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

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

SUPPORTING AMENDMENT NO. 29 TO

FACILITY OPERATING LICENSE NO. R-38

GENERAL ATOMICS

DOCKET NO. 50-89

1.0 INTRODUCTION

General Atomics (GA) 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. In December 1988, GA published their safety analysis of the new reactor instrumentation and control system. In this report GA concluded that the new system was 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 (i) 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 (ii) 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 (iii) if the margin of safety as defined in the basis for any technical specification is reduced."

The staff concluded from its review of the GA safety analysis report that NRC review and approval of the replacement computerized control system was required, 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) changes to the Technical Specifications were required.

Pursuant to 10 CFR 50.90, the licensee submitted by letter dated July 19, 1990, a request to amend Appendix A of Facility Operating License No. R-38, "Technical Specifications for the Torrey Pines TRIGA Reactor." The licensee's submittal of July 19, 1990 included the December 1988 safety analysis. The requested amendment would (1) allow installation of the micro-processor based instrument and control system, (2) add the watchdog (software failure) scram to Table 1 of the Technical Specifications, "Minimum Reactor Safety System Scrams", and (3) add a requirement that no more than one of the required two independent power level scram channels in Table 1 be a digital scram channel.

The licensee has installed, in parallel to their existing control console, the new digital microprocessor based instrumentation and control system. The transfer of control from the old to the new system (including scram) was via a

series of gradual steps accompanied by tests which demonstrated 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 was 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 was disconnected. The new console replaced the old analog console in the control room. The primary functions of the new system remained 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 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 reduce the probability of fuel damage to a minimum; 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, 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 GA's Mark I reactor 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).

Similar to AFRRI, the GA Safety System Scram Circuit consists of two analog nuclear power monitor channels (NP-1000, and NPP-1000) and two fuel temperature channels which are hardwired. Different from AFRRI, the NM-1000 microprocessor based nuclear power channel that monitors reactor power is wired to the scram circuit and provides input to rod block. Also, wired into the scram circuit at GA are contacts for manual scram, facility power supply failure scram, key switch scram, and watchdog (software failure) scram. Further, although not required by Technical Specifications, there are scram features on (1) detector

high voltage failure on any one power channel, (2) loss of ac power to the Instrumentation and Control System due to earthquake switch trip, (3) externally generated conditions, and (4) reactor power reaching 1100 MW during a pulse.

2.1 Environmental and Seismic Qualification

The new control system is installed in the control room and the reactor hall. The staff considers the reactor hall 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 and operations, to date, have 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 considered the equipment to determine general ruggedness. The licensee indicated that the equipment is mounted in a 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 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; and 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 significant challenge to safety systems, though it might cause operational difficulties such as disrupting an experiment.

Industrial-type isolators are generally used which prevent conducted EMI from being transmitted between the control and safety mechanisms. 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 perturbance in the system it will most likely cause a scram, which as previously discussed is not a safety concern. 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 December 1988 safety analysis included 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 considered. The staff concludes that the failure modes and effects of the new system were acceptably addressed.

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. The operators are provided with 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. In addition, the safety channels provide inputs to the Non-Class 1E Data Acquisition Computer (DAC) through isolators. The 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, but the staff concluded it was not necessary for the current application at GA.

Further, the scram circuit is essentially unchanged in that it maintains the fail safe design using the same automatic and manual contacts which open to remove power to the control rod magnets. For the GA facility, redundant fuel temperature inputs are provided to the scram circuit. Redundant power level inputs (NP-1000, NPP-1000) to the scram circuit are also provided.

This system has also added the computer watchdog scram and the digital NM-1000 scram. At GA, in addition to the NM-1000 being wired to the scram circuit, it provides inputs to the rod withdrawal prevent interlock system. The use of both analog and digital neutron monitoring, and the watchdog scram function provides 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 level of independence, redundancy and diversity which has been maintained is acceptable for the GA TRIGA reactor.

2.6 Testing and Operating History

Extensive testing of the new system has been done by both GA and AFFRI. A significant number of design changes took place during the testing and phase-in of the new system. The staff has reviewed the problems discovered during testing of the system and has concluded that the resolutions appear acceptable. The staff also agrees with the licensee that long-term operability and safety is enhanced due to installation of equipment which has spare parts readily available. 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 GA, the NM-1000 provides inputs to the scram circuit and 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 audited the verification and validation documentation provided by General Atomics. For the installation at the GA TRIGA the NM-1000 is wired directly into the scram circuit, and therefore requires highly reliable software to perform its safety function when required. The assessment of the

NM-1000 software built by General Atomics is an assessment of the methodology and procedures used to develop the software. The process is evaluated by reviewing the verification and validation trail through the development process.

Verification and validation (V&V) are two separate but related activities that follow the development of software. Verification determines whether the requirements of one phase of the development cycle have been consistently, correctly, and completely transformed (fulfill the requirements) to the subsequent phase of the cycle. 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 a well written document.
- Development methodology to guide the production of software.
- Comprehensive testing procedures.
- Independence of the V&V team from the development organization.

These principles can serve as a comprehensive reference base for applying the applicable criteria for software evaluations of Class 1E safety systems, and were used as guidance in the following review areas.

3.3 Independence

A key ingredient in an effective verification process is the independence of the verifier. For the NM-1000 the original software was developed by Sorrento Electronics. After General Atomics obtained the rights to market the NM-1000 for research reactors, a software consultant was used to modify the software. After many changes had been made another contractor was brought in. Each contractor in turn assured an additional level of independent review from the original design. Though the requirements imply a concurrent review the staff finds that the verification has been sufficiently independent and is therefore acceptable for research reactors.

3.4 Validation Testing

The validation testing must be done by a team that did not participate in the design or implementation of the software product. General Atomics used the Neutron Monitoring System Acceptance Test Procedure as part of the validation testing. In addition the staff reviewed substantial additional validation testing which has been performed at the AFRRI facility. The staff did note a functional description of unknown date which included samples of the computer code. Though the people involved in development knew the specific functions

which the NM-1000 was to perform these had never been written down, which allows substantial possibilities for omission when preparing test procedures. Upon request from the staff, General Atomics provided the functional specification E117-1001 (March 1989) which lists in detail the functions performed by the NM-1000. Included in this specification was a cross reference where the vendor verified that each specific functional requirement had been tested. The staff finds that this testing and verification is acceptable.

3.5 Discrepancy Resolution

A key element in any verification and validation effort is the process by which discrepancies uncovered during development are recorded, identified, resolved and corrected. The resolution of a discrepancy must be reflected in all applicable documents (e.g., source code, the software design specification, the software requirements, and the original systems specification). The staff reviewed discrepancies and other comments provided to General Atomics by the Console Owners Group and found that the process and resolution were documented and appeared adequate. When discrepancies resulted in code modification, a description of the changes and it's reason was added to the code annotation. The staff finds the discrepancy resolution methods by General Atomics to be acceptable.

3.6 Design Approach

The primary, software specification provides the foundation for not only sound development, but also for effective verification and validation activities. The individual requirements in the specification for any software system describe how 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.
- Maintainability - The requirements will be satisfied for the lifetime of the equipment.
- Accuracy - The requirements include the acceptable bounds of operation.

The staff reviewed the design approach with General Atomics. The documentation was found to be lacking in several areas with the most significant being the lack of a functional requirements specification which GA has since prepared. Documentation of the early development was sketchy which was attributed partially to the transfer of the product without including all of the backup information. The documentation of recent changes has improved significantly. Though the staff finds that the design approach for the NM-1000 since inception has been erratic, the recent, development work appears to be improved in structure and control.

3.7 Software Evaluation

The software development plan for the NM-1000 appears to the staff to be a very specific design goal oriented development, where the application and basic hardware and software requirements were known by the designers; however, there was no step by step plan developed. The failure to have a step by step plan such as described in ANSI/IEEE 7-4.3.2 - 1982 resulted in the need for General Atomics to retrofit the functional requirements document and verify that each requirement had been tested. To meet this requirement GA developed the NM-1000 software verification program (E117-1002 March 1989). The staff also reviewed working copies of the NM-1000 design input which demonstrates that the functional requirements are currently well understood by the design team and concludes that the software should perform its intended safety function as required.

The staffs review indicated that GA could benefit through the development of a corporate software development plan that can be applied to any future Class 1E software prior to starting design. The plan could include a description of the development phases in sufficient detail so that the verification and validation efforts can be initiated at the beginning of any design effort. The plan could also contain a taxonomy of documentation, and reviews which demark the injection points for verification and validation activities. A corporate software development plan for Class 1E systems could prove to be effective in the development of reliable software consistent with the intent of ANSI/IEEE-ANS-7-4.3.2 - 1982.

3.8 Operator Task Analysis

In reviewing the documents it became apparent that there was not a formal task analysis to support the design of the operator interface. The initial specifications and descriptions were vague. After the equipment and software were substantially designed, the functional requirements and working level descriptions did include the operator task requirements. A task analysis prior to development would probably have minimized the software iterative process and therefore provided less opportunities for error. The staff concluded that through the V&V process the requirements have been specified, and incorporated in the design. Therefore, the V&V plan is acceptable.

4.0 TECHNICAL SPECIFICATIONS

As previously discussed, the presentation of correct, timely information to the reactor operator contributes to the safe operation of the reactor. The scram circuit at GA will include watchdog timer contacts which will provide a scram upon software failure. Therefore to assure the presentation of timely, correct information to operators or the proper safety system scram, the watchdog scram inputs are added to Table I, Minimum Reactor Safety System Scrams of the Technical Specifications. Additionally to assure acceptable diversity of the new system, Table I has been amended to specify that of the minimum required two independent power level channels, no more than one channel shall use digital processing of power detector signals.

5.0 ENVIRONMENTAL CONSIDERATION

This amendment involves changes in a requirement with respect to 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 GA TRIGA 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 technical specifications are amended to include the watchdog scram inputs and maximum use of digital power measurement channels.

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: October 4, 1990