

September 8, 2005

MEMORANDUM TO: ACRS Members

FROM: Eric A. Thornsby, ACRS Senior Staff Engineer 

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE
ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION &
CONTROL SYSTEMS, JUNE 14-15, 2005 - ROCKVILLE,
MARYLAND

The minutes of the subject meeting, issued July 21, 2005, have been certified as the official record of the proceedings of that meeting. A copy of the certified minutes is attached.

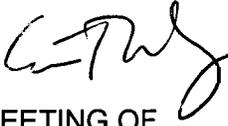
Attachment: As stated

electronic cc: J. Larkins
A. Thadani
M. Scott
S. Duraiswamy
M. Snodderly

PREDECISIONAL

July 21, 2005

MEMORANDUM TO: George E. Apostolakis, Chair
Digital Instrumentation & Control Systems Subcommittee

FROM: Eric A. Thornsbury, ACRS Senior Staff Engineer 

SUBJECT: WORKING COPY OF THE MINUTES OF THE MEETING OF
THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION
& CONTROL SYSTEMS, JUNE 14-15, 2005 - ROCKVILLE,
MARYLAND

A working copy of the minutes for the subject meeting is attached for your review. Please review and comment on them. If you are satisfied with these minutes, please sign, date, and return the attached certification letter.

Attachment: Minutes (DRAFT)

cc: Digital Instrumentation & Control Systems Subcommittee Members
T. Kress
J. Larkins
A. Thadani
M. Scott
S. Duraiswamy
M. Snodderly

MEMORANDUM TO: Eric A. Thornsby, ACRS Senior Staff Engineer

FROM: George E. Apostolakis, Chair
Digital Instrumentation & Control Systems Subcommittee

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE
ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION &
CONTROL SYSTEMS, JUNE 14-15, 2005 - ROCKVILLE,
MARYLAND

I do hereby certify that, to the best of my knowledge and belief, the minutes of the subject meeting on June 14-15, 2005, are an accurate record of the proceedings for that meeting.


George E. Apostolakis
Subcommittee Chair

9/8/05
Date

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MEETING OF THE ACRS SUBCOMMITTEE ON
DIGITAL INSTRUMENTATION & CONTROL SYSTEMS
MEETING MINUTES - JUNE 14-15, 2005
ROCKVILLE, MARYLAND

INTRODUCTION

The ACRS Subcommittee on Digital Instrumentation & Control Systems held a meeting on June 14-15, 2004, in Rooms T-2B1 & T-2B3, 11545 Rockville Pike, Rockville, MD. The purpose of this meeting was to review the status of the draft Digital Systems Research Plan, projects from two sections of the plan, and work related to a draft Regulatory Guide. The meeting was open to public attendance. Mike Snodderly was the Designated Federal Official for this meeting. Eric Thornsburly was the cognizant staff engineer. There were no written comments or requests for time to make oral statements from the public. The meeting was convened by the Subcommittee Chair at 8:30 a.m. on June 14, 2005, recessed at 5:02 p.m., reconvened at 1:31 p.m. on June 15, 2005, and adjourned at 5:23 p.m..

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chair
M. Bonaca, Member
T. Kress, Member

J. White, Consultant
S. Guarro, Consultant
M. Snodderly, Designated Federal Official
E. Thornsburly, Cognizant Staff Engineer

Principal NRC Speakers

W. Kemper, RES
G. Tartal, RES
S. Arndt, RES
H. Hamzehee, RES
S. Morris, NSIR

M. Waterman, RES
N. Carte, RES
R. Shaffer, RES
T. Hilsmeier, RES

Other Principal Speakers

J. Calvo, NRR
C. Grimes, NRR
T. Chu, BNL
R. Torok, EPRI

R. Barrett, RES
M. Li, UMD
T. Aldemir, OSU

Other members of the public were present at this meeting. A complete list of attendees is in the ACRS Office File and will be made available upon request. The presentation slides and handouts used during the meeting are attached to the office copy of these minutes.

OPENING REMARKS BY CHAIR

George Apostolakis, Chairman of the ACRS Subcommittee on Digital Instrumentation & Control Systems, convened the meeting at 8:30 a.m.. Dr. Apostolakis stated that the purpose of this meeting was to discuss the NRC staff's Draft Digital Systems Research Plan, the staff's approach to revising Regulatory Guide 1.97, and two specific research programs discussed in the plan: software quality assurance and the risk assessment of digital systems. He said the Subcommittee would gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee. The rules for participation in the meeting were announced as part of the notice of the meeting published in the Federal Register on May 31, 2005. Dr. Apostolakis acknowledged that no written comments or requests for time to make oral statements had been received from the public.

DISCUSSION OF AGENDA ITEMS

Reconciliation of Comments on Draft Research Plan

William Kemper, RES, introduced the presenters the Subcommittee would be hearing and stated that the objective of the meeting was to brief the Subcommittee on various topics contained within the draft research plan. Mr. Kemper commented on the proactive communications with NRR, NSIR, and NMSS to improve the research plan. He then introduced Mr. Michael Waterman to discuss the resolution of comments on the research plan.

Mr. Waterman discussed the goal to make the research plan a "living document" that will be updated in response to communications with the supported offices as new needs are identified. The major focus of the research plan is to augment and supplement the agency's existing process, such as those in the Standard Review Plan. The purpose of the research is to investigate current and emerging methods and knowledge and, where appropriate, augment and supplement NRC processes to enable NRC staff to evaluate digital systems consistently and effectively. The Office of Research is also trying to incorporate informal comments from NRR into the plan. Mr. Waterman then reviewed the public comments and their resolution section-by-section through the research plan.

Mr. Jose Calvo of NRR also asked to make comments regarding the research plan. He first described the current way NRR performs reviews – to review the process and not the product. They then can perform audits to make sure the system performs consistently. He also discussed the recent reviews the staff has done. He stressed the idea of the offices getting together to discuss the research plan and working out differences. Disagreements still exist, but the offices are moving closer.

Mr. Evangelos Marinos of NRR also added comments regarding the current Standard Review Plan issued in 1997 and the upcoming review of a submittal from Oconee, which will be a good test of the current process. The staff has also monitored international use of the standard review plan process in Taiwan and South Korea. Mr. Marinos believes that concurrence by the NRR/EEIB branch would have constituted a user need request, where the staff did not feel one was necessary. However, the staff does support anticipatory research. Mr. Calvo recommended that the Committee get involved with the upcoming Oconee review.

Mr. Richard Barrett, RES Division Director, commented on the various processes by which RES gains user-office support for research programs. They are sometimes more proactive and do not necessarily wait for user needs from the other offices. Mr. Christopher Grimes, NRR deputy division director, commented on the focus on process improvements, the need for constructive comments from NRR, and the use of TAGs to facilitate ongoing communication.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. White asked about the use of metrics to evaluate the research effectiveness. Mr. Waterman responded that the office has internal reviews of programmatic effectiveness to accomplish this purpose, and that it might be a good topic for a supplemental document.
- Dr. Apostolakis asked about the use of Technical Advisory Groups (TAGs). Mr. Kemper answered that they are examining the use of TAGs, and would likely use one TAG with all offices included (NRR, NMSS, and NSIR).
- Dr. Apostolakis suggested that RES get input from the other offices regarding their urgent needs to help prioritize the work.
- Dr. Apostolakis asked how operating experience, both nuclear and non-nuclear, is being used to develop the plan. Mr. Kemper commented how they are examining operating experience. Different systems in different industries are qualified to different levels of quality, and that is being taken under consideration as they examine operating experience.
- Dr. Apostolakis commented on how the state of digital systems review is similar to the whole regulatory structure from 40 or 50 years ago, where the application of risk assessments found holes in the traditional approaches and improved the overall process.
- Dr. Bonaca commented on the resistance to developing risk-informed approaches in other disciplines, much like here. He commented that often, research such as this must be viewed more long-term than your immediate needs.

Draft Revision of Reg Guide 1.97

Mr. Kemper introduced the session on the draft Revision 4 to Regulatory Guide 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants." The regulatory guide is a work in progress, and the staff asked the Subcommittee for informal comments on the approach. Mr. Kemper described the new regulatory guide's endorsement of IEEE Std. 497-2002, which describes a new approach to identifying post-accident monitoring instrumentation. The new revision has broader guidance to accommodate non-light-water reactors and other advanced reactor designs. He then introduced Mr. George Tartal to lead the presentation.

Mr. Tartal provided a brief background on the history of accident monitoring, then discussed the current revision, Rev. 3 of Reg Guide 1.97. Then he provided a brief overview of IEEE Standard 497-2002, a revised standard for the selection, performance, design, qualification,

display, and quality assurance criteria for accident monitoring. Mr. Tartal then described the draft guide, DG-1128, focusing on the regulatory positions and the issues the staff addressed in trying to endorse the IEEE standard.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Bonaca commented on the less-prescriptive approach taken in the new revision of the regulatory guide. He expressed concern about piecemeal applications and how that could take plants away from the standardization implemented in the plants today.

Software Quality Assurance (3.2)

Mr. Kemper provided an overview of the upcoming detailed presentations for section 3.2 of the research plan, software quality assurance. He then provided background on the current process for evaluating the software quality of licensee applications using SRP Chapter 7 (Revision 4 issued in 1997). To do this, NRC reviews the developmental process and the measures produced by the licensees. This review depends on qualitative evaluations. The software quality assurance evaluations are done manually, without the aid of computerized assessment tools or other means of obtaining quantitative measures of software quality. Mr. Kemper compared this with the way the agency does independent analysis of fuel designs or probabilistic risk analysis to verify the licensee's conclusions.

Mr. Kemper also discussed the approach to reviewing the software quality assurance methods and tools that exist in other sectors of the process industry. If possible, the staff will adapt these tools for deployment on software systems within the nuclear industry. The research in this area will focus on assessing possible analysis methods currently used in design and analysis of safety-critical software systems.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis asked why formal methods were not pursued. Mr. Arndt described previous research performed as part of the cooperative agreement with the Halden project. The staff continues to follow the work to provide background information to the research program.
- Dr. Apostolakis asked about the distinction between software quality assurance and risk analysis. Mr. Arndt described the quality assurance issue as an effort to get a higher level of confidence that the software is performing safety functions appropriately. The quality assurance may or may not produce quantitative estimates.

Assessment of Software Quality (3.2.1)

To lead the discussion on this portion of the research plan, Mr. Kemper introduced Mr. Norbert Carte, a member of the RES I&C team. Assisting with the presentation was Dr. Ming Li, of the University of Maryland.

Mr. Carte provided an overview of the Assessment of Software Quality program. The basic issue facing NRC is the increasing size and complexity of software in upcoming submittals. Mr.

Carte described the objective of the project: to perform a large-scale validation of measures identified through previous research to assess the quality of software quantitatively. One challenging portion of the project is the development of acceptance criteria. He also discussed the large literature base supporting the use of software quality metrics, though such use does not eliminate the need for human judgment.

Mr. Carte specifically discussed the issues raised during previous ACRS meetings. The project is now looking at an actual nuclear safety system rather than the low-reliability system examined earlier in the project. He also discussed the ease of obtaining the metrics and the uncertainty in these measurements.

Dr. Li then discussed some technical details of the work. He discussed the connection between software engineering measurements and software quality and two specific measures being used. First he discussed defect density and the techniques to measure the number of defects remaining in software.

Mr. Arndt discussed the multiple roles of the software quality assurance program. First is to understand the system better. Second is to produce a quantitative assessment of software quality.

Mr. Li then discussed his second measure, test coverage. Test coverage is the portion of software statements executed against a set of test cases. Mr. Li stated that the end goal is to produce the probability of failure per demand for software.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis questioned the assumptions underlying the capture/recapture approach to measuring defect density. Mr. Carte further described the process and Dr. Kress noted his acceptance of the methods to correlate the data.
- Dr. Apostolakis asked about the assignment of probabilities to different conditions. He specifically commented that the methods needed to consider accident conditions more than normal operations. Dr. Guarro also cautioned the staff against extrapolating statistics for routine operation to rare accident scenarios.
- Dr. Apostolakis stated his support for the objective of gaining a better understanding of the system, but expressed doubts about calculating probabilities.
- Dr. Apostolakis expressed a concern that the focus seems to be on the number of defects, rather than the kinds of defects and their severity.

Digital System Dependability (3.2.2)

After a brief introduction, Mr. Arndt introduced Mr. Shaffer, who discussed the goals of the research, the motivation for performing the work, some fundamental concepts, and its applicability to the regulatory assessment process. The effort will supplement and augment the current regulatory process by defining objective acceptance criteria for digital technology from a system perspective. Another aspect of this research is to investigate if the data from this

research, such as on failure modes and likelihoods, will be applicable to probabilistic risk assessments.

Mr. Shaffer used several figures to illustrate the modeling approaches being taken to the digital system dependability analysis. He also described tools and models developed at the University of Virginia to perform the fault injection experiments on which this work is based. Mr. Shaffer discussed similar goals as the previous project. First, to gain a better understanding of the system, and then to gain numerical estimates of the dependability of digital systems.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. White asked about the inclusion of common failures (i.e., multiple faults) in the assessment. Mr. Shaffer answered that they do indeed handle multiple faults, and let the assessment determine whether they produce common mode failures.
- Dr. Apostolakis discussed his concern with numerical estimates, particularly due to changes in the software once faults are discovered and corrected.

Self-Testing Methods (3.2.3)

Mr. Arndt provided a brief presentation on the research into self-testing methods. Not a lot has been done yet on this project, so he provided a general overview. He described self-test methods as continuous hardware or software tests done to improve the system's availability. One big issue is the complexity added by these functions. Mr. Arndt said the real issue was the tradeoff between improved system performance and the new failure modes that may be introduced by the self-test features due to the increased complexity.

Risk Assessment of Digital Systems (3.3)

Mr. Arndt provided general background on the overall risk assessment program, including the reasons for doing it, its importance, and the structure of the overall program. He referred to the NRC's PRA policy statement, which encourages the use of PRA to the extent supported by the state-of-the-art and data. The issue for this project is whether the state-of-the-art supports such use for digital systems.

The research in this section of the research plan is oriented toward improving the NRC's knowledge and providing consistent regulatory processes for regulating digital systems. To do so, Mr. Arndt stated that they would gather and understand the data, assess the modeling methods that might be used, and understand the systems that need to be modeled. They will also need to develop regulatory acceptance criteria.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis asked for an example of how the current licensing criteria are difficult to meet. Mr. Arndt described the diversity and defense-in-depth requirements in BTP-19, which requires an analysis of the results of a common mode software failure. Because this is a deterministic analysis with conservative assumptions, meeting it for some design-basis accidents can be difficult. Mr. Torok (EPRI) provided his opinion that the

probability of failure for most systems is dominated by the large rotating machinery, and not the instrumentation and control. Therefore, the requirements that may be imposed by the current licensing structure may not be necessary.

- Dr. Apostolakis reinforced his comments from a previous ACRS letter that we should question the basic assumptions behind any model because the evidence suggests that most problems come from specification errors, requirements, and design-type errors.

Development and Analysis of Digital System Failure Data (3.3.1), Investigation of Digital System Failure Assessment Methods (3.3.2), Investigation of Digital System Risk Characteristics (3.3.3), & Investigation of Digital System Reliability Assessment Models (3.3.4)

To start the second day of the meeting, Mr. Kemper introduced Mr. Arndt, who discussed how this project is being performed in coordination with the RES Probabilistic Risk Analysis branch. The 3.3.1-3.3.4 section is being worked on by two teams; one team is from PRAB, with Brookhaven National Laboratory, and the other team is from the I&C section, with The Ohio State University. He then turned the presentation over to PRAB.

Mr. Hamzehee, the section chief in charge of this work, started the presentation. He stated the goal of the work to develop a probabilistic method for modeling the potential failures of a digital I&C system that can later be integrated with the probabilistic risk assessment using traditional methods. To be able to quantify the reliability of a digital system, we need to have both models and data. He then introduced Mr. Hilsmeier, a member of his staff, to provide more details.

Mr. Hilsmeier presented the details of each task in the Digital Systems PRA Project Plan.

Mr. Torok suggested several questions for the staff to consider. Had looked at the sensitivity of the core damage frequency to how the I&C is modeled in the PRA? What is the target reliability needed from I&C to make it a negligible contributor to risk? How are they using data from other industries? Have they looked at the possibility of comparing the reliability of the analog systems to the digital systems? Mr. Torok also offered to brief the subcommittee on EPRI's method for addressing the risk of digital system upgrades.

For the second part of the presentation, Mr. Arndt provided some background on the work, then stated that the idea behind the work is to look at the different kinds of methods to examine their usefulness. This part of the work focuses on the dynamic interactions in the process. He then introduced Professor Aldemir to provide details of the work.

Dr. Aldemir discussed the differences between analog and digital systems that make them a challenge. Among these differences is the lack of good definition in the potential failure modes of a digital system. He described three types of dynamic methods: continuous time methods, discrete time methods, and visual methods. Dr. Aldemir presented some details of the two methods chosen for further investigation: the dynamic flowgraph methodology and Markov models.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis suggested the staff consider soliciting comments from the public on the data collection project before the end. Mr. Hamzehee and Mr. Kemper agreed.
- Dr. Apostolakis asked about the Reliability Analysis Center and access to their data. Mr. Hamzehee and Mr. Chu stated that the data was proprietary, but they had purchased access to the data. If it relied upon heavily during the project, Dr. Apostolakis suggests that we examine it more closely.
- Dr. Apostolakis stated his belief that the data collection task is one of the most important tasks in the program, particularly when it includes real operating experience events. The operating experience also provides a test for the potential methods to see if they can model actual events.
- Dr. Bonaca pointed out that the concern in most applications will be the application code, not necessarily the pre-approved digital platform. Mr. Torok agreed.
- Dr. Apostolakis suggested using the challenges with digital systems as a way to judge the helpfulness of the methods. Also, he suggested measuring them against the needs of the agency and the reviewers.
- Dr. Apostolakis suggested that both groups (PRAB/BNL and OSU) use the same requirements for measuring the usefulness of potential assessment methods. He suggested closer collaboration between the groups overall.
- Dr. Apostolakis warned against the use of the Procrustean bed – taking existing models from reliability and forcing them upon software. This is not typically an acceptable approach (as Hercules demonstrated).

Closing Discussions

Mr. Morris provided comments from NSIR regarding section 3.4 of the draft research plan. Because they look at everything differently from a security standpoint, they are interested in any research that helps promote an understanding of the vulnerabilities that exist and how they could be exploited.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Kress stated that he is glad to see research doing this work. He believes it will be badly needed in the near future. He particularly pointed out that he liked the idea of looking for modes of failure first, especially from operating experience. He liked the thought about looking at whether one can declare digital systems better than analog systems, and therefore declare them not risk-significant or bound them with analog values. He also stated that since these failures are not random events, they will be sequence dependent. This leads to difficulty finding a failure probability. Overall, he believes the research will bear fruit and be very useful.

- Dr. Bonaca stated that the work on Reg Guide 1.97 is good, but he has questions about backfitting the Reg Guide to older plants. He stated that he was somewhat confused by the software quality presentations and is not too convinced about it yet. He agreed with Dr. Kress regarding the overall need for this work. He stated that he would like to have us involved in the Oconee upgrade. He thinks the research plan is quite significant and he hopes the offices can work out their differences. He believes the agency should continue to look ahead on these issues.
- Dr. Apostolakis agreed with Dr. Kress and Dr. Bonaca that he is pleased that the staff is pursuing this work. Overall, he feels it is a very good program plan, though he feels there are still some fundamental issues that need resolved.

SUBCOMMITTEE DECISIONS AND ACTIONS

The Full Committee will review and comment upon the draft Digital Systems Research Plan. We also expect Regulatory Guide 1.97 to come to the Committee for review soon.

BACKGROUND MATERIALS PROVIDED TO THE SUBCOMMITTEE PRIOR TO THIS MEETING

0. Subcommittee status report, including agenda.
1. Memorandum from J. E. Dyer, Director, NRR, to Carl J. Paperiello, Director, RES, "Comments on Draft, 'NRC Digital System Research Plan, FY 2005 - FY 2009'," 6 May 2005. [ML051020435]
2. Memorandum from Glenn M. Tracy, Director, Division of Nuclear Security, NSIR, to Richard J. Barrett, Director, Division of Engineering Technology, RES, "Office of Nuclear Security and Incident Response Comments on a Draft of 'NRC Digital System Research Plan, FY 2005 - FY 2009'," 2005. [ML050840481]
3. Memorandum from Robert C. Pierson, Director, Division of Fuel Cycle Safety and Safeguards, NMSS, to Richard J. Barrett, Director, Division of Engineering Technology, RES, "Comments on the Draft 'NRC Digital System Research Plan, FY 2005 - FY 2009'," 30 March 2005. [ML050830122]
4. Email from John Jankovich, Team Leader, MSIB/IMNS/NMSS, to Michael Mayfield, then Director, Division of Engineering Technology, RES, "IMNS/NMS Response to Digital System Research Plan," 16 March 2005.
5. Memorandum from Michael E. Mayfield, Director, Division of Engineering, NRR, to Jose A. Calvo, Chief, Electrical & Instrumentation and Controls Branch, Division of Engineering, NRR, "Response to Non-Concurrence on the Draft 'NRC Digital Systems Research Plan, FY 2005 - FY 2009'," 3 May 2005. [ML051220503]
6. Memorandum from Jose A. Calvo, Chief, Electrical & Instrumentation and Controls Branch, Division of Engineering, NRR, to Michael E. Mayfield, Director, Division of Engineering, NRR, "Non-Concurrence on the Draft 'NRC Digital Systems Research Plan, FY 2005 - FY 2009'," 19 April 2005. [ML051100056]
7. United States Nuclear Regulatory Commission, "Draft Regulatory Guide DG-1128 (Proposed Revision 4 of Regulatory Guide 1.97), Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," May 2005.

8. United States Nuclear Regulatory Commission, "Regulatory Guide 1.97, Revision 3, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," May 1983.
9. IEEE Power Engineering Society, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," IEEE Std. 497-2002, 30 September 2002.
10. United States Nuclear Regulatory Commission, "Preliminary Validation of a Methodology for Assessing Software Quality," NUREG/CR-6848, July 2004.
11. University of Virginia Center for Safety-Critical Systems, "A Numerical Safety Evaluation Process for Safety-Critical Systems," UVA-CSCS-NSE-001, Revision 2, 1 August 2003.
12. University of Virginia Center for Safety-Critical Systems, "A Technique for Performing Fault Injection Using Simics," UVA-CSCS-SFI-001, Revision 0, 31 December 2004.
13. United States Nuclear Regulatory Commission, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," Draft Report for Comment, October 2004.
14. EPRI, "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades," #1002835, December 2004.

Note: Additional details of this meeting can be obtained from a transcript of this meeting available for downloading or viewing on the Internet at <http://www.nrc.gov/reading-rm/doc-collections/acrs/tr/> or can be purchased from Neal R. Gross and Co., Inc., (Court Reporters and Transcribers) 1323 Rhode Island Avenue, N.W., Washington, DC 20005 (202) 234-4433.

**ADAMS DOCUMENT PROFILE
FOR SUBCOMMITTEE MEETING MINUTES**

[Required fields in red]

Originator: **EAT2**

Document Properties:	Value:
Item ID:	
Accession Number:	
Estimated Page Count:	10
Document Date:	July 21, 2005
Document Type:	Meeting Minutes
Availability:	Publicly Available
Title:	Certified Minutes of the ACRS Subcommittee on Digital Instrumentation & Control Systems, June 14-15, 2005
Author Name:	Eric Thornsby
Author Affiliation:	NRC/ACRS
Addressee Name:	
Addressee Affiliation:	NRC/ACRS
Docket Number:	
License Number:	
Case/Reference Number:	GT200
Document/Report Number:	
Keyword:	Digital Instrumentation and Control Systems Research Plan
Package Number:	
Document Date Received:	
Date Docketed:	
Related Date:	
Comment:	
Vital Records Category:	No
Document Status:	
Media Type:	Electronic
Physical File Location:	ADAMS
FACA Document:	ACRS
Date To Be Released:	
Distribution List Codes:	
Contact Person:	Thornsby, E - 301-415-8716
Text Source Flag:	Native Application
Official Record:	
Document Sensitivity:	Non-Sensitive
Replicated:	No
ForeMost File Code (Latest):	
ForeMost Document Number:	
ForeMost File Code Set:	

SECURITY:

ACRS-ACNW Document Custodians
ACRS
NRC Users

Owners (on all documents)
Viewers
Viewers (only if not sensitive or 'internal only')

EAT

Portland, Oregon. TNP began commercial operation in May 1976. The reactor output was rated at 3411 MWt with an approximate net electrical output rating of 1130 MWe. The nuclear steam supply system was a four-loop pressurized water reactor designed by Westinghouse Electric Corporation. TNP was shut down for the last time on November 9, 1992.

In August 1999, PGE submitted its License Termination Plan (LTP) for the TNP facility. Under the provisions of 10 CFR 50.82(a)(10), the NRC approved the LTP by license amendment dated February 12, 2001. PGE conducted decommissioning activities at TNP in accordance with the approved LTP from February 2001 to December 2004. In accordance with the approved LTP, the licensee conducted final status surveys (FSSs) to demonstrate that the facility and site meet the criteria for unrestricted release as presented in 10 CFR 20.1402. Details of the FSS results were submitted to the NRC in 10 separate FSS reports (FSSRs).

PGE submitted an application for termination of the TNP Facility Operating (Possession Only) License, No. NPF-1, on December 20, 2004. The application states that PGE has completed remaining radiological decommissioning and FSSs of the TNP facility and site in accordance with the NRC-approved LTP, and the FSSs demonstrate that the facility and site meet the criteria for decommissioning and release of the site for unrestricted use that are stipulated in 10 CFR part 20, subpart E.

The NRC conducted a number of performance-based in-process inspections of the licensee's FSS program during the decommissioning process. The purpose of the inspections was to verify that the FSS was being conducted in accordance with of the commitments made by the licensee in the LTP, and to evaluate the quality of the FSS by reviewing the FSS procedures, methodology, equipment, surveyor training and qualifications, document quality control, and survey data supporting the FSSRs. In addition, the NRC conducted a number of independent confirmatory surveys to verify the FSS results obtained and reported by the licensee. Confirmatory surveys consisted of surface scans for beta and gamma radiation, direct measurements for total beta activity, and collection of smear samples for determining removable radioactivity levels.

The NRC staff reviewed the FSS Report and concludes that: (1) Dismantlement and decontamination activities were performed in accordance

with the approved LTP; and (ii) The FSS and associated documentation, including an assessment of dose contributions associated with parts released for use before approval of the LTP, demonstrate that the facility and site have met the criteria for decommissioning in 10 CFR Part 20, Subpart E. Therefore, NRC is terminating TNP Facility Operating License No. NPF-1.

FOR FURTHER INFORMATION CONTACT: See the application dated December 20, 2004, and the Safety Evaluation Report, available for public inspection at the Commission's Public Document Room (PDR), located at One White Flint North, Public File Area O1 F21, 11555 Rockville Pike (first floor), Rockville, Maryland. Publicly available records will be accessible electronically from the Agency-wide Documents Access and Management System's (ADAMS) Public Electronic Reading Room on the Internet at the NRC Web site, <http://www.nrc.gov/reading-rm/adams.html> (ADAMS Accession Nos. ML050030054, and ML050680345). Persons who do not have access to ADAMS or who encounter problems in accessing the documents located in ADAMS, should contact the NRC PDR Reference staff by telephone at 1-800-397-4209, 301-415-4737 or by e-mail to pdr@nrc.gov.

Dated in Rockville, Maryland this 23rd day of May, 2005.

For the Nuclear Regulatory Commission.

Andrew Persinko,

Acting Deputy Director, Decommissioning Directorate, Division of Waste Management and Environmental Protection, Office of Nuclear Material Safety and Safeguards.

[FR Doc. E5-2734 Filed 5-27-05; 8:45 am]

BILLING CODE 7590-01-P

NUCLEAR REGULATORY COMMISSION

Advisory Committee on Reactor Safeguards; Meeting of the Subcommittee on Digital Instrumentation and Control Systems; Notice of Meeting

The ACRS Subcommittee on Digital Instrumentation and Control Systems will hold a meeting on June 14-15, 2005, Room T-2B1, 11545 Rockville Pike, Rockville, Maryland.

The entire meeting will be open to public attendance.

The agenda for the subject meeting shall be as follows:

Tuesday, June 14, 2005—8:30 a.m. until the close of business.

Wednesday, June 15, 2005—1 p.m. until the close of business.

The purpose of this meeting is to review selected digital instrumentation and control research projects and related matters. The Subcommittee will hear presentations by and hold discussions with representatives of the Office of Nuclear Regulatory Research and other interested persons regarding this matter. The Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee.

Members of the public desiring to provide oral statements and/or written comments should notify the Designated Federal Official, Mr. Michael R. Snodderly (telephone 301-415-6927) or the Cognizant Staff Engineer, Mr. Eric A. Thornsby (telephone 301-415-8716), five days prior to the meeting, if possible, so that appropriate arrangements can be made. Electronic recordings will be permitted.

Further information regarding this meeting can be obtained by contacting the Designated Federal Official or the Cognizant Staff Engineer between 7:30 a.m. and 4:15 p.m. (e.t). Persons planning to attend this meeting are urged to contact one of the above named individuals at least two working days prior to the meeting to be advised of any potential changes to the agenda.

Dated: May 24, 2005.

Michael L Scott,

Branch Chief, ACRS/ACNW.

[FR Doc. E5-2735 Filed 5-27-05; 8:45 am]

BILLING CODE 7590-01-P

NUCLEAR REGULATORY COMMISSION

Sunshine Act Meeting

AGENCY HOLDING THE MEETINGS: Nuclear Regulatory Commission.

DATES: Weeks of May 30, June 6, 13, 20, 27, July 4, 2005.

PLACE: Commissioners' Conference Room, 11555 Rockville Pike, Rockville, Maryland.

STATUS: Public and Closed.

MATTERS TO BE CONSIDERED:

Week of May 30, 2005

Tuesday, May 31, 2005

2 p.m. Discussion of Security Issues (Closed—Ex. 1) (This meeting was originally scheduled for June 1st).

Wednesday, June 1, 2005

9:30 a.m. Briefing on Threat Environment Assessment (Closed—Ex. 1) (This meeting was originally scheduled for May 25th).

**Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee Meeting
Rockville, MD
14-15 June 2005**

- Proposed Agenda -

Cognizant Staff Engineer: Eric Thornsbury (301-415-8716, eat2@nrc.gov)

Topic		Presenter(s)	Time
June 14			
I	Opening Remarks and Objectives	G. Apostolakis, ACRS	8:30 - 8:45 am
II	Reconciliation of Comments on Draft Research Plan	M. Waterman, RES	8:45 - 10:15 am
	Break		10:15 - 10:30 am
III	Draft Revision of Reg Guide 1.97	G. Tartal, RES	10:30 - 11:30 am
	Lunch		11:30 am - 12:30 pm
IV	Software Quality Assurance (3.2)	W. Kemper, RES	12:30-12:45 am
	Assessment of Software Quality (3.2.1)	S. Arndt, RES N. Carte, RES M. Li, UMd	12:45 - 2:30 pm
		Break	2:30 - 2:45 pm
	Digital System Dependability (3.2.2) Self-testing Methods (3.2.3)	S. Arndt, RES R. Shaffer, RES	2:45 - 5:00 pm
V	Risk Assessment of Digital Systems (3.3)	S. Arndt, RES	5:00 - 5:30 pm
	Recess for the day		5:30 pm
June 15			
	Reconvene		1:00 pm
V	Development and Analysis of Digital System Failure Data (3.3.1)	T. Hilsmeier, RES T. Chu, BNL	1:00 - 1:45 pm
	Investigation of Digital System Failure Assessment Methods, Risk Characteristics, and Reliability Assessment Models (3.3.2, 3, 4)	T. Hilsmeier, RES H. Hamzehee, RES T. Chu, BNL	1:45 - 2:30 pm
		Break	2:30 - 2:45 pm
		S. Arndt, RES T. Aldemir, OSU	2:45 - 4:45 pm
VI	Closing Discussion and Future Plans	G. Apostolakis, ACRS	4:45 - 5:00 pm
	Recess		5:00 pm

Notes:

- " (3.X) refers to the corresponding section of the draft research plan
- " Presentation time should not exceed 50% of the total time allocated for a specific item.
- " Number of copies of presentation materials to be provided to the ACRS - 35.

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE MEETING ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

June 14, 2005

Date

NRC STAFF PLEASE SIGN IN BELOW

PLEASE PRINT

<u>NAME</u>	<u>ORGANIZATION</u>
PAUL LOESER	NRR/DE/EEIB
CLIFF DOUTT	NRR/DSSA/SPSB
STEVE ARNPT	RES/DET/ERAB
Norbert Carte	RES/DET/ERAB/ICS
E.C. Marinis	NRR/DLPM
George Tartal	RES/DET/ERAB/ICS
Mike Waterman	RES/DET/ERAB/ICS
Manan Patel	NRR/DE/EEIB
Jed VORA	NRC RES DET
FRED BURROWS	NRC/NMSS/FCSS
TERICA V. GIOVAN	RES/DET/ERAB
Doug Hill	MPA ASSOC.
Mike Miller	Duke Energy
Tony HARRIS	NEI
Ray Torok	EPR I
June AZEMIR	OHIO STATE U.
Chris GRIMES	NRR/DE
Michele Evans	RES/DET
Roman Shaffer	RES/DET
Allen Howe	NRR/EEIB

DATA SHEET - RETURN TO BJWHITE AFTER MEETING

SUBCOMMITTEE MEETING DATE SHEET

1. Subcommittee (Name) - DIGITAL INSTRUMENTATION & CONTROL SYSTEMS

a. Date 1a. June 14-15, 2005

b. Cognizant Staff Engineer 1b. Eric A. Thornsbury

2. Amount of Time Spent in Open Sessions 2. 12:00
(hours and minutes)

3. Amount of Time Spent in Closed Session 3. 0

(1) Exemption 1 - Natl. Security Info. _____

(2) Exemption 4 - Proprietary Material* _____

(3) Exemption 6 - Undue Invasion of
Personal Privacy _____

(4) Exemption 9 - Premature Disclosure
(e.g., Budget and Financial Info) _____

(5) Exemption 10 - Adjudicatory Matters _____

4. Number of Written Comments from the
Public (submitted for consideration)
(Names) 4. 0

5. Number of Oral Statements
(Names) 5. 0

6. Number of Public Attendees 6. 11

*Currently includes Plant Security Information



RESEARCH PLAN COMMENTS

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS DIGITAL INSTRUMENTATION AND CONTROL SUBCOMMITTEE MEETING

JUNE 14, 2005

Michael E. Waterman, Sr. I&C Engineer

William E. Kemper, Section Chief

I&C Engineering Section

Engineering Research Application Branch

Division of Engineering Technology

Office of Nuclear Regulatory Research

(301-415-2818, mew1@nrc.gov)

(301-415-5974, wek@nrc.gov)



OVERVIEW

- NRC Licensing Bases
- NRC Licensing Process
- Emphasis on Communications
- Comment Disposition Summary Table
- Disposition of Comments
- Summary



SUMMARY

- 34 comments were received from NRR, NMSS, and NSIR
- 31 of the 34 comments were incorporated into the Research Plan
- The remaining 3 comments address topics that are outside the scope of this Research Plan or required no change
 - Metrics to evaluate research effectiveness (NRC internal reviews of programmatic effectiveness)
 - Incorporation of human factors considerations in PRAs (Human Performance Plan)
 - NRR SRP considered sufficient guidance by NMSS/FCSS
- RES revised the Research Plan to reflect the need for additional information in several areas on the basis of communications with the supported Offices
- The Research Plan will continue to be updated in response to communications with the supported Office(s) as new needs are identified and as research projects are completed

- metrics
 - HF in PRA
 - NRR SRP is sufficient for NMSS

Dr. White?
 Other doc available?
 - not part of this presentation



living document



NRC LICENSING BASES

- The NRC uses an extensive set of regulations, guidance, standards, and technical reports to license digital safety systems
 - Code of Federal Regulations
 - Commission policy statements
 - Standard Review Plans (SRPs)
 - Branch Technical Positions in SRPs
 - Consensus standards
 - Regulatory Guides endorsing consensus standards
 - Topical reports
 - Research reports

*- alignment + supplement procedures/SRP
for consistency
- formalize current process
example: correctness*



NRC LICENSING PROCESS

- The regulations, guidance, standards, and technical reports identify several hundred important attributes and associated criteria that must be addressed appropriately for digital systems to be licensed for safety-related applications
- The purpose of conducting research is to investigate current and emerging methods and knowledge and, where appropriate, to augment and supplement NRC processes to enable NRC staff to evaluate digital systems consistently and effectively



ADDITIONAL EMPHASIS ON COMMUNICATIONS

- The Research Plan was revised to provide additional emphasis on
 - Development of research products (review procedures, tools, etc.) that augment and supplement existing NRC review plans and processes as part of a general process improvement initiative
 - Enabling communications between RES and supported Office(s) during the initial stages of research project planning to identify specific research products that must be developed, and during performance of research to keep the supported Offices informed on the progress of research
- Meetings were held with supported Offices to describe the Research Plan, and to discuss changes to the Research Plan that better reflect the objectives of the research projects. These meetings are the precursor for future TAG meetings to address specific issues.

NRR waived/declined mtg in ~Jan



COMMENT DISPOSITION



COMMENT DISPOSITION

SECTION CHANGED	RESEARCH PLAN SECTION TITLE	COMMENT #	TYPE OF CHANGE			
			REVISED INFO	ADDED INFO	REVISED SCOPE	NO REVISION
2.1	Objective of the Research Plan	NMSS/IMNS 2	X	X		
2.2	Scope of the Research Plan	NRR/SPSB 5		X		
3.1.1	Environmental stressors	NRR/EEIB 1	X	X		
3.1.3	COTS digital systems	NMSS/IMNS 3		X		
3.1.3	COTS digital systems	NRR/EEIB 5	X	X	X	
3.1.4	Electrical power distribution system interactions with nuclear facilities	NRR/EEIB 2	X	X	X	
3.1.6	Operating systems	NMSS/IMNS 3		X		
3.1.6	Operating systems	NRR/EEIB 3	X	X		
3.2	Software Quality Assurance	NMSS/IMNS 3		X		
3.2.1	Assessment of software quality	NRR/EEIB 5	X	X	X	
3.2.2	Digital system dependability	NRR/EEIB 5	X	X	X	
3.2.3	Self-testing methods	NRR/EEIB 4	X	X		



COMMENT DISPOSITION (cont.)

SECTION CHANGED	RESEARCH PLAN SECTION TITLE	COMMENT #	TYPE OF CHANGE			
			REVISED INFO	ADDED INFO	REVISED SCOPE	NO REVISION
3.3	Risk Assessment of Digital Systems	NRR/SPSB 11	X			
3.3.2	Investigation of digital system failure assessment methods	NMSS/IMNS 3		X		
3.3.2	Investigation of digital system failure assessment methods	NRR/SPSB 2		X	X	
3.3.3	Investigation of digital system characteristics important to risk	NRR/SPSB 7	X		X	
3.3.3	Investigation of digital system characteristics important to risk	NRR/SPSB 6	X			
3.3.4	Investigation of digital system reliability assessment methods	NRR/EEIB 5	X	X	X	
3.3.4	Investigation of digital system reliability assessment methods	NRR/SPSB 1	X	X		
3.3.4	Investigation of digital system reliability assessment methods	NRR/EEIB 4	X			
3.3.4	Investigation of digital system reliability assessment methods	NRR/SPSB 8	X			



COMMENT DISPOSITION (cont.)

*-Kemper:
-will use TAG process
to prioritize
-some already in Sect. 4*

SECTION CHANGED	RESEARCH PLAN SECTION TITLE	COMMENT #	TYPE OF CHANGE			
			REVISED INFO	ADDED INFO	REVISED SCOPE	NO REVISION
3.4	Security aspects of digital systems	NSIR/DNS 1	X	X		
3.4.1	Security assessments of cyber vulnerabilities	NSIR/DNS 2				X
3.4.2	Security assessments of EM vulnerabilities	NSIR/DNS 3	X			
3.4.2	Security assessments of EM vulnerabilities	NRR/EEIB 6	X	X		
3.4.3	Network Security	NRR/SPSB 3	X	X		
3.4.3	Network Security	NSIR/DNS 4		X	X	
3.5.2	Radiation-hardened integrated circuits	NRR/EEIB 7	X	X	X	
3.5.5	ASICs and FPGAs	NRR/EEIB 8	X	X		
3.6	Advanced Nuclear Power Plant Digital Systems	NRR/SPSB 5		X		
3.6.3	Advanced NPP digital system risk	NRR/EEIB 5	X	X	X	
GENERAL		NMSS/FCSS 3	X			
GENERAL		NMSS/FCSS 2	X			
GENERAL		NRR/SPSB 9	X			
NONE		NMSS/FCSS 1				X
NONE		NMSS/IMNS 1				X
NONE		NRR/SPSB 10				X



RESEARCH PLAN RELATIONSHIP TO THE NRC STRATEGIC PLAN

- A general comment from NRR was that the research projects should have as their purpose a focus on safety, security, effectiveness, or openness
 - In section 4 of the Research Plan, each research project is linked to specific NRC Strategic Plan supporting strategies for achieving the NRC Goals of Safety, Security, Openness, and Effectiveness (Management is the other Strategic Goal)
 - An in-depth discussion relating each research project to corresponding Strategic Plan supporting strategies would have been repetitive and distracting. The tabular format in section 4 was considered the best alternative for succinctly relating the NRC Strategic Plan goals to the research projects



SECTION 2 OBJECTIVE AND SCOPE

- Schedule periodic, formal briefings for the supported Offices on the interim results and status of the tasks (§ 2.1)
 - RES is developing more formal processes to improve communications with the supported Offices
 - TAGs, project development meetings, project status reviews, etc.

- Advanced instrumentation and controls research would also be beneficial for existing plants undergoing digital retrofits (§ 2.2)
 - Recommendation incorporated into Section 2.2 and Section 3.6
 - These sections were revised to reflect the potential applicability of advanced reactor research products to existing plants



SECTION 3.1 SYSTEM ASPECTS OF DIGITAL TECHNOLOGY

- The justification in Section 3.1.1 is to “reduce licensing uncertainty.” The justification should be focused on safety, improved efficiency, effectiveness and realism, or openness.
 - Recommendation incorporated into Section 3.1.1
 - Additional focus was placed on safety, although, because licensing uncertainty is a key issue in the nuclear industry with regard to digital retrofits, the focus on reducing licensing uncertainty was retained
- Section 3.1.4 is not clear why this SBO research is included in the digital research plan
 - Recommendation incorporated into Section 3.1.4
 - This section was revised to address the effect of grid voltage fluctuations on digital equipment in NPPs
 - This research supports on-going research, and could be used to identify safety-related components and systems that are vulnerable to grid voltage fluctuations



SECTION 3.1 SYSTEM ASPECTS OF DIGITAL TECHNOLOGY (cont.)

- The Research Plan and SOWs should include digital technology involving byproduct materials
 - Recommendation incorporated into Sections 3.1.3, 3.1.6, 3.2, 3.3.2, and other sections as appropriate

- The state-of-the-art in software engineering may not be sufficiently matured for [quantitative] digital safety system reviews. This concern applies to the activities described in Sections 3.1.3, 3.2.1, 3.2.2, 3.3.4, and 3.6.3.
 - Recommendation incorporated into Sections 3.1.3, 3.2.1, 3.2.2, 3.3.4, and 3.6.3
 - Various methods will be validated as part of research and before recommendations are made to develop digital safety system review procedures
 - The research projects are expected to validate and increase the state-of-the-art in digital system licensing capabilities



SECTION 3.1 SYSTEM ASPECTS OF DIGITAL TECHNOLOGY (cont.)

- Section 3.1.6 is not clear on how proprietary restrictions for “COTS operating systems” can be resolved in a way that can improve the assessment of digital systems
 - Section 3.1.6 was revised to reflect that not all operating systems are proprietary, and to address issues regarding features of operating systems that may adversely affect safety
 - Nuclear industry digital system developers have expressed willingness to allow access to proprietary operating system design and development information



SECTION 3.2 SOFTWARE QUALITY ASSURANCE

- The plan should recognize that integrating digital systems into PRAs may not be practical and that a PRA may not be an efficient or accurate tool for digital system reviews.
 - Recommendation incorporated into Section 3.3
 - Acknowledged potential conclusion
 - This issue ultimately will be addressed by the “Risk” research projects
- Link the objective of Section 3.2.3 to safety, improved efficiency, etc., and explain how NRC reviews can be improved to assess self-test features
 - Section 3.2.3 was lengthened to discuss the development of technical guidance regarding the use and review of self-testing features in digital safety systems

- Turkey Point load sequencer

*GA - use of operating experience?
- yes, Wed presentation*



SECTION 3.3 RISK ASSESSMENT OF DIGITAL SYSTEMS (cont.)

- Include the integration of external events, environmental, and security issues unique to digital system risk
 - Section 3.3.2 was revised to state that these failure modes will be evaluated as part of the investigation of digital system failure assessment methods
 - Initial development efforts will exclude external events, etc., until the methodology is sufficiently developed to address these additional issues
- The goal of the Section 3.3.3 research should be to provide methods for incorporating a digital component or system into a PRA
- In addition, acceptance guidelines should be considered as part of the deliverable *(quality of ~~product~~ process analysis)*
 - Section 3.3.3 was revised to address these comments



SECTION 3.3 RISK ASSESSMENT OF DIGITAL SYSTEMS (cont.)

- Section 3.3.3 should be clarified to reflect potential capabilities and to ensure “risk” is not used as in the plan as a synonym for “safety”
 - Section 3.3.3 was revised to reflect the comment and the Research Plan was revised to ensure that the term “risk” is used where “risk” is required *difference?*
- Risk assessment should investigate advantages and disadvantages of analog and digital system architectures and implementation characteristics
 - Section 3.3.4 was revised to include a discussion on the evaluation of an analog RPS and FW control system for comparison with equivalent digital systems
 - Ongoing research is addressing this suggested approach



SECTION 3.3 RISK ASSESSMENT OF DIGITAL SYSTEMS (cont.)

- Justify Section 3.3.4 statement that digital reliability assessment methods will reduce staff review effort by 20 to 30 percent
 - Recommendation incorporated into Section 3.3.4
 - The statement was removed
 - The Research Plan was revised to emphasize that the research products will augment and supplement existing review processes



SECTION 3.4 SECURITY ASPECTS OF DIGITAL SYSTEMS

- Support development of 10CFR73 requirements that implement NRC post-September 11, 2001, security-related orders and regulatory guidance
- Support NSIR development of a comprehensive cyber security plan
 - Recommendations incorporated into section 3.4
- Section 3.4 should include research that supports industry implementation of NUREG/CR-6847, “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants”
 - Recommendations incorporated into section 3.4.1 and section 3.4.3

*- similar to an SRP
- being developed in
inter-agency work*



SECTION 3.4 SECURITY ASPECTS OF DIGITAL SYSTEMS

- Section 3.4.2 does not directly support NSIR plans, but it seems prudent to conduct research. Though the Commission has not considered EM weapons as a credible threat to nuclear power facilities, some limited anticipatory research in this area is likely warranted
 - Comments incorporated into section 3.4.2
- Section 3.4.2 describes an assessment of electromagnetic (EM) vulnerabilities. How does this activity relate to TEMPEST programs?
 - Recommendation incorporated into Section 3.4.2
 - The discussion of EM attacks was amplified to state that measures to address EM attacks are different than measures to address passive surveillance of emanated signals by unauthorized personnel (TEMPEST)
 - This project will address only EM attack vulnerabilities

*low
priority*



SECTION 3.4 SECURITY ASPECTS OF DIGITAL SYSTEMS (cont.)

- Wireless technology and firewalls should be subsets of a network security research project
 - Section 3.4.3 was renamed, “Network Security;” and the discussion in Section 3.4.4, “Firewalls,” was incorporated into the renamed Section 3.4.3
 - The focus of section 3.4.3 was revised to address network security issues, including wired communications, wireless communications, and firewalls.



SECTION 3.4 SECURITY ASPECTS OF DIGITAL SYSTEMS (cont.)

- Section 3.4.3 should reference NUREG/CR-6847, ["Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants"] which covers the assessment of wireless devices. The proposed research projects described in this section should be informed with the assumption that licensees will implement the cyber security self-assessment tool described in the NUREG/CR
- Section 3.4.4, Firewall Security, should state that NUREG/CR-6847 can be applied to assess all digital devices, including firewalls, in nuclear power plants. Revise the proposed research project to develop regulatory guidance on the use of firewalls and expand review guidance of NUREG/CR 6847 to assist reviewers in evaluating the security risk of different firewalls
 - These comments were incorporated into the Research Plan



SECTION 3.5 EMERGING DIGITAL TECHNOLOGY AND APPLICATIONS

- Discuss use of system diagnosis, prognosis, on-line monitoring (SDPM) for virtual instrumentation and parameter estimation
 - Section 3.5.1 was revised to include a discussion on the advantages and disadvantages of using virtual instrumentation. The research objectives remain the same
- The regulatory applicability is not clear for the confirmatory studies of radiation-hardened integrated circuits in Section 3.5.2
 - Recommendation incorporated into Section 3.5.2
 - The tasks and products were revised to reflect the focus on guidance for the staff
 - Discussions with the supported Offices clarified the issue as presented in the Research Plan



SECTION 3.5 EMERGING DIGITAL TECHNOLOGY AND APPLICATIONS (cont.)

- Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs) described in Section 3.5.5 are not currently used in generically-qualified safety platforms. Include, early on, an assessment of the existing or potential uses of this equipment in power reactors
 - The first paragraph of Section 3.5.5 was revised to reference current and future applications of ASICs and FPGAs



SECTION 3.6 ADVANCED NUCLEAR POWER PLANT DIGITAL SYSTEMS

- Advanced instrumentation and controls research would also be beneficial for existing plants undergoing digital retrofits
 - Recommendation incorporated into Section 2.2 and Section 3.6
 - These sections were revised to reflect the potential applicability of advanced reactor research products to existing plants



NMSS/FCSS GENERAL COMMENTS

- Review guidance in NRR SRP has been used recently by NMSS/FCSS for digital system reviews
 - Section 1.4 was revised to state the NRC is conducting research to continually augment and supplement NRC capabilities (including the NRR SRP) for reviewing and assessing digital technology implementations in safety systems
- NMSS/FCSS Regulations (10CFR70) are based on a risk-informed approach supported by qualitative acceptance criteria. Therefore, quantitative safety assessments and quantitative acceptance criteria may not be useful for FCSS needs
 - The Research Plan projects in section 3.3 address development of risk-based approaches for licensing digital safety systems. The results of this research may support existing risk-informed licensing approaches



SPSB GENERAL COMMENTS

- The terms “software reliability” and “software quality” are used somewhat interchangeably
 - The Research Plan was revised to ensure there is a clear distinction between the use of the term “reliability” and the term “quality”



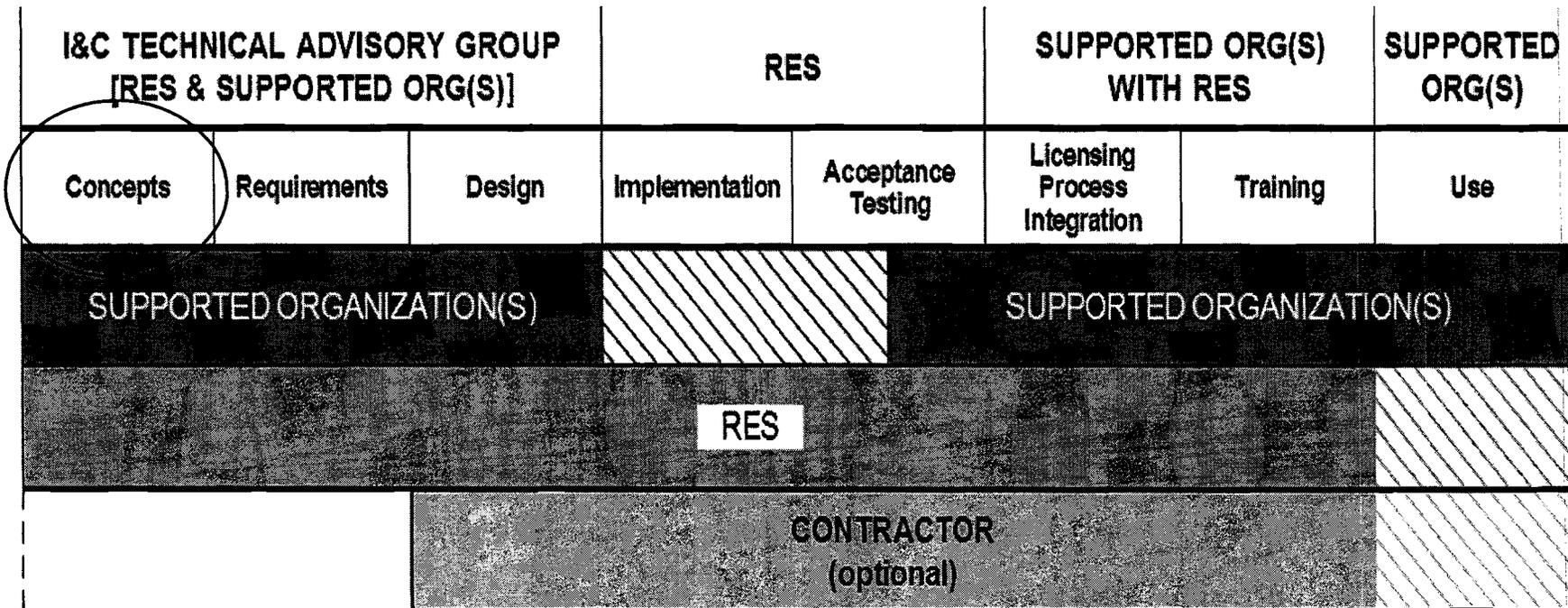
SUMMARY

- 34 comments were received from NRR, NMSS, and NSIR
- 31 of the 34 comments were incorporated into the Research Plan
- The remaining 3 comments address topics that are outside the scope of this Research Plan or required no change
 - Metrics to evaluate research effectiveness (NRC internal reviews of programmatic effectiveness)
 - Incorporation of human factors considerations in PRAs (Human Performance Plan)
 - NRR SRP considered sufficient guidance by NMSS/FCSS
- RES revised the Research Plan to reflect the need for additional information in several areas on the basis of communications with the supported Offices
- The Research Plan will continue to be updated in response to communications with the supported Office(s) as new needs are identified and as research projects are completed





COMMUNICATIONS BETWEEN RES AND SUPPORTED OFFICES



Digital Systems Review



Presentation to ACRS

June 14, 2005

**Jose A. Calvo, Chief
Evangelos Marinos
Paul Loeser
Electrical and Instrumentation & Controls Branch
Division of Engineering, NRR
U. S. Nuclear Regulatory Commission**



SUMMARY OF STAFF REVIEW OF DIGITAL SYSTEMS

- **The Staff reviews the process, not the product.**
- **We depend on the licensee using a good process to develop and test the system, and, should the worst occur and the system does not work correctly, we depend on diversity and defense-in-depth.**
- **We sample portions of the product to check in greater detail during the thread audit.**



PAST DIGITAL SYSTEM REVIEWS

- **Westinghouse Eagle 21 - Completed 1993**
- **B&W Star - Completed 1995**
- **Siemens (Now Framatome) Teleperm XS - Completed 2000**
- **Westinghouse ASICS - completion 2000**
- **ABB-CE (Now Westinghouse) Common Q - completed 2000**
- **Triconex PLC - completed 2002**



CURRENT AND UPCOMING DIGITAL REVIEWS

- **HF Controls topical report on HFC 6000 - submitted November 19, 2004.**
 - **Microprocessor based digital I&C replacement system.**
 - **HFC 6000 used in Korean nuclear plants and non-nuclear applications.**
- **Oconee digital replacement of RPS and ESF with Framatome TXS**
 - **License amendment received February 16, 2005.**
 - **The first safety related use of TXS, and first use of a single system to replace all RPS and ESF safety systems.**
- **Toshiba Field Programable Gate Arrays (FPGA)**
 - **Originally Submitted in Spring of '04.**
 - **Put on hold while Toshiba prepared documentation.**
- **Framatome AV-42 Priority Logic Module - expected summer of '05**
 - **Module combines safety and non-safety signals to control safety-related equipment.**
 - **May require policy decision on combining safety and non-safety.**
- **NRC expects an additional major digital replacement from a W plant this summer.**
- **Within 2 years, NRC expects one Navy reactor, NASA reactor, and new commercial reactor submissions.**



RESEARCH PLAN

- **RES should identify in each of the proposed projects the problem to be solved, and why current guidance is not sufficient.**
- **The method we use to review digital systems is contained in the SRP.**
 - **The SRP was written by knowledgeable engineers.**
 - **The SRP was reviewed by industry, senior management, and various groups such as EPRI, IEEE and ACRS.**
- **While this may not be the perfect document, it does exist, is being used, and it works. Research should be aimed at the type of review we actually do.**

<u>Research Project</u>	<u>Desirable to EEIB</u>	<u>Discussed with EEIB</u>
3.1.1 Environmental Stressors	No	Yes*
3.1.2 System Communications	No	Not Discussed
3.1.3 COTS Digital Systems	No	Yes*
3.1.4 Develop Models, Tools, and Methodologies to Simulate Station Blackout	No	Yes*
3.1.5 Determine the Effect of Total Harmonic Distortion on Digital Systems	No	Not Discussed
3.1.6 Operating Systems Used in Digital I&C Systems	No	Yes*
3.1.7 Investigate the Vulnerabilities of Digital I&C Systems to Determine Adequacy of D3	No	Not Discussed
3.2.1 Assessment of Software Quality	No	Yes*
3.2.2 Digital System Dependability	No	Yes*
3.2.3 Self-testing Methods	No	Yes*
3.3.1 Development and Analysis of Digital System Failure Data	No	Not Discussed
3.3.2 Digital Systems Failure Assessment Methods	No	Not Discussed
3.3.3 Model Digital Systems, Including Embedded Systems for Risk - Importance	No	Not Discussed
3.3.4 Investigation Digital System Reliability Assessment Methods	No	Yes*
3.4.1 Provide Security Assessments of Cyber Vulnerabilities	No	Not Discussed
3.4.2 Security Assessments of EM Vulnerabilities	No	Yes*
3.4.3 Wireless Network Security	No	Not Discussed
3.4.4 Firewall Security	No	Not Discussed
3.5.1 System Diagnosis, Prognosis, and On-line Monitoring	No	Not Discussed
3.5.2 Radiation-hardened Integrated Circuits	No	Yes*
3.5.3 Advanced Instrumentation and Controls	No	Not Discussed
3.5.4 Smart Transmitters	No	Not Discussed
3.5.5 Application Specific Integrated Circuits (ASICS) and Field Programmable Gate Arrays (FPGAS)	No	Yes*
3.5.6 Wireless Technology	No	Not Discussed
3.6.1 Advanced NPP Instrumentation	No	Not Discussed
3.6.2 Advanced NPP Controls	No	Not Discussed
3.6.3 Advanced NPP Digital System Risk	No	Yes*
3.7.1 Standards Development	Yes	Not Applicable
3.7.2 Maintenance of Resources and Knowledge Management	Yes	Not Applicable
3.7.3 Collaborative and Cooperative Research	Yes	Not Applicable

* Project discussed, but final version of project has not been seen, and therefore may still not meet EEIB expectations.



Project 3.3.2

Digital Systems Failure Assessment Methods

- **Project will survey various analytical methods of identifying system faults, assess these methods by conducting case studies, and recommend methods for NRR use.**
 - **The reason for this study is because not all failures may be safety-significant.**
- **EEIB fails to see how this will be useful to assess digital systems.**
- **This project may have been requested by some other branch or office.**



NEEDED RESEARCH

- **Housekeeping stuff - Updates to old Reg Guides endorsing new versions of standards, or new Reg Guides on new standards.**
- **State-of-the-Art stuff. Monitoring the cutting edge of what is being done in other industries or in academia.**
- **New ways to regulate. At the moment, these are primarily software related.**
 - **Requires an explicit discussion on application of this method, and how to tell if the licensee application of this method good enough.**
 - **How do we know that the method is properly applied, and that the licensee knows what he is doing? Detailed acceptance criteria is needed.**
 - **We need justification for rejection of the licensee submittal if the required quality is not present.**
 - **If RES suggests a change to regulation or methods, exact changes are needed.**
- **Most important RES & NRR working level staff must work together to ensure that the application of the digital technology in NPP's continues to be safe.**

Digital Systems Review



Presentation to ACRS

June 14, 2005

**Jose A. Calvo, Chief
Evangelos Marinos
Paul Loeser
Electrical and Instrumentation & Controls Branch
Division of Engineering, NRR
U. S. Nuclear Regulatory Commission**



SUMMARY OF STAFF REVIEW OF DIGITAL SYSTEMS

- **The Staff reviews the process, not the product.**
- **We depend on the licensee using a good process to develop and test the system, and, should the worst occur and the system does not work correctly, we depend on diversity and defense-in-depth.**
- **We sample portions of the product to check in greater detail during the thread audit.**



PAST DIGITAL SYSTEM REVIEWS

- **Westinghouse Eagle 21 - Completed 1993**
- **B&W Star - Completed 1995**
- **Siemens (Now Framatome) Teleperm XS - Completed 2000**
- **Westinghouse ASICS - completion 2000**
- **ABB-CE (Now Westinghouse) Common Q - completed 2000**
- **Triconex PLC - completed 2002**



CURRENT AND UPCOMING DIGITAL REVIEWS

- **HF Controls topical report on HFC 6000 - submitted November 19, 2004.**
 - **Microprocessor based digital I&C replacement system.**
 - **HFC 6000 used in Korean nuclear plants and non-nuclear applications.**

- **Oconee digital replacement of RPS and ESF with Framatome TXS**
 - **License amendment received February 16, 2005.**
 - **The first safety related use of TXS, and first use of a single system to replace all RPS and ESF safety systems.**

- **Toshiba Field Programable Gate Arrays (FPGA)**
 - **Originally Submitted in Spring of '04.**
 - **Put on hold while Toshiba prepared documentation.**

- **Framatome AV-42 Priority Logic Module - expected summer of '05**
 - **Module combines safety and non-safety signals to control safety-related equipment.**
 - **May require policy decision on combining safety and non-safety.**

- **NRC expects an additional major digital replacement from a W plant this summer.**

- **Within 2 years, NRC expects one Navy reactor, NASA reactor, and new commercial reactor submissions.**



RESEARCH PLAN

- **RES should identify in each of the proposed projects the problem to be solved, and why current guidance is not sufficient.**
- **The method we use to review digital systems is contained in the SRP.**
 - **The SRP was written by knowledgeable engineers.**
 - **The SRP was reviewed by industry, senior management, and various groups such as EPRI, IEEE and ACRS.**
- **While this may not be the perfect document, it does exist, is being used, and it works. Research should be aimed at the type of review we actually do.**

Research Project	Desirable to EEIB	Discussed with EEIB
3.1.1 Environmental Stressors	No	Yes*
3.1.2 System Communications	No	Not Discussed
3.1.3 COTS Digital Systems	No	Yes*
3.1.4 Develop Models, Tools, and Methodologies to Simulate Station Blackout	No	Yes*
3.1.5 Determine the Effect of Total Harmonic Distortion on Digital Systems	No	Not Discussed
3.1.6 Operating Systems Used in Digital I&C Systems	No	Yes*
3.1.7 Investigate the Vulnerabilities of Digital I&C Systems to Determine Adequacy of D3	No	Not Discussed
3.2.1 Assessment of Software Quality	No	Yes*
3.2.2 Digital System Dependability	No	Yes*
3.2.3 Self-testing Methods	No	Yes*
3.3.1 Development and Analysis of Digital System Failure Data	No	Not Discussed
3.3.2 Digital Systems Failure Assessment Methods	No	Not Discussed
3.3.3 Model Digital Systems, Including Embedded Systems for Risk - Importance	No	Not Discussed
3.3.4 Investigation Digital System Reliability Assessment Methods	No	Yes*
3.4.1 Provide Security Assessments of Cyber Vulnerabilities	No	Not Discussed
3.4.2 Security Assessments of EM Vulnerabilities	No	Yes*
3.4.3 Wireless Network Security	No	Not Discussed
3.4.4 Firewall Security	No	Not Discussed
3.5.1 System Diagnosis, Prognosis, and On-line Monitoring	No	Not Discussed
3.5.2 Radiation-hardened Integrated Circuits	No	Yes*
3.5.3 Advanced Instrumentation and Controls	No	Not Discussed
3.5.4 Smart Transmitters	No	Not Discussed
3.5.5 Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAS)	No	Yes*
3.5.6 Wireless Technology	No	Not Discussed
3.6.1 Advanced NPP Instrumentation	No	Not Discussed
3.6.2 Advanced NPP Controls	No	Not Discussed
3.6.3 Advanced NPP Digital System Risk	No	Yes*
3.7.1 Standards Development	Yes	Not Applicable
3.7.2 Maintenance of Resources and Knowledge Management	Yes	Not Applicable
3.7.3 Collaborative and Cooperative Research	Yes	Not Applicable

* Project discussed, but final version of project has not been seen, and therefore may still not meet EEIB expectations.



Project 3.3.2

Digital Systems Failure Assessment Methods

- **Project will survey various analytical methods of identifying system faults, assess these methods by conducting case studies, and recommend methods for NRR use.**
 - **The reason for this study is because not all failures may be safety-significant.**
- **EEIB fails to see how this will be useful to assess digital systems.**
- **This project may have been requested by some other branch or office.**



NEEDED RESEARCH

- **Housekeeping stuff - Updates to old Reg Guides endorsing new versions of standards, or new Reg Guides on new standards.**
- **State-of-the-Art stuff. Monitoring the cutting edge of what is being done in other industries or in academia.**
- **New ways to regulate. At the moment, these are primarily software related.**
 - **Requires an explicit discussion on application of this method, and how to tell if the licensee application of this method good enough.**
 - **How do we know that the method is properly applied, and that the licensee knows what he is doing? Detailed acceptance criteria is needed.**
 - **We need justification for rejection of the licensee submittal if the required quality is not present.**
 - **If RES suggests a change to regulation or methods, exact changes are needed.**
- **Most important RES & NRR working level staff must work together to ensure that the application of the digital technology in NPP's continues to be safe.**



Thornsbury notes
G-Tartal

Draft Guide DG-1128
“Criteria for Accident Monitoring Instrumentation
for Nuclear Power Plants”
(Proposed Regulatory Guide 1.97, Revision 4)

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee Meeting
June 14, 2005

George Tartal, I&C Engineer
I&C Engineering Section
Engineering Research Applications Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research



OVERVIEW

- BACKGROUND
- REGULATORY GUIDE 1.97, REVISION 3
- IEEE STANDARD 497-2002
 - Selection, performance, design, qualification, display and quality assurance criteria
- DG-1128 (REGULATORY GUIDE 1.97, REVISION 4)
 - Regulatory positions
- APPROACHES CONSIDERED
- CONCLUSION



BACKGROUND

- Instrumentation required to monitor variables and systems under accident conditions
 - 10 CFR Part 50, Appendix A, Criteria 13, 19, 64
- Reg Guide 1.97 Rev. 1 issued in August 1977
 - Provided general design and qualification criteria
- Lessons learned from TMI
 - NUREG-0737
 - 10 CFR Part 50.34(f)
- Reg Guide 1.97 Rev. 2 issued in December 1980
 - Implementation via NUREG-0737 Supp. 1
- Reg Guide 1.97 Rev. 3 issued in May 1983



REGULATORY GUIDE 1.97, REV. 3

- **Endorses ANSI/ANS-4.5-1980**
 - This standard has been withdrawn and is inactive
- **Organizes accident monitoring variables by variable type**
 - Type A are for planned manual actions with no automatic control
 - Type B are for assessing plant critical safety functions
 - Type C are for indicating breach of fission product barriers
 - Type D are for indicating safety system performance and status
 - Type E are for monitoring radiation levels, releases and environs
- **Design and qualification criteria applied by category**
 - Cat 1 is for indicating accomplishment of safety function (~SR)
 - Cat 2 is for indicating safety system status (~AQ)
 - Cat 3 is for backup and diagnostic variables (~NSR)
- **Rev. 3 is the defacto standard for accident monitoring**



IEEE STANDARD 497-2002

- Consolidates and updates criteria from ANSI/ANS-4.5-1980, IEEE Std 497-1981 and Reg Guide 1.97 Rev. 3
- Technology-neutral approach intended for advanced design plants
- Performance-based, non-prescriptive approach to accident monitoring variable selection
 - Prescriptive tables of variables are replaced by criteria for selection based on the accident mitigation functions in EOPs, etc.
 - This is the most significant difference from Reg Guide 1.97 Rev. 3
- Selected variable type determines the applicable performance, design, qualification, display and QA criteria
- Recent industry standards cited in the criteria
- Provides criteria for digital instrumentation



IEEE STANDARD 497-2002 CRITERIA

- Selection
 - Defines variable types A, B, C, D and E and lists typical sources
- Performance
 - Range; Accuracy; Response Time; Duration; Reliability
- Design
 - Single & Common Cause Failure; Independence; Separation; Isolation; Power Supply; Calibration; Portable Instruments
- Qualification ^{- Enu} _{- 503 m.c.}
- Display
 - Characteristics; Identification; Display Types; Recording
- Quality Assurance



DRAFT GUIDE DG-1128 (REGULATORY GUIDE 1.97, REV. 4)

- Responds to User Need Request NRR-2002-017
- Regulatory Guide 1.97, Revision 4, endorses IEEE Standard 497-2002 with exceptions and clarifications
- Intended for new nuclear power plants
- Conversion to this new method by current operating plants may be done on a comprehensive, voluntary basis
- Regulatory positions



DG-1128

REGULATORY POSITIONS

1. How might current operating plants using Rev. 2 or 3 of Reg Guide 1.97 apply the criteria
 - “The guidance provided in this standard may prove useful for operating nuclear power stations desiring to perform design modifications or design basis modifications.”
 - Licensees may be interested in converting to Rev. 4
 - IEEE Std 497-2002 provides no guidance in translating from RG 1.97 Rev. 3 to the IEEE Std 497-2002 selection criteria
 - Generally: Type A,B,C = Cat 1, Type D = Cat 2, Type E = Cat 3
 - ex.: Subcooling Margin Monitor is a Type B Cat 2 variable
 - New criteria may be more or less stringent than existing criteria
 - Partial conversions could result in an incomplete analysis
 - The draft guide recommends conversion to be comprehensive and is strictly voluntary by the licensee



DG-1128

REGULATORY POSITIONS (cont.)

2. Calibration during an accident

- IEEE Std 497-2002 requires this by means of recalibration, interval specification, equipment selection or cross-calibration
- DG-1128 reduces requirement to “extent possible.”

3. Does not address severe accidents

- IEEE Std 497-2002 requires Type C variables to have extended ranges
- DG-1128 clarifies the requirement for extended ranges based on current regulatory requirements



DG-1128 REGULATORY POSITIONS (cont.)

4. Excludes contingency actions from the scope of selecting variables
 - IEEE Std 497-2002 assumes all contingency actions are to mitigate accident conditions that are beyond the licensing basis of the plant
 - DG-1128 recommends considering all EOP actions for design basis events during the selection process, regardless of contingency or otherwise
5. Number of points of measurement
 - IEEE Std 497-2002 does not address this topic
 - DG-1128 states that the number of points of measurement should be sufficient to adequately indicate the variable value



APPROACHES CONSIDERED

1. Take no action
2. Revise Reg Guide 1.97 to incorporate approved deviations, clarifications and rule changes for current operating plants and endorse IEEE Std 497-2002 for current and new plants
3. Produce new regulatory guide 1.XXX to endorse IEEE Std 497-2002 for new plants and leave Regulatory Guide 1.97 at Rev. 3 for current plants
4. Revise Reg Guide 1.97 to endorse IEEE Std 497-2002 intended for new plants, and current plants may voluntarily and comprehensively convert to Rev. 4
 - This is the approach chosen by the staff
 - NRR and OGC have no technical or legal concerns



CONCLUSION

- DG-1128 (proposed Regulatory Guide 1.97, Rev. 4) endorses current IEEE Standard 497-2002 with exceptions and clarifications
- Consistent with NRC requirements
- SRP Chapter 7 will require updating
- Intended for new nuclear plants, with current operating plant conversion on a comprehensive, voluntary basis
- No backfit issues
- Final Comments or Questions?



Tabornsky notes
W. Kemper

NRC DIGITAL SYSTEM RESEARCH PLAN

Overview of Software Quality Assurance Program

3.2

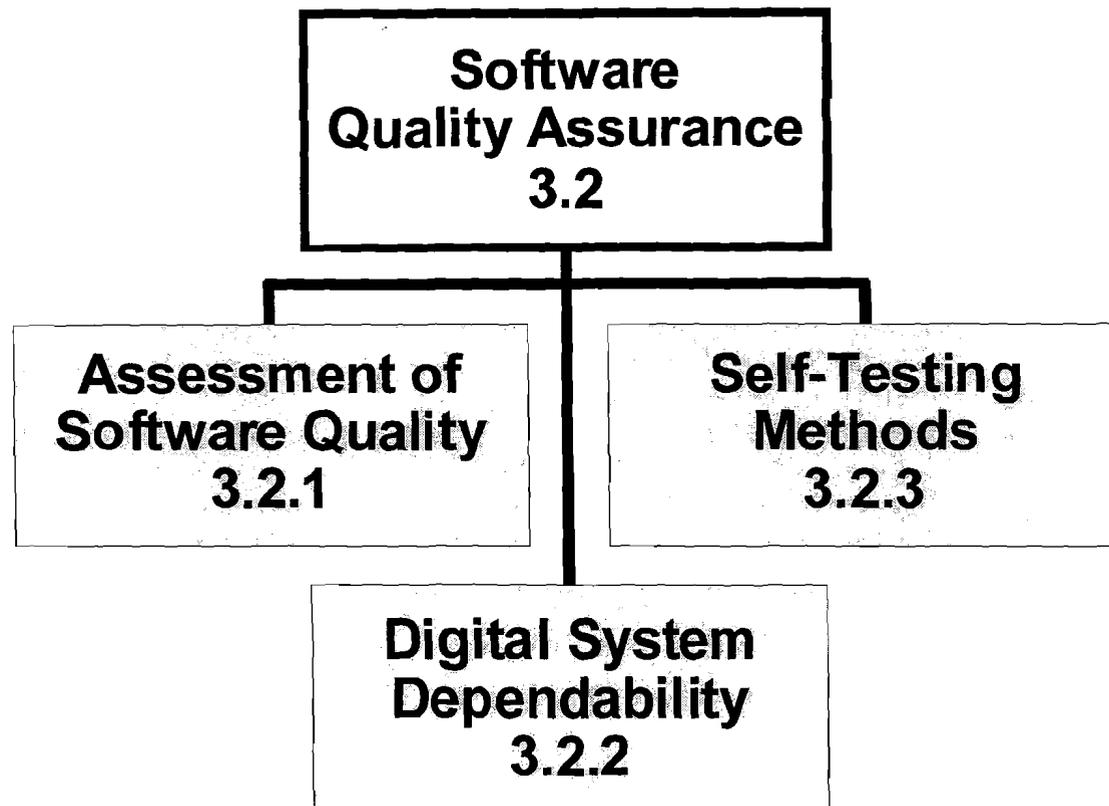
Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control subcommittee

June 14, 2005

William E. Kemper
Chief, I&C Engineering Section
Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-7585, wek@nrc.gov)



SOFTWARE QUALITY ASSURANCE PROGRAM 3.2





SOFTWARE QUALITY ASSURANCE

- NRC SRP Chapter 7, Rev. 4, June 1997 provides the regulatory framework for the review and approval of digital safety systems
- As part of its review of digital safety systems, NRC evaluates safety related software quality by reviewing
 - development processes (e.g., V&V, CM) and
 - Software development products (e.g., SRS, SDD, Test plans, Code listings, RTM) Software requirement specs
- The SRP is adequate to provide guidance (i.e., what to review) to the staff in performing safety reviews pertaining to digital safety systems



SOFTWARE QUALITY ASSURANCE

- Review and approval of digital safety systems currently depend on qualitative evaluations of digital system features and development processes
- *Software Quality Assurance* SQA evaluations are performed manually, without the aid of assessment tools or other means of obtaining quantitative measures of software quality
- NRC SRP Chapter 7 BTP HICB-14 identifies digital system development attributes that should be reviewed, but does not provide detailed guidance on the process for confirming that the software conforms to the acceptance criteria



SOFTWARE QUALITY ASSURANCE

- NRC reviews the results of software development processes and safety assessments, but the reviews do not include a means for independent assessments of software products

*want to create independent
NRC tools, like PRA and fuels have*

- Given the complexity and sophistication of current digital safety systems, **the goal of this Research Program is to provide independent assessment methods and objective acceptance criteria that can supplement and augment the existing guidance in Chapter 7 of the SRP**
- This information can be provided as formal review procedures for verifying consistency with SRP Guidelines, which could improve effectiveness and consistency of SQA reviews



SOFTWARE QUALITY ASSURANCE

- The current state-of-the-art in software system safety assessment includes a number of methods and tools for ~~quantitatively~~ assessing the quality of software:
 - Software system analysis techniques (e.g., Petri-net analysis, Markov Analysis, Dynamic Flow Modeling)
 - Software metrics
 - Formal verification methods
 - Testing Techniques (e.g., Data Flow Testing, Fault Injection, and Mutation Testing)



SOFTWARE QUALITY ASSURANCE RESEARCH FOCUS

- Research in this area will focus on assessing possible analysis methods that are currently used in design and analysis of safety critical software systems for use in the regulatory process
- Will focus on methods that have likely short term application without the need to do extensive development and apply these to nuclear industry applications
 - Fault injection testing has been used by a number of industries including some nuclear platform suppliers
 - Formal methods have been used in several industries to support safety critical applications
 - Software metrics are currently used for software quality control and continuous improvement (e.g., for programs at CMM level 4 and 5 respectively)



SOFTWARE QUALITY ASSURANCE SUMMARY

- This research area currently focuses on three initiatives to develop independent methods for assessing software quality and/or reliability
 - The use of Software Metrics to evaluate quality
 - The use of Fault Injection Techniques to evaluate digital system dependability
 - Technical guidance and review procedures for evaluating self-testing features in digital systems
- These research projects will provide objective acceptance criteria and review procedures that augment and supplement existing SRP guidance for approving (or denying) digital safety system license applications



Thornsbury notes
NCarte / MLi

3.2.1

ASSESSMENT OF SOFTWARE QUALITY

Norbert N. Carte
Steven A. Arndt
I&C Engineering Section
Office of Nuclear Regulatory Research
(301-415-5890, nnc@nrc.gov)
(301-415-6502, saa@nrc.gov)

Ming Li
University of Maryland
Center for Reliability Engineering
College Park, MD 20705
(301-405 1705, mli@wam.umd.edu)



OVERVIEW

(3.2.1 Assessment of SW Quality)

- Issues Facing NRC
- Current Research
- Future Work
- Conclusions



Issues Facing NRC

(Increasing Size and Complexity of Submittals)

- SW is Being Used in More Systems
- Increase in Use of Self Checking SW and Other Techniques Result in More Complex Systems
- More Powerful Development Environments
 - SW Programming is Becoming more Abstract
 - More Details are Hidden
- SW Engineering Methods are becoming more Powerful and Usable



Current Review Processes

(SRP Rev. 4 - June 1997)

- SW Development Process Review
 - Sample Thread Audits (Selected by Reviewer)
 - Manual
- Generic Plan
 - Requires Application Specific Review Plan
- Different Programming Paradigms
 - SP (i.e. C), OO (i.e. C++), & PLC (i.e. Function Block)
- Reg. Guides Endorse Generic IEEE Stds
 - The 3 SERs are for PLCs
- Does Not Address Use of Measures

*GA: this structure of
- here we are
- here are issues
- where we are going
needs to be in play*



Current Research Goals

The objective of this research is to perform a large scale validation of measures, identified previously, to quantitatively assess the quality of software.

- Quantifiable SW Quality Assessment
 - Incorporation of Measures
 - Standardized Quantifiable Evaluations
 - Objective Acceptance Criteria
 - Theoretical,
 - Benchmarked against Current Methodology, or
 - Benchmarked Theoretically
- Flexible
 - Useable by Licensee, NRC, and/or Both
 - Compare/Combine Different Assessments
 - Probability/Confidence Goals are Met (i.e. Bayesian), or
 - Normalized Quality Assessment (i.e. Defect Density or Reliability)
- Address Issues Raised Previously



Current Research

(Basis - Quantifying SW Quality)

- Large Body of Literature on Metrics (Both Technical & Managerial)
 - IEEE 982.1 Dictionary of Measures To Produce Reliable SW
 - IEEE 982.2 Guide for the Use of 982.1
 - IEEE 1061 Software Quality Metrics Methodology
 - “... the use of software metrics does not eliminate the need for human judgment in software evaluations. The use of software metrics within an organization or project is expected to have a beneficial effect by making the software quality more visible.”
 - IEEE 1045 Software Productivity Metrics
- Lawrence Livermore National Laboratory
 - Identified Pool of 78 Measures
- University of Maryland
 - Selected 30 Measures
 - Categorize Measures
 - Life-cycle Phase (i.e. Design, Test, ...), & Semantic Family (i.e. Size, Complexity, ...)
 - Breadth – Cover all Areas of Interest
 - Elicitation of Expert Opinion to Rank Measures & Families
 - Peer Review of Research Performed
 - Publication in peer Reviewed Journals *IEEE Transactions on software engineering*
 - Preliminary Validation - NUREG/CR-6848



Large Scale Validation

- Use a Sample of Measures for Validation
 - Ranking for use in Predicting Proper System Operation
 - Class of Measures
 - High Ranked Measures
 - Cyclomatic Complexity, Mean Time to Failure, Defect Density, & Coverage Factor
 - Medium Ranked Measures
 - CMM, Fault Days Number, Requirements Specification Change Requests, Requirements Traceability, & Test Coverage
 - Low Ranked Measure
 - Function Points, Bugs per Line of Code, Cause & Effect Graphing, & Mutation Testing
 - Family
 - Functional Size (i.e. Feature Point, Function Point, & Full Function Point)
 - Complexity (i.e. Cyclomatic Complexity)
- All Phases of SW Development
- Nuclear RPS (Safety System)



Large Scale Validation (Issues Raised Previously)

- NUREG/CR-6848
 - Peer Review
 - Relatively Small SW Application
 - Application Not a Nuclear Safety System
 - Benchmark of Measures did not use real Operational Profile
 - Looked at only one Phase of SW Development
 - Looked at a low Reliability System
- ACRS
 - Ease of Obtaining Metric
 - Ease of Use Evaluation will be Included in Final Report
 - SW Centric vs. System Approach
 - Uncertainty Greater than Required Reliability
 - Issue Not Visible in a Qualitative Evaluation Process
 - Measures “ ... do not eliminate the need for human judgment ...”
 - Validity / Robustness of Measures
 - Different Types of Functions (RPS vs. Door Entry)
 - Different Programming Languages (C & Assembler vs. C++)



Measures for Assessing SW Quality

- Goal
 - Quantify SW Quality through SW engineering measurement
- Philosophy
 - SW Quality is determined by:
 - Software product characteristics (number of defects)
 - Project characteristics
(application type, application's functional size, etc)
 - Process characteristics
(personnel skill, budget, development method, tools, etc.)
 - How software is used (operational profile)
- Steps:
 - Estimate the number of defects remaining in the SW
 - Quantify the likelihood that these defects result in System Failures



Defect Density

- Defect Density (DD) Definition
 - A ratio of unique defects found by inspections (requirements, design and code) to the size of the product.
 - Defects are classified into different criticality levels.
 - The product can be either requirements/design document or source code
 - Research on Defect Density
 - Included in IEEE Standard 982.2 “IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software”
 - A *de facto* standard measure of software quality [Fenton].
 - Quality indicator: Grady 1987, *IEEE Software*
 - Quality indicator: Mohagheghi, 2004, ICSE
 - Module size vs DD: Malaiya 2000, ISSRE
 - etc.
- Does not capture requirements "defects"
← other metrics would capture



Defect Density

- Number of Known Defects
 - # of defects = $DD * Size$
- Number of Latent Defects
 - Capture/Recapture (CR) models: were initially developed to estimate the size of an animal population.
 - The use of CR models in software inspection
 - # of defects ~ Animal population size
 - Inspectors ~ Traps
 - Error discovery ~ Animal trapped and marked



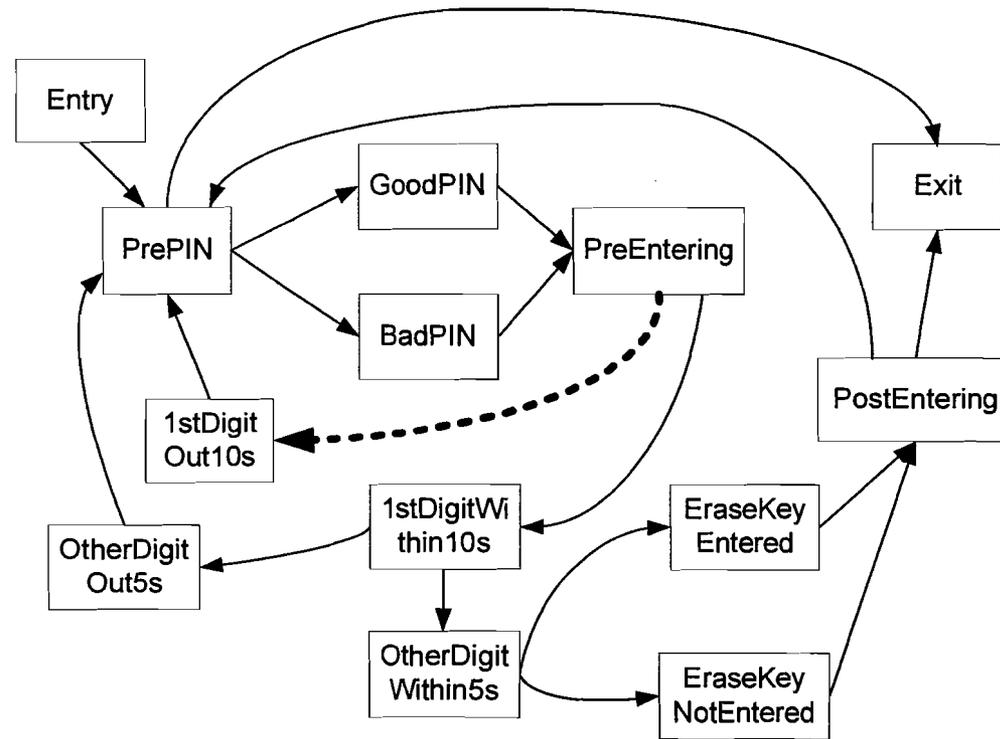
System Failure Estimation

- From Defect to Failure
 - E: probability that a particular section of a program (termed “location”) is executed.
 - I: probability that the execution of a problematic location (defect) affects the data state.
 - P: probability that an infection of the data state affects system output.
- DD RePS
 - The probability of failure per demand is given by:



Estimation of Impact of Defect Density to an Example System

- Quantification (Defect Propagation)
 - Finite State Machine Model (FSM)
 - An Example





Test Coverage (Statement)

- Test Coverage (TC) Definition
 - The portion of SW statements executed against a set of test cases.
- Research on Test Coverage
 - Included in IEEE Standard 982.2 “IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software”
 - Widely accepted in industry to control testing process:
 - Fenton, Pfleeger, 1997, PWS Publishing
 - Briand, Pfahl, 2000, *IEEE Transactions on Reliability*
 - # of defects vs. TC: Malaiya 1994, ISSRE.



Test Coverage

- Test Coverage vs. Number of Defects
 - Derive the number of defects remaining from the number of defects found in testing.

*Empirical
curve fit
equation*

C_0 : defect coverage

C_1 : statement coverage

a_0, a_1, a_2 : coefficients

N : number of defects remaining

N_0 : number of defects found in testing



Test Coverage

- Number of Defects and Impact on System Operation
 - K : fault exposure ratio obtained using the finite state machine model.



Current Project Status

	<u>Completion Date</u>
• Measurement in Progress	
– Completeness	June 22
– Requirements Traceability	July 7
– Requirements Spec. Change Request	July 8
– Test Coverage	July 15
– Coverage Factor	July 31
– Fault Days Number	August 15
– Defect Density	August 31
• Analysis in Progress	
– Operational Profile	July 15
– Finite State Machine	August 15
– Testing	August 15
– Calculations & Comparisons	September 30



Current Project Status

(Preliminary Results)

- Measurement Completed (No. of Defects Predicted)
 - High Ranked Measures
 - Cyclomatic Complexity (210.37)
 - Medium Ranked Measures
 - CMM (4.58)
 - Low Ranked Measures
 - Function Point (8.0)
 - Bugs per LOC (590)
 - Cause Effect Graphing (5)



Future Work

- Large Scale Validation
 - Develop Regulatory Guidance
 - Acceptability of Methods
 - Acceptance Criteria
 - Benchmark
 - Other Industries
 - Training on Usable Measures
- Coordinate Subsequent Research with NRR
 - Validate & Train on Additional Measures
 - Technology Specific Measures (i.e. PLC)



Conclusions

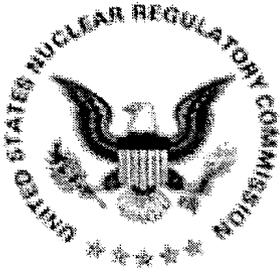
- SW Engineering Measures are Sufficiently Mature for use in Assessing SW Quality in Safety Related Nuclear Applications *very strong*
- Measures of SW Quality are Related to Proper System Operation
 - This large scale validation project provides a promising methodology for estimating the impact of SW quality on proper system operation.



System Failure Estimation

- From Defect to Failure
 - E: probability that a particular section of a program (termed “location”) is executed.
 - I: probability that the execution of a problematic location (defect) affects the data state.
 - P: probability that an infection of the data state affects system output.
- DD RePS
 - The probability of failure per demand is given by:

$$p_s = \int_i E(i) * I(i) * P(i)$$



Test Coverage

- Test Coverage vs. Number of Defects
 - Derive the number of defects remaining from the number of defects found in testing.

$$C_0 = a_0 \ln[1 + a_1 (\exp(a_2 C_1) - 1)]$$

$$N = \frac{N_0}{C_0} - N_0$$

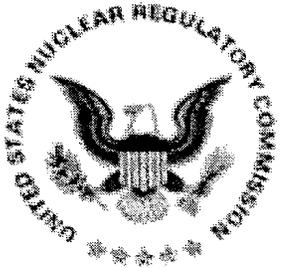
C_0 : defect coverage

C_1 : statement coverage

a_0, a_1, a_2 : coefficients

N : number of defects remaining

N_0 : number of defects found in testing



Test Coverage

- Number of Defects and Impact on System Operation

$$p_s = e^{-\frac{K}{T_L} N \tau}$$

$$\nu K = \frac{K}{T_L} \tau$$

$$p_f = 1 - e^{-\nu KN} \approx \nu K \times N$$

- K : fault exposure ratio obtained using the finite state machine model.



Thornsbury notes
5 Arndt / R Shaffer

DIGITAL SYSTEM DEPENDABILITY (3.2.2)

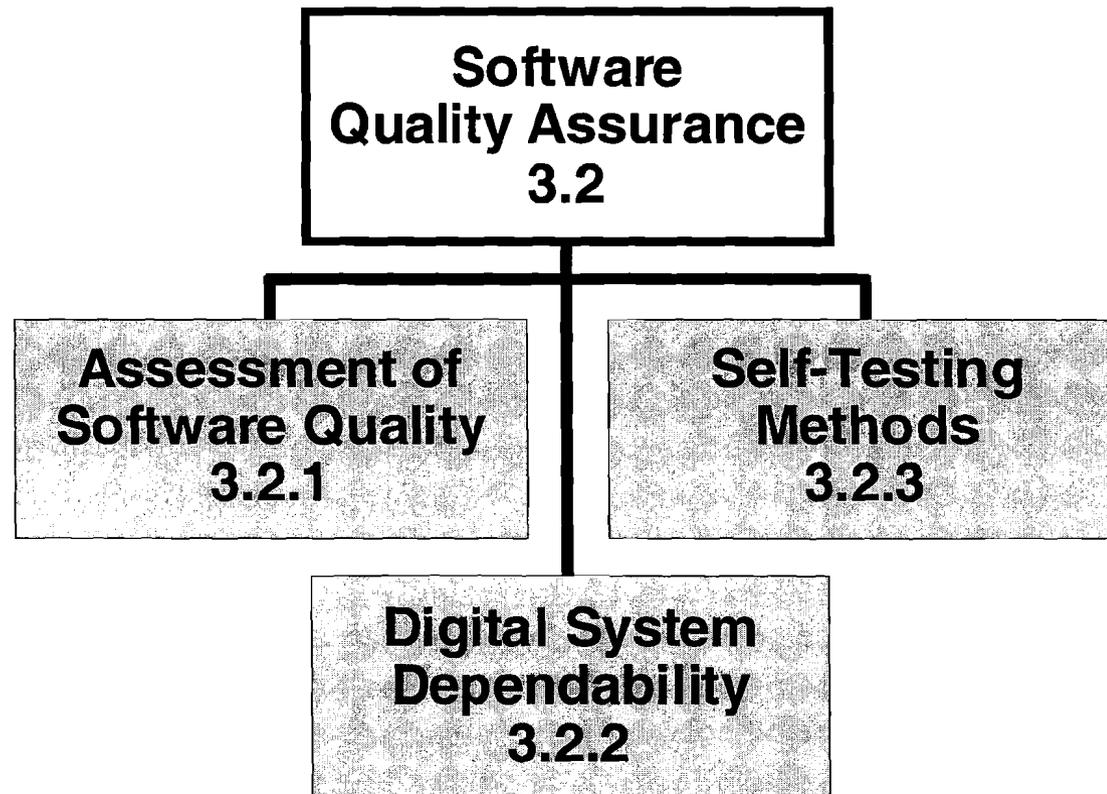
Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Sub-committee Meeting

June 14, 2005

Roman Shaffer and Steven Arndt
Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-7606, ras3@nrc.gov, 301-415-6502, saa@nrc.gov)



SOFTWARE QUALITY ASSURANCE PROGRAM 3.2





~~SOFTWARE QUALITY ASSURANCE~~

- The current state-of-the-art in software system safety assessment includes testing techniques such as fault injection testing that permits analysis of the systems under review
- Information obtained as part of testing can support software system analysis techniques (Petri-net analysis, Markov, DFM, etc)
- Methods can be use to Characterize the behavior of digital systems



3.2.2 DIGITAL SYSTEM DEPENDABILITY: OVERVIEW

- GOALS
- MOTIVATION
- CONCEPTS
- PROCESS
- PROJECTS
- CONCLUSION



3.2.2 DIGITAL SYSTEM DEPENDABILITY: GOALS

- Support acceptability decision-making pertaining to digital system safety
- Refine the technical basis for digital systems to obtain objective acceptance criteria
- Augment and supplement current process with modeling/analysis methodology and tools that are not technology dependent



3.2.2 DIGITAL SYSTEM DEPENDABILITY: GOALS, cont.

- Understand behavior of hardware/software systems
 - Under the influence of internal and external faults
 - Analyze any consequent errors that might produce system failures

- Properly characterize and analyze systems for:
 - Performance
 - Reliability/Availability
 - Failure modes
 - Subsystem and system safety
 - Integration into PRAs

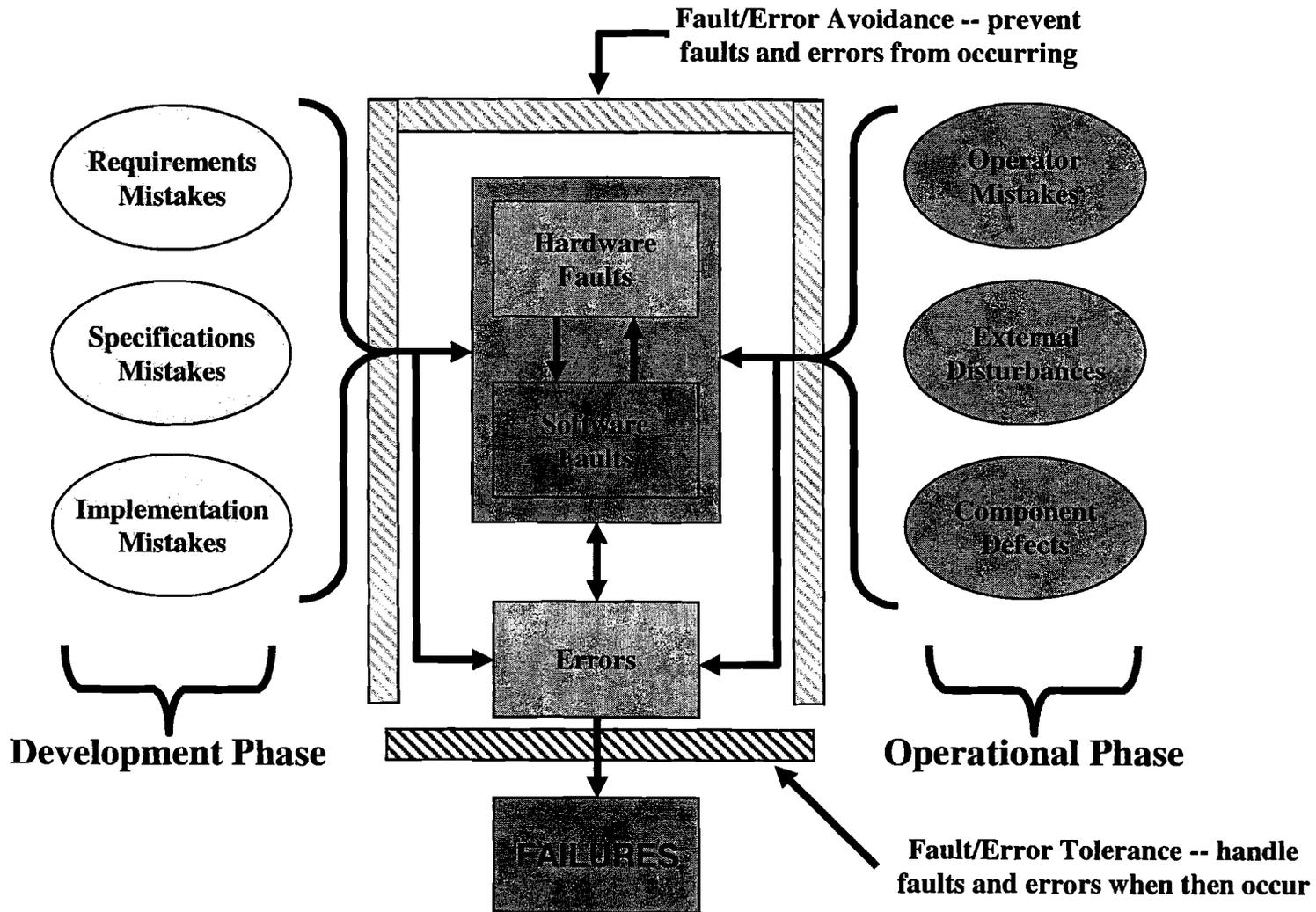


3.2.2 DIGITAL SYSTEM DEPENDABILITY: MOTIVATION

- Data and experience indicate that:
 - Software in digital systems can have severe design defects even after V&V
 - There is a greater reliance on software-based systems
 - Digital hardware components can have design and random defects
 - The interaction of hardware and software defects can cause a new class of defects
- Understanding of defects
 - How frequent are defects triggered?
 - How critical are the defect on the system?
 - What are the practical methods for determining their risk?

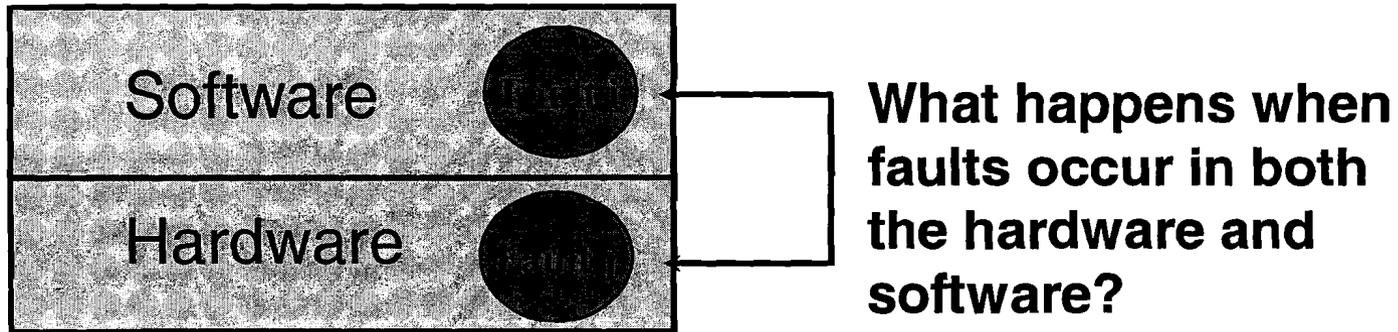


3.2.2 DIGITAL SYSTEM DEPENDABILITY MOTIVATION, cont.





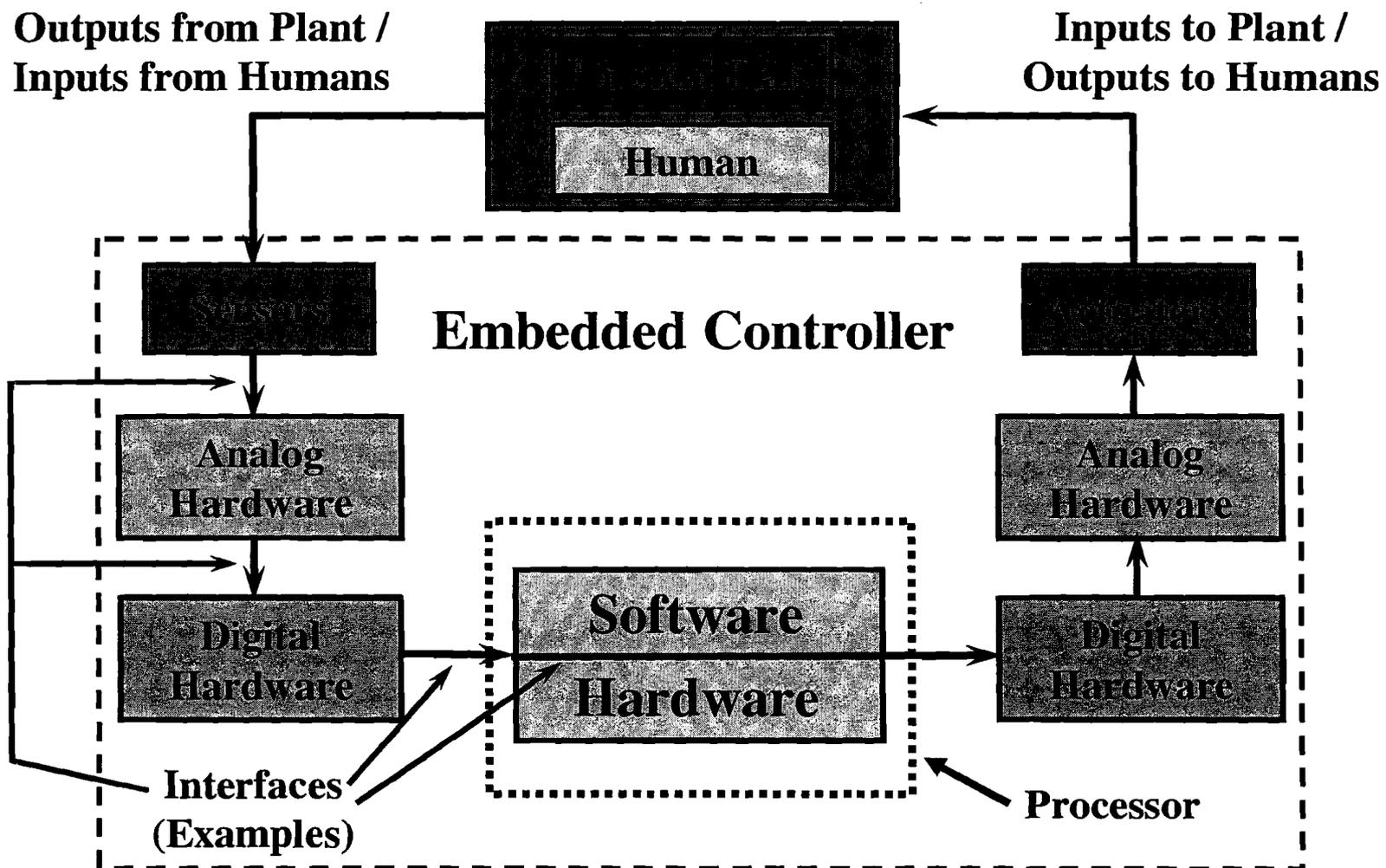
3.2.2 DIGITAL SYSTEM DEPENDABILITY MOTIVATION, cont.



- Software must execute on a hardware platform. The operation of the integrated hardware/software system is critical.
- A fault in software (Fault i) in combination with a fault in hardware (Fault j) could result in unsafe conditions and/or unreliable operation.
- Much of the software in safety-critical systems is designed to handle fault detection, fault location, fault isolation, and fault recovery. Such software may not be exercised sufficiently.



3.2.2 DIGITAL SYSTEM DEPENDABILITY: MOTIVATION, cont.





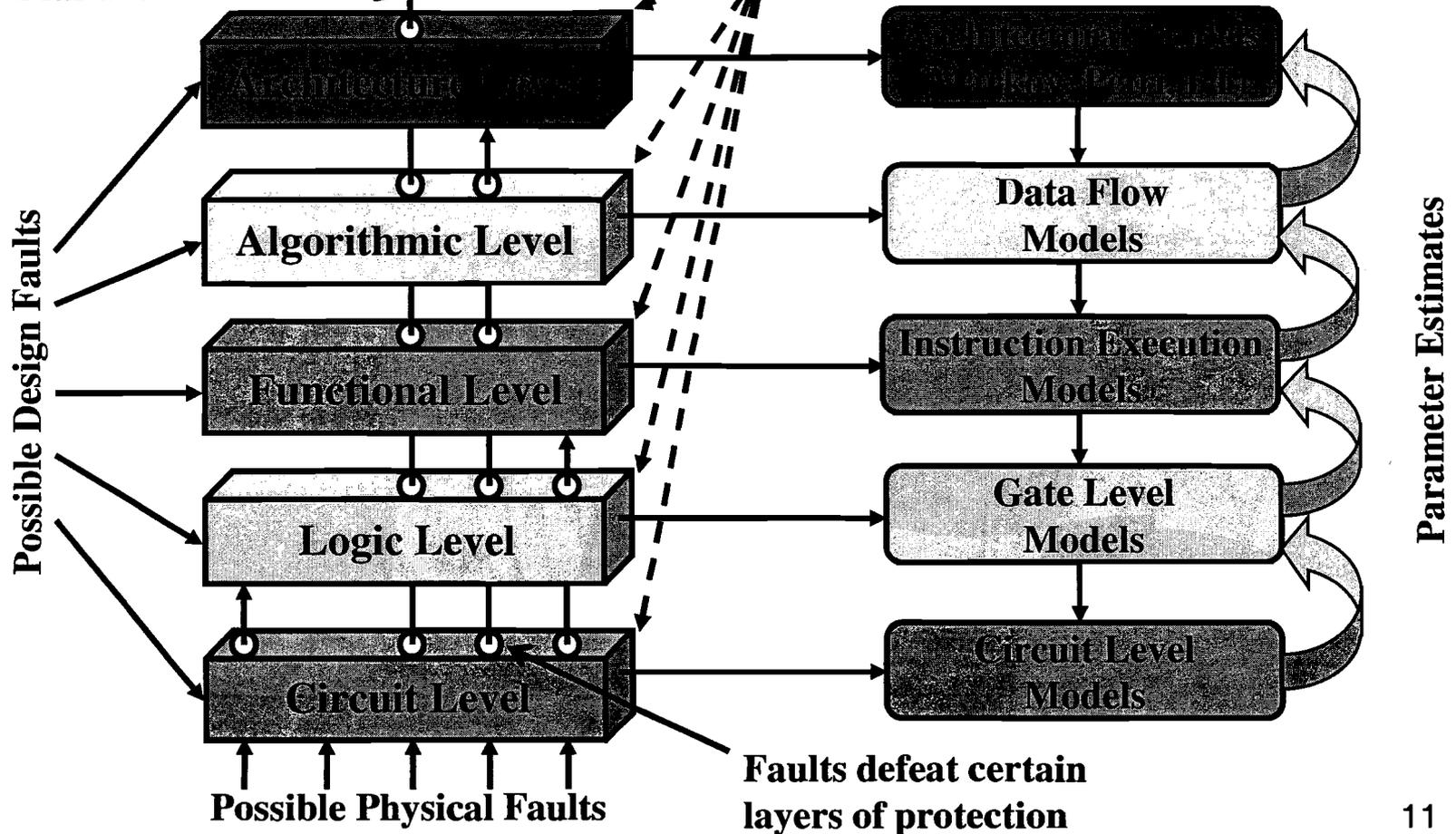
3.2.2 DIGITAL SYSTEM DEPENDABILITY: CONCEPTS

Faults that defeat all layers yield system failure

System Failure

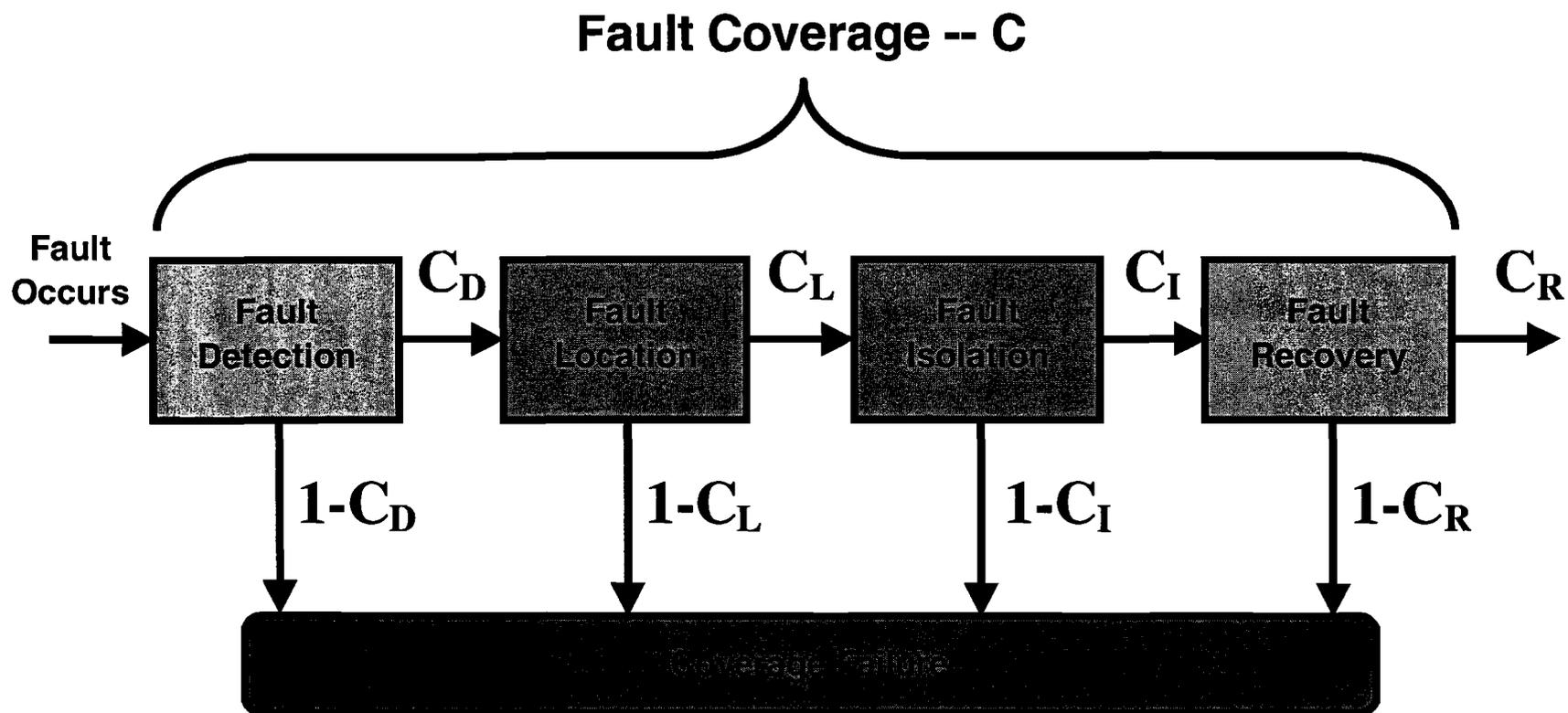
Layers of Design and Protection

Layers of Modeling





3.2.2 DIGITAL SYSTEM DEPENDABILITY: CONCEPTS, cont.



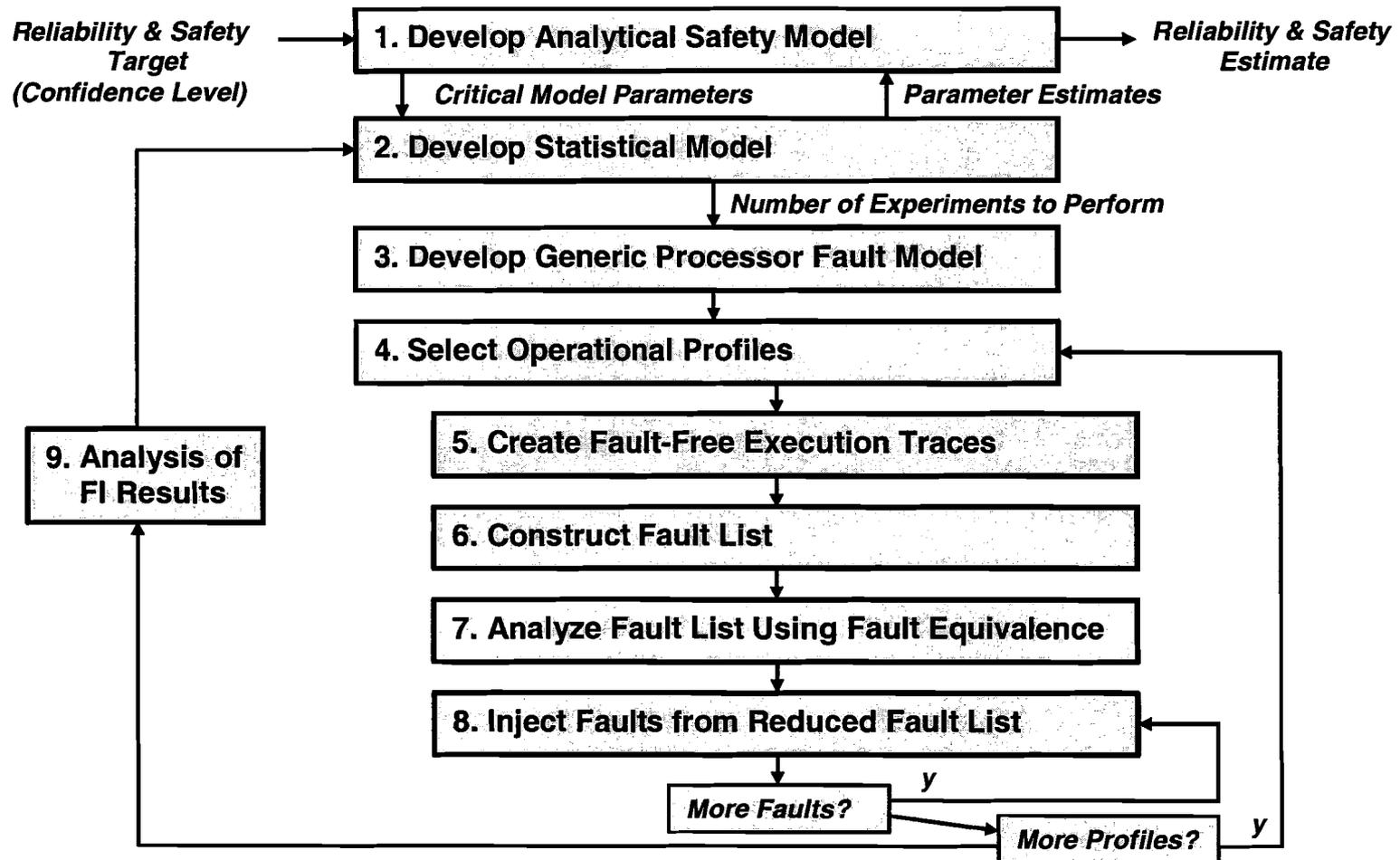


3.2.2 DIGITAL SYSTEM DEPENDABILITY: CONCEPTS, cont.

- **Digital reliability assessment methods**
 - **Several reliability assessment methods have been used by other industries and show potential for use in the nuclear industry**
 - **The Digital System Dependability research will undertake several case studies of nuclear-qualified digital systems**
 - **Achieve better understanding of failure behavior**
 - **Diverse applications of the methodology**
 - **Criteria for their proper use will be developed in order to supplement and augment the current regulatory process**

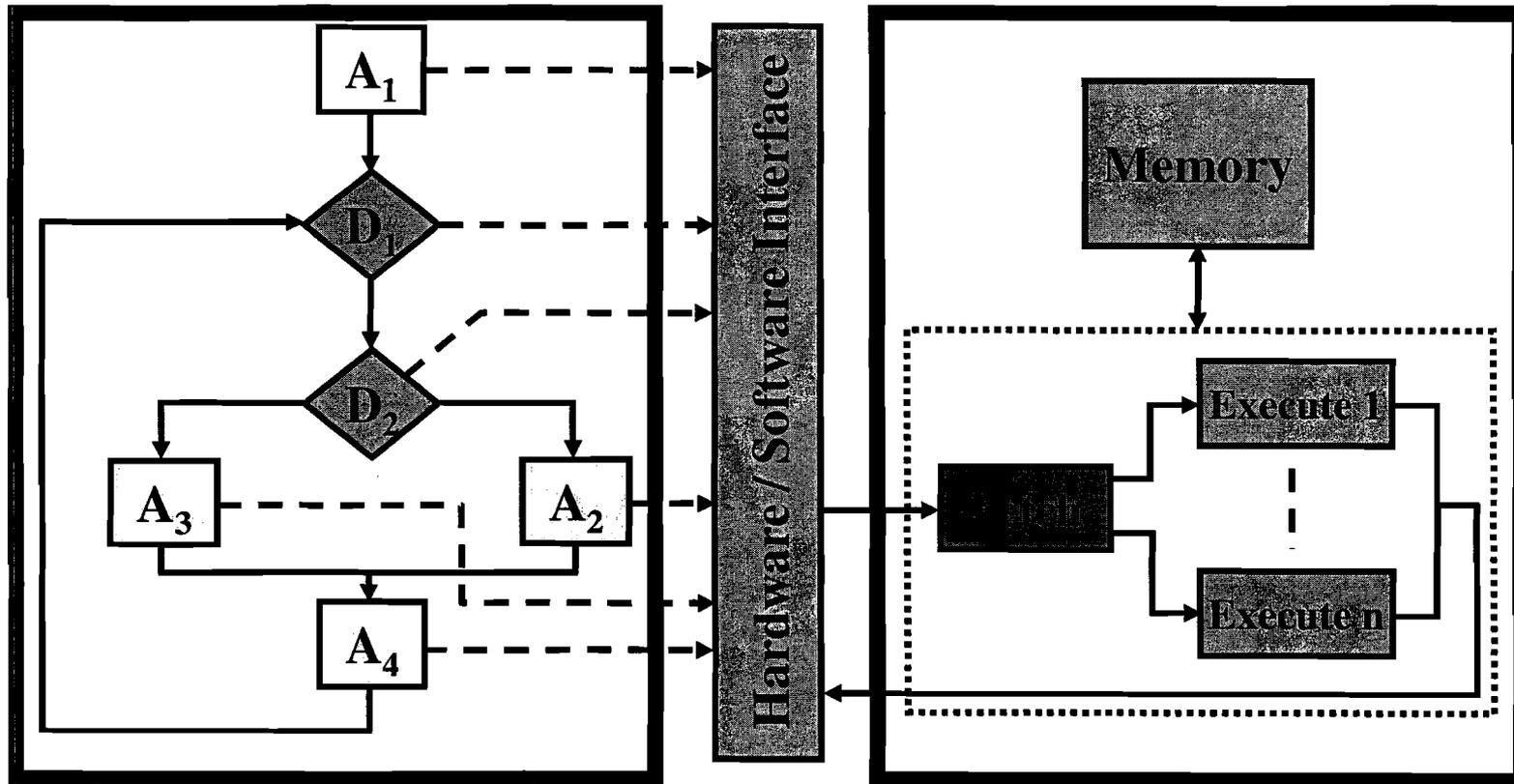


3.2.2 DIGITAL SYSTEM DEPENDABILITY: PROCESS





3.2.2 DIGITAL SYSTEM DEPENDABILITY: PROCESS, cont.



Software Model

- Data Flow
- Actual Code

Hardware Model

- Execution Model
- Gate-level Model



Analytical Model

- The analytical safety model provides the mathematical framework for calculating Reliability and/or Safety estimates
- Represents the faulty behavior of the system under analysis
- Several suitable analytical modeling techniques available from the literature
- Critical model parameter of interest is Coverage

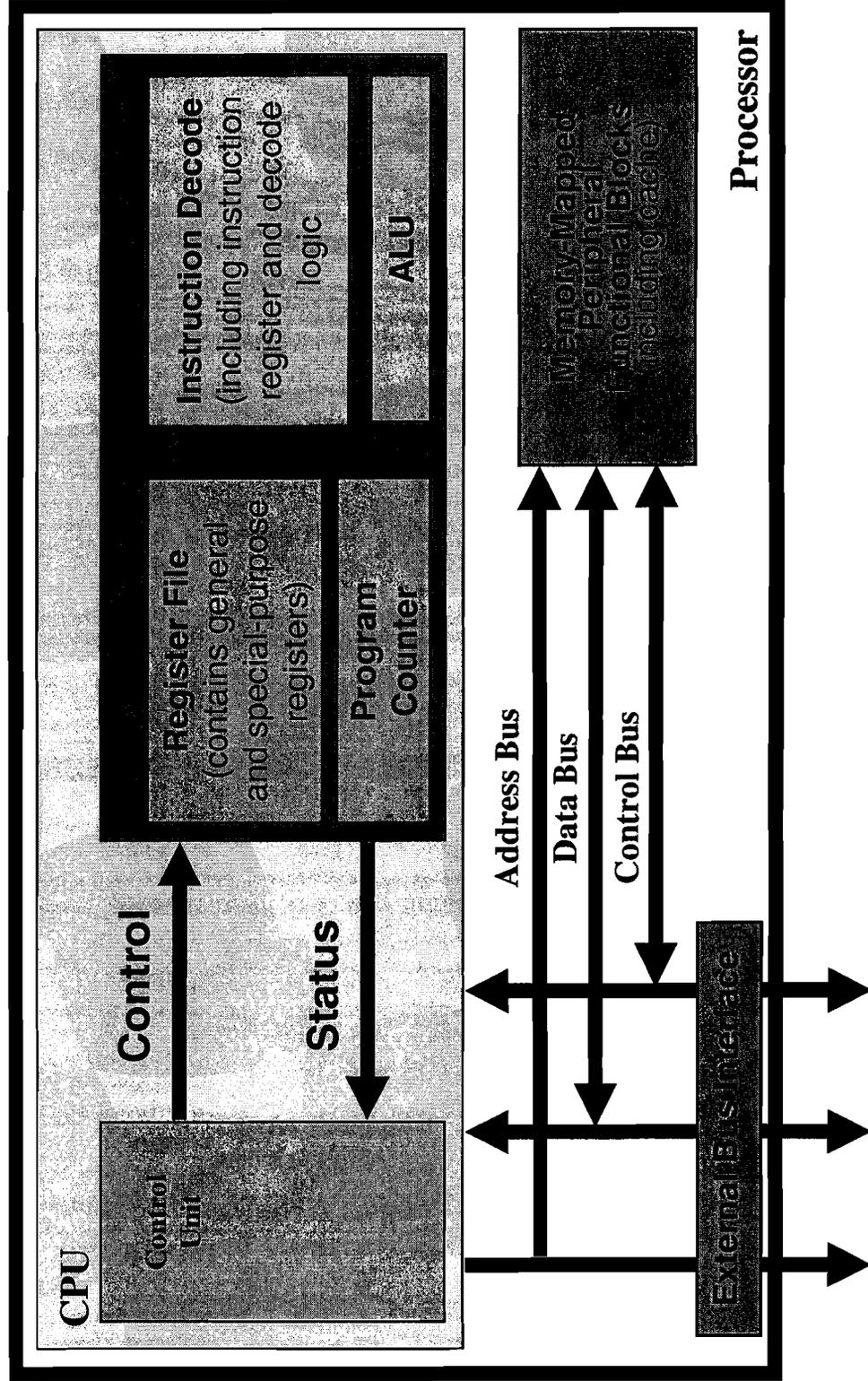


Statistical Model

- The statistical model is used to estimate the critical model parameters required by the analytical model
- Several statistical models from the literature can be used to estimate critical model parameters
- The statistical model is also used to determine the number of fault injection experiments necessary to achieve the desired confidence levels of the parameter estimates



Generic Processor Fault Model, cont.





Operational Profiles

- Operational profiles to be used in the experiments must be representative of the system under various modes of operation and configuration
 - light workloads
 - heavy workloads
- Transient and permanent faults have different activation characteristics under different workloads

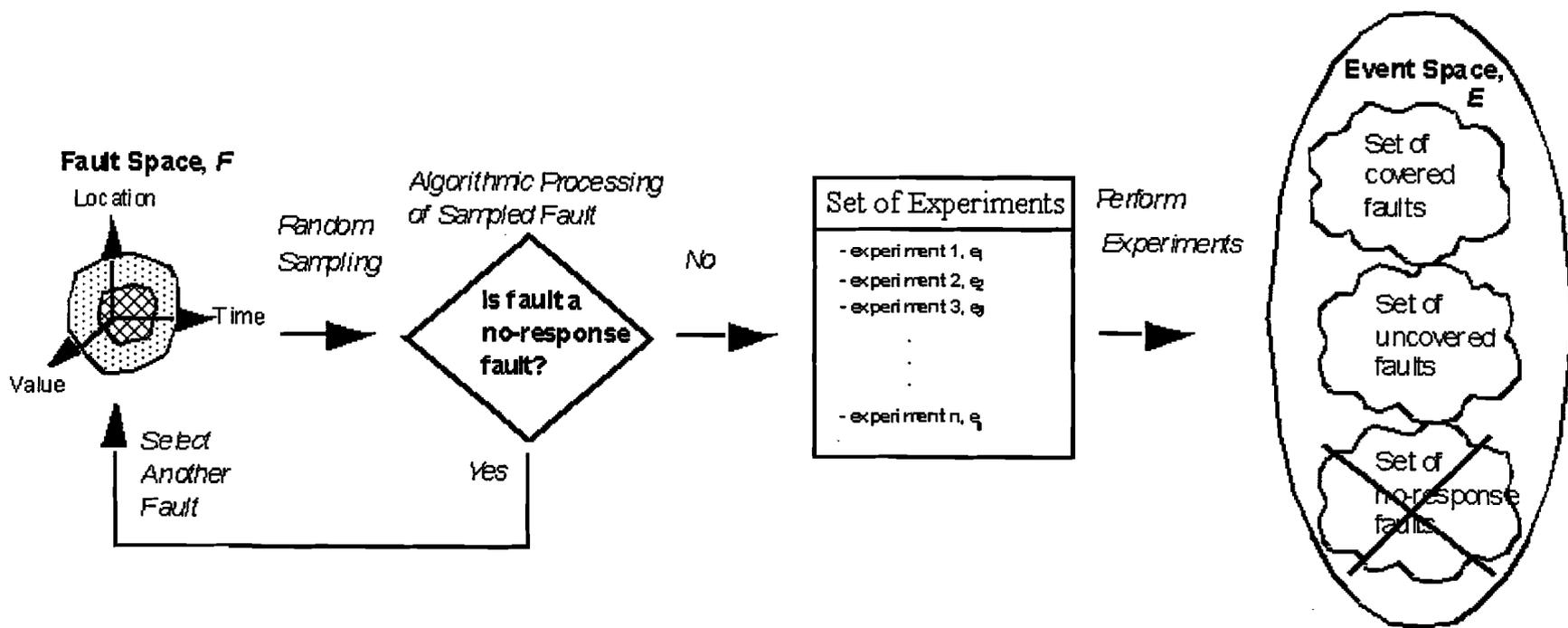


Fault-free execution traces

- For each operational profile selected, a fault-free execution trace must be created
- Trace contains sequence of instructions as well as state information that is visible
- Experimental environment is used to generate trace using Logic analyzers, Bus analyzers, In-circuit emulators, and Software debuggers
- Effectiveness of the fault list generation and analysis efforts depends on amount of detail in fault-free execution trace

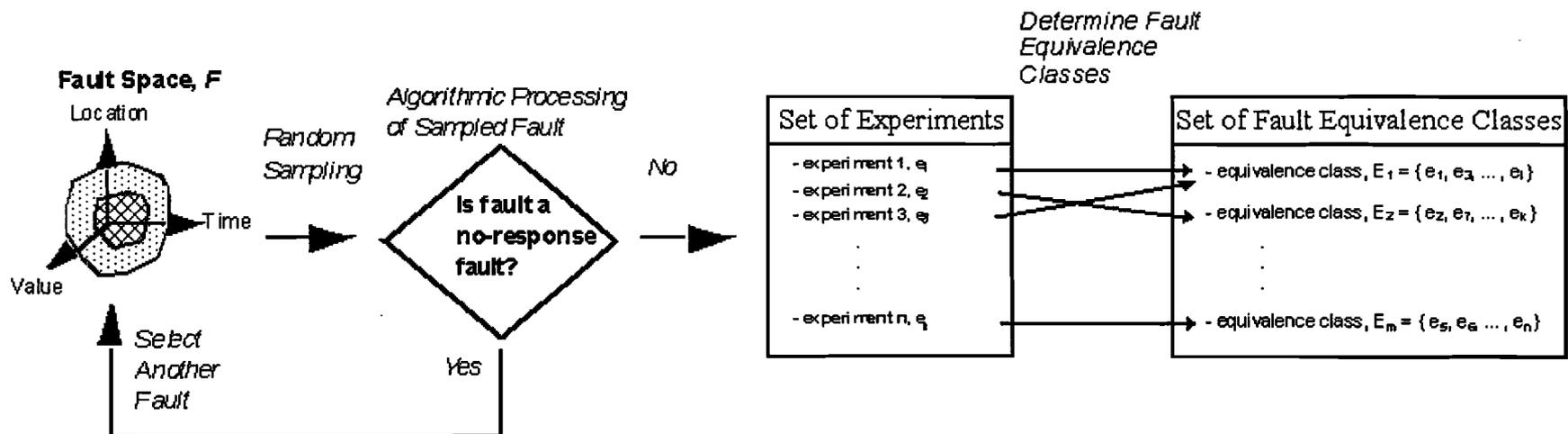


Fault list construction





Fault Equivalence





Fault-Injection Methods

- Hardware-based fault injection
 - Augment system with fault injection hardware to allow injections at pin-level (or sometimes internal to processor)
- Software-based fault injection
 - System software is modified in order to provide the capability to modify the system state (processor registers and memory) according to programmer's model
- Simulation-based fault injection
 - Construct a simulation model, including detailed model of processor
- Hybrid approaches
 - Combinations of above three approaches



3.2.2 DIGITAL SYSTEM DEPENDABILITY: RESEARCH PROJECTS

- Digital Feedwater Control System assessment, continuing under cooperative agreement with OSU
- Digital System Dependability Performance
 - Kick-off end of FY05
 - Multi-year effort
- Future effort will explore other dependability metrics (i.e., maintainability, confidentiality, integrity)



3.2.2 DIGITAL SYSTEM DEPENDABILITY: RESEARCH PROJECTS, cont.

- Digital System Dependability Performance
 - Work with vendors and licensees to
 - Obtain access to safety systems
 - Obtain engineering support on determine relevant design details
 - Perform fault-injection testing following the process described earlier
 - Approximately 12 months per system evaluation



3.2.2 DIGITAL SYSTEM DEPENDABILITY: CONCLUSION

- The Digital System Dependability research will augment and supplement the current regulatory process by:
 - Characterizing significant hardware, software and interface errors;
 - Understanding potential new failure modes and the criteria for detecting these failure modes;
 - Identifying or developing methods and data that enable the NRC to establish the risk of digital safety systems; and
 - Modeling of digital systems that could be used to provide system reliability metrics.



Thornsby notes
SArndt

SELF-TEST METHODS PROJECT 3.2.3

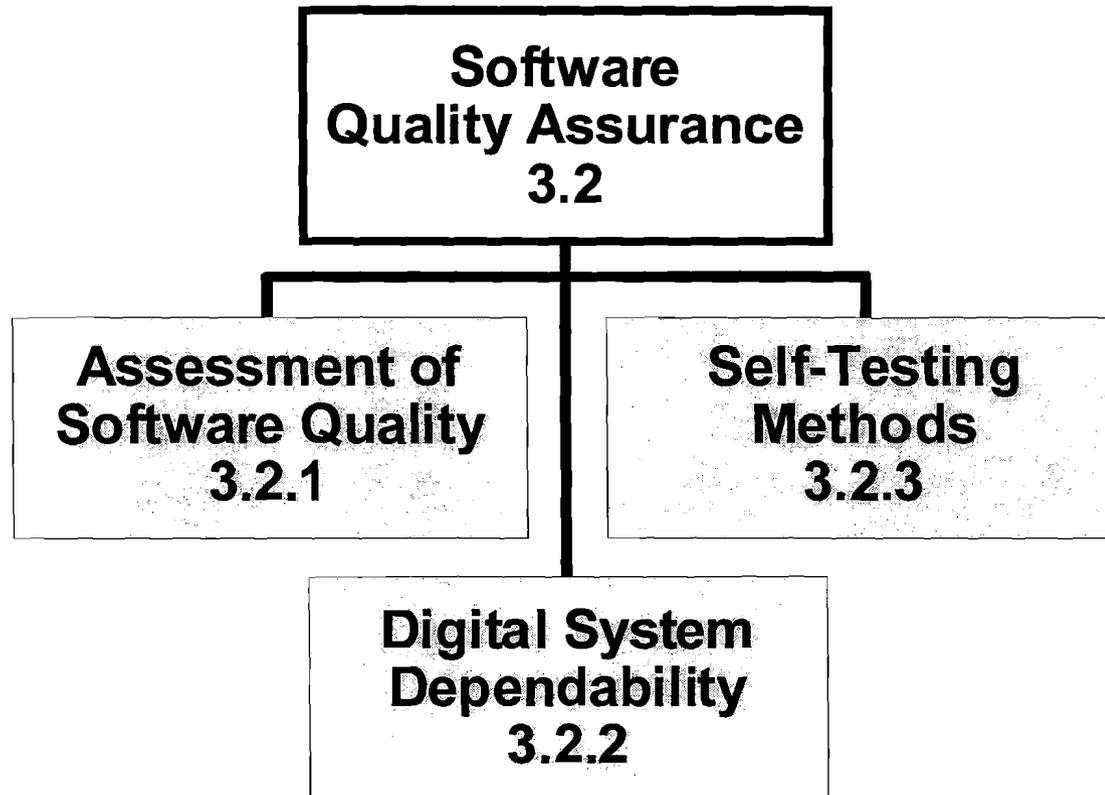
Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 14, 2005

Steven A. Arndt
Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)



SOFTWARE QUALITY ASSURANCE PROGRAM 3.2





OVERVIEW

- Self-testing methods test hardware and software on a continuous basis to improve system availability
- Because of the power of the systems has dramatically increased over the few years the overhead associated with self-testing methods are less of a concern
- Self-testing is used in basic acceptance tests as well as a number of fault tolerant applications including recovery blocks, N-version programming, etc.
- There is no consensus as to how to trade increased availability associated with self-testing versus the negative effects of increased code size and complexity



CURRENT SITUATION

- Currently NRC reviews of digital safety systems focus on safety function of the digital system
- Only limited focus is placed on interaction of self-testing features with safety functions
- Staff resource and time constraints during reviews limit the amount of time that can be spent on self-testing features



Self-testing Methods Research Program

- Technical issues concern
 - Effectiveness in determining system performance
 - Adverse effects on safety system performance
 - Identifying acceptable self-testing methods
 - The amount of self-testing that is sufficient
- This research project will develop technical guidance and review methodologies for evaluating self-test features in digital systems



SUMMARY

- This research will provide technical guidance regarding the use and review of self-testing features in digital systems
 - The effect of self-test methods on system performance
 - Characteristics of self-testing methods that might have adverse effects on safety systems performance
 - Develop information that will permit assessment of the most appropriate amount of self-testing
- Answer the questions
 - How much self-testing is enough, how much is too much
 - What kind is appropriate for real-time safety-critical and what kind is not appropriate



Thornsbury notes

S Arndt

OVERVIEW OF RISK ASSESSMENT OF DIGITAL SYSTEMS PROGRAM 3.3

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 14, 2005

Steven A. Arndt
Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)



OVERVIEW

- NRC PRA Policy Statement
- Research is oriented toward improving NRC knowledge and providing more consistent processes for regulating digital system applications
 - Gathering, understanding and using failure data
 - Assessing what modeling methods might be usable
 - Determining which systems need to be modeled and at what level of detail
 - Developing and testing methods
 - Developing regulatory acceptance criteria



CURRENT SITUATION

- Issues facing NRC
 - Licensees are replacing analog systems with digital systems
 - Licensing these digital systems presents challenges to NRC
 - Some of the current licensing criteria (BTP-19) are difficult to meet
 - Industry has expressed interest in using risk-informed regulation (Regulatory Guide 1.174) as an alternate method for licensing these systems
 - Research into the limitations of digital systems reliability modeling to support the needed analysis does not currently support expanded use of risk information in licensing digital systems
 - As the NRC licensees replace analog systems with digital systems the current PRA's are not keeping up with these changes
 - NRC risk analysis tools and data (SAPHIRE and SPAR models) do not provide an independent means of assessing licensee analyses at present



ACRS Comments 6/9/2004

- In additional comments to the June 9, 2004, ACRS letter, Prof. George Apostolakis recommended that:
 - Databases containing software-induced failures should be reviewed and their conclusions should be used
 - Available methods for assessment of reliability of systems that are software driven should be reviewed critically



Digital System Risk Program

- **The research program is designed to use available information, including failure data and known capabilities of available methods to develop the needed outcomes**
- **Available methods and tools for including digital system models will be reviewed and the most promising ones will be investigated**
- **Review of current data and development of application-specific databases will be completed**



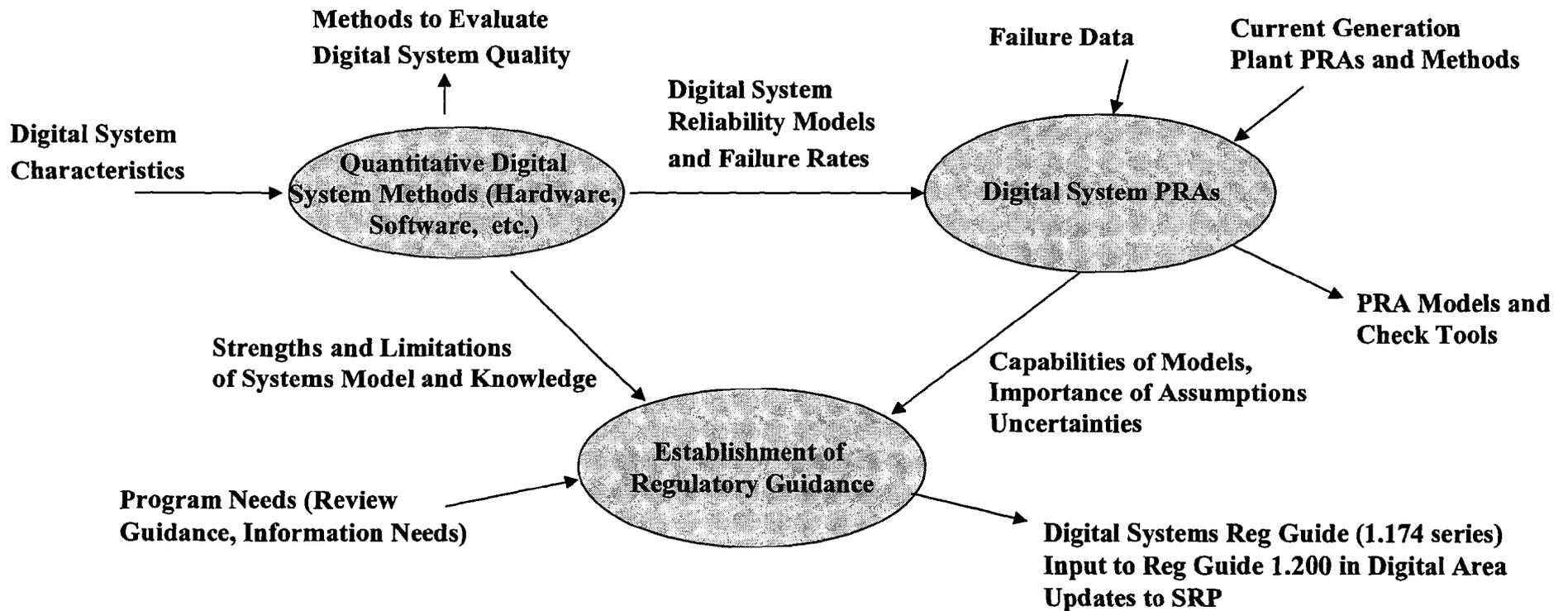
Digital System Risk Program

- **New methods for integrating current digital system models into PRAs will be developed**
 - Pilot methods using both traditional methods and dynamic methods using models
 - Benchmarks of the capabilities of several methods will be completed
 - Uses and limitations of both methods will be explored
- **Guidance for regulatory applications involving digital systems reliability**
 - acceptance criteria
 - limitations
 - evaluation methods
 - reliability data



NRC Approach Verse EPRI Approach

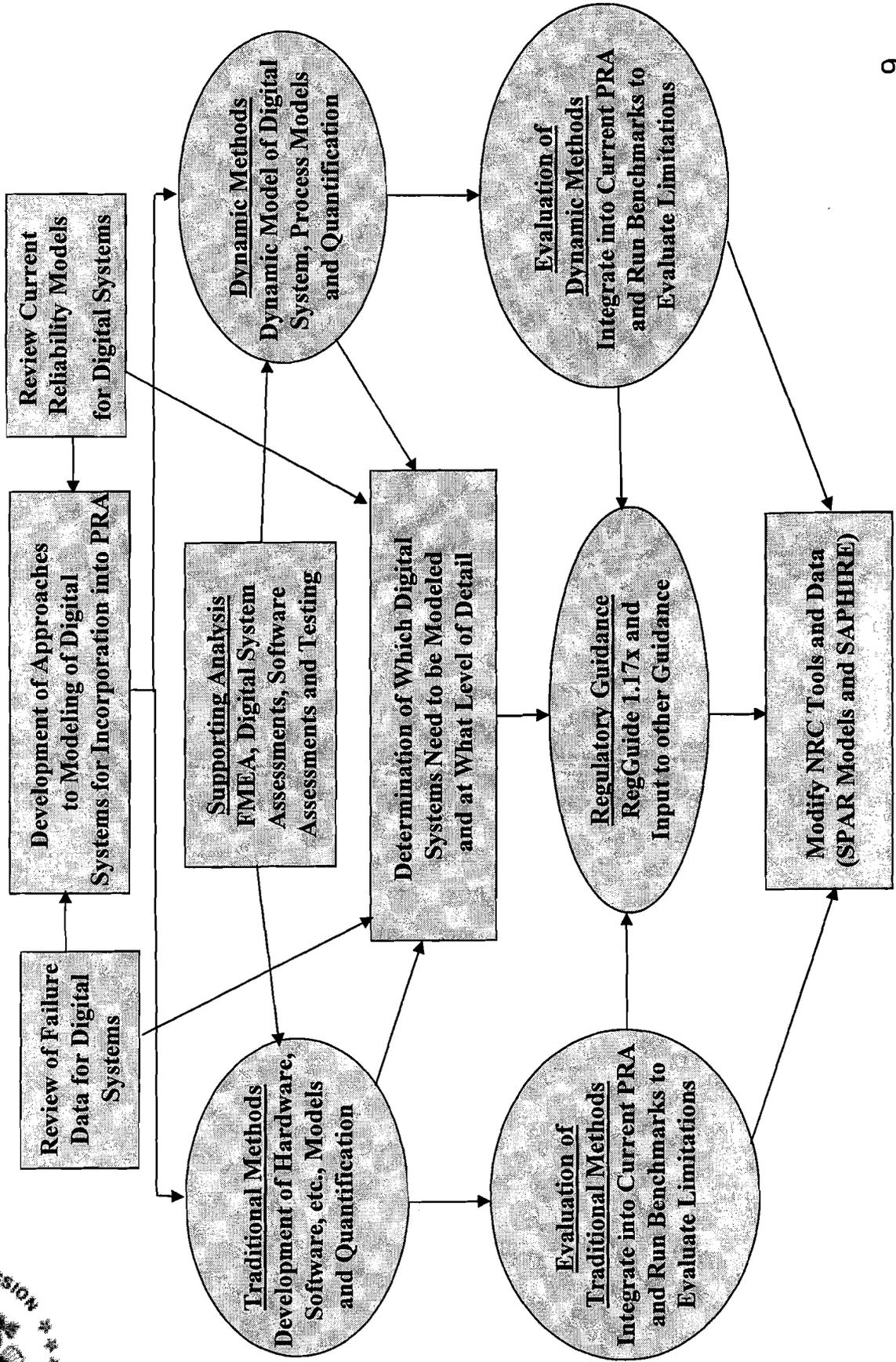
- EPRI has proposed a method for incorporating digital systems into current generation PRAs to support their Diversity and Defense-in-Depth Topical Report (TR-1002835)
 - Includes digital systems with assumed failure rates and beta factors based on IEC 61226 and other assumptions
 - Relies on digital system failure probabilities being bounded compared to the probability of random hardware failures
 - NRC research is focused on development of detailed models of digital systems and development of reliability modeling methods that can integrate these models into traditional PRAs
 - Review of available methods
 - Development of both traditional and dynamic methods
 - Investigation of what models are acceptable
 - Benchmarking results
- under acceptance review at NRC*



NRC Digital System Risk Program

for some applications,
less sufficient models
may be adequate

NRC Digital System Risk Program





RESEARCH FOCUS

- **Structured to support three major outcomes**
 - Determine what systems need to be modeled, at what level of detail, and what level of accuracy
 - Develop new capability to support independent analysis of digital systems
 - New or modified versions of current NRC PRA tools and data
 - Develop acceptance criteria for application of risk-informed approaches
- **Broad-based research, focusing on review of possible methods, and data to support reliability analysis and acceptance criteria**



DEVELOPMENT AND ANALYSIS OF DIGITAL SYSTEM FAILURE DATA

- To assess failure probabilities the NRC needs to have a standard process for collecting, analyzing, and using digital system data
- There is currently very little directly applicable failure data
- This part of the research will
 - Collect and assess digital system failure data (from international databases, LER database, EPIX, data from other industries, etc.)
 - Evaluate digital system failure assessment methods and data used by defense, aerospace, and other industries
 - Develop a process to identify the frequency, severity, cause, and possible prevention of digital system failures
 - Maintain the digital system reliability data to support modeling of digital systems in PRAs



INVESTIGATION OF DIGITAL SYSTEM RELIABILITY METHODS

- ACRS recommended that NRC review methods for assessment of the reliability of software driven systems
- Guidance and criteria on the use of these methods and how to support risk assessments of digital systems in an integrated process needs to be defined
- This part of the research will
 - Survey analytical methods for identifying digital system faults and their impact on safety
 - Describe the advantages and disadvantages of each method
 - Provide guidance for using digital system failure assessment techniques, and the criteria for using the techniques



INVESTIGATION OF DIGITAL SYSTEM CHARACTERISTICS IMPORTANT TO RISK

- PRAs currently model digital systems as “black boxes”
- There is not a clear understanding as to what level of detail is needed to support inclusion of digital systems into PRAs
- An approach and acceptance criteria is needed for developing digital system PRAs and reviewing risk-informed applications
- This research project will
 - Evaluate risk models of digital systems
 - Identify systems to be modeled and at what level of detail
 - Identify sub-components that may warrant attention
 - Develop methods for performing these activities
 - Complete Benchmarks



INVESTIGATION OF DIGITAL SYSTEM RELIABILITY ASSESSMENT METHODS

- Without a methodology, NRC can not independently assess risk-informed digital system applications
- The NRC does not have a standard methodology for analyzing digital system reliability
- This research project will
 - Analyze digital system reliability assessment methods
 - Develop a digital system reliability assessment methodology
 - Conduct case studies to assess usability of the methodology
 - Update NRC PRA tools
 - Support the development of acceptance criteria



SUMMARY

- This research will provide data, analysis methods, and acceptance criteria to support the use of risk-informed regulatory methods for the review of digital systems
- Broad-based program that will look at a number of potentially viable methods for developing acceptable digital system risk models to assess the capabilities and limitations of the state-of-the-art and develop appropriate regulatory requirements
- RES is looking forward to working closely with the ACRS as these programs are implemented

Overview and Status of “Digital Systems PRA” Project



Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 15, 2005

Hossein Hamzehee

Probabilistic Risk Assessment Branch
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
(301-415-6228, hgh@nrc.gov)

Todd Hilsmeier

Probabilistic Risk Assessment Branch
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research
(301-415-6788, tah1@nrc.gov)

Tsong-Lun Chu

Brookhaven National Laboratory
(631-344-2389, chu@bnl.gov)

Overview and Status of “Digital Systems PRA” Project

Purpose:

- **The purpose of this presentation is to:**
 - **Describe the “Digital Systems PRA” project plan.**
 - **Provide status of project.**
 - **Discuss tasks that are completed or in progress.**

Overview and Status of “Digital Systems PRA” Project

Presentation Outline:

- **Background**
- **Objectives of Digital Systems PRA**
- **Integrated Project Plan and Technical Tasks**
- **Discussion and Status of Tasks in Project Plan**
- **Schedule**

Background

- **Nuclear power plants are replacing obsolete analog I&C systems with digital ones. Advanced reactors will use integrated digital I&C systems.**
 - The following plants express interest in upgrading their analog RPS system to a digital platform: Oconee, Callaway, Wolf Creek, and Comanche Peak.

- **NRR will be reviewing submittals on analog to digital system upgrades at nuclear power plants, which will require RES support. The PRA modeling of digital systems is important to support a risk-informed approach to evaluation and selection of digital systems (NRC's PRA Policy Statement, Regulatory Guide 1.174).**

- **Status of EPRI TR 1002835 Review:**
 - EPRI TR 1002835: "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades".
 - NRR/RES currently performing an "acceptance review" to determine if NRC will review EPRI TR 1002835 in its current form.
 - After the acceptance review, NRR will develop a review schedule.

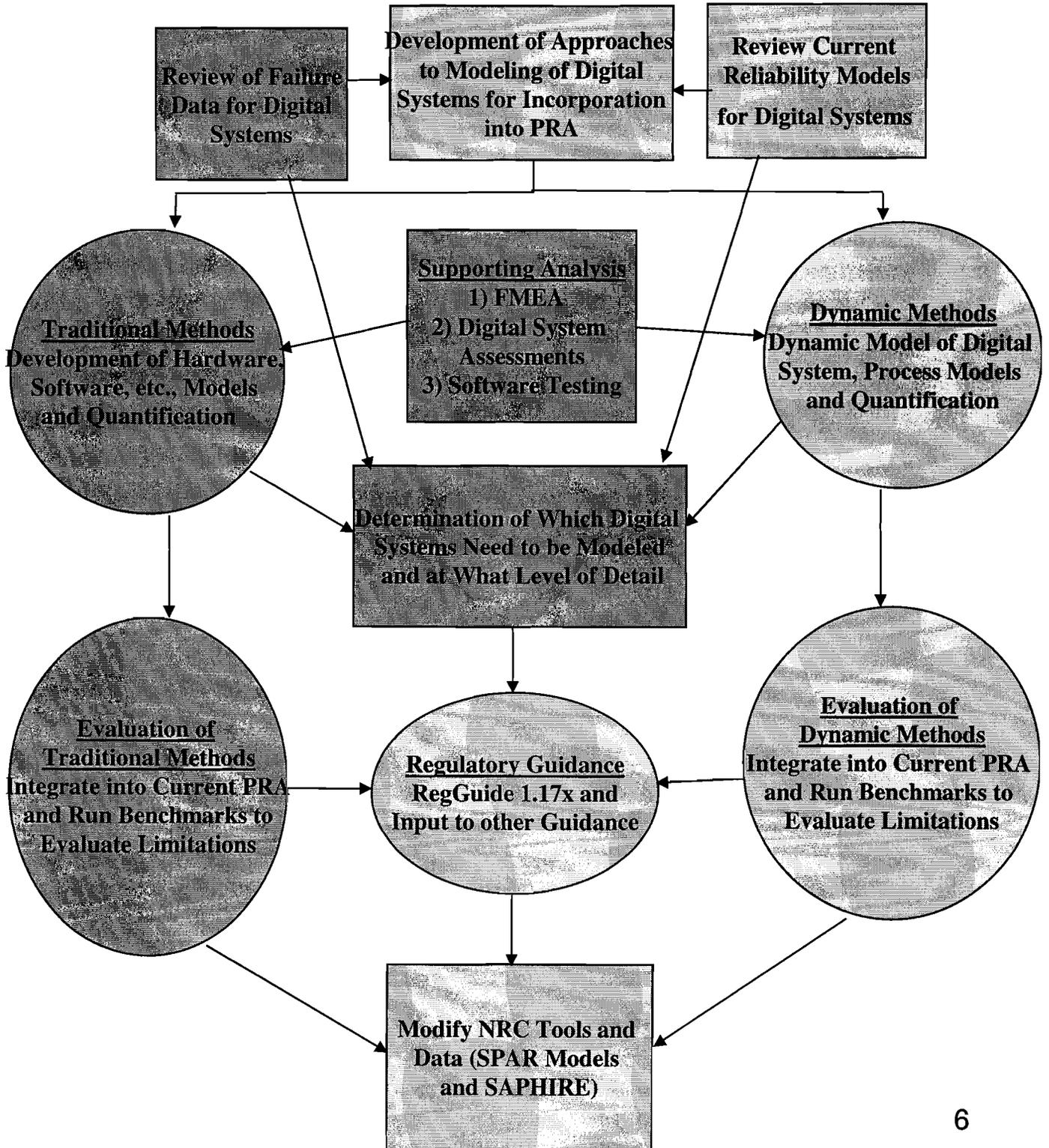
*If reviewed,
A&S would review
the SER*

Objectives of Digital Systems PRA

- **The objective of the project is to develop a probabilistic method for modeling failures of digital I&C systems that can be integrated with a PRA using traditional PRA methods (fault trees, event trees).**

- **Digital systems are not currently being treated adequately and uniformly in PRAs.**
 - **Lack of an acceptable approach for modeling digital systems in PRA (e.g. black box approach).**
 - **Current methods and data on modeling digital systems are not adequate.**

NRC Digital System Risk Program



Intermediate reports for public comment

Keiper: Public mtg to be held at some point in process

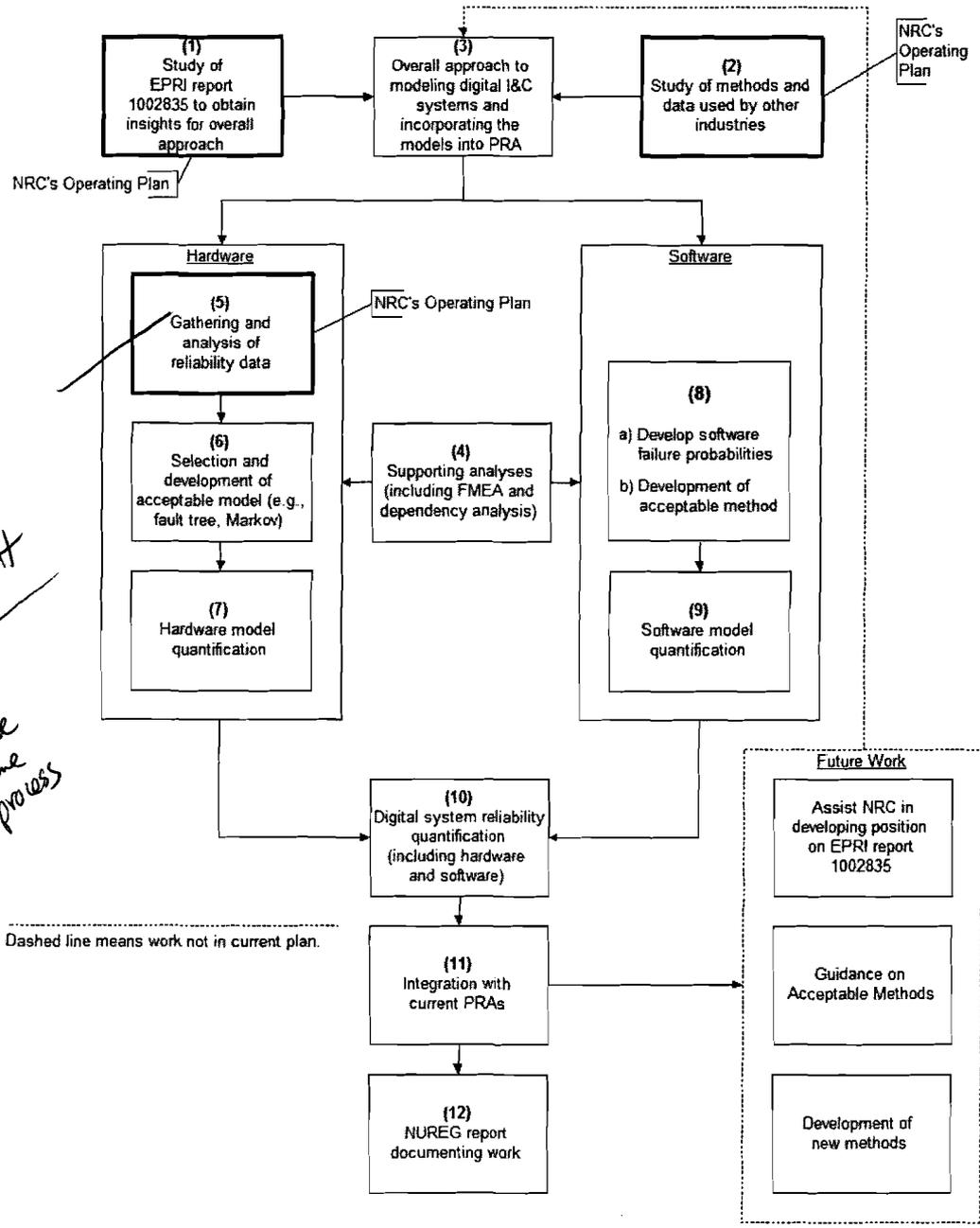


Figure 1
Technical Tasks/Activities Associated with Digital Systems PRA Project

Task 1 Insights from EPRI TR-1002835

Objective:

Review EPRI TR-1002835 (“Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital I&C Upgrades”) to obtain insights on reliability modeling of digital systems.

Observations:

- EPRI TR advocates the risk-informing of digital I&C systems. ✓
- EPRI TR proposed to use simplified and standard risk-informed methods as alternatives to current deterministic method. ✓
- The “Simplified Risk-Informed” method should be clarified and demonstrated with examples (may not provide conservative risk values). *RES opinion of earlier version current does provide examples*
- EPRI TR does not provide information on how to develop models needed in the “Standard Risk-Informed” method.
- EPRI TR does provide some characteristics to consider in model development.

Schedule:

Incorporating Research review comments into draft report.
Final report on Task 1 will be completed by June 30, 2005.

Task 2

Study Methods and Data Used by Other Industries

Objective:

Review industry experience for methods and databases used to model digital systems (including ways quantitative reliability analyses are used).

Observations:

- Approach:
 - Establish contacts (e.g., NASA, Army, Navy, Air force, DOE, DOD, DNFSB, FAA, Automotive, OMNICON, RAC, INL).
 - Search and collect guidance and reports.
 - Review reports.

for Navy *for Army* *no access*
- Most industries manage digital system risk through software development process, management, and testing.

Qualitative approach
Very little Quantitative
- NASA appears to be moving to a quantitative risk evaluation approach using PRAs.
 - NASA Fault Tree Handbook and NASA PRA Procedures Guide were developed by experts with extensive nuclear plant PRA experience.
 - NASA Fault Tree Handbook contains standard fault tree methods with introduction of fault coverage of digital components.
 - NASA PRA Procedures Guide contains standard PRA methods tailored for NASA applications, and has a section on software risk assessment, which presented a frame work for considering software failures and proposed an approach for quantifying software failures.

Schedule:

Final Report to be completed by August 30, 2005.

Task 4

Supporting Analyses of Digital Features

Objective:

Obtain information about the behavior of a digital system.

- Develop a FMEA and a dependency analysis of the system (foundation of reliability modeling).
- Develop guidance on how communication and voting should be modeled.
- Analyses will support development of the digital system's reliability model.
- Applied to digital RPS system proposed for Oconee.

Estimated Period of Performance:

This task is expected to start in July 2005 and will be completed by September 2006.

Task 5

Collection of Failure Data and Development of Database for Probabilistic Modeling of Digital Hardware

Objective:

Develop failure database for digital hardware, based on currently available data, for quantifying digital system reliability models.

Analysis:

- **Database Development Approach:**

- Review failure rate databases - Military Handbook 217F, Telcordia, PRISM.
- Search industries for additional digital failure data (e.g., LERs, EPIX, NASA, SPAR, FAA).
- Development of population variability distributions using proprietary PRISM failure records.

- we can review

Task 5 - Hardware Analysis (continued)

- **Military Handbook 217F, Telcordia, PRISM Failure Rate Prediction Methods:**
 - Use of empirical formula (not laws of physics) in predicting failure rates has been found to be inaccurate.
 - Applicability of empirical formula is limited to cases where applicable and adequate failure data is available. Extrapolation could lead to significant errors.
 - Lack of uncertainty consideration.

Task 5 - Hardware Analysis (continued)

● Review of Industry Experience:

- Existing PRA failure databases (SPAR database, NASA PRA guide, IEEE Std 500) do not include digital component failure rates.
- Advanced reactor PRAs (e.g. AP600 PRA -Westinghouse 1996) may contain limited digital failure rate data that are proprietary.
Will evaluate further in second phase of data analysis.
- Industry operating experience (e.g., nuclear plant - LER/EPIX, FAA, Army, DOE) contain digital failures, but do not contain information on: subcomponents that failed, how many of the same components/systems are in operation, and how long they have been in operation, which are needed to derive failure rate estimates.
Will evaluate further in second phase of data analysis.
- NASA failure database is proprietary. Database for public use will be available in 2006.
Will evaluate further in second phase of data analysis.
- COMPSIS [OECD 1999] is an international effort to collect I&C operating experience, and is still at its early stage of data collection.
Will evaluate further in second phase of data analysis.

~~IEEE Std 500~~

Task 5 - Hardware Analysis (continued)

- **Population variability distributions using PRISM failure records:**

- PRISM is a software developed by the Reliability Analysis Center (RAC) for making reliability predictions of series systems, e.g. circuit boards.
- PRISM contains failure records of components (e.g., microprocessors and RAMs) from different sources (i.e., warranty repair data) in the form of “n failures in m hours”.
- Large variations in failure data exist among different sources due to different specific designs, operating conditions, manufacturers, etc.
- Development of Population Variability Distributions:
 - a) Hierarchical Bayes Analysis of PRISM Data.
 - b) More than 20 different digital components were analyzed.
 - c) Wide population variability distributions were obtained due to large variations in failure record.
- This will be further evaluated in the second phase of data analysis.

*meetings
twice a year
want to hear about
actual data what
we learned at
future meetings
preliminary docs
available*

Task 5 - Hardware Analysis (continued)

- **Conclusion:**

- PRISM data is main source for hardware failure rate development.
- Generated error factors could be large.
- Second phase of data development will review: possible additional failure modes, and additional databases (Manufactures, Advance Reactor PRA, INL, NASA, COMPSIS, LER/EPIX with cooperation from plants).

Schedule:

Final Report to be completed by August 30, 2005.

Task 6

Selection and Development of Acceptable Hardware Reliability Model

really flowchart

Objective:

Develop reliability model for digital system hardware (i.e., digital RPS system proposed for Oconee).

- Develop reliability block diagrams and transition diagrams that capture the behavior of digital system.
- Review industry guidance on Markov modeling.
- Either a fault tree or a Markov model will then be developed for failure on demand of the system.
- Develop guidance on modeling the behavior of digital features.
- Identify the data needed to support the quantification of the models.
- Comparison of digital and analog designs of I&C systems (i.e., digital RPS system proposed for Oconee).

Estimated Period of Performance:

This task is expected to start in October 2005 and will be completed by December 2007.

Task 7

Hardware Reliability Model Quantification for Selected Platform

Objective:

Quantify hardware reliability model using best available data for selected platform (i.e., digital RPS system proposed for Ocone).

- Discuss important contributors to system failure probability.
- Discuss assumptions that may have significant impacts on the results.

Estimated Period of Performance:

This task is expected to start in October 2006 and will be completed by December 2007.

Task 8

Development of Methods for Modeling Software Failures

Objective:

Develop an acceptable method for including software failures in a digital system probabilistic failure model.

- Review software-induced failure events in different industries to identify the failure modes, failure causes, occurrence frequencies, and the insights on modeling software failures in a PRA.
- Review additional literature to develop basis for modeling software failures in PRA.
 - Address issue of whether software failure rates are meaningful.
 - Consideration of uncertainties.
 - Evaluate different reliability methods (e.g., fault trees, Markov, reliability growth models, etc...).
- Develop quantitative software failure model.
 - Evaluate existing software reliability models.
 - Establish linkage between software and hardware models.
 - Determine software failure parameters that have to be quantified.
 - Different types of software have different effects on digital systems and may have to be modeled differently.
 - Apply them to specific example designs (i.e., digital RPS system proposed for Oconee).

Estimated Period of Performance:

This task is expected to start in July 2005 and will be completed by September 2008.

Task 9

Software Reliability Quantification for Selected Platform

Objective:

Quantify the software failure probabilities identified in Task 8 for selected platform (i.e., digital RPS system proposed for Ocone).

- The results of the task could be used in an integrated model of the digital systems (Task 10).

Estimated Period of Performance:

This task is expected to start in October 2007 and will be completed by September 2008.

Task 10

Digital System Reliability Quantification

Objective:

Perform quantification of the probability of failure on demand of the digital RPS system proposed for Oconee.

- Perform sensitivity calculations to evaluate Important assumptions.
- The combined model (hardware and software) will provide a system model to be integrated with the PRA, Task 11.

Estimated Period of Performance:

This task is expected to start in October 2007 and will be completed by December 2008.

Task 11

Integration of Reliability Models With PRA

Objective:

Integrate the digital system reliability model into the PRA.

- If a Markov model is developed for the Oconee RPS, its integration with a PRA requires that an integration method be developed.
- Develop guidance on when diverse systems can be considered independent (digital systems can be used at 4 different echelons of defense: control, protection, mitigation, and indications. Dependencies may exist between systems at different echelons, e.g., RPS and ATWS mitigation system).

Estimated Period of Performance:

This task is expected to start in October 2007 and will be completed by March 2009.

*only using Oconee because
info available; not in
support of licensing action*

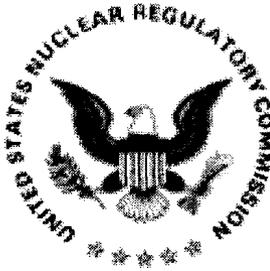
Task 12 Develop NUREG Report

Objective:

Prepare a NUREG report that documents all the tasks completed in this project.

Estimated Period of Performance:

This task is expected to start in October 2007 and will be completed by March 2009.



CURRENT STATE OF RELIABILITY MODELING METHODOLOGIES FOR DIGITAL SYSTEMS AND ACCEPTANCE CRITERIA FOR NUCLEAR POWER PLANT ASSESSMENTS

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Subcommittee

June 1~~4~~⁵, 2005

Steven A. Arndt

Engineering Research Application Branch
Division of Engineering Technology
Office of Nuclear Regulatory Research
(301-415-6502, saa@nrc.gov)

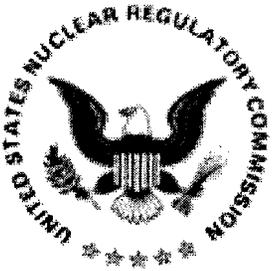
Tunc Aldemir

Nuclear Engineering Program
The Ohio State University
(614-292-4627, aldemir.1@osu.edu)



Background

- U.S. NRC policy encourages the use of PRA and associated analyses to the extent supported by the state-of-the-art
- ACRS issued a Letter Report in 1997 that recommended that the NRC staff develop methods for estimating failure probabilities in software-based digital systems, including commercial off-the-shelf (COTS) software and hardware
- The preferred method of evaluating a digital system is from a system stand point that requires modeling system interaction as well as hardware and software modeling
- For near term PRA applications, a digital I&C system reliability model needs to be compatible with the structure of current nuclear power plant PRAs, which use the static event-tree/fault-tree (ET/FT) approach

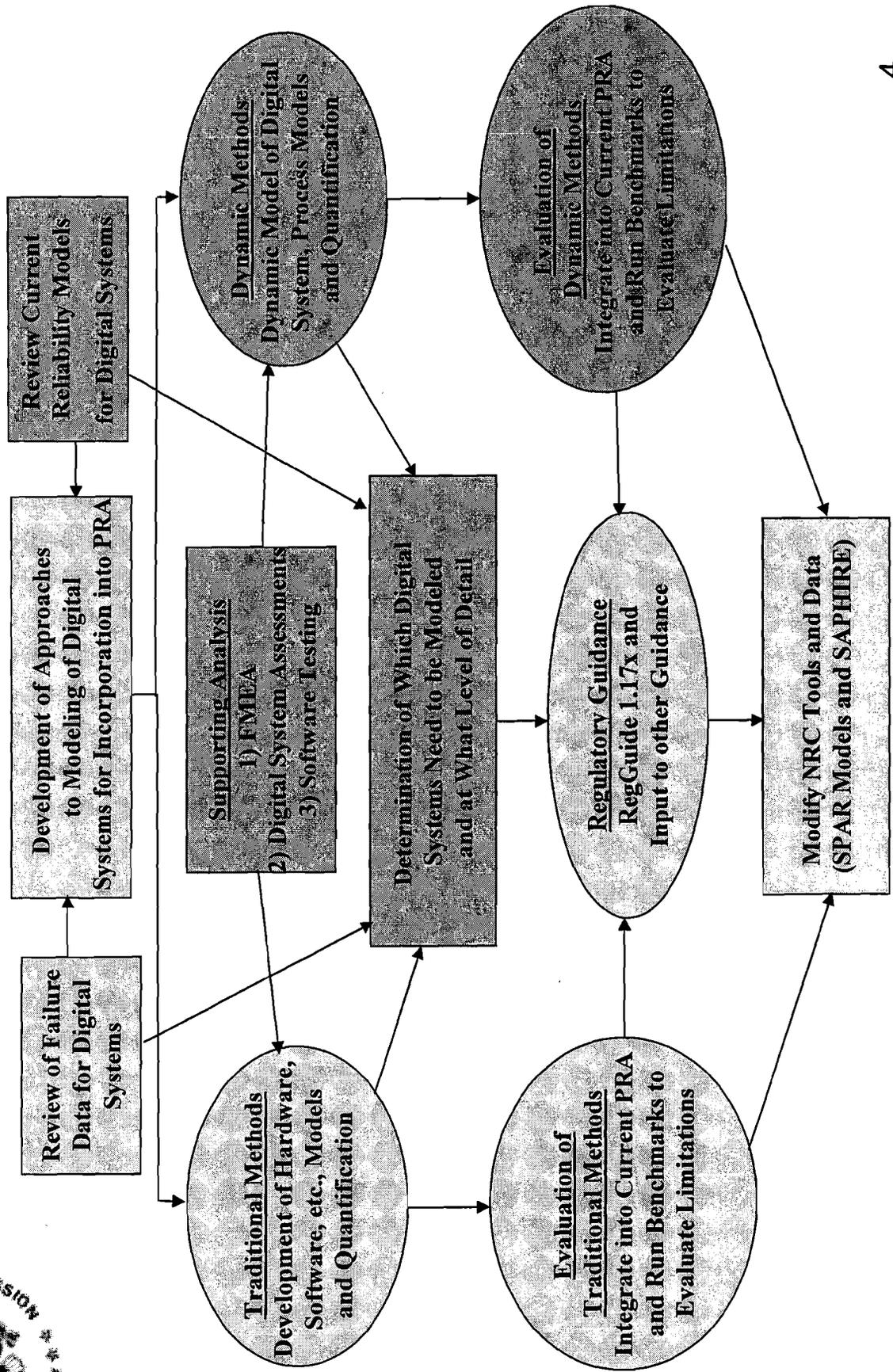


Background (Cont.)

- From a reliability modeling perspective, these conclusions imply that there may be a need to account for the dynamic interactions
 - between digital I&C systems and controlled/monitored plant physical processes (e.g., heatup, pressurization), and
 - within digital I&C systems (e.g., communication between different components, multi-tasking, multiplexing)
- Digital I&C system reliability models accounting for such effects need to be incorporated into the existing PRA to assess whether the Δ CDF due to proposed change in the I&C system vs. existing CDF will be acceptable according to RG 1.174 acceptance criteria



NRC Digital System Risk Program





Objectives

Develop both policies and methods for inclusion of reliability models for digital systems into current generation nuclear power plant PRAs, including

- a pilot study of the proposed methods,
- detailed reviews of the potential pitfalls of the methods developed, and
- detailed reviews of other methods when used to develop Δ CDF and LERF numbers needed to support risk informed regulation of nuclear power plant instrumentation and control criteria



Overall Approach

- Investigate the applicability of the current static event tree/fault tree (ET/FT) approach to digital I&C systems
- Review the advantages and limitations of available dynamic methodologies as they pertain to digital I&C systems relevant to reactor protection and control
- Review other industries for practices in the reliability modeling of digital I&C systems
- Review the existing regulatory framework with regard to requirements that a digital I&C control system must meet
- Identify the overall minimum requirements a digital system model must meet for successful incorporation into an existing PRA
- Identify available methodologies that meet these requirements



Differences Between Analog and Digital I&C Systems

- The firmware and software components of digital I&C systems do not demonstrate any wear characteristics and do not respond to accelerated life testing, stress testing, etc.
- The firmware/software reliability cannot be accurately modeled using a bathtub curve approach
- There may be complex interactions between the constituents of the digital I&C system and between the digital I&C system and process physics which may lead to potentially significant dependencies between failures events:
 - Digital I&C systems rely on sequential circuits that have memory. Consequently, digital I&C system outputs may be a function of system history, as well as the rate of progress of the tasks.
 - Tasks may compete for a digital controller's resources which may lead to problems such as deadlock and starvation.
 - The choice of internal/external communication mechanisms for the digital I&C system (such as buses and networks) and the communication protocol affect the rate of data transfer.
 - Ability to coordinate multiple digital controllers directly and explicitly may necessitate a finer degree of communication and coordination between the controllers.
 - A digital controller can remain active and not only react to data, but can anticipate the state of the controlled/monitored system



Differences Between Analog and Digital I&C Systems (Cont.)

- The failure modes of digital I&C system are not well defined:
 - Errors in design and software implementation can cause the digital system to fail due to some specific input being received.
 - The system may fail not only on that specific input but also on other inputs that are semantically similar or even equivalent/correlated
- Software may be able to mask intermittent failures in hardware
 - A protocol for Ethernet is able to coordinate collision of packets transmitted when more than one node on the network attempts to transmit
- Digital I&C systems share data transmissions, functions, and process equipment to a greater degree than analog systems and hence may be more vulnerable to common cause failure



Differences Between Analog and Digital I&C Systems (Cont.)

- It is possible for digital I&C systems to introduce new initiating events:
 - Protocols may introduce dependencies between different systems such that system failures may introduce 'garbage' data as input to the other devices
 - Multi tasking may introduce new failure dependencies between systems.
- Software is not a physical entity and testing alone is not sufficient to verify that software is complete and correct
- Software defects may remain hidden for long periods after a product has been in general use and failures may occur without any advance warning when a particular execution path is exercised



Practices in Other Industries

- Most, if not all, approaches taken by the medical device, defense system, telecommunication industries and the aircraft industry (under the FAA) include software development process, management, and testing as their primary activities to manage digital system risk
- Only the spacecraft industry, under NASA guidance, appears to be moving to a true risk evaluation system using PRAs.
- The NASA guidelines identify
 - black box software reliability models exemplified by the Schneidewind model
 - semi-dynamic methodologies exemplified by the dynamic fault-tree and dynamic flowgraph methodologies.
- There has been NASA supported work using dynamic methodologies (e.g. space shuttle engine assessment).



Need for Dynamic Methodologies

- Dynamic interactions between the plant physical processes and triggered or stochastic logical events of reactor protection and control systems may lead to coupling between failure events
- Cases reported in the literature imply that the conventional ET/FT approach may yield conservative (but maybe overly conservative) results
- Omission of some failure scenarios is possible if dynamic interactions between the plant physical processes and triggered or stochastic logical events are not accounted for*
- Dynamic methodologies will only be needed for systems for which significant interactions are possible

*P. C. CACCIABUE, A. AMENDOLA, G. COJAZZI, "Dynamic Logical Analytical Methodology Versus Fault Tree: The Case Of Auxiliary Feedwater System of a Nuclear Power Plant", *Nucl. Technol.*, **74**, 195-208 (1986)



Review of Dynamic Methodologies

- Two types of dynamic interactions need to be accounted for in the reliability modeling of digital reactor protection and control systems:
 - Interaction between the reactor protection and control system and controlled/monitored plant physical processes such as heatup and pressurization of the reactor and level control (Type I interactions)
 - Interaction between the constituents of the reactor protection and control system itself, such as communication between different components, multi-tasking, multiplexing (Type II interactions)
- From a reliability modeling viewpoint, Type I and Type II interactions are separable only for single-input, single-output I&C systems
- Generally it is difficult to integrate a dynamic model into existing plant PRAs, almost all of which are based on the ET/FT approach



Dynamic Methodologies for Type I Interactions

- Continuous time
 - CET (Continuous Event Tree)
 - CCCMT (Continuous Cell-to-Cell Mapping Technique) *TOSU*

- Discrete time
 - MC (Monte Carlo)
 - DYLAM
 - DETAM *SK* } Dynamic Event
 - ADS *UMD* } Tree Generation
 - ISA
 - CCMT (Cell-to-Cell Mapping Technique) *TOSU*
 - DDET/MC

- Visual
(mostly semi-dynamic)
 - PETRI NETS
 - DYNAMIC FLOWGRAPHS
 - GO-FLOW
 - DFT (Dynamic Fault Tree)
 - ESD (Event Sequence Diagrams)



Evaluation of Dynamic/Semi-Dynamic Methodologies

Issue/ Method	Accuracy in the Representation of System Dynamics	Ease of Probabilistic Model Construction	Desirability of Computational Features for Quantification	Compatibility with Existing PRAs
CET	10	5	1	1
CCCM	7	1	3	3
DYLAM	10	7	5	9
DETAM	10	7	5	9
DDET	10	7	5	9
ADS	10	7	5	9
MC	10	6	1	1
DDET/MC	10	6	6	9
ISA	10	7	7	9
CCMT	7	7	3	3
PN	3	5	7	8
DFM	3	5	7	7
ESD	10	4	5	8
GO-FLOW	3	7	8	7

1: Worst – 10: Best



Dynamic Methodologies for Type II Interactions

- Markov models (Johnson)
- Bayesian methodologies (Golay)
- Dynamic flowgraph methodology
- Petri nets
- Test based approaches
- Software metric-based approach
- Black-box models (Schneidewind)



Evaluation of Available Methodologies and Desirable Model Features

Requirements

1. The model must be able to predict future failures well.
2. The model must account for the relevant features of the system under consideration.
3. The model must make valid and plausible assumptions.
4. The model must be able to represent dependencies between failure events accurately and quantitatively
5. The model must be designed so it is not hard for an analyst to learn the concepts and is not hard to implement.
6. The data used in the quantification process must be credible to a significant portion of the technical community.



Evaluation of Available Methodologies and Desirable Model Features

Requirements

7. The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones.
8. The model must be able to differentiate between faults that cause function failures and intermittent failures.
9. The model must have the ability to provide relevant information to users, including cut sets, probabilities of failure and uncertainties associated with the results.
10. The methodology must be able to model the digital I&C system portions of accident scenarios to such a level of detail and completeness that non-digital I&C system portions of the scenario can be properly analyzed and practical decisions can be formulated and analyzed
11. The model should not require highly time-dependent or continuous plant state information.



Evaluation of Available Methodologies and Desirable Model Features

Requirement/ Methodology	1	2	3	4	5	6	7	8	9	10	11
Continuous Event Trees [59]	X	X	X	X	O	?	?	X	?	?	O
Dynamic Event Trees [61,62, 63,64,65, 67]	X	X	X	?	X	?	?	?	X	X	O
Markov Models [30, 60, 68]	X	X	X	X	O	?	X	X	?	?	O
Monte Carlo Simulation [66]	X	X	X	X	?	?	?	?	?	?	O
Petri Nets [45, 46, 47, 69, 70]	X	X	X	X	O	?	?	?	?	?	O
DFM [14, 57]	X	X	X	?	X	?	?	?	X	X	X
Dynamic Fault Trees [71, 72]	X	?	?	?	X	?	X	?	X	?	X
ESD [73]	X	X	X	X	O	?	?	?	X	X	O
GO-FLOW [74,3]	X	?	X	?	O	?	?	?	X	X	X
Bayesian Methodologies [43, 44]	X	?	?	?	O	O	?	?	?	?	X
Test Based Approaches [51]	?	?	X	O	X	?	X	X	?	O	X
Software Metric Based Approaches[52]	O	?	O	O	?	?	X	X	O	O	X
Schneidewind Model [34,53]	X	?	?	?	?	?	?	?	O	O	X

X: Fulfills requirement

O: Does not fulfill requirement

? Needs further study to determine whether or not the methodology fulfills the requirement



Available Methodologies According to Desirable Model Features

- Dynamic flowgraph methodology
- Markov approach or dynamic event tree construction
- Event sequence diagrams
- Petri nets or GO-FLOW
- Monte Carlo simulation



Minimum Acceptance Criteria for Methodologies from a Regulatory Viewpoint

- **The model must be able to quantitatively represent dependencies between failure events accurately, including common cause failures, those arising due to interaction of the digital I&C systems with the controlled process (Type II interactions) and within the digital I&C systems (Type I interactions)**
- **The model should not require highly time-dependent or continuous plant state information**
- **The model must be able to predict future failures well and cannot be purely based on previous experience**
- **The model must make valid and plausible assumptions and the consequences of violating these assumptions need to be identified**

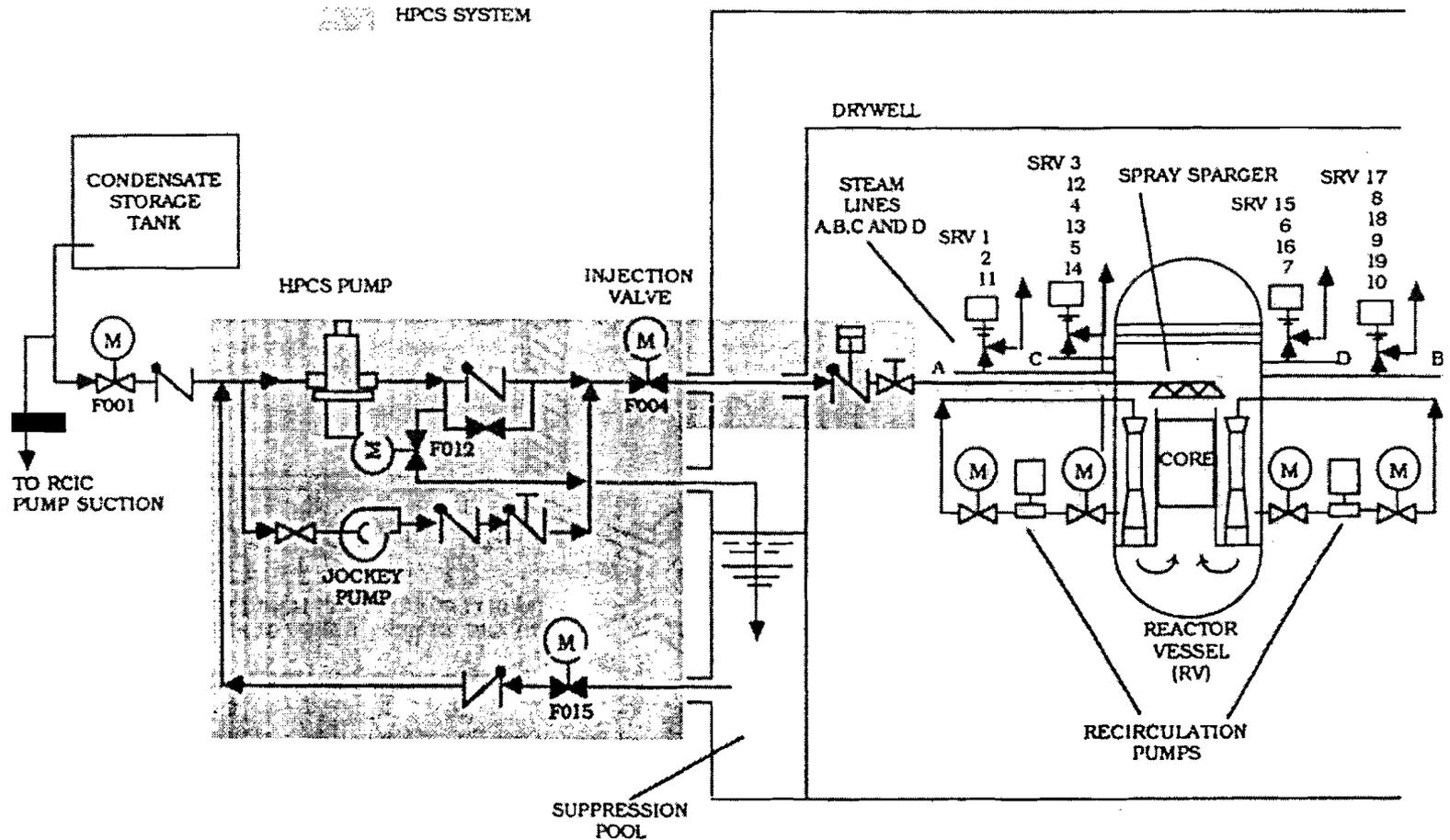


Minimum Acceptance Criteria for Methodologies from a Regulatory Viewpoint (Cont.)

- **The data used in the quantification process must be credible to a significant portion of the technical community**
- **The model must be able to differentiate between a state that fails one safety check and those that fail multiple ones**
- **The model must be able to differentiate between faults that cause function failures and intermittent failures**
- **The model must have the ability to provide uncertainties associated with the results**

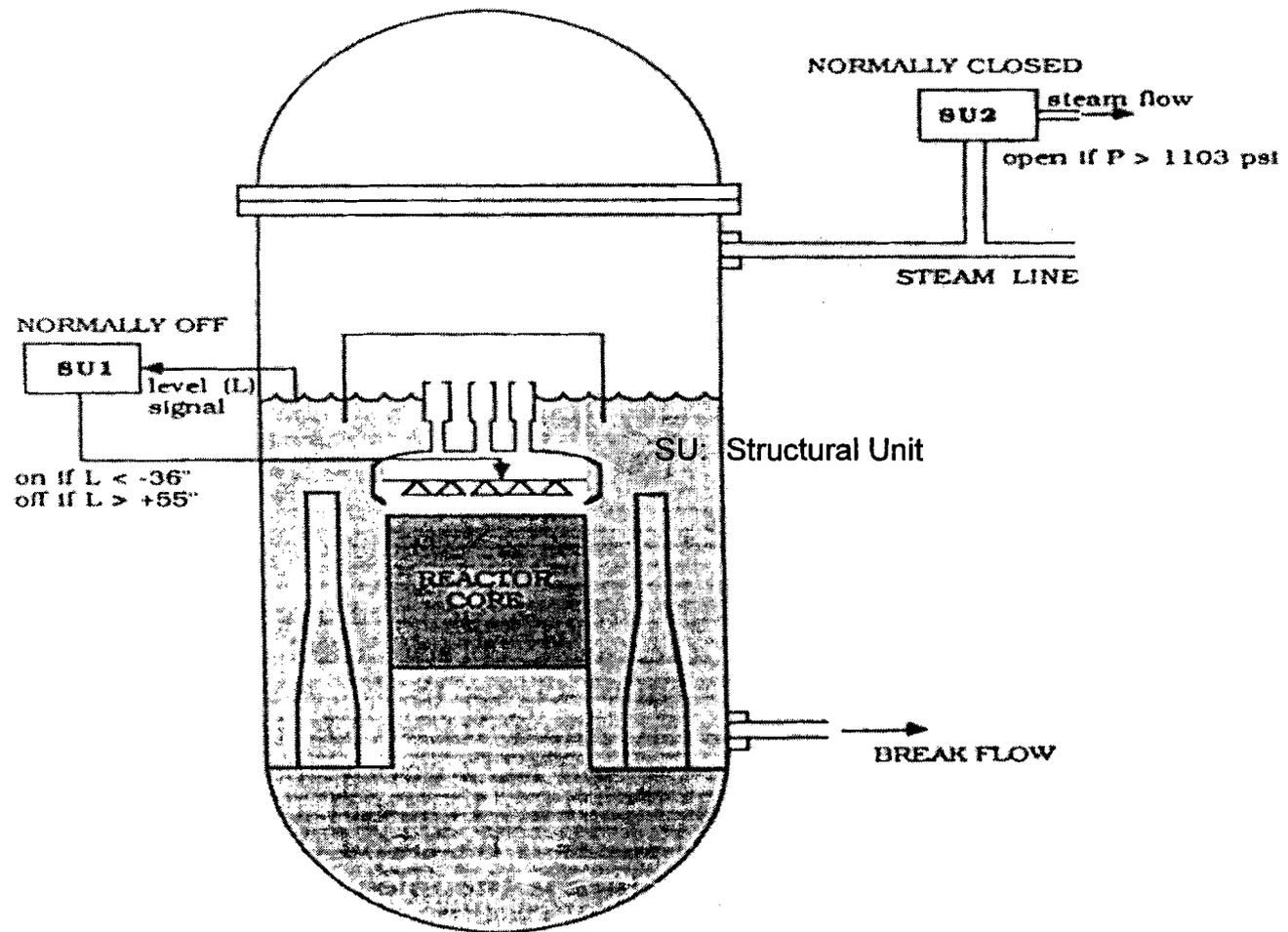


Example for Type I Effects: Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System





Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System: Modularized System





Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System: Example Initiating Event and Assumptions

- 1% double-ended guillotine break
- Pressure reaches 1039.4 psi within 2 minutes following the LOCA
- Level reaches 36.0 in within 2 minutes following the LOCA
- Major contributor to SU 1 failure is injection valve



Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System: Competition Between Top Events*

- Low level (<-148 in) occurs if only SU1 fails-off or only SU2 fails-open
- High level (>+60 in) occurs if SU2 fails-closed after SU1 fails-off
- High pressure (>1110 psi) occurs if the level at the time SU2 fail-closed is such that it takes longer for the level to reach -148 in than the time it takes pressure to reach 1110 psi
- Low level occurs if the level at the time SU2 fail-closed is such that it reaches -148 in before pressure reach 1110 psi
- High level occurs if the level at the time SU2 fails-closed is such that the level reaches +60 in before pressure reaches 1110 psi

*M. Hassan, T. Aldemir, "A Data Base Oriented Dynamic Methodology for the Failure Analysis of Closed Loop Control Systems in Process Plants", *Reliab.Engng & System Safety*, **27**, 275-322 (February 1990)



Feed-Bleed Cooling of a BWR/6 Following a Break Incapacitating RCIC System: Some Significant Findings*

- The competition between the Top Events does not just depend on the order of SU failure but exact timing of the failure and/or exact magnitudes of the pressure and level at the time of the failure
- ET/FT overestimates low pressure probability by a factor of 3**
- ET/FT overestimates low level probability by a factor of 2**
- ET/FT results for high level and high pressure are close to dynamic methodology results*

**ET/FT results assume the demand on SU1 is 3/h and demand on SU2 is and 30/h

*M. Hassan, T. Aldemir, "A Data Base Oriented Dynamic Methodology for the Failure Analysis of Closed Loop Control Systems in Process Plants", *Reliab.Engng & System Safety*, **27**, 275-322 (February 1990)



Conclusions

- **No single available methodology satisfies all the requirements**
- **It is not clear that the data used in the quantification process would be credible to a significant portion of the technical community for any methodology**
- **While DFM ranks as the most promising methodology, it is not clear that it can quantitatively represent dependencies between failure events accurately for all digital I&C systems**
- **An alternative methodology is the Markov approach**



Conclusions (Cont.)

- Scant computational evidence in the literature on dynamic systems seems to indicate that the ET/FT approach yields satisfactory results when a system:
 - has a single failure mode, or,
 - does not have logic loops*, and/or,
 - substantial time delay (with respect to system time constants) between the initiation of the fault and system failure
- Extrapolated to digital I&C systems, existing computational evidence on dynamic systems would indicate that the ET/FT approach may yield satisfactory results when a digital I&C system does not:
 - interact with a process that has multiple Top Events, logic loops* and or substantial time delays between the initiation of the fault and Top Event occurrence,
 - rely on sequential circuits which have memory,
 - have tasks that compete for the I&C system resources, and,
 - anticipate the future states of controlled/monitored processes.

*It may be possible to model logic loops using digraphs for fault-tree construction



Next Steps

- **Two benchmark problems will be defined that respectively capture important features of the existing analog I&C systems and their digital counterparts expected to be encountered in applications**
- **The benchmark problems will be used to compare DFM and the Markov approach with a common set of failure data**
- **If the result of the benchmark study indicates that DFM performs satisfactorily on the benchmark problems, then the impact of analog to digital I&C conversion will be investigated on a full PRA using SAPHIRE**
- **A study will be initiated as to how Markov model outputs can be utilized in a mechanical fashion to provide compatible input to SAPHIRE**
- **Alternatively, the feasibility of developing a dynamic methodology on the SAPHIRE platform may be investigated**