scram on failure (which includes contact chatter). Therefore, the staff concludes that the system is acceptable.

2.2.2. Electromagnetic Interference (EMI)

The staff evaluated the new equipment to determine if common mode EMI could disable more than one system at a time. The design characteristics of the TRIGA reactor do not allow an inadvertent scram to present a significant challenge to safety systems, although it might hinder operations such as by disrupting an experiment.

The TRIGA uses industrial isolators, which prevent conducted EMI from being transmitted between the control and safety mechanisms. The neutron flux signal cables are shielded to reduce the effect of radiated EMI. Previous experience with similar equipment provided by several different vendors at other facilities has indicated that if EMI causes any perturbance in the system, it will most likely cause a scram, which is not a safety concern. Therefore, the staff concludes that EMI should not prevent a scram when required and that the design is acceptable.

2.2.3 Power Supplies

The power supplies for the system are buffered to reduce the effect of minor fluctuations in the line power. 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 random access memory (RAM) with alternate dc battery power to store constant data during a loss of power. The NM-1000 has self-diagnostic circuits and also has a watchdog timer circuit which places the NM-1000 in a tripped condition and scrams the reactor if power fluctuations prevent the software from operating properly. The General Atomics document, "NM-1000 Software Functional Specification and Software Verification Program" (March 1989) describes the tests performed on the NM-1000 to verify that the system returns to proper operation after the power is restored. The staff finds this acceptable.

2.2.4 Failure Modes and Effects

The licensee's safety analysis included reference to the April 22, 1988 scram circuit safety analysis performed by the University of Texas at Austin to identify the various ways in which the reactor safety system could fail. The staff reviewed this analysis for the AFRRI system installation. These include the following:

(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 analysis was performed using fault trees to predict a failure to scram for various failure modes. The analysis concluded that a failure of all safety systems and therefore, failure to scram was extremely unlikely. The analysis evaluated all failures attributable to the unique failure modes of the software of the NM-1000. The staff has reviewed the analysis of the failure modes and effects of the new system and finds that this analysis is applicable to the UIUC system and that the analysis is acceptable.

2.2.5 Independence, Redundancy, and Diversity

The staff reviewed the data link between the safety channels and the nonsafety systems. The safety channels provide hard-wired scram inputs and are also wired directly to independent indicators on the control console. The operators receive information from both the analog NP-1000 and NPP-1000 power monitors and the digital NM-1000 monitor. The information is displayed on both direct wired bar graphs and on a graphic CRT. The safety channels also provide inputs to the non-class 1E data acquisition computer (DAC) through isolators. The isolators used have not been tested for the maximum credible faults that the staff requires for isolators used in power plants. However, the manufacturer has tested them to standard commercial criteria. The staff concludes that the use of isolators tested to standard commercial criteria is acceptable for the UIUC TRIGA reactor. The DAC is then connected through 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. The CSC would not meet the independence requirements of a power plant because the CSC does interface with the safety channels. However, the staff concluded that this independence was not necessary for the current application at UIUC.

The scram circuit is essentially unchanged from the old to new system in that it has a fail safe design using automatic and manual contacts which open to remove power to the control rod magnets. Redundant fuel temperature inputs are provided to the scram circuit at the UIUC facility. Redundant power level inputs (NP-1000, NPP-1000) to the scram circuit are also provided.

The analog and digital neutron monitors and the addition of a watchdog scram function provide additional diversity and redundancy to the scram system. The system as installed 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."

The staff has concluded that the UIUC control system design maintains an acceptable level of independence, redundancy, and diversity for the UIUC Advanced TRIGA reactor.

2.2.6 Testing and Operating History

GA, AFRRI, the Dow Chemical Company, GSTR, and the University of Texas at Austin have extensively tested the new system and made a significant number of changes to the design during the testing and initial operation of the new system. The staff has reviewed the problems discovered during testing of the

system and concluded that the resolutions appear acceptable. The staff concludes that the installation of equipment having readily available spare parts improves operability and safety. The new self-diagnostic feature allows continuous online testing and reduces the possibility of undetected failures.

2.3 Software Assessment

2.3.1 Criteria

The staff requires an approved verification and validation (V&V) plan for software that performs a safety function or provides information to the operator. At UIUC, the NM-1000 provides inputs to the scram circuit and to the rod withdrawal prevent interlock system block function. As part of the AFRRI and GA amendment approval process, the staff reviewed GA's program for developing the NM-1000 software to determine if the V&V plan was acceptable. The staff has determined that the GA V&V plan is applicable to the UIUC system. The staff compared the GA 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.

2.3.2 Verification and Validation Plan

The staff audited the V&V documentation provided by GA. The NM-1000 at the UIUC TRIGA is wired directly into the scram circuit, and therefore, requires highly reliable software to perform its safety function when required. To assess the NM-1000 software developed by GA, the staff assessed the methodology and procedures used to develop the software by reviewing the V&V documentation through the development process.

Verification and validation are two separate but related activities performed throughout the development of software. Verification is the process by which to determine if the requirements of one phase of the development cycle have been consistently, correctly, and completely transferred to the next phase of the cycle (that is, to determine if the requirements have been fulfilled).

Validation is the testing of the final product to ensure that performance conforms to the requirements of the initial specification. The need for V&V arose because software is very complex, and prone to human errors of omission, commission, and interpretation. V&V provides for an independent verifier to work in parallel with, but independent of, the development team to ensure that human errors do not hinder the production of safety software that is reliable and testable.

In executing V&V, certain principles have proven over time to be very effective in software programs:

- Well defined systems requirements expressed in well written documents
- Development methodology to guide the production of software
- Comprehensive testing procedures
- Independence of the V&V team from the development organization

These principles comprise the foundation from which to apply the applicable criteria for software evaluations of Class 1E safety systems. These principals were used by the staff as guidance in the following review areas.

2.3.3 Independence

The independence of the verifier is a key ingredient in an effective verification process. Sorrento Electronics developed the original software for the NM-1000. After GA obtained the rights to market the NM-1000 for research reactors, it used a software consultant to modify the software. After many changes had been made, GA hired another contractor. Each contractor provided an additional level of independent review for the original design. Although the requirements imply a concurrent review, the staff finds that the verification has been sufficiently independent and is therefore acceptable for research reactors.

2.3.4 Validation Testing

The validation testing must be done by a team that did not help design or implement the software product. GA used the neutron monitoring system acceptance test procedure as part of the validation testing. The staff also reviewed substantial additional validation testing performed at the AFRRI facility. The staff did note a functional description of unknown date which included samples of the computer code. Though the developers knew the specific functions which the NM-1000 was to perform, these functions had never been documented which allows possibilities for omission when preparing test procedures. Upon request from the staff, GA provided functional specification E117-1001 "NM-1000 Software Functional Specification," (March 1989) which lists in detail the functions performed by the NM-1000. This specification included a system of cross reference by which the vendor verified that each specific functional requirement had been tested. The staff finds that this testing and verification is acceptable.

2.3.5 Discrepancy Resolution

Each V&V program should include a process by which to identify, record, correct, and resolve discrepancies uncovered during development. The resolution of a discrepancy must be reflected in all applicable documents, including the source code, the software design specification, the software requirements, and the original systems specification. The staff reviewed discrepancies and other comments provided to GA by the Console Owners Group and found that the process and resolution were documented and appeared adequate. When discrepancies prompted GA to modify the code, GA added to the code notation a description of the changes and the corresponding rationale. The staff finds that GA used acceptable methods to resolve discrepancies.

The licensee provided, at the staff's request, a description of all of the software changes that have occurred since the staff completed the GA review and the configuration management control used to control the various changes and distributions. This information was prepared for UIUC by the vendor, General Atomics. This information included changes made to provide customer specific modifications, product improvement changes, and safety related changes (corrections). The licensee also provided information on six specific

software changes for the UIUC instrumentation and control system. For each of the 21 changes, General Atomics described the requirement, provided the reason for the change, described the solution selected, and assessed the impact on safe operation. The staff has concluded that General Atomics has made appropriate changes and has maintained the necessary configuration control.

2.3.6 Design Approach

The primary software specification provides the foundation for sound development and effective V&V. The individual requirements in the specification for any software system describe the manner in which the software is to behave in any circumstance. The specification must be reliable and testable. A reliable specification exhibits the following characteristics:

- Correct - Each requirement of the safety function has been stated correctly.
- Complete - All of the requirements for the safety function are included.
- Consistent - The requirements are complementary and do not contradict each other.
- Feasible - The requirements can be satisfied with available technology.
- Maintainable - The requirements will be satisfied for the lifetime of the equipment.
- Accurate - The requirements include the acceptable bounds of operation.

The staff reviewed the design approach with GA. The early development is not well documented because the product was sold to GA without all of the supporting information. Though the staff finds that the design approach for the NM-1000 since inception has been erratic, the staff finds acceptable the recent developmental work and the design approach, because it appears to be better organized and controlled.

2.3.7 Software Evaluation

The software development plan for the NM-1000 indicates that GA developed the software for a very specific design goal and that the designers knew the application and the basic requirements for the hardware and software. However, GA did not develop a plan to specify the individual steps in the design project. To verify that each design requirement had been tested, GA developed the NM-1000 software verification program E117-1002 "NM-1000 Software Verification Program" (March 1989). The staff also reviewed working copies of the NM-1000 design input, which demonstrated that the design team clearly understands the functional requirements. The staff concludes that the software should perform its intended safety function as required.

2.3.8 Operator Task Analysis

In reviewing the documents, the staff found that GA had not provided a formal task analysis to support the design of the operator interface. After the equipment and software were substantially designated, the functional requirements and working level descriptions did include the operator task requirements. The staff concluded that, through the V&V process, GA had specified the requirements and incorporated them in the design. Therefore, the task analysis is acceptable.

2.4 Startup Program

The licensee provided their startup routine for the digital control console. Because of space limitations, the new console will not operate in parallel with the old console. The startup routine describes a series of data runs for natural circulation, forced circulation, small reactivity insertions, and pulses. The data will be compared to the data collected with the previous analog control console. The staff concludes that the startup routine provides adequate assurance that the new console will be properly calibrated and, therefore, is acceptable.

2.5 Operator Training

The licensee provided a plan of training for the licensed reactor operators, senior reactor operators, and reactor operator trainees concerning the new console. The training will consist of 40 hours of details of the operation of the console, the structure and operation of the NM-1000, NP-1000, and NPP-1000, the software, the safety circuits, and the computer systems. In addition, GA will provide a one week hands on operation and maintenance course during installation of the console. Each operator will gain experience operating the console in various modes of operation at different power levels with a GA operator present. The staff concludes that the operator training plan for the new digital console will provide operators with classroom and hands on training and is, therefore, acceptable.

2.6 Changes to the Technical Specifications

The only change directly related to the installation of the digital control system is the addition of the watchdog scram to the list of minimum number of reactor safety system channels in TS 3.5.

In addition, the licensee has requested three other changes to TS 3.5. The first would remove a phrase that the reactor power level scram applies to power levels less than 50 kw(t) in the steady state mode of operation. This is incorrect. The power level scram is required at all times when the reactor is in steady state mode and square-wave mode. The staff concludes that this change corrects an inconsistency in the TS and is, therefore, acceptable.

A note in the TS concerning the startup count rate that expired on April 21, 1981 is removed from the TS. The staff has determined that this change is editorial in nature and is therefore, acceptable.

The bases for the power level scrams states that the scrams are provided as added protection against abnormally high fuel temperatures and to assure that the reactor operation stays within the licensed limits. It is more accurate to state that the scrams are provided as added protection against abnormally high fuel temperature such that the reactor will scram before a safety limit is exceeded as discussed in the Safety Analysis Report. The staff concludes that this change more accurately describes the bases for the TS and is, therefore, acceptable.

3.0 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 and changes in inspection and surveillance requirements. 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). This amendment also involves changes in recordkeeping, reporting, or administrative procedures or requirements. Accordingly, with respect to these items, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(10). 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.

4.0 CONCLUSION

The staff concludes that the hardware design of the new GA console is acceptable for use in the UIUC Advanced TRIGA Research Reactor. The software design in the CSC, DAC and NM-1000 will not prevent the safety functions of the hardwired scram circuit from performing and is therefore acceptable.

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 Contributors: J. Stewart
A. Adams, Jr.

Date: February 16, 1993