



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

July 17, 1997

Mr. Raymond C. Torok  
Project Manager, Nuclear Power Group  
Electric Power Research Institute  
3412 Hillview Avenue  
Post Office Box 10412  
Palo Alto, CA 94303

SUBJECT: REVIEW OF EPRI TOPICAL REPORT TR-106439, "GUIDELINE ON  
EVALUATION AND ACCEPTANCE OF COMMERCIAL GRADE DIGITAL  
EQUIPMENT FOR NUCLEAR SAFETY APPLICATIONS" (TAC NO.  
M94127)

Dear Mr. Torok:

By letter dated December 4, 1996, the Electric Power Research Institute (EPRI) submitted topical report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," for staff review. The staff has completed its review of EPRI's topical report and prepared the enclosed safety evaluation report.

The staff has determined that TR-106439 contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications and meets the requirements of 10 CFR Part 21. Further, the staff concludes that when digital equipment is dedicated using the methods described in TR-106439, it may be considered equivalent to digital equipment designed and manufactured under a 10 CFR Part 50, Appendix B quality assurance program. Licensees may utilize the TR-106439 approach when installing digital modifications utilizing commercial grade equipment. This includes microprocessors that are embedded in electrical and mechanical equipment as well as process instrumentation and control systems. While the staff finds TR-106439 acceptable, it is a generic proposal and therefore, licensees referencing TR-106439 will need to document the details regarding the dedication process and specific critical characteristics including the verification information described in Standard Review Plan Chapter 7 such as qualification reports, system description and software and hardware design and quality assurance documentation. The staff will include a reference to TR-106439 in Chapter 7 of the Standard Review Plan.

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

Sincerely,

A handwritten signature in black ink, appearing to read "D B Matthews". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

David B. Matthews, Chief  
Generic Issues and Environmental  
Projects Branch  
Division of Reactor Program Management

Project No. 669

Enclosure: As stated

cc w/ Enclosure: See next page

SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION  
ELECTRIC POWER RESEARCH INSTITUTE TOPICAL REPORT, TR-106439,  
"GUIDELINE ON EVALUATION AND ACCEPTANCE OF COMMERCIAL GRADE  
DIGITAL EQUIPMENT FOR NUCLEAR SAFETY APPLICATIONS"

1.0 SUMMARY

By letter dated December 4, 1996, the Electric Power Research Institute (EPRI) submitted topical report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," dated October 1996, for staff review. This non-proprietary topical report was developed by an EPRI utility working group to recommend guidance for the dedication of commercial grade digital equipment for use in nuclear power plant safety systems (commonly referred to as commercial grade dedication). The guidance provided in TR-106439 addresses: (1) application of the preexisting non-digital commercial grade dedication guidance to digital systems, (2) identification of applicable codes and standards, (3) a process to perform the evaluation of commercial grade digital equipment, and (4) acceptance criteria for using commercial grade equipment in a safety system. Examples are also provided to illustrate the application of the TR-106439 commercial grade dedication process.

The commercial grade dedication process described in TR-106439 indicates that equipment which has a high degree of importance to safety or is significantly complex will require more effort to verify that the critical characteristics necessary for the equipment to perform required safety functions are present than for equipment which has a low potential impact on safety or is composed of relatively simple devices. The safety significance will require the use of existing plant safety determinations. The TR does not change existing priorities for safety classification. In all cases, as a minimum, the equipment used in safety-related applications will comply with NRC quality assurance requirements in 10 CFR Part 50, Appendix B.

The staff has determined that TR-106439 contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications. Licensees may utilize the TR-106439 approach when installing digital modifications utilizing commercial grade equipment. This includes microprocessors that are embedded in electrical and mechanical equipment as well as process instrumentation and control systems. Because TR-106439 is a generic proposal, licensees referencing TR-106439 will need to document the details regarding the dedication process and specific critical characteristics including the verification information described in Standard Review Plan (SRP) Chapter 7 such as qualification reports, system description and software and hardware design and quality assurance documentation. This is discussed in more detail subsequently in this safety evaluation.

## 2.0 BACKGROUND

### Commercial Dedication per 10 CFR Part 21

Due to obsolescence, increasing maintenance costs, and improvement in performance, nuclear power plant licensees are replacing and upgrading the existing analog-based instrumentation and control systems with digital systems. For many of these safety and non-safety related systems, the licensees have selected microprocessor-based digital equipment for the replacements. In addition to meeting the system level requirements, the components (individually or as part of a system or subsystem) must be qualified for the proposed application.

Licensees have two options for qualifying equipment for use in safety systems. The first is to procure the equipment from a vendor that produced it in accordance with a quality assurance (QA) program that meets the requirements of Appendix B to 10 CFR Part 50. The second method is to dedicate commercial grade equipment for use in the safety system as addressed in 10 CFR Part 21. 10 CFR Part 21 requires, in part, that the dedicated commercial equipment be deemed equivalent to equipment produced under a 10 CFR Part 50 Appendix B program. This latter approach is addressed for commercial digital equipment in this safety evaluation.

Dedicating commercial off-the-shelf (COTS) equipment has been specifically described since the October 1978 revision to 10 CFR Part 21 which clarified how to identify and dedicate these commercial grade items. Definitions were provided in 10 CFR Part 21 for "basic component" and "commercial grade item (CGI)." 10 CFR Part 21 states, in part, that a basic component is any structure, system, component or part thereof that affects a safety function. Basic components are items that have been designed and manufactured under a quality assurance program complying with 10 CFR Part 50 Appendix B or items that have been dedicated for use in safety systems. CGIs are those items that were not developed under an Appendix B program and must go through the commercial dedication process to become designated for use as a basic component in a safety-related application. Another key definition for commercial dedication consideration is "critical characteristics." Critical characteristics are those important design, material, and performance characteristics of a CGI item that, once verified, will provide reasonable assurance that the item will perform its intended safety function. The CGI dedication process is a safety-related activity that must be performed in accordance with an Appendix B QA program.

A recent (October 19, 1995) revision to 10 CFR Part 21 was promulgated to facilitate dedication efforts by clarifying definitions and by providing added flexibility in using CGI. Analog and digital hardware, software, firmware, services, analyses, and systems assembled from any combination of the above are all candidates for dedication. Layering of commercially dedicated components and Appendix B components is allowed. An example of layering would be the use of a commercially dedicated programmable logic controller with the ladder logic prepared under an Appendix B program.

The second sentence of the new Part 21 definition of CGI excludes "... items where the design and manufacturing process require[s] many in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more critical

characteristics of the item cannot be verified)." The staff considers verification and validation activities common to software development in digital systems to be a critical characteristic that can be verified as being performed correctly following the completion of the software development by conducting certain dedication activities such as audits, examinations, and tests.

#### REVIEW CRITERIA APPLICABLE TO COTS

The following are criteria applicable to COTS equipment for use in safety-related systems. There is also a large body of information (not cited below) available from other industries that have similar COTS qualification issues for computers such as the Department of Defense.

Regulatory Guide 1.33, Revision 2 (February 1978), "Quality Assurance Program Requirements (Operation)," endorsed with some exceptions ANSI N18.7-1976, "Administrative Controls and Quality Assurance for the Operational Phase of Nuclear Power Plants," which was the first nuclear industry standard that specifically addressed COTS items. The standard states that care should be taken to assure the COTS item displays equivalent performance to a 10 CFR Part 50 Appendix B item although it does not describe a method to provide this assurance.

To provide additional detail on the commercial dedication process, the nuclear industry developed topical report EPRI NP-5652 (June 1988), "Guidelines for the Utilization of Commercial Grade Items in Nuclear Safety Applications," which describes four methods to perform the commercial dedication process. The four methods are: (1) special tests and inspections, (2) commercial grade survey of the supplier, (3) source verification, and (4) acceptable supplier/item performance record. These methods are applicable to many of the safety-related components in a nuclear power plant but do not provide specific guidance for dedication of digital equipment.

Generic Letter (GL) 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," (March, 1989) conditionally endorses EPRI NP-5652. GL 89-02 listed three characteristics of effective procurement and dedication programs identified during NRC staff inspections. These characteristics are: (1) the involvement of engineering staff in the procurement and product acceptance process, (2) effective source inspection, receipt inspection, and testing programs, and (3) thorough, engineering based, programs for review, testing, and dedication of commercial-grade products for suitability for use in safety-related applications.

Topical report EPRI NP-6406 (1989), "Guidelines for the Technical Evaluation of Replacement Items for Nuclear Power Plants," provides more detailed guidance for technical evaluation of replacement items. Guidance is provided to help determine when a replacement item is sufficiently different from the original to warrant a design change evaluation. This document has not been formally reviewed by the NRC staff.

EPRI topical report TR-102260, "Supplemental Guidance for the Application of EPRI Report NP-5652," provides additional guidance and clarification to NP-5652 regarding the commercial dedication process. This document has not been formally reviewed by the NRC staff.

Generic Letter 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs," (April 1991) was issued to notify the industry of the staff's pause in conducting certain procurement inspection and enforcement activities and to identify a number of failures in licensees' commercial-grade dedication programs. The purpose of the pause in inspections was to allow licensees sufficient time to fully understand and implement the guidance that was developed by the industry in NP-5652. Staff positions were provided in GL 91-05 regarding certain aspects of licensee commercial-grade procurement and dedication programs which would provide acceptable methods to meet regulatory requirements.

NUREG/CR-6421 (March 1996), "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications," which was prepared by Lawrence Livermore National Laboratory is similar to EPRI TR-106439 in that it proposes an approach to the efforts required for commercial dedication based upon the importance to safety of the CGIs. This NUREG provides a mapping of the acceptance criteria in applicable IEEE, ANSI/ANS and IEC standards used to evaluate the critical characteristics of digital systems. The NUREG also provides guidance on testing existing software for safety-related applications which may be used to supplement the CGI vendor's original testing as needed. NUREG/CR-6421 is referenced in SRP Chapter 7 as a source of additional guidance for performing commercial dedication of digital systems.

SRP Chapter 7, Instrumentation and Controls, (NUREG-0800), provides the general staff review criteria for instrumentation and control systems. It includes reference to IEEE 7-4.3.2 which contains general COTS guidance and also includes additional COTS-specific guidance. SRP Chapter 7 also contains guidance on the various technical topics for the qualification of digital equipment in safety-related applications.

IEEE 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (September 1993) was endorsed by Regulatory Guide 1.152, Revision 1 (January 1996), "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." This standard includes guidance for the qualification of existing commercial computers. The qualification process is accomplished by comparing the existing commercial product to the design criteria described in the standard. The use of compensating factors such as additional testing to compensate for shortcomings in a vendor's digital system design development process or lack of documentation for the design process is permitted.

#### EPRI ON COTS

An EPRI utility working group was formed in 1994 in order to develop an approach for evaluation and acceptance of commercial software-based equipment in nuclear safety systems. It was recognized by the nuclear industry that use of commercially available digital equipment would be necessary in order to upgrade existing instrumentation and control systems in a cost effective manner. The working group's specific objectives were: (1) to produce guidelines for COTS digital equipment that are practical, cost-effective and technically defensible, (2) to promote industry use of the guidelines, and (3) to gain regulatory support for the approach to COTS digital equipment dedication. This working group developed EPRI TR-106439.

The working group held its first meeting on January 25-26, 1995, with subsequent meetings on March 20-21, 1995, and June 21-22, 1995. The working group kept the NRC staff continuously apprised of the direction of their considerations. Following the June 1995 meeting the working group invited the NRC staff to participate at its subsequent working group meetings. The staff attended meetings on September 20-21, 1995, January 24-25, 1996, May 8-9, 1996, and August 8-9, 1996, and provided verbal comments on the draft working group documents and presentations. In May 1996, the staff provided written comments on a draft version of TR-106439. On October 4, 1996, the working group submitted an "information only" version of TR-106439 to facilitate further discussion with the staff. The membership of the working group included a variety of disciplines from licensees' staffs including electrical, instrumentation and control, computer, procurement and quality assurance engineers. The working group also invited digital equipment vendors to participate at some of the meetings. The working group has indicated an interest in continuing development of more specific COTS digital equipment implementing guidance.

TR-106439 describes an approach for evaluation and acceptance of COTS software-based digital products for use in safety systems. The scope is intended to be limited to that aspect. There are some related aspects, such as using the information contained in TR-106439 as input to a 10 CFR 50.59 evaluation, that are mentioned; however, the entire scope of activities and determinations necessary to the 10 CFR 50.59 modification implementation process are not addressed. TR-106439 does not specifically address the plant modification process or system-level design activities that must be considered for a design change, nor does it provide a level of detail necessary to ensure completion of the plant design basis verification activities. In addition, TR-106439 does not provide a comprehensive listing of potential instrumentation and control system modifications and the specific design considerations for different applications. The above issues need to be addressed as part of the licensees proposed design change and may be addressed in other documents.

### 3.0 APPLICABLE REGULATORY REQUIREMENTS FOR DIGITAL MODIFICATIONS

Following is a description of the regulatory requirements applicable to any safety-related digital instrumentation and control system modification used by the staff in evaluating TR-106439:

- 1) 10 CFR 50.55a(h) references IEEE 279 - 1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE 279-1971 states in section 4.3 that:

"Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration and test."

IEEE 279-1971 states in section 4.4 that:

"Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system

equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements."

- 2) 10 CFR Part 50 Appendix A, General Design Criterion 1, states in part that systems and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed and that recognized codes and standards shall be used when available.
- 3) The 18 criteria of Appendix B to 10 CFR Part 50 describe the basic quality assurance requirements to which a commercial dedication activity must be shown to be equivalent as stated in 10 CFR Part 21.

#### 4.0 EVALUATION

The following evaluation of TR-106439 is presented in the same order as the topics are presented in the document.

##### Section 1, Introduction

The introduction to TR-106439 discusses the background and reasons for the creation of the EPRI working group on COTS. There has been an increased use of digital technology to replace the analog equipment that was originally installed in the existing operating plant instrumentation and control systems. The reasons for the use of digital replacement equipment include the cost benefits, availability, and flexibility of the newer digital designs compared to the previous analog systems.

TR-106439 builds upon the previous commercial dedication work performed by the industry in the past which focused upon mechanical and electrical equipment by relating this earlier effort to qualification of commercial digital equipment. References are provided to EPRI topical report TR-102438, "Guideline on Licensing Digital Upgrades," for digital issues not specifically related to commercial dedication but which are important for consideration in any safety-related digital modification. The difficulties of evaluating pre-existing software which often has less documentation of the development process than is usually expected for a product produced under a 10 CFR Part 50 Appendix B program are discussed.

TR-106439 is intended to be used for COTS digital equipment by any dedicating organization. This may include the utility licensee, a third party, or the original vendor. TR-106439 includes guidelines for maintenance of the COTS dedication basis as well as the original dedication effort itself. TR-106439 is not intended to be used as a detailed "how-to" manual. The lists and examples presented were constructed to illustrate specific points regarding application of the guidance. They are not necessarily all-inclusive. Differences in the proposed COTS equipment or the application may require different critical characteristics, acceptance criteria, and verification methods from those shown in the examples. The staff concludes that TR-106439 provides an acceptable level of detail and agrees with statements in the document that additional detailed specific information for an actual commercial dedication project would be needed. In accordance with the requirements of Criterion V, "Instructions, Procedures, and



Drawings," of Appendix B to 10 CFR Part 50, each user of TR-106439 (when used for safety systems) is required to develop and implement procedures that prescribe the "detail" necessary to implement the program. The staff notes that the guidance in TR-106439 will not eliminate the need for a certain amount of engineering judgment in the commercial dedication process by the dedicating organization. However, the basis for the engineering judgment used by the dedication organization during the dedication process shall be documented.

## Section 2, Definitions and Terminology

The TR-106439 definitions and terminology section provides a listing of terms used in the document. These terms are primarily derived from 10 CFR Parts 50 and 21 and from relevant IEEE and IEC standards. The remaining terms are in common use in the industry. The staff finds the definitions and terminology acceptable.

## Section 3, Overview

This section of TR-106439 provides an overview of the approach taken for addressing digital issues within the previously existing commercial grade item dedication process. Figure 3-2 provides a comparison of a dedicated commercial grade item with an item specifically designed to meet 10 CFR Part 50 Appendix B requirements. The figure shows that the commercial grade item must be shown to be equivalent to an item designed under a 10 CFR Part 50 Appendix B program, however, the specific steps taken to verify that there is reasonable assurance that the item will adequately perform its safety function may vary between the two methods. The staff notes that there may also be significant variation in the specific steps taken within either method depending upon vendors, components, and applications.

Typically, the commercial grade vendor may be lacking some of the documentation that would be expected of a 10 CFR Part 50 Appendix B program. To compensate for the lack of documentation for commercial grade items and reach an equivalent level of assurance, the licensees (or dedicating entity) may need to perform additional product inspection (including source inspections and CGI surveys), testing, analyses, verifications, and/or documentation development, or request the commercial product vendor to augment their existing program to address these areas.

Successful operating experience in applications that are relevant to nuclear power plant safety systems may be used as part of the means for determining the acceptability of a commercial item. As shown in Figure 3-2, applicable operating experience can be a determining factor for COTS product qualification but is only a part of the dedication process and should not be considered the only determining factor.

The supplemental effort that a dedicator must use depends upon several variables including; the safety significance (contribution to risk) associated with the specific application (this sets the overall level of assurance needed), how rigorous are the vendor's development and quality assurance practices, the maturity of the commercial device, and the complexity of the device - the more complex the device, the greater the effort needed to develop adequate confidence it will meet the requirements of the application, particularly with regard to potential failure modes. The safety significance and relative complexity create a "graded approach" to the commercial

dedication process. Examples are provided in TR-106439 to illustrate the process of assessing the safety significance.

The overview section of TR-106439 also references other documents for guidance on digital system licensing and technical issues. These include: (1) Regulatory Guide 1.152 which endorses IEEE-7.4.3.2-1993, (2) Generic Letter 95-02, "Use of NUMARC/EPRI Report TR-102348, "Guideline on Licensing Digital Upgrades," in Determining the Acceptability of Performing Analog-to-Digital Replacements under 10 CFR 50.59," and (3) EPRI NP-5652, EPRI NP-6406, EPRI TR-102260, Generic Letter 89-02 and Generic Letter 91-05 which provide guidance on commercial grade item dedication. The TR-106439 overview section provides a brief description of the four methods for commercial dedication that are described in more detail in the referenced documents. These four methods are: (1) special tests and inspections, (2) commercial grade survey of supplier, (3) source verification, and (4) acceptable supplier/item performance record. It is noted that Generic Letter 89-02 places restrictions on the use of methods 2 and 4 above as follows:

- 1) Acceptance method 2, "Commercial-Grade Survey of Supplier," should not be employed as the basis for accepting items from suppliers with undocumented commercial quality control programs or with programs that do not effectively implement their own necessary controls. Likewise, method 2 should not be employed as the basis for accepting items from distributors unless the survey includes the part manufacturer(s) and the survey confirms adequate controls by both the distributor and the part manufacturer(s).
- 2) Acceptance method 4, "Acceptable Supplier/Item Performance Record," should not be employed alone unless:
  - a. The established historical record is based on industry-wide performance data that is directly applicable to the item's critical characteristics and the intended safety-related application; and
  - b. The manufacturer's measures for the control of the design process, and material changes have been adequately implemented as verified by audit (multi-licensee team audits are acceptable.)

For typical digital applications using commercially dedicated equipment, no one of the above methods will suffice by itself. The TR-106439 guideline proposes that for digital applications, a combination of methods 1,2 and 4 will be needed. The staff concludes that the TR-106439 guidance is consistent with previously established staff criteria for commercial dedication, and is, therefore, acceptable.

#### Section 4, Evaluation and Acceptance

This section of TR-106439 provides guidance for identifying and verifying critical characteristics for commercial grade digital equipment. A summary of the commercial dedication process is presented showing the interaction of the procurement activities and the design and licensing activities for all stages from the proposal for a design change through operation and

maintenance. Two items are emphasized as important due to the use of digital technology while most of the process steps are the same for the commercial dedication of any component or system regardless of technology. The first item emphasized is the need for a failure analysis. This will assist in determining the correct critical characteristics of the commercial grade digital item and its impact on the instrumentation and control system failure modes. The second item emphasized is the need to include digital expertise in the evaluation of the digital equipment.

TR-106439 identifies three categories for grouping the commercial grade item critical characteristics as shown in Figure 4.1. The first category is "physical." These include characteristics such as physical size, power requirements, part number, hardware and software version, and data communications. The second category is "performance" which includes response time, and human machine interface (HMI) functionality. It also includes the environmental items such as temperature, humidity, seismic and electromagnetic qualification. These two categories are similar to the typical critical characteristics for any electrical and mechanical equipment dedication effort. The third category referred to is "dependability." This category receives additional emphasis when compared with typical electrical and mechanical equipment because of the potential for design errors unique to software development. This category includes the design process characteristics needed to verify the built-in quality. Typical examples include verification and validation activities and configuration control. For each of the above three critical characteristics, TR-106439 provides acceptance criteria, and guidance on methods of verification and application of the verification methods.

Examples are provided in Table 4-2 of TR-106439 to show activities used in assessment of item quality and design factors that can be evaluated in assessing item quality. For example, in the review of the vendor configuration control program and practices, TR-106439 recommends a review of the vendor and product historical record for control of changes and versions, and notification of changes, especially required repairs. The examples described are not all-inclusive. Depending upon application and product specifics, some of the recommended evaluations may not be needed. Conversely, there may be additional verification activities needed that are not mentioned in the example.

TR-106439 provides guidance on several additional commercial dedication topics such as the timing of the audit activities, the specific document reviews and expertise required, who and where to survey as part of the audit activities, and specific qualification requirements on the dedicator. For example, TR-106439 notes that the dedication process must be performed in accordance with an approved 10 CFR Part 50 Appendix B program. One point that is emphasized is the need to document engineering judgment. This judgment should be documented sufficiently such that a comparably qualified individual would reach the same conclusion. The staff concludes that the guidance provided in this section of TR-106439 is consistent with the above acceptance criteria and guidance for qualification of safety-related digital systems and is, therefore, acceptable.

## Section 5, Maintenance

This section of TR-106439 indicates that the licensee is responsible for maintaining the validity of a commercial grade item dedication for as long as the dedicated device remains in service.

The licensee may choose to use the services of the vendor, sub-vendors, separate dedication organization or other contract support to assist them in the dedication maintenance effort. The primary emphasis of this section is on maintaining the commercial dedication for upgrades or error corrections in the digital system software throughout the lifetime of the product. The dedication effort for design changes in commercial products must be comparable to that for the original equipment dedication in order to ensure proper safety functions are maintained. The 10 CFR Part 21 reporting requirements, and quality assurance document retention requirements continue to apply to the modified commercially dedicated equipment.

Depending on the agreement between the vendor, dedicator and licensee, the licensee may be notified that a new revision is available at the time new equipment is ordered, or when equipment is sent to the vendor for servicing. The licensee should obtain a written description of the proposed changes to the dedicated equipment, if any. The licensee should ensure that the software is not updated to a new revision level without prior evaluation as approved for the initial design. Any proposed changes should be evaluated by the licensee to determine if a design change is required and if corresponding rededication is, therefore, necessary.

TR-106439 notes that care should be taken to ensure that a modified commercially dedicated device is not operated in a configuration that is outside the bounds of the original dedication. The original dedication package should clearly define the critical characteristics and acceptance criteria applied in verifying them, and it should document the conditions and assumptions under which the characteristics were verified in order to permit an effective rededication effort for the proposed modification.

Typically, the commercial grade digital item is designed for use in a variety of applications; the vendor is not involved in the specifics of the application and is not in a position to judge the safety significance of an identified defect in the product. TR-106439 recommends that the licensee arrange to be notified by the vendor when defects are discovered. The licensee should confirm that the vendor's processes will adequately support the user licensee's need for notification of defects reported to the vendor including those found from non-nuclear users of the same commercial product.

If a third party organization is used as the dedicating organization the licensee should take appropriate care to assure the success of maintenance of the dedication process by this organization if their dedication role is to continue. This section of TR-106439 describes the need for long term viability of error reporting to a third party and offers several options. This involves assessing the qualifications, experience, and long term viability of the third party dedicator. Where the maintenance of the software is to be performed by the licensee user or a third party, the licensee or third party should procure the tools and associated design and development information necessary in order to properly implement required software changes. The staff concludes that this section provides sufficient guidance to ensure that modification to commercially dedicated digital equipment receives a level of quality verification comparable to the originally installed equipment.

## Section 6, Examples

This section provides examples to illustrate how the guidance in the previous sections can be applied for commercial digital items of varying complexity and safety significance. Four examples are provided starting with a relatively simple digital meter up through a Engineered Safety Features Actuation System (ESFAS) upgrade that is both relatively complex and of high safety significance. This section notes that even though the examples provided lead to successful commercial dedication there may be cases where the use of the document should lead to rejection of an item for dedication in a safety-related application.

The first example is the replacement of a Reg Guide 1.97 Category 1 analog indicator with a microprocessor-based device. There are two redundant devices whose only function is to provide operator information. In addition, the indicated variable can also be read or inferred using other instruments available to the operators. There are no contacts for initiation of any other equipment. The device is a single-function component with no programmable or software configurable features. Several thousand of the devices have been in successful service for several years as a parameter indicator in non-nuclear industrial applications.

Because of the simplicity and testability of the device, and its successful and relevant operating history, TR-106439 concludes that a detailed survey and associated visit to the vendor's facility are not required. The TR-106439 guidance notes that even though no formal credit is being taken for the vendor's quality assurance program or development process in the dedication of the device, the licensee or dedicator would typically contact the vendor to obtain this information. Testing of the device is the primary means of verification that the critical characteristics (including both hardware and software) have been met. The example provides a table of the critical characteristics, acceptance criteria, and methods of verification. After completion of the verification of the physical, performance, and dependability characteristics, the TR-106439 guidance concludes that this item was acceptable for use in safety-related applications.

The second example involves the replacement of an existing analog level indicator for a reactor building sump level with a microprocessor-based unit. The device also has a contact output for starting the sump pump at a preset level following a design basis accident. In this example, the TR-106439 guidance indicates that the added functionality, complexity and safety significance warrants greater scrutiny of the device's design, internal architecture, and the vendor's QA program. Most of the critical characteristics are similar to the first example; however, for this example, the methods of verification include the need for a commercial grade survey of the vendor to verify the adequacy of the vendor's design development process.

The third example is a multi-purpose, highly configurable device that controls the heating, ventilation and air conditioning for a room containing safety-related switchgear. In this example, the basic unit is commercially dedicated while the application program is developed by the licensee under its 10 CFR Part 50 Appendix B QA program. A commercial grade vendor survey was performed as with the previous example; however, due to the increased complexity of the digital modification, this survey was more extensive and involved a detailed review of the vendor's software development practices and design programs. Additional testing of the modification was also performed beyond the factory acceptance testing of the basic commercial unit.

The fourth example involves the use of programmable logic controllers (PLC) in an Engineered Safety Features Actuation System replacement. This example illustrates that the complexity of the commercial PLC and the high safety significance of the application warrant a significantly higher level of effort to evaluate and commercially dedicate the devices when compared to the previous examples. More interaction is required among the licensee, the designer/integrator of the replacement system, and the PLC commercial vendor. The example indicates that the same model PLC is being used for different functions so the dedication effort must include review of all of the application configurations. In this example, the licensee's first choice for the PLC vendor was found unacceptable due to the vendor's unwillingness to provide assurance that the licensee would be notified of operating system software errors or support the necessary configuration controls for any future required changes in software. A second PLC product was evaluated and after extensive vendor documentation surveys, testing, and design reviews was found acceptable.

These examples illustrate a generic approach for commercial dedication based on the type of commercial digital product application that is acceptable to the staff. While the general approach and information provided in TR-106439 are acceptable to the staff there is a substantial amount of detailed documentation required to be evaluated by the dedicating organization in order to establish equivalent qualification for commercial products under 10 CFR Part 50 Appendix B requirements.

## 5.0 CONCLUSION

The TR-106439 guidance provides for some flexibility in the specific methods for performing the verification activities for commercial dedication consistent with the staff requirements. Licensees referencing TR-106439 in either a license amendment or 10 CFR 50.59 evaluation for a proposed digital modification should document the dedication process such that there are descriptions and justifications for the alternative selected which will support the use of the commercial product in a safety related application.

The examples in TR-106439 used to illustrate the commercial dedication process were drawn from actual product and plant experiences. However, they are not intended to contain complete information on acceptance criteria and methods of verification. Additional critical characteristics may need to be considered in similar modifications proposed by licensees in the future. The examples also do not fully illustrate the level of detail that would be required to perform the activities credited in the dedication process.

Based on its review of TR-106439, the staff concludes that it contains an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications, and meets the requirements of 10 CFR Part 21. Further, the staff concludes that when digital equipment is dedicated using the methods described in TR-106439, it may be considered equivalent to digital equipment designed and manufactured under a 10 CFR Part 50, Appendix B quality assurance program. Licensees may utilize the TR-106439 approach when installing digital modifications utilizing commercial grade equipment. This includes microprocessors that are embedded in electrical and mechanical equipment as well as in instrumentation and control systems. While the staff finds the TR-106439 acceptable, it provides only a general generic proposal and thus licensees must ensure that the specific

documentation of the details of the dedication process and the identification and verification of specific critical characteristics for the commercial product are available including a combination of design verification information, performance testing and successful comparable operating history per the guidance of Generic Letters 89-02 and 91-05.