

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

| NEI Comment Number | Section    | NEI's Comment   | NRC Staff's Resolution of NEI's Comment  |
|--------------------|------------|---|--|
| NEI-1              | NEI Letter | Industry expressed concerns throughout the development process with the "...unnecessary level of complexity and detail in the guide that may, inadvertently, dissuade facilities from installing digital instrumentation and control systems" | NRC staff has addressed the industry's concerns throughout the development process by incorporating comments received from industry. The public comments received with this letter do not identify which paragraphs or sections of the draft ISG are overly complex. The NRC staff does not believe that the draft ISG is either unnecessarily complex or unnecessarily detailed. Where the application of appropriate safety criteria to meet the facility performance objectives seems challenging to implement, alternative acceptable methods for achieving the facility performance objectives have been provided. However, to enable a more rapid understanding of the goals being achieved within each section, modifications to the ISG format will be made in the form of highlights or bullets depicting the key criteria being addressed. |
| NEI-2              | NEI Letter | Industry expressed concerns throughout the development process with the "...overtones and references to cyber "security" rather than a cyber program focused on safety pursuant to 10 CFR Part 70;"   | The NRC staff has already taken into account industry concerns regarding implementation of programmatic actions to ensure the protection of digital IROFS in this version of the ISG. However, NRC staff will enhance its distinction between facility cyber security and digital IROFS cyber safety by ensuring that the guidance provided to reviewers appropriately falls under the context of 10 CFR Part 70. See Discussion of NEI-8 and NEI-9 below.   |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|       |            |  |   |
|-------|------------|--|---|
| NEI-3 | NEI Letter | <p>Industry expressed concerns throughout the development process with the "...references and language more aligned with the higher risk operations at a commercial nuclear power reactor rather than the lower risk and more diverse fleet of fuel cycle facilities in operation today or planned for the future."</p> <p>Further, some gradation of a risk-informed approach should be used for the various categories of fuel cycle facilities licensed under Part 40 or 70 or certified under Part 76.</p> | <p>The references and languages used in this draft ISG are aligned with the lower risk and more diverse fleet of fuel cycle facilities in operation today or planned for the future. The program advocated in the guidance is one in which risks, vulnerabilities of digital IROFS, and consequences of their loss of compromise, and appropriate management measures are applied to ensure IROFS protection commensurate with the level of risk identified. On page 2 of the ISG, the statement is made that management measures may be applied in a graded manner, commensurate with the level of risk, to achieve the facility performance requirements. This concept will be reflected elsewhere within the document by providing additional guidance in the form of examples distinguishing between the level of risk reduction required for "sole IROFS" and that required for multiple redundant or diverse IROFS.</p> |
| NEI-4 | NEI Letter | <p>"..., it must be recognized that the health and safety consequences from a compromised system at a fuel facility are significantly much lower than those at a power reactor, and the guidance should reflect this reduced risk."</p>  | <p>During the development process it was recognized that the health and safety consequences from a compromised system at a fuel facility are lower than those at a power reactor. The guidance presented in this draft ISG reflects this reduced risk at fuel cycle facilities. On page 2 of the ISG, the statement is made that management measures may be applied in a graded manner, commensurate with the level of risk, to achieve the facility performance requirements. As stated in the NRC staff response to NEI-3 above, the NRC staff will provide additional guidance in the form of examples distinguishing between the level of risk reduction required for "sole IROFS" and that required for multiple redundant or diverse IROFS.</p>   |
| NEI-5 | NEI Letter | Third, the Draft ISG describes difficulties of   | The NRC staff does not believe that the draft ISG is  |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|       |            |   |   |
|-------|------------|---|---|
|       |            | demonstrating adequate systems but generally lacks practical and achievable solutions and clear and rational criteria for accepting systems in safety applications. In this regard, we are concerned that the Draft ISG is far too complex for the average NRC license reviewer, inspector, manager or some fuel facility management.   | too complex for the average NRC license reviewer, inspector, manager or some fuel facility management. Where the application of appropriate safety criteria to meet the facility performance objectives seems challenging to implement safely, alternative acceptable methods for achieving the facility objectives have been provided. However, to enable a more rapid understanding of the goals being achieved within each section, modifications to the ISG format will be made in the form of highlights or bullets depicting the key criteria being addressed.  |
| NEI-6 | NEI Letter | Further, and most importantly, the guidance forces DI&C systems to undergo a much higher level of scrutiny and demonstration of adequacy than many other systems and applications that are readily accepted today as meeting the applicable NRC regulations. We believe that this is an unfair burden for systems that have a far better track record of managing safety functions than many other systems relied on today. | NRC staff does not believe the level of scrutiny and demonstration of adequacy for DI&C systems in the draft ISG is higher than needed. 10 CFR Part 70 requires that management measures be applied to IROFS to ensure that they are designed, implemented, and maintained to ensure they are available and reliable when needed to perform their safety functions in the context of the facility performance objectives. The NRC staff is required to evaluate the applicant's proposed design, implementation, and maintenance criteria and programs to determine whether there is reasonable assurance that the applicant has provided appropriate measures to ensure IROFS will be available and reliable to perform their required safety actions when needed. |
| NEI-7 | NEI Letter | Industry disagrees however with the remaining Note language which states that this guide will also be applied to the "review and evaluation of proposed amendments to existing fuel cycle facilities, and the   | This comment is still under consideration by the NRC staff. When this item is resolved, the participants in the TWG-7 activities will be notified as to how the NRC staff intends to resolve this   |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|       |                                  |   |   |
|-------|----------------------------------|---|---|
|       |                                  | <p>review and evaluation of license renewal applications.” This approach is not consistent with industry’s understanding over the course of the guidance development process. Instead, industry suggests that this guide be applied to new licenses and amendments to existing licenses for new processes or previously un-reviewed control schemes that are submitted to NRC for approval after the effective date of the final staff DI&amp;C guidance.</p>   | comment.  |
| NEI-8 | Cyber Security - General Comment | <p>Page 3: The NRC should consider deleting the section and, instead, refer to NRC-issued orders that require licensees to perform cyber security. This approach would also address the issue of malevolent acts which are not part of a site specific Integrated Safety Analysis evaluation. For Part 70 Category 3 facilities, the cyber security in place to protect intellectual property and MC&amp;A information is adequate for protecting the IROFS.</p>  | <p>From the very first meeting of TWG-7 participants, it was elected to have a section within the TWG regarding cyber security. The NRC-issued security orders described in the comment were for facility protection, and do not provide guidance for the evaluation and protection of the availability and reliability of digital I&amp;C IROFS. The protection of the digital information systems used to store and reference intellectual property and to support MC&amp;A activities, do not provide adequate guidance for the evaluation and protection of digital process control systems within the facility that are required to accomplish safety actions. The NRC staff does not plan to delete this section, but will ensure that the identified good practices described within this guidance are consistent with Part 70 requirements.</p> |
| NEI-9 | Cyber Security - Discussion      | <p>Page 5, second paragraph: As stated, 10 CFR Part 70 requires licensees to implement management measures to ensure that digital assets performing safety functions or that support the performance of safety functions for the facility are continually protected. The guidance addresses performance goals, elements, and characteristics of management measures that could be used in fuel cycle facilities to provide reasonable assurance that the functions performed by digital safety equipment will be designed, implemented, and</p> | <p>The referenced standards describe a risk-management framework for protecting digital systems and assets within any type of facility, including nuclear facilities. Personnel who use these standards would make conclusions that recognize that fuel facilities have fewer risks and safety consequences than other types of facilities, but would nevertheless be performing an assessment of the assets, threats, and vulnerabilities for his facility, and would be</p>   |

|               |  |   |  |
|---------------|--|---|--|
|               |  | <p>maintained such that they are programmatically protected. Further, management measures should be implemented to ensure that effective cyber security provisions are in place to prevent cyber events from compromising the confidentiality, integrity, and availability of all IROFS.</p> <p>These standards appear to be taken from the guidance related to power reactor facilities. As stated previously, the level of risk for a fuel cycle facility is not commensurate with that of a reactor facility; therefore, different assumptions about the treatment for cyber security for fuel cycle facilities should be considered. Beginning with the discussion in paragraph b(2) and continuing through paragraph (g), the ISG appears to go beyond guidance for new applications and states new requirements: a cyber security plan, program, procedures, etc. are required for all licensees or applicants, regardless of need, and regardless of whether requesting licensing action of the NRC.</p> | <p>identifying security controls commensurate with the level of risk identified. The note at the bottom of page 2 of the ISG and a careful reading of paragraphs (b)(2) through (g) reveals that there are no new requirements for fuel cycle facilities, but instead, an acceptable set of management measures and good practices for review of designs, operations, and maintenance for ensuring that digital IROFS are protected in a programmatic manner. If the licensee or applicant chooses approaches other than those presented in this ISG, the licensee or applicant should identify the portions of its licensee application that differ from the good design practices and acceptance criteria contained within the ISG, and should demonstrate how the proposed alternatives provide an acceptable method of complying with the regulations.</p> |
| <p>NEI-10</p> | <p>Cyber Security - Staff Guidance</p> | <p>Page 8, second bullet: This item implies that the licensee must add dedicated personnel to monitor against cyber intrusion. At some fuel cycle facilities, computer personnel would be used for this purpose. Industry does not believe that NRC should determine what category of employee performs this task. Therefore, the bullet should be modified to remove this implication.</p>   | <p>As noted above, there are no new requirements for fuel cycle licensees indicated in this ISG. The statement on page 8 does not state that the personnel who perform the implementation of management measures for cyber security must exclusively work on cyber security program activities. The NRC staff will modify the wording as follows:</p> <p>"applying appropriate and sufficient qualified personnel resources within the facility whose responsibilities include the protection of facility safety functions against compromise by cyber events."</p>  |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|               |   |   |  |
|---------------|---|---|--|
| <p>NEI-11</p> | <p>Cyber Security -<br/>Technical Review<br/>Guidance</p> | <p>Page 12, first full paragraph, second sentence: The purpose of this sentence appears to redefine the ISA Summary. This appears to be outside the scope of defining cyber security requirements. It should be revised to indicate it is intended to refer only to cyber-security aspects of the ISA Summary or it should be relocated to the general introduction of the ISG.</p>   | <p>The NRC staff agrees that the paragraph, as written, is confusing. The staff proposes to revise the paragraph as follows:</p> <p>"The reviewer should use the guidance in this ISG to evaluate the adequacy of the applicant's License Application and ISA Summary. When reviewing the cyber security aspects of the application and ISA Summary, the reviewer should evaluate the applicant's proposed management measures to ensure that digital IROFS are designed, implemented, and maintained, as necessary, to ensure that they are available and reliable to comply with the facility performance requirements. The management measures proposed should be evaluated to confirm that appropriate cyber security practices, including those described herein, are applied to ensure the availability and reliability of digital IROFS by protecting them from the effects of cyber events."</p> |
| <p>NEI-12</p> | <p>Independence -<br/>General</p>                         | <p>Recommend changing the title of this section to "Independence of Controls used for IROFS".</p>   | <p>The NRC staff agrees with the comment. The title of this section will be changed to "Independence of Controls used for IROFS"</p>   |
| <p>NEI-13</p> | <p>Independence -<br/>General</p>                         | <p>Pages 14 –17: Discussions in this major section suggest a new level of granularity to the individual instrument. The last sentence of the first paragraph on page 17 suggests that when identical equipment or operator actions provide the necessary redundancy that all credible common-case failures have been identified and taken into account when estimating the reliability of the protective measure. Please clarify whether this language is intended to suggest that redundancy is not accomplished by identical equipment performing the same function or by two operators performing the same</p> | <p>The language in the discussion implies that redundancy of IROFS may be accomplished by identical equipment performing the same function and by two operators performing the same procedure. However, the IROFS may be considered independent when credible common-cause failures have been identified and taken into account when estimating the reliability of the protective measure. The NRC staff proposes to revise this statement by clarifying the intention that independence may only be credited for redundant</p>  |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|        |   |  |  |
|--------|---|--|--|
|        |   | procedure irrespective of configuration due to common cause concerns.  | IROFS when credible common-cause failures have been identified and taken into account.   |
| NEI-14 | Independence - Discussion                   | Page 16: Events and accident sequences are different. Events, especially initiating events, do not all have to be identified if the IROFS protect against the entire group of initiating events. For example, if an IROFS provides adequate protection in the event of the maximum credible flood, it does not matter how many specific events could cause the flood. In addition, NUREG-1520 allows for bounding of accident sequences.   | The NRC staff agrees with the comment. The discussion presented on Page 16 will be revised to address credible accidents sequences.  |
| NEI-15 | Independence - Double Contingency Principle | Page 17: This entire section should be removed from this document. This is a requirement that is reviewed and implemented by nuclear criticality specialists, not instrumentation and control specialists.   | The NRC staff believes that this section could be revised to address the important criteria for accomplishing any type of IROFS, regardless of whether it is a preventative function such as for criticality prevention, or mitigative for consequence reduction. The title of this section will be revised to be more generic, such as "Criteria for the Design of Preventative and Mitigative IROFS". The specific definitions applicable to double contingency will be removed and instead, references will be made to FCSS-ISG-03 where these definitions are described in greater detail. |
| NEI-16 | Independence - Double Contingency Principle | Page 19, bullet item 2: This item identifies a situation that may not result in two IROFS being independent from one another as the situation where two individuals use the same equipment or procedure. This seems to suggest that, for each system using an administrative control, two independent reviews using different procedures would have to occur for the reviews to be independent. This seems counter-intuitive because when an operator is performing an administrative procedure, such as calibrating a scale, a verification of the first operator's result is desirable. The ISG should | The NRC staff intended this list to be used as examples for assisting the reviewer in identifying important criteria to consider when evaluating independence of IROFS. The statement will be revised as follows:<br><br>"Administrative actions that are performed by two different individuals but using the same equipment."  |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|        |                               |   |  |
|--------|-------------------------------|---|--|
|        |                               | be revised to clarify what is intended by this bullet.  |  |
| NEI-17 | Independence - Staff Guidance | <p>Page 22, paragraph 2, "1E-6/year": This frequency meets the criteria for "not credible". If the likelihood of an accident sequence / initiating event is "not credible," it does not need to be considered. Additionally, if the risk acceptance criteria for an accident sequence is E-4, then a common failure causing the accident at anything less than or equal to E-4 should be considered acceptable.</p> | <p>The NRC staff believes the commenter is referring to the NRC staff's guidance for estimating event frequencies, which is contained in Chapter 3 of NUREG-1520, pp. 3-23 to 3-28. In general, event frequencies on the order of 1E-6/year fall into the category of "less than 1E-5 per year" which are considered "highly unlikely." The term "not credible" in the context of event frequencies would apply to estimates of external event frequencies which can conservatively be estimated to occur less than once in a million years.</p> <p>Within the context of DI&amp;C-ISG-07, a dependent credible common-cause failure contribution should be taken into consideration in evaluating the final risk reduction factor achieved by the proposed set of IROFS. These applied risk reduction factors associated with each IROFS are then taken into consideration when evaluating the resulting risk index following implementation of all risk reduction factors for that accident sequence. When using the risk index method, it should be demonstrated that the likelihood of common-cause dependent failure contribution should be sufficiently low that it does not change (or has minimal impact) on the index score for a system of IROFS. The NRC staff proposes to enhance the ISG through incorporation of a figure depicting an example event tree analysis illustrating the principle of what happens to the estimate of overall risk reduction factor for a set of IROFS, when the dependent common cause failure contribution is sufficiently small.</p> |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|               |  |   |  |
|---------------|--|---|--|
| <p>NEI-18</p> | <p>Independence - Staff Guidance</p>   | <p>Page 22, paragraph 2, last sentence: One order of magnitude is more than adequate. A common mode failure of 1E-4 would, in a qualitative sense, still meet the acceptance criteria. If the risk acceptance criteria is E-4 for an accident, then a common failure of the IROFS at anything less than or equal to E-4 should be considered acceptable—likewise, if the risk acceptance criteria is E-5, then anything less than or equal to E-5 should be acceptable.</p> | <p>The acceptance criteria of “two orders of magnitude or smaller” originated in Interim Staff Guidance document FCSS-ISG-01. DI&amp;C-ISG-07 was written to be consistent with this guidance. FCSS-ISG-01 states that if the cumulative likelihood of all common-mode failures of a system of IROFS is significantly less than the independent failure of the system of IROFS, then the IROFS may be treated for all practical purposes as independent. Quantitatively, this means the likelihood of the common-cause failure should be at least two orders of magnitude less than that of the independent failure of the system of IROFS. Qualitatively, this means the likelihood of the common-cause failure should be sufficiently low that it does not change the score for the system of IROFS.</p> |
| <p>NEI-19</p> | <p>Independence - Software CCFs Considerations</p>   | <p>Page 25, paragraph 3: “there is evidence that 100% of the time...” It is recommended that NRC change the wording regarding “100%” to address credible failure modes. As long as the PFOD or failure frequency credited is maintained, 100% fail safe is not required.</p>  | <p>The NRC staff proposes to change the sentence to read:</p> <p>“In order to make this argument, however, one must have had previous knowledge that for the type of software fault that occurred, there is sufficient evidence that the logic outputs will all change to the “faulted conditions” or “safe states” intended in the design.”</p>   |
| <p>NEI-20</p> | <p>Independence - Evaluation of Vendor-Identified Digital Control System Failure Alert Notices</p> | <p>Page 27, sentence one: Delete “applied for use in safety applications”. The licensee should evaluate controls/instrumentation notifications for their impact on IROFS.</p>   | <p>The NRC staff proposes to delete the words indicated in the comment, and point out that prior to completing the design of digital systems used as IROFS, and after actual implementation of such systems, licensees should evaluate vendor product alerts or notices for their impact on proposed IROFS.</p>  |

|               |   |  |   |
|---------------|---|--|---|
| <p>NEI-21</p> | <p>Independence-Implementation of Safety Control System</p> | <p>Page 27: This section implies that all IROFS related controls are third-party rated. It must be made very clear that third-party rated safety controls shall only be required for the following:</p> <ul style="list-style-type: none"> <li>▪ An accident sequence that has a sole IROFS that is an active engineered control.</li> <li>▪ An accident sequence that has multiple IROFS that rely on the same control system (non-independent).</li> <li>▪ IROFS that required operation during and/or after an incident or do not fail safe.</li> </ul> | <p>The intent of this section on page 27 of the Draft ISG is to provide guidance to reviewers of applications in which third-party certified systems have been proposed, and there is no implication that all IROFS related controls are third party certified. The guidance provided within this section is that if an applicant has proposed the use of such systems for IROFS, the reviewer should look for evidence that the applicant has verified that his implementation of such a system is consistent with the third-party certifier's boundary conditions identified within the certification statement or "safety manual." The NRC staff has not established specific conditions for when the use of such systems is warranted. In general, applicants should apply measures to select the quality level for controls that is commensurate with the level of risk reduction attributable to the IROFS. The NRC staff will revise the first sentence in this paragraph to be clear that such third party certified safety control systems are considered acceptable for use in some IROFS applications, commensurate with the degree of risk reduction needed to prevent or mitigate an event sequence.</p> |
| <p>NEI-22</p> | <p>Independence-Implementation of Safety Control System</p> | <p>The safety evaluation of the PLC should be based on proper configuration and/or installation of the hardware, proper use of software/hardware watchdogs, use of communication "Heartbeats" where applicable, and proper implementation of fault detection and response. This section is clearly excessive for systems with independent controller for each IROFS.</p>   | <p>As stated above, there is no implication that every IROFS should make use of third-party certified safety controllers. Each IROFS must be designed, implemented, and maintained to ensure that the IROFS will be available and reliable when needed. The section regarding the use of safety controllers was incorporated to allow NRC staff reviewers to recognize applications where licensees have chosen to implement safety controllers in the context of IEC 61508/61511 and ISA S84.00 design criteria, which is allowable for use in fuel cycle facility applications, but is not a Part 70</p>  |

|               |   |  |   |
|---------------|---|--|---|
|               |   |  | <p>requirement. The NRC staff has agreed to clarify that this methodology is allowable, but is not a requirement.</p>   |
| <p>NEI-23</p> | <p>Digital Communications<br/>- General</p> | <p>This section implies requirements relevant to 10 CFR 50 requirements for commercial nuclear reactors. The safety risks at part 70 facilities do not require this level of rigor on communications systems. The scheme presented implies completely separate safety and process systems. This is not a standard controls scheme at a part 70 facility. The communications protocols and error checking provided by high end process control systems will meet all of the requirements necessary for IROFS. A more rigorous communications review would be required for the following type of situations:</p> <ul style="list-style-type: none"> <li>▪ An accident sequence that has a sole IROFS that is an active engineered control.</li> <li>▪ An accident sequence that has multiple IROFS that rely on the same control system (non-independent).</li> <li>▪ IROFS that required operation during and/or after an incident or do not fail safe.</li> </ul> <p>Isolation of safety and process controls would have a significant impact on human factors related to how an operator interacts with the process and alarm/interlock situations.</p> | <p>The guidance presented describes a method for maintaining isolation and separation between safety controls and non-safety controls, so that the safety controls are protected from adverse interactions, failures, or faults arising within the non-safety portions of the circuitry. It does not advocate completely separate systems.</p> <p>The code requires that each item relied on to accomplish safety functions in the context of the facility performance requirements be designed, implemented, and maintained to ensure that the item is available and reliable when needed. This requires that any HMI station used in the accomplishment of safety functions also be designed, implemented, and maintained to ensure this availability and reliability requirement. The guidance provided in this ISG describes criteria which could be incorporated to protect the portion of the system accomplishing safety actions from the portion that achieves non-safety actions.</p> <p>NRC staff recognizes that there are potential human factors benefits for the use of control stations that incorporate data originating within both safety and non-safety local controls. The NRC staff will enhance this section by incorporating clarifying text that provides guidance for reviewers indicating that licensees or applicants may utilize a risk-informed approach, based on level of risk reduction needed.</p> |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|               |  |   |   |
|---------------|--|---|---|
| <p>NEI-24</p> | <p>Software Quality<br/>- General</p>                          | <p>Most references and requirements are all based on part 50 requirements with the key reason being common mode failures. Common mode failures are only an issue if:</p> <ul style="list-style-type: none"> <li>▪ An accident sequence that has a sole IROFS that is an active engineered control.</li> <li>▪ An accident sequence that has multiple IROFS that rely on the same control system (non-independent).</li> </ul> <p>IROFS that required operation during and/or after an incident or do not fail safe.</p> | <p>The guidance presented describes a high quality software method for minimizing software failures in safety systems, in order to provide reasonable assurance that the safety systems are protected from all potential credible common-cause failures of a system of IROFS. The NRC staff will enhance this section by incorporating clarifying text that provides guidance for reviewers indicating that licensees or applicants may utilize a risk-informed approach, based on level of risk reduction needed.</p> <p>Not all of the guidance provided in this section pertains to the development of high quality software. Some of the guidance is provided pertains to the methodology for ensuring that high quality digital systems are procured for use in safety applications. The NRC staff plans to modify the title of this section to reflect this.</p>                            |
| <p>NEI-25</p> | <p>Software Quality<br/>- High-Quality<br/>Software Design</p> | <p>Page 42: Industry does not agree with the statement that software functioning cannot be tested after initial installation. On the contrary, management measures are in place to verify stimulus to response testing on a regular frequency (preventative maintenance (PM) program) and issue tracking systems are in place to react to any abnormal finding during operations or PM's. Reference to common mode failure only applies to multiple IROFS for a given accident sequence in one system.</p>              | <p>The section cited does not state that software functioning cannot be tested after initial installation. Rather, it states that it is prudent that the software be initially of a high quality to provide assurance that the facility objectives can be met. Stimulus-to-response testing can help to identify the proper functioning of the expected responses from the control system to the applied stimuli only. Usually, such testing is performed by defining test conditions for stimuli that approximate a subset of only the most likely process conditions anticipated to be present when the safety function is required, and usually this testing is applied in steps, in a sequential manner. Such testing is usually not detailed enough to simulate the full range of credible modes of operation, the possible external influences or combinations of postulated faulted or</p> |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|        |   |   |   |
|--------|---|---|---|
|        |   |   | <p>upset ambient or process conditions that could occur during the life of the facility. Unless such testing is performed in such a fashion that simulates all possible combinations of anticipated operational occurrences for a fuel cycle facility safety application, one cannot conclude that all possible results of the system response have been verified. Therefore, it is prudent that the software development process be conducted in such a quality manner that provides reasonable assurance that the controller will achieve its safety functions so that facility performance requirements will be met under all credible conditions.</p> |
| NEI-26 | Software Quality - High-Quality Software Design | <p>Page 44: Regarding the four items listed by level of risk, Item 3 is not currently required by SIL certification companies to have the PC based software verified in order to certify a PLC for specific SILs. The PC based software that is provided by the PLC vendor is an engineering environment that contains the toolsets that are used to create the instructions used by the PLC firmware. The engineering environment should not be considered as part of the safety basis for the system, since this tool is only used during configuration and/or testing of the system.</p> | <p>The NRC staff does not agree with the comment that the tool sets used to create the instructions and to perform maintenance or configuration changes do not have to be verified. If the tool set contains an error that provides an incorrect software code to be downloaded into the PLC, then that error will be introduced every time changes are made to the software functions implemented by the PLC, which is undesired. The engineering tool's compiler affects the safety design basis for the system each time it is used to make such changes.</p>  |
| NEI-27 | Software Quality - High-Quality Software Design | <p>References to "Commercial Grade Dedication" should be removed from this section as this is a software QA section and Commercial Grade Dedication is typically related to hardware. It should also be noted that NQA-1 Part II, Subpart 2.7 Section 302 discusses the requirements for acquired software that was not developed using a standard for its intended application. The acceptable documentation required is demonstrating that the limitations and capabilities of the intended use are tested and bounded. There is no</p>   | <p>This section of the ISG regarding commercial grade dedication is based on acceptance processes that specifically address digital systems, including their software. The section of the ISG regarding ANSI/NQA-1-2008 does not require that vendors provide a second-party certification for the configuration software. It requires that the limitations and capabilities of the software intended for use are tested and bounded. (See p. 47, 5<sup>th</sup> paragraph.)</p>  |

NRC Staff Disposition of NEI's Comments on the Interim Staff Guidance DIC-ISG-07

|  |  |   |   |
|--|--|---|---|
|  |  | requirement to have the vendor provide a second-party certification for the configuration software. | However, as described in the NRC staff response to NEI-24 above, the NRC staff plans to augment the text in this section to indicate that high quality digital systems may be identified for applications requiring a high level of risk reduction using such processes as commercial grade dedication. |
|--|--|---|---|