NEI | TECHNICAL REPORT

NEI 17-06, "Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications" Revision B

Prepared by the Nuclear Energy Institute
September 2019

Table of Contents

1 INTRODUCTION

1.1 Purpose

The purpose of this supplemental guidance is to provide an acceptable approach for procuring and accepting commercial grade digital equipment that have a safety integrity level (SIL) certification by an accredited third party SIL certification body for nuclear safety-related applications. Making use of internationally accredited SIL certification services benefits licensees and their suppliers through expanded access to expert services, improved standardization on equipment quality evaluations, improved regulatory confidence, and reduced cost without compromising safety.

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

1.2 Regulatory Basis

Basic components are items and services relied upon to perform a safety related function at US commercial nuclear power plants and are required to be controlled under a quality assurance program complying with 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants". A commercial grade item is an item that is not a basic component. Dedication (commercial grade dedication) is an acceptance process undertaken to provide reasonable assurance that a commercial grade item 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 10CFR50, Appendix B-compliant QA program, items can be purchased as commercial grade items and accepted via the dedication process. The entity performing this dedication is referred to as the Supplier (i.e., third party dedicator, OEM or licensee 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 must be performed under a Quality Assurance Program that meets the requirements of 10 CFR Part 50, Appendix B.

The NRC has endorsed EPRI TR-106439 as "*an acceptable method for dedicating commercial grade digital equipment for use in nuclear power plant safety applications and meets the requirements of 10 CFR Part 21.*"[1]

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

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

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

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

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

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].

[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.

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

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

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

Section 2 describes the third party SIL certification process, and Section 3 provides the US nuclear industry's evaluation of the third party SIL certification process including a comparison with NRC accepted practices (i.e., EPRI TR-106439). Section 6 describes the approach for the US nuclear industry to provide continued oversight of the third party SIL certification process in order to confirm that the third party SIL certification process can continue to be used in lieu of commercial grade surveys for the purpose of verifying the EPRI TR-106439 dependability critical characteristics.

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

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

1. The method to use a third party SIL certification by a company accredited by a signatory to IAF in lieu of a commercial grade survey (alternative method) for verification of EPRI TR-106439 dependability critical characteristics is documented in the Purchaser's QA program.

2. The method the Purchaser needs to follow, and document in their QA Program, consists of:

i. Adopt NRC-endorsed NEI 17-06 into the QA program

ii. The purchase documents require that:

a. A copy of the SIL certificate for the commercial grade digital equipment being purchased be provided

b. SIL certification has not expired

c. SIL certification precautions and limitations be included in the SIL certificate or in the safety manual

d. A certificate of conformance that the third party SIL certifier is accredited by a signatory to IAF.

iii. It is validated, at receipt inspection, that the commercial grade digital equipment supplier documentation certifies that:

e. The commercial grade digital equipment matches that defined in the SIL certificate provided

f. The purchase order's requirements are met

1.4 Acronyms

AB	Accreditation Body
AC	Administrative Controls
ANSI	American National Standards Institute
CB	Certifying Body
CC	Critical Characteristics
CDR	Critical Design Review
CFR	Code of Federal Regulations
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
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
PFDavg	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

1.5 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. 9810150223.

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, US 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

2 SAFETY INTEGRITY LEVEL (SIL)

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

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

This process is initiated by a manufacturer identifying a business case for producing products that are capable of a particular SIL, commonly 2 or 3, for a defined scope of safety functions. Then they plan out their development based on the requirements of 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. That 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 implemented in tables that correlate a Average Probability of Dangerous Failure on Demand (PFDavg) 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 this document contains tables that are used to select those processes and procedures that will be used to build the case of meeting a systematic capability level. IEC 61508 introduces the concept of systematic capability, which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level. For example, a table is shown below 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

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

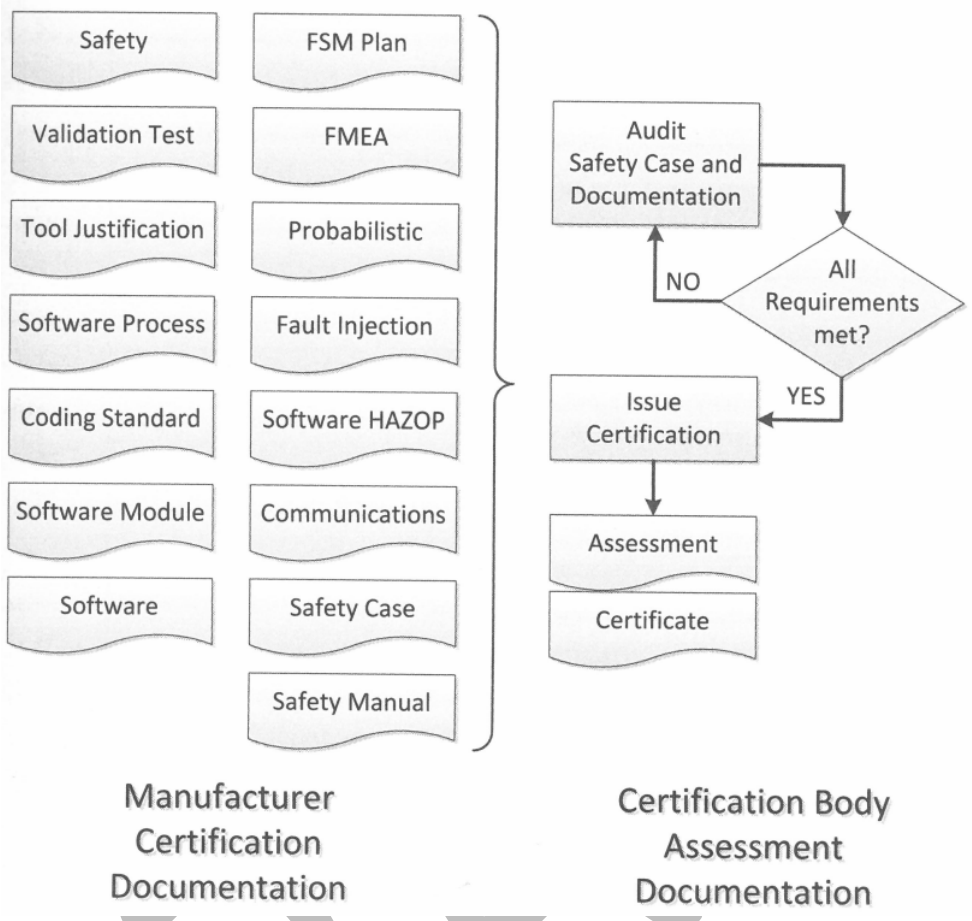


Figure 2.1. Typical Certification Process (Figure 1.3 from Reference 21)

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

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

To be a credible entity, the certification body is accredited by the national accreditation body. This accreditation is typically in accordance with ISO 17065. The accreditation bodies that primarily perform this type of work are the Deutsche Akkreditierungsstelle (DAkkS), in Germany, and the American National Standards Institute (ANSI), in the USA. The accreditation body performs audits and monitors activities of the certification body in order to confirm that their processes and procedures, and their

corresponding implementation follows ISO 17065. Accreditations remain valid for a certain time period and then must be re-established through repeating the appropriate audits and evaluations.

2.2 Description of the Critical Dependability Characteristics per NRC-Endorsed EPRI-TR 106439

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

The process of commercial grade dedication as described in 10 CFR 21 requires the identification of critical characteristics for the basic component to be dedicated. EPRI TR 106439 adds a special type of critical characteristic 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 design review (CDR). The CDR requires an understanding of the specific programmable logic and hardware features embodied in the design, to verify that they are correct and appropriate in light of the requirements of the intended application.

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

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

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

Often, the CDR is considered synonymous with the use of method 2, commercial grade surveys (CGS), and this can sometimes cause confusion. While the CDR and CGS both involve seemingly similar vendor assessment activities, the goals of these two activities are very 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 US 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 ultimate conclusion that a product has met the dependability critical characteristics is based on engineering judgement. EPRI TR 106439 describes this in the following manner, “A commercial product may be judged to have sufficient quality, even if its development process lacked some of the rigorous steps of modern software engineering and/or some formal documentation. Reaching a reasonable level of assurance of quality of a commercial grade digital item typically involves making a judgment based on a combination of the product development process and its documentation, operating history, testing, review of design features such as failure management, and other factors noted in the critical characteristics matrix, Table 4-1.”

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

- Reliability and maintainability related to the required functionality
- Built-in quality
    - Quality of design
    - Quality of manufacture
    - Failure management
    - Compatibility with human operators, maintainers

[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

- Configuration control and traceability
    - Hardware
    - Software/firmware (i.e., programmable logic)
    - Problem reporting

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

Section 4.1, "Application of the SIL Certification Process", demonstrates that the IEC 61508 SIL certification process encompasses the assessment of the dependability critical characteristics as described in this section.

3 EPRI RESEARCH OF THE SIL CERTIFICATION PROCESS

3.1 Scope of the EPRI Research

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 original equipment manufacturers (OEMs) and end users, identifying that all parties benefit when using this functional

safety framework. The OEMs 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 (PFDavg), depending on the mode of operation (e.g., 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. The last section of chapter 3 is "Supplier Quality Management" and is very interesting because it reviews some older EPRI research that compares the type of quality system OEMs within the SIL ecosystem utilize (ISO 9001) to a nuclear quality program based on 10CFR50 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)

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 OEM has completed the design of the product and has established the manufacturing processes, the OEM 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 certification body (CB) for evaluation. This chapter discusses

what is involved in the CB's review of the safety case and lists the capabilities that a CB must have to be able perform the evaluation. 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 OEM 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 OEM when defects are identified that impact the safe operation of the SIL certified equipement. There are no requirements in IEC 61508 for the OEM to report defects to the CB, but the report also explains why that is still likely to occur. For the dedicating entity to receive defect reporting directly from the OEM is ideal to support their 10CFR21 defect reporting responsibilities. A relevant quote from the report is included is included. In this quote it is important to understand that "end-users" are the purchasers of the equipment, and therefore would be the dedicating entity:

> "OEM's 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 third-party 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 OEMs. 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 an OEM can manufacture 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 OEM. 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 OEMs. The report explains that each country has their own accreditation body (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 American National Standards Institute (ANSI) is the AB for exida in the USA. It also provides some details about ANSI'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. It was particularly interesting that these results illustrated how the probabilistic failure rates and 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. It is also valuable to note that systematic integrity/issues is a parallel concept to the nuclear industry's concept of common cause failure. The overall assessment of the field failure analysis also included these observations:

> "There were no examples of software common cause failures in any of the data sets evaluated. When asked to comment on this, Dr. William Goble, cofounder of exida, indicated that while some design related failures are due to software errors, the improvements in (safety-related) PES development processes over the last several decades have made the risk of software common cause failures much less of a concern today. In his experience, manufacturing process issues are more frequent contributors to systematic failures than are software errors. Furthermore, in Dr. Goble's opinion, high-volume production software-based equipment has higher quality software than any custom-designed, low-volume production equipment." (p6-14 to 6-15)

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*, and
- 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.

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

4.1 Application of the SIL Certification Process

Based on the EPRI report (Reference 8) summarized in section 3 of this document, it has been concluded that the IEC 61508 SIL certification process encompasses the assessment of the dependability critical characteristics as described in section 2.2. SIL certifications can be used as the evidence of acceptability of dependability critical characteristics (CCs) as defined by EPRI 106439. Whether dependability is discussed as "built-in quality" or "systematic integrity," the goals are the same. Those goals are for the equipment to always perform its safety function correctly, and for the owner/operator and regulatory body to have confidence in the equipment. This commonality means that there is significant potential for the nuclear industry to utilize commercial off the shelf (COTS) components that have been designed and manufactured using IEC 61508, and tap into the benefits of a large pool of equipment certified for safety applications. The nuclear industry can take advantage of these COTS components that have been designed and manufactured with reliability and systematic integrity when dedicating this equipment for safety-related applications.

4.2 Technical Evaluation & Acceptance Method

To see how crediting the SIL certification process can be used as part of the commercial grade dedication process, consider Table 4-1 of EPRI TR 106439. This table would be the same until reaching the dependability CCs. These characteristics are typically evaluated for acceptability using commercial grade surveys (EPRI method 2) including critical design reviews (CDRs) and reviewing operating history (EPRI method 4). Table 4-2 in this document shows how the SIL certification process (column 4 in Table 4-2) evaluates these dependability CCs for acceptability in lieu of a commercial grade survey (column 3 of Table 4-2). The resulting process is illustrated in Figure 4.2.

There are no major changes to the high level CGD process, but this approach yields significant efficiency gains for the commercial grade dedicator. Note that EPRI method 2, 3 and/or 4 could be used as the verification approach to any of the remaining physical or performance (non-dependability) CCs, but it typically makes technical and economic sense to verify those CCs using EPRI method 1.

Table 4.2- 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 Built-in quality including: • Quality of design • Quality of manufacture • Failure management • Compatibility with human operators, maintainers Configuration control and traceability of: · Hardware · Software · Firmware (aspects of both hardware and software configuration	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 requirements traceability	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 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*	<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. • 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>

EPRI TR-106439 CCs for Acceptance	EPRI TR-106439 Acceptance Criteria	EPRI TR-106439 Methods of Verification	SIL Certification Process Method of Verification
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).	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.	Field failure data informs the reliability determination (PFH or PFD_{avg}), see Chapter 6 of Reference 8

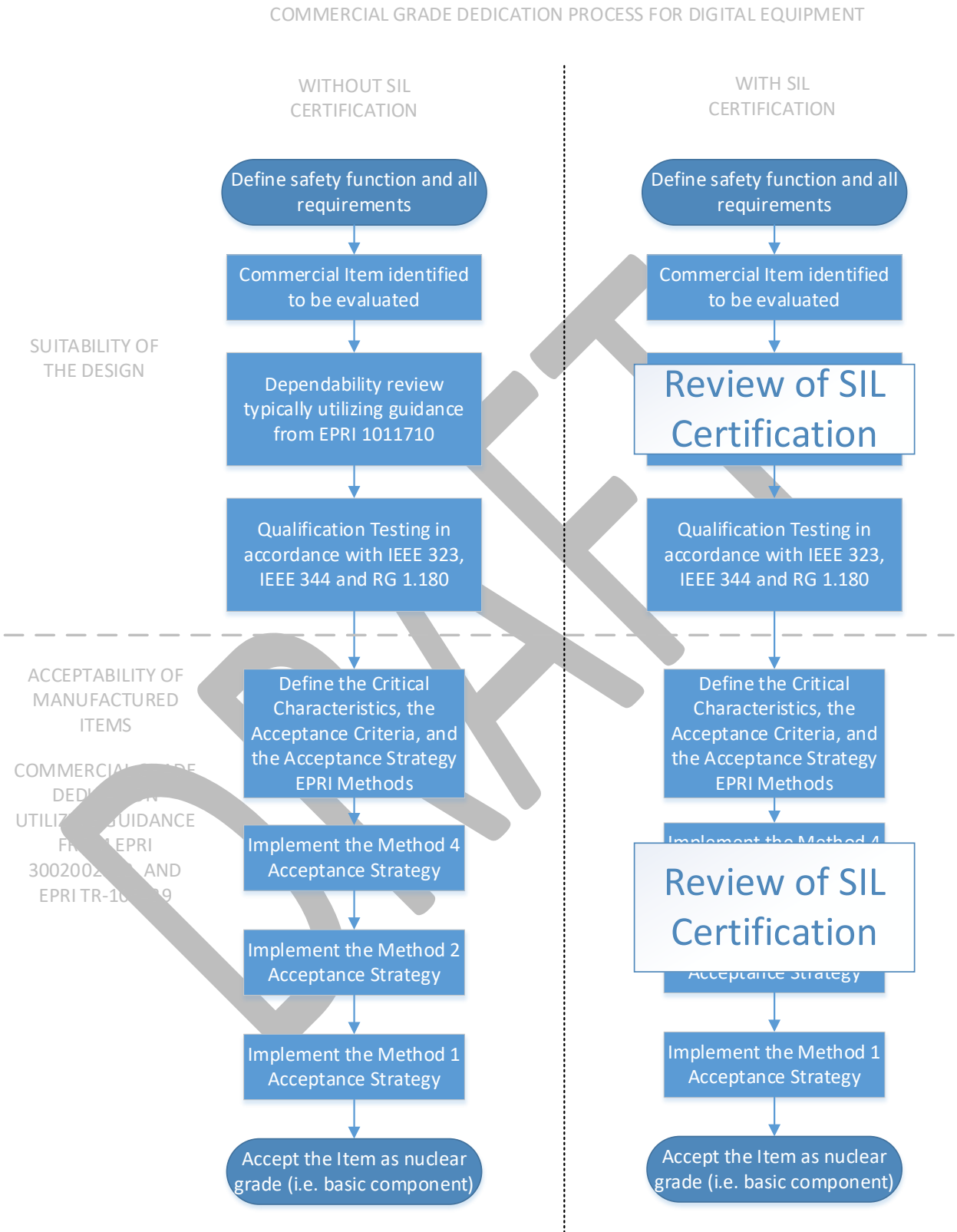


Figure 4.2- Commercial Grade Dedication and Qualification Process with and without SIL Certification

4.3 Selection of SIL Certified Equipment

To be able to properly utilize the process laid out in the previous section equipment must be selected that meets the functional requirements of the application, be certified for a safety function that encompasses the safety function of the application, and must be SIL certified by an accredited certifying body. After potential equipment has been identified that meets the functional requirements of the application, these steps shall be followed.

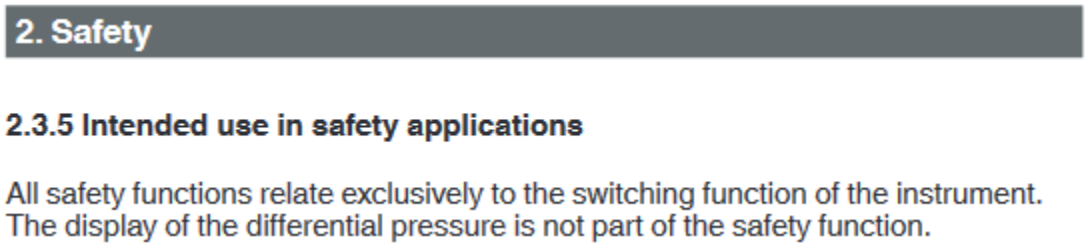
1. Obtain the equipment's SIL certificate and the safety manual. Refer to Appendix B of this document to review two example certificates.

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

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

4. 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 safety function used for the certification 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:



2. Safety

2.3.5 Intended use in safety applications

All safety functions relate exclusively to the switching function of the instrument. The display of the differential pressure is not part of the safety function.

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

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

5 SUPPLIER'S QUALITY ASSURANCE PROGRAM

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

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

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

Note: *The supplier can be any entity with a 10 CFR 50 Appendix B QQ program including the Original Equipment Manufacturer (OEM), a 3rd part commercial dedicator, or the Licensee.*

5.1 Organization

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

5.2 Procurement Document Control

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

These shall be included as a minimum:

1) The component must be provided in accordance with the CB's accredited program and scope of certification and accreditation.

2) An IEC 61508 SIL certificate report is a deliverable to the purchasing organization and must contain adequate information to ensure performance and applicability to the intended safety function. The types of information that is produced by the certification are described in sections 3 and 4.

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

4) The NUPIC SIL certification oversight report for the AB.

5.3 Control of Purchased Material, Equipment, and Services

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

1) Reviewing the Certification Body's (CB) Certification report and ensuring applicability to the defined safety function and has adequate information to support Commercial Grade Dedication requirements as defined in the following sub-sections.

2) Reviewing the up-to-date Accrediting Body's (AB) documentation of the CB that certified the component and ensure there are no outstanding deficiencies or findings.

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

5.4 QA Evidence for Digital Dependability

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

5.4.1 QA Evidence for Digital Dependability

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

1) An up-to-date IEC 61508 SIL certification report applicable to the component and its safety related function. Reviewing and approving the up-to-date AB's accreditation document of the CB, that provided the SIL certificate for the component, and verifying that there are no outstanding issues with the CB that could impact the SIL certification

2) An up to date and acceptable NUPIC observation report.

Note that other CCs such as performance CCs will be accessed by the normal commercial grade dedication process

5.4.2 Supplier Tasks Associated Digital Dependability Evidence

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

1) Review and approval of the certification report and ensuring applicability to the defined safety function.

2) Reviewing and acceptance of the up-to-date AB's accreditation document of the CB, that provided the SIL certification for the component, and verifying that there are no outstanding issues with the CB that could impact the SIL certification .

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

Note: If 1) above is successfully completed, the Supplier does not need to directly perform technical verification of data produced nor should they need to perform commercial grade surveys beyond the CB's accreditation of the vendor/manufacturer of the SIL certified component (such as to verify the dependability CC). Note that there may be other reasons to perform a commercial grade survey besides dependability CC verification such as crediting performance CCs (i.e., environmental testing, accuracy, EMI/RFI testing, etc.).

5.5 Corrective Action

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

2) Once acceptance is successfully completed, the supplier is required to notify Licensees and the NRC of any significant conditions adverse to quality as required by Part 21.

3) The SIL certification process requires the component vendor to identify problems as part of the certification process. The supplier shall have a contractual relationship in place to ensure notification of errors is obtained.

6 U.S. NUCLEAR INDUSTRY OVERSIGHT OF THE SIL CERTIFICATION PROCESS

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

6.1 Organization

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

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

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

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

Any time the IEC 61508 standard is under revision, NEI will evaluate whether the potential changes impact the 3rd Party IEC 61508 SIL certification process and its coverage of the EPRI TR 106439 Dependability Critical Characteristics. If changes adversely impact coverage of the EPRI TR 106439 Dependability Critical Characteristics, then the nuclear industry through NEI has the ability to provide feedback to the IEC 61508 standards development committee to change the draft revision to encompass these critical characteristics.

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

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

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

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

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

exida

The manufacturer may use the mark:

exida • CERTIFIED • IEC 61508 • SIL 3 CAPABLE •

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

IAF

ANSI ACCREDITED

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.

exida Certification

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 downstream 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

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_{SU} [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 61 201 VA3:2013.
(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}**	**4,64 E-05**	
Mean Time to Dangerous Failure	**$MTTF_D$**	**9,86 E+07 h**	**11.016 a**

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

B_{10} 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**	**1.188 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.