EDO Principal Correspondence Control

FROM: DUE: 09/30/10 EDO CONTROL: G20100516
DOC DT: 08/09/10
FINAL REPLY:

Said Abdel-Khalik, ACRS

TO:

Chairman Jaczko

FOR SIGNATURE OF : ** GRN ** CRC NO: 10-0368

Borchardt, EDO

DESC:

Closure of Design Acceptance Criteria for New Reactors (EDATS: SECY-2010-0410)

ROUTING:

Borchardt
Weber
Virgilio
Mamish
OGC/GC
Sanfilippo,OEDO

DATE: 08/10/10

ASSIGNED TO: CONTACT:

NRO Johnson

SPECIAL INSTRUCTIONS OR REMARKS:

Please prepare response to ACRS for the signature of the EDO. Add the Commission and SECY as cc's. Also, include: RidsAcrsAcnw_MailCTR Resource to your distribution on the concurrence page. USE SUBJECT LINE IN THE RESPONSE.

TEMPLATE: SECY-017 E-RIDS: SECY-01

EDATS

Electronic Document and Action Tracking System

EDATS Number: SECY-2010-0410 **Source:** SECY

General Information

Assigned To: NRO **OEDO Due Date:** 9/30/2010 11:00 PM

Other Assignees: **SECY Due Date:** NONE

Subject: Closure of Design Acceptance Criteria for New Reactors

Description:

CC Routing: NONE

ADAMS Accession Numbers - Incoming: NONE **Response/Package:** NONE

Other Information

Cross Reference Number: G20100516, LTR-10-0368 **Staff Initiated:** NO

Related Task: **Recurring Item:** NO

File Routing: EDATS **Agency Lesson Learned:** NO

OEDO Monthly Report Item: NO

Process Information

Action Type: Letter **Priority:** Medium

Sensitivity: None

Signature Level: EDO **Urgency:** NO

Approval Level: No Approval Required

OEDO Concurrence: NO

OCM Concurrence: NO

OCA Concurrence: NO

Special Instructions: Please prepare response to ACRS for the signature of the EDO. Add the Commission and SECY as cc's. Also, include: RidsAcrsAcnw_MailCTR Resource to your distribution on the concurrence page. USE SUBJECT LINE IN THE RESPONSE.

Document Information

Originator Name: Said Abdel-Khalik **Date of Incoming:** 8/9/2010

Originating Organization: ACRS **Document Received by SECY Date:** 8/10/2010

Addressee: Chairman Jaczko **Date Response Requested by Originator:** NONE

Incoming Task Received: Letter

OFFICE OF THE SECRETARY
CORRESPONDENCE CONTROL TICKET

Date Printed: Aug 10, 2010 13:07

PAPER NUMBER:	LTR-10-0368	**LOGGING DATE:**	08/10/2010
ACTION OFFICE:	EDO		

AUTHOR:	Said Abdel-Khalik
AFFILIATION:	ACRS
ADDRESSEE:	CHRM Gregory Jaczko
SUBJECT:	Closure of Design Acceptance Criteria for New Reactors
ACTION:	Appropriate
DISTRIBUTION:	RF
LETTER DATE:	08/09/2010
ACKNOWLEDGED	No
SPECIAL HANDLING:	
NOTES:	
FILE LOCATION:	ADAMS

DATE DUE: **DATE SIGNED:**

EDO --G20100516

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

August 9, 2010

The Honorable Gregory B. Jaczko
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: CLOSURE OF DESIGN ACCEPTANCE CRITERIA FOR NEW REACTORS

Dear Chairman Jaczko:

During the 574th meeting of the Advisory Committee on Reactor Safeguards (ACRS), July 14-16, 2010, we discussed the closure of Design Acceptance Criteria (DAC) for new reactors. We had the benefit of discussions with representatives of the U.S. Nuclear Regulatory Commission (NRC) staff and a member of the public. We also had the benefit of the documents referenced.

CONCLUSIONS AND RECOMMENDATIONS

1. DAC closure requires expertise, judgment, and interpretation. It should be performed by NRC staff experts with an independent assessment by the ACRS.

2. It is preferable that all DAC be resolved no later than the Combined License (COL) stage. However, whether resolved as part of the COL process or post-COL, proper closure of DAC requires a consistent scope and depth of evaluation in accord with our first recommendation.

BACKGROUND

Conformance with a certified nuclear power plant design under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," is verified through Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC). When practicalities forced the submission of less-than-complete designs, the staff developed the concept of a special kind of ITAAC called DAC to permit certification by replacing elements of the design with acceptance criteria that could be confirmed later. We have been involved in discussions of DAC with the staff and the Commission since this concept was first introduced nearly 20 years ago. We have also been closely following the evolution of the DAC concept and its application to design certification. In our July 24, 2009, report on Regulatory Guide (RG) 1.215, "Guidance for ITAAC Closure under 10 CFR Part 52," we discussed our current concerns with the DAC closure process, particularly for digital instrumentation and control (DI&C).

During an Advanced Boiling Water Reactor (ABWR) Subcommittee meeting on May 20, 2010, the staff clarified its position on DI&C DAC emphasizing three points:

1. The staff recognizes the importance of DI&C and intends to address concerns raised by the ACRS.

2. Review and approval of DI&C systems is a licensing activity and needs to be done as part of the design certification and COL processes, not as part of field inspections. The staff has experience with trying to inspect safety and quality into systems in the field, and it doesn't work well.

3. The staff, ACRS, and Commission have struggled with DI&C for more than a decade. Since it is difficult to conclude that a DI&C system is without flaws, the NRC's current approach is to assure a quality design and also require a diverse, independent, and reliable backup protection system.

We appreciate the staff's first point and acknowledge the third, although we think that it is difficult to assure an adequate design, while substantial DAC remain open. Regarding the second point, the staff encouraged us to make safety findings on DI&C at the design certification stage, or, if necessary, at the COL stage and not try to use the inspection process as a second level of review. However, a final safety determination requires assurance that DAC have been properly closed. If this is not done in the COL stage, it must be done in the post-COL stage but the scope and depth of the evaluation of the DAC closure should be the same in either case.

The Statements of Consideration (SOC) for 10 CFR Part 52 states that early site permit, design certification, and COL processes do not eliminate any material safety issue from consideration; they just move their resolutions to earlier review stages. The fundamental principle is that the NRC cannot allow operation of a nuclear power reactor unless all material safety issues are resolved. The introduction of DAC under 10 CFR Part 52 effectively shifts some of the uncertainty to later in the regulatory process.

Since the issuance of 10 CFR Part 52, the staff and Commission have recognized that judgment would be required to ensure that some ITAAC actually provide assurance that the design has been safely implemented, i.e., that no material safety issue goes unreviewed. The SOC for Part 52 states:

> The Commission does not believe that it is prudent to decide now, before the Commission has even once gone through the process of judging whether a plant built under a combined license is ready to operate, that every finding the Commission will have to make at that point will be cut-and-dried-proceeding according to highly detailed "objective criteria" entailing little judgment and discretion in their application, and not involving questions of "credibility, conflicts, and sufficiency"

DAC are clearly among those ITAAC for which judgment will be required in order to reach a finding that the acceptance criteria have been satisfied.

DISCUSSION

History of DAC

The historical development and evolution of the DAC concept provides important context for decisions in the current environment—an environment with four certified designs, five design certification applications under review, and 13 COL applications under active review.

The concept of DAC was discussed in SECY-92-053, "Use of Design Acceptance Criteria during 10 CFR Part 52 Design Certification Reviews," which was prepared in response to the Staff Requirements Memorandum (SRM) dated November 7, 1991. It had become clear that vendors were not providing detailed design information in some areas because (1) some technologies were changing so rapidly that it would be unwise for the NRC to freeze the details of the design many years before an actual plant is ready to be constructed, and (2) there were design areas such as pipe stress and support analyses, where vendors did not have sufficient as-built or as-procured information to complete the final design. At that time, it was unclear when new plant orders might be placed.

SECY-92-053 defined DAC as a set of prescribed limits, parameters, procedures, and attributes in a limited number of technical areas. DAC were intended to be objective (measurable, testable, or subject to analysis using pre-approved methods) and were to be sufficiently detailed to provide an adequate basis for the staff to make a final safety determination regarding the design. SECY-92-053 acknowledged that DAC would result in less design detail and more reliance on analysis methods, performance tests, and inspections. It further recognized that "although there is nothing in Part 52 which would necessarily limit the use of DAC, the staff believes that the use of DAC should be limited." It noted that "restrictions should be based upon a consideration of those design areas affected by rapidly changing technologies, or design areas for which as-built, or as-procured, information is not available."

SECY-92-053 also noted that "the applicant should minimize the use of DAC to reduce the potential for systems interactions" and that "the staff will require applicants to identify possible systems interactions which result from the use of DAC."

Our February 14, 1992, report supported the DAC approach for limited applications and stated the following:

> We believe that carefully defined limits relating to scope and extent of design coverage should be placed on the use of DAC by the staff. We recommend that the use of DAC be limited to that portion of each given design feature where either the technology is still evolving (e.g., certain portions of the plant instrumentation and control or control room design) or the required information is unavailable for good reason. In any case, DAC should be used only when it is possible to specify practical and technically unambiguous criteria.

This report also noted that DAC can hide unforeseen systems interactions that might be uncovered if an actual design were available. Finally, our report stated that "if DAC are employed extensively in lieu of design detail, this would place an additional design burden on the COL holder and create a possible discontinuity in the design and review process that may be adverse to safety."

The ACRS formed an Ad Hoc Subcommittee on DAC in response to a Commission SRM issued on April 1, 1992. We agreed with the staff on the content of the ABWR DAC for radiation protection, piping design, and control room design (now part of human factors engineering). DI&C DAC were more troublesome. Our letter report dated October 16, 1992, closes with a theme that is still a concern for us:

> Finally, we are concerned about the significant number of post-design certification activities associated with these two DACs – control room design, and instrumentation and controls. The COL applicant or holder will be responsible for carrying out these activities. This will involve extensive future negotiations with the staff. It will also have the effect of diminishing the value of certified designs and seems to us to be contrary to the spirit of 10 CFR Part 52. We believe that the argument that these DACs represent areas of rapidly changing technology is being overplayed by both the staff and GE in justifying the extent to which the DAC process is being used.

In a November 13, 2007, SRM, the staff was directed to submit recommendations to the Commission on ways to reduce future use of DAC for designs not yet certified. The staff responded to this SRM in a memo to the Commission, "Evaluation of Potential Recommendations to Reduce the Future Use of Design Acceptance Criteria," dated May 6, 2008. This memo states that "with or without the use of DAC, the staff will ensure that...the application will contain a level of design information sufficient...to reach a final conclusion on all safety questions associated with the design before the certification is granted." Despite this assertion, for current DAC, evaluation of DAC closure requires expertise, judgment, and interpretation, and should include an independent assessment by the ACRS.

For future design certifications we urge the staff to require better specification of design acceptance criteria and to minimize the number of DAC.

Expectations

Our expectations have consistently been: (1) DAC would be limited to the extent possible and generally closed by the time of COL issuance; (2) for DAC to be closed after COL issuance and before fuel load, staff evaluation of the inspections, tests, and analyses used to close DAC would be thorough; and (3) we would be involved in an independent assessment of the staff's evaluation of DAC closure, at least for the first few applications.

Observations

DI&C systems for new designs are highly integrated, probably more so than imagined 20 years ago. The DI&C system is pervasive, affecting nearly all plant equipment. Unanticipated failure modes could create very confusing situations that could place the plant or lead operators to place the plant in unexpected or unanalyzed configurations.

The fundamental reliability of DI&C systems is based on four essential objective design principles—redundancy, independence, determinant data processing and communication, and defense-in-depth and diversity—and one subjective attribute, simplicity. The logic and hierarchy of DI&C designs are well established, as are the individual digital component technologies for implementing these functional system designs. Thus, the design of DI&C systems can be functionally specified and shown to meet the essential criteria regardless of the parts technology (digital and analog electronic components) used in developing the designs of the hardware assemblies and sub-assemblies.

Some of the essential design principles (e.g., multiple redundant divisions and defense in depth) can be specified in functional block diagrams in the Design Control Document (DCD) and

verified by objective ITAAC. Others, such as, redundant interdivision independence, determinant data processing within each division from plant parameter input to control/trip device actuation, and interdivision communication protocols that do not compromise division independence, must be confirmed as implemented in the final design of the DI&C systems. Notwithstanding the ability to eliminate many DI&C DAC from design certifications or COL applications, most are not planned to be resolved until after COL issuance.

Many current DI&C DAC are not technically unambiguous. No DCD has developed DAC that have the level of depth and clarity needed to ensure successful conformance with the design by simple inspection. To illustrate why expertise and judgment are required in evaluating DAC closure, consider the following example. One DAC calls for a Failure Modes and Effects Analysis (FMEA) per NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," of safety-related protection system platforms to be completed to validate the Diverse Protection System. The acceptance criterion is only that a report exists and concludes that the FMEA has been successfully completed. This criterion is inadequate. To pass, it only requires that a report exists and concludes success. There are no criteria for reviewing the analysis. A meaningful inspection requires expertise in FMEA and keen judgment to ensure that the analysis is complete and properly implemented.

Only careful review of detailed designs can identify unusual aspects of a design that are vulnerable to common cause and other dependent failure mechanisms. During development of the "Reactor Safety Study" (WASH-1400), engineers from the aerospace industry brought fault tree analysis to the project. Their experience had been that the use of fault tree analysis invariably uncovered many system weaknesses. They were quite surprised by the high reliability of nuclear power plant systems; it was well outside their experience in other industries. Good design and rigorous single failure analysis, with careful review by NRC staff, was exceptionally successful. Such techniques only work for complete designs.

Many DI&C DAC are process oriented. Process is important in ensuring a consistent high quality approach to design. It is possible to have substance (a good design) without a formal process. Such success is highly dependent upon the skill, competence, and expertise of the designer. Even so, the lack of process often permits holes in design detail and leads to inconsistencies. Process, however, does not guarantee success. Only an evaluation of the complete design can reveal the intricacies of possible interactions and failures.

Post-COL approval of DI&C DAC has never been done and no clear guidance for NRC approval of the closure process currently exists. Thus, there is no history of operating experience following post-COL DAC closure to confirm that the process is effective in ensuring adequacy of the final design. When operating properly, DI&C systems can provide operational flexibility and improved safety; however, potential degraded conditions of these systems could offer new challenges to operators.

Path Forward

COL reviews nearing completion are focusing attention on the use of DAC. With so many DAC positioned to pass through the COL stage in current applications, we have a growing concern that our long-held expectations may not be met.

We are following the work of the staff's Task Working Group on DAC closure to monitor their progress in developing effective inspection procedures.

We look forward to working with the staff to resolve these significant technical issues.

Sincerely,

/RA/

Said Abdel-Khalik
Chairman

References:

1. SECY-92-053, "Use of Design Acceptance Criteria During 10 CFR Part 52 Design Certification Reviews," 02/19/1992 (ML003707942)

2. SECY 90-377, "Requirements for Design Certification Under 10 CFR Part 52," 11/8/1990 (ML003707889)

3. SECY-90-377, "Requirements for Design Certification Under 10 CFR Part 52," 02/05/1991 (ML003781628)

4. SECY-02-059, "Use of Design Acceptance Criteria for the AP1000 Standard Plant Design," 04/01/2002 (ML013310041)

5. WASH-1400, "Reactor Safety Study – An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," 10/01/1975 (ML072350618)

6. Letter to Ivan Selin, Chairman, "Second Interim Report on the Use of Design Acceptance Criteria Process in the Certification of the GE Nuclear Energy Advanced Boiling Water Reactor Design, 10/16/1992 (ML051680301)

7. Staff Requirements-Periodic Briefing on New Reactor Issues, 9:30 A.M. and 1:30 P.M., Wednesday, October 24, 2007, Commissioners' Conference Room, One White Flint North, Rockville, Maryland (Open to Public attendance)", 11/13/2007 (ML073180039)

8. Memorandum to Chairman Klein and Commissioners Jaczko, Lyons, and Svinicki, "Evaluation of Potential Recommendations to Reduce the Future Use of Design Acceptance Criteria," 05/06/2008 (ML080420294)

9. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," 12/31/1994 (ML071790509)

10. Regulatory Guide (RG) 1.215, "Guidance for ITAAC Closure Under 10 CFR Part 52," 10/31/2009 (ML091480076)

11. Letter to Ivan Selin, Chairman, "Use of Design Acceptance Criteria during 10 CFR Part 52 Design Certification Reviews," 02/14/1992 (ML051750347)

12. Staff Requirements – Periodic Meeting with the Advisory Committee on Reactor Safeguards (ACRS), 2:00 P.M., Thursday, March 5, 1992, Commissioners' Conference Room, One White Flint North, Rockville, Maryland (Open to Public Attendance), 04/01/1992 (ML003771229)

13. Statements of Consideration (SOC) for the final 10 CFR Part 52 (54 FR 15372, April, 1989, pg 15381) (ML003711593)

14. Staff Requirements – Briefing on Staff Recommended Course of Action on Adhering to 10 CFR Part 52, 2:00 P.M., Thursday, October 17, 1991, Commissioners' Conference Room, One White Flint North, Rockville, Maryland (Open To Public Attendance), 11/07/1991 (ML010100406)

11. ACRS Letter to Ivan Selin, Chairman, "Use of Design Acceptance Criteria during 10 CFR Part 52 Design Certification Reviews," 02/14/1992 (ML051750347)

12. SRM "Staff Requirements – Periodic Meeting with the Advisory Committee on Reactor Safeguards (ACRS), 2:00 P.M., Thursday, March 5, 1992, Commissioners' Conference Room, One White Flint North, Rockville, Maryland (Open to Public Attendance)," 04/01/1992 (ML003771229)

13. Statements of Consideration (SOC) for the final Part 52 (54 FR 15372, April, 1989, pg 15381) (ML003711593)

14 SRM "Staff Requirements – Briefing on Staff Recommended Course of Action on Adhering to 10 CFR Part 52, 2:00 P.M., Thursday, October 17, 1991, Commissioners' Conference Room, One White Flint North, Rockville, Maryland (Open To Public Attendance)," 11/07/1991 (ML010100406)

Distribution:
See next page

Accession No:ML102000425 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☐ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	CSantos	EHackett	EHackett for SAbdel-Khalik
DATE	8/6/10	8/6/10	8/9/10	8/9/10	8/9/10

OFFICIAL RECORD COPY

Letter to the Honorable Gregory B Jaczko, Chairman, NRC, from Said Abdel-Khalik, Chairman, ACRS, dated August 9, 2010

SUBJECT: CLOSURE OF DESIGN ACCEPTANCE CRITERIA FOR NEW REACTORS

Distribution:
ACRS Staff
ACRS Members
B. Champ
A. Bates
S. McKelvin
L. Mike
J. Ridgely
RidsSECYMailCenter
RidsEDOMailCenter
RidsNMSSOD
RidsNSIROD
RidsFSMEOD
RidsRESOD
RidsOIGMailCenter
RidsOGCMailCenter
RidsOCAAMailCenter
RidsOCAMailCenter
RidsNRROD
RidsNROOD
RidsOPAMail
RidsRGN1MailCenter
RidsRGN2MailCenter
RidsRGN3MailCenter
RidsRGN4MailCenter