



UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
ADVISORY COMMITTEE ON NUCLEAR WASTE
WASHINGTON, D.C. 20555

OFFICE OF
ACRS/ACNW

July 12, 1994

MEMORANDUM FOR: ACRS Members

FROM: Chad B. Little, ACRS/ACNW Intern

SUBJECT: WORKSHOP ON LICENSING DIGITAL UPGRADES FOR
NUCLEAR POWER PLANTS, JUNE 13-15, 1994,
ANNAPOLIS, MARYLAND

A EPRI/NUMARC workshop recently brought together the regulatory, commercial and academic communities to discuss digital upgrade licensing issues. A brief summary of the conference is attached for your information. To obtain specific conference materials, please contact me at 492-8158.

A handwritten signature in cursive script that reads "Chad B. Little".

Chad B. Little
ACRS/ACNW Intern

Enclosures:

1) Licensing Digital Upgrades Memorandum

CC:

J. Larkins
S. Duraiswamy
S. Mays
D. Coe
ACRS/ACNW Fellows/Interns
ACRS/ACNW Members

Licensing Workshop

On June 13-15, 1994, a Licensing Digital Upgrades for Nuclear Power Plants Workshop was held for the following purposes:

- 1) "familiarize utility engineers with the
Guideline on Licensing Digital Upgrades
(EPRI TR-102348, December 1993) and
supporting documents
(IEEE 7-4.3.2-1993)
(EPRI TR-102323, EMI Handbook)
(EPRI TR-013291, V&V Handbook)
(NSAC-125, Guideline for 10 CFR 50.59
Safety Evaluations)
(NSAC-105, Guideline for Design and
Procedure Changes)."
- 2) "discuss NRC reaction/perspective"
- 3) "forum for interaction at application level on specific examples", and
- 4) "feedback on next steps from EPRI, NEI, NRC, and utility perspectives"

The workshop outlined how the Guideline may be used to assist in applying 10 CFR50.59 Unreviewed Safety Question USQ criteria by asking seven clarifying questions. These questions are intended to assist the industry in determining whether or not a USQ exists, and therefore whether NRC review and approval are necessary before implementation of the digital system. It is the responsibility of the licensee doing the retrofit to show that the change doesn't involve a USQ. This view was supported by the NRC. Retrofit acceptance remained dependent on the complexity of the change, effect on the safety function, and the ability to prove that a USQ is nonexistent.

The Guideline focuses on system level analysis with both top-down (i.e. overall system analysis) and bottom-up (i.e. digital component analysis) techniques filling in the gaps to assure that the safety function provided by the system is achieved. Addressing the need to evaluate the "black box" digital equipment, it was stressed that failure analysis must include evaluation of digital component failures which could:

- increase probability of a known failure mode
- increase consequences of a known failure
- cause new system-level failure mode
- reduce safety margin

The panel discussion combined the views of the NRC and EPRI into

three important elements that the workshop was working to exemplify:

- 1) Chapter 15 Accident Analysis gives context for digital retrofit analysis.
- 2) Doing large complex modifications to RPS (Reactor Protection Systems) or ESFAS (Engineered Safety Features Actuation System), aside from SCMF (Software Common Mode Failure) issues, is a grey area. The Guideline says show NRC defense-in-depth for complex retrofits.
- 3) Diversity - Attenders were referred to the February 17, 1994 ACRS letter concerning diversity. Although a possible benefit, the NRC stated that diversity for diversity sake adds complexity.

Questions related to the definition of sufficient diversity were presented but not resolved.

The NRC staff proposed methods for protecting against digital safety system failures and presented their perspective on the Guideline (see attachments 1 and 2). Some controversial points, listed below, were illustrated and will likely be addressed in the generic letter to be reviewed by the ACRS.

- 1) the definition of "system level" was not consistent between the NRC and EPRI, relative to the required failure modes analysis.
- 2) the determination of Unreviewed Safety Question based on a possible new type of accident or malfunction (i.e. common mode failure)
- 3) the dedication of commercial-grade hardware and software

The breakout sessions on the second day of the workshop involved five separate sessions. These were detailed presentations of actual digital retrofit experiences including planning, cost, implementation and operating experience. Synopses of each session are attached (see attachment 3). Presentation slides are available upon request.

Attachments:

- 1) NRC methods of protecting against failures
- 2) NRC perspective on Guideline document
- 3) Synopses of breakout sessions
- 4) Workshop agenda

Attachment #1

Methods for Protecting against failures caused by above concerns:

(Continued)

- **Provide diversity**
 - **Different manufacturer, function, hardware, software language, or design team**
 - **Diverse if: all are different, different function with same software language, or different manufacturer with same function**

Attachment #2

NRC Perspective on Guideline Document

- *EPR/Kumar* **Guideline provides useful guidance on both the design of analog-to-digital retrofits and their implementation (determination of unreviewed safety question) under 10 CFR 50.59**

- ★ ● **NSAC-125 not endorsed by NRC, therefore use of guidelines based on NSAC-125 is advisory only. Actual determination must be done in accordance with 10 CFR 50.59:**

- **For determination of unreviewed safety question (USQ) or new type of "system-level" failure mode, system-level is the digital system modification being installed.**

Tony Piatrangola
need to use
both ^① analog system
and ^② digital system

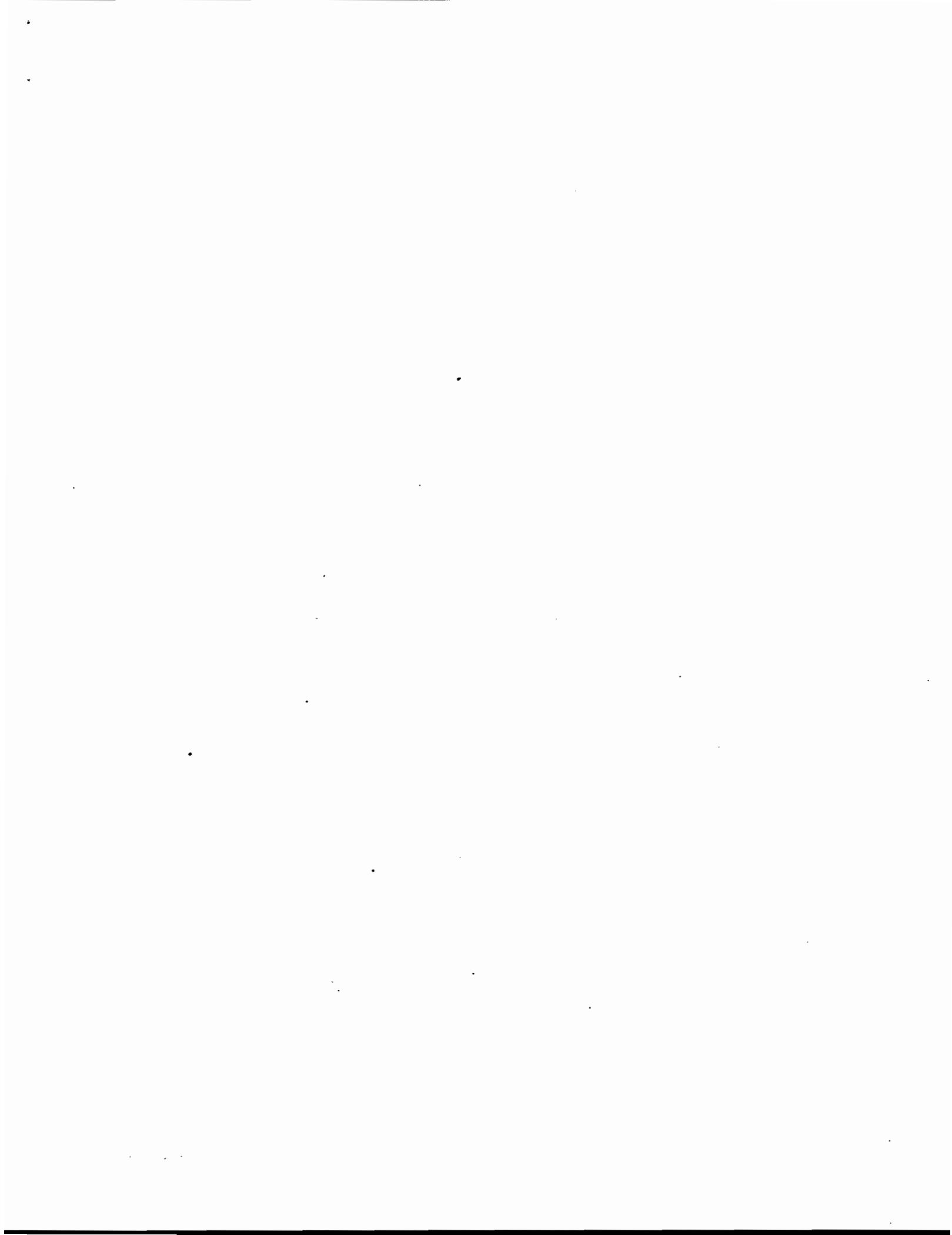
Controversial

NRC Perspective on Guideline Document

- ★ ● **When making 50.59 evaluation, if uncertainty exists in determination of USQ, the licensee should take conservative position that a USQ exists.**
- ★ ● **Basis for the engineering judgment and the logic used in the determination should be documented to the extent practicable.**
- ↘ ● **Generic Letter endorsing EPRI TR-102348 with above noted clarifications is in approval process.**
- **Staff will develop inspection guidance and training for regional inspectors on digital modification 10 CFR 50.59 evaluations and system designs.**

Attachment #3

SYNOPSIS OF
BREAKOUT SESSIONS



Lessons Learned Digital Controller Retrofit

EPRI Workshop on Licensing Digital Upgrades for Nuclear Power Plants

Synopsis of Breakout Session #1

June 14-15, 1994

Carl Yoder
Baltimore Gas Electric

Julie Sickle
Baltimore Gas Electric

Objectives of Session

- Demonstrate an actual application of digital upgrades
- Illustrate changes to that application using the recently published EPRI guidelines on Licensing Digital Upgrades

Approach of Session

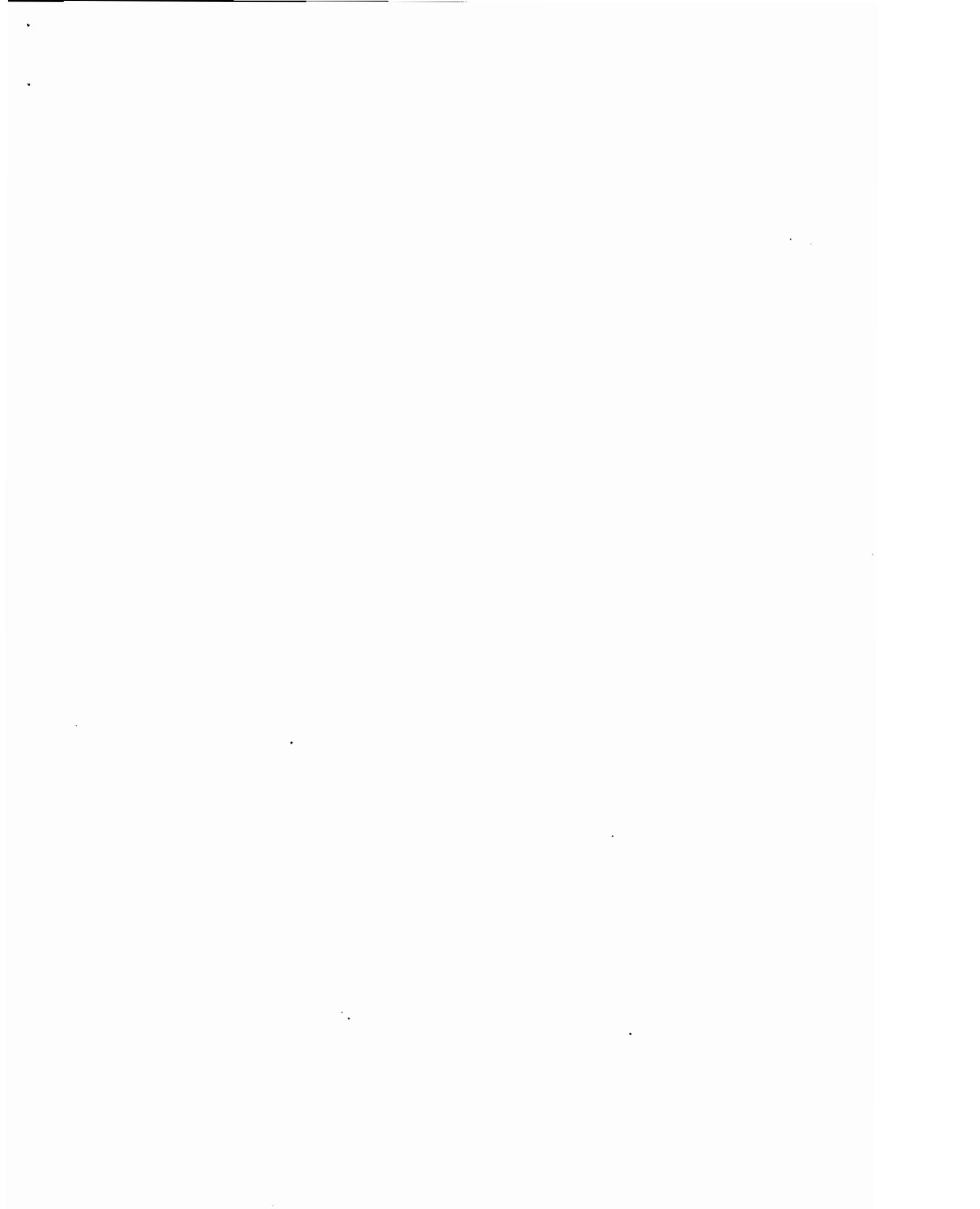
This first portion of this session will describe a digital upgrade at Calvert Cliffs Nuclear Power Plant. The upgrade described in this example was accomplished prior to the availability of EPRI 102348 and related standards and guidelines. Therefore, the second portion of this session will describe enhancements recommended to a project of this type using the existing guidelines.

Organization of Session

- *Description of the Digital Controller Retrofit Project.* All of Calvert Cliff's control room controllers had become obsolete. The latest technology was digital. This project evaluated all of the replacement options to arrive at a solution that met our human factors needs and design requirements.
- *Discussion of digital upgrade considerations based on EPRI 102348 guidelines.* Cover the process for determining new safety concerns regarding digital equipment used in previously analog applications. Discuss how these considerations would have effected the Digital Controller Retrofit Project.

Main Points to be Conveyed

- Good Engineering Judgment should be used in digital upgrades.
- The EPRI guidelines provide an approach to digital upgrades that focuses on new issues associated with digital upgrades.



Lessons Learned From the Salem Annunciator Upgrade

EPRI Workshop on Licensing Digital Upgrades for Nuclear Power Plants

Synopsis of Breakout Session #2

June 14-15, 1994

Charles Waite
Public Service Electric & Gas

Bob Fink
MPR Associates

Objectives of Session

- To illustrate from actual experience the issues that can arise with digital upgrades.
- To demonstrate how one utility has applied lessons learned from an early upgrade to develop improved processes for accomplishing digital upgrades.
- To demonstrate the potential cost benefit of following the approach outlined in EPRI TR-102348

Approach of Session

The upgrade described in this example was accomplished prior to the availability of EPRI 102348 and related standards and guides. The approach in this session will be first to describe the modification as it was originally done and the experience obtained with the system in operation. Then we will take a retrospective view of this experience, discussing the process that was used in the original upgrade, how the guidance in EPRI 102348 might have been applied, and how this might have affected the results. Finally, the cost benefit of applying this approach will be discussed.

Organization of Session

The session will consist of the following parts:

- *Description of the annunciator upgrade project.* The main control room overhead annunciator system was replaced with a new microprocessor-based system. We will describe the annunciator system briefly and explain how and why it was upgraded.

Breakout Session #2, cont'd

- *Discussion of the engineering environment at the time of the upgrade.* This was one of the early digital upgrades undertaken by the utility, and the engineering environment at that time for this type of modification was an important factor in determining how the upgrade was defined and implemented.
- *Description of the upgrade process – old and new.* We will describe the process that was used in the upgrade, the results obtained, and how the results might have been affected had the guidance in EPRI TR-102348 been applied in making the upgrade.
- *Discussion of cost benefit.* We will discuss the costs associated with following the latest guidance for digital upgrades, considering both the initial costs and the overall life cycle cost.
- *Open discussion and question-and-answer session.* Time will be allowed for participants to ask questions and for general discussion on the topics covered in this breakout session.

Main Points to be Conveyed

- The licensing guideline approach is applicable to more than just safety systems and licensing.
- The utility's process in defining the upgrade, interacting with and providing oversight of the vendor process is crucial. Digital systems should not be treated simply as "black boxes."
- The approach outlined in EPRI TR-102348 and the related standards and guides can be cost beneficial when viewed on the basis of life cycle costs.

PWR Feedwater Upgrade

EPRI Workshop on Licensing Digital Upgrades for Nuclear Power Plants

**Synopsis of Breakout Session #3
June 14-15, 1994**

**John W. Hefler
Pacific Gas & Electric Co.**

Objectives of Session

- To show how the licensing guideline (TR-102348) could be applied to a PWR digital feedwater upgrade
- To show how a failure analysis approach can improve reliability and identify potential problems
- To show how a safety evaluation on an upgrade of a non-safety system could result in an unreviewed safety question (USQ)
- To describe the features of and the benefits obtained by the digital upgrade
- To elicit feedback from participants on their related experience and problems with analog-to-digital upgrades

Approach of Session

This session will present a digital feedwater upgrade as it might be implemented using the licensing guideline approach. The example is based on the actual feedwater upgrade at PG&E's dual unit Diablo Canyon Power Plant. Although the plant upgrade was completed prior to the licensing guideline document, many of the elements in the guideline were part of the PG&E upgrade process. A simple failure analysis using fault trees will be presented to illustrate the key licensing issues and how they were resolved. A subjective assessment of the system and process will be described during which audience participation will be encouraged.

Breakout Session #3, cont'd

Organization of Session

The session will be divided into the following parts:

- An overview of the digital feedwater upgrade project at Diablo Canyon in terms of the licensing guideline and digital system capabilities
- A presentation and discussion of a failure analysis using fault trees to describe key issues in design and implementation
- A review and discussion of the 50.59 evaluation
- A review and discussion of PG&E's experience and lessons learned from the upgrade
- Open discussion (i.e., questions, comments, etc.)

Main Points to be Conveyed

- The licensing guideline is applicable to safety and non-safety systems
- The licensing guideline is generic, but can easily be applied within the design change system of a typical nuclear utility
- The failure analysis, using fault trees, identifies and resolves key issues pertaining to design and licensing
- Digital systems offer features not previously available on analog systems that improve availability and reliability
- The benefits, based on actual operating experience, are greater than the ones used to justify the project

Digital Recorder Upgrade

EPRI Workshop on Licensing Digital Upgrades for Nuclear Power Plants

Synopsis of Breakout Session #4
June 14, 1994

Daniel E. Sipple
Northeast Nuclear Energy Co.

Objectives of Session

- To describe issues associated with digital upgrades, such as vendor qualification programs and utility dedication processes, based on actual experience of a digital recorder replacement at Millstone Unit One.
- To demonstrate how the Licensing Guideline (TR-102348) can be applied to a simple analog-to-digital upgrade.
- To elicit feedback from participants on their related experience and problems with analog-to-digital upgrades.

Approach of Session

This session will describe a digital recorder upgrade using the licensing guideline approach. The example is based on an actual recorder upgrade at NNECO Millstone Unit One Power Plant. The project involved dedicating commercially available products for nuclear 1E applications. The utility and vendor processes in this dedication process will be described. Digital issues from the 50.59 evaluation, operational benefits, and cost/benefit assessments will also be discussed.

Breakout Session #4, cont'd

Organization of Session

The session will consist of the following parts:

- An overview of the digital recorder upgrade project in terms of the licensing guideline.
- A review and discussion on experiences with vendors on qualification of digital equipment.
- A presentation and discussion of a failure analysis describing key issues in design and implementation.
- A review and discussion of the 50.59 evaluation process.
- A review and discussion of NNECO experience and lessons learned from the upgrade.
- Open discussion and question-and-answer session. Time will be allowed for participants to ask questions and for general discussion on the topics covered in this breakout session.

Main Points to be Conveyed

- The licensing guideline is applicable to safety and non-safety upgrades.
- The licensing guideline is generic, but easily applied to a typical analog-to-digital upgrade.
- Digital systems provide features which reduce operator burdens, improve readability, availability, and reliability.
- Cost benefits of performing a digital upgrade based on the approach outlined in EPRI TR-102348.

Applications of V&V Handbook for Upgrades to Digital Systems

EPRI Workshop on Licensing Digital Upgrades for Nuclear Power Plants

Synopsis of Breakout Session #5

June 14-15, 1994

Charles A. Lewis
Arizona Public Service Company

Randall S. May
S. Levy Incorporated

Objectives of Session

- To show how the V&V Handbook can provide guidance for typical upgrades.
- To provide specific examples of V&V activities and documentation.
- To elicit feedback from participants on their own upgrade problems and issues.

Approach of Session

The approach of this session will be to relate the V&V Handbook's recommendations for software development, verification and validation to upgrade projects of current interest to utilities. A previously developed system design already exists which closely follows the recommendations of the V&V Handbook. Elements of this system will be discussed first to provide examples and context. Then a new project will be described, and the participants will be asked to assist the presenters in defining elements of a V&V plan, while walking through sections of the V&V Handbook as a guide.

Organization of Session

The session will be divided into three roughly equal parts:

- *V&V program for the B&W Owners' Group Advanced Control System (ACS) prototype.* This ambitious control system development effort employed distributed control system products, an advanced plant-wide control algorithm and triply redundant logic. The development and V&V activities, as well as documentation were quite consistent with V&V handbook guidance, so they provide good examples for how it can be applied.
- *V&V Handbook guidance for Control System Upgrades anticipated by Palo Verde.* Arizona Public Service has recently begun planning for the coordinated upgrade of three major control systems. The participants will be asked to interactively provide suggestions, aided by guidance from the V&V Handbook, to help the presenters build up a few elements of a V&V Plan. To achieve this, the session presenters and participants will walk through selected sections of the handbook, with the examples from the B&W ACS serving as a starting point.

The session presenters will have prepared in advance several slides of their own solution, which can be compared with suggestions of session participants.

- *Open discussion based upon interest of participants.* With the time remaining in the session, participants may select or propose topics for open discussion. Possible topics include: differences among V&V activities for upgrades of large systems, small systems or individual components; differences in V&V practices among specific system types such as reactor protection systems, engineered safety features systems, and non-safety systems whose failure may challenge a safety system; impact of different development approaches such as custom development versus application of commercial product lines (Programmable Logic Controllers and Distributed Control Systems); independent review, and relation to system level licensing issues. The presenters will attempt to provide pointers to helpful sections of the V&V Handbook, as appropriate.

Main Points to be Conveyed

- *V&V applies not only to safety systems, but also to important control systems.* While the V&V Handbook allows much greater latitude in how non-safety systems are to be verified, validated and documented, the basic principles of what to do are similar. In fact, because of their relative complexity and plant feedback, control systems are in some respects more difficult to specify and test than safety systems.
- *Development and V&V documentation provide the transparency needed for independent review.* For safety systems, it is not sufficient that the installed system be sound; the process must be sufficiently rigorous and the supporting documentation must be sufficient clear and complete to convince an independent reviewer to have high confidence in the soundness of the system.
- *V&V techniques may actually be useful!* For example, a traceability matrix constructed at the beginning of a project can be of great practical use to the system engineer; it should not be viewed as just an odious regulatory requirement. Furthermore, if designed sensibly and at the start of a project, it need not take much effort. Similarly, independent review and analysis of specifications may be quite valuable for catching high level requirements defects, before they find their way into code or data and become very expensive to fix.
- *The V&V Handbook provides a road map and examples of practical techniques.* The V&V Handbook design recognizes that a wide range of applications and implementation approaches are of interest in digital upgrades. The handbook provides the project engineer or manager with a range of options and techniques, while allowing enough flexibility to use engineering judgement and experience to accommodate the special needs of a project. The examples and walkthroughs should demonstrate its practical value.

Attachment #4

Monday, June 13

- 7:00 Registration and Continental Breakfast
- 8:00 **General Session**
- Welcome/Overview of Workshop *Ray Torok*
EPRI
- Keynote Address *Peter Katz*
Baltimore Gas & Electric
- 8:30 Industry Perspective *Carl Yoder*
EPRI/NUMARC Committee
- 9:00 NRC Perspective *Bruce Boger*
NRC
- 9:45 **BREAK**
- 10:00 Guideline on Licensing Digital Upgrades *Bob Fink*
MPR Associates
Ray Torok
EPRI
- 11:30 Testing the Guideline Approach *Gerry van Noordennen*
Northeast Utilities
- 12:00 **LUNCH**
- 1:00 Defense in Depth for a Reactor Protection System Upgrade *Rick Mason*
Commonwealth Edison
- 1:45 Incorporation of A/D Considerations into Utility Procedures *Ray DiSandro*
Philadelphia Electric
Carl Yoder
Baltimore Gas & Electric
- 3:00 **BREAK**
- 3:30 Panel Discussion on the Licensing Environment for Future Digital Upgrades
- 5:00 **ADJOURN**
- 5:30 **RECEPTION**

Tuesday, June 14

- 7:00 Continental Breakfast
- 8:00 **General Session - Updated Guidance for Digital Upgrades**
- The Licensing Process, 50.59 Safety Evaluations & Failure Analysis *Charles Waite
Public Service Electric & Gas
Ray Torok
EPRI*
- 9:00 Applying the New IEEE 7-4.3.2 Standard *Rick Blawie
Commonwealth Edison*
- 9:30 EPRI V&V Handbook/Approach *Ray Rettberg
GPU Nuclear
Randy May
S. Levy Inc.*
- 10:15 **BREAK**
- 10:30 EPRI EMI Design Guide and Handbook/Approach *Carl Yod
Baltimore Gas & Electric
Jim Shank
Public Service Electric & Gas*
- 11:15 Commercial Dedication Issues *Joe Naser
EPRI*
- 12:00 **LUNCH**

Tuesday, June 14 (cont.)

1:00

Breakout Sessions on Application of Guidelines

3:00

Session 1. Digital Controller Retrofit - a typical small scale upgrade *Julie Sickle*
Baltimore Gas & Electric

Session 2. Salem Annunciator Upgrade - lessons learned *Charles Waite*
Public Service Electric & Gas

1:00

Session 3. PWR Feedwater Upgrade - addresses safety and nonsafety considerations *John Hefler*
Pacific Gas & Electric

Session 4. Digital Recorder Upgrade - a simple upgrade with commercial dedication aspects *Daniel Sipple*
Northeast Nuclear Energy

Session 5. V&V Handbook Treatment of Software Development Example *Charles Lewis*
Arizona Public Service
Randy May
S. Levy Inc.

2:45

BREAK

3:00

Repeat of Breakout Sessions

4:45

ADJOURN

Wednesday, June 15

- 7:00 Continental Breakfast
- 8:00 Repeat of Breakout Sessions
- 9:45 **BREAK**
- 10:00 Road map to Related EPRI Activities
- 10:30 Panel Discussion on Perspective from Breakout Sessions and Future Utility Needs
- 12:00 **ADJOURN**

Albert Machiels
EPRI