

TABLE OF CONTENTS

1	<u>INTRODUCTION</u>	III
1.1	PURPOSE	III
1.2	REGULATORY BASIS.....	III
1.3	ACCEPTANCE OF SAFETY INTEGRITY LEVEL AS-VERIFICATION OF DEPENDABILITY CRITICAL CHARACTERISTICS.....	V
1.4	ACRONYMS	VI
2	SAFETY INTEGRITY LEVEL (SIL)	7
3	ACCEPTANCE OF COMMERCIAL GRADE DIGITAL EQUIPMENT FOR SAFETY APPLICATIONS CERTIFIED TO A PARTICULAR SIL	7
4	PURCHASER'S QUALITY ASSURANCE PROGRAM	7
5	US NUCLEAR INDUSTRY REVIEW OF THE SIL CERTIFICATION PROCESS	7
5.1	TECHNICAL EVALUATION OF SIL CERTIFICATION REQUIREMENTS AND PROCEDURES.....	7
5.2	VERIFICATION THAT THE SIL CERTIFICATION PROCESS CONTINUES TO BE CONSISTENT WITH NRC ENDORSED PRACTICES.....	7
5.3	VERIFICATION THAT IMPLEMENTATION OF THE ILAC PROCESS CONTINUES TO BE CONSISTENT WITH NRC ACCEPTED PRACTICES	8
	US NUCLEAR INDUSTRY OVERSIGHT OF THE SIL PROCESS	
6.1	ORGANIZATION.....	
6.2	VERIFICATION THAT THE SIL CERTIFICATION PROCESS CONTINUES TO BE CONSISTENT WITH NRC ACCEPTED PRACTICES	
6.3	VERIFICATION THAT IMPLEMENTATION OF THE SIL CERTIFICATION PROCESS CONTINUES TO BE CONSISTENT WITH NRC ACCEPTED PRACTICES	
6.4	OPTIONAL ACTIVITIES	

END OF GUIDELINE

ATTACHMENT A – NRC FINAL SAFETY EVALUATION REPORT ATTACHMENT A-1

ATTACHMENT B – NRC RAIS AND NEI RESPONSES ... ATTACHMENT B-1

DRAFT

1 INTRODUCTION

1.1 PURPOSE

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

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) that provided the necessary evidence of dependability critical characteristics described in EPRI Technical Report 106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications". 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 a substantial reduction in duplication of effort for accepting commercial grade equipment across the industry, while ensuring that the identified dependability critical characteristics defined in EPRI TR-106439 continue to be met.

1.2 REGULATORY Basis

Items and services used in safety related applications at US commercial nuclear power plants are designated as basic components and are required to be provided in accordance with 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants".

It is not always possible or practical to procure items and services directly from suppliers that implement quality assurance programs that meet 10 CFR Part 50, Appendix B. Therefore, the NRC established requirements in 10 CFR Part 21 "Reporting of Defects and Noncompliance" that permit the use of commercial grade items and services in nuclear safety related applications through a commercial grade dedication process. 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 process for accepting items and services for use as basic components from commercial suppliers is known as commercial grade dedication. 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."*

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 [underling 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].

This supplemental guidance document describes a method for using the accredited SIL certification process as evidence of verification of the EPRI TR-106439 dependability critical characteristics within the commercial grade dedication process. This supplemental guidance is applicable to dedicating entities subject to the quality assurance requirements of 10 CFR Part 50, Appendix B (e.g., 10 CFR Part 50, 10 CFR Part 52, 10 CFR Part 71 and 10 CFR Part 72 licensees and affected suppliers).

1.3 ACCEPTANCE OF SAFETY INTEGRITY LEVEL AS-VERIFICATION OF DEPENDABILITY CRITICAL CHARACTERISTICS

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

Section 2 describes the third party SIL certification process, and Section 5 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. This conclusion requires procurement documents to include a few requirements. Section 3 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 4 describes information that Purchasers should ensure is included in their Quality Assurance Programs.

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

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

1. A documented review of the third party SIL certifier's accreditation is performed and includes a verification of the following:
 - a. The third party SIL certifier holds accreditation by an accrediting body that is a signatory to IAF.
 - b. The published scope of accreditation for the third party SIL certifier covers IEC 61508 SIL certification.
2. The purchase documents require that:
 - a. A copy of the SIL certificate for the commercial grade digital equipment being purchased be provided
 - b. The IEC 61508 Systematic Capability SIL be identified in the certificate
 - 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.
 - e. The customer must be notified of any condition that adversely impacts the third party SIL certifier's ability to maintain its SIL certification accreditation or the scope of accreditation.
3. It is validated, at receipt inspection, that the commercial grade digital equipment supplier documentation certifies that:
 - a. The commercial grade digital equipment matches that defined in the SIL certificate provided
 - b. The purchase order's requirements are met

1.4 ACRONYMS

AB – Accreditation Body

CFR – Code of Federal Regulations

EPRI – Electric Power Research Institute

IAF – International Accreditation Forum

IEC – International Electrotechnical Commission

NEI – Nuclear Energy Institute

NRC – Nuclear Regulatory Commission

NUPIC – Nuclear Procurement Issues Corporation

QA – Quality Assurance

QC – Quality Control

SIL - Safety Integrity Level

2 SAFETY INTEGRITY LEVEL (SIL)

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

4 PURCHASER'S QUALITY ASSURANCE PROGRAM

5 US NUCLEAR INDUSTRY REVIEW 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.

5.1 TECHNICAL EVALUATION OF SIL CERTIFICATION REQUIREMENTS AND PROCEDURES

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.

5.2 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.

5.3 VERIFICATION THAT IMPLEMENTATION OF THE 3rd PARTY IEC 61508 SIL CERTIFICATION PROCESS CONTINUES TO BE CONSISTENT WITH NRC ACCEPTED PRACTICES

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

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