C.III.5. Design Acceptance Criteria

As defined in SECY-92-053, dated February 19, 1992, design acceptance criteria (DAC) are "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." The DAC are objective (measurable, testable, or subject to analysis using pre-approved methods), and must be verified as part of the inspections, tests, analyses, and acceptance criteria (ITAAC) performed to demonstrate that the as-built facility conforms to the certified design.

The policy of accepting the use of DAC in lieu of providing detailed design information in a limited number of design areas was implemented as requested by the design certification applicants and on a case-by-case basis. DAC have been utilized in the four already-certified designs in the areas of radiation protection (ABWR), piping (ABWR, System 80+, and AP1000), instrumentation and controls (I&C) (ABWR, System 80+, AP600, and AP1000), and human factors engineering (ABWR, System 80+, AP600, and AP1000). The reasons for allowing the use of DAC were that (1) providing detailed design information was not desirable due to utilization of technologies that change so rapidly that the design may have become obsolete between the time the design was certified and the time a plant was eventually built (e.g., digital I&C systems and human factors engineering), and (2) completing the final design was impractical given the unavailability of sufficient as-built, or as-procured information (e.g., in the shielding and piping areas).

Utilizing the approach of limited use of DAC along with sufficient other detailed design information, the NRC staff reached a final conclusion on all safety questions on the certified designs as required by 10 CFR 52.47 (a)(2). To reach this conclusion, the applicants proposed and the NRC staff reviewed, approved, and certified sufficient ITAAC to ensure the DAC will be met during construction by the licensee prior to loading fuel.

C.III.5.1 *Detailed Design Information and the Combined License Application*

The staff recommends, to the greatest extent practicable, that the COL applicant include detailed design information in the areas where DAC was used during the design certification. This information should be submitted early enough in the process to allow the NRC staff sufficient time to review the information and determine compliance with the DAC and associated ITAAC. Early submission of such information should help avoid potential impacts on the licensee's plans and schedules for loading fuel. The COL applicant should identify those design areas where detailed information cannot be provided and supply the NRC a schedule for completion of detailed engineering, procurement, fabrication, installation, and testing. This also should be done in a manner to support timely NRC inspection of DAC information.

The path to successfully satisfying DAC and completing the associated ITAAC may include review of information or procedures that occur early in the construction, fabrication, or development processes that may necessitate early involvement by NRC inspectors and staff, e.g., in development of reactor protection system software. For this reason, it is crucial that the NRC staff have timely access to detailed design information to resolve any potential issues.

Furthermore, the use of DAC has the potential to increase the likelihood of post-construction hearing petitions and to expand the scope of a hearing, if it occurs. While the staff and a licensee may agree at various points during construction that DAC are met, compliance with DAC, including those intended to be verified early in the construction process, can be the subject of a hearing just prior to operation. This is another reason for the COL applicant to submit and/or make available for inspection, early in its application, the detailed design information in the areas in which DAC was used in the design certification. (Note: Recognizing that this regulatory guide is primarily intended for the use of COL applicants, design certification applicants may also wish to utilize this guidance with respect to the advantages of submitting sufficiently detailed design information at the time of design certification.)

Although numerous detailed design configurations may satisfy a given set of DAC, the staff expects standardization of the design in keeping with the letter and intent of 10 CFR Part 52. This will also support the NRC's design-centered review approach (DCRA) to licensing as discussed in Regulatory Issue Summary (RIS) 2006-06, dated May 31, 2006. Deviations to standardization may challenge this proposed "one issue, one review, one position" approach.

Consistent with RIS 2006-06, the DCRA will focus on those designs in which potential COL applicants have expressed interest. At the time of the publication of DG-1145, these designs include the ABWR and AP1000 certified designs, as well as the ESBWR which is in the design certification review phase, and the EPR which is in the design certification pre-application review phase. Only the ITAAC of the ABWR and AP1000 have been certified. As such, the following information is applicable.

C.III.5.1.1 Information Necessary to Verify Completion of Instrumentation and Controls Design

Due to the use of DAC during the design certification review stage, the digital I&C system design was not completed. The NRC staff was able to reach a final conclusion on the designs by relying on the DAC. To ensure the validity of the safety conclusion for the I&C portion of the certified design, a COL applicant should submit where feasible sufficiently detailed design information in the areas where DAC was used. The digital I&C system design development process, as documented in the certified design's design control document (DCD), should be addressed to the greatest extent possible in the COL application. If not practical to submit during the COL application, the applicant should identify those areas and provide a schedule to the NRC as to when the information will be available for NRC review. The staff will confirm the COL applicant's implementation of this process through the ITAAC at various phases of the design development. Complying with the DAC and satisfactorily completing the associated ITAAC will provide the necessary assurance that the I&C system has been designed, tested, and operated in accordance with the certified design. The guidance for I&C design process ITAAC development is addressed in Section C.II.2. Following is a list that the staff believes is necessary for a COL application to demonstrate that the implementation of the I&C system design process has complied with the DAC and the ITAAC:

(1) Identify all I&C-related ITAAC related to areas that used DAC in the certified design

(2) Describe the implementation process for both hardware and software of I&C system life cycle design processes (stages) in the COL application.

(3) Provide reference documents related to the I&C design process planning documents from the referenced certified design. The typical software life cycle process planning documents include the following:

- software management plan
- software development plan
- software test plan
- software quality assurance plan
- integration plan
- installation plan
- maintenance plan
- training plan
- operations plan
- software safety plan
- software verification and validation plan
- software configuration management plan

(4) Provide implementation documents on which the I&C system design is based for each design stage. Typical software life cycle process design implementation documentation includes the following:

- safety analyses
- verification and validation analysis and test reports
- configuration management reports
- requirement traceability matrix
- one or more sets of these reports should be available for each of the following activity groups: requirements, design, implementation, integration, validation, installation, operations, and maintenance

(5) Provide information confirming that the I&C system design life cycle implementation is based on the life cycle plans in the referenced DCD. Provide the life cycle activities output documents at the completion of each life cycle stage in accordance with the ITAAC in the referenced DCD. Typical software life cycle process design outputs documentation includes the following:

- The conformance of the requirement document and hardware and software specifications to the functional requirements identified in the DCD of the referenced Certified Design.
- A sample of software design outputs should be provided to confirm that they address the functional requirements allocated to the software, and that the expected software development process characteristics are evident in the design outputs.
- The system test procedures and test results (validation tests, site acceptance tests, pre-operational and start-up tests) that provide assurance that the system functions as intended.
- The application should confirm that Defense-in-Depth and Diversity design conforms to the guidance of SRP Chapter 7, BTP 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."
- The application should confirm that digital safety system security guidance is in conformance with or commits to NRC Regulatory Guide 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."

- software requirements specifications (SRS)
- hardware and software architecture descriptions
- software design specifications (SDS)
- code listings
- build documents
- installation configuration tables
- operations manuals
- maintenance manuals
- training manuals

(6) Provide information that demonstrates Equipment Qualification in the following areas:

- Computer System Testing: Computer system qualification testing should be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, should be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the central processing unit, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing should demonstrate that the performance requirements related to safety functions have been met.
- Qualification of Existing Commercial Computers: EPRI TR-106439 "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," and the Safety Evaluation approving this topical for reference should be used as guidance. The dedication process for the computer should entail identification of the physical, performance, and development process requirements necessary to provide adequate confidence that the proposed digital system or component can perform its required safety function(s). The dedication process shall apply to the computer hardware, software, and firmware that are required to accomplish the safety function. The dedication process for software and firmware should include an evaluation of the design process.

(7) Provide information (such as test procedures or reports) that demonstrate capability for testing and calibration of safety system equipment.

The capability for testing and calibration of safety system equipment during power operation and the periodic testing should duplicate, as closely as practicable, performance required of the safety function should be provided. Testing of Class 1E systems should be in accordance with the requirements of IEEE Std 338-1987. The test should confirm operability of both the automatic and manual circuitry. The capability should be provided to permit testing during power operation. When this capability can only be achieved by overlapping tests, the test scheme must be such that the tests do, in fact, overlap from one test segment to another. Test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment during power operation should be avoided. A sample test procedure should be provided to demonstrate this capability.

(8) Provide information (such as test procedures or component layout drawings) that demonstrate the Information Displays capability.

The information displays for manually controlled actions should include confirmation that displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary. Safety system bypass and inoperable status indication should conform with the guidance of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

(9) Provide information (such as administration procedures or room layout drawings) that demonstrate the Control of Access.

The COL application should confirm that design features provide the means to control physical access to protection system equipment, including access to test points and means for changing setpoints. Typically such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located. The digital computer-based systems should consider controls over electronic access to safety system software and data. Controls should address access via network connections, and via maintenance equipment.

(10) Repair provision

Digital safety systems may include self-diagnostic capabilities to aid in troubleshooting. The COL application should describe the characteristics of the digital computer-based diagnostic capabilities.

(11) Identification provision

The COL application should address equipment identification provision. Guidance on identification is provided in RG 1.75, "Criteria for Independence of Electrical Safety Systems," which endorses IEEE Std 384, "Standard Criteria for Independence of Class 1E Equipment and Circuits." The preferred identification method is color coding of components, cables, and cabinets. For computer-based systems, the configuration management plan should describe for maintaining the identification of computer software.

(12) Human factors considerations

Safety system human factors design should be consistent with the applicant's commitments documented in Chapter 18 of the COL application.

(13) Demonstrate automatic control capability

The COL application should include analysis to confirm that the safety system has been qualified and demonstrate that the performance requirements are met. The evaluation of the precision of the protection system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. For digital computer-based systems, the application document should confirm that the general functional requirements have been appropriately allocated into hardware and software requirements. The application document should also confirm that the system's real-time performance is deterministic and known.

(14) Demonstrate manual control capability

The COL application should include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified) during plant conditions under which manual actions may be necessary. Features for manual initiation of protective action should conform with RG 1.62, "Manual Initiation of Protection Action."

(15) Interaction Between the Sense and Command Features and Other Systems

The COL application should confirm that non-safety system interactions with protection systems are limited such that the requirements of 10 CFR 50 Appendix A, GDC 24, "Separation of Protection and Control System," are met. Where the event of concern is single failure of a sensing channel shared between control and protection functions, previously accepted approaches have included:

- isolating the protection system from channel failure by providing additional redundancy
- isolating the control system from channel failure by using data validation techniques to select a valid control input
- designing the communications path to be a broadcast only from the protection system to the control system

(16) Derivation of System Inputs

For both direct and indirect parameters, the applicant should verify that the characteristics (e.g., range, accuracy, resolution, response time, sample rate) of the instruments that produce the protection system inputs are consistent with the analysis provided in Chapter 15 accident analyses of the COL application. A safety system that requires loss of flow protection would, for example, normally derive its signal from flow sensors (a direct parameter). An indirect flow indication design might use a parameter such as a pressure signal or pump speed. In selecting an indirect parameter, the COL application should verify that the indirect parameter is a valid representation of the desired direct parameter for all events.

(17) Setpoint determination

The COL application should confirm that an adequate margin exists between operating limits and setpoints, such that there is a low probability for inadvertent actuation of the system. The application document should include an analysis to confirm that an adequate margin exists between setpoints and safety limits, such that the system initiates protective actions before safety limits are exceeded. Regulatory Guide 1.105, "Setpoint for Safety-Related Instrumentation," provides guidance for setpoint determination.

(18) Identify the I&C design process that deviates from or does not comply with the DAC of the referenced certified design. Any modification to, addition to, or deletion from the DAC should follow the change process in Section VIII of the respective design certification rule (10 CFR Part 52, Appendix A through D, as applicable).

C.III.5.1.2 Information Necessary to Verify Completion of Human Factors Engineering Design

To ensure the validity of the safety conclusions for the HFE portion of the certified design, a COL applicant should, where practicable, submit and/or make available for inspection sufficiently detailed design information in the HFE-related areas where DAC was used. The HFE design development process, as documented in the certified design control document (DCD), should be addressed in the COL application. The staff will confirm the COL applicant's implementation of the process through the ITAAC at various phases of design development and implementation. Complying with the DAC and satisfactorily completing the associated ITAAC will provide the necessary assurance that the human systems interfaces (HSI) have been designed, tested, and implemented in accordance with the certified design and that the COL applicant has a satisfactory HFE program. The guidance for HFE design process ITAAC development is addressed in Section C.II.2. The COL applicant should address the following information to demonstrate that the implementation of the HFE design process has complied with the DAC and ITAAC.

For each element listed in NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, February 2004, that has not been completed as part of the certified design referenced by the COL, the COL is encouraged to submit, as part of its application, information to successfully complete those elements not resolved as part of the certified design. For those DAC-related elements that the COL does not complete in its combined license application, the COL should provide implementation plans including schedule. The implementation plans should be developed with a level of detail that will allow the COL to ensure ITAAC can be successfully completed and verified.

C.III.5.1.3 Information Necessary to Verify Completion of Piping Design

Completed design reports for piping and supports, satisfying the design criteria specified in Section C.1.3.12 of this DG should be made available for NRC review.

C.III.5.1.4 Information Necessary to Verify Radiation Protection Design

Completed design reports for radiation protection, satisfying the design criteria specified in Section C.1.12 of this DG should be made available for NRC review.

C.III.5.2 *ABWR DAC-related ITAAC*

Design Area	ITAACs Associated with DAC (DCD, Tier 1 Information)
Human Factors Engineering (DCD Tier 1, Section 3.1)	Table 3.1, 1 through 7
Radiation Protection (DCD Tier 1, Section 3.2)	Table 3.2a, 1 and 2
Piping (DCD Tier 1, Section 3.3)	Table 3.3, 1 through 3
Instrumentation and Control (DCD Tier 1, Section 3.4)	Table 3.4, 1 through 16

C.III.5.3 *AP1000 DAC-related ITAAC*

Design Area	ITAACs Associated with DAC (Tier 1 Information)
Piping (DCD Tier 1, Section	Tables 2.1.2-4, 2 through 4 and 5b); 2.2.1-3, 2 through 4; 2.2.2-3, 2 through 4 and 5b); 2.2.3-4, 2 through 4 and 5b); 2.2.4-4, 2 through 4 and 5b); 2.2.5-5, 2 through 4 and 5b); 2.3.2-4, 2 through 4; 2.3.6-4, 2 through 4 and 5b); 2.3.7-4, 2 through 4; 2.3.10-4, 2 through 4 and 5b); 2.3.13-3, 2 through 4
Instrumentation and Control (DCD Tier 1, Section 2.5.1)	Table 2.5.1-4, 1 through 4
Human Factors Engineering (DCD Tier 1, Section 3.2)	Table 3.2-1, 1 through 13

C.III.5.4 ***References***

(1) 10 CFR Part 52, "Early Site Permits: Standard Design Certifications: and Combined Operting Licenses for Nuclear Power Plants"

(2) NUREG-1503, "Final Safety Evaluation Report Related to the Certification of the ABWR Design," July 1994

(3) NUREG-1462, "Final Safety Evaluation Report Related to the Certification of the System 80+ Design," August 1994

(4) NUREG-1512, "Final Safety Evaluation Report Related to the Certification of the AP600 Standard Design," September 1998

(5) NUREG-1793, "Final Safety Evaluation Report Related to the Certification of the AP1000 Standard Design," September 2004 (ADAMS Accession No. ML043450274)

(6) SECY 92-053, "Use of Design Acceptance Criteria During 10 CFR Part 52 Design Certification Reviews," dated February 19, 1992 (ADAMS Accession No. ML)

(7) SECY 92-196, "Development of Design Acceptance Criteria for the Advanced Boiling-Water Reactor (ABWR)," dated May 28, 1992

(8) SECY 92-299, "Development of Design Acceptance Criteria for the Advanced Boiling-Water Reactor (ABWR) in the Areas of Instrumentation and Control (I&C) and Control Room Design," dated August 27, 1992

(9) SECY 02-059, "Use of Design Acceptance Criteria for the AP1000 Standard Plant Design," dated April 1, 2002 (ADAMS Accession No. ML013310041)

(10) U.S. ABWR Design Control Document, GE Nuclear Energy, Revision 4, dated March 1997

(11) System 80+ Design Control Document, ABB-CE, with revisions dated January 1997

(12) AP600 Design Control Document (December 1999 Revision)

(13) AP1000 Design Control Document, Revision 15, dated December 8, 2005