UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D.C. 20555-0001

February 4, 2000

MEMORANDUM TO: ACRS Members

FROM: Noel Dudley, Senior Staff Engineer
ACRS

SUBJECT: CERTIFICATION OF THE MINUTES OF THE ACRS SUBCOMMITTEE ON HUMAN FACTORS NOVEMBER 19, 1999 - ROCKVILLE, MARYLAND

The minutes of the subject meeting, issued December 17, 1999, have been certified as the official record of the proceedings of that meeting. A copy of the certified minutes is attached.

Attachment: As stated

cc: via E-mail
J. Larkins
R. Savio
S. Duraiswamy
ACRS Staff Engineers
ACRS Fellows

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D.C. 20555-0001

MEMORANDUM TO: Juan D. Peralta, Staff Engineer
ACRS

FROM: Dr. George Apostolakis, Chairman
Human Factors Subcommittee

SUBJECT: CERTIFICATION OF THE SUMMARY/MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON HUMAN FACTORS, NOVEMBER 19, 1999, ROCKVILLE, MARYLAND

I do hereby certify that, to the best of my knowledge and belief, the minutes of the subject meeting held on November 19, 1999, are an accurate record of the proceedings for that meeting.

2/4/00

George Apostolakis, Chairman — Date
Human Factors Subcommittee

cc: N. Dudley

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D.C. 20555-0001

December 17, 1999

MEMORANDUM TO: Dr. George Apostolakis, Chairman
Human Factors Subcommittee

FROM: Juan D. Peralta, Staff Engineer
ACRS

SUBJECT: WORKING COPY OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON HUMAN FACTORS, NOVEMBER 19, 1999, ROCKVILLE, MARYLAND

A working copy of the minutes for the subject meeting is attached for your review. Please review and comment on them at your soonest convenience. Copies are being sent to each ACRS Member who attended the meeting for information and/or review.

Attachment:
As Stated

cc: ACRS Members
J. Larkins
H. Larson
S. Duraiswamy
N. Dudley

CERTIFIED BY:
G. Apostolakis - 2/4/00

CERTIFIED

Date: 12/17/99

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
HUMAN FACTORS SUBCOMMITTEE MEETING
REVIEW OF ATHEANA METHOD AND RELATED MATTERS
NOVEMBER 19, 1999
ROCKVILLE, MARYLAND

INTRODUCTION

The ACRS Subcommittee on Human Factors held a meeting on November 19, 1999, at 11545 Rockville Pike, Rockville, MD, in Room T-2B3. The purpose of the meeting was to hear presentations by and hold discussions with representatives of the NRC staff concerning the ATHEANA process, use of the ATHEANA process to evaluate selected operational events, and related matters.

The entire meeting was open to public attendance. Mr. Juan Peralta was the cognizant ACRS staff engineer and Designated Federal Official for this meeting. The meeting was convened by the Subcommittee Chairman at 8:30 a.m., November 19, 1999, recessed at 10:23 a.m. and reconvened at 10:40 a.m., and later recessed at 11:40 a.m. and reconvened at 12:45 p.m. that day. Finally, the meeting was adjourned for the day at 3:10 p.m.

ATTENDEES

ACRS Members/Staff:

G. Apostolakis, Chairman
T. Kress, Member
D. Powers, Member
J. Barton, Member
J. Peralta, ACRS Staff
M. Bonaca, Member
J. Sieber, Member
R. Uhrig, Member
R. Seale, Member
N. Dudley, ACRS Staff

Principal NRC Speakers:

C. Thompson, RES*
M. Cunningham, RES
A. Ramey-Smith, RES
J. Forester, RES (Sandia National Laboratories)
A. Kolaczkowski, RES (SAIC*)
J. Sorensen, ACRS Fellow

RES Office of Nuclear Regulatory Research
SAIC Science Applications International Corporation

There were approximately 7 other members of the public in attendance during 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 SUBCOMMITTEE CHAIRMAN

Dr. Apostolakis convened the meeting at 8:30 a.m. He stated that the purpose of this meeting was to hear presentations by and hold discussions with representatives of the NRC staff regarding a proposed revision to NUREG-1624, "Technical Basis and Implementation for A Technique for Human Event Analysis (ATHEANA)," application of the ATHEANA method to assess design basis accidents or operational events, and other related matters.

Dr. Apostolakis mentioned that Mr. Jack Sorensen, ACRS Fellow, would be making a presentation to the Subcommittee on "safety culture" and requested RES staff participation and feedback on this topic.

Finally, Dr. Apostolakis stated that the Subcommittee had received no written comments or requests for time to make oral statements from members of the public.

DISCUSSION OF AGENDA ITEMS

ATHEANA

Mr. Mark Cunningham, RES, made introductory remarks and outlined the agenda for the staff's presentation. He noted that the staff's presentation would focus on current efforts associated with the incorporation of peer review comments on ATHEANA followed by other topics related to human reliability analysis (HRA) international efforts by RES.

RES Staff Presentation

Dr. Catherine Thompson, RES, led the staff's presentation on ATHEANA. Messrs. John Forester and Alan Kolaczkowski, RES (contractors) also participated in the discussions.
Dr. Thompson provided a brief outline of her presentation indicating that it would consist of four parts: overview and introduction, structure of ATHEANA, application of ATHEANA, and conclusion and follow-up activities.

Dr. Thompson provided a brief background on the need and basis of the ATHEANA method. She identified the main three objectives of ATHEANA — (1) enhance HRA representation of human behavior during accidents, (2) develop insights to improve plant safety and performance, and (3) support resolution of regulatory and industry issues. Dr. Thompson concluded her portion of the presentation by summarizing the current status of the ATHEANA project, i.e., Revision 1 of NUREG-1624 is being prepared for publication and public comment.

Mr. Forester discussed the structure of ATHEANA by explaining that ATHEANA includes both a process for performing retrospective as well as prospective analyses of plant events. He clarified that one of the peer review comments involved a recommendation to include in ATHEANA an explicitly documented process for performing a retrospective analyses. As a result of that comment, such a process is now included in ATHEANA.

Mr. Forester briefly described the use of the "base case" scenario in ATHEANA, operational vulnerabilities, deviations, and ATHENA's four search " schemes, i.e., (1) the identification of deviations from the base case scenario, (2) the identification of deviations for vulnerabilities associated with procedures and plant "informal rules", (3) the identification of deviations caused by subtle failures in support systems, and (4) the identification of deviations that can set up operator action tendencies and errors leading towards human failure events and unsafe acts of interest to the analysts. Mr. Forester's presentation culminated with a discussion on ATHEANA's integrated quantification process.

Mr. Kolaczkowski's presentation focused on an example of the application of the ATHEANA method to the re-analysis of 2 fire probabilistic risk assessment (PRA) scenarios in a self-induced station blackout (SISBO) plant. Mr. Kolaczkowski described in detail the process by which ATHEANA would identify the potential human failure events and unsafe actions during these postulated fire scenarios. In his concluding remarks, Mr. Kolaczkowski emphasized that while current fire HRAs generally fail to address the potential unexpected effects on equipment and corresponding impact on plant behavior, ATHEANA provides a better vehicle for identifying specific plant improvements needed to eliminate human factors-related vulnerabilities.

Dr. Thompson concluded the staff's presentation by briefly reiterating the staff's perspective on ATHEANA and by outlining planned follow-up activities related to this effort.

Overview of International HRA Research

Mr. Cunningham led the staff's discussion on this portion of the presentation. Dr. Thompson, and Ms. Ann Ramey-Smith also participated.

Mr. Cunningham briefly described current mechanisms of RES interaction with international organizations on HRA methods. Mr. Cunningham provided a brief synopsis of the goals and results achieved so far by RES through its involvement with international organizations working in the HRA field.

Safety Culture

Dr. Apostolakis introduced the next speaker, Mr. Jack Sorensen, ACRS Fellow, who, on behalf of the ACRS, is formulating a white paper dealing with the subject of "safety culture." Mr. Sorensen clarified that the white paper is a "tutorial" that aims to articulate the fundamental tenets of HRA to non-practitioners. He added that the white paper does not attempt to advance the state-of-the-art on safety culture not does it attempt to review or critique the NRC HRA program. Mr. Sorensen welcomed and requested feedback from the audience on any part of his presentation.

Mr. Sorensen provided a brief background on the history of the term "safety culture" and its use in the nuclear industry, discussed the relevance and significance of the term in relation to significant, past industrial accidents and events, and elaborated briefly on the idea of "culture" as a concept in organizational behavior.

Committee members exchanged views and opinions on the critical attributes and characteristics shared by successful, safety-conscious organizations.

SUBCOMMITTEE CONCERNS, COMMENTS, AND RECOMMENDATIONS

ATHEANA

Drs. Powers and Apostolakis emphasized that a better "screening" process, i.e., that allows the user to tailor the ATHEANA method to the rigor demanded by specific circumstances, is needed if nuclear utilities are to effectively avail themselves of its benefits. Mr. Cunningham and his staff agreed that such a screening process would be helpful.

Dr. Apostolakis expressed concern with ATHEANA's inadequate treatment of the impact that "safety culture" has on the decision-making process, i.e., when plant crews are confronted by situations that involve conflicting safety and economic objectives.

Dr. Bonaca asked whether and how ATHEANA considers "informal" processes that operators typically rely on to perform their duties, particularly, during abnormal conditions. Mr. Forester replied that "informal" processes are considered in ATHEANA's error-forcing context development stage albeit not explicitly.

Drs. Apostolakis and Powers also expressed concern about the inordinate complexity of searching for error-forcing contexts in the current ATHEANA methodology. Mr. Cunningham agreed that a better description of the process is needed and that RES is currently evaluating its options in terms of ATHEANA's budget and previously planned work.

Mr. Barton, Mr. Sieber, and Dr. Bonaca questioned the value and usefulness of the data that would be generated by using ATHEANA, and whether the NRC should continue to expend resources on this program.

Safety Culture

Mr. Barton suggested that rather than focusing on accidents or disasters when evaluating organizational data to determine or gauge "safety culture" at a given institution, the review must concentrate on precursors or on those less significant events that may augur an impending accident, e.g., industrial mishaps, operational errors, and recurrent failure of maintenance personnel to follow procedures, etc.

Mr. Sorensen cautioned that not all investigators in the field agree that smaller or less significant incidents extrapolate to accidents. Dr. Seale pointed out that the extent to which an organization is wiling to tolerate such smaller or less significant incidents nonetheless may provide an indication or "measurement" of safety culture.

SUBCOMMITTEE DECISIONS

ATHEANA

The Subcommittee decided to recommend to the ACRS that a letter be written to the EDO on this subject.

Safety Culture

The Subcommittee made no decisions on this subject.

BACKGROUND MATERIAL PROVIDED TO THE SUBCOMMITTEE PRIOR TO THE MEETING

1. NUREG-1624, "Technical Basis and Implementation for A Technique For Human Event Analysis (ATHEANA)." A copy of NUREG-1624, Revision 1.
2. Memorandum dated July 30, 1998, from Mr. Noel Dudley to ACRS Members, Subject: Peer Review Meeting Concerning A Technique for Human Event Analysis (ATHEANA).
3. Peer Review Members Comments (Dr. P. Carlo Cacciabue — Joint Research Center, Italy; Dr. Erik Hollnagel — University of Linkoping, Sweden; Dr. Oliver Sträter — GRS mbH, Germany; and Mr. Stewart Lewis — SAROS, Inc.)

PRESENTATION SLIDES AND HANDOUTS PROVIDED DURING THE SUBCOMMITTEE MEETING

The presentation slides and non-proprietary handouts used during the meeting are attached (see Attachment 1).

••

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/ACRSACNW or can be purchased from Ann Riley & Associates, LTD., 1025 Connecticut Ave, NW, Suite 1014, Washington, D.C. 20036, (202) 842-0034.

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE MEETING ON HUMAN FACTORS

NOVEMBER 19, 1999
Date(s)

NOVEMBER 19, 1999
Today's Date

ATTENDEES - PLEASE SIGN BELOW

PLEASE PRINT

NAME	AFFILIATION
JOHN FORESTER	SANDIA NAT. LABS
Susan E. Cooper	Science Applications International Corp
DENNIS C BLEY	Buttonwood Consulting Inc
Alan Kolaczkowski	SCIENCE APPLICATIONS INT'L. CORP.
BRIAN HAAGENSEN	PSHA
Paul Swetland	PSHA
Rick Weil	MIT

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

SUBCOMMITTEE MEETING ON HUMAN FACTORS

NOVEMBER 19, 1999
Date(s)

NOVEMBER 19, 1999
Today's Date

NRC STAFF SIGN IN FOR ACRS MEETING

PLEASE PRINT

NAME	BADGE #	AFFILIATION
GARETH W. PARRY	B-8060	NRC/NRR/DSSA
NATHAN SIU	B-8130	NRC/RES/DRAA
J PERSENSKY	B-8413	NRC/RES/DSARE
Ann Ramey-Smith	B6966	NRC/RES/DRAA
Paul Lewis	B6680	NRC/RES/DSARE

ATHEANA

A Technique for Human Event Analysis

A Presentation to the Advisory Committee on Reactor Safeguards

Catherine Thompson
Probabilistic Risk Analysis Branch, RES, NRC
John Forester
Sandia National Laboratories
Alan Kolaczkowski
Science Applications International Corporation

November 19, 1999

Attachment 1

Overview and Introduction

Outline of Presentation

- Overview & Introduction
- Structure of ATHEANA
- Application of ATHEANA
- Conclusions and Follow-up Activities

Overview and Introduction

Why a New HRA Method?

Real-World Accidents

- Problems involve failures in situation assessment
- Plant behavior not understood
  - operations outside design range
  - biases limit ability to understand
- Indications not recognized as cues to the event
- Procedures do not help
  - often do not "match" sequence of event

Current HRA Modeling

- Inadequate consideration of impact of plant behavior on information processing
- Plant behavior assumed to be understood by operators
  - misunderstanding of plant behavior by operators is not a major contributor
- Minimal
- Mostly focuses on missed steps

Overview and Introduction continued

Basis and Purpose of ATHEANA

- Basis: people behave "rationally" even if reason for action is wrong. Hence find contexts that create *appearance* that action is needed when, in fact, it is not.
  - Operating events show this
- Purpose: to provide a workable, realistic way to:
  - identify & quantify for PRAs:
    - *errors of commission*, wherein operators deliberately intervene with equipment to create new hazard states as defined by PRA models
    - *errors of omission* that result from situations

Overview and Introduction continued

Objectives of ATHEANA

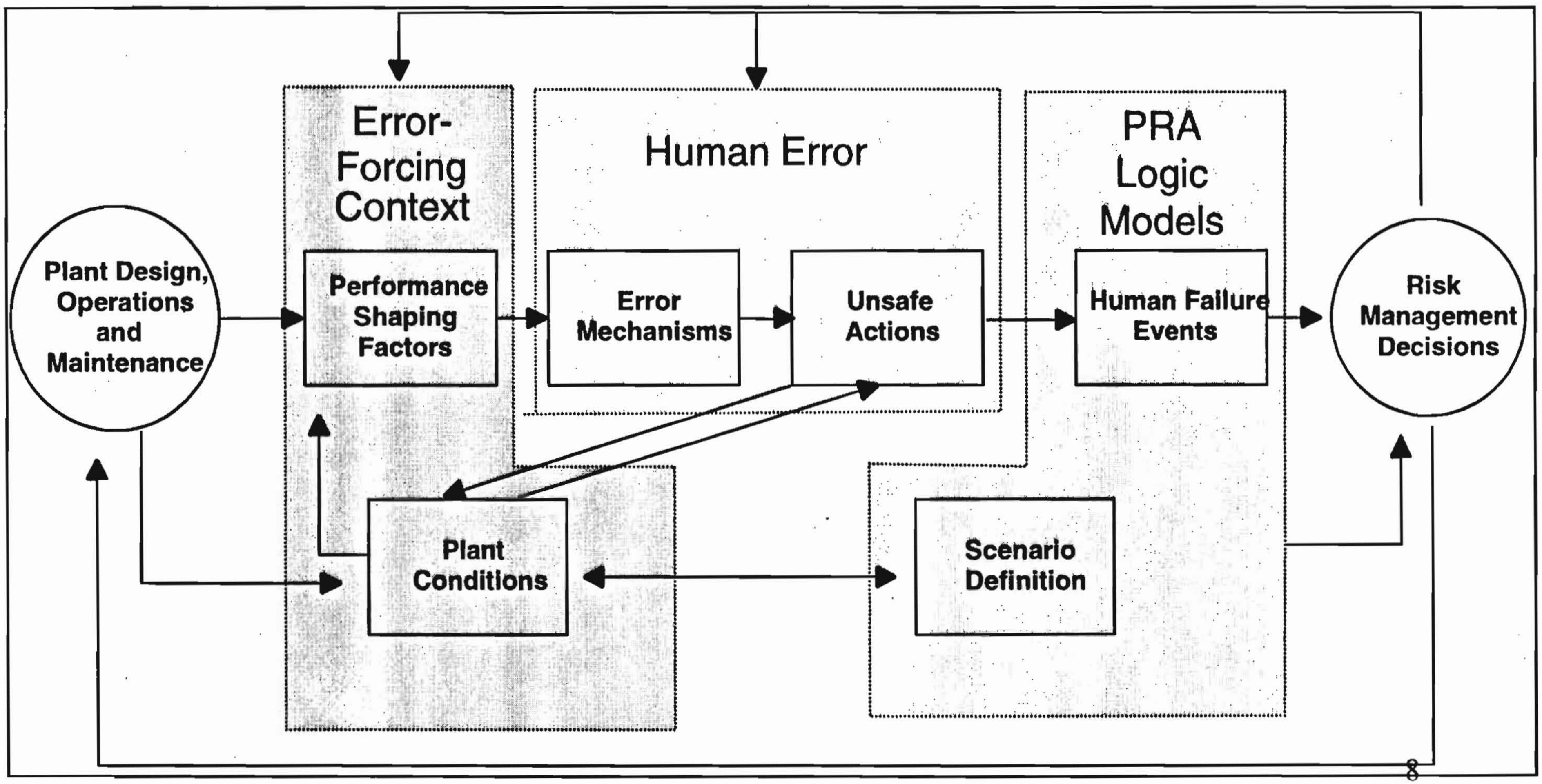
- **Enhance HRA's representation of human behavior seen in accidents and near-miss events:**
  - more realistically incorporate kinds of human-system interactions found important in accidents and near misses
    - errors in decision processes
    - dependencies among sequential human actions
  - integrate perspectives of PRA, plant engineering, operations & training, psychology, & risk-informed regulation
- **Develop insights to improve plant safety and performance**
- **Support resolution of regulatory and industry issues**

Overview and Introduction continued

Characteristics of ATHEANA

- Experience-based
- Focuses on context-driven behaviors
- Links plant conditions, PSFs and error mechanisms
- Consideration of dependencies
- Uses multidisciplinary approach
- Structured search for problem scenarios and unsafe actions

Multidisciplinary Framework



ATHEANA Team

- Catherine Thompson, NRC
- Ann Ramey-Smith, NRC
- John Forester, SNL
- Susan Cooper, SAIC
- Alan Kolaczkowski, SAIC
- Dennis Bley, Buttonwood Consulting, Inc.
- John Wreathall, JWCo, Inc.

Project Status

- Technical basis and implementation guidelines issued as a draft report for public comment (NUREG-1624) in May 1998
  - Documented first demonstration of ATHEANA
- Peer review meeting held over a two-day period in June 1998 in Seattle, Washington
- Method improvements based on experience in initial trial and inputs from peer review,
  - illustrated through case studies
- Rev. 1 of NUREG-1624 being prepared for publication

Structure of ATHEANA

Retrospective and Prospective Applications of ATHEANA

- To better understand events
  - Individually
  - Collectively
- To provide a tool for addressing and resolving issues:
  - Expected (or base case) scenarios for issues of interest
  - Deviations from base case scenarios (four level search)
  - Relationship between deviations (plant conditions), human error mechanisms, and PSFs
  - Integrated Recovery Analysis/Quantification

Prospective Analysis

- Most serious accidents involve human unsafe acts performed when the plant enters conditions not understood by its crew
- Need to identify such possible conditions prospectively
  - identify "base case" scenarios
    - Conditions expected by operators
  - identify operational vulnerabilities
    - Procedures, knowledge, ...
  - Identify deviations from "base case" conditions
    - How can problematic conditions occur?
- How can we find them?

"Base Case" Scenario

- **The base case scenario:**
  - represents a realistic description of expected plant and operator behavior for selected issue and initiator
  - provides basis to identify and define deviations from such expectations (found in Step 6)
- **Ideal base case scenario:**
  - is the consensus operator model (COM)
  - is well-defined operationally
  - has well-defined physics
  - is well documented
  - is realistic
- **Scenario description often based on FSAR or other well-documented analyses**

Operational Vulnerabilities

- Investigation of potential vulnerabilities due to biases in operator expectations
- Understanding of base-case scenario timeline and any inherent difficulties associated with required response
- Identification of operator-action tendencies based on
  - "standardized" responses to indications of plant conditions
  - informal rules
- Evaluation of formal rules and EOPs
  - critical decision points, ambiguities, sources of confusion, timing mismatches, etc.

Deviations?

- Deviations are plant behaviors or conditions that set up unsafe actions by creating mismatches between the proposed plant behavior and:
  - operators' knowledge, expectations, biases & training
  - procedural guidance & timing
- Plant conditions, associated PSFs, & error mechanisms found in this step define an initial error-forcing context
- ATHEANA search schemes guide analysts to find real deviations in plant behavior and conditions
  - not just false perceptions in the operators' minds

Four Search Schemes

- Identify deviations from the base case scenario using "HAZOP" guide words to discover troublesome ways that the scenario may differ from base case
  - more, less, quicker, slower, repeat ...
- Identify deviations for vulnerabilities associated with procedures & informal rules
  - changes in timing, sequencing of decision points, etc.
- Identify deviations caused by subtle failures in support systems
  - cause problems for operators to identify what's happening
- Identify deviations that can set up operator action tendencies & error types leading towards HFEs/UAs of interest

What is Effect of Deviation on Operators?

- For first three searches:
  - Determine whether deviation characteristics lead to ("trigger") relevant error mechanisms & error types
    - Does error type match HFE & UAs of concern?
      - If "No", then screen out
      - If "Yes", then keep for further analysis
- In the fourth scheme, approach is reversed; identify possible error types & tendencies that could cause the HFEs & UAs, then identify deviations containing appropriate characteristics

Deviation Scenario Development

- Deviation characteristics are the product of all four searches
- Deviation scenarios are developed:
  - from all deviation characteristics
  - using plant operations & T-H knowledge
- Consider additional complicating factors
  - additional hardware failures, configuration problems, unavailabilities, indicator failures
  - additional PSFs
- Deviation description is extended to include the scenario characteristics up to the last opportunity for recovery

19

Integrated Quantification

- Entire scenario, including recovery possibilities quantified in integrated fashion:
  - Frequency of plant conditions calculated by standard systems analysis tools
  - Probability of unsafe act and non-recovery, given plant conditions and PSFs, estimated in an integrated fashion:
    - operating experience
    - operator/trainer/analyst judgment
    - other quantification methods
- Full quantification is not only way to resolve issues:
  - qualitative evaluations
  - simplified reliability/risk modeling

Application of ATHEANA

Fire Scenario

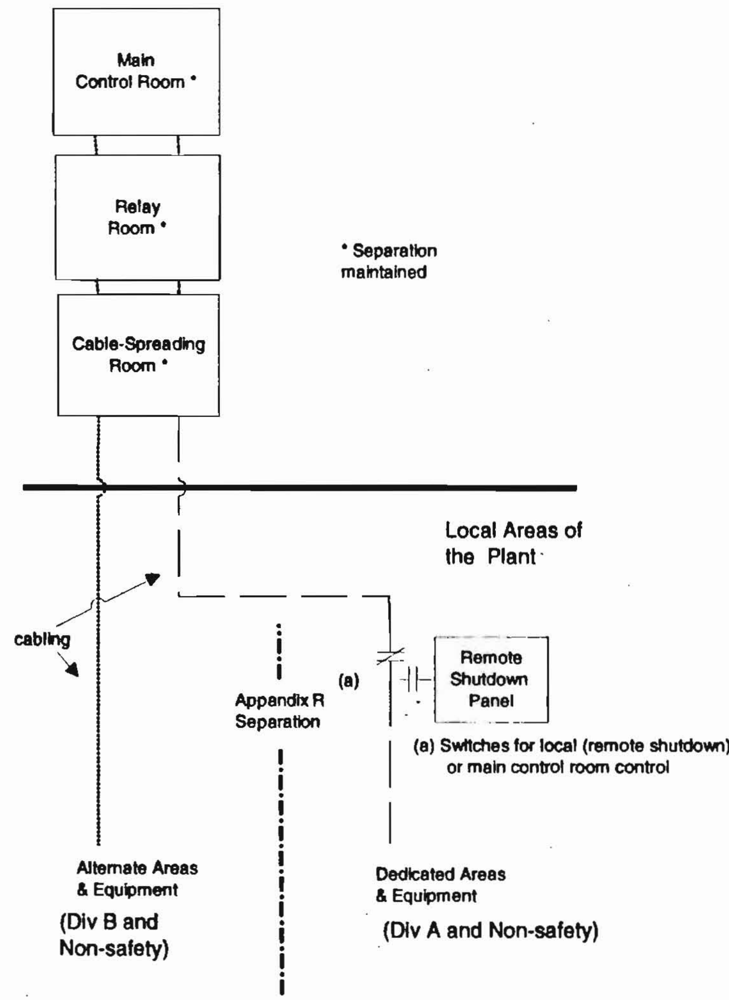
Introduction to the Fire Example

- Fire events can lead to cognitively challenging events
- Few fire event reports discuss impacts of fire event context on control of plant operations
- Current fire HRAs generally fail to account for the special context produced by fires (potential unexpected effects on equipment, erratic plant behavior…)
  - Most fire HRAs simply use or modify the human errors quantified in the IPE
  - Often, only the direct impact of flames preventing access to certain locations and heavy smoke physically interfering with response implementation are considered

- Issue: Can we identify useful ways to improve operator preparedness for fires in SISBO plants?

ATHEANA Used to Reanalyze Two Fire PRA Scenarios In a "SISBO" Plant

(deenergize all buses/loads (i.e., no offsite power) & restore safety division power & certain equipment NOT affected by the fire)



23

ATHEANA Used to Reanalyze Two Fire PRA Scenarios in a "SISBO" Plant (cont'd)

- AFWS Pump B Room Oil Fire (Alternate Area Fire) [CDF approx 1E-5/yr]
  - Loss of 4/4 non-safety 4160v buses - balance-of-plant not operable
  - Loss of safety Div B 4160v bus, EDG, and loads
  - Loss of both AFWS pump B and AFWS turbine pump
  - Expected to leave MCR and shutdown using limited Div A ("dedicated") equipment and remote shutdown panel (use EOP-FP-Y)
- Fire in Room Containing Safety Div A 480v Buses & Remote Shutdown Panel (Dedicated Area Fire) [CDF approx 1E-5/yr]
  - Loss of safety Div A buses, EDG, and loads
  - Expected to shutdown using Div B ("alternate") equipment from the MCR (use EOP-FP-Z)

- Existing PRA Dominant HRA Insights (using existing HRA methods) for Above 2 Fire Scenarios
  - Diagnosis error to appropriately enter EOP-FP-Y or -Z due to
    - misreading or miscommunicating cues to enter EOP-FP-Y or -Z
    - skipping step to enter EOP-FP-Y or -Z
    - misinterpreting the instruction regarding entrance to EOP-FP-Y or -Z
  - Implementation errors primarily due to switch positioning errors or omissions under high stress

Identifying Base Case for Fire Example (1)

- Fire detection alarm occurs during plant operation
- Operators enter Fire Response Procedure and have fire visually validated
- Fire brigade assembled, doors unlocked to area, plant staff notified, etc.
- MCR staff attempt to maintain plant on-line and under proper control
- Erratic operation of normally running equipment, progressively worse over time
- Effects on standby equipment; may or may not be noticed
- Periodic communication between fire brigade and MCR staff

Identifying Base Case for Fire Example (2)

- As conditions worsen, judgment is made that ability to monitor plant status & control equipment is in jeopardy
- EOP-FP-Y or -Z entered & implemented appropriately
- Plant restabilized and shutdown successfully
- Fire eventually extinguished
- Technical support staff may have been convened and the Emergency Plan enacted

Define HFE and UAs for Fire Example

- HFE is: Failure to accomplish heat removal
- UAs are:
  - (UA1) Failure to enter EOP-FP-Y or -Z or wait too long to enter the appropriate EOP (could result in more equipment damage and possibility of "hot short" equipment actuations and further loss of plant configuration & control)
  - (UA2) Failure to carry-out actions required by EOP-FP-Y or -Z
  - (UA3) Failure to appropriately respond/recover if conditions are worse or otherwise different than "expected" per the EOPs

Identifying Operational Vulnerabilities

- Training, experience, expectations
  - Rare event and trained infrequently - unfamiliarity
  - Disbelief that fire is "this bad" and not yet extinguished (expect fires to be put out quickly)
- Timing considerations
  - Time delays likely (i.e., actions postponed); verify alarm, delay decision to enter EOP-FP-Y or -Z
  - Limited time available (no longer than an hour) to reenergize equipment and restabilize the plant once equipment deenergization has occurred
- Tendencies/informal rules
  - Reluctance to deenergize significant portions of the plant at a time
  - High reluctance to evacuate MCR in the case of using EOP-FP-Y
- Formal rules/procedures/EOPs
  - Vague guidance on when to enter EOP-FP-Y or -Z (judgment by crew)
  - Limited/no guidance on alternatives if conditions are not as expected per the EOPs (e.g., what to do if "good" diesel will not start)

Deviation Search (1)

- **Initiator/Scenario deviations**
  - Fire growth faster/larger than expected [effects different/greater than expected]
  - Fire effects slower than expected or not detected (for standby equip) [missing/misleading info]
  - Fire detection failure [missing information]
  - Appendix R barriers not as expected or ineffective [effects different/greater than expected]
  - Equipment failures (especially of "good" equipment) [impasses, tradeoffs, shifts in attention, higher tempo, missing information]
  - Operators make implementation errors or take too long to carry-out actions (due to missing/wrong labeling, poor area conditions...) [misleading information, new effects, higher tempo]
  - Communication equipment problems [missing information, higher tempo]
  - MCR operators told fire "will be out momentarily" [missing or misleading information]
  - Fire extinguishing activities affect/fail "good" equipment [see equipment failures above]

"Triggered" error mechanisms include no/wrong/delayed entry into procedure/steps, lack of knowledge about plant condition, situation/indications conflict with procedures and/or expectations, anxiety about taking wrong action, reluctance/cautiousness

Tends to lead to unsafe acts including taking no action, delaying appropriate action, taking an inappropriate action (e.g., no or delayed entry into EOP, entry into wrong EOP, spread of effects across divisions, unexpected/undetected plant configurations, conditions "beyond" procedures...)

Deviation Search (2)

- **Deviations that "enable" rule problems**
  - No specific criteria as to when to enter/implement EOPs
  - No guidance regarding alternatives when conditions different, worse, or "beyond" that which is expected such as Appendix R breakdowns, "good" equipment failures...
- **Support system "deviations" -- nothing new**
- **Deviations that "enable" potentially unsafe tendencies**
  - Two strong tendencies exist: do not want to leave MCR and do not want to "SBO"

"Triggered" error mechanisms include no/wrong/delayed entry into procedure/steps, situation/indications conflict with procedures and/or expectations, anxiety about taking wrong action, reluctance/cautiousness

Tends to lead to unsafe acts including taking no action, delaying appropriate action, taking an inappropriate action (e.g., no or delayed entry into EOP, entry into wrong EOP, spread of effects across divisions, unexpected/undetected plant configurations, conditions "beyond" procedures...)

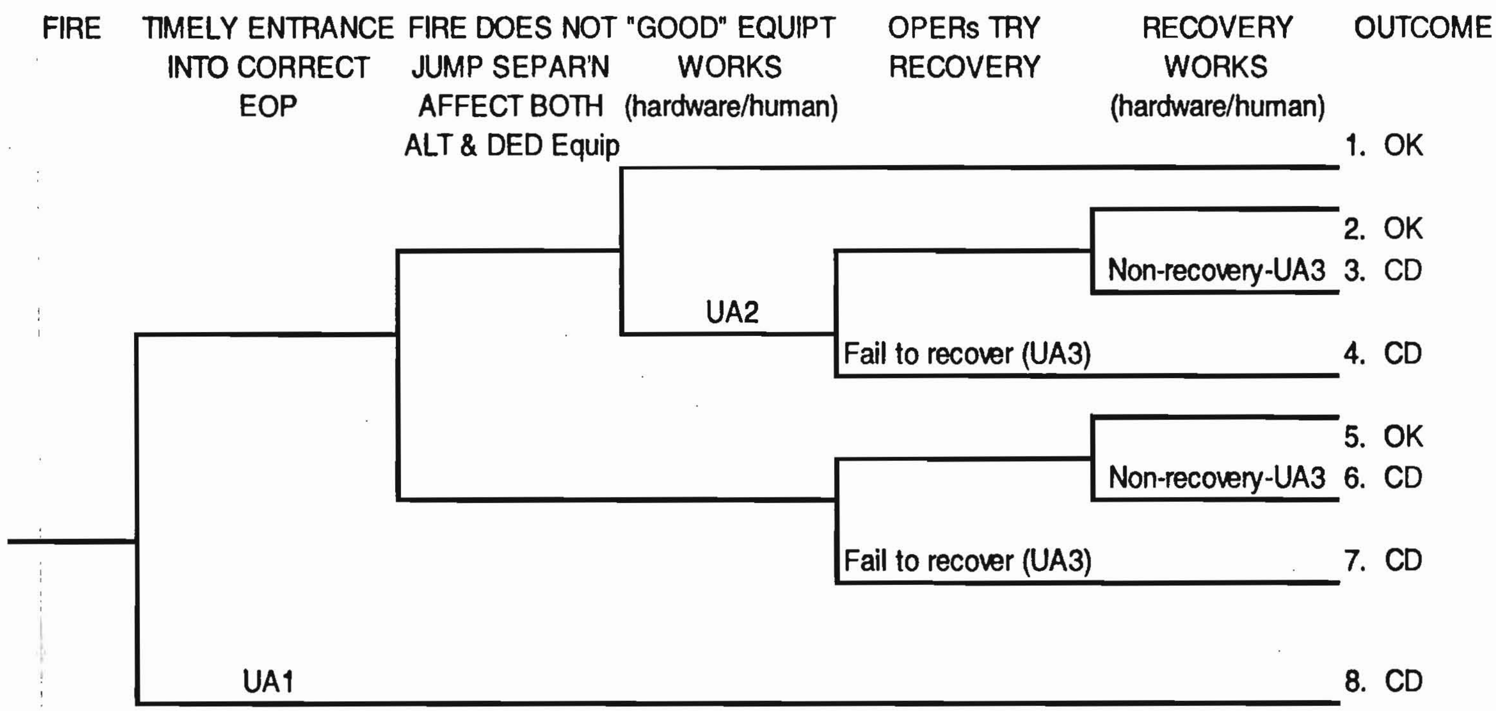
Deviation Scenario Development

- Summary characteristics of "troublesome" deviation scenario
  - Fire detection delayed
  - Fire effects occur somewhat slowly but progressively
  - Fire brigade has trouble putting out fire though believes/reports "it is almost under control"
  - Beyond initial fire conditions, the following are also important later deviations in the scenarios:
    - Fire duration & progression ultimately causes cross-divisional equipment effects, OR
    - Key "good" equipment item fails to function (e.g., diesel)
- No other complicating factors necessary for "troublesome" context

Recovery Analysis

- If entry into EOP does not occur or is too late (UA1):
  - it is assumed sufficient equipment "fails" so result is core damage (like done in existing PRA)
- If fire grows and affects *both* alternate & dedicated equipment or "good" equipment is tried but fails randomly or due to operator miscues (UA2):
  - Recovery considered - go back to reenergizing & using "fire-affected" divisional equipment as possible with no procedures
  - significant time may be taken with continuing to try to get "good" equipment operable again
- Failure to try recovery &/or implement it properly is UA3

Fire Example - Event Tree for Both Fire Scenarios



33

Quantification

- Plant condition inputs:
  - Slowly developing fire with uncertain status/effects: approx. 5E-5/yr for both fires (from PRA)
  - Fire does not cross separation & affect *both* dedicated & alternate equipment: 0.01(failure) (judgment simply to illustrate the possibility-not in current PRA)
  - Hardware contribution for failure of "good" equipment: 6E-2 to 0.1 depending on which fire (from PRA)
- PSFs: considered to exist (1.0 probability)
- UA1: our judgment and use of HEART both suggest 0.5 or greater for both fires (unfamiliar, complex, reluctance...), compared with existing PRA value of 9E-3
- UA2: approx. 2-9E-2 depending on which fire (from existing PRA - not examined closely by ATHEANA; would require specific plant layout, labeling, other info.)
- Fail to attempt timely recovery: judged to be less than 0.1 (operators will try something!)
- Non-recovery/UA3: our judgment and use of HEART both suggest 0.5 or greater for both fires (unfamiliar, untrained, no procedure guidance, complex...). Additionally, equipment may not work, erratic equipment responses, etc. also contribute.
- Resulting CDF for each sequence is ~3E-5/yr.

Existing PRA Results		ATHEANA Results	
Human Performance Observations	Implied "Fixes"	Human Performance Observations	Implied "Fixes"
misreading or miscommunicating cues	• training on cues • practice communication	• Rare event; unfamiliarity • Disbelief about fire "this bad" • Vague guidance on when to enter EOP-FP-Y or -Z (what are the cues and how to determine?)	• need minimum & definitive criteria for entering EOP-FP-Y or Z • do <u>not</u> treat fire status as criteria • need strategy for how to detect standby equipt failure
skipping step to enter EOP-FP-Y or Z	• highlight step in EOP-FP-X	• Reluctance to deenergize significant portions of the plant at a time • High reluctance to evacuate MCR in the case of using EOP-FP-Y	• train on new criteria to especially get over these concerns and build confidence
misinterpreting instruction to enter EOP	• train on entrance step	• must be able to implement	• ensure labeling, etc. unambiguous for local actions
positioning errors during implementation	• better labeling and/or mimics • training	Limited time available (no longer than an hour) to reenergize equipment and restabilize	• include training &/or walkthroughs of deviation scenarios with "added" difficulties
implementation errors caused by high stress	• more practice & training	Limited/no guidance on alternatives if conditions are not as expected per the EOPs	• add contingency actions for addressing "good" equipt failure

Conclusions and Follow-up Activities

Conclusions

- ATHEANA provides a workable approach to achieve realistic assessments of risk
  - straight-forward search process
  - causal explanations consistent with real events
- Develops insights to improve plant safety and performance
  - more specific explanation for errors
  - "fixes" based on mismatches between plant conditions, PSFs, operators' expectations & biases, etc.
- Supports resolution of regulatory and industry issues

37

Follow-Up Activities

- Perform additional applications
  - Digital I&C
  - Pressurized Thermal Shock
  - Fire
  - full-scale HRA/PRA
- Expand ATHEANA to incorporate:
  - Team aspects
  - M&O factors
- Develop software tools & aids, books
- Develop improved quantification tools
- Gather, analyze & disseminate data
- Collect data from other industries
- Apply ATHEANA to other industries

Discussion of Peer Review Comments

Overview of Presentation on Peer Review

- Peer reviewers and review process
- General strengths of ATHEANA as indicated by peer reviewers
- Specific criticisms or suggestions for improvements from reviewers and the ATHEANA team's responses
  - The ATHEANA framework and underlying models
  - The ATHEANA analysis process
  - The ATHEANA quantification process
  - Improving the efficiency, effectiveness and usefulness of ATHEANA
- Conclusion

Peer Review Team

- Dr. Erik Hollnagel
  - Principal Advisor at the OECD Halden Reactor Project, Adjunct Professor of Human-Machine Interaction at Linköping University, Sweden.
- Dr. Oliver Straeter
  - Researcher for GRS in Germany in the Safety Analysis and Operational Experience Branch.
- Dr. Pietro Carlo Cacciabue
  - Sector Head at the European Commission, Joint Research Centre, Institute for Systems, Informatics, and Safety, in Ispra , Italy
- Mr. Stuart R. Lewis
  - President of Safety and Reliability Optimization Services (SAROS), Inc., specializes in application of reliability and quantitative risk analysis methods.

Peer Review Process

- Technical basis and implementation guidelines issued as a draft report for public comment in May 1998
- Peer review meeting held over a two-day period in June 1998
- Peer review team's charter:
  - are the basic premises on solid ground & is the conceptual basis adequate?
  - is the ATHEANA implementation process adequate?
- Comments by others welcomed and received

General Strengths of ATHEANA
(As Indicated by Reviewers)

- <u>Treatment of Errors of Commission</u> (EOCs)
  - No other published approach addresses EOCs in PSA in such an extensive way
  - General approaches and concepts ...are appropriate to deal with problem of EOCs
  - Methods clearly provide a framework for identifying certain types of unsafe actions (especially errors of intention) that generally are not considered using current methods.

General Strengths of ATHEANA (Continued)

- Provides a <u>systematic way</u> of exploring how and why human failure events (HFEs) can occur:
  - ATHEANA can be used to develop detailed qualitative insights into conditions that may cause problems
  - Focuses on the important issues of context and cognition that need to be tackled
  - Process will allow knowledge to be shared and captured in a way that enhances both the completeness and realism of the PRA, and the quality of training and procedures
  - Develops a solid basis for redesign of working procedures, training, and interface

Specific Criticisms from Reviewers and ATHEANA Team Responses

- The ATHEANA framework and underlying models
- The ATHEANA analysis process
- The ATHEANA quantification process
- Improving the efficiency and usefulness of ATHEANA

ATHEANA Framework and Underlying Models

- *Comment:* Definitions and distinctions between the components of the framework and their interrelationships with each other and with the cognitive model were not sufficiently clarified
- *Response:* Explicitly describes and ties together the relationship between plant conditions, PSFs, error mechanisms, and the cognitive model
  - Guidance is provided for how to use this information to identify potential unsafe actions and the associated error-forcing contexts (now part of the process)
    - much less of “a miracle occurs”

ATHEANA Analysis Process

- *Comment:* Regarding retrospective analysis
  - Need a formalized, structured procedure, separate from the proactive search process detailed in ATHEANA
  - Important for assisting analysts in evaluating their plant and supporting the proactive HRA analysis

- *Response:* Provides explicit description and examples of how to perform a retrospective analysis (Section 8)

ATHEANA Analysis Process (Continued)

- *Comment:* Need further development of prioritization process:
  - For helping analysts focus limited resources
  - Early evaluation of the potential risk of possible HFEs
  - Need identification and incorporation of crew characteristics and other M&O factors

ATHEANA Analysis Process (Continued)

- *Response:* (to prioritization process issues)
  - Issue-driven process limits scope
  - Priority-ordered search aims at particular problem scenarios
  - M&O factors
    - consideration of crew characteristics, informal rules & priorities, maintenance & training philosophies
    - other M&O factors - *still not developed*

ATHEANA Quantification Process

- *Comment:*
  - ATHEANA focuses only on human failure events where a particular context creates a very high likelihood of unsafe actions
    - EFCs where the unsafe action probability will be close to 1.0
    - Are there other EFC-UA combinations that are risk-important?

ATHEANA Quantification Process (Continued)

- *Response:*
  - Search process restructured:
    - structured to identify challenging contexts
    - then identifies *sets* of UAs relevant to those contexts
  - ATHEANA quantification process provides tools for quantifying UA likelihoods across a wide range of probabilities
    - mainly concerned with high and intermediate likelihood UAs
    - use most relevant existing quantification tools

ATHEANA Quantification Process
(Continued)

- *Comment:* Consideration of dependencies and treatment of recovery potential is not adequately addressed
- *Response:*
  - New search process explicitly includes searches for dependencies of all sort and kinds
  - Analysis of unsafe acts (including recovery) is integrated
  - Entire sequence of potential cues is outlined in a "Scenario Log" (time/symptom/possible actions), with parameter plots used to help identify symptoms (alarms, automatic actuations, and physical events) and possible actions

Improving Efficiency, Effectiveness, and Usefulness of ATHEANA

- *Comment:* Concerned about resource requirements, consistency, completeness, importance, etc.
  - Process perceived by some to be too "freewheeling" and "open-ended" in places
- *Response:*
  - New process is directed at resolving issues and identifying the problem scenarios
  - The process is more structured by using 4 specific searches with detailed guidance
  - Learning ATHEANA and initial data gathering can demand a significant effort, but analytical process is efficient
  - Computer-based tool would expedite application process

Reviewers' General Opinion of ATHEANA

- Method represented a significant improvement in HRA methodology
  - found to be useful
  - a "good alternative to first-generation HRA approaches"
- However, the method was open-ended and unstructured, and therefore resource-intensive

55

United States
Nuclear Regulatory Commission

Overview of International Human Reliability Analysis Research

Mark Cunningham, Ann Ramey-Smith, Catherine Thompson
Division of Risk Analysis and Applications
Office of Nuclear Regulatory Research

Presentation to ACRS Subcommittee
November 19, 1999

Summary

- Two principal mechanisms for NRC's international cooperation in HRA
  - PWG5
    - Task Group 97-2 project
  - COOPRA working group - impact of organizational influences on risk

Errors of Commission in PSA
PWG5 Task 97-2

Three general goals:

1. To develop insights on errors of commission
2. To apply methods for the quantitative and non-quantitative analysis of errors of commission
3. To identify data needs

Approach:

It was agreed that those countries participating in the task would select an analysis methods of their own choice and apply that method in the analysis of one or more events or cases, also of their own choice. The findings from these analyses would then be shared to permit the development of insights on errors of commission.

PWG5 Task 97-2 (cont.)

Methods applied and/or described in the report:

1. ATHEANA[a], USA
2. ATHEANA, applied by Japan
3. ATHEANA, applied by The Netherlands
4. Borssele PSA, The Netherlands
5. CAHR, Germany
6. CODA, Switzerland
7. FACE, Finland
8. French PSA, France
9. MERMOS, France
10. SHARP, applied by the Czech Republic
11. Input was also provided by the United Kingdom on several analysis methods.

---

[a] Draft NUREG-1624

PWG5 Task 97-2 (cont.)

Some conclusions regarding EOCs:

- Rational identification of EOCs is difficult.
- The structure of current PSA may be too fixed for a full analysis of EOCs.
- The slip/mistake distinction is not very helpful for understanding EOCs.
- Although it may be helpful for communication, the distinction between EOCs and EOOs may not be useful from the point of view of analysis.
- Cognitive dissonance may be a useful psychological concept for the analysis of EOCs.
- Quantification procedures must take into account that EOCs have multiple contributors that are interrelated.
- Crew performance is in most cases a function of procedure adequacy for the situation rather than a function of transient difficulty per se.

Some conclusions regarding EOCs (cont.)

- A strong mismatch between the situation and procedures/training does not necessarily lead to a higher error probability; there is no clear linear relationship. A small (or subtle) mismatch can cause high probability errors.
- Plant modifications can cause subtle interactions and dependencies between systems that can become vulnerable to single human errors.
- Many EOCs have harmless consequences and need not be modeled in PSAs.
- Some EOCs are significant to PSA because they introduce new accident sequences, dependencies, and failure modes.
- It is unclear whether there is a difference in recovery likelihood between EOCs and EOOs.

COOPRA Working Group - Risk Impact of Organizational Influences

Technical Goal of Working Group Activities

Identify the relationships between measurable organizational variables and PRA parameters for the purpose of reducing the uncertainty that exists in PRA due to a lack of knowledge of these relationships.

COOPRA Working Group - Risk Impact of Organizational Influences (continued)

Outcomes of Working Group Technical Activities

Better understanding of the influence of M&O variables on PRA parameters will:

- reduce the uncertainty in risk assessments due to inadequate knowledge of organizational influences on PRA parameters
- provide the basis required to explicitly account for organizational influences in assessments of plant risk
- provide NPP management with the basis for risk-informed assessments of organizational effectiveness and performance, improving their risk management capability
- provide the regulator with the knowledge necessary to assess and predict changes in NPP risk due to organizational influences

COOPRA Working Group - Risk Impact of Organizational Influences (cont.)

Early stage of effort is to develop work plan:

- Exchange background concerning organizational influences, including operating experience and PSA issues
- Define approach to study the issue
  - define and list organizational influences
  - define and list front-line and secondary work processes, including their scope
  - define and list PSA parameters, including scope and level of detail
- Propose model that relates these 3 lists with each other
- Describe process for investigating relationships and conduct case study

Safety Culture

Presentation to Subcommittee on Human Factors

Advisory Committee on Reactor Safeguards

November 19, 1999

J. N. Sorensen

Viewgraphs - Rev. 5a, 11/17/99

Slide 1

Safety Culture

What is it?

Why is it important?

What should the ACRS and NRC do about it?

Slide 2

INSAG-4 Definition of Safety Culture

"Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance."

Universal Features

Policy Level Requirements

Management Requirements

Individual Response

Slide 4

Accidents Involving Organizational Factors

1979 - TMI

1979 - American Airlines - Chicago (271)

1984 - Bhopal (2500)

1986 - Challenger (7)

1986 - Chernobyl (30)

1987 - Herald of Free Enterprise (188)

1988 - Piper Alpha (167)

Slide 5

Nuclear Power Plant Experience
Wolf Creek Blowdown

- Plant initially shut down at 350 psig, 300 F
- Heat removal via RHR system
- 9200 gallon blowdown in 1 minute
- Caused by overlapping activities that created flow path from RCS to RWST

Slide 6

Wolf Creek Blowdown

Failure to Control Work Activities

- Numerous activities in progress
- Work control process placed heavy reliance on control room crew
- Simultaneous performance of incompatible activities
- Mode 5 or 6 was prerequisite for one test (plant was in Mode 4)
- Potential for draindown was identified but not acted upon
- Planning process for retests was not used

Slide 7

Indian Point 2 Trip and Partial Loss of AC Power

- Plant Initially at 99% power
- Unit tripped on spurious overtemperature delta T (OTdT) signal
- Offsite power lost to all vital 480v buses
- One bus remained de-energized for extended period
- Caused eventual loss of 125vdc bus and 120vac instrument bus

Slide 8

Indian Point 2 Trip and Partial Loss of AC Power

- Noise in OTdT channel had not been corrected

- Load tap changer was not in auto

- EDG tripped because of improper setpoint and improper loading sequence

- Post trip activities were not focused on understanding and limiting risk

Slide 9

Validity of Culture as a Concept

- Evolution of Organizational Culture
- Culture vs. Character
- Safety Culture as a Component of Culture

Slide 10

Organizational Culture

Shared values (what is important) and beliefs (how things work) that interact with an organization's structures and control systems to produce behavioral norms (the way we do things around here).

Slide 11

Competing Terms

- Safety Culture
- Organizational Culture
- Management & Organizational Factors
- Safety Climate
- Safety Attitudes
- High Reliability Organizations
- Culture of Reliability

Slide 12

Characteristics of a Safety Culture

- Reporting
- Just
- Flexible
- Learning

(Ref.: Reason, Managing the Risks of Organizational Accidents)

Slide 13

Common Attributes of Safety Culture

- Good Communications
- Senior Management Commitment to Safety
- Good Organizational Learning
- Rewards for Safety Conscious Behavior

Slide 14

Larger Context of Human Factors

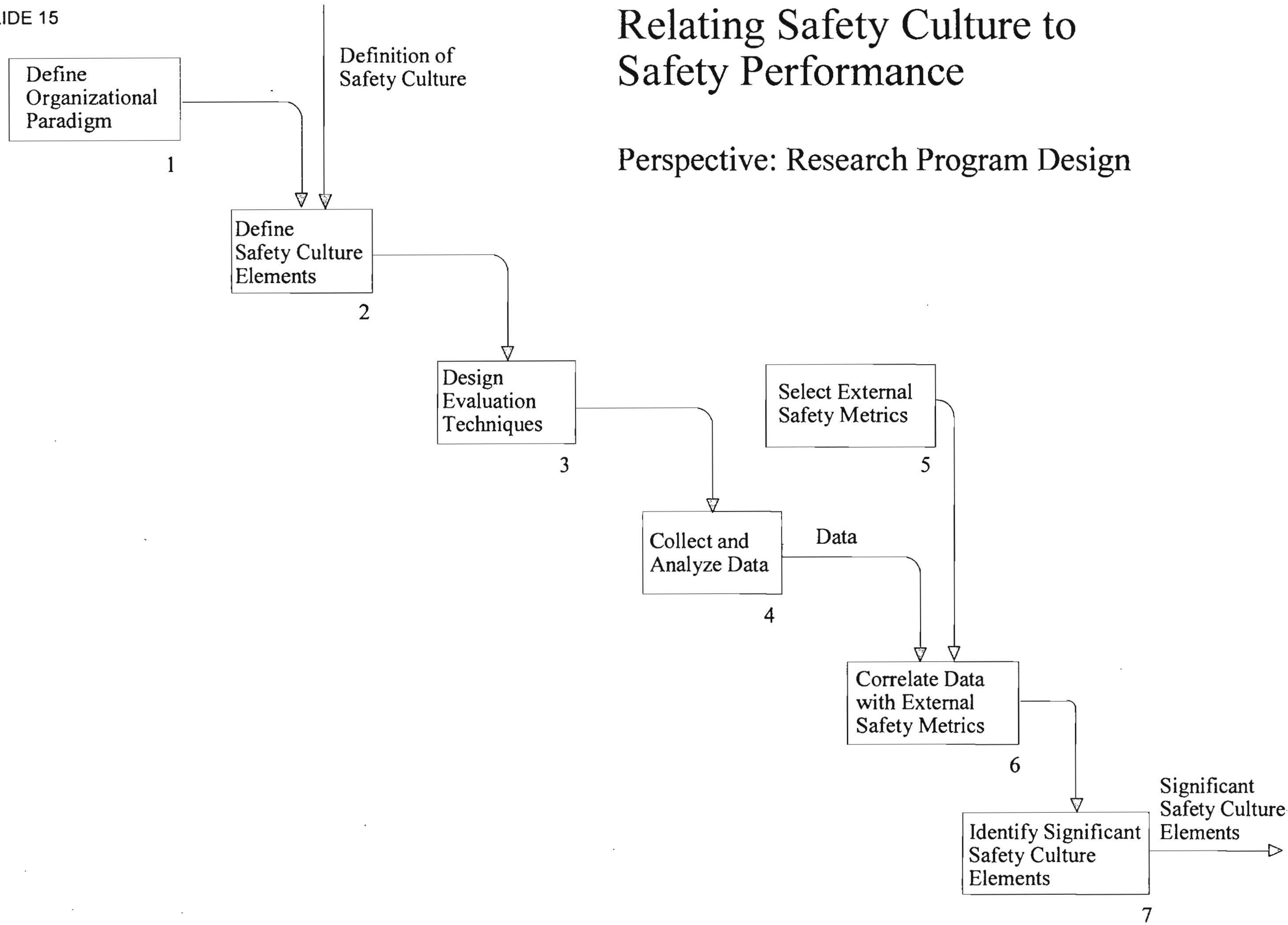
National Research Council Report (1988)

- Human-System Interface
- Personnel Subsystem
- Human Performance
- Management and Organization
- Regulatory Environment

SLIDE 15

Relating Safety Culture to Safety Performance

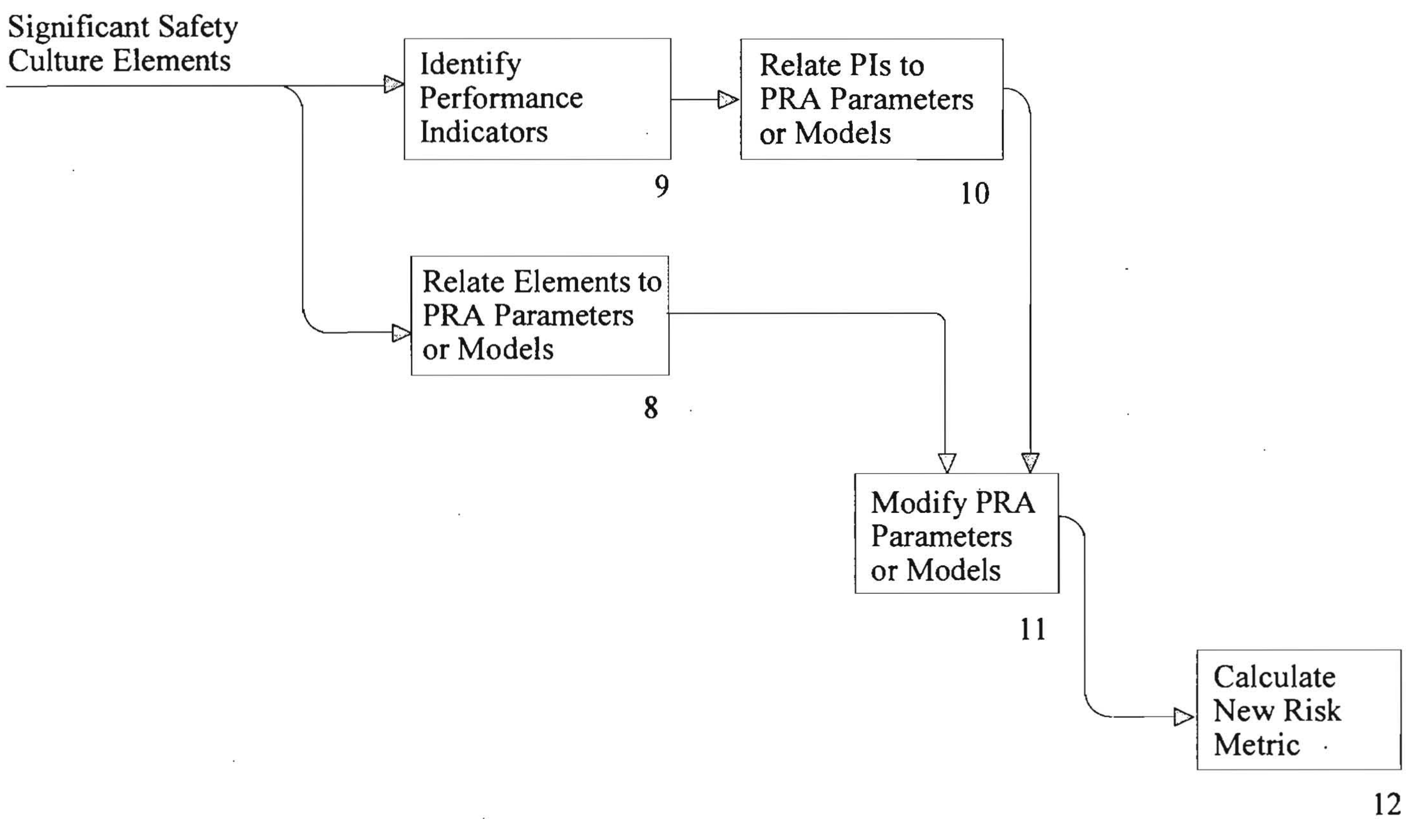
Perspective: Research Program Design



SLIDE 16

Relating Safety Culture to Risk Metrics

Perspective: Research Program Design



Modeling Organizations

- Structure
- Behavior (Attitudes)
- Processes

Slide 18

Example - Structure (Olson, Osborne, et al.)

Environmental Conditions

- General Environment
  - Abundance of resources
  - Amount of volatility
  - Amount of interdependence
- Task Environment
  - Abundance of resources
  - Amount of volatility
  - Amount of interdependence

Contextual Conditions

- Size (staff and budget)
- Technological sophistication
- Technological variability

Organizational Governance

- Traditional, Modern or Federal

Organizational Design

- Mechanistic, Organic or Diverse

Intermediate Outcomes

- Efficiency
- Compliance
- Quality
- Innovation

Slide 19

Example - Process & Behavior (Haber, et al.)

Administrative Knowledge
- Coordination of Work
- Formalization
- Organizational Knowledge
- Roles and responsibilities

Communications
- External
- Interdepartmental
- Intradepartmental

Culture
- Organizational Culture
- Ownership
- Safety Culture
- Time urgency

Decision Making
- Centralization
- Goal Prioritization
- Organizational Learning
- Problem Identification
- Resource Allocation

Human Resource Allocation
- Performance Evaluation
- Personnel Selection
- Technical Knowledge
- Training

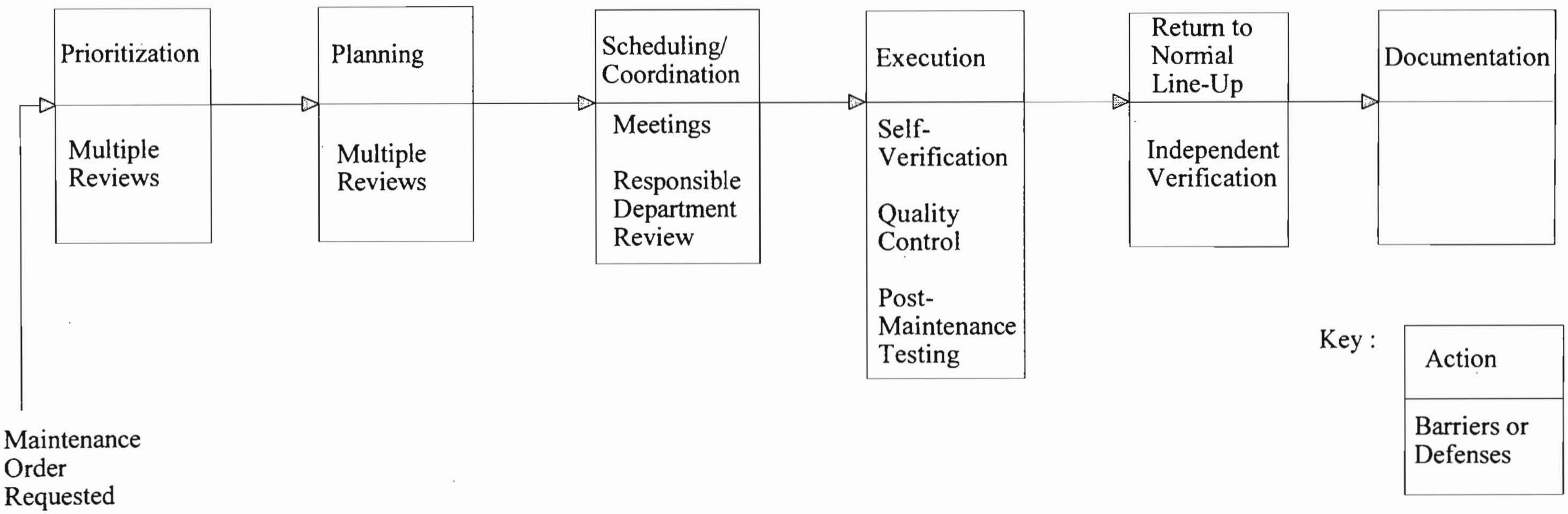
Slide 20

Example - Work Process Analysis Model (Apostolakis, et al.)

- Communications
- Formalization
- Goal Prioritization
- Problem Identification
- Roles and Responsibilities
- Technical Knowledge

Flow Diagram for Corrective Maintenance Work Process

(From Weil & Apostolakis)



85

Slide 22

Measuring Safety Culture

- Document Reviews
- Interviews
- Questionnaires
- Audits
- Performance Indicators

Slide 23

Selecting External Safety Metrics

- Performance Evaluations
- Performance Indicators
- Expert Elicitation
- Accident Rates

Slide 24

Example - Process Industry Audits

Safety Attitudes and Safety Climate

VS

Self Reported Accident Rates and Loss of Containment Accident Rates

Slide 25

Areas of Weakness

How Safety Culture Affects Safety (Mechanism)

Lack of Nuclear Plant Field Data

Lack of Human Performance Indicators

Slide 26

Evidence That Safety Culture Is Important

Consensus of Investigators

Process Industry Accident Rate Data

Preliminary Data from NPP Studies

Slide 27

Research Needs

Field Data for NPP Operations

Mechanism by Which Safety Culture Affects Safety

Safety Culture Performance Indicators

Role of Regulator in Promoting Safety Culture

Knowledge, Skills and Abilities of Front Line Inspectors