U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-18

GUIDANCE ON THE USE OF PROGRAMMABLE LOGIC CONTROLLERS IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

Review Note: The revision numbers of Regulatory Guides (RG) and the years of endorsed industry standards referenced in this branch technical position (BTP) are centrally maintained in Standard Review Plan (SRP) Section 7.1-T (Table 7-1). Therefore, the individual revision numbers of RGs (except RG 1.97) and years of endorsed industry standards are not shown in this BTP. References to industry standards incorporated by reference into regulation (IEEE Std 279-1971 and IEEE Std 603-1991) and industry standards that are not endorsed by the agency do include the associated year in this BTP. See Table 7-1 to ensure that the appropriate RGs and endorsed industry standards are used for the review.

Draft Revision 6 – August 2015

A. BACKGROUND

This branch technical position (BTP) provides guidelines for reviewing the use of programmable logic controllers (PLCs) in instrumentation and control (I&C) systems. These guidelines are based on reviews of licensee submittals and the analysis of PLC-related issues documented in NUREG/CR-6090, "The PLC and Its Application in Nuclear Reactor Protection Systems."

1. Regulatory Basis

Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," Appendix A, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," General Design Criterion (GDC) 1, "Quality Standards and Records," requires in part that "structures, systems, and components important to safety shall be designed, fabricated, and tested to quality standards commensurate with the importance of the safety functions to be performed."

10 CFR Part 50, Appendix A, GDC 21, "Protection System Reliability and Testability," requires in part that "the protection system shall be designed for high functional reliability … commensurate with the safety functions to be performed."

2. Relevant Guidance

RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," provides guidance for complying with the requirements for safety systems that use digital computer systems. The guidance in RG 1.152 refers to the Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." SRP, Appendix 7.1-D provides additional guidance.

NUREG/CR-6090 covers the application of PLCs to nuclear reactors. The guidance in this NUREG will aid the reviewer in the evaluation of an I&C system containing one or more PLCs. NUREG/CR-6463, Revision 1, "Review Guidelines on Software Languages for use in Nuclear Power Plant Safety Systems," describes recommended practices in the use of common PLC programming languages.

Electric Power Research Institute (EPRI) Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," as accepted by the U.S. Nuclear Regulatory Commissions (NRC) safety evaluation (SER) report dated July 17, 1997, provides more detail on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors. The guidance of SRP BTP 7-14 may be applied to the evaluation of vendor processes described in EPRI TR-106439. Appendix 7.1-D, Subsection 5.4.2 which references IEEE Std 7-4.3.2, Sub-clause 5.4.2 contains the guidance of EPRI TR-106439. EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," as accepted by the NRC SER dated July 30, 1998. EPRI TR-106439 describes the generic functional and qualification requirements for a PLC. Generic qualification is the first of a two-step process; further qualification for a plant-specific application is required.

NUREG/CR-6421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications," discusses graded acceptance processes for commercial off-

the-shelf software used in reactor applications. The guidance in this NUREG will aid the reviewer in the evaluation of acceptance processes that are part of commercial dedication of PLC embedded, operating system software, and programming tools.

3. Purpose

The purpose of this BTP is to provide guidance for NRC staff to verify conformance with the previously cited regulatory bases and standards in the design of digital computer systems using PLCs. This BTP has two objectives:

- To assure that embedded and operating systems software, programming tools, and peripheral components are reviewed, and the appropriate acceptance criteria are applied.

- To assure that the PLC application software (e.g., ladder-logic software) are developed using an appropriate software development process.

B. BRANCH TECHNICAL POSITION

1. Introduction

PLCs are often used to monitor and control industrial processes. They are typically commercial-grade computer systems that include simplified operating systems and standard service functions such as self-testing and communications. Most PLCs are configured for their specific application using a high-level language, such as ladder logic. The software for PLCs should be designed and implemented using a process that conforms to the guidance in SRP BTP 7-14. Software design and implementation for specific applications may be easier to implement for PLCs due to the use of high level languages and the fact that many service functions are already included as part of the commercial product.

PLC application software can be expected to use standard functions provided by the PLC vendor. Standard functions may have considerable industrial experience. This experience may supplement other methods of evaluating the quality of the PLC software, provided the experience is commensurate with the reactor application and field trouble reports are generated, available, and reviewed. If existing industrial experience cannot be shown to be applicable to the safety system application, it is of limited use.

SRP Appendix 7.0-A, Subsection C.3, describes the advantages of using high-level languages such as ladder logic and function charts. It also describes precautions that should be observed when reviewing systems specified or designed using such languages.

Many vendors of PLCs allow programming languages other than ladder-logic to be used (e.g., C). The reviewer should take this possibility into account and assess the impact of using programming languages on the design of the PLC and the application.

An I&C system built using PLCs contains a number of purchased components: hardware, including the processor, memory, I/O equipment, communications equipment, terminals, etc., and software, consisting of one or more operating systems, interpreters, compilers, libraries, configuration software, tools, and variations thereof. This purchased equipment should be of a quality appropriate to the proposed application.

Other issues associated with the application of digital computers to I&C systems, such as maintenance, verification and validation, electromagnetic interference, and calibration, apply and should be reviewed. The staff should not accept an argument that the PLC is somehow simpler or different from a computer and hence does not require the rigorous review that a computer system would receive.

2. Information to be Reviewed

Information to be reviewed is contained in the safety analysis report (SAR), revisions to the SAR, license amendment requests, topical reports, or other applicant or licensee documentation. Inspections, tests, analyses, and acceptance criteria (ITAAC) or detailed design documents describe designs, tests, analyses, or other methods of demonstrating that design commitments have been satisfied. Information that is not contained in the licensee's or applicant's submittal should be available for review.

3. Acceptance Criteria

Purchased PLC hardware; embedded and operating systems software, programming tools, and peripheral components should be qualified to a level commensurate with the system they are designed to support. EPRI TR-106439 and EPRI TR-107330 describe an acceptable process for qualifying commercial systems. NUREG/CR-6421 provides additional information on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors for purchased PLC software. See the discussion of the commercial dedication of pre-developed software (PDS) in SRP Appendix 7.0-A.

PLC hardware, embedded and operating system software, and peripheral components built specifically for nuclear power plant applications should meet the appropriate quality criteria. The embedded and operating system software should meet the acceptance criteria contained in SRP BTP 7-14, appropriately graded for the application in which the PLC will be used.

The application software (ladder logic or other) should meet the acceptance criteria contained in SRP BTP 7-14 commensurate with the system it is designed to support. Application software should conform to the recommended practices of NUREG/CR-6463.

Tools for developing application software or loading it into the PLC should be qualified to a level commensurate with the system they are designed to support.

PLC-based functions should conform to the guidance regarding real-time performance and testing outlined in SRP BTP 7-21 and SRP BTP 7-17.

Administrative or hardware lockout controls that prevent unauthorized modification of the PLC software should be in place. This is particularly important because many PLCs are designed so that their software is easy to modify. All software changes should be under configuration management control. In particular, administrative procedures for maintaining control of the software implemented in the PLC should be detailed in the configuration management plan.

4. Review Procedures

PLC applications should be reviewed in the same manner as other digital computer I&C applications. SRP Appendix 7.0-A, SRP Section 7.1, SRP BTP 7-14, SRP BTP 7-17, and SRP BTP 7-21 describe these review procedures.

C. REFERENCES

1. EPRI Topical Report TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” EPRI, October 1996.

2. EPRI TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” EPRI, December 1996.

3. IEEE Std 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

4. NUREG/CR-6090, “The PLC and Its Application in Nuclear Reactor Protection Systems,” September 1993.

5. NUREG/CR-6421, “A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications,” June 1996.

6. NUREG/CR-6463, Revision 1, “Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems,” October 1997.

7. RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.”

8. Safety Evaluation by the Office of Nuclear Reactor Regulation, “EPRI Topical Report TR-106439, Guidance on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” July 17, 1997.

9. 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,” July 30, 1998.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the Standard Review Plan are covered by the requirements of 10 CFR Part 50, and were approved by the Office of Management and Budget, approval number 3150-0011.

PUBLIC PROTECTION NOTIFICATION

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

BTP Section 7-18
Description of Changes

BTP 7-18, "Guidance on the Use of Programmable Logic Controllers In Digital Computer-Based Instrumentation and Control Systems"

This BTP Section affirms the technical accuracy and adequacy of the guidance previously provided in BTP 7-18, Revision 5, dated March 2007. See ADAMS Accession Number ML070550073.

The main purpose of this update is to incorporate the revised software Regulatory Guides and the associated endorsed standards. For organizational purposes, the revision number of each Regulatory Guide and year of each endorsed standard is now listed in one place, Table 7-1. As a result, revisions of Regulatory Guides and years of endorsed standards were removed from this section, if applicable. For standards that are incorporated by reference into regulation (IEEE Std 279-1971 and IEEE Std 603-1991) and standards that have not been endorsed by the agency, the associated revision number or year is still listed in the discussion.

References to vendor-specific SERs have been removed from this BTP. Additional changes were editorial.