C.III.5 Design Acceptance Criteria

As defined in SECY-92-053, 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 preapproved methods) and must be verified as part of the ITAAC used to demonstrate that the as-built facility conforms to the certified design.

The NRC implemented the policy of accepting the use of DAC in lieu of detailed design information in a limited number of design areas on a case-by-case basis, as requested by the design certification applicants. The four already-certified designs used the DAC in the areas of radiation protection (ABWR), piping (ABWR, System 80+, and AP1000), I&C (ABWR, System 80+, AP600, and AP1000), and HFE (ABWR, System 80+, AP600, and AP1000). The NRC allowed the use of DAC because (1) providing detailed design information was not desirable for applicants using technologies that change so rapidly that the design may have become obsolete between the time the agency certified the design and the time a plant was eventually built (e.g., digital I&C systems and HFE) 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).

Using 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. To enable the agency to reach this conclusion, the applicants proposed and the NRC staff reviewed, approved, and certified sufficient ITAAC to ensure that the licensee will meet the DAC during construction prior to loading fuel.

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

The NRC staff recommends, to the greatest extent practicable, that the COL applicant include detailed design information in the areas where DAC were used during the design certification. The applicant should submit this information early enough in the process to allow the NRC staff sufficient time to review it 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 should supply the NRC with a schedule for completion of detailed engineering, procurement, fabrication, installation, and testing information. The applicant should similarly do this in a manner to support timely NRC inspection of DAC information.

The path to successfully satisfying the 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.

Although numerous detailed design configurations may satisfy a given set of DAC, the NRC 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 RIS 2006-06, "New Reactor Standardization Needed To Support the Design-Centered Licensing Review Approach," dated May 31, 2006. Deviations from standard designs or practices used to satisfy DAC may challenge the NRC's goal to implement its "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 this regulatory guide, these designs included the ABWR and AP1000 certified designs as well as the Economic Simplified Boiling-Water Reactor, which is in the design certification review phase, and the EPR, which is in the design certification preapplication review phase. As such, the following information is applicable.

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

Because of 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 were used. To the greatest extent possible, the COL application should address the digital I&C system design development process, as documented in the certified design's DCD. If it is not practical to submit this information 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. Section C.II.1 of this guide addresses the guidance for I&C design process ITAAC development. The NRC staff believes that the following is necessary for a COL application to demonstrate that the implementation of the I&C system design process has complied with the DAC and ITAAC:

(1) Identify all I&C-related ITAAC corresponding 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 QA 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, which should be available for requirements, design, implementation, integration, validation, installation, operations, and maintenance activities

(5) Provide information confirming that implementation of the I&C system design life cycle 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 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, preoperational and startup tests) that provide assurance that the system functions as intended
- confirmation that the defense-in-depth and diversity design conforms to the guidance of SRP BTP 7-19
- confirmation that digital safety system security guidance conforms with, or commits to, RG 1.152, Revision 2
- software requirements specifications
- hardware and software architecture descriptions
- software design specifications
- code listings
- build documents
- installation configuration tables
- operations manuals
- maintenance manuals
- training manuals

(6) Provide information that demonstrates equipment qualification in the following areas:

- Applicants should perform computer system qualification testing with the computer functioning with software and diagnostics that are representative of those used in actual operation. Testing should exercise all portions of the computer necessary to accomplish safety functions or those portions whose operation or failure could impair safety functions. This includes, as appropriate, exercising and monitoring the memory, 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.

- For the qualification of existing commercial computers, applicants should use the guidance in EPRI TR-106439 and the safety evaluation approving this topical for reference. 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 functions. 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 demonstrates capability for testing and calibration of safety system equipment.

The capability for testing and calibration of safety system equipment during power operation and periodic testing should duplicate, as closely as practicable, the performance required of the safety function. 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 applicant should provide the capability 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 performing other similar modifications of the installed equipment during power operation should be avoided. Applicants should provide a sample test procedure 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.

(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 the equipment identification provision. RG 1.75 which endorses IEEE Std. 384 provides guidance on identification. The preferred identification method is color coding of components, cables, and cabinets. For computer-based systems, the

configuration management plan should describe procedures 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 application should address the evaluation of the precision of the protection system 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.

(15) Interaction between the sense and command features and other systems.

The COL application should confirm that nonsafety-system interactions with protection systems are limited such that the requirements of GDC 24 of Appendix A to 10 CFR Part 50 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 the following:

- 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 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 the 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. RG 1.105 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 (Appendices A through D to 10 CFR Part 52, 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 on the HFE-related areas where DAC were used. The COL application should address the HFE design development process, as documented in the certified DCD. 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 have been designed, tested, and implemented in accordance with the certified design and that the COL applicant has a satisfactory HFE program. Section C.II.1 of this guide addresses the guidance for HFE design process ITAAC development. The COL applicant should address the information described below to demonstrate that the implementation of the HFE design process has complied with the DAC and ITAAC.

For each element listed in NUREG-0711, Revision 2, that has not been completed as part of the certified design referenced by the COL, the staff encourages the COL applicant 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 applicant does not complete in its COL application, the applicant should provide implementation plans, including schedule. The applicant should develop the implementation plans with a level of detail that will allow the COL to ensure that ITAAC can be successfully completed and verified.

C.III.5.1.3 ***Information Necessary To Verify Completion of Piping Design***

Applicants should make available for NRC review completed design reports for piping and supports that satisfy the design criteria specified in Section C.I.3.12 of this guide.

C.III.5.1.4 ***Information Necessary To Verify Radiation Protection Design***

Applicants should make available for NRC review completed design reports for radiation protection that satisfy the design criteria specified in Section C.I.12 of this guide.

C.III.5.2 ABWR DAC-Related ITAAC

Design Area	**ITAACs Associated with DAC (DCD, Tier 1 Information)**
HFE	(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
I&C	(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, various sections) 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
I&C	(DCD Tier 1, Section 2.5.1) Table 2.5.1-4, 1 through 4
HFE	(DCD Tier 1, Section 3.2) Table 3.2-1, 1 through 13