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

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

EPRI TR-106439 CCs for Acceptance	**EPRI TR-106439 Acceptance Criteria**	**EPRI TR-106439 Methods of Verification**	**SIL Certification Process Method of Verification**	**Augmented Checklist (Questions?)**
<u>Dependability</u> Reliability and maintainability related to the required functionality Built-in quality including: • Quality of design • Quality of manufacture • Failure management • Compatibility with human operators, maintainers	Criteria for reliability, availability and maintainability should be derived from the requirements of the intended application(s). Specific criteria may be established such as numerical criteria for reliability or availability of required functions, or maintainability criteria including software. If numerical criteria are used, the method of demonstration should be specified (e.g., hardware reliability prediction using classical methods, or statistical analysis of failure rate data from field experience) Basic criterion for built-in quality is equivalence to the quality of a device developed and applied. under a 10 CFR 50 Appendix B program. Judgment of equivalent quality is based on a combination of: • Design and design review processes, including software life cycle, V&V, etc.	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	<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	Is there evidence of evaluation of reliability in an approved method in IEC 61508? Is the reliability criteria appropriate for the application of the product? Is the IEC Safety Lifecycle (including configuration management) conform to p3-13 through p3-21 of Reference 8 [EPRI Report]? Does the certification process include a review of the OEM safety case for the product? Does the certification process review the self-diagnostics to detect dangerous failures and force the

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

EPRI TR-106439 CCs for Acceptance	EPRI TR-106439 Acceptance Criteria	EPRI TR-106439 Methods of Verification	SIL Certification Process Method of Verification	Augmented Checklist (Questions?)
	be established (e.g., on coverage, timeliness, reporting to the right organization or department).			