Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose

The purpose of this supplemental guidance is to provide an acceptable approach for procuring and accepting commercial grade digital equipment for nuclear safety applications that have a safety integrity level (SIL) certification by an accredited third party SIL certification body. Making use of internationally accredited SIL certification services benefits licensees and their suppliers through expanded access to expert services, improved standardization on equipment quality evaluations, improved regulatory confidence, and reduced cost.

This approach takes advantage of the internationally recognized SIL certification process when accepting commercial grade digital equipment for use in safety applications for the nuclear industry. Purchasers (licensees and suppliers of basic components) that procure commercial grade equipment for safety applications are able to rely on the third party SIL certification process in lieu of conducting a commercial grade survey (including a critical design review) to provide reasonable assurance that critical characteristics, and in particular dependability critical characteristics described in EPRI Technical Report 106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" are adequately controlled. The third party SIL certifiers are companies with accreditation by an accreditation body (AB), such as the American National Standards Institute [ANSI]), that are signatories to the International Accreditation Forum [IAF]. The net result will be higher confidence in the ability of these devices to perform their safety functions, as well as substantial reduction in duplication of effort for accepting commercial grade equipment across the industry.

1.2 Regulatory Basis

Basic components are items and services relied upon to perform a safety related function at US commercial nuclear power plants and are required to be controlled under a quality assurance program complying with 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants". A commercial grade item is an item that is not a basic component. Dedication (commercial grade dedication) is an acceptance process undertaken to provide reasonable assurance that a commercial grade item to be used as a basic component will perform its intended safety function.

When it is not possible to purchase items from a supplier that controls items in accordance with a 10CFR50, Appendix B-compliant QA program, items can be purchased as commercial grade items

Although the suppliers of commercial grade items and services are not required to comply with 10 CFR Part 50, Appendix B requirements, the commercial grade dedication activities must be performed under a Quality Assurance Program that meets the requirements of 10 CFR Part 50, Appendix B.

The NRC has endorsed EPRI TR-106439 as "*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.*"[1]

EPRI TR-106439 contains guidance on all aspects of commercial grade dedication of commercial grade digital equipment. EPRI TR-106439 identifies a unique type of critical characteristics for commercial grade digital equipment called *dependability.* The following excerpts from EPRI TR-106439 are germane to the scope of third party SIL certification [underlining added for emphasis]:

…a third type of critical characteristics, referred to in this guideline [EPRI TR-106439] *as dependability, becomes significantly more important when dedicating digital equipment including software…*

This is the category in which dedication of digital equipment differs the most from that of other types of components. It addresses attributes that typically cannot be verified through inspection and testing alone and are generally affected by the process used to produce the device…

The dependability attributes, which include items such as reliability and built-in quality, are generally influenced strongly by the process and personnel used by the manufacturer in the design, development, verification, and validation of the software-based equipment...

The dependability of a digital device also can be heavily influenced by designed-in elements, including robustness of the hardware and software architectures, self-checking features such as watchdog timers, and failure management schemes such as use of redundant processors with automatic fail-over capabilities. Evaluation of these attributes requires that the dedicator focus on more than just the development and QA processes. It may require gaining an understanding of the specific software and hardware features embodied in the design, and ensuring that they are correct and appropriate in light of the requirements of the intended application. Accordingly, a survey team may need to include specialists who understand the device design, the software, and the system in which it will be applied, in addition to quality assurance and programmatic issues.

[1] U.S. Nuclear Regulatory Commission, Safety Evaluation Report, "Review of EPRI Topical Report TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." TAC No. M94127, ADAMS accession no. 9810150223.

The dependability category captures those critical characteristics that must be evaluated to form an appropriate judgment regarding built-in quality of a software-based device. It also includes characteristics related to problem reporting and configuration control. Verification of these characteristics typically involves a survey of the vendor's processes (Method 2 [of NP-5652]*), and review of the vendor performance record and product operating history (Method 4)… Source inspections would not be used in verifying built-in quality of pre-existing software, because the software development has already occurred.*

…A commercial product may be judged to have sufficient quality, even if its development process lacked some of the rigorous steps of modern software engineering and/or some formal documentation. Reaching a reasonable level of assurance of quality of a commercial grade digital item typically involves making a judgment based on a combination of the product development process and its documentation, operating history, testing, review of design features such as failure management, and other factors noted in the critical characteristics matrix, Table 4-1 [in EPRI TR-106439].

This supplemental guidance document describes a method for using the accredited SIL certification process in lieu of a commercial grade survey as a dedication acceptance method to provide reasonable assurance that critical characteristics of digital devices, and in particular dependability characteristics, are adequately controlled. This supplemental guidance is applicable to dedicating entities subject to the quality assurance requirements of 10 CFR Part 50, Appendix B (e.g., 10 CFR Part 50, 10 CFR Part 52, 10 CFR Part 71 and 10 CFR Part 72 licensees and affected suppliers).

1.3 Acceptance of Safety Integrity Level As-Verification of Dependability Critical Characteristics

Third party SIL certification, provided by international bodies accredited by such accreditation organizations as ANSI, is a commercial grade service. The supplemental guidance within this document describes an approach to rely on third party SIL certifications, by companies accredited by ANSI and other signatories to IAF, in lieu of a commercial grade survey to verify adequate control of critical characteristics, in particular dependability characteristics described in EPRI TR-106439. The approach used to develop this guidance was to compare the third party SIL certification process with the EPRI TR-106439 dependability critical characteristics to evaluate their similarity and determine whether any additional actions are necessary to address differences.

Section 2 describes the third party SIL certification process, and Section 3 provides the US nuclear industry's evaluation of the third party SIL certification process including a comparison with NRC accepted practices (i.e., EPRI TR-106439). Section 6 describes the approach for the US nuclear industry to provide continued oversight of the third party SIL certification process in

order to confirm that the third party SIL certification process can continue to be used in lieu of commercial grade surveys for the purpose of verifying the EPRI TR-106439 dependability critical characteristics.

Based upon the conclusion that the third party SIL certification process is essentially equivalent to a commercial grade survey verifying the EPRI TR-106439 dependability critical characteristics, it has been determined that the third party SIL certifications, by companies accredited by IAF signatories, can be used in lieu of a commercial grade survey. This conclusion requires procurement documents to include a few requirements. Section 4 describes how Purchasers of commercial grade digital equipment should use the third party SIL certifications as part of their commercial grade dedication activities. It is noted that this supplemental guidance should be used in conjunction with the overall guidance on commercial grade dedication (i.e., EPRI TR-106439 and EPRI 3002002982). In addition, Section 5 describes information that Purchasers should ensure is included in their Quality Assurance Programs.

The following are the actions and steps that are necessary in order for a Purchaser to accept third party SIL certification of commercial grade digital equipment, by companies accredited by IAF signatory organizations, in lieu of performing a commercial grade survey to evaluate the EPRI TR-106439 dependability critical characteristics. Additional detail on performing these steps is discussed in subsequent sections of this guidance.

1) The method to use a third party SIL certification by a company accredited by a signatory to IAF in lieu of a commercial grade survey (alternative method) for verification of EPRI TR-106439 dependability critical characteristics is documented in the Purchaser's QA program.
2) The method the Purchaser needs to follow, and document in their QA Program, consists of:
    1. Adopt NRC-endorsed NEI 17-06
    2. The purchase documents require that:
        a. A copy of the SIL certificate for the commercial grade digital equipment being purchased be provided
        b. SIL certification has not expired
        c. SIL certification precautions and limitations be included in the SIL certificate or in the safety manual
        d. A certificate of conformance that the third party SIL certifier is accredited by a signatory to IAF.
    3. It is validated, at receipt inspection, that the commercial grade digital equipment supplier documentation certifies that:

a. The commercial grade digital equipment matches that defined in the SIL certificate provided
b. The purchase order's requirements are met

1.4 Acronyms

AB – Accreditation Body

CB – Certifying Body

CFR – Code of Federal Regulations

EPRI – Electric Power Research Institute

IAF – International Accreditation Forum

IEC – International Electrotechnical Commission

NEI – Nuclear Energy Institute

NRC – Nuclear Regulatory Commission

NUPIC – Nuclear Procurement Issues Corporation

QA – Quality Assurance

QC – Quality Control

SIL - Safety Integrity Level

2 SAFETY INTEGRITY LEVEL (SIL)

2.1 Description of the Third Party certification process for performance of safety functions of a particular safety integrity level (SIL)

The third-party certification process involves manufacturers seeking compliance with IEC 61508, the third-party certifier reviewing their efforts, and an accreditor verifying the third-party certifier's review practices. The main aspect that makes this process interesting is that the manufacturer is engaged and seeking to develop & manufacture products to meet the safety focused requirements defined in IEC 61508.

This process is initiated by a manufacturer identifying a business case for producing products that are capable of a particular SIL, commonly 2 or 3, for a defined scope of safety functions. Then they plan out their development based on the requirements of IEC61508. That standard drives the development process to incorporate measures to ensure both systematic integrity and reliability. One of the methods used to achieve systematic integrity is the use of rigorous lifecycle style development processes such as requirements definition, hardware and software design documentation, and verification and validation. Another method is the use of failure analysis, and to then use those results to build in safety features such as self-diagnostics, failure tolerance, failure recovery, fail to safe state, and environmental tolerance. To achieve reliability, care is taken to choose proven subcomponents, follow design margin and derating practices, and to use fault tolerant architectures. Reliability is then verified to be of an adequate level by modeling and estimating it using subcomponent failure rates and schematics of the product.

The significance of choosing a particular SIL is that it drives the level of rigor applied to the development process and it sets specific quantitative reliability goals. The application of the SIL to the quantitative goals is straight forward, but the impact on the developmental level of rigor (built-in quality/ systematic integrity) is a bit more complex. It is understood that systematic integrity (built-in quality) can't be measured in terms of a quantitative value, such as the probability of failure, so a qualitative case must be built to provide the necessary evidence. This case for systematic integrity is based on the use of processes and procedures during the product development phase that reduce the likelihood of design errors. The specific processes and procedures used are what are driven by a particular SIL. Part 3 of IEC 61508 focuses on the software development aspects and this document contains tables that are used to select those processes and procedures that will be used to build the case of meeting a systematic capability level. For example, a couple tables are shown below from IEC 61508 (in the tables R means recommended and HR means highly recommended):

Annex B
(informative)

Detailed tables

Table B.1 – Design and coding standards

(Referenced by Table A.4)

	Technique/Measure *	Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1	Use of coding standard to reduce likelihood of errors	C.2.6.2	HR	HR	HR	HR
2	No dynamic objects	C.2.6.3	R	HR	HR	HR
3a	No dynamic variables	C.2.6.3	---	R	HR	HR
3b	Online checking of the installation of dynamic variables	C.2.6.4	---	R	HR	HR
4	Limited use of interrupts	C.2.6.5	R	R	HR	HR
5	Limited use of pointers	C.2.6.6	---	R	HR	HR
6	Limited use of recursion	C.2.6.7	---	R	HR	HR
7	No unstructured control flow in programs in higher level languages	C.2.6.2	R	HR	HR	HR
8	No automatic type conversion	C.2.6.2	R	HR	HR	HR

Table B.2 – Dynamic analysis and testing

(Referenced by Tables A.5 and A.9)

	Technique/Measure *	Ref	SIL 1	SIL 2	SIL 3	SIL 4
1	Test case execution from boundary value analysis	C.5.4	R	HR	HR	HR
2	Test case execution from error guessing	C.5.5	R	R	R	R
3	Test case execution from error seeding	C.5.6	---	R	R	R
4	Test case execution from model-based test case generation	C.5.27	R	R	HR	HR
5	Performance modelling	C.5.20	R	R	R	HR
6	Equivalence classes and input partition testing	C.5.7	R	R	R	HR
7a	Structural test coverage (entry points) 100 % **	C.5.8	HR	HR	HR	HR
7b	Structural test coverage (statements) 100 %**	C.5.8	R	HR	HR	HR
7c	Structural test coverage (branches) 100 %**	C.5.8	R	R	HR	HR
7d	Structural test coverage (conditions, MC/DC) 100 %**	C.5.8	R	R	R	HR

Table B.7 – Semi-formal methods

(Referenced by Tables A.1, A.2 and A.4)

	Technique/Measure *	Ref	SIL 1	SIL 2	SIL 3	SIL 4
1	Logic/function block diagrams	See Note 1	R	R	HR	HR
2	Sequence diagrams	see Note 1	R	R	HR	HR
3	Data flow diagrams	C.2.2	R	R	R	R
4a	Finite state machines/state transition diagrams	B.2.3.2	R	R	HR	HR
4b	Time Petri nets	B.2.3.3	R	R	HR	HR
5	Entity-relationship-attribute data models	B.2.4.4	R	R	R	R
6	Message sequence charts	C.2.14	R	R	R	R
7	Decision/truth tables	C.6.1	R	R	HR	HR
8	UML	C.3.12	R	R	R	R

Table B.8 – Static analysis

(Referenced by Table A.9)

	Technique/Measure *	Ref	SIL 1	SIL 2	SIL 3	SIL 4
1	Boundary value analysis	C.5.4	R	R	HR	HR
2	Checklists	B.2.5	R	R	R	R
3	Control flow analysis	C.5.9	R	HR	HR	HR
4	Data flow analysis	C.5.10	R	HR	HR	HR
5	Error guessing	C.5.5	R	R	R	R
6a	Formal inspections, including specific criteria	C.5.14	R	R	HR	HR
6b	Walk-through (software)	C.5.15	R	R	R	R
7	Symbolic execution	C.5.11	---	---	R	R
8	Design review	C.5.16	HR	HR	HR	HR
9	Static analysis of run time error behaviour	B.2.2, C.2.4	R	R	R	HR
10	Worst-case execution time analysis	C.5.20	R	R	R	R

The manufacturer's efforts culminate into a final safety case that contains the evidence of meeting the reliability goals and the systematic integrity (built-in quality) capability levels that are associated with the particular SIL. The final safety case is then a deliverable to the entity that has been asked by the manufacturer to certify the subject product. This safety case typically consists of a Functional Safety Management (FSM) Plan, Safety Requirements Specification (SRS), Validation Test Plan, Tool Justification, Software Development Process Description, Coding Standard, Software Module Testing, Software Integration Testing, Failure Analysis, Probability of Failure Calculation, and the Safety Manual. This list can vary depending on the product and manufacturer, but the overall collection of documents is consistently intended to make the case for dependable operation. Figure 2.1 illustrates an example collection of documents that could be provided to a third-party certifier and highlights the certifier's evaluation process of the subject product.

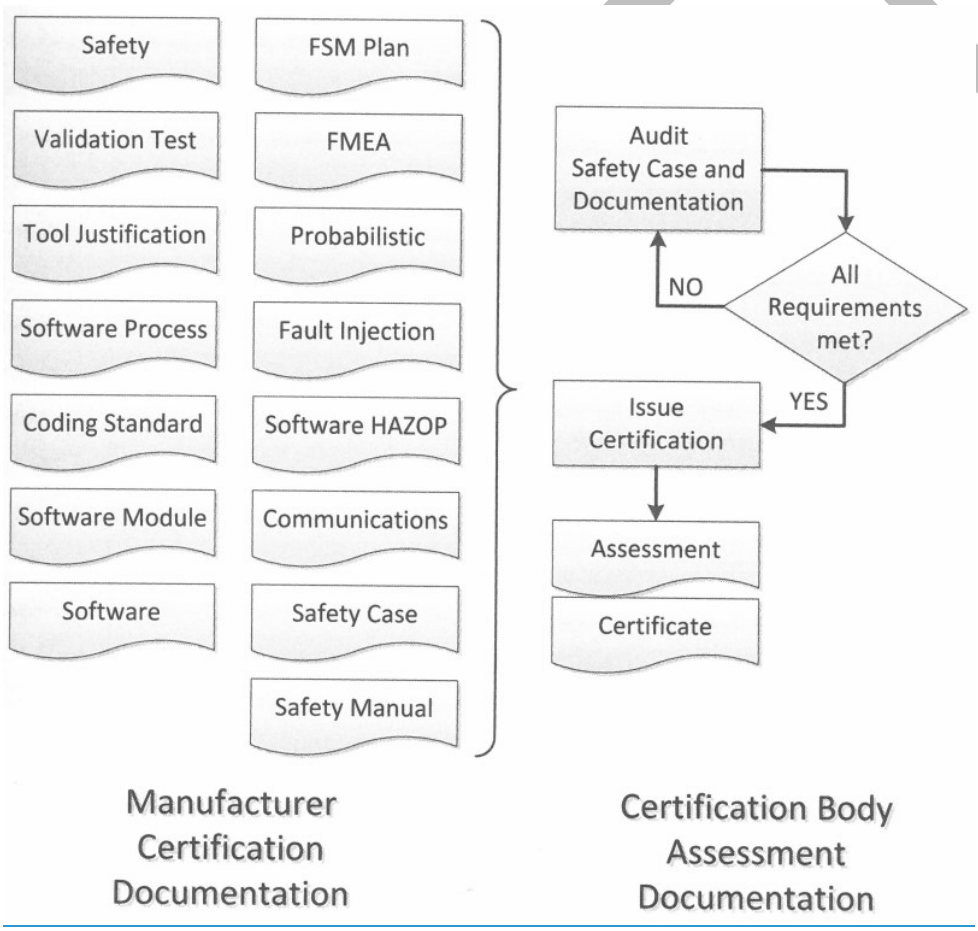

Figure 2.1. Typical Certification Process (Figure 1.3 from "Functional Safety- An IEC 61508 SIL 3 Compliant Development Process- 3rd Edition")

The third-party certifier (typically referred to as the certification body) proceeds to evaluate the documentation, manufacturer, and product to determine whether the requirements of IEC

61508 have been met for the desired SIL. The certification body's process includes visiting and auditing the manufacturer's design and manufacturing facilities, reviewing design documentation, and verifying calculations and technical evaluations. The certification body will also evaluate data such as warranty returns and failure rates. After this process is complete a certificate is granted, or gaps are identified to the manufacturer to be addressed before a certificate can be granted. The manufacturer can address gaps and re-initiate the certification process as many times as necessary or can abandon the effort if gaps are too significant.

When a certificate is granted, the certification body will establish criteria for maintaining its validity. The criteria may be time-period based, and/or change management based. Whenever any of the criteria are no longer being met the manufacturer must initiate a new effort to have the certification body perform the appropriate actions to re-establish the validity of the certificate.

To be a credible entity, the certification body is accredited by the national accreditation body. This accreditation is typically in accordance with ISO 17065. The accreditation bodies that primarily perform this type of work are the Deutsche Akkreditierungsstelle (DAkkS), in Germany, and the American National Standards Institute (ANSI), in the USA. The accreditation body performs audits and monitors activities of the certification body in order to confirm that their processes and procedures, and their corresponding implementation follows ISO 17065. Accreditations remain valid for a certain time period and then must be re-established through repeating the appropriate audits and evaluations.

2.2 Description of the critical dependability characteristics per NRC-endorsed EPRI-TR 106439

EPRI TR 106439 defines dependability as, "…a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others. [Adapted from NUREG/CR-6294]"

The process of commercial grade dedication as described in 10 CFR 21 requires the identification of critical characteristics for the basic component to be dedicated. EPRI TR 106439 adds a special type of critical characteristic unique to digital components to be dedicated: dependability.

EPRI TR 106439 describes dependability critical characteristics as attributes that typically cannot be verified through inspection and testing alone and are generally affected by the process used to produce the device. The dependability attributes are influenced by the process and personnel in the design, development, verification, and validation of the digital equipment (e.g., such as reliability and built-in quality). High quality is assessed by examining the

systematic life cycle approach from requirements through implementation, with verification and validation steps, and appropriate documentation for each phase of the lifecycle.

The dependability attributes also include designed-in elements, including robustness of the hardware and programmable logic architectures, self-checking features, real-time performance, and failure management schemes (e.g., fail safe). EPRI TR 106439 refers to this assessment as a critical design review (CDR). The CDR requires an understanding of the specific programmable logic and hardware features embodied in the design, to verify that they are correct and appropriate in light of the requirements of the intended application.

The CDR includes the evaluation of complexity of the programmable logic and device architecture (e.g., number of functions, inputs and outputs, internal communications, and interfaces with other systems or devices). EPRI TR-106439 includes a list of example activities that could be included in this review, but ultimately states that "The dedicator must determine which activities are appropriate for each application. In general, the choice and extent of activities undertaken to verify adequate quality, and the specific criteria applied in making the assessment, depend on the safety significance and complexity of the device." Since the evaluation of safety significance and complexity is not clearly defined in the US nuclear industry, this guidance leads to some ambiguity as to how this review should be performed. EPRI TR-106439 does include four examples of how the process can be utilized for various situations, and the US NRC's safety evaluation of the EPRI report adds that "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."

Assessment of dependability also includes characteristics related to problem reporting and configuration control.

Assessment of dependability typically involves a survey of the vendor's processes (Method 2[2]), and review of the vendor performance record and product operating history (Method 4). Source inspections (Method 3) would not be used in verifying built-in quality and designed-in elements, when implementation of the design has already occurred. Source inspections may be necessary to verify certain hardware quality characteristics during manufacture, or to ensure the quality of changes made to the programmable logic as part of a particular procurement.

Often, the CDR is considered synonymous with the use of method 2, commercial grade surveys (CGS), and this can sometimes cause confusion. While the CDR and CGS both involve seemingly similar vendor audit activities, the goals of these two activities are very different. A CDR is a

[2] These methods are described in EPRI 3002002982, "Plant Engineer: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications", Section 4.6

very technically focused activity that includes some quality assurance (QA) oriented reviews, which results in a determination of the suitability of the design for the application. A CGS is a very QA focused activity that includes some technical reviews resulting in a determination of whether items are being manufactured in compliance with the already approved design. Although it is not endorsed by the US NRC, EPRI 1011710 is often used as guidance for performing the CDR.

EPRI TR 106439 suggests that to accomplish this assessment requires a survey team that includes specialists who understand the device design, the programmable logic, and the system in which it will be applied, in addition to quality assurance and programmatic issues.

The ultimate conclusion that a product has met the dependability critical characteristics is based on engineering judgement. EPRI TR 106439 describes this in the following manner, "A commercial product may be judged to have sufficient quality, even if its development process lacked some of the rigorous steps of modern software engineering and/or some formal documentation. Reaching a reasonable level of assurance of quality of a commercial grade digital item typically involves making a judgment based on a combination of the product development process and its documentation, operating history, testing, review of design features such as failure management, and other factors noted in the critical characteristics matrix, Table 4-1."

Table 4-1 in EPRI TR 106439 provides a summary of a set of attributes associated with dependability critical characteristics. This same table provides acceptance criteria, methods of verification and remarks on the method of verification (e.g., guidance on how to perform the verification). The summary list includes:

- Reliability and maintainability related to the required functionality
- Built-in quality
    - Quality of design
    - Quality of manufacture
    - Failure management
    - Compatibility with human operators, maintainers
- Configuration control and traceability
    - Hardware
    - Software/firmware (i.e., programmable logic)
    - Problem reporting

Table 4-2 in EPRI TR 106439 provides more detail on attributes that can be evaluated in assessing built-in quality.

Section 3 demonstrates that the IEC 61508 SIL certification process encompasses the assessment of the dependability critical characteristics as described in this section.

3 EPRI RESEARCH OF THE SIL CERTIFICATION PROCESS

3.1 Scope of the EPRI Research

3.2 Summary of the EPRI Research

4 ACCEPTANCE OF COMMERCIAL GRADE DIGITAL EQUIPMENT FOR SAFETY APPLICATIONS CERTIFIED TO A PARTICULAR SIL

4.1 Application of the SIL Certification Process

4.2 Technical Evaluation & Acceptance Method

5 SUPPLIER'S QUALITY ASSURANCE PROGRAM

The supplier is the entity that is responsible to the Commercial Grade Dedication of the digital component/s. This can be an Appendix B supplier or licensee with an Appendix B program and would not normally be the vendor of the SIL certified component/s but could be. This section addresses how the IEC 61508 SIL certification process will be integrated into that Appendix B program.

Suppliers that rely on the accreditation IEC 61508 SIL certification process for the dependability critical characteristics (CC) in lieu of commercial grade surveys are required by 10 CFR Part 50, Appendix B to document this alternative method in their QA program. See sections 3 and 4 more details on this process.

The following sections discuss criteria that need to be addressed in the QA Program in order to credit the IEC 61508 SIL certification process. The Appendix B supplier will ensure certification and accreditation as described in Section 4 of this guidance and will impose any additional technical or quality program requirements, as necessary, to meet regulatory requirements and Purchaser QA program commitments.

Note: *The supplier can be the OEM, a 3rd part commercial dedicator, or the Licensee.*

5.1 Organization

The Supplier retains overall responsibility for assuring that purchased digital device meets applicable technical and regulatory requirements and that reasonable assurance of quality is provided. There are no special requirements beyond Appendix B.

5.2 Procurement Document Control

When purchasing IEC 61508 SIL certified components/systems by certifying bodies (CB) that have been accredited by approved NUPIC accreditation services, the procurement documents will impose additional technical and quality requirements, as necessary, to satisfy the Purchaser/Supplier's QA Program and technical requirements.

These shall be included as a minimum:

1) The component must be provided in accordance with the CB's accredited program and scope of certification and accreditation.
2) An IEC 61508 SIL certificate report is a deliverable to the purchasing organization and must contain adequate information to ensure performance and applicability to the intended safety function.

3) The purchaser must be notified of any condition that adversely impacts the component's certification and the CB's accreditation. This should be part of the supplier's Part 21 program.

5.3 Control of Purchased Material, Equipment, and Services

For the digital dependability critical characteristic, the Supplier can take credit for the IEC 61508 SIL certification and accreditation processes. Suppliers using the IEC 61508 SIL certification process for the dependability CC will be responsible for:

1) Reviewing the Certification Body's (CB) Certification report and ensuring applicability to the defined safety function and has adequate information to support Commercial Grade Dedication requirements as defined in the following sub-sections.
2) Reviewing the up-to-date Accrediting Body's (AB) documentation of the CB that certified the component and ensure there are no outstanding deficiencies or findings.
3) The Suppliers do not need to directly perform technical verification of data produced nor do they need to perform commercial grade surveys of the certification activities.
4) The supplier will review the objective evidence for conformance to the procurement documents as part of the dedication process to verify that the technical and quality requirements identified in the purchase documents are met.

5.4 QA Evidence for Digital Dependability

For the digital dependability critical characteristic, the Supplier can take credit for the IEC 61508 SIL certification and accreditation processes.

5.4.1 QA Evidence for Digital Dependability

The IEC 61508 SIL certification process for the dependability CC will be demonstrated by:

1) An up to date IEC 61508 SIL certification report applicable to the component and its safety related function
2) An up to date and acceptable NUPIC observation report per the guidelines of "NUPIC DOCUMENT NO. XX SIL CERTIFICATION ACCREDITATION BODY OVERSIGHT"

5.4.2 Supplier Tasks associated Digital Dependability Evidence

Suppliers using the IEC 61508 SIL certification process for the dependability CC will be responsible for:

1) Review and approval of the certification report and ensuring applicability to the defined safety function.
2) Reviewing and approving the up-to-date AB's accreditation document of the CB in that is it is consistent with the component being received and that there are no outstanding findings.

3) The supplier will review the objective evidence for conformance to the procurement documents as part of the dedication process to verify that the technical and quality requirements identified in the purchase documents are met.

Note: The Supplier does not need to directly perform technical verification of data produced nor should they need to perform commercial grade surveys of the vendor/manufacturer of the SIL certified component, such as to verify the dependability CC. Note that there may be other reasons to perform a commercial grade survey besides dependability CC verification.

5.5 Corrective Action

1) The supplier shall have a Corrective action program and assume 10 CFR Part 21 responsibility.
2) The supplier is required to notify Licensees and the NRC of any significant conditions adverse to quality as required by Part 21.
3) The SIL certification process requires the component vendor to identify problems as part of the certification process. The supplier shall have a contractual relationship in place to ensure notification from the vendor.

6 US NUCLEAR INDUSTRY OVERSIGHT OF THE SIL CERTIFICATION PROCESS

The objective of the oversight of the IEC 61508 3rd Party SIL Certification Process by the U.S. nuclear industry is to confirm that the process continues to cover the EPRI TR 106439 Dependability Critical Characteristics and is implemented consistently for all vendor equipment evaluations, so that the process can be used in lieu of commercial grade surveys as part of the Purchaser's commercial grade dedication activities. Early identification of potentially adverse conditions will afford the nuclear industry the opportunity to discuss any impact with the NRC and to modify this guidance as necessary.

6.1 Organization

NUPIC and NEI are responsible for the industry oversight of the IEC 61508 3rd party SIL certification process as it relates to industry's use of the process as part of commercial grade dedication. NUPIC has formed a group to support the industry's efforts to monitor the 3rd Party IEC 61508 SIL accreditation process. NUPIC plays a central role in the continued oversight activities, and a NUPIC member leads or participates in the oversight activities described below.

6.2 Verification that the SIL Certification Process Continues to be Consistent with NRC Endorsed Practices

The assessments and conclusions of the consistency of the 3rd Party IEC 61508 SIL certification process documented herein include the evaluation of any future changes to the 3rd Party IEC 61508 SIL certification process, since NRC endorsement, to make sure the process continues to cover the EPRI TR 106439 Dependability Critical Characteristics.

As part of the continued oversight, the nuclear industry through NEI will monitor the 3rd Party IEC 61508 SIL Certification requirements to verify that they continue to cover the EPRI TR 106439 Dependability Critical Characteristics. Because IEC 61508 is the main standard that assures consistency with NRC accepted practices and because it is not often revised, it is expected that changes that would make the 3rd Party IEC 61508 SIL certification process no longer consistent with EPRI TR 106439 Dependability Critical Characteristics would be few and infrequent, if at all.

Any time the IEC 61508 standard is under revision, NEI will evaluate whether the potential changes impact the 3rd Party IEC 61508 SIL certification process and its coverage of the EPRI TR 106439 Dependability Critical Characteristics. If changes adversely impact coverage of the EPRI TR 106439 Dependability Critical Characteristics, then the nuclear industry through NEI has the

ability to provide feedback to the IEC 61508 standards development committee to change the draft revision to encompass these critical characteristics.

As a result, the nuclear industry has an opportunity to vet changes to 3rd Party IEC 61508 SIL certification requirements before they are implemented, and thus provide the nuclear industry and NRC with substantial advanced notification, and would have time to implement changes to this guidance or otherwise issue communications to users of the guidance.

NEI will make the NRC aware of any potential adverse changes and industry's actions to mitigate them. A summary of the monitoring of 3rd Party IEC 61508 SIL certification requirements will be documented whenever IEC 61508 is revised.

6.3 Verification that Implementation of the 3rd Party IEC 61508 SIL Certification Process Continues to be Consistent With NRC Accepted Practices

The assessments and conclusions of the consistency of the implementation of the 3rd Party IEC 61508 SIL certification process documented herein are based in part on the direct observations of the performance by accreditation bodies (e.g., ANSI and Deutsche Akkreditierungsstelle [DAkks]) for SIL certification. These evaluations are performed to verify the accreditation process continues to be consistently applied.

NUPIC and other Industry Representatives will observe accreditation bodies that accredit 3rd party IEC 61508 SIL certifiers to ensure that the 3rd Party IEC 61508 SIL certification process continues to be implemented consistently. U.S. nuclear industry observations will be performed initially on a three (3) year frequency with the possibility of reducing the frequency if it is observed that the process is demonstrably consistent. The initial 3 year frequency is consistent with the guidance in NRC Regulatory Guides 1.28 and 1.144 for auditing 10 CFR 50 Appendix B suppliers. The NRC may request to participate on these observations.

Appendix A - Quality Assurance Program Template