Staff Perspective on Concerns Raised With Design Acceptance Criteria

Summary

In a letter dated August 9, 2010, the Advisory Committee on Reactor Safeguards (ACRS) made two conclusions and recommendations. In addition, the letter raised concerns regarding design acceptance criteria (DAC) proposed for use in the current applications under review by the U.S. Nuclear Regulatory Commission (NRC). Like the August 9, 2010, letter, this discussion will focus on the use of DAC for digital instrumentation and controls (DI&C).

The following describes the staff's perspective on the use of DAC:

- The Commission's policy on DAC, and the NRC staff's implementation of that policy, has been consistent for nearly 20 years in terms of definition, and the role of DAC in the overall licensing and construction process, and the ramifications of their use are well understood.

- When viewed in isolation, especially in DI&C systems, DAC as written may appear insufficient to make the required safety finding. When viewed in the broader context of all the information used by the staff in making its safety finding (e.g., the design control document, reference technical reports, and approved topical reports), the approach used for DAC is sufficient.

- DI&C DAC have unique attributes. The DI&C systems are likely to change during both the life of the certification and throughout operation, unlike much of the facility. Therefore, in the case of DI&C, the current regulatory approach enables safe reactor operations by establishing the safety functions and limiting conditions of the design during certification while allowing implementation changes to occur as technology evolves.

- For the certified designs and some of the designs currently under review, the staff was able to make a safety finding with the use of DAC and less design detail in the final safety analysis report (FSAR). However, other designs that are highly interconnected and rely on software to protect redundant components would require a more complete design to make the safety finding. In these cases, DAC may not be necessary since the designs would need to be complete in order to resolve all safety issues. As a result, these designs may require more resources during the certification review, during the life of the certification, and throughout the life of the facility for applicants, licensees, and the NRC.

Design Acceptance Criteria Policy

The NRC initially developed the policy for DAC in 1992, and all four designs certified between 1997 and 2006 have used DAC, as do all design certifications currently under review. The agency has periodically reaffirmed the viability of the DAC concept and the implementation of DAC through numerous Commission papers and memoranda and staff requirements memoranda dating back to 1992 and as recently as 2008.

ENCLOSURE

The use of DAC was narrowed from the original four areas to three. The original DAC included radiation protection, piping, control room (now human factors engineering), and DI&C. Radiation protection was only used in the Advanced Boiling Water Reactor design. The extent or number of DAC used varies by application, is largely at the discretion of the applicant, and reflects the degree of design completion in each of the three areas. In general, while DAC are still used, the applications under review use DAC to a lesser extent than the certified designs.

DAC have consistently been defined as "a set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies, in a limited number of technical areas, in making a final safety determination to support a design certification." In terms of what constitutes an acceptable DAC, the policy has been that "DAC are to be objective (measurable, testable, or subject to analysis using pre-approved methods)." Last, a measure of the collective acceptability of the DAC is that the DAC "need to be sufficient for the staff to conclude that any additional design detail developed after the design certification, which satisfies those criteria, would not alter the staff's safety conclusion."

To summarize DAC policy:

- DAC should be objective.

- A design certification, including one that relies on DAC, represents a final safety determination with respect to the design.

- Additional design detail developed after the design certification that satisfies the acceptance criteria will not alter the staff's safety conclusion.

The definition and role of DAC as described may give the impression that the safety finding at the certification stage relies exclusively on the DAC. This is not the case; the NRC makes the safety finding based on the entire application, and DAC are one part of that safety finding. The DAC are important because they provide the methods by which an acceptable detailed design will be created.

The use of DAC allows less design detail in the application. While additional design information aids in understanding how the system operates, the additional information would not change the safety basis for which the certification was granted. Conceptually, the additional detailed information would not affect when license amendments are required, as that more fundamental information is required in the FSAR under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 52, Section 52.47. In effect, the FSAR serves as an interface between the licensee and the NRC that establishes the boundary between changes permitted without prior NRC approval and those requiring license amendments.

This process is no different than for licenses issued under 10 CFR Part 50. Pursuant to 10 CFR Part 50, in which a final implemented design is reflected in the FSAR and included in the licensing review, licensees can subsequently change the design under 10 CFR 50.59. This regulation uses the updated FSAR as the basis for comparing those changes permitted without NRC approval, and those requiring license amendments. As in 10 CFR Part 52, under 10 CFR Part 50, the information that triggers a license amendment is a subset of the information in the updated FSAR and is likely similar to the type of information necessary to include in an FSAR under 10 CFR Part 52 that uses DAC.

The licensing basis can be changed prior to DAC closure provided the appropriate change management process is followed, which depends on whether the affected information is in Tier 1, Tier 2*, or Tier 2. Regardless of what detailed design results from the processes in DAC, the resultant design must still meet the licensed design, as modified.

Although DAC allow for less design information to be provided, the applications include substantial detail. To provide some context on the information reviewed to support the safety finding, the following information was reviewed for the DI&C systems of a representative application:

- The design control document (DCD), Tier 1, contains about 150 DAC in 50 pages.

- Chapter 7 of the DCD is more than 500 pages, and incorporates by reference, five topical reports totaling about another 500 pages. Chapter 7 provides the information required by 10 CFR 52.47, which is basically the same information required for an FSAR under 10 CFR Part 50.

- The NRC issued about 400 requests for additional information for DI&C, about 300 specific to Chapter 7, and 100 related to DI&C inspections, tests, analyses, and acceptance criteria (ITAAC).

- The staff received numerous other pieces of correspondence from and held many meetings with the applicant.

Reviewing this information required about 15,000 staff hours and resulted in development of an approximately 250 page safety evaluation report that summarizes the staff's review and provides the basis for the staff's conclusion that the proposed design, with DAC, meets the regulations.

DAC create flexibility for the designer, and a variety of different detailed designs could be shown to meet DAC for a given certification. When the agency created the concept of DAC, the staff expected that "economic considerations will likely prompt all subsequent combined license (COL) holders to make their final designs identical to the first unless major technical advances prompt consideration of a design change." For DI&C, change is possible during both the life of the certification and throughout operation of the facility, and less standardization should be expected in terms of the detailed design.

Implementation of Design Acceptance Criteria Policy for Digital Instrumentation and Control

The agency's practice for the last 15 years has been to use process-oriented DI&C DAC. This approach works when taking into consideration the entire process. All the certified designs, and all the certification applications under review, use DAC for the DI&C systems to varying degrees. DI&C DAC may be unique for three reasons: (1) the way in which the NRC has implemented the DAC policy is unique, (2) the flexibility in detailed design allowed by DAC may be the desired approach for DI&C, and (3) the viability of DI&C DAC is dependent on the level of design completion necessary to demonstrate that essential design principles are met.

DI&C DAC are almost exclusively procedures and attributes, although they may be better described as processes (e.g., hardware and software development process). These processes

have flexibility in their implementation. Even though numerous detailed design implementations may satisfy a given set of DAC, those implementations must conform to the licensing basis. Further, even though the DAC resemble processes, the processes used in DI&C DAC apply well-understood methods, standards, and best practices that experts use to reliably create high quality designs. Process-type DAC may be preferable to specific DAC, because DI&C is an area where technology continues to change. A downside to this practice is that these types of DI&C DAC can appear ambiguous when read in isolation.

Since the DI&C system may change during both the life of the certification and operations, too much specificity in the DAC may be counterproductive. As Tier 1 information, the change process is exemptions or amendments to the certification. If the details are retained in the FSAR as practiced, the more flexible departure route is available. To illustrate this concern, in both the current reviews that involve already-certified designs, the AP1000 amendment and the South Texas Project (STP) COL application, changes to the DI&C were requested from the previously certified information due to new technology being available.

A more recent observation is that DAC for DI&C may be restricted to designs where the essential design principles (e.g., redundancy, independence, determinant data processing and communication, and defense-in-depth and diversity) can be specified in functional block diagrams with a relatively short design description in the FSAR, and verified by objective ITAAC regardless of implementation technology (i.e., analog or digital). In this case, use of DAC may be appropriate to confirm that the design bases and limits on operations for the DI&C system described in the FSAR have been properly implemented. Even though the DAC allow flexibility in design, the detailed design developed will not alter the staff's safety conclusion, as required.

For highly interconnected systems that rely on software to protect against potential undesirable interactions among redundant components, it is more difficult for the applicant to demonstrate the safety basis without providing more details on the design. In this case, the detail necessary in the FSAR for the staff to make its safety finding would be those software features that provide the necessary protection. Depending on the type of interconnections, in some cases this information would be the actual implemented algorithms or source code. Given the significance of this information to the staff's safety finding, such information would likely be Tier 2* - the information predetermined to require a license amendment.

These systems will need a nearly complete design such that there may be no need for DAC; there would only be ITAAC. While the elimination of DAC as a result of more complete design information may be perceived as an advantage, it has the disadvantage of requiring substantially more information to be included in the FSAR, and likely much more detail in Tier 2*. This approach will result in a more resource-intensive regulatory framework during the certification review, during the life of the certification, and throughout the life of the facility for applicants, licensees, and the NRC.

Specific Issues Raised in the ACRS Letter

The staff reviewed the August 9, 2010, letter from ACRS and identified five areas of additional concerns and expectations highlighted by the ACRS. This section provides the staff's perspective based on its interpretation of the positions described in the letter. The parentheses include the page of the letter where the staff identified the issues described.

a. *It is difficult to assure an adequate design, while substantial DAC remain open* (page 2)

The safety finding is based on the controlling parameters and design information contained in the FSAR plus the processes contained in the DAC. The DAC can remain open since the design that results from the DAC processes will not alter the staff's safety conclusion.

b. *Detailed design information enhances safety* (page 3)

Detailed design information, that is, information beyond that required to satisfy 10 CFR 52.47 with process-type DAC, is useful in that it provides a better understanding of how the design to be implemented will work and how it meets requirements. This additional information does not change our safety finding. It is expected that this detailed information reflects those aspects of the design that the licensee could later change.

c. *DAC should be more specific and the number of DAC should be minimized* (page 4)

Including detailed and specific DAC is an alternative approach to the agency's practice for DI&C DAC. Under the current approach, these details reside in the FSAR. Including those details in the DAC descriptions results in a more restrictive regulatory process that could stifle innovation in an area where change is expected over the life of the certification because the details would be in Tier 1. Thus, exemptions from the certified design would be needed for future COL applicants, with no safety benefit. In both the AP1000 amendment and the STP COL application, changes to the DI&C were requested from the previously certified information due to new technology being available. In both cases, the desired changes were to the Tier 2 information.

d. *Some of the essential design principles…must be confirmed as implemented in the final design of the DI&C systems* (page 5)

All design principles in accordance with agency requirements need to be addressed during certification. The design to be implemented as a result of the processes in DAC is confirmed against the acceptance criteria and must be consistent with the licensing basis. For highly interconnected DI&C systems that rely on software to protect against potential undesirable interactions among redundant components, the implementation information would likely need to be part of the certification review and such systems may not need DAC.

e. *Many current DI&C DAC are not technically unambiguous and process-oriented. No DCD has developed DAC that have the level of depth and clarity needed to ensure successful conformance with the design by simple inspection* (page 5)

The agency's practice has been to allow DAC that are process-oriented and technology neutral, and the staff continues to believe that this approach works. Having a sound licensing review process that focuses on the importance of having a clear and complete FSAR, combined with a thorough construction inspection process that employs the right level of expertise with the right scope and depth of evaluation, are what ultimately ensures a safe design implementation. The agency never expected DAC to be closed through simple inspection, i.e., checklists. Qualified inspectors, with the right level of expertise and technical background, would lead the efforts and would be supported by qualified agency personnel. Expert judgment combined with the adequate inspection procedures and complete FSARs support the thorough evaluation by the agency to confirm that the key design features of the design have been properly implemented.