UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC, 20555-0001

July 30, 1998

Mr. Joseph Naser
Manager, Instrumentation and Control
Energy Conversion Division
Electric Power Research Institute
3412 Hillview Venue
PO Box 10412
Palo Alto, CA 94303

SUBJECT: SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION ELECTRIC POWER RESEARCH INSTITUTE (EPRI) TOPICAL REPORT, TR-107330, FINAL REPORT, "GENERIC REQUIREMENTS SPECIFICATION FOR QUALIFYING A COMMERCIALLY AVAILABLE PLC FOR SAFETY-RELATED APPLICATIONS IN NUCLEAR POWER PLANTS"

Dear Mr. Naser:

By letter dated January 9, 1998, EPRI submitted topical report TR-107330, Final Report, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety - Related Applications in Nuclear Power Plants," dated December 1996, for staff review. EPRI submitted an amendment letter dated 4/24/98 to address some additional quality assurance issues. The staff has completed the review of the non-proprietary topical report and the amendment letter dated 4/24/98 and prepared the enclosed safety evaluation report approving TR-107330 as modified by letter of 4/24/98.

TR-107330 presents a requirements specification for generically qualifying a commercially available PLC for safety-related applications. The goal of this requirements specification is to define the essential, critical technical characteristics that must be included as part of a PLC design for use in a range of safety applications. System and software development and quality processes are addressed in t,..s specification primarily by references to published standards and guidelines.

The TR-1 07330 guidance provides for some flexibility in the specific methods for performing the verification activities involved in qualifying a PLC consistent with staff requirements. Licensees referencing T R-107330 for a proposed digital modification should document the qualification process such that there are descriptions and justifications for the methods selected which will support the use of the specific PLC product in a safety-related application. Because the term "PLC" is used by various manufacturers to label digital equipment with capabilities that vary from relatively simple to very complex, care should be exercised to assure that the TR-107330 guidance is not used to attempt to qualify equipment beyond the intended scope.

Based on the review of TR-107330 and the 4124/98, EPRI letter the staff concludes that TE-107330 contains acceptable requirements specification guidelines for licensees use in procuring a particular vendor's PLC for use in safety system applications. Use of the TR-

107330 approach when designing digital modifications will provide licensees with a requirements specification that will enable the PLC design to meet the requirements of 10 CFR Part 50 as identified in section 1 of this SER and the guidance of SRP, Chapter 7, "Instrumentation and Controls" concerning digital instrumentation and control systems.

While the staff finds TR-107330, as modified by the 4/24/98 EPRI letter, acceptable, it should be noted that TR-1 07330 provides only generic requirements for pre-qualifying commercial PLCs for use in safety-related applications. For a plant specific PLC application, the staff review will ensure that the PLC requirements specification has in fact been followed and that the system design meets all of the applicable regulations and guidance as provided in 10 CFR Part 50 and in SRP Chapter 7, for the specific application proposed. This includes a number of plant specific concerns such as diversity, EMI/RFI, separation criteria, and maintenance training that must be satisfied before the PLC system design can be found acceptable in a plant specific safety system design. For plant specific applications, the licensee is responsible for determining whether the specific design incorporating the PLC can be implemented without prior NRC staff approval in accordance with the requirements of 10 CFR 50.59. NRC staff approval of EPRI TR-107330 does not provide this determination.

If you have any questions regarding this safety evaluation report, please contact Jim Stewart at (301) 415-2824, e-mail: jcs1@nrc.gov.

Sincerely,

Thomas Essig, Acting Chief
Generic Issues and Environmental
Projects Branch
Division of Reactor Program Management
Office of Nuclear Reactor Regulation

Project No. 669

Enclosure: Safety Evaluation

cc: See next page

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION ELECTRIC POWER RESEARCH INSTITUTE TOPICAL REPORT, TR-107330, "GENERIC REQUIREMENTS SPECIFICATION FOR QUALIFYING A COMMERCIALLY AVAILABLE PLC FOR SAFETY-RELATED APPLICATIONS IN NUCLEAR POWER PLANTS"

1.0 SUMMARY

By letter dated January 9, 1998, the Electric Power Research Institute (EPRI) submitted TR-107330 Final Report, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," (December 1996) for staff review. A modification to TR-107330 clarifying quality assurance commitments was submitted by letter dated April 24, 1998. This non-proprietary topical report was prepared by the EPRI Working Group on Qualification of Commercially Available Programmable Logic Controllers for Safety Related Applications. The EPRI working group included utility engineering staff from multiple disciplines including instrumentation and control, electrical, quality assurance and procurement. The EPRI working group also invited participation from vendors and NRC staff.

TR-107330 presents a specification in the form of a set of requirements to be applied to the generic qualification of Programmable Logic Controllers (PLCs) for application and modification to safety-related instrumentation and control systems in nuclear power plants. This includes the use of PLCs in safety systems that may not be categorized as instrumentation and control systems such as PLCs that are embedded as part of electrical (switchgear control) or mechanical (motor operated valve limit switch control) applications. The requirements specification is intended to be suitable for use in:

- Procuring a PLC with an appropriate selection of input/output (I/O) and other types of modules that encompasses a broad range of potential safety related applications.

- Demonstrating that the PLC operating software quality is adequate for use in nuclear power plant safety systems.

- Demonstrating that a selection of PLC hardware is suitable for use in safety systems whose requirements lie within the qualification envelope.

- Defining requirements and contents for an application guide that will define the qualification envelope, the baseline configuration control information, and other appropriate information. The guide is intended to be used as the basis for a specific application.

In addition, the specification is intended to be consistent with the [associated] requirements of 10 CFR Part 50, Appendix B[1].

---

[1] The term [associated] requirements of 10 CFR 50 Appendix B is used to clarify that the QA criteria addressed in EPRI TR-107330, while intended to be consistent with the criteria given in Appendix B, are bounded by the activities directly related to the development and manufacture of a PLC and are, therefore, not complete. That is requirements contained in this document do not include all quality assurance (QA) procedures that are necessary for a PLC vendor to be a qualified 10 CFR Part 50, Appendix B supplier.

This safety evaluation report (SER) provides the results of the staff's review of TR-107330 as modified by the 4/24/98 letter, against applicable regulatory guidance for safety-related digital instrumentation and control (I&C) systems. The staff has determined that the TR-107330 guidance is in compliance with the acceptance criteria identified in Chapter 7, "Instrumentation and Controls," Table 7-1 of the SRP, that are applicable to the generic qualification of a PLC as a component for safety-related applications. The associated regulatory requirements (10 CFR Part 50) are: 50.55a(a)(1), "Codes and Standards," 50.55a(h), "Protection Systems," General Design Criteria (GDC-10 CFR Part 50 Appendix A), GDC 1, "Quality Standards and Records," GDC 2, "Design Bases for Protection Against Natural Phenomena," GDC 4, "Environmental and Dynamic Effects Design Bases," GDC 21, "Protection System Functions," GDC 23, "Protection System Failure Modes," GDC 24, "Separation of Protection and Control Systems," GDC 25, "Protection System Requirements for Reactivity Control Malfunctions," and GDC 29, "Protection against Anticipated Operational Occurrences." TR-107330 is intended to provide a qualification envelope that should meet the above listed criteria for a wide range of plant specific applications. Any plant specific application will need to verify that the qualification envelope provided by qualification to the guidance of TR-107330 does meet the requirements of the application. TR-107330 is intended to meet the guidelines given in SRP Table 7-1 which includes applicable regulatory guides and branch technical positions. TR-107330 also includes specification information that may be important for a vendor/system designer/utility (e.g., ease of maintenance, cost, potential future upgrades, etc.) but are not required for regulatory considerations. Because the term "PLC" is used by various manufacturers to label equipment with capabilities that vary from very simple to very complex, care should be exercised to assure that TR-107330 guidance is not used to attempt to qualify equipment beyond the intended scope. Because TR-107330 is generic, licensees referencing TR-107330 will need to document the details regarding the use of this specification in plant specific applications. This is discussed in more detail in the following sections. This SER is organized with the same section numbering and topics as TR-107330.

1.1 Background

PLCs have been widely used in industrial facilities for more than 20 years. A PLC is a collection of hardware and software specifically designed to perform a sequence of user-defined control actions that were traditionally implemented using electro-mechanical (e.g. relays) and single function electronic devices (e.g. single-loop controllers). The controls for most of the safety systems in nuclear power plants are of this type.

Since its inception, PLC hardware was designed to operate reliably in industrial environments. Therefore, most commercially available PLC hardware should be capable of withstanding the stresses applied to it during qualification testing for use in a nuclear safety system in a mild environment. However, PLCs contain both application and operating software which require a broader qualification effort.

An advantage of a PLC is that its programming “language” uses symbols that are readily related to control and protective actions or to electro-mechanical devices that are used to implement these actions. A second advantage is that they can utilize existing operator controls, final actuating devices, and isolation devices by connections to input/output (I/O) points on the PLC.

1.2 Overview of Technical Scope and Focus and Regulatory Review

The goal of TR-107330 (the PLC Generic Specification) is to define the essential technical characteristics, (e.g., I/O points and options, scan rates, software features, etc.) that must be included to cover the needs of a range of plant safety-related I&C system applications. Process-oriented activities, including system and software development and quality processes, are addressed in this specification primarily by reference to published standards and guidelines.

The technical scope focus and content of this specification is based on the steps involved in completing a generic qualification effort. Performing the qualification requires, in effect, creating a synthetic application so the steps are similar to those used in qualifying any device for nuclear safety-related service. The steps are:

A. Selecting a PLC product line that supports the requirements of this specification (§4, System Requirements) and the required functionality of nuclear safety-related applications. The selection process includes selecting the set of PLC modules to be qualified.

B. Evaluating the manufacturer's (including third party or sub-tier suppliers) hardware and software QA programs (§7, Quality Assurance) applied to the products of interest to determine if they are adequate to support nuclear safety-related applications with a reasonable set of supplementary activities. The evaluation includes factors relating to both generic qualification and future applications of the qualified products.

C. Procuring a set of modules and any required supporting devices and software from the PLC manufacturer or third party suppliers to be used as the qualification test specimen.

D. Defining and producing a Test Specimen Application Program (TSAP) (§5, Acceptance/Operability Testing). The TSAP involves creation of a synthetic application designed to aid in the qualification tests and operability testing.

E. Combining the modules and the TSAP into a suitable test configuration and performing a set of acceptance tests on the test specimen. This involves conducting a system integration test for the test specimen.

F. Specifying the set of qualification tests to be performed on the test specimen (§6, Qualification Testing and Analysis), including defining a set of operability tests to be performed at suitable times in the qualification process. The operability tests are designed to demonstrate satisfactory operation under the stresses applied during qualification tests.

G. Performing the qualification tests and documenting (§8, Documentation) the results. Results documentation includes producing documentation that defines the qualification envelope[2], specific products that were qualified, and other application information and application guidance for using the qualified PLC in a specific application.

---

[2] Since a PLC is a modular device, the arrangement of the modules has the potential to change the stresses that occur during seismic and environmental testing. Therefore, the testing should be designed to provide bounding conditions for these stresses.

The goal of this specification is to provide generic requirements for pre-qualifying commercial PLC lines for use in safety-related applications in nuclear power plants, therefore, the utility or its designee will need to complete the tasks necessary to actually apply the qualified PLC in a specific plant application.

The staff's review of TR-107330 was limited to the generic qualification of a PLC as a commercially available component and the requirements needed to qualify the PLC for safety-related applications. For a few topics contained in the EPRI topical it was necessary to consider system level application requirements or guidelines to assure that the PLC as a component was in compliance with such applications. This was accomplished by reviewing the PLC generic requirement specification against the acceptance criteria and guidelines given in Sections 7.2 through 7.9 of the SRP. In addition, since TR-107330 and, therefore, the SER are primarily concerned with the PLC as a commercially available component, an effort was made to maintain consistency with the applicable sections of the related topical report EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," and the staff SER approving this topical report.

The format and content of EPRI TR-107330 was selected to provide a logical organization of the material presented. This SER compares this material to the guidance in SRP Chapter 7 which provides the staff determination of acceptability of that material. When additional guidance is necessary to ensure that a particular aspect in the TR-107330 material is complete, the SER provides that information. Licensees using TR-107330 should also consider the contents of this SER when pursuing plant specific modifications.

The assessment of compliance of TR-107330 guidance with the applicable regulations, identified as acceptance criteria in SRP Table 7-1, are given in the following sections of the SER.

1.3 Overview of Roles in PLC Applications To Nuclear Safety Systems

The demonstration of qualification of a PLC involves a defined process. A discussion of process-oriented activities should consider the question of what organizations perform each of the activities. The process requirements in this specification only relate to completion of the activities, without specifying which organization actually performs them. Nevertheless, it is useful to clarify key roles that are referred to throughout the generic specification. In any given circumstance, different organizations (utility, consultant, reactor vendor, equipment manufacturer, etc.) may assume one or more of the roles in the PLC qualification process. Some important roles in the process are:

The **manufacturer** (sometimes called the PLC vendor) produces the generic PLC product line for the commercial marketplace.

The **qualifier** (or generic qualifier) is responsible for confirming that the PLC product meets the requirements of this specification. The qualifier could be one or more utilities, an independent consultant or test lab, EPRI, or another organization. The role of qualifier is not concerned with any particular application. The qualifier is responsible for demonstrating that 10 CFR Part 50, Appendix B and 10 CFR Part 21 requirements are met. The qualifier is the principal user of this generic specification.

The **applier** is responsible for designing, implementing, and testing the specific application in a specific plant. This role includes the application-specific activities which are not covered by the generic qualification. The applier could be the utility, a contractor, system integrator, or a reactor vendor.

The **utility** itself has ultimate responsibility as operator of the plant for the safety application of the PLC and its impact on plant safety, regardless of whether the utility itself has performed any of the above roles.

Note that a particular organization, such as the utility or a consulting firm, can assume multiple roles on a particular application project. Alternatively, one of the roles (e.g., qualifier) may be performed jointly by multiple organizations (e.g., the utility and its consultant). Thus, the generic specification in no way prescribes what organization fulfills the responsibilities of these roles.

1.4 General Overview

This section provides the overall basis for the various PLC requirements described below, discusses generic vs. application specific considerations and addresses the use of third party hardware and software modules.

The PLC architecture overview describes a main chassis with a selection of input/output (I/O) modules, processor modules and power supplies. The application program is executed in a continuous loop. Because TR-107330 is a generic qualification document, it includes many requirements that are not addressed by the regulatory criteria. These were included by the working group so that TR-107330 could be used in preparing procurement specifications. In addition to items of regulatory concern, TR-107330 addresses issues of ease of maintenance, future expansion, cost, the number and types of I/O that the PLC platform can support for multiple applications, etc. It is acceptable to the staff for these additional design requirements to be included in TR-107330.

The qualification parameters generally assume that the PLC will be located in a mild environment. TR-107330 notes that some of the qualification parameters may be tailored for a particular site. In any case, the generic qualification envelope must meet the plant specific application requirements, or alternative plant specific qualification is necessary.

The generic PLC qualification is intended to provide a platform that meets a wide range of safety system applications. The implementation of a specific application may fall within the generic qualification envelope, or additional qualification activities may be needed when the generic qualification envelope can not be met. TR-107330 provides several examples of licensing issues that need to be considered, depending on the specific application proposed for the generically qualified PLC. An example is a defense in depth analysis which requires a plant wide evaluation for a reactor protection system upgrade proposal.

TR-107330 notes that for some PLCs, software and hardware may be available from third party vendors. Third party items are not included in TR-107330 and, therefore, would need to be qualified or dedicated as part of the specific application.

TR-107330 discusses the various amount of redundancy that PLC configurations may have. These equipment redundancies are provided for reasons of availability or maintainability, not necessarily to meet regulatory requirements. For example, a PLC could have redundant power supplies within a single safety channel which would exceed the licensing basis single failure criterion per IEEE 279. The licensing basis redundancy requirements for the safety-related system undergoing modification remains the same as before the PLC retrofit. The system level requirements of IEEE 279 (or IEEE 603 depending upon the licensing basis) would still be maintained. This section of the TR-107330 is acceptable to the staff.

1.5 Specification Organization

This section describes the layout of the specification. For ease of review, this SER follows the same layout. TR-107330, Table 1-1, provides a cross reference from the requirements to the various test and documentation sections.

2.0 DEFINITIONS, ABBREVIATIONS, ACRONYMS

The definitions, abbreviations and acronyms (including some from IEEE 610.12) are in common usage in the industry, or are clearly defined. These are acceptable to the staff.

3.0 REFERENCE DOCUMENTS

Applicable reference documents are those documents that are used primarily as a basis for some of the requirements given in the specification. In addition to the requirements that apply to all safety system equipment (such as 10 CFR 50, Appendix B quality assurance requirements), the document list in TR-107330 includes the IEEE computer standards currently endorsed by the staff with regulatory guides. The list of applicable documents is acceptable. Information documents are used primarily for additional information and guidance. This list includes the regulatory guides, other EPRI publications, and additional US and international standards. The use of these documents for additional information is acceptable.

4.0 SYSTEM REQUIREMENTS

4.1 Overview of Performance Basis

The basic PLC performance requirements identified in TR-107330 (e.g. speed, accuracy) are derived from the plant equipment characteristics and safety analyses. With respect to environmental conditions, this specification assumes the equipment will be located in a mild environment.

4.2 Functional Requirements

TR-107330 specifies an overall response time from input to output of 100 milliseconds or less. TR-107330 notes that some system's response time requirements will not be met by this response time (such as a BWR Reactor Protection System input that may require a response time of 20 milliseconds or less), therefore, a PLC that meets the requirements specified in TR-107330 may not be suitable for all applications. The selected response time is a compromise that is intended to envelope the largest number of potential applications. With the caveat that the actual application response must be verified, this requirement is acceptable to the staff.

TR-107330 specifies the number of I/O points. These were selected to provide coverage of as many applications as reasonable. The control functional requirements will be provided in a high-level language with symbology that is related to the specific control action. The PLC will have standard control features such as the emulation of relay coils and contacts, timers, comparators, etc. The capability for special features (calculated math functions, etc.) may also be provided. The control features are acceptable to the staff.

TR-107330 establishes an overall availability goal of 0.99 for a PLC with a specified configuration to support plant/system availability and maintenance goals. EPRI notes that this is not a requirement and the deterministic criteria of IEEE 603 and IEEE 7-4.3.2 will still be applied to the PLC design. The calculation of availability will conform to IEEE 352 and will use MIL STD 217F for estimating the reliability of individual components. The calculation will consider failures that are detected by on-line diagnostics, various surveillance intervals, mean time to repair, and environmental stress. Testing criteria are provided. Guidance is provided on calculating availability for PLCs that include redundancy within one channel. Fault tolerant and failure detection features may be used to increase the availability of the PLC. The potential negative effects of increased complexity and scan time will be included in the availability analysis. TR-107330 also allows operating experience to be used as a basis for establishing module failure rates if adequate data and supporting information are available. The staff does not consider numerical reliability/availability as a sole means of meeting NRC regulations, however, it can provide additional insight into the expected operation of the PLC and is acceptable to the staff as supporting information to the deterministic criteria of the SRP. Use of numerical reliability/unavailability for software-based systems is not acceptable as a sole means of meeting NRC requirements because software-based system failures are not random."

A failure mode and effects analysis (FMEA) will also be performed on the PLC platform during generic qualification in accordance with the relevant sections of IEEE 352. This information can then be used as an input to the system level application specific FMEA.

The PLC will have a watchdog timer or equivalent method of detecting a failure to complete a scan. The timer will not depend on the same clock source as the processor. The staff finds this acceptable.

The qualification process will include an analysis to provide the information needed to support an application specific setpoint analysis per ISA SP 67.04 (as endorsed by Regulatory Guide 1.105). This includes uncertainty/allowables, calibrated accuracy, hysteresis, repeatability, temperature sensitivity, drift, and the effects of power supply variations. The accuracy of any mathematical calculations will be included. Environmental effects are considered. This is acceptable to the staff, however, the final setpoint determinations are plant specific and will be reviewed as part of the plant specific application. The staff finds the PLC functional requirements specified in Section 4.2 of TR-107330 to be consistent with the guidelines of SRP Chapter 7 and, therefore, acceptable.

4.3 Hardware Requirements

The generic qualification of the PLC will require several different types of I/O modules while any specific application will typically only require a few. All of the modules will be qualified to the guidance in section 4.2 of TR-107330. While TR-107330 discourages the use of external (from the PLC) devices it acknowledges that there may be some applications that require it. If

external devices are used, they must be included in the qualification program.

The analog input requirements specify that the converted value will stay at the maximum/minimum value during over range and under range conditions up to twice the rated input. The out of range condition will be indicated with a flag that is available to the application program. The application will determine if these conditions are to be alarmed.

The voltage input requirements specify the standard voltage input values used in operating plants. Group-to-group and module isolation requirements are specified. This isolation is provided to minimize interference between different signals in the same PLC and should not be confused with the isolation requirements of IEEE 603/279 for separation between safety and non-safety and between different channels of a safety system.

The current input requirements specify the standard current input ranges and isolation parameters. The hardware response time for the modules are not specified but rather are to be evaluated to show that they can support the overall response time for all modules and processors. The individual contribution of any module type to the overall response time may vary.

The RTD input modules will support both European and US standard 2,3, and 4 wire elements. The thermocouple input modules will have 8 (or more) measurement spans included. The maximum cable length and minimum cable size are also specified. The cable parameters were selected as the extremes for most applications. The temperature ranges were selected as the most commonly used industrial thermocouple types, 4 of which are the most commonly used in LWRs. The modules must detect open thermocouples.

The PLC I/O modules will provide for discrete AC and DC inputs. Surge withstand and group-to-group isolation will be provided and tested in accordance with IEEE C62.41. The PLC modules will provide for transistor-transistor logic (TTL) input. The modules will also provide for at least two pulse inputs with the parameters as provided in TR-107330. As previously noted, all of the inputs must be verified to be adequate for any particular application. The inputs listed above should meet a wide variety of applications and are acceptable to the staff.

The output modules listed in TR-107330 follow a similar format to the input modules in specifying output levels, accuracy, resolution, isolation and surge withstand. The output modules include voltage, current, solid state discrete (AC and DC), relay, and TTL capabilities. The output modules should be capable of satisfying the requirements for a wide variety of applications and are acceptable to the staff.

TR-107330 provides processor loop time requirements, memory capacity and data retention capability requirements. The ranges selected should support a wide range of applications. The memory used to contain the application program, constants, and parameters will be capable of retaining the information for a minimum of 6 months without power. Section 4.7.4 of TR-107330 identifies any batteries used in the PLC to maintain memory as items to be identified and included in a scheduled maintenance/surveillance program. The plant specific application should identify any requirements for fire protection as a result of using batteries.

Data acquisition requirements are provided including the specification that isolation and surge withstand will be provided such that applying the voltage levels specified in section 4.6 of TR-

107330 to the interconnection path between the main processor and the I/O modules will not damage any other module in the main chassis nor cause disruption of the operation of the main chassis backplane signals that could result in the loss of the ability to generate a trip signal. The staff considers that the isolation and surge withstand requirements of this section of TR-107330 provides a significant degree of segmentation and functional diversity between signals within a single safety channel and is, therefore, acceptable.

Communication port requirements are provided in TR-107330. The ports are specified as supporting at least 9600 Baud and providing RS-232, RS-422, RS 485 or other widely used standard physical layer protocol. The staff notes that the Baud rate must be shown to support the timing requirements for any specific application.

TR-107330 notes that coprocessors may be provided and specifies the hardware requirements that should be applied. TR-107330 specifies that the chassis of the PLC will be suitable for mounting in a standard 19 inch rack and will have positive hold downs sufficient to meet the generic seismic requirements. If redundancy within a channel is provided to meet availability/reliability goals, TR-107330 provides requirements for transfer mechanisms and failure detection.

The normal (60-104°F) and abnormal (40-120°F) temperature range requirements are specified in TR-107330. The staff notes that the a plant specific environmental conditions must be evaluated for the specific application including consideration of the power source for the ventilation of the cabinet and room (IE or non-IE) and the length of time of the station blackout requirements of the plant. The PLC will be qualified to the electromagnetic interference/radio frequency interference (EMI/RFI) levels and electrostatic discharge (ESD) requirements as specified in EPRI TR-102323 which has been previously accepted by the staff (SER dated April 17, 1996) as an acceptable means of qualifying digital equipment for EMI/RFI. The staff finds the PLC hardware requirements specified in Section 4.3 of TR-107330 to be consistent with the guidance of SRP Chapter 7 and, therefore, acceptable.

4.4 Software/Firmware

The main processor executive capability requirements are listed. Though not a requirement, the main processor operating system is often a relatively (when compared with general purpose operating systems) small and simple system referred to as an "executive." TR-107330 describes a preference for a continuous deterministic cycle behavior with a minimum of interrupts. This is consistent with the acceptance criteria in SRP, Chapter 7 and is, therefore, acceptable to the staff.

Unintended and unused functions are not addressed in any specific requirements in TR-107330, however, the failure modes and effects analysis (FMEA) (section 6.4.1) supports the analysis and resolution of abnormal conditions and events described in IEEE 7.4.3.2 including potential unintended functions.

Coprocessor (if used) requirements are provided and are similar to the main processor executive requirements.

The application software media provided may be on either 3-1/2 inch floppy discs or on CD-ROM. The media will be labeled with contents, revision level, and any serial numbers assigned.

The software will include electronic identification. Configuration management consistent with the standards listed in SRP Chapter 7 will be maintained by the vendor, dedicator, and/or licensee.

TR-107330 was written with the assumption that the PLC will use ladder logic or similar language for programming the application. TR-107330 specifies that the PLC will have the capability to simulate relay coil and contacts, timers, counters, comparators, and proportional integral derivative (PID) controls. In addition to simulating traditional electromagnetic and electronic instrumentation and control equipment the PLC will also be capable of performing a variety of math functions such as multiplication and square roots.

Development tools for programming, debugging, and program documentation will be provided. These tools may be used in a personal computer or special programming device. The requirements specify interfaces (PLC, printer, display, remote storage capability) and debugging aids. The specification also includes the ability to perform a bit-by-bit comparison between the program that is in the PLC and a program contained in the programming device. Security requirements are also specified. Tools will be maintained under configuration management. The quality of the tools and their appropriate use are reviewed during the quality assurance review activities described in section 7 of TR-107330. The staff finds the above requirements for tools acceptable.

General configuration control issues are addressed in section 7.7 of TR-107330. Section 4.4.5 specifies the attributes that the PLC executive and/or software tools will include from the vendor in order to facilitate maintaining configuration management following delivery. This is in addition to the guidance of IEEE 828 and the guidance of IEEE 1042 that should have been used during the manufacture of the PLC and the tools. An electronic revision level will be embedded in the PLC executive. Any device that contains firmware or other programmed information will be marked with the revision level. Any software tool or other device that is capable of modifying an item that is under configuration control will include security features to prevent unauthorized access. This is acceptable to the staff.

TR-107330 provides a list of 14 fault conditions that may occur in a PLC, a method or test to detect the fault, and action to be taken upon fault detection. Power up diagnostic requirements are also provided. These diagnostics in combination with the continuous self-diagnostics and surveillance testing are intended to detect all failures that could prevent the PLC from performing its intended safety function. The staff considers that detection of all failures is difficult to prove, however, the staff finds the described self-diagnostics and fault detection features to be acceptable.

Data base management capabilities include storing the user-defined constants in non-volatile memory and providing for reading and modifying the constants. Redundant PLCs (within a channel) will provide features to verify that the constants are the same.

Ladder logic is the prominent language for PLCs, however, sequential logic languages and high level languages are also addressed in the TR-107330 requirements. The staff finds the use of these languages in place of or to supplement ladder logic to be acceptable.

The PLC is required by TR-107330 to provide a sequence of events (change in state of inputs or outputs) recording capability with up to 50 events and an accuracy of one scan cycle +/-

50ms. The PLC software/firmware requirements described in section 4.4 of TR-107330 are acceptable to the staff, as they are consistent with the guidelines in SRP Chapter 7 for safety-related systems.

4.5 Human/Machine Interface (HMI)

Most of the HMI features used by the operators in a PLC-based system are not part of the PLC itself and, therefore, would be qualified separately. Requirements are provided for HMI actions that are on the PLC such as increasing and decreasing a setpoint. The interactive equipment for programming and maintenance are connected through a dedicated port on the PLC. System response times, display requirements and alarm processing requirements are provided. Plant specific HMI requirements will be addressed during the specific application design. The above HMI approach is acceptable to the staff.

4.6 Electrical

TR-107330 specifies AC and DC voltage requirements that are intended to envelope most operating plant electrical systems. As with the other generic specifications of TR-107330, there may be some unique applications that the requirements of TR-107330 do not bound. This case would be addressed in the plant specific application. The power supplies will be qualified in accordance with sections 4.3 and 4.6. Specifications are also provided for power supplies to drive external instrumentation loops.

Surge withstand capability will be tested per Section 9 of IEEE C62.41. TR-107330 lists 11 test points and specifies that the surge will not damage any other module or device in the PLC or cause disruption of the operation of the backplane signals or any other data acquisition signals that could result in a loss of the ability to generate a trip. These tests are within one device and are not intended to demonstrate isolation between channels or between Class 1E and non-Class 1E systems. Any isolation devices provided as part of the PLC or as stand-alone components will meet the requirements of IEEE 279 and IEEE 384. Grounding and shielding requirements will meet the guidelines of IEEE 1050 and EPRI TR-102323. The staff finds the electrical component design requirements to be consistent with the guidelines of SRP Chapter 7 and, therefore, acceptable.

4.7 Maintenance

Descriptions are provided in TR-107330 of the features that the PLC will have to support maintenance activities including surveillance testing requirements. A table is provided listing the IEEE 338 surveillance test, how the test is to be performed, and the need for any special equipment or features that the PLC should have to support those tests. The requirements include the capability to install and remove input/output modules while the system is in service. Guidance is provided for maintenance human factors such as the requirement for help screens to be provided with the software. The plant specific maintenance program will be evaluated during the application design review. The staff finds the maintenance requirements consistent with the guidelines of SRP Chapter 7 and, therefore, acceptable.

4.8 Requirements for Third Party/Sub-Vendor Items

The PLC qualifier is responsible for verifying that all the items provided by third party vendors

comply with the requirements of TR-107330 and the applicable NRC requirements.

4.9 Other Requirements

This section of TR-107330 includes communication and software isolation requirements. Data that is being sent out via the serial port will be broadcast only with no provision for hardware or software handshaking. The application program will ignore any incoming signals at the serial port. All communication between redundant PLCs (within a single channel) will be deterministic. The loss of communications will be detectable.

Security will be provided by both hardware and software. The hardware will be provided with a mechanism such as a keylock that prevents the PLC from being turned off without the key. The software will be designed to prevent modification while in service. There have been recent problems associated with on-line changes (Ref. NRC Information Notice 96-56: Problems Associated with Testing, Tuning, or Resetting of Digital Control Systems While At Power, October 22, 1996). The staff finds the above requirement to be consistent with the guidelines of SRP Chapter 7 and, therefore, acceptable.

4.10 Shipping and Handling Requirements

Shipping and handling will be in accordance with ANSI N45.2.2. The PLC manufacturer will provide any specific requirements for storage and shelf life limits. This is acceptable to the staff.

5.0 ACCEPTANCE/OPERABILITY TESTING

This section of TR-107330 includes requirements on testing performed prior to the qualification tests to confirm that the application is performing as expected and the PLC is operating properly. These pre-qualification testing requirements will include the application, initial PLC calibration, system integration, operability, prudency, and burn-in. These tests will establish the baseline for comparison subsequent qualification tests. Testing will also include verification of accuracy, time response and loss of power tests. Acceptance criteria is provided for each of the tests. Prudency testing is a set of tests which are not intended to satisfy any specific requirement, but will simulate in-service stresses. A burst of events test simultaneously toggling a large number of the inputs and outputs will be conducted to verify PLC response. Testing of the serial ports for loss of signal and noise are also included. Included in this section is a table that identifies which of the operability and prudency tests will need to be performed during environmental, seismic, and EMI qualification tests. A list is also provided referring to other sections of TR-107330 for the tests that need to be performed to qualify the various software objects. Additional test requirements are listed for cases of combining objects or special cases such as, an object that is not normally in the PLC library. The staff finds the testing requirements of this section to be consistent with the guidelines of SRP Chapter 7 and, therefore, acceptable.

6.0 QUALIFICATION TESTING AND ANALYSIS

This section of TR-107330 describes the process that will be followed to demonstrate that all requirements that can be shown by test and analysis have been satisfied. The process begins with the benchmark set of tests described in Section 4 of TR-107330. The PLC package to be

qualified will then have a representative application installed. This meets the IEEE 7-4.3.2 guidance (Section 5.3.2, commercial dedication) and the guidance of EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications: (NRC SER dated July, 17, 1997) and is, therefore, acceptable to the staff. The application will be monitored during each of the tests.

The hardware configuration will be developed and documented. At least one of each type of module that is used to meet Section 4 of TR-107330 will be included in the testing. The main chassis, power supplies and cables will also be included. Guidance is provided for the seismic and environmental tests so that a worst case condition is established. This is intended to ensure that any installation will be enveloped by the qualification test.

Guidance is provided for developing the test specimen application program. Program sequences should be selected to support the acceptability/operability testing specified in TR-107330 Section 5. Some of the suggested applications included lead/lag functions, timers and a range of input and out functions. If a coprocessor is used, it will also have its application tested. The test support equipment guidance is provided.

The testing will include environmental, ESD, seismic, EMI/RFI, and surge withstand. The environmental testing will be performed before any of the other tests. Guidance is provided for test mounting. For example, for the EMI/RFI test, there will be no secondary enclosure. The EMI/RFI tests will be performed in accordance with TR-107330 Section 4.

The environmental tests will be conducted without additional cooling fans and the power supplies will be set to maximize the heat load. The plant specific application will need to verify that the installed condition is enveloped by the generic qualification.

The seismic testing will be done in accordance with IEEE 344. Additionally, if relay output modules are to be included in the qualification package, they must be monitored during the seismic testing. The seismic testing will include a resonance search, five tri-axial operational basis earthquakes (OBEs), one tri-axial safe shutdown earthquake (SSE), and a complete operability test. Seismic qualification by analysis of electromagnetic output contacts is not acceptable.

The surge withstand testing will be performed in accordance with IEEE C62.45 and Section 4 of TR-107330. Class 1E to non-Class IE isolation, if needed, may be provided with the PLC or provided as separate components. ESD and power quality tests will be performed in accordance with Section 4 of TR-107330. All of the tests will be checked for conformance with the requirements of Sections 4 and 5 of TR-107330. Development of the test application program, procurement, and the tests described in Chapter 6 of TR-107330 will be in accordance with 10 CFR 50, Appendix B. The staff finds the qualification testing and analysis requirements to be consistent with the guidelines of SRP Chapter 7 and, therefore, acceptable.

7.0 QUALITY ASSURANCE

The requirements of TR-107330 apply to PLCs that were developed under a 10 CFR 50, Appendix B program or were procured as commercial products and dedicated for safety-related applications. If dedicated, the dedication process itself must be performed under a 10 CFR 50, Appendix B program. The Appendix B program will apply to any activities performed to provide

generic qualification of the product. It will also apply to application-specific design and development, including the system integration.

For commercial items that are dedicated, the qualifier will perform audits to verify that the vendor's QA program is equivalent to 10 CFR 50, Appendix B or compensating tests can provide that verification. TR-107330 also states that certification to ISO-9001 is not sufficient without additional qualifier audits or tests to demonstrate compliance with 10 CFR Appendix B requirements.

The utility and/or the qualifier will comply with the requirements of 10 CFR 21 for reporting of defects and nonconformances. In addition, the PLC manufacturer (if not already complying with 10 CFR 21) will have a program in place supporting problem reporting and tracking. The plant specific procurement process will need to verify this during the application design phase.

The PLC software verification and validation (V&V) activities will be evaluated to determine that they have been performed in accordance with the criteria of IEEE 7-4.3.2 and IEEE 1012. The EPRI V&V Handbook, EPRI TR-103291, "Handbook for Verification and Validation of Digital Systems, Volume I, Volume II, & Volume III," provides additional guidance in this regard. The software requirements documents will be reviewable for completeness, correctness and consistency. The manufacturer will provide traceability of requirements throughout the life cycle. There will be both functional and structural testing of the software. Reference is provided to IEEE 1008, 829, 1028, 1074 and 830 for guidance on reviewing the software development process. These are the standards endorsed by the staff in the regulatory guides and the acceptance criteria as described in SRP Chapter 7. The above is acceptable to the staff for the software quality demonstration.

If the software V&V process used by the PLC manufacturer does not meet the applicable requirements described above, then the qualifier is directed to the guidance provided by EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" to determine if appropriate compensatory actions have to be taken in the qualification process. The compensatory actions may be developed as either part of the generic qualification or as a plant specific requirement.

For the generic qualification to be valid for subsequent versions of the PLC, the manufacturer must maintain at least the same level of rigor in the development process as originally approved. This rigor applies to the hardware, firmware, software, tools, and the documentation. To maintain this generic qualification over a period of time, the qualifier must perform periodic audits and reviews. TR-107330 also provides guidance on commitments from the vendor concerning upward compatibility and support.

Legacy software (pre-existing software developed prior to the implementation of the current software standards and guides) used in the PLC may be evaluated using the guidance of EPRI TR-106439. A combination of experience and additional testing may permit legacy software to be acceptable in a new application. If accepted, that software will then be placed under configuration control by the manufacturer. Configuration control by the qualifier and the utility are described in section 4 of TR-107330.

The guidelines of NQA-1 will be used for hardware configuration management. Regulatory Guides RG 1.28, "Quality Assurance Program Requirements (Design and Construction), Revision 3 and RG 1.144, "Auditing of Quality Assurance Programs for Nuclear Power Plants, Revision 1 provide additional guidance on the implementation of NQA-1 and related ANSI/ASME N45 standards. Software configuration management will be in accordance with Reg Guide 1.169 (which endorses IEEE 828 and 1042). The plant specific configuration management plan will address the need for computer specific configuration management for the application.

The PLC qualifier will confirm that the PLC manufacturer maintains a problem reporting and tracking system that provides an effective means of collecting error reports from all customers and a timely mechanism for reporting that information to all nuclear customers. This is an important part of assuring that the intent of 10 CFR Part 21 for reporting of defects and nonconformances is maintained. The staff finds the quality assurance requirements of TR-107330 as modified by the EPRI 4/24/98 letter to be consistent with the guidelines of SRP Chapter 7, Instrumentation and Controls and SRP Chapter 17.2, Quality Assurance During the Operations Phase, and therefore, acceptable.

8.0 DOCUMENTATION

The documentation requirements of this section of TR-107330 provide a description of the equipment, handling and installation information. The PLC manufacturer will provide the general specification for the PLC including the information required to support the requirements of the previous sections. The PLC manufacturer will provide information on the operation of the PLC including status indications, switches or controls. The PLC manufacturer will also provide detailed information for the application programmers including a summary of the available functions, a detailed description of the usage of each function, and examples of the applications of complex function blocks. Limitations and methods for managing resource allocation will also be included. TR-107330 provides additional guidance on the information that should be provided for the programmer.

Calibration, troubleshooting, and maintenance information will be provided. Any special equipment or software needed will be described in the manufacturer's manuals. The qualifier will provide all documentation supporting the qualification testing described in the previous sections of TR-107330. This will include the plans, test specifications, procedures, test reports and design evaluations. A qualification summary document will be provided. This document will describe the qualification envelope which includes the qualification test results. A complete description of all configuration items will be provided. The FMEA and availability/reliability analyses will be included in the documentation.

The plans, specifications, and reports from the implementation of the V&V process will be documented. A description of the hardware and software used in the test specimen(s) will be provided. The qualification documentation will include a definition of the critical characteristics (if commercially dedicated) covered by the qualification tests.

All documents necessary to form a description of the PLC will be provided. These include a functional description, schematics, ladder diagrams, wiring layouts, and installation instructions. The software and hardware configuration used for qualification will be documented. This

includes all revision/version numbers of the hardware, software, and tools. Serial numbers of the specific hardware modules will also be provided. The database used in qualification will be documented. All values and ranges of parameters will be included.

The setup, calibration and checkout procedures used for qualification will be documented. The qualification test plan and report will be documented. The test requirements, acceptance criteria and sequence of testing will be included. The method of recording the test data and the requirements for test equipment will be included. A summary test report is also required. The PLC manufacturer will provide the QA plan and certifications of conformance to specifications and requirements. This includes replacement parts. The staff finds the above documentation requirements consistent with the guidelines of SRP Chapter 7 and, therefore, acceptable.

9.0 CONCLUSION

TR-107330, as modified by the 4/24/98 EPRI letter, presents a requirements specification for generically qualifying a commercially available PLC for safety-related applications. The goal of this requirements specification is to define the essential, critical technical characteristics that must be included as part of a PLC design to cover the needs of a range of safety applications. System and software development and quality processes are addressed in this specification primarily by references to published standards and guidelines.

The TR-107330 guidance provides for some flexibility in the specific methods for performing the verification activities necessary to qualify a PLC consistent with staff guidance. Licensees referencing TR-107330 for a proposed digital modification using PLCs should document the qualification process such that there are descriptions and justifications for the alternatives selected which will support the use of the selected product in a safety-related application. Because the term "PLC" is used by various manufacturers to label digital equipment with capabilities from relatively simple to very complex, care should be exercised to assure that TR-107330 is not used to attempt to qualify equipment outside its scope.

Based on its review of TR-107330, the staff concludes that it contains acceptable requirements specification guidelines that licensees can use in procuring a particular vendor's PLC for use in a safety system. By following the TR-107330 approach in conjunction with RG 1.28 when designing digital modifications, licensees will have a requirements specification that will enable the PLC design to meet the requirements of 10 CFR 50, Appendix A, GDC 1, and Appendix B for quality of safety-related equipment, and the guidance of the SRP, Chapter 7 as related to demonstration of qualification of digital systems.

While the staff finds TR-107330 acceptable, it should be noted that it only provides generic requirements for pre-qualifying commercial PLCs for use in safety-related applications. For plant-specific applications, the licensee is responsible for ensuring that the system design incorporating the PLC meets all applicable regulations (e.g., 10 CFR 50.59 and Appendices A and B to 10 CFR Part 50) and associated NRC guidance (SRPs and RGs). Specifically, plant-specific concerns such as diversity, EMI/RFI, separation criteria, operations and maintenance training, and associated QA commitments must be satisfactorily addressed by the licensee before the PLC system design can be found acceptable for safety-related applications. Additionally, the licensee is responsible for ensuring that the qualifier has satisfactorily implemented TR-107330 in accordance with Appendix B to 10 CFR Part 50 and 10 CFR Part

21 requirements.