Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications Revision 0 – DRAFT B

Prepared by the Nuclear Energy Institute
October 2021

Revision Table

Revision	Description of Changes	Date Modified	Responsible Person
Rev. 0 – Draft B	Incorporated NRC Comments	Oct. 2021	Andy Nack
Rev. 0	Initial Issuance	Feb. 2021	Andy Nack

Acknowledgements

This document was developed by the Nuclear Energy Institute. NEI acknowledges and appreciates the contributions of NEI members and other organizations in providing input, reviewing and commenting on the document including

NEI Project Lead: Maria Assard and Andy Nack

Notice

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

Table of Contents

1 INTRODUCTION

1.1 Scope

The scope of the methodology contained in this document is as follows:

- Applies only to commercial digital I&C equipment that is IEC 61508 SIL certified
- Applies only to IEC 61508 certifications that have been issued by a functional safety certifying body (CB) that has been accredited to ISO 17065 by an accreditation body (AB) who is a signatory of the International Accreditation Forum (IAF) Multi-Lateral Agreement (MLA)
- Applies only to the dependability critical characteristics (CC) and not to the physical or performance CCs of the commercial graded dedication process as defined by EPRI Technical Report (TR) 106439 and EPRI 3002002982
- Applies only to 10 CFR Part 50 and 10 CFR Part 52 power reactors

1.2 Purpose

The purpose of this supplemental guidance is to provide an acceptable approach for taking advantage of the internationally recognized IEC 61508 SIL certification process when determining acceptability of the dependability critical characteristics of equipment that fit into the scope as defined by section 1.1. Dedicating entities are able to rely on the SIL certification to provide reasonable assurance that dependability CCs described in EPRI TR 106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," are adequately controlled in lieu of conducting a Method 2- commercial grade survey (including a critical digital review) and/or Method 4- Acceptable Item Performance Record. The physical and performance CCs continue to be evaluated using the traditional methodologies. The net result will be increased 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.

1.3 Pre-Requisites

Prior to utilizing the methodology contained in this document ensure the following pre-requisites are met:

- The quality assurance program of the dedicating entity and of the US NRC licensee must be revised as described in section 6 of this document.
- The CB's services must be determined to be acceptable for use using one of the paths described in section 5.3 of this document. (NOTE: exida's certification services have been determined to be acceptable through NEI's observations and evaluations described in section 5.4 - 5.6 and Appendix E of this document. This determination is valid for 3 years from the date noted on the checklist in Appendix E [Jan 2021]).

1.4 Regulatory Basis

Basic components are items and services relied upon to perform a safety related function at U.S. 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 accepted for use as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, QA program.

When it is not possible to purchase items from a supplier that controls items in accordance with a 10 CFR 50, Appendix B-compliant QA program, items can be purchased as commercial grade items and accepted via the dedication process. The organization performing this dedication is referred to as the dedicating entity (i.e., licensee, third party dedicator, or manufacturer with an Appendix B program) in this document.

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 are required to be performed in compliance with those requirements.

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 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

[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.

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.

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 the dependability critical characteristics of digital devices are adequately controlled. This supplemental guidance is applicable to dedicating entities subject to the quality assurance requirements of 10 CFR Part 50, Appendix B.

1.5 Acceptance of Safety Integrity Level as Verification of Dependability Critical Characteristics

The guidance within this document describes an approach to rely on SIL certifications, by companies accredited by ANAB and other signatories to IAF, in lieu of a commercial grade survey to verify adequate control of dependability characteristics described in EPRI TR-106439. The approach used to develop this guidance was to compare the 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 SIL certification process and describes dependability critical characteristics, and Section 3 summarizes research performed by EPRI to evaluate the SIL certification process and compare it to NRC accepted practices (i.e., EPRI TR-106439). Section 5 evaluates the ISO 17065 accreditation process of SIL CBs. Section 7 describes the approach for the U.S. NRC licensees (or their designee) to provide continued oversight of the SIL certification process in order to confirm that the 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 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 SIL certifications, issued by CBs that are accredited by ABs which both have been evaluated and approved by the US NRC and their licensee (or their designees) as described in this methodology, can be

used in lieu of a commercial grade survey to verify EPRI TR-106439 dependability critical characteristics. This conclusion requires procurement documents to include a few requirements. Section 4 describes how dedicating entities of commercial grade digital equipment should use the SIL certifications as part of their commercial grade dedication activities. It is noted that this guidance should be used in conjunction with the overall guidance on commercial grade dedication (i.e., EPRI TR-106439, EPRI 3002002982, U.S. RG 1.164). In addition, Section 6 describes information that dedicating entities should ensure is included in their Quality Assurance Programs.

1.6 Acronyms

AB Accreditation Body

AC Administrative Controls

ANAB ANSI National Accreditation Board

ANSI American National Standards Institute

CB Certification Body

CC Critical Characteristics

CDR Critical Digital Review

CFR Code of Federal Regulations

CGD Commercial Grade Dedication

CGS Commercial Grade Surveys

COTS Commercial Off the Shelf

DSA Documented Safety Analyses

E/E/PE Electrical, Electronic, and Programmable Electronic

EPRI Electric Power Research Institute

FMEA Failure Modes Effects Analysis

FMEDA Failure Modes, Effects and Diagnostic Analysis

FSM Functional Safety Management

HW Hardware

IAF International Accreditation Forum

IEC International Electrotechnical Commission

MLA Multi-Lateral Agreement

NEI Nuclear Energy Institute

NRC Nuclear Regulatory Commission

NUPIC Nuclear Procurement Issues Corporation

OEM Original Equipment Manufacturer

OQAP Operating Quality Assurance Program

PFD_{avg} Average Probability of Dangerous Failure on Demand

PFH Probability of Failure per Hour

QA Quality Assurance

QC Quality Control

SIL Safety Integrity Level

SIF Safety Instrumented Function

SIF Safety Instrumented System

SLM Safety Layer Matrix

SQA Software Quality Assurance

SRS Safety Requirements Specification

SS Safety Significant

SSC Safety, Systems, and Components

SW Software

1.7 References

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

2. 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.”

3. U.S. Nuclear Regulatory Commission, “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.” TAC No. M94127, ADAMS accession no. ML12205A284.

4. EPRI 3002002982, “Plant Engineer: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications: Revision 1 to EPRI NP-5652 and TR-102260,” September 22, 2014, Electric Power Research Institute.

5. IEC 61508, Edition 2.0, “Functional safety of electrical/electronic/programmable electronic safety-related systems,” International Electrotechnical Commission.

6. ISO/IES 17065, “Conformity assessment — Requirements for bodies certifying products, processes and services,” September 15, 2012.

7. EPRI 1011710, “Handbook for Evaluating Critical Digital Equipment and Systems,” November 2005, Electric Power Research Institute.

8. EPRI 3002011817, “Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power,” Electric Power Research Institute, July 2019.

9. IEC 61511-1, “Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements, Edition 2.1,” August 2017.

10. IEC 61513, “Nuclear power plants - Instrumentation and control important to safety - General requirements for systems.”

11. IEC 60880, “Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems.”

12. IEC 62138, “Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions.”

13. IEC 60987, “Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems.”

14. IEEE 603-2018, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

15. IEEE 379, “IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”

16. IEEE 7-4.3.2, “IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations.”

17. EPRI TR-107330, “Generic Requirement Specifications for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” Electric Power Research Institute.

18. NRC Regulatory Issue Summary 2002-22 Supplement 1, “Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,” May 31, 2018, ML18143B633, U.S. Nuclear Regulatory Commission.

19. NRC Regulatory Guides RG 1.28, Revision 5, “Quality Assurance Program Criteria (Design and Construction),” ML17207A293, U.S. Nuclear Regulatory Commission.

20. NRC Regulatory Guides 1.144, Revision 1, “Auditing of Quality Assurance Programs for Nuclear Power Plants,” ML13038A428, September 1980, U.S. Nuclear Regulatory Commission.

21. Functional Safety- An IEC 61508 SIL 3 Compliant Development Process- 3rd Edition, M. Medoff & R. Faller, exida, 2014.

22. WIKA, “Operating Instructions for the Differential Pressure Gauge with Micro Switches, Model DPGS40TA, with Component Testing,” https://www.wika.us/upload/OI_DPGS40TA_en_de_fr_es_69312.pdf

23. EPRI 3002011817, “HAZCADS: Hazards and Consequences Analysis for Digital Systems,” Electric Power Research Institute, December 2018.

24. NRC Regulatory Guide 1.164, Revision 0, “Dedication of Commercial-Grade Items for Use In Nuclear Power Plants,” ML17041A206, June 2017, U.S. Nuclear Regulatory Commission.

2 SAFETY INTEGRITY LEVEL (SIL)

2.1 Description of the Safety Integrity Level (SIL) Certification Process

The SIL certification process involves manufacturers seeking compliance with IEC 61508, a separate entity called the CB that reviews the manufacturer’s efforts, and an AB that verifies the CB’s review practices.

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 IEC 61508. This international standard provides a generic approach for all safety life-cycle activities for systems comprised of electrical, electronic, and/or programmable electronic elements that are used to perform safety functions and adopts a risk-informed approach by which the safety integrity requirements can be determined. This standard drives the development process to incorporate measures to ensure both systematic integrity and reliability. Part of the approach 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 part 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 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 reliability goals is implemented in tables that correlate an Average Probability of Dangerous Failure on Demand (PFD_{avg}) or Probability of Failure per Hour (PFH) range to each SIL. 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 contains tables that list processes and procedures that are correlated to specific SILs. These tables are used to drive the development process and build the case of meeting a systematic capability level. IEC 61508 introduces the concept of systematic capability as a measure of confidence in equipment to be free of systematic errors or faults. This confidence is built on the development process of the equipment being in compliance with these tables. For example, a table is shown on the following page from IEC 61508 (in the table R means recommended and HR means highly recommended):

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 2.1- IEC:2010 Dynamic Analysis and Testing

The manufacturer's efforts culminate into a safety case that contains the evidence of meeting the reliability goals and the systematic capability requirements that are associated with the targeted SIL. The safety case is then a deliverable to the CB 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 CB and highlights the CB's evaluation process of the subject product.

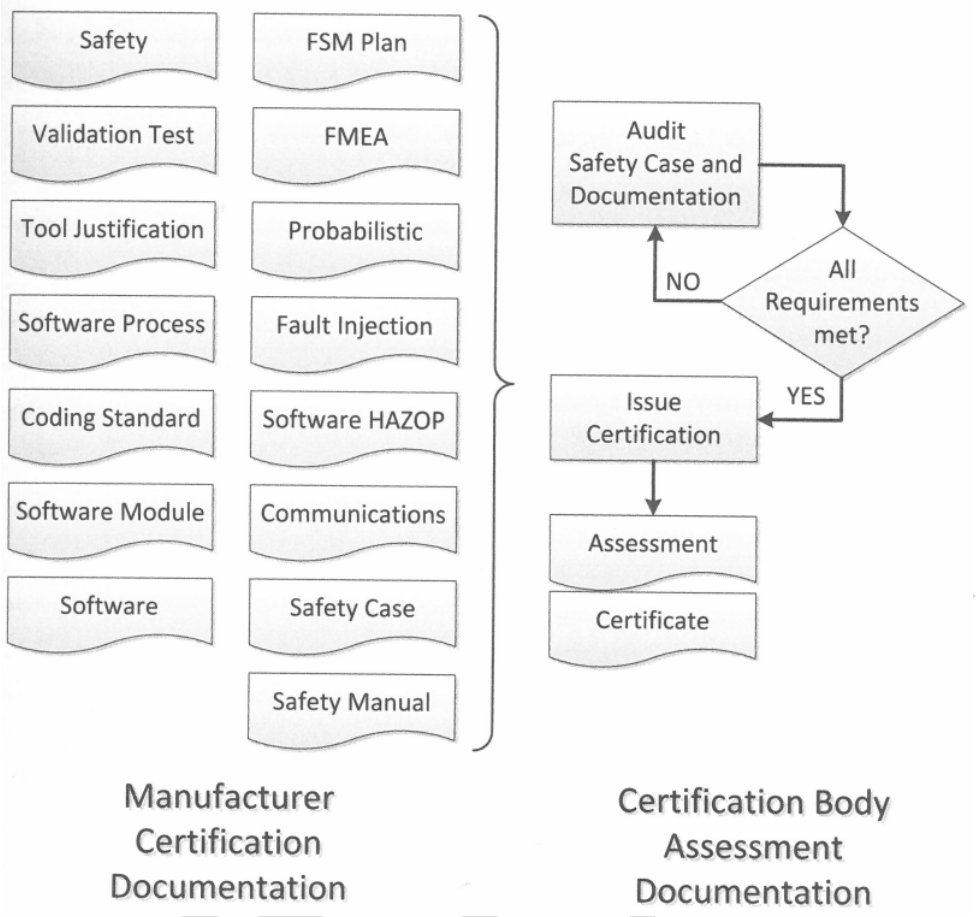

Figure 2.1- Typical Certification Process (Figure 1.3 from Reference 21)

The CB proceeds to evaluate the documentation, manufacturer, and product to determine whether the requirements of IEC 61508 have been met for the targeted SIL. The CB's process includes visiting and auditing the manufacturer's design and manufacturing facilities, reviewing design documentation, and verifying calculations and technical evaluations. The CB 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. 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 CB 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 CB perform the appropriate actions to re-establish the validity of the certificate.

To be established as a credible entity, the CB is accredited by the national AB. This accreditation is typically in accordance with ISO 17065 supplemented by an IEC 61508 compliant certification scheme. The ABs that primarily perform this type of work are the Deutsche Akkreditierungsstelle (DAkkS), in Germany, and the ANAB, in the U.S.. The AB performs audits and monitors activities of the CB in order to confirm that their processes and procedures, and their corresponding implementation follows ISO

17065 (including an IEC 61508 compliant scheme). Accreditations remain valid for a certain time period and then must be re-established by repeating the appropriate audits and evaluations.

2.2 Description of the Dependability Critical 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 applicable 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 digital 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 U.S. 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 U.S. 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 manufacturer's processes (Method 2[2]), and review of the manufacturer's performance record and product operating history (Method 4). Source inspections (Method 3) would not be used in verifying built-in quality and designed-

[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

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 manufacturer assessment activities, the goals of these two activities are quite different. A CDR is a 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 accepted design. Although it is not endorsed by the U.S. NRC, EPRI 1011710 is often used as guidance for performing the CDR.

EPRI TR 106439 suggests that to accomplish the CDR 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 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 methods 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.

3 EPRI RESEARCH OF THE SIL CERTIFICATION PROCESS

3.1 Scope of the EPRI Research

In support of the industry's interest in SIL certified equipment, EPRI conducted research on this topic and issued a report that is referenced as, *Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power*, EPRI, Palo Alto, CA: 2019. 3002011817 (Reference 8). All page number references in Section 3.1 and 3.2 refer to Reference 8.

In this report, EPRI explained that the motivation of this work comes from the desire of the nuclear industry to utilize the existing ecosystem of SIL certified electrical, electronic, and programmable electronic (E/E/PE) equipment. This equipment has come into existence over the past 15-20 years to serve other industries that also "have the potential to cause harm through the operations of their facilities" (p1-1). The report further explains that:

> The nuclear industry is interested in leveraging this ecosystem to take advantage of its highly reliable and relatively low-cost certified equipment and to reduce detailed technical reviews, at the platform level, by regulatory bodies of such equipment. Use of this ecosystem for nuclear safety-related equipment would provide several important benefits. It would allow platform selection during the detailed design phase of a project (rather than during the conceptual design phase), would expand the market of available products, and could ease the regulatory interface. Most importantly, it could produce substantial improvement in lifecycle efficiency and plant safety. (p1-1)

During this research effort, EPRI reviewed the standards that shape the SIL framework and implementation methodology to establish a basic understanding. They also interviewed individuals with knowledge of and experience with SIL processes to gain deeper insights. They also gathered and analyzed failure data to determine if actual operating experience of SIL certified equipment aligned with the reliability claimed by the certification process. The report describes this effort as:

> The EPRI Team gathered information and data from various SIL certifiers, OEM's, and accreditation authorities. This information and data was correlated and analyzed to provide accurate insights on how the SIL certification process works, its level of validity, and the measurable level of safety reliability afforded to digital I&C equipment by adherence to the SIL certification process (p vii).

3.2 Summary of the EPRI Research

At a high level, the report can be summarized in the following points. First, the technical and QA requirements involved with SIL certification are very similar to that of nuclear grade equipment. Second, Certification Bodies (CBs) have a standardized, rigorous, and reliable evaluation process. Third, Accreditation Bodies (ABs) hold CBs accountable and maintain an internationally consistent set of expectations to ensure accredited CBs can be trusted by end-users from any industry in any country

(i.e., in any regulatory framework). Fourth, the analysis of field failure data supports the conclusions of reliable operation of certified equipment. Finally, the fifth point is a direct quote from the report: "based on the equipment studied, SIL certifications appear to be an accurate indicator of hardware and software safety reliability for programmable electronic equipment at the platform/product level" (p7-2). To make these points, the report consists of nine chapters and six (A-F) appendices. Chapter 1 of the report provides introductory and background information that has already been summarized in Section 3.1 of this document.

Chapter 2 focuses on explaining what functional safety is and how the standards have developed around it as a central concept. Regarding functional safety, the report states:

> It can be thought of as a set of rules and methods for the specification, design, and operation of safety functions which are part of automatic protection systems. These safety functions are accomplished by equipment (e.g., sensors, logic solver, and final elements) that automatically mitigates a hazard. (p2-1)

The report then presents IEC 61508 as the foundational standard addressing functional safety, and describes it as:

> an international, performance-based (i.e., it avoids prescriptive rules, such as redundancy and self-test capability) standard for the functional safety of E/E/PE equipment (p2-1)

And as:

> a basic safety publication of the IEC. As such, it is an umbrella document covering multiple industries and applications. One objective of the standard is to help individual industries develop supplemental standards, tailored specifically to those industries, based on IEC 61508. Another objective is to enable the development of E/E/PE safety-related systems in the absence of industry specific standards. (p2-2)

The industry specific standards the report describes are IEC 61511 (very similar to ISA 84.00.01) for the process industry, and IEC 61513 for the nuclear industry. IEC 61511 has been widely implemented by the process industries and represents the most significant sector of the SIL ecosystem. This standard is very consistent with the framework laid out by the parent document (IEC 61508). IEC 61513 has been implemented by the nuclear industries in some countries, mostly in Europe, but this standard breaks from the performance-based requirements for systematic integrity and the probabilistic approach to reliability. It points to other standards such as IEC 60880, IEC 62138, and IEC 60987 that implement a very prescriptive and deterministic approach that is very similar to the IEEE Nuclear Power Engineering Committee's (NPEC's) suite of standards (e.g., IEEE 603, IEEE 379, IEEE 7-4.3.2).

The final section of Chapter 2 explains why the SIL ecosystem is embraced by manufacturers and end users, identifying that all parties benefit when using this functional safety framework. The manufacturers increase the customer base for their products while the end users increase confidence in the safety of their facilities, protect investments, and satisfy requirements of regulators and insurance companies.

Chapter 3 describes the details of the SIL methodology and describes its fundamental concepts. The report states:

> IEC 61508 is based on two fundamental concepts:
>
> - safety lifecycle, which uses probabilistic, performance-based system analysis and design to minimize random failures and an engineering process to minimize systematic faults resulting from design and documentation errors
>
> - safety integrity levels, which are used to implement a graded approach to achieving functional safety (with respect to both random and systematic failures) (p3-1)

The report then goes into further detail on the implementation of the safety lifecycles and the four safety integrity levels (SILs), with SIL 1 being the least rigorous through to SIL 4 which is the most rigorous. Next the report describes the concept of risk reduction and the three aspects that are used to realize the desired level of reduction. Those aspects are probability of failure, architecture constraints, and systematic capability. The report describes these as:

> 1. Systematic capability must be verified for IEC 61508 certified elements or prior use justification must be documented.
>
> 2. Architectural constraints must satisfy applicable SIL requirements.
>
> 3. Probability of failure per hour (PFH) or average probability of dangerous failure on demand (PFD_{avg}), depending on the mode of operation (i.e., low demand mode, high demand mode, or continuous mode), must be calculated and satisfy applicable SIL requirements. (p3-4)

The report explains that the overall SIL is ultimately the most limiting of these three aspects, and then includes a significant amount of detail related to these three aspects. The aspect of systematic integrity is further explained in Chapter 3 starting with the section titled "The IEC 61508 Safety Lifecycle Applied to Products" and continues through to the end of the chapter.

One aspect of systematic integrity to highlight is the level of independence that is required for the various SILs. Details of this aspect are included in Table 3-8 of the report. This is highlighted because reviewer independence is an important aspect of NRC digital safety system guidance.

The last section of Chapter 3 is "Supplier Quality Management." It reviews some older EPRI research that compares the type of quality system utilized by manufacturers within the SIL ecosystem (ISO 9001) to a nuclear quality program based on 10 CFR 50, Appendix B. This section concludes with the following statement:

> These EPRI research results indicate that there is no reason to believe that E/E/PE equipment certified to IEC 61508 SIL 2 or 3 is not suited to perform safety-related functions merely because its OEM utilizes a QA program certified to ISO 9001 (or similar), rather than a nuclear industry specific QA program.(P3-21)

It is important to understand that the point of this statement is that SIL products should not be discarded just because the underlining quality management system is usually based on ISO 9001. This is an acknowledgement of the issues the NRC had previously identified with ISO 9001. EPRI's observation

was that layering IEC 61508 on top of ISO 9001 sufficiently addresses most of the gaps identified by the NRC.

It is important to note that NEI 17-06 is still using most of the traditional aspects of commercial grade dedication in the proposed process so there is already an established approach to addressing the fact that the manufacturer does not have a 10 CFR 50, Appendix B QA program.

The scope of Chapter 4 is the third-party certification process. This aligns with the scope of Section 2.1 of this document. Refer to Section 2.1 of this document for supplemental information. Once the manufacturer has completed the design of the product and has established the manufacturing processes, the manufacturer will assemble evidence of their compliance with the desired SIL, in accordance with IEC 61508, into a safety case. Then they present this safety case to a CB for evaluation. This chapter discusses what is involved in the CB's review of the safety case and lists the actions a CB must perform. This list is:

- audit the product development process
- audit the product developer's internal verification and validation efforts and assess their level of independence
- audit/prove that the developer is executing its V model (or a repeatable form of lean agile)
- oversee the self-validation process to ensure that the developer does what it says it does
- revalidate that the product developed complies with the relevant governing standard(s)
- validate that the product developer is doing what is necessary, traceable, and reproducible to comply with IEC 61508 (p4-2 to 4-3)

To better understand safety cases, EPRI received an example safety case from a CB that had been redacted to remove the manufacturer's proprietary information. EPRI reviewed this redacted safety case and made the following observation in the report:

> The redacted safety case content was also compared to the dependability attributes addressed in EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," and TR-107330, "Generic Requirement Specifications for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." the topics of which are summarized as follows:
>
> - Development Personnel Qualifications/Experience
> - HW/SW Design, Development, Verification & Validation Processes
> - Availability/Reliability Requirements
> - Failure Modes Analysis/Testing/Management
> - Design Documentation

- Configuration Management
- Quality Assurance (QA) Program and Practices, including Software Quality Assurance (SQA) (consistent with 10 CFR 50, Appendix B)
- SW Requirements Definition & Requirements Traceability
- Vendor Testing (Performance, Environmental, SW V&V, Fault Insertion)
- Product Operating History (Documented, Sufficient, Successful, Relevant)
- Error Tracking/Problem Reporting [47][48]

> The redacted safety case addresses each of these bullet items in whole, or at least in part. With respect to quality assurance, while it doesn't address 10 CFR 50, Appendix B requirements, per se, it does address the OEM's QA program and practices, including SQA. Most OEM QA programs have been certified to ISO 9001 or similar. (See Section 3 of this report for further discussion of QA aspects of SIL certification.) (p4-8 to 4-9)

The report also explains why the dedicating entity can expect to receive notification directly from the manufacturer when defects are identified that impact the safe operation of the SIL certified equipment. Receiving defect reporting directly from the manufacturer is important to support 10 CFR 21 defect reporting responsibilities. In the following quote, "end-users" are the purchasers of the equipment, and therefore would be the dedicating entity:

> OEM's [sic] of certified products are, however, required to comply with IEC 61508, clause 7.8.2.2, which says, "Manufacturers or system suppliers that claim compliance with all or part of this standard shall maintain a system to initiate changes as a result of defects being detected in hardware or software and to inform users of the need for modification in the event of the defect affecting safety." This provides confidence that end-users will be notified of a certified product's defect if that defect affects safety. (p4-9)

Chapter 4 then identifies the three primary CBs within the SIL ecosystem as exida, TUV Rheinland, and TUV SUD. These companies perform the vast majority of SIL certification evaluations. Next, the report provides details about how these CBs perform their evaluations. The report also explains that these CBs work together through the consensus standards working groups (e.g., IEC 61508) to continually improve the functional safety ecosystem in a cooperative manner.

The next section of Chapter 4 generally discusses the results of the CBs' evaluations and their impacts on the associated manufacturers. The report states:

> The SIL 3 certification process is rigorous enough that many products 'fail' a certification audit, at least the first time around (i.e., they do not achieve SIL 3 certification without needing some sort of design change). The most common type of design change needed is an improvement in diagnostic coverage. Superior diagnostics, along with the associated programming to ensure the equipment is placed in a safe state once the diagnostics detect a failure, drive the safe failure fraction up by converting dangerous undetected failures into safe detected failures. This is often necessary to satisfy the SIL 3 failure rate requirements, as well as the SIL 3 architectural constraints. [26]

> Another common barrier to successful certification is product development process deficiencies, particularly the IEC 61508 techniques and measures designed to minimize susceptibility to systematic failures involving both hardware and software. Based on results and observations from their certification process experiences, some equipment suppliers have revised their entire product development process to become IEC 61508 compliant.

The final certification specific topic covered in Chapter 4 is the long-term validity of a CB's certificate. This varies from 3 to 5 years, depending on the CB. The CBs dictate how long a manufacturer can fabricate and sell products under the current certificate before an update to the evaluation must be performed. The products that are purchased during the window of validity remain certified for the entirety of their useful life, as specified in the safety manual by the manufacturer. The certification of these purchased products does not end after the window of validity of the certificate expires.

The final section of Chapter 4 adds additional background and perspective on the certification process from countries and individual practitioners from the nuclear power industry that already have some experience with SIL certified equipment.

Chapter 5 covers the accreditation of the certification bodies. Accreditation is an important topic in the SIL ecosystem because it ensures the CBs are competent to perform the necessary evaluations of the manufacturers. The report explains that each country has their own AB, but the ABs are linked together by the International Accreditation Forum (IAF) Multi-Lateral Agreement (MLA). The report states that, "As part of the IAF MLA, accreditation bodies get peer-reviewed by other accreditation bodies." (p5-1) The report goes on to say:

> Accreditation is awarded when a certification body passes a detailed multi-day audit, where the certification body's (CB's) product certification program is assessed against the requirements of ISO/IEC 17065:2012, "Conformity assessment – Requirements for bodies certifying products, processes and services." As part of the accreditation process, CBs must demonstrate to the accreditation body that they carry out their activities with technical competence, in compliance with statutory and standards-based requirements, and at an internationally comparative standard. The accreditation body also assesses and monitors the management system and the competence of the certification bodies' assigned personnel. To certify that a programmable electronic product meets the requirements of IEC 61508, the certification body must have competency in:
>
> - software design procedures and software failure mechanisms
> - electronic hardware design procedures, electronic hardware failure mechanisms
> - hardware failure modes, effects and diagnostic analysis (FMEDA)
> - hardware probabilistic failure analysis: stress conditions and useful life
> - hardware and software testing procedures and methods
> - quality procedures, document control, and functional safety management [27] (p5-1)

The report then identifies that Deutsche Akkreditierungsstelle (DAkkS) is the AB for the TUV CBs in Germany, and that ANAB is the AB for exida in the USA. It also provides some details about ANAB's and DAkkS's processes and procedures.

Chapter 6 presents EPRI's analysis of field failure data. The intent of this analysis was to determine if SIL certified equipment performed at the level predicted by their certifications. Ultimately, EPRI was able to collect 12 data sets to analyze. The report provides the summary of these data sets as:

> In total, these 12 data sets represent 1,797,768,480 estimated operating hours, and there was a total of 205 actual reported failures, which corresponds to 323 estimated total failures. Except for the third logic solver, they all had estimated failure rates either less than or approximately equal to their predicted (i.e., FMEDA) failure rates. Several systematic failures contributed to the elevated failure rate of the third logic solver. They resulted from manufacturing process issues that were subsequently corrected by the OEM. The issue with lead-free solder was somewhat common years ago, but that manufacturing process is now well known and under control. (p6-14)

These results show that the estimated failure rates are conservative since 323 failures were expected but only 205 occurred. These results also illustrated how the probabilistic failure rates and the systematic integrity could both be evaluated through the review of field failure data. The investigation into the case where the failure rates were higher than expected became a mechanism to identify systematic issues and correct them.

Chapter 7 provided the final summary and conclusions. The first conclusion to highlight is, "The use of IEC 61508 certified equipment, in combination with application-specific functional and environmental qualification, can provide a significant improvement in dependability, as well as lower costs" (p7-1). The other conclusions drawn by the report were:

- The SIL certification process, especially for products developed to comply with SIL 3 requirements, takes a deep look into the product's hardware and software, as well as the project's functional safety management processes and documentation, to demonstrate the product's safety integrity for performing safety functions, specifically:
    - Hardware probabilistic failure analysis that may, in some cases, be validated with quality field failure data and analysis
    - Best practice techniques and measures used during HW and SW design/development to achieve systematic fault avoidance and fault tolerance, applied with varying levels of rigor as a function of SIL (Note: This item goes well beyond what is addressed in typical nuclear industry guidance documents, which mostly focus on process rather than best practice techniques and measures.)
    - Requirements tracing, testing, modification, user documentation, and manufacturing processes
    - OEM's functional safety management and quality management system documentation
- SIL certifications are valid for 3-5 years, depending on the Certifying Body, and can be renewed prior to expiration or when non-trivial product modifications are made.

- SIL Certifying Bodies are regularly accredited to accepted international standards that apply to a wide variety of certification schemes, including the SIL certification in accordance with IEC 61508.

- Based on field failure data from twelve SIL certified logic solvers (e.g., PLCs, process controllers), representing almost 1.8 billion operating hours, SIL certified products performed consistently with their predicted failure rates in all but a few cases. For those cases where systematic failures caused the estimated field failure rate to exceed the predicted failure rate, the systematic failures typically resulted from manufacturing process issues, and in no cases did they result from software faults (i.e., no instances of software CCF).

- SIL certifications are an accurate indicator of hardware and software safety reliability for programmable electronic equipment at the platform/product level. SIL certification efficacy at the integration and application level were not evaluated. (p7-1 to p7-2)

The final sentence of the last point, "SIL certification efficacy at the integration and application level were not evaluated," was simply clarifying that the methodologies used to implement SIL certified equipment into applications in other industries was not studied. Since the intent of the nuclear industry is to interweave the SIL certification ecosystem into the existing nuclear integration and application processes (e.g., commercial grade dedication and qualification), this aspect of the research was not important to this effort.

The balance of the report includes:

- Chapter 8- Definitions and Acronyms
- Chapter 9- References
- Appendix A- Summary of IEC 61508:2010, Edition 2.0 Changes
- Appendix B- Programable Electronic System Product Development Process Requirements
- Appendix C- Programmable Electronic Systems Certified to IEC 61508
- Appendix D- Sample Quotation for the Assessment of a PLC Based on IEC 61508:2010 SIL 3
- Appendix E- DAkkS Accreditation Assessment Checklist
- Appendix F- Field Failure Data Collection, Statistical Analysis, and Presentation Strategies

These additional two chapters and six appendices are intended to be referenced while utilizing Chapters 1 through 7.

3.3 Conclusion from EPRI Research

The key takeaway from the EPRI research is that the technical content of a SIL certification encompasses the technical content of a commercial grade dedication, as it pertains to the dependability critical

characteristics. This is most clearly demonstrated in p4-8 to 4-9 of Reference 8 where the safety case is compared to the dependability attributes addressed in EPRI TR-106439.

The conclusion regarding the technical content is the critical point of focus for the approach to commercial grade dedication laid out in this guidance. There are potentially some conclusions to be drawn concerning the quality assurance aspects of the manufacturer's process, but those are not being pursued as a part of this guidance document. This guidance document later addresses the quality aspects of the CB as an overseer of the manufacturer.

4 ACCEPTANCE OF COMMERCIAL GRADE, SIL CERTIFIED, DIGITAL EQUIPMENT FOR NUCLEAR SAFETY APPLICATIONS

4.1 Application of the SIL Certification Process

The approach provided in this document for performing commercial grade dedication of digital equipment is based on the correlation between SIL requirements and the dependability critical characteristics (CCs) defined by EPRI TR-106439 as demonstrated by the Supplemental Accreditation Checklist (Appendix D). The basis for Supplemental Accreditation Checklist is included in Appendix C. Implementation of this demonstrated correlation is that SIL certifications can be used as the evidence of acceptability of dependability CCs, as defined by EPRI 106439. In this process, the traditional activity of a CDR and the traditional use of Methods 2 & 4 to determine the acceptability of dependability CCs are replaced by a SIL certification that meets all the criteria laid out in this guidance. Since SIL certifications are issued by CBs that do not operate under a 10 CFR 50, Appendix B QA program, additional measures are involved to dedicate the service being provided by the CB producing the SIL certification. This approach also involves measures for the U.S. NRC Licensees or their designees to provide oversight of the SIL certified equipment ecosystem. The approach is illustrated in Figure 4.1.

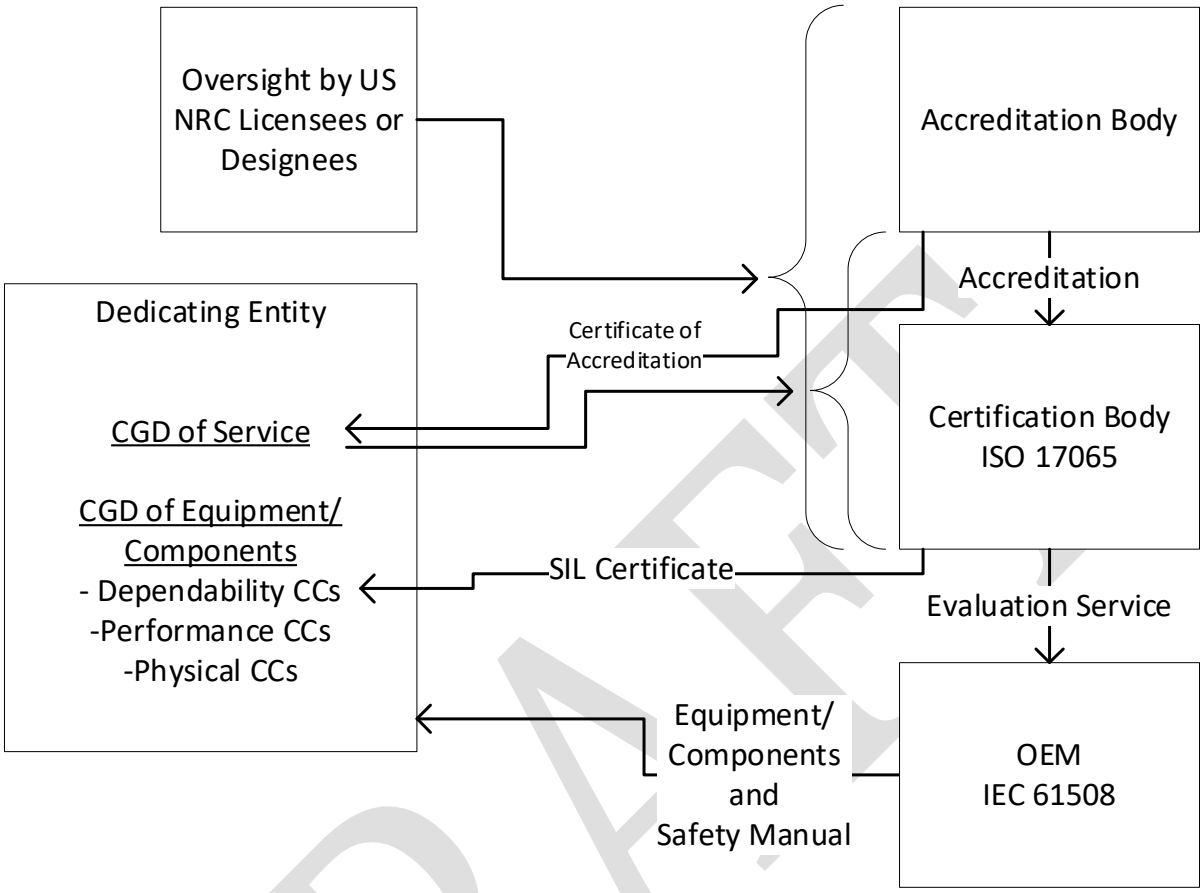

Figure 4.1- The CGD process for Digital Equipment with an Accredited SIL Certification

The steps to this approach are as follows:

1. Identify the requirements of the end user's application (see Section 4.2 for more details).

2. Identify SIL certified equipment, and review the SIL certification and the manufacturer's safety manual to confirm they encompass the requirements of the application (see Section 4.3 for more details).

3. Perform a technical evaluation of the equipment to identify physical, performance, and dependability critical characteristics according to EPRI 3002002982, EPRI TR-106439, and Section 4.4 of this document.

4. Perform a technical evaluation of the CB's service of evaluating manufacturer's equipment and issuing the appropriate SIL certificate. This evaluation identifies the critical characteristics of the service, in accordance with the guidance in EPRI 3002002982, so that the service can be dedicated as nuclear grade.

5. Review the CB's certificate of accreditation to confirm that IEC 61508 certifications are within the CB's scope.

6. Use the CB's certificate of accreditation and the supplemental U.S. nuclear industry evaluation (see Chapter 5 for more details) to complete the CGD of the service similarly to how accreditations to ISO 17025 are used in NEI 14-05.

7. Use the SIL certification to complete the determination of acceptability of the dependability CCs of the item CGD (see Section 4.4 for more details).

8. Use traditional methods to determine acceptability of the physical and performance CCs.

At this point the commercial grade dedication process would be complete, and all traditional processes and procedures would be followed to maintain the equipment as nuclear grade (i.e., a basic component). Looking at this approach from a high level, there are no significant changes to the CGD process, but this approach yields significant efficiency gains for the commercial grade dedicator by replacing the need for a CDR and by replacing the use of the CGS acceptance method.

4.2 Determination of SIL for End User's Application

To complete step 1 of the approach laid out in Section 4.1, establish the safety function and the required SIL systematic capability level for the end user's application. These aspects may be established for a generic use case to cover a range of end user's applications. The required SIL systematic capability level shall be based upon the safety significance of the safety function using a risk-based approach that addresses both consequence and probability of failure aligning with the SIL probability criteria. A risk-informed method is suggested to establish the SIL systematic capability level requirement. The design would quantify the required risk factor reduction needed for the specific safety function such as using existing PRA results and then select the SIL digital components/systems that would meet the requirement to maintain or improve the PRA results. This selection would utilize the SIL failure thresholds for the risk reduction needed (see Figure 4.2) and the frequency of demand (high or low). The EPRI HAZCADS process is one example of how this risk-informed approach can be implemented (Reference 23).

Safety Integrity Level	Risk Reduction Factor	Probability of Failure on Demand
SIL 4	100,000 to 10,000	10^{-5} to 10^{-4}
SIL 3	10,000 to 1,000	10^{-4} to 10^{-3}
SIL 2	1,000 to 100	10^{-3} to 10^{-2}
SIL 1	100 to 10	10^{-2} to 10^{-1}

Figure 4.2- SIL Failure Thresholds for Low Demand (Based on Reference 9)

4.3 Selection of SIL Certified Equipment

To complete step 2 of the approach laid out in Section 4.1, equipment must be selected that meets the functional requirements of the application, must be certified for a safety function that encompasses the safety function of the application, and must be certified to meet or exceed the SIL systematic capability that has been established for the application (as described in Section 4.2). After potential equipment has been identified that meets the functional requirements of the application, these steps shall be followed:

1. Obtain the equipment's SIL certificate and the safety manual. Refer to Appendix A of this document to review example certificates.

2. Review the certificate and confirm, through the CB, the validity of the certification.

3. Confirm that the certification is to IEC 61508.

4. Confirm that the certified SIL systematic capability meets or exceeds the SIL determined to be appropriate for the application.

5. Confirm that the CB is accredited by an organization that is a signatory to the IAF.

6. Confirm that the safety function identified on the certificate and/or in the safety manual encompasses the scope of the safety function of the intended application.

It is common for the certified safety function to exclude some of the functionality of the equipment. For example, the second SIL certificate included in Appendix B of this document is for a differential pressure gauge with a built-in setpoint switching function. When the safety manual for this device is reviewed it becomes clear that the indication of the gauge is not covered by the SIL certification. The SIL certification only applies to the switching function. Here is the excerpt from the manual:

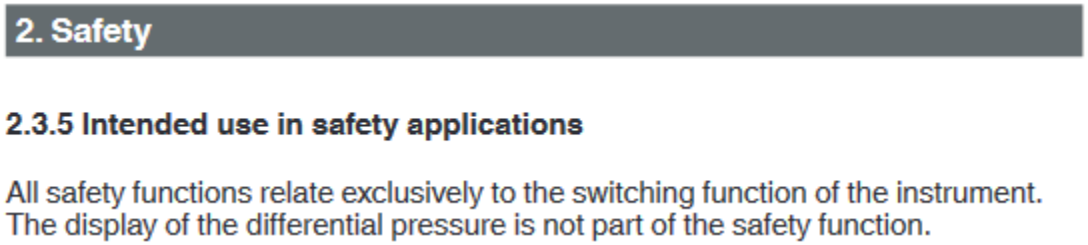

Figure 4.3- Safety Function Excerpt (Section 2.3.5) from Reference 22

If the safety function of the intended application included the gauge indication, then the SIL certification could not be credited to satisfy the dependability critical characteristics during the commercial grade dedication.

4.4 Technical Evaluation & Acceptance Method

Concerning steps 3 and 7 of Section 4.1 of this document, Table 4-1 of EPRI TR-106439 provides an example of CCs, acceptance criteria, and verification methods that can be used in a commercial grade dedication of digital equipment. This table sorts the CCs into the categories of physical, performance, and dependability. The CCs in the dependability category are the focus of this section. These

dependability CCs are typically evaluated for acceptability using commercial grade surveys (EPRI method 2) supported by CDRs and reviewing operating history (EPRI method 4). Table 4-4 of this document extracts the dependability category of the table from EPRI TR-106439 and identifies how the SIL certification process (column 4 in Table 4-4) evaluates these dependability CCs for acceptability in lieu of a commercial grade survey (column 3 of Table 4-4). The resulting process is illustrated in Figure 4.4. Note that EPRI methods 2, 3, or 4 could be used as the verification approach to any of the remaining physical or performance (non-dependability) CCs, but it is common industry practice to verify those CCs using EPRI method 1. Figure 4.4 is structured with this common practice in mind.

Table 4.4- Dependability Critical Characteristics Matrix

The first three columns are from Table 4-1 of EPRI TR-106439. The fourth column is the methodology of the SIL certification by an accredited CB.

EPRI TR-106439 CCs for Acceptance	**EPRI TR-106439 Acceptance Criteria**	**EPRI TR-106439 Methods of Verification**	**SIL Certification Process Method of Verification**
<u>Dependability</u> Reliability and maintainability related to the required functionality	Criteria for reliability, availability and maintainability should be derived from the requirements of the intended application(s). Specific criteria may be established such as numerical criteria for reliability or availability of required functions, or maintainability criteria including software. If numerical criteria are used, the method of demonstration should be specified (e.g., hardware reliability prediction using classical methods, or statistical analysis of failure rate data from field experience).	Reliability: Review vendor reliability calculation/testing methods and results. Review operating history data. Review and assess design. Perform reliability analysis. *(Method* 2)	<u>Reliability</u> Numerical criteria are established by IEC 61508 in terms of PFH and PFD_{avg}. See IEC 61508-2 Section 7.4.5
Built-in quality including: • Quality of design • Quality of manufacture • Failure management • Compatibility with human operators, maintainers Configuration control and traceability of:	Basic criterion for built-in quality is equivalence to the quality of a device developed and applied under a 10 CFR 50, Appendix B program. Judgment of equivalent quality is based on a combination of: • Design and design review processes, including software life cycle, V&V, etc. • Design documentation • Configuration management • QA program and practices • Software requirements definition and requirements traceability	Review of vendor processes and documentation *(Method 2 or 3):* • Design, development and verification processes • Quality assurance program and practices • V&V program and practices Design reviews --architecture review, code reviews, walkthroughs, use of analytical techniques, etc. *(Method* 2 *"& CDR" **text in quotes added**)* Failure analysis, at the system level and of the commercial grade item	<u>Built-in Quality</u> • The IEC Safety Lifecycle (includes configuration management) as detailed in IEC 61508-2 Section 7.4.6 and IEC 61508-3 Section 7.4. • CB's review process including the safety case, see IEC 61508-2 Section 7.4.6, IEC 61508-3 Section 7.4 and ISO 17065 Section 7. • AB's review process, see ISO 17065 Section 7. • Self-diagnostics to detect dangerous failures and force the equipment to

EPRI TR-106439 CCs for Acceptance	EPRI TR-106439 Acceptance Criteria	EPRI TR-106439 Methods of Verification	SIL Certification Process Method of Verification
• Hardware • Software • Firmware (aspects of both hardware and software configuration control) • Problem reporting	• Consideration of failure modes and ACEs in design and verification • Qualifications and experience of personnel involved in design and verification activities • Product operating history • Testing by the vendor or dedicator Minimum criterion for configuration control and traceability is that these be sufficient to support use of operating history data and to ensure the item delivered can be traced back to the documents reviewed as part of acceptance. Additional criteria may apply if the dedicator wishes to procure more of the same item in the future. As a minimum, problem reporting must be sufficient to support use of product operating history and to allow dedicator to carry out 10 CFR 21 responsibilities. Specific criteria should be established (e.g., on coverage, timeliness, reporting to the right organization or department).	itself Comparison of device's failure modes to needs of the application Review of product operating history (from vendor, users, user groups, industry reports, INPO, etc.) *(Method 4*): • Documented (records, traceable) • Sufficient (units, years in service) • Successful (error tracking shows good performance and device including software is stable) • Relevant (same or similar hardware/software configuration, functions used, operated similarly, etc.) Configuration control: review vendor configuration management program and practices. Examine actual practices, records. *(Method 2 or 3)* Problem reporting: review vendor procedures and practices. Assess performance record with previous customers *(Method 2).* Enter into contractual agreement. Assess maintainability of dedication.	a safe state. See IEC 61508-2 Sections 7.4.7- 7.4.8. • Defect reporting, see IEC 61508-2, Section 7.8.2.2. • SIL Certification Aging, see ISO 17065 Section 7.7. <u>Operating History</u> Field failure data informs the reliability determination (PFH or PFD_{avg}), see IEC 61508-1, Section 6.2.6

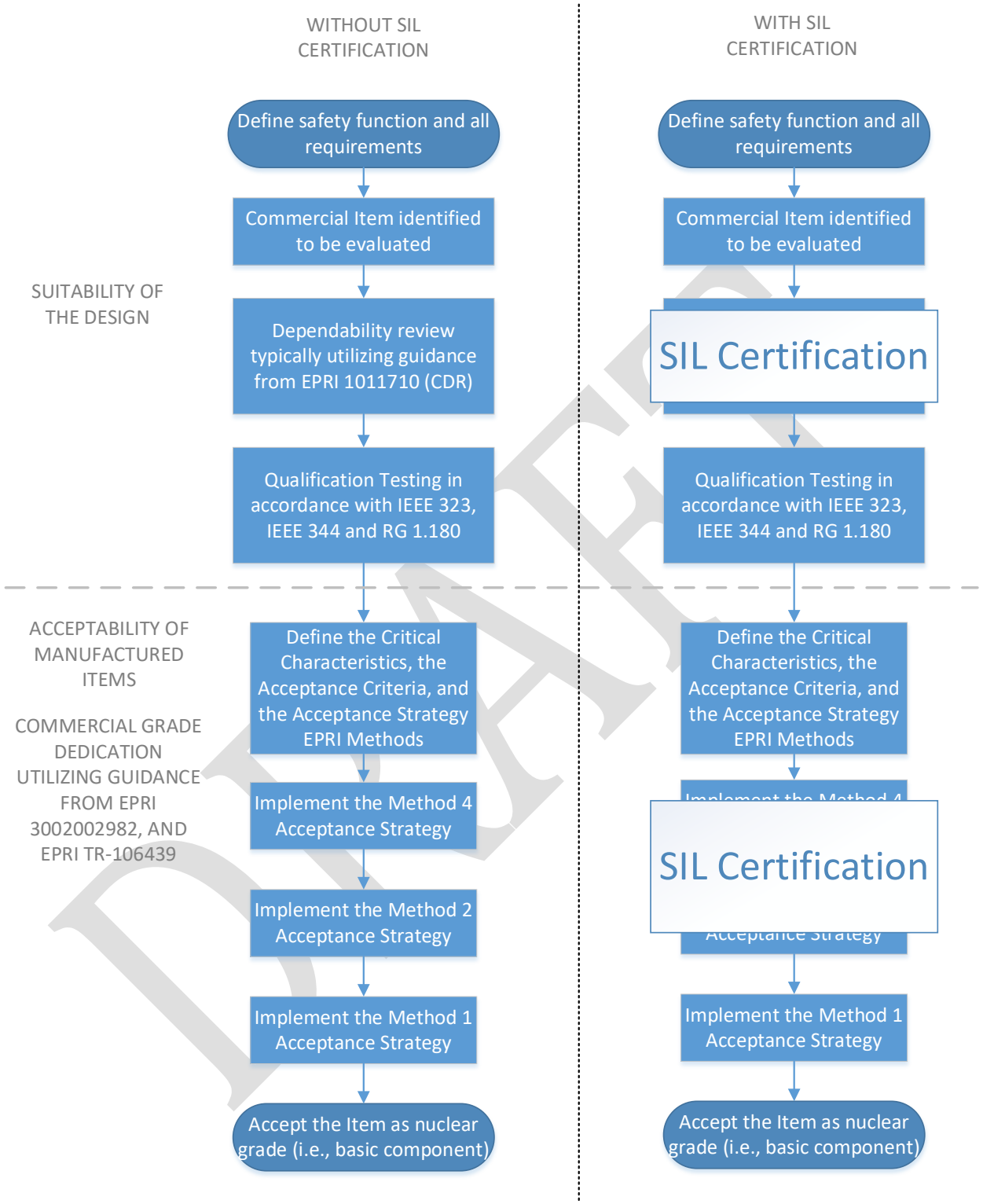

Figure 4.4- Commercial Grade Dedication and Qualification Process with and without SIL Certification

5 NEI EVALUATION OF THE ACCREDITATION PROCESS

5.1 Description of Evaluation

To build on the results EPRI reported (Reference 8), further investigation was performed on the details of the accreditation process. Accreditation is an important aspect of the SIL ecosystem since it is how the CBs are determined to be competent to perform the evaluations of the manufacturers' products. The AB is essentially the entity that checks the checkers and having confidence in their process is critical to maintaining confidence in the entire ecosystem.

As described in Section 4.1, the methodology for being able to utilize SIL certifications is to perform a CGD of the service provide by the CB. With this approach in mind, a comparison was performed of a CGS and of an AB's 17065 accreditation activity to identify the similarities. This comparison began with a technical evaluation of the CB's service to identify the CCs and acceptance criteria. The CCs provided the basis for the scope of what the CGS would cover. A CGS checklist was then assembled using the identified CCs and a NUPIC audit checklist (based on 10 CFR 50, Appendix B). The CGS checklist consisted of the sections of the NUPIC checklist that related to the identified CCs. This tailored NUPIC checklist was then compared to the accreditation requirements of ISO 17065 to identify if there were any potential gaps. The overall idea of this comparison was that if the ISO 17065 accreditation scope encompassed the CGS scope then the ISO 17065 accreditation would be a valid approach to dedicating the CB's service. See Appendix B for the complete comparison.

5.2 Result of CGS and Accreditation Comparison

There were many areas of similarity between these two scopes, and significant benefits were observed for a CB being accredited to ISO 17065. The following topics were covered in both scopes:

- Contract Management
- Document Control and Records Management
- Product Configuration Management
- Personnel Competency
- Management of Impartiality
- Non-conformances
- Corrective Actions
- Self-assessments (internal audits)
- Surveillance of Certifications
- Complaint and Appeal Management
- Reporting Requirements

As described in the conclusion in Appendix B, only one potential gap was identified, and it was related to the topic of design control (Section 2) from the CGS checklist. In reviewing ISO 17065 it was unclear how the AB would confirm that the CB's scheme complied with IEC 61508. Section 7.1.1 of ISO 17065 states, "The certification body shall operate one or more certification scheme(s) covering its certification activities," and Section 7.1.2 of ISO 17065 states, "Evaluation requirements of products shall be contained in specified standards." These two requirements are what link the accreditation process to IEC 61508. ISO 17065 is an adequate source of requirements to address the QA aspects of the CB's service, but IEC 61508 is the primary source for the technical requirements that would address this design control aspect.

Based on this comparison of requirements, additional information was needed to be able to further evaluate the potential gap. It was concluded that observing the AB's activities during an accreditation activity was necessary to understand the level of rigor applied to confirming the requirements of Sections 7.1.1 and 7.1.2 of ISO 17065. If the AB demonstrated a sufficient level of rigor to confirm that the CB's scheme did comply with IEC 61508 then there would not be a gap, but if the level of rigor was observed to be lacking then a compensating measure would be needed to be able to complete the CGD of the CB's service.

5.3 Paths to Accepting CB Services

Based on the comparison described in the previous section, there are two paths to being able to complete the CGD of the CB's services. One path is via "Accreditation Only", and the other path is via "Accreditation Plus Scheme Evaluation".

The "Accreditation Only" path involves the following elements for the AB responsible for the accreditation of the CB whose services are being commercially dedicated:

1. A U.S. NRC licensee, their designee, or the dedicating entity must confirm that the AB is a Signatory of the IAF MLA.

2. A U.S. NRC licensee, their designee, or the dedicating entity performs an observation of the AB as they conduct an ISO 17065 accreditation assessment of a CB. The following characteristics must be satisfactorily observed:

    a. The AB's assessors must be knowledgeable of and have experience with ISO 17065.

    b. The AB's assessment must be of a level of rigor that provides confidence in the conclusions about the CB's compliance with ISO 17065.

        5.3.1.1.1

3. A U.S. NRC licensee, their designee, or the dedicating entity performs an observation of the AB as they conduct an assessment of a CB's scheme against the requirements of IEC 61508. The following characteristics must be satisfactorily observed:

    a. The AB's assessors must be knowledgeable of and have experience with IEC 61508.

    b. The AB's assessment must be of a level of rigor that provides confidence in the conclusions about the CB's compliance with IEC 61508.

4. A U.S. NRC licensee, their designee, or the dedicating entity performs an observation or evaluation of the AB to confirm that they implement adequate measures to manage the accreditation of CBs over a periodic timeframe.

The “Accreditation Plus Scheme Evaluation” path involves the following elements for the AB responsible for the accreditation of the CB whose services are being commercially dedicated:

1. A U.S. NRC licensee, their designee, or the dedicating entity must confirm that the AB is a Signatory of the IAF MLA.

2. A U.S. NRC licensee, their designee, or the dedicating entity performs an observation of the AB as they conduct an ISO 17065 accreditation assessment of a CB. The following characteristics must be satisfactorily observed:

    a. The AB's assessors must be knowledgeable of and have experience with ISO 17065.

    b. The AB's assessment must be of a level of rigor that provides confidence in the conclusions about the CB's compliance with ISO 17065.

3. A U.S. NRC licensee, their designee, or the dedicating entity performs an observation or evaluation of the AB to confirm that they implement adequate measures to manage the accreditation of CBs over a periodic timeframe.

4. A U.S. NRC licensee, their designee, or the dedicating entity interacts with the CB to complete the supplemental accreditation checklist (included in Appendix D) to confirm that the CB’s scheme meets the relevant requirements of IEC 61508.

Three years after the initial observations were performed, these assessments (for accreditation and for scheme evaluation) would be reperformed. The three-year time frame was chosen to be consistent with U.S. 10 CFR 50 App B auditing and commercial grade surveying U.S NRC accepted practices.

5.4 Description of Observation

To investigate the potential gap discussed in section 5.2 and to demonstrate the paths described in section 5.3, an observation was planned of ANAB as they performed an assessment of exida (a U.S.-based CB). An observation checklist was prepared to guide the NEI observers during this observation. This checklist highlighted the requirements of IEC 61508 that aligned most with the dependability CCs in Table 4-1 of EPRI TR-106439. This resulted in the checklist also aligning with Table 4.4 of this document. See Appendix C for more details for the basis of this checklist. IEC 61508 is a large standard that contains many requirements, so structuring this checklist as it has been described allowed the NEI observers to focus in on the most important aspects when confirming compliance of the CB’s scheme.

5.5 Results of Observation

In November 2020, NEI and NRC personnel participated in the planned observation. The observation of ANAB yielded confirmation of the benefits identified in Section 5.2 of this document. The ANAB assessors thoroughly confirmed exida was operating in compliance with ISO 17065, but a concern regarding the level of rigor applied to Section 7.1.2 of ISO 17065 was noted. It was the perspective of the NEI and NRC observers that the ANAB technical assessor responsible for assessing Section 7.1.2 of ISO

17065 did not demonstrate a sufficient understanding of IEC 61508, and therefore, was not able to sufficiently assess exida's scheme for compliance. The NEI observers were not able to complete their checklist during the observation.

While much of the ANAB assessment was viewed as a valuable activity, the concern of the ANAB technical assessor confirmed that the "Accreditation Only" path described in section 5.3 was not going to be able to be used, and that the "Accreditation Plus Scheme Evaluation" path would be required.

During the observation it was also confirmed that after the initial accreditation, ANAB operates on a two-year accreditation cycle, and also performs a surveillance of the CB on the off year. It is ANAB's general practice to perform either a re-certification activity or a surveillance activity once every year for every CB ANAB accredits.

5.6 Initial Use of the Supplemental Accreditation Checklist

Preliminary discussions with ANAB indicated they desire to address the observed deficiencies, but until that effort reaches a satisfactory conclusion, the "Accreditation Plus Scheme Evaluation" path will be used.

To enable the implementation of the guidance of this document, an assessment of exida was performed by the NEI MP3 working group (acting as a designee of the U.S. NRC licensees), using the Supplemental Accreditation Checklist (Appendix D). This assessment utilized information about exida that had been compiled into Reference 8, and information collected through interviews of exida personnel. The supplemental accreditation checklist used to document this assessment is included in Appendix E. Based on the supplemental assessment, exida is considered an acceptable CB for use, within the structure of the guidance of the "Accreditation Plus Scheme Evaluation" path.

6 DEDICATING ENTITY'S QUALITY ASSURANCE PROGRAM

Dedicating entities that rely on the accredited IEC 61508 SIL certification process for the dependability critical characteristics (CC) in lieu of commercial grade surveys are required to document this method in their 10 CFR 50, Appendix B QA program. Prior to a licensee implementing this methodology, the U.S. NRC requires a licensee to submit a revision to its Operating Quality Assurance Program (OQAP) for NRC acceptance in accordance with 10 CFR 50.54(a)(4) since implementation of this methodology represents a reduction in commitment.

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 10 CFR 50, Appendix B dedicating entity shall ensure certification and accreditation as described in Section 4.1 of this guidance and will impose any additional technical or quality program requirements, as necessary, to meet regulatory requirements and the licensee's QA program commitments (end user).

6.1 Organization

Commercial Grade Dedication of the digital equipment shall be performed by a "dedicating entity" that has a 10 CFR 50, Appendix B QA program. The "dedicating entity" may be the licensee, a third-party dedicator, or even the manufacturer. This section addresses how the IEC 61508 SIL certification process will be integrated into that Appendix B program.

The dedicating entity retains overall responsibility for assuring that purchased digital devices meet applicable technical and regulatory requirements and that reasonable assurance of quality exists. There are no special requirements beyond 10 CFR Part 50, Appendix B and 10 CFR Part 21.

6.2 Procurement Document Control

When purchasing equipment using the method described in this guidance, the procurement documents will impose requirements to satisfy the dedicating entity's QA program and technical requirements.

These shall be included as a minimum:

1. The equipment must be certified to the IEC 61508 SIL that is required by the application, or to a higher SIL.

2. The scope of the SIL certification must encompass the scope of the safety function required by the application (include a version of the required safety function that is just specific enough to allow the manufacturer to confirm it can be performed by their equipment).

3. The SIL certification must be issued by a CB that is accredited to IEC 17065 and has IEC 61508 within its scope of accreditation.

4. The AB must be a signatory to the International Accreditation Forum (IAF).

5. The IEC 61508 SIL certificate and safety manual must be deliverables to the purchasing organization.

6. Clause 7.8.2.2 of IEC 61508 must be imposed. This will require notification of any condition that impacts safety, and this notification will support the dedicating entity's Part 21 reporting responsibility.

6.3 Tasks Associated with Digital Dependability Evidence

For the digital dependability critical characteristics, the dedicating entity can take credit for the IEC 61508 SIL certification and accreditation processes. The dedicating entity using the IEC 61508 SIL certification process for the dependability CCs will be responsible for:

1. Ensuring that all deliverables defined in Section 6.2 have been received from the equipment manufacturer.

2. Reviewing the CB's certificate and ensuring the equipment meets or exceeds the required IEC 61508 SIL.

3. Ensuring the certificate is not expired or otherwise invalidated. It may be necessary to contact the CB directly or to utilize the CB's certification database (typically accessible via the CB's website) to confirm this. The accreditation must also be supported by the appropriate compensating measure identified in Section 5.5.

4. Reviewing the CB's certificate and/or the manufacturer's safety manual and confirming that the certified safety function encompasses the application's safety function.

5. Confirming that the CB's scheme and/or safety case has been verified to satisfy the criteria of the supplemental accreditation checklist (Appendix D) included in this document.

6. Reviewing the AB's certificate of accreditation. This review must confirm that the CB is accredited to ISO 17065 and that IEC 61508 is in the CB's scope of accreditation.

7. Confirm that the AB is a signatory of the IAF.

6.4 QA Evidence for Digital Dependability

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

1. The manufacturer's safety manual

2. The CB's IEC 61508 SIL certificate for the subject equipment

3. The AB's certificate of accreditation for the subject CB

4. Documentation of the CB's scheme being confirmed to satisfy the criteria of the supplemental accreditation checklist (Appendix D), or documentation of successful completion of the long-term compensating measure path, described in Section 5.5

5. Documentation of the dedicating entity completing the responsibilities listed in Section 6.3

Note that physical and performance CCs will be assessed using the traditional commercial grade dedication methods.

6.5 Corrective Action

1. The dedicating entity shall have a Corrective Action program and assume 10 CFR Part 21 responsibility.

2. The dedicating entity is required to notify the NRC of defects and failures of dedicated items which could result in substantial safety hazards as required by 10 CFR Part 21.

3. For the identification of component problems, the dedicating entity shall have a contractual relationship with the manufacturer in place to ensure notification of errors is obtained. This aligns with requirement 6 in Section 6.2.

7 U.S. NRC LICENSEE OVERSIGHT OF THE SIL CERTIFICATION PROCESS

The objective of the oversight of the IEC 61508 SIL Certification Process by the U.S. NRC Licensees (or their designee) is to confirm that the process continues to cover the EPRI TR 106439 Dependability Critical Characteristics and is implemented consistently for all manufacturer equipment evaluations. This ensures the process can be used as described in Chapter 4. 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.

7.1 Organization

U.S. NRC Licensees, and their designees are responsible for the industry oversight of the IEC 61508 SIL certification process as it relates to industry's use of the process as part of commercial grade dedication.

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

The assessments and conclusions of the consistency of the IEC 61508 SIL certification process documented herein include the evaluation of any future changes to the 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, a nuclear industry team, through NEI, will monitor the 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 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, the nuclear industry team will evaluate whether the potential changes impact the 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 IEC 61508 SIL certification requirements before they are implemented, and thus provide the U.S. 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.

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

7.3 Verification that Implementation of the 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 IEC 61508 SIL certification process documented herein are based in part on the direct observations of the performance of accreditation bodies (e.g., ANAB and DAkkS) for SIL certification. These evaluations are performed to verify the accreditation process continues to be consistently applied.

U.S. NRC Licensees, or their designees will observe ABs that accredit IEC 61508 SIL CBs to ensure that the IEC 61508 SIL certification process continues to be implemented consistently. These observations will be like what was described in Section 5.3 and will be used to continue to evaluate the implementation of compensating measures identified in Section 5.5. The 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 be an observer for these observations.

APPENDIX A. EXAMPLE SIL CERTIFICATES

https://www.exida.com/2019/EMM_18-01-017_C001_R1.1_61508_Certificate_-_4200.pdf

The manufacturer may use the mark:

Revision 1.1 July 22, 2019
Surveillance Audit Due
August 1, 2022

ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

Certificate / Certificat
Zertifikat / 合格証

EMM 1801017 C001

exida hereby confirms that the:

4200 Coriolis Flowmeter

Micro Motion, Inc.
Emerson
Boulder, CO USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:
The 4200 Coriolis Flowmeter provides direct, high accuracy, mass flow measurement for liquids, gases or slurries and transmits a proportional signal within its safety accuracy.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

John C Yozallinas
Evaluating Assessor

Steven H Close
Certifying Assessor

Page 1 of 2

4200 Coriolis Flowmeter

Certificate / Certificat / Zertifikat / 合格証

EMM 1801017 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Systematic Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This element meets *exida* criteria for Route 2_H.

IEC 61508 Failure Rates in FIT*

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
4200 Flowmeter	0	152	2130	76

* FIT = 1 failure / 10^9 hours

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: EMM 18-01-017 R002 V1R2 (or later)

Safety Manual: 4200SIS_ENG_20049802A, Rev A or later

80 N Main St
Sellersville, PA 18960

T-002, V5R3

https://www.certipedia.com/fs-products/files/certificates/certificates_asi/2015/V/V_495_01_15/V_495_01_15_de_en_el.pdf

Certificate

Nr./No.: V 495.01/15

Prüfgegenstand **Product tested**	Differenzdruckmessgerät und -wächter Differential pressure gauge and monitor	**Zertifikats-inhaber** **Certificate holder**	WIKA Alexander Wiegand SE & Co. KG Alexander-Wiegand-Str. 30 63911 Klingenberg Germany
Typbezeichnung **Type designation**	DELTA-comb DPGS40TA.100-XXS		
Prüfgrundlagen **Codes and standards**	IEC 61508 Parts 1-2 and 4-7:2010 IEC 61511 Parts 1-3:2004		EN ISO 13849-1:2008 + AC:2009 EN 13611:2007+A2:2011 (in extracts)
Bestimmungsgemäße Verwendung **Intended application**	Erfassung und Überwachung eines Differenzdruckes. Zur Verwendung in sicherheitsgerichteten Systemen nach IEC 61508 und IEC 61511 bis SIL 2 und nach EN ISO 13849-1 bis PL d bei Verwendung beider Ausgangskanäle, wenn eine externe Diagnose (DC low) in der nachgeschalteten Einheit realisiert wird. In einer redundanten Gerätekonfiguration (HFT=1) können sie bis SIL 3 eingesetzt werden. Measuring and monitoring of differential pressure. For use in safety-related systems acc. to IEC 61508 and IEC 61511 up to SIL 2 and acc. to EN ISO 13849-1 up to PL d, if both output channels are used and monitored (DC low) by the down-stream safety device. In a redundant device configuration (HFT=1) they may be used up to SIL 3.		
Besondere Bedingungen **Specific requirements**	Die Hinweise in der zugehörigen Installations- und Betriebsanleitung sind zu beachten. The instructions of the associated Installation and Operating Manual must be considered.		

Zusammenfassung der Testergebnisse siehe Seite 2 des Zertifikates.
Summary of test results see page 2 of this certificate.

Gültig bis / Valid until 2020-11-23

Der Ausstellung dieses Zertifikates liegt eine Prüfung zugrunde, deren Ergebnisse im Bericht Nr. V 495.01/15 vom 23.11.2015 dokumentiert sind.
Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen. Es wird ungültig bei jeglicher Änderung der Prüfgrundlagen für den angegebenen Verwendungszweck.
The issue of this certificate is based upon an examination, whose results are documented in Report No. V 495.01/15 dated 2015-11-23.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2015-11-23

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Stephan Häb

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

Manufacturer: WIKA SE & Co. KG
Alexander Wiegand SE & Co. KG
63911 Klingenberg, Germany

Product tested: DELTA-comp DPGS40TA.100-XXS

Device-Specific Values[1]

Confidence Level	1-α	95 %
Safe Failure Fraction (see note)	SFF (2)	73,9 %
Hardware Fault Tolerance	HFT	0
Diagnostic Coverage	DC	0 %
Common Cause Factor	β_{int} (3)	10 %
Type of Sub System		Type A
Mode of Operation		Low and High Demand

(1): The stated values are only valid for usage in idle current principle
(2): The Safe Failure Fraction (SFF) was estimated by an alternative method with a FMEA according to EN 161:2011/A3:2013.
(3): The Common Cause Factor is always to be examined taking into consideration the safety-related overall system with regard to the certain application.

Low Demand Mode[4] **(derived Values for 1oo1-Architecture)**

Assumed Demands per Year	n_{op}	1 / a	1,14 E-04 / h
Total Failure Rate	$\lambda_S + \lambda_D$	3,97 E-08 / h	40 FIT
Lambda Dangerous Detected	λ_{DD}	0,00 E+00 / h	0 FIT
Lambda Dangerous Undetected	λ_{DU}	1,04 E-08 / h	10 FIT
Lambda Safe	λ_S	2,93 E-08 / h	29 FIT
Recommended Test Interval	Ti	1 / a	1,14 E-04 / h
Average Probability of Failure on Demand	PFD_{avg}	4,54 E-05	
Mean Time to Dangerous Failure	$MTTF_D$	9,65 E+07 h	11.016 a

High Demand Mode[4] **(derived Values for 1oo2-Architecture)**

B_{10d} value	B_{10D}	259.835	
Assumed Demands per Year	n_{op}	2190 / a	2,50 E-01 / h
Lambda Dangerous Undetected	λ_{DU}	9,62 E-08 / h	
Average Frequency of dangerous Failure per Hour	PFH	9,62 E-08	
Mean Time to Dangerous Failure	$MTTF_D$	1,04 E+07 h	1.186 a

(4): The suitability for certain applications can only be realised through the evaluation of the respective safety-related overall system including all safety-related components and the calculation of the application oriented PFH_D, $MTTF_D$ and λ_D value.
PFH_D, $MTTF_D$ and λ_D depend on frequency of demand n_{op} of the safety-related overall systems and will be calculated according the following equation.

$$PFH = \lambda_D = \frac{1}{MTTF_D} = \frac{0.1}{B_{10D}} \cdot n_{op}$$

Time of Usage

A time of usage of more than 5 years (+ 1.5 years of storage) can only be favored under responsibility of the operator, consideration of specific external conditions (securing of required quality of media, max. temperature, time of impact), and adequate test cycles. Further, the maximum cycle lifetime is limited to the B10d value of the test item.

APPENDIX B. COMPARISON OF AN ISO 17065 ACCREDITATION TO A COMMERCIAL GRADE DEDICATION, (IN THE CONTEXT OF THE CRITICAL CHARACTERISTICS OF THE SERVICE PROVIDED BY THE CERTIFYING BODY)

Introduction

The traditional approach to taking credit for a commercial grade service is to perform a commercial grade dedication (CGD). The typical acceptance method used to perform this type of CGD is a commercial grade survey (CGS). This document evaluates the ISO 17065 accreditation process as a replacement to that traditional approach. The context of this evaluation/comparison is the service being provided by an IEC 61508 functional safety certifying body (CB).

Summary of Process

The comparison process used in this document is to develop a CGS checklist and then compare it to ISO 17065 accreditation. To develop the CGS checklist, the following steps are used: identify the safety function, perform a technical evaluation to identify the critical characteristics (CCs), and then identify the applicable audit sections of the Nuclear Procurement Issues Corporation (NUPIC) audit checklist. A commercial grade survey is typically performed using a tailored 10 CFR 50, Appendix B checklist. The checklist is trimmed down to specifically address the identified critical characteristics. The NUPIC checklist encompasses the requirements of 10 CFR 50, Appendix B and is therefore an acceptable starting point. To complete this process, this tailored NUPIC checklist is then compared to the accreditation requirements of ISO 17065.

CGS Checklist Development

Safety Function: Evaluate the safety case for specific equipment to determine if an adequate level of safety integrity exists.

Technical Evaluation:

Failure Mode	Effect	Critical Characteristic	Acceptance Criteria
Personnel are not qualified to perform the work.	Conclusions of the evaluations will likely be inaccurate.	1. Personnel qualification	Documented evidence exists to confirm qualification of personnel.
Outsourced evaluations are not conducted by an entity that is qualified to perform the work.	Conclusions of the evaluations will likely be inaccurate.	2. Outsourced entity qualification	Documented evidence exists to confirm qualification of entity performing evaluations.
Standards, procedures, and/or schemes used as the basis for evaluation requirements are not correct.	Conclusions of the evaluations will likely be invalid.	3. Standards, procedures, and/or **schemes** validity	Basis documents are appropriate for the evaluation being performed.

Failure Mode	Effect	Critical Characteristic	Acceptance Criteria
Input information (e.g., OEM Safety Case, Failure Data) is not correct.	Conclusions of the evaluations will likely be invalid.	4. Input information validity	Input information is applicable and valid.
Changes have occurred during ongoing production of a certified product that invalidate the certification.	The results of the evaluation are not applicable to the product currently being produced.	5. Change management and reporting mechanisms	Contractual arrangements are in place between the OEM and the CB to ensure the CB is notified of changes made to the product.
The certifying body does not have organizational discipline to ensure consistency in evaluations.	Conclusions of the evaluations will likely be invalid.	6. Organizational management	The discipline of the organization is demonstrated by implementation and adherence to a quality management program that ensures consistent performance of evaluations.

Identifying Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections:

Audit Section	Section Description	Applicability	Critical Characteristics
1	Contract Review	Yes- 1.2 & 1.4 only	5
2	Design	Yes- 2.2, 2.4-2.6 only	3-5
3	Commercial Grade Dedication	No	
4	Software Quality Assurance	No	
5	Procurement	Yes- 5.3 only	2
6	Fabrication/Assembly Activities, Material Control and Handling, Storage and Shipping	No	
7	Special Processes	No	
8	Tests, Inspections, and Calibration	No (ISO 17025 & NEI 14-05 scope)	
9	Document Control/Adequacy	Yes	1-6
10	Organization/Program	Yes	6
11	Nonconforming Items/Part 21	Yes (with no Part 21)- 11.3 only	5
12	Internal Audits	Yes	6
13	Corrective Action	Yes	6
14	Training/Certification	Yes	1
15	Field Services	No	
16	Records	Yes	1-6

ISO 17065 Table of Contents- For Reference:

Contents

Page

Comparison

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
1.2 - Verify that measures are established and implemented for the translation of customer purchase order/contract technical and quality requirements into the supplier's control documents.	4.1.2.1 the certifying body (CB) shall have a legally enforceable agreement for the provision of the certification activities to its client 4.1.2.2.a the CB shall ensure its certification agreement requires the client always fulfills the certification requirements, including directed corrective actions 4.1.2.2.b the CB shall ensure its certification agreement requires that ongoing production of the certified product continues to fulfill requirements 4.1.2.2.c.1 the CB shall ensure its certification agreement requires the client to make arrangements for the conduct of the evaluation and surveillance 4.1.2.2.c.2 the CB shall ensure its certification agreement requires the client to make arrangements for investigation of complaints 4.1.2.2.c.3 the CB shall ensure its certification agreement requires the client to make arrangements for the participation of observers 4.1.2.2.d. the CB shall ensure its certification agreement requires the client to make claims consistent with the scope of certification 4.1.2.2.e. the CB shall ensure its certification agreement requires the client not to use the product certification in a negative manner or make misleading statements concerning the cert 4.1.2.2.f the CB shall ensure its certification agreement requires the client to discontinue marketing the cert after it is no longer valid.	The contract between the certifying body (CB) and the client (equipment manufacturer) is an important aspect of the certification process. This contract must establish the CB as the authority over the resulting certification of the product being evaluated. The commercial grade survey (CGS) checklist, which is 10 CFR 50, Appendix B based, is focused on product procurements where the purchaser is the authority. This makes it less than a perfect fit for the service being surveyed, but this Section 1.2 is the best place to capture the requirements for this client-certifier agreement (contract). These requirements highlighted from ISO 17065 meet or exceed the expectations of the CGS.	None needed

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
	4.1.2.2.g the CB shall ensure its certification agreement requires the client to only reproduce certification documents in their entirety 4.1.2.2.h the CB shall ensure its certification agreement requires the client to comply with the requirements of the certification in all marketing material 4.1.2.2.i the CB shall ensure its certification agreement requires the client to comply with certification marking requirements 4.1.2.2.j the CB shall ensure its certification agreement requires the client to keep a record of all complaints made known to it relating to the certification, and to make these records available to the CB when requested. The client shall also be required to act in response to complaints and to document those actions. 4.1.2.2.k the CB shall ensure its certification agreement requires the client to inform the CB, without delay, of changes in their ability to conform to cert requirements 4.1.3.1 the CB shall control the mechanisms for indicating a product is certified 4.1.3.2 the CB shall take action to correct any inaccurate indications of product certifications 4.2 certification activities shall be undertaken impartially, and CBs must track and manage any potential and confirmed risks to maintaining impartiality on an ongoing basis. This does not preclude the CB from providing information to the client regarding identified deficiencies.		

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
1.4 - Verify that measures are established and implemented to ensure that final record packages, including Certificates of Compliance/Conformance, demonstrate that purchase order/contract technical and quality requirements were satisfied.	7.4 Evaluation- The CB shall have a plan for performing the evaluation and shall follow the plan ensuring compliance with the other applicable sections of this standard. 7.4.6 & 7.4.7 The client shall be informed of any nonconformities and given the option to work to resolve them. 7.4.8 If the client choses that path, the evaluation shall be repeated. 7.4.9 The results of all evaluation activities shall be documented prior to review. 7.5 Review- The CB shall assign a person to review the evaluation results who was not involved in the evaluation. This review shall be used to determine if a certificate will be issued. 7.6.1 Certification decision- the CB shall be responsible for its decisions relating to certification. 7.6.2 The CB shall assign at least one person to make the certification decision based on the evaluation, review, and any other relevant information. This person or group shall be independent from the performance of the evaluation. 7.7 Certification documentation- The certificate issued to the client shall meet all the requirements of this section. 7.8 The CB shall maintain information on certified products including the details of what the product is, who the manufacturer is, and what certificates were granted. 7.12 Records- The CB shall retain records to demonstrate that all certification process	Again, the NUPIC checklist is not a perfect fit for an audit or survey of a certifying body, but this Section 1.4 is the best fit for capturing this aspect of the CB's responsibility to ensure certification requirements are met and appropriately documented. These requirements highlighted from ISO 17065 meet or exceed the expectations of the CGS.	None

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
	requirements (for this standard and the scheme) have been fulfilled. 7.13 Complaints and appeals- The CB shall have a documented process to receive, evaluate and make decisions on complaints and appeals. The CB shall record and track complaints and appeals, as well as action undertaken to resolve them.		
2.2 - Verify that measures are established and implemented to control the translation of design requirements into design documents. 2.4 - Verify that measures are established and implemented for the identification and control of design interfaces. 2.5 - Verify that measures are established and implemented for the verification of design adequacy. 2.6 - Verify that measures are established and implemented to control design changes including changes for spare/replacement parts.	7.1.1 General- The CB shall operate using a certification scheme **7.1.2 Evaluation requirements of products shall be contained in specified standards** 7.1.3 If explanations are needed to link the standards to the scheme, those explanations must be developed by technically competent and impartial persons or committees 7.2 Application- the CB shall obtain all the necessary information to complete the certification process in accordance with the scheme. 7.3.1.a- The CB shall ensure the information collected about the client and product is sufficient 7.3.1.b- Differences in understanding between the CB and client are resolved 7.3.1.c- The scope of certification is defined 7.3.1.d- The means are available to perform all evaluation activities 7.3.1.e- The CB has the competence and capability to perform the certification activities 7.3.2- The CB shall have a process to identify when the client's request for certification includes a type of product, a normative document, or a certification scheme with which the CB has no prior experience	The CB is not engaged in any design activities but is heavy focused on verifying that the design of the product being evaluated meets the requirements of the applicable standards (in this case, the focus is IEC 61508). This Section 2 of the NUPIC checklist is the best fit for capturing the technical aspects of the certification process. The CB's scheme is especially important for accurately evaluating the manufacturer and their product against the relevant standards.	At this time, it is unclear how an accreditation team is structured to be able to verify the technical adequacy of the CB's scheme. Additional observations and interviews of CBs and ABs are needed to gain a deeper understanding of this technical aspect.

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
	7.3.3- In cases of 7.3.2, the CB shall ensure it has the necessary competence 7.3.4- The CB shall decline to undertake a specific certification if it lacks competence or capability 7.3.5- If the CB relies on previous certifications to omit any activities that shall be recorded in their records		
5.3 - Verify that measures are established and implemented for the evaluation, selection and assessment of sub-suppliers including distributors, services (calibration, NDE, testing, heat treatment, etc.) and software.	6.2.2.1- When the CB utilizes external resources to perform tasks such as testing, those resources shall be in compliance with the appropriate standard, such as ISO 17025	ISO 17025 has already been evaluated to be acceptable to support CGD of testing and calibration services. If testing is utilized during the certification process, that previous evaluation becomes relevant. These requirements highlighted from ISO 17065 meet or exceed the expectations of the CGS.	None
9.2- Verify that measures are established and implemented to control the preparation, review/approval, and issue of documents (e.g., procedures, instructions, drawings, work orders, etc.) including changes.	8.3 Control of documents- The CB shall establish procedures to control the document that relate to the fulfillment of this standard.	These requirements highlighted from ISO 17065 meet or exceed the expectations of the CGS.	None
10.2- Verify that adequate measures are established and implemented for management, direction and execution of the Quality Assurance Program.	4.1.1 the CB shall be a legal entity that can be held responsible 4.3.1 the CB shall have adequate financial arrangements to cover liabilities arising from its operations	It is important to note that option B (discussed in 8.1.3) requires that even if a certifying body is accredited to ISO 9001 the	None

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
	4.3.2 the CB shall have the financial stability and resources required for its operations 4.4 the CB shall conduct operations in a non-discriminatory manner 4.5 the CB shall be committed to maintaining confidentiality of clients' information 4.6 the CB shall maintain and make available upon request information about their cert scheme, a description of how the CB makes money, a description of the rights and duties of applicants and clients, and information about handling complaints and appeals 5.1.1 certification activities shall be structured and managed so as to safeguard impartiality 5.1.2 the CB shall document its organizational structure 5.1.3 the management of the CB shall identify the person or group of people who have overall authority and responsibility for keys areas of the operations of the CB (listed out in the standard) 5.1.4 the CB shall have formal rules for the appointment, terms of reference and operation of any committees that are involved in the certification process 5.2.1 the CB shall have a mechanism for safeguarding its impartiality 5.2.2.a the mechanism shall be formally documented to ensure a balanced representation of significantly interested parties 5.2.2.b the mechanism shall be formally documented to ensure access to all the information necessary to enable it to fulfil all its functions	CB must still demonstrate compliance to the management system requirements of this ISO 17065 standard.	

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
	5.2.3 if the top management of the certification body does not follow the input of this mechanism, the mechanism shall have the right to take independent action 5.2.4 although every interest cannot be represented in the mechanism, a certification body shall identify and invite significantly interested parties 8.1.1 The CB shall establish and maintain a management system that is capable of achieving the consistent fulfillment of the requirements of this standard in accordance with either of the following two options 8.1.2 Option A- the management system shall address Sections 8.2- 8.8 of this standard 8.1.3 Option B- the management system can be in accordance with ISO 9001 and must also address Sections 8.2- 8.8 of this standard. 8.2 General management system documentation- The CB's top management shall establish, document, and maintain policies and objectives for fulfillment of this standard and the certification scheme, and shall ensure they are implemented throughout the organization 8.5 Management review- The CB's top management shall establish procedures to review its management system at planned intervals, in order to ensure its continuing suitability, adequacy and effectiveness, including the stated policies and objectives related to the fulfilment of this standard		
11.3- Verify that measures are established and implemented to	7.4.6 & 7.4.7 The client shall be informed of any nonconformities and given the option to work to resolve them.	The CB is not evaluating specific physical items. They are evaluating the	None

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
disposition items which do not conform to requirements.	7.4.8 If the client choses that path, the evaluation shall be repeated. 7.9 Surveillance- The CB shall perform surveillances of the use of certification marks 7.10.1 Changes affecting certification- When the certification scheme requirements change the clients shall be informed. 7.10.2 The CB shall consider other changes affecting certification, including changes initiated by the client, and shall decide upon the appropriate action. 7.11 Termination, reduction, suspension or withdrawal of certification- When a nonconformity with certification requirements is substantiated, either as a result of surveillance or otherwise, the CB shall consider and decide upon the appropriate action. 7.13 Complaints and appeals- The CB shall have a documented process to receive, evaluate and make decisions on complaints and appeals. The CB shall record and track complaints and appeals, as well as action undertaken to resolve them.	design and processes of specific items. Therefore, non-conformities are handled from a design or process adequacy perspective.	
12.2- Verify that measures are established and implemented to ensure a comprehensive system of planned and periodic internal audits.	8.6 Internal audits- The CB shall establish procedures for internal audits to verify that it fulfils the requirements of this standard and that the management system is effectively implemented and maintained.	These requirements highlighted from ISO 17065 meet or exceed the expectations of the CGS.	None
12.3- Assess the overall effectiveness of the internal audit process by review of previous internal audits and comparison of the results/issues identified in these audits with those identified by this NUPIC audit.			

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
13.2- Verify that measures are established and implemented to assure that conditions adverse to quality are promptly identified and corrected.	7.13 Complaints and appeals- The CB shall have a documented process to receive, evaluate and make decisions on complaints and appeals. The CB shall record and track complaints and appeals, as well as action undertaken to resolve them. 8.7 Corrective actions- The CB shall establish procedures for identification and management of nonconformities in its operations. 8.8 Preventative actions- The CB shall establish procedures for taking preventive actions to eliminate the causes of potential nonconformities.	The ISO 17065 requirements exceed the 10 CFR 50, Appendix B based requirements by including "preventative actions."	None
13.3- Verify that deficiencies identified/reported by customers, to the supplier, (e.g., receipt inspection rejections, source verification rejections, return material authorizations, site nonconformances, etc.) are adequately evaluated and entered into the supplier's nonconformance or corrective action program, as applicable.			
13.4- Verify the overall effectiveness of the corrective action process.			
14.2- Verify that measures are established and implemented to ensure quality program indoctrination and training of personnel who perform activities affecting quality.	6.1.1.1 The CB shall have a sufficient number of people 6.1.1.2 The people shall be competent 6.1.1.3 The people shall keep confidential information related to certification activities 6.1.2.1 The CB shall establish, implement, and maintain a procedure for managing competencies of personnel 6.1.2.2 The CB shall maintain records on the personnel involved in the certification process 6.2.1 When the CB's internal resources perform tasks such as testing, those resources shall be in compliance with the appropriate standard, such as ISO 17025	These requirements highlighted from ISO 17065 meet or exceed the expectations of the CGS.	None
14.3- Verify that inspection/test personnel, auditors, calibration, repair personnel and similar specialists (i.e., ASME Code design personnel to ASME Section III) are qualified and have certifications on file.			

Applicable NUPIC Checklist (10 CFR 50, Appendix B based) Audit Sections	ISO 17065 Elements	Notes	Compensatory Measures
	6.2.2.2 Records must be kept to justify confidence in evaluations outsourced to non-independent bodies (e.g., client laboratories)		
16.2 - Verify that adequate measures are established and implemented to ensure that all QA records not transferred to the member are maintained in facilities that provide storage, retention requirements and protection against environmental effects, damage and loss.	7.12 Records- The CB shall retain records to demonstrate that all certification process requirements (for this standard and the scheme) have been fulfilled. 8.3 Control of documents- The CB shall establish procedures to control the document that relate to the fulfillment of this standard. 8.4 Control of records- The CB shall establish procedures to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of its records related to the fulfilment of this standard	These requirements highlighted from ISO 17065 meet or exceed the expectations of the CGS.	None

Conclusion

Based on this comparison, accreditation to ISO 17065 covers the majority of the scope of a CGS. The only aspect that still needs further investigation is how the accreditation relates to ensuring the CB's scheme is in compliance with the requirements of IEC 61508. This directly relates to critical characteristic #3 from the technical evaluation. Additional interactions with CBs and ABs are needed to gain a better understanding of how the technical requirements of the CB's scheme are verified. Beyond this technical aspect, this comparison shows that accreditation to ISO 17065 provides adequate confirmation of the CB's processes and management systems (i.e., quality assurance aspects). All critical characteristics except #3 would be able to be determined to be acceptable within the scope of a CGD of the CB service, based on the CB's accreditation to ISO 17065.

APPENDIX C. BASIS FOR AUGMENTED OBSERVATION CHECKLIST

The purpose of this document is to establish a basis for an augmented observation of a certifying body (CB). The table in this document is based on Table 4.2 in NEI 17-06 that duplicates the information from EPRI TR 106439 Table 4-1 in its first three columns for identifying and assessing dependability critical characteristics (CCs). Column 4 in in this table and NEI 17-06 Table 4.2 demonstrate how the SIL certification process evaluates these same dependability CCs. The table in this document includes a fifth column to propose questions that will form a basis for a checklist for an augmented observation of the certifying body (CB). These same basis questions address the needed compensatory measure identified in the document "Comparison of an ISO 17065 Accreditation to a Commercial Grade Survey."

Note that Reference 8 in this table refers to the EPRI report 3002011817, "Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power," Electric Power Research Institute, July 2019.

EPRI TR-106439 CCs for Acceptance	**EPRI TR-106439 Acceptance Criteria**	**EPRI TR-106439 Methods of Verification**	**SIL Certification Process Method of Verification**	**Augmented Checklist (Questions?)**
<u>Dependability</u> Reliability and maintainability related to the required functionality Built-in quality including: • Quality of design • Quality of manufacture • Failure management • Compatibility with human operators, maintainers	Criteria for reliability, availability and maintainability should be derived from the requirements of the intended application(s). Specific criteria may be established such as numerical criteria for reliability or availability of required functions, or maintainability criteria including software. If numerical criteria are used, the method of demonstration should be specified (e.g., hardware reliability prediction using classical methods, or statistical analysis of failure rate data from field experience) Basic criterion for built-in quality is equivalence to the quality of a device developed and applied. under a 10 CFR 50, Appendix B program. Judgment of equivalent quality is based on a combination of: • Design and design review processes, including software life cycle, V&V, etc. • Design documentation • Configuration management • QA program and practices • Software requirements definition and	Reliability: Review vendor reliability calculation/testing methods and results. Review operating history data. Review and assess design. Perform reliability analysis. *(Method* 2) Review of vendor processes and documentation *(Method 2 or 3):* • Design, development and verification processes • Quality assurance program and practices • V&V program and practices Design reviews --architecture review, code reviews, walkthroughs, use of analytical techniques, etc. *(Method* 2 *"& CDR" **text in quotes added***) Failure analysis, at the system level and of the commercial	<u>Reliability</u> Numerical criteria are established by IEC 61508 in terms of PFH and PFD_{avg}. See p3-7 through p3-13 of Reference 8 for details. <u>Built-in Quality</u> • The IEC Safety Lifecycle (includes configuration management) as detailed in p3-13 through p3-21 of Reference 8. • CB's review process including the safety case, see Chapter 4 of Reference 8. • AB's review process, see Chapter 5 of Reference 8.	Is there evidence of evaluation of reliability in an approved method in IEC 61508? Is the reliability criterium appropriate for the application of the product? Is systematic integrity of the design process supported by the use of the IEC Safety Lifecycle (including configuration management), as described on p3-13 through p3-21 of Reference 8 [EPRI Report]? Does the certification process include a review of the OEM safety case for the product?

EPRI TR-106439 CCs for Acceptance	EPRI TR-106439 Acceptance Criteria	EPRI TR-106439 Methods of Verification	SIL Certification Process Method of Verification	Augmented Checklist (Questions?)
Configuration control and traceability of: • Hardware • Software • Firmware (aspects of both hardware and software configuration control) • Problem reporting	requirements traceability • Consideration of failure modes and ACEs in design and verification • Qualifications and experience of personnel involved in design and verification activities • Product operating history • Testing by the vendor or dedicator Minimum criterion for configuration control and traceability is that these be sufficient to support use of operating history data and to ensure the item delivered can be traced back to the documents reviewed as part of acceptance. Additional criteria may apply if the dedicator wishes to procure more of the same item in the future. As a minimum, problem reporting must be sufficient to support use of product operating history and to allow dedicator to carry out 10 CFR 21 responsibilities. Specific criteria should be established (e.g., on coverage, timeliness, reporting to the right organization or department).	grade item itself Comparison of device's failure modes to needs of the application Review of product operating history (from vendor, users, user groups, industry reports, INPO, etc.) *(Method* 4): • Documented (records, traceable) • Sufficient (units, years in service) • Successful (error tracking shows good performance and device including software is stable) • Relevant (same or similar hardware/software configuration, functions used, operated similarly, etc.) Configuration control: review vendor configuration management program and practices. Examine actual practices, records. *(Method 2 or 3)* Problem reporting: review vendor procedures and practices. Assess performance record with previous customers *(Method 2).* Enter into contractual agreement. Assess maintainability of dedication.	• Self-diagnostics to detect dangerous failures and force the equipment to a safe state. See the discussion of the Safe Failure Fraction on p3-5 through p3-6 of Reference 8 for more details. • Defect reporting, see p4-9 of Reference 8. • SIL Certification Aging, see p4-20 of Reference 8. <u>Operating History</u> Field failure data informs the reliability determination (PFH or PFD_{avg}), see Chapter 6 of Reference 8	Does the certification process review the self-diagnostics to detect dangerous failures and force the equipment to a safe state? See the discussion of the Safe Failure Fraction on p3-5 through p3-6 of Reference 8 for more details. Does the certification process evaluate the defect reporting process in accordance with p4-9 of Reference 8? What is the CB's policy on SIL certification validity over time? Does the CB use OE in support of determining reliability similar to Chapter 6 of Reference 8? Is the OEM configuration control and traceability sufficient to support use of operating history data and to ensure the item delivered can be traced back to the documents reviewed as part of acceptance? Does the SIL certification process review OEM's policy for defect reporting, see p4-9 of Reference 8?

APPENDIX D. SUPPLEMENTAL ACCREDITATION CHECKLIST

Supplemental Accreditation Checklist Certification Body: ____ Date:_____

Assessors:_____

A certification body (CB) that is accredited to ISO 17065 is required to have a scheme, as prescribed in Section 7 of ISO 17065, to be used to evaluate products. Part of the requirements of this scheme is that it, at a minimum, encompasses the requirements of a specified standard. In this case the standard that provides this foundation is IEC 61508. The purpose of this checklist is to confirm the CB's scheme to be, at a minimum, in compliance with IEC 61508.

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
1.	Is there evidence of evaluation of reliability using an IEC 61508 approved methodology?		
1.1.	How does the CB's scheme address: IEC 61508-2 Section 7.4.5, Requirements for quantifying the effect of random hardware failures.		
2.	Is the reliability criterium appropriate for the application of the product?		
2.1.	How does the CB's scheme address: IEC 61508-2 Section 7.4.5.1 For each safety function, the achieved safety integrity of the E/E/PE safety-related system due to random hardware failures (including soft-errors) and random failures of data communication processes shall be estimated in accordance with 7.4.5.2 and 7.4.11, and shall be equal to or less than the target failure measure as specified in the E/E/PE system safety requirements specification (see IEC 61508-1, 7.10). The target failure measures are as defined in IEC 61508-1, 7.6.2.9 Tables 2 & 3. (NEI recognizes that this requirement is intended to apply to the end user, but the intent of its inclusion in this checklist is to verify that the CB ensures the failure estimates satisfy the target certification SIL)		

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
3.	Is systematic integrity of the design process supported using the IEC Safety Lifecycle (including configuration management), as described on p3-13 through p3-21 of Reference 8 [EPRI Report]?		
3.1.	How does the CB's scheme address: IEC 61508-2 Section 7.4.6, Requirements for the avoidance of systematic faults (including Table B.2)		
3.2.	How does the CB's scheme address: IEC 61508-3 Section 7.4.2, Software design and development-General requirements		
3.3.	How does the CB's scheme address: IEC 61508-3 Section 7.4.3, Requirements for software architecture design		
3.4.	How does the CB's scheme address: IEC 61508-3 Section 7.4.4, Requirements for support tools, including programming languages		
3.5.	How does the CB's scheme address: IEC 61508-3 Section 7.4.5, Requirements for detailed design and development – software system design		
3.6.	How does the CB's scheme address: IEC 61508-3 Section 7.4.6, Requirements for code implementation		
3.7.	How does the CB's scheme address: IEC 61508-3 Section 7.4.7, Requirements for software module testing		
3.8.	How does the CB's scheme address: IEC 61508-3 Section 7.4.8, Requirements for software integration testing		
4.	Does the certification process review the self-diagnostics to detect dangerous failures and force the equipment to a safe state? See the discussion of the Safe Failure Fraction on p3-5 through p3-6 of Reference 8 for more details.		

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
4.1.	How does the CB's scheme address: IEC 61508-2 Section 7.4.7, Requirements for the control of systematic faults		
4.2.	How does the CB's scheme address: IEC 61508-2 Section 7.4.8, Requirements for system behavior on detection of a fault		
5.	Does the certification process evaluate the defect reporting responsibilities of the manufacturer? See p4-9 of Reference 8.		
5.1.	How does the CB's scheme address: IEC 61508-2, Section 7.8.2.2: Manufacturers or system suppliers that claim compliance with all or part of this standard shall maintain a system to initiate changes as a result of defects being detected in hardware or software and to inform users of the need for modification in the event of the defect affecting safety.		
6.	What is the CB's policy on SIL certification validity over time?		
6.1.	Describe the CB's appropriate to maintaining the validity of certificates over time, and how this approach is consistently implemented. The approach must address change management of the design and manufacturing processes of the product under evaluation.		
7.	Does the CB use OE in support of determining reliability similar to Chapter 6 of Reference 8? Is the OEM configuration control and traceability sufficient to support use of operating history data and to ensure the item delivered can be traced back to the documents reviewed as part of acceptance?		
7.1.	How does the CB's scheme address: IEC 61508-1, Section 6.2.6, Management of functional safety: Procedures shall be developed for ensuring that all detected hazardous events are analyzed, and that recommendations are made to minimize the probability of a repeat occurrence.		

APPENDIX E. EXIDA SUPPLEMENTAL ACCREDITATION CHECKLIST

Supplemental Accreditation Checklist Certification Body: exida Date: Jan 2021

Assessors: NEI MP3 Working Group

A certification body (CB) that is accredited to ISO 17065 is required to have a scheme, as prescribed in Section 7 of ISO 17065, to be used to evaluate products. Part of the requirements of this scheme is that it, at a minimum, encompasses the requirements of a specified standard. In this case the standard that provides this foundation is IEC 61508. The purpose of this checklist is to confirm the CB's scheme to be, at a minimum, in compliance with IEC 61508.

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
1.	Is there evidence of evaluation of reliability using an IEC 61508 approved methodology?		
1.1.	How does the CB's scheme address: IEC 61508-2 Section 7.4.5, Requirements for quantifying the effect of random hardware failures.	EPRI Report Section 4, "Certifying Bodies," "exida," starting on P. 4-10	"The exida scheme goes beyond IEC 61508 and requires: … performance of a Calibrated FMEDA™ that derives all failure rates for each failure mode of the product, including false trip data not required by IEC 61508 or other CBs" "exida considers there to be three key elements to an IEC 61508 equipment certification: … means and measures against random failures (this is what FMEDA addresses)" Figure 4-1, "exida certification assessment process" includes an FMEA and a FMEDA. Each FMEDA must be … "Each analysis must be backed up by extensive fault injection testing and, if not for a new product, a detailed field failure study. This analysis covers both dangerous failures and failure that cause a false trip. exida does not accept

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
			manufacturer's failure studies alone, as they sometimes show overly optimistic results."
		P. 4-12 *Proven in Use*	exida maintains an internal Proven in Use Evaluation Criteria document with guidelines on how to assess and justify the Proven in Use applicability of an equipment item.
		P. 4-13 *Failure Rate Calculation*	"When calculating the field failure rate, a single-sided upper confidence limit of at least 70% shall be considered."
2.	Is the reliability criterium appropriate for the application of the product?		
2.1.	How does the CB's scheme address: IEC 61508-2 Section 7.4.5.1 For each safety function, the achieved safety integrity of the E/E/PE safety-related system due to random hardware failures (including soft-errors) and random failures of data communication processes shall be estimated in accordance with 7.4.5.2 and 7.4.11, and shall be equal to or less than the target failure measure as specified in the E/E/PE system safety requirements specification (see IEC 61508-1, 7.10). The target failure measures are as defined in IEC 61508-1, 7.6.2.9 Tables 2 & 3.	exida safety case tool, reviewed during NEI observation of ANAB accreditation (Nov 2020) and during interview of exida personnel (Jan 2021): William Goble, Ted Stewart, and David Butler	exida safety case requirement ID# SAD-8 requirement addresses the data communications aspect, and ID# HW-50 requirement addresses the hardware failure aspect. ID# 50 also clarifies that this requirement (IEC 61508 7.4.5.1) is the responsibility of the end user, but that the manufacturer must provide the estimated failures rates. The exida certification procedure (OP 1023) does include verifying that the estimated failure rates satisfy the target failure measures as defined in IEC 61508-1, 7.6.2.9 Tables 2 & 3.
3.	Is systematic integrity of the design process supported using the IEC Safety Lifecycle (including configuration management), as described on p3-13 through p3-21 of Reference 8 [EPRI Report]?		

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
3.1.	How does the CB's scheme address: IEC 61508-2 Section 7.4.6, Requirements for the avoidance of systematic faults (including Table B.2)	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-10	"exida considers there to be three key elements to an IEC 61508 equipment certification [only the 1st two listed]: 1. functional safety lifecycle, essentially the V model (i.e., evaluate the design process) 2. means and measures to protect against systematic failures …" "A typical assessment begins with a complete review and assessment of the OEM's development processes – hardware and software design, development, and testing process requirements and associated documentation, including environmental test reports and user documentation (e.g., safety manual) – against exida's certification scheme requirements, which includes the relevant IEC 61508 requirements."

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
		P. 4-13 *Proven in Use - Hours in Use*	"IEC 61508 lists techniques and measures to avoid systematic failures and their effectiveness. Field experience can be used as a measure to avoid systematic failures. To claim low effectiveness, 10,000 hours of operation time are required for at least one year of experience with at least 10 devices in different applications (i.e., equivalent to the 100,000 hours requirement). The statistical accuracy claimed should be 95%, and no safety critical failures may have occurred. To claim high effectiveness, 10 million hours of operation time are required for at least two years of experience with at least 10 devices in different applications. The statistical accuracy claimed should be 99.9%, and detailed documentation of all changes (including minor) during past operation should be available. The exida adequate operating experience requirement is that the equipment item needs to meet a minimum of 30 million Hours in Use. These 30 million hours of estimated usage should be obtained from a minimum of 10 different applications with stress conditions equal to or above average conditions of the application. When estimating the number of hours in use, the equipment item actual installation dates shall be considered, not the shipment dates of the equipment items. In case the actual installation dates are not available for the hours in use estimation, it shall be

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
			assumed that the installation occurs six months after the equipment item shipment. If the equipment item has a wear out mechanism, it shall be assumed that all units operate no longer than the useful life period. Furthermore, it shall be assumed that no wear out failures are reported to the manufacturer. This is a worst-case assumption as wear out failures will be treated as random hardware failures."
3.2.	How does the CB's scheme address: IEC 61508-3 Section 7.4.2, Software design and development- General requirements	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-11	"A typical assessment begins with a complete review and assessment of the OEM's development processes – hardware and software design, development, and testing process requirements and associated documentation, including environmental test reports and user documentation (e.g., safety manual) – against exida's certification scheme requirements, which includes the relevant IEC 61508 requirements."

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
3.3.	How does the CB's scheme address: IEC 61508-3 Section 7.4.3, Requirements for software architecture design	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-11	"Product requirements (e.g., the SRS) and design documents are reviewed next. The documents supplied should match those required by the design procedures."
		Interview of exida personnel (Jan 2021): William Goble, Ted Stewart, and David Butler	exida safety case template has an entire section labeled as "SWA" that contains several requirements that directly address this section of IEC 61508. These requirements must be met by the manufacturer to satisfy the exida scheme.
3.4.	How does the CB's scheme address: IEC 61508-3 Section 7.4.4, Requirements for support tools, including programming languages	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-11, Figure 4-1	The final safety case provided by the manufacturer must include a "Tool Justification" that exida evaluates against IEC 61508.
3.5.	How does the CB's scheme address: IEC 61508-3 Section 7.4.5, Requirements for detailed design and development – software system design	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-11	"Figure 4-1 illustrates the exida certification assessment process. [27] A typical assessment begins with a complete review and assessment of the OEM's development processes – hardware and software design, development, and testing process requirements and associated documentation, … – against exida's certification scheme requirements, which includes the relevant IEC 61508 requirements."
3.6.	How does the CB's scheme address: IEC 61508-3 Section 7.4.6, Requirements for code implementation	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-11, Figure 4-1	The final safety case provided by the manufacturer must include a "Coding Standard" that exida evaluates against IEC 61508.
3.7.	How does the CB's scheme address: IEC 61508-3 Section 7.4.7, Requirements for software module testing	EPRI Report Section 4, "Certifying Bodies,"	The final safety case provided by the manufacturer must include a "Software

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
		"exida," P. 4-11, & Figure 4-1	Module Test Plan" that exida evaluates against IEC 61508. "Figure 4-1 illustrates the exida certification assessment process. [27] A typical assessment begins with a complete review and assessment of the OEM's development processes – hardware and software design, development, and testing process requirements and associated documentation,… – against exida's certification scheme requirements, which includes the relevant IEC 61508 requirements."
3.8.	How does the CB's scheme address: IEC 61508-3 Section 7.4.8, Requirements for software integration testing	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-11, Figure 4-1	The final safety case provided by the manufacturer must include a "Software Integration Test Plan" that exida evaluates against IEC 61508.
4.	Does the certification process review the self-diagnostics to detect dangerous failures and force the equipment to a safe state? See the discussion of the Safe Failure Fraction on p3-5 through p3-6 of Reference 8 for more details.		
4.1.	How does the CB's scheme address: IEC 61508-2 Section 7.4.7, Requirements for the control of systematic faults	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-10	"The exida scheme goes beyond IEC 61508 and requires: • performance of a Calibrated FMEDA™ that derives all failure rates for each failure mode of the product, including false trip data not required by IEC 61508 or other CBs" "exida considers there to be three key elements to an IEC 61508 equipment certification: 1. functional safety lifecycle, essentially the V model (i.e., evaluate the design process)

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
			2. means and measures to protect against systematic failures 3. means and measures against random failures (this is what FMEDA addresses)"
		Figure 4-1	Exida performs or reviews a FMEDA, Software Hazard Analysis, and a Communication Protocol Analysis as part of their review of the final safety case and ensures the requirements of IEC 61508 are meet.
4.2.	How does the CB's scheme address: IEC 61508-2 Section 7.4.8, Requirements for system behaviour on detection of a fault	EPRI Report Section 4, "Certifying Bodies," "exida," P.4-11	"Product requirements (e.g., the SRS) and design documents are reviewed next. The documents supplied should match those required by the design procedures…" "In parallel with these document reviews, a detailed FMEDA of the equipment is performed (or reviewed, if the OEM has previously performed one) to document the hardware architecture and failure behavior. Each analysis must be backed up by extensive fault injection testing and, if not for a new product, a detailed field failure study. This analysis covers both dangerous failures and failure that cause a false trip."
5.	Does the certification process evaluate the defect reporting responsibilities of the manufacturer? See p4-9 of Reference 8.		
5.1.	How does the CB's scheme address: IEC 61508-2, Section 7.8.2.2: Manufacturers or system suppliers that claim compliance with all or part of this standard shall maintain a system to initiate changes as a result of defects being detected in hardware or software and to inform users of the need for modification in the event of the defect affecting safety.	Interview of exida personnel (Jan 2021): William Goble, Ted Stewart, and David Butler	exida safety case requirement ID# MOD-4 specifically requires the manufacturer to comply with this clause from IEC 61508. exida requires the manufacturer to have a procedure for notifying users of detected product defects that affect safety.

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
6.	What is the CB's policy on SIL certification validity over time?		
6.1.	Describe the CB's appropriate to maintaining the validity of certificates over time, and how this approach is consistently implemented. The approach must address change management of the design and manufacturing processes of the product under evaluation.	EPRI Report Section 4, "Certifying Bodies," "exida," P. 4-12	"exida's certifications are valid for three years. If a product does not initially pass the recertification assessment (i.e., changes must be made before it can pass), then a surveillance audit is scheduled for approximately one year later. These time intervals are self-imposed by exida and not driven by IEC 61508 requirements."
		Interview of exida personnel (Jan 2021): William Goble, Ted Stewart, and David Butler	The exida procedure, OP1004, documents exida's approach to maintaining certificates. A tool exida chooses to use is surveillance audits. exida's approach to surveillance audits is documented in OP1030. Within exida's process, it is possible that certificates can be issued for 1 year instead of 3. This may occur in cases where there are management or administrative improvements needed but the design of the product meets safety requirements.

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
7.	Does the CB use OE in support of determining reliability similar to Chapter 6 of Reference 8? Is the OEM configuration control and traceability sufficient to support use of operating history data and to ensure the item delivered can be traced back to the documents reviewed as part of acceptance?		
7.1.	How does the CB's scheme address: IEC 61508-1, Section 6.2.6, Management of functional safety: Procedures shall be developed for ensuring that all detected hazardous events are analysed, and that recommendations are made to minimise the probability of a repeat occurrence.	Interview of exida personnel (Jan 2021): William Goble, Ted Stewart, and David Butler EPRI Report Section 7, P. 7-1	exida safety case requirement ID# FSM-1 specifically requires the manufacturer to comply with this clause from IEC 61508. "IEC 61508 is an international standard for functional safety that specifies design process requirements to provide integrity against systematic errors and performance requirements to provide integrity against random hardware failures. To accomplish that, it includes comprehensive and detailed software quality requirements. Key points of functional safety are to provide or maintain a safe state under hazard conditions, to reduce the likelihood of systematic errors, and to control random failures. The use of appropriate sets of techniques and measures are required by the standard."

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
		Section 4, P. 4-10	"exida operates its IEC 61508 functional safety certification program based on a scheme that lists all requirements that a product manufacturer must meet to receive an exida certificate. These requirements are documented in a safety case template. The exida scheme goes beyond IEC 61508 and requires: • performance of a Calibrated FMEDA™ that derives all failure rates for each failure mode of the product, including false trip data not required by IEC 61508 or other CBs • cyber security audits per IEC 62443 standards • practical manual proof test procedures or automatic proof test functionality • surveillance audits, where engineering changes, field failure data, and design procedure changes are audited to determine if the product still meets IEC 61508 requirements (some functional safety certification programs done per IEC 61508 do not require surveillance audits)"

Item #	Requirement	Evidence References	Discussion: How does the CB's scheme meet or exceed this requirement?
		P. 4-11	Figure 4-1 illustrates the exida certification assessment process. [27] A typical assessment begins with a complete review and assessment of the OEM's development processes – hardware and software design, development, and testing process requirements and associated documentation, including environmental test reports and user documentation (e.g., safety manual) – against exida's certification scheme requirements, which includes the relevant IEC 61508 requirements."
		P. 4-12	"A safety case is a list of all requirements of exida's scheme along with arguments and evidence that the product under assessment meets the requirements. It is a tool to ensure completeness of the certification audit, providing a systematic method to ensure that no requirements are overlooked. When unsatisfied requirements are identified, the OEM must return to a previous safety lifecycle step and correct the problem. When the safety case is judged to be accurate and complete, the certification report describing all assessment activities and their results is written. The documentation is given to an independent auditor to verify. Once the audit is complete and the independent auditor supports the certification, the certificate is issued."