NEW

Branch Technical Position HICB-18

Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

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

10 CFR 50 Appendix A, General Design Criterion 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 50 Appendix A, General Design Criterion 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

Reg. Guide 1.152, "Criteria for Digital 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 Reg. Guide 1.152 refers to IEEE Std 7-4.3.2, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

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, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," describes recommended practices in the use of common PLC programming languages.

EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," provides more detail on the characteristics of an acceptable process for qualifying existing software, and discusses the use of engineering judgment and compensating factors.

NUREG/CR-6421 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 dedications of PLC embedded, operating system, and programming tools software.

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 ensure that embedded and operating system software and programming tools are reviewed, and the appropriate acceptance criteria are applied.

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

B. Branch Technical Position

1. Introduction

The PLC is typically a commercial-grade computer system that employs a particular high-level language, such as ladder logic, for the purpose of monitoring and controlling industrial processes. The PLC is a computer system, and as such, the software used on it should be designed and implemented using a process that conforms with the guidance in BTP HICB-14. The detailed design and implementation activities of such a process, however, may be easier to implement for applications produced using the high-level languages typical of PLCs.

PLC applications are usually coded using ladder logic or sequential function charts. The resulting programs 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 program, provided that the experience is commensurate with the reactor application, and that 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.

Appendix 7.0-A, Section 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 on the application.

An I&C system built using PLCs contains a number of purchased components: the hardware, including the processor, memory, I/O equipment, communications equipment, terminals, etc.; and the 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 (e.g., maintenance, verification and validation, EMI, 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/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/applicant's submittal should be available for review.

3. Acceptance Criteria

Purchased PLC hardware, embedded, programming, and operating system software, and peripheral components should be qualified to a level commensurate with the system they are designed to support. EPRI TR-106439 describes an acceptable process for qualifying commercial systems. NUREG/CR-6421 provides more detail 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 predeveloped software (PDS) in 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 BTP HICB-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 BTP HICB-14 commensurate with the system it is designed to support. Application software should conform with 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 with the guidance regarding real-time performance and testing outlined in BTP HICB-21 and BTP HICB-17.

Administrative or hardware lockout controls that prevent casual modification of the PLC program should be in place. This is particularly important because many PLCs are designed so that their programming is easy to modify. All program changes must 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 instrument and control system applications. SRP Appendix 7.0-A, Section 7.1 and BTPs HICB-14 and HICB-17 describe these review procedures.

C. References

EPRI Topical Report TR-106439. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." Electric Power Research Institute, October 1996.

IEEE Std 7-4.3.2-1993. "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

NUREG/CR-6090. "The PLC and Its Application in Nuclear Reactor Protection Systems." September 1993.

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

NUREG/CR-6463. "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems." June 1996.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, January 1996.

Safety Evaluation by the Office of Nuclear Reactor Regulation. "EPRI Topical Report TR-106439." May 1997.