PROBABILISTIC RISK ANALYSIS OF NUCLEAR POWER PLANTS: LESSONS AND APPLICATIONS TO PERFORMANCE ASSESSMENT

by F. H. Rowsome

FHR Associates, Inc.

Formerly:

Deputy Director, Division of Risk Analysis, RES
&
Assistant Director for Safety Technology, NRR
U. S. Nuclear Regulatory Commission

ORIGINS OF REACTOR RISK ASSESSMENT:

I. FIRST PROBABILISTIC RISK ASSESSMENT OF NUCLEAR POWER PLANT ACCIDENTS: THE REACTOR SAFETY STUDY, WASH-1400, PREPARED BETWEEN 1972 AND 1975.

II. MOTIVES FOR UNDERTAKING REACTOR RISK ASSESSMENT:

A. PRICE ANDERSON ACT

B. AEC CURIOSITY ABOUT THE RISKS

C. AEC DESIRE TO ELIMINATE EXAGGERATIONS IN AN EARLIER STUDY BOUNDING THE CONSEQUENCES OF REACTOR ACCIDENTS.

III. INVENTION OF THE METHODOLOGY — THE REACTOR SAFETY STUDY GROUP INVENTED REACTOR RISK ASSESSMENT BY COMBINING:

A. A NEW METHOD OF CATALOGING ACCIDENT SEQUENCES ADAPTED FROM DECISION TREE TECHNIQUES.

B. SYSTEM RELIABILITY ANALYSIS TECHNIQUES PIONEERED IN AEROSPACE, DEFENSE, AND ELECTRONICS INDUSTRIES.

C. SIMPLE, REALISTIC MODELS OF THE RELEASES TO BE EXPECTED OF REACTOR ACCIDENTS

D. REALISTIC MODELS OF THE OFFSITE CONSEQUENCES (CASUALTIES, PROPERTY DAMAGE) TO BE EXPECTED OF RELEASES.

E. A SIMPLE MONTE CARLO METHOD FOR PROPAGATING UNCERTAINTY DISTRIBUTIONS THROUGH THE CALCULATIONS.

IV. RECEPTION OF WASH-1400

A. THE AEC REGULATORY STAFF FOUND IT FOREIGN, PROFESSIONALLY THREATENING TO MANY SPECIALISTS, AND AT ODDS WITH THEIR CONVENTIONAL WISDOM: SEVERE ACCIDENTS COULD NOT BE SO LIKELY NOR SO BENIGN AS THE STUDY SUGGESTED: IT WAS DISMISSED AND LICENSING REVIEWS WENT ON AS BEFORE.

B. CRITICS OF NUCLEAR POWER SAW THE VERY LOW LEVELS OF RISK PROJECTED IN WASH-1400 AS DAMAGING TO THEIR CASE; THEY LAUNCHED CAMPAIGNS TO DISCREDIT THE STUDY.

C. THE COMMERCIAL INDUSTRY LIKED THE RESULT: THE RISKS WERE PROJECTED TO BE VERY SLIGHT.

V. RISK ASSESSMENT REVIEW GROUP

A. THE NUMEROUS INQUIRIES INTO THE BIASES AND ACCURACY OF WASH-1400 LED TO THE FORMATION OF A BLUE-RIBBON PANEL, CHAIRED BY HAL LEWIS.

B. THE LEWIS PANEL FOUND THAT:

1. PRA IS AN ESSENTIALLY SOUND METHOD OF NUCLEAR SAFETY ANALYSIS.

2. WASH-1400 UNDERSTATED THE UNCERTAINTIES IN ITS ESTIMATES OF THE RISK.

VI. EFFECT OF THE ACCIDENT AT THREE MILE ISLAND ON REACTOR RISK ASSESSMENT.

A. THE OCCURRENCE OF THE TMI ACCIDENT AND THE ASSESSMENTS THAT FOLLOWED VINDICATED REACTOR RISK ASSESSMENT AND RESCUED IT FROM REGULATORY OBLIVION:

1. THE OCCURRENCE OF SUCH AN ACCIDENT WAS CONSISTENT WITH THE INDUSTRY RISK PROFILE AS ASSESSED IN WASH-1400.

2. MOST FEATURES OF THE ACCIDENT SEQUENCE, CONTRIBUTORY MECHANISMS AND PHENOMENA THAT HAPPENED AT TMI WERE AMONG THOSE MODELED OR PREDICTED IN WASH-1400.

B. PRA GRADUALLY EMERGED THEREAFTER FROM A LOW-BUDGET RESEARCH ACTIVITY OF LITTLE RELEVANCE TO REACTOR SAFETY REGULATION INTO AN IMPORTANT REGULATORY TOOL.

VII. USES OF REACTOR RISK ASSESSMENT WITHIN 5 YEARS OF TMI:

A. 30 PLANT-SPECIFIC NUCLEAR POWER PLANT RISK ASSESSMENTS HAD BEEN DONE, HALF SPONSORED BY THE INDUSTRY, HALF BY THE NRC.

B. NRC APPLICATIONS OF PRA

1. WASH-1400 RESULTS ROUTINELY EMPLOYED TO EVALUATE SEVERE REACTOR ISSUES UNDER NEPA.

2. PRA SUCCESSFULLY USED TO RESOLVE THE ISSUE OF UNDUE RISK FROM PLANTS AT PARTICULARLY HIGH POPULATION DENSITY SITES.

3. SEVERE ACCIDENT POLICY RESEARCHED AND RESOLVED WITH THE AID OF PRA.

4. RISK IMPORTANCE MEASURES DERIVED FROM PRA EMPLOYED IN RESOURCE ALLOCATION IN NRR AND RES.

5. RISK IMPORTANCE MEASURES DERIVED FROM PRA EMPLOYED IN SCREENING NEW SAFETY REQUIREMENTS AND REGULATIONS.

6. "INTEGRATED SAFETY ASSESSMENT PROGRAM," UTILIZING PRA, FOUND TO BE THE MOST SUCCESSFUL METHOD TO ESTABLISH THE SAFETY OF EARLY-LICENSED PLANTS THAT WERE NOT BUILT TO CONTEMPORARY SAFETY STANDARDS.

7. COMMISSION ISSUED SAFETY GOAL POLICY, EXPRESSING GOALS IN TERMS OF COMPARATIVE RISKS.

8. COMMISSION DETERMINED THAT ANY NEW POWER REACTOR LICENSE APPLICATION MUST INCLUDE A PRA, TO SUPPLEMENT DEMONSTRATED COMPLIANCE WITH THE PREVAILING DETERMINISTIC REGULATIONS.

9. MOST GENERIC SAFETY ISSUES CONCERNING REACTORS ARE EXAMINED FOR RISK SIGNIFICANCE

USING PRA METHODS AND INSIGHTS.

C. INDUSTRY APPLICATIONS OF PRA

1. MOST REACTOR VENDORS AND AE'S DEVELOPED PRA CAPABILITIES, AND BEGAN TO USE PRA AS A DESIGN AND LICENSING TOOL.

2. SOME FEW UTILITIES VOLUNTARILY ADOPT PRA AS SAFETY DESIGN AND LICENSING MANAGEMENT TOOLS, WITH VARYING LEVELS OF SUCCESS.

3. INDUSTRY SUPPORT GROUPS (EPRI, NSAC) DEVELOP CENTERS OF EXPERTISE, BENCHMARK EFFORTS, AND METHODOLOGY DEVELOPMENT FOR REACTOR RISK ASSESSMENT.

4. PRA-BASED MEASURES OF IMPORTANCE TO RISK BECOME A ROUTINELY EMPLOYED LANGUAGE IN DIALOGUE ABOUT OVER-REGULATION ON TECHNICAL SAFETY ISSUES.

VIII. DEVELOPMENTS OF THE LAST FIVE YEARS IN THE REGULATORY ROLE OF REACTOR RISK ASSESSMENT.

A. ALL OPERATING NUCLEAR POWER PLANTS MUST USE PRA IN INDIVIDUAL PLANT EVALUATIONS TO FIND AND EVALUATE PLANT-SPECIFIC VULNERABILITIES TO SEVERE ACCIDENTS.

B. PERSPECTIVES DRAWN FROM THESE "IPE"s AND GENERIC RESEARCH ARE TO BE USED TO UPGRADE THE SEVERE ACCIDENT MANAGEMENT PROVISIONS IN DESIGN, OPERATIONAL PROCEDURES AND TRAINING.

C. EFFORTS TO MAKE BETTER CONNECTIONS BETWEEN THE SAFETY ISSUES CENTERED ON MANAGEMENT, INSTITUTIONAL, AND HUMAN FACTORS SAFETY AND REACTOR RISK ASSESSMENT HAVE BORNE LITTLE FRUIT.

D. PRA LITERACY HAS BECOME WIDESPREAD AMONG HEADQUARTERS AND SOME REGIONAL REACTOR REGULATORS.

IX. STRENGTHS AND WEAKNESSES OF REACTOR RISK ASSESSMENT AS A TOOL FOR USE IN SAFETY DESIGN & REGULATION.

A. THE QUANTITATIVE RISK PREDICTIONS PRODUCED BY REACTOR RISK ASSESSMENTS ARE KNOWN TO SUFFER FROM SUBSTANTIAL UNCERTAINTIES:

1. DATA ON THE LIKELIHOOD OF INITIATING EVENTS, CONTRIBUTORY FAILURES AND HUMAN ERRORS HAVE SEVERE STATISTICAL LIMITATIONS, YIELDING VERY IMPRECISE PREDICTIONS OF ACCIDENT SEQUENCE FREQUENCY.

2. THE MODELING OF ACCIDENT PROCESSES AND PHENOMENA MUST EMPLOY MANY SIMPLIFYING APPROXIMATIONS THAT INTRODUCE POSSIBLE BIAS OR ERROR IN PREDICTIONS OF THE COURSE OR CONSEQUENCE OF ACCIDENTS.

3. ANY PRA MAY BE SUBJECT TO

SERIOUS OMISSIONS, E.G., CLASSES OF ACCIDENT SEQUENCES NOT MODELLED AT ALL.

4. DIFFERENT TEAMS OF PRA ANALYSTS MAY COME UP WITH SOMEWHAT DIFFERENT RESULTS FOR THE SAME PLANT, BECAUSE OF THE OTHER SOURCES OF UNCERTAINTY LISTED ABOVE.

   ANALYSTS HAVE RESISTED PROPOSALS TO STANDARDIZE PRA'S BY LIMITING THE ANALYST'S DISCRETION IN THE USE OF MODELING APPROXIMATIONS AND DATA.

B. REACTOR RISK ASSESSMENTS FURNISH UNIQUE INSIGHTS INTO THE SAFETY OF SUBJECT PLANTS. NO OTHER FORM OF SAFETY ANALYSIS APPROACHES ITS SUCCESS RATE FOR UNCOVERING OBSCURE BUT IMPORTANT VULNERABILITIES WARRANTING REGULATORY ATTENTION.

1. PRA'S FURNISH A CATALOG OF SEVERE REACTOR ACCIDENTS TO WHICH THE FACILITY MIGHT BE SUBJECT.

2. PRA'S IDENTIFY THE COMPARATIVE (AND, SUBJECT TO GREATER UNCERTAINTY, THE ABSOLUTE) IMPORTANCE OF ACCIDENT SEQUENCES AND CONTRIBUTORY FAULTS AND PROCESSES.

3. BY REVEALING THE UNDERLYING "WHAT, HOW, AND WHY" OF THE RISK-DOMINANT ACCIDENT VULNERABILITIES OF A PLANT, PRA'S AFFORD MANY INSIGHTS INTO:

   a. HOW TO REDUCE THE RISK POSED BY THE PLANT BY SELECTIVE CHANGES TO DESIGN, OPERATION, SURVEILLANCE AND MAINTENANCE.

   b. HOW TO BETTER TARGET THE NRC'S RULES, REGULATIONS,

AND INSPECTION PRACTICES TO CONTROL RISK.

c. HOW TO VERIFY WHETHER KEY INFERENCES FROM THE PRA ARE RELIABLE OR MERELY ARTIFACTS OF THE APPROXIMATIONS THAT WENT INTO THE PRA. AS A RESULT, MANY OF THESE INSIGHTS ARE VERY MUCH MORE RELIABLE THAN THE BOTTOM LINE RISK PREDICTIONS.

C. PRA'S GIVE MORE AND BETTER INSIGHTS INTO THE IMPORTANCE OF SAFETY ISSUES THAN DO ANY ALTERNATIVE APPROACH TO SAFETY ANALYSIS. BY VIRTUE OF ITS FOCUS ON THE INTEGRAL RISKS, PRA'S ARE SUPERIOR TOOLS FOR ALLOCATING RESOURCES AND PRIORITIES TO AND AMONG SAFETY UPGRADE PROGRAMS:

1. THE NRC STAFF EMPLOYS PRA INSIGHTS IN ALLOCATING RESOURCES TO ISSUE RESOLUTION, RESEARCH, AND STANDARDS

DEVELOPMENT.

2. UTILITIES USE PRA INSIGHTS TO PRIORITIZE PLANT UPGRADES, ETC.

3. PLANT DESIGNERS FIND PRA TO BE AN OUTSTANDING TOOL TO AID IN SAFETY DESIGN DECISION-MAKING FROM CONCEPTUAL DESIGN ON THROUGH CONSTRUCTION AND STARTUP.

4. PRA METHODS LEND THEMSELVES TO COST/BENEFIT ANALYSIS, VALUE ENGINEERING, ETC., WHEN DESIRED.

5. PRA METHODS ARE EFFECTIVE IN REVEALING THE ATTENDANT RISKS OR COMPETING RISK ISSUES SURROUNDING PROPOSED CHANGES IN REACTOR DESIGN OR OPERATION.

D. THE USE OF PRA IN REACTOR SAFETY REGULATION HAS FACED ADJUDICATORY

TESTS BEFORE THE ASLB IN SEVERAL CONTEXTS:

1. SEVERE ACCIDENT CONSIDERATIONS UNDER NEPA,

2. INDIAN POINT SPECIAL PROCEEDING,

3. LICENSING OF PLANTS AT HIGH POPULATION DENSITY SITES: LIMERIC & MILLSTONE UNIT 3.

ALTHOUGH PRA IS KNOWN TO BE SUBJECT TO LARGE QUANTITATIVE UNCERTAINTIES AND THUS THOUGHT TO BE VULNERABLE IN A JUDICIAL CONTEXT, PRA HAS NEVER FAILED TO SUPPORT THE REGULATORY ROLE ASSIGNED TO IT BY THE COMMISSION IN A HEARING ARENA.

E. HEARING EXPERIENCE SUGGESTS THAT PRA CREDIBILITY RESTS IN:

1. MATURE, TECHNICALLY EXPERT TESTIMONY AND WITNESSES.

2. FORTHRIGHT ACKNOWLEDGEMENT OF THE UNCERTAINTIES INVOLVED.

3. DIVERSE AND REDUNDANT DECISION LOGICS OR PERSPECTIVES SO THAT DECISIONS ARE CLEARLY NOT UNDULY DEPENDENT UPON ONE OR A FEW UNCERTAIN TESTS OF COMPLIANCE.

4. DEMONSTRATED NRC STAFF WILLINGNESS TO REFUSE A LICENSE, IMPOSE LICENSE

CONDITIONS, OR SHUT DOWN AN UNSAFE FACILITY.

5. CONSISTENT FOCUS ON THE BIG PICTURE, AND CARE TO PUT INTO CONTEXT THE CONTROVERSIES ON TRIVIA THAT DO NOT SIGNIFICANTLY INFLUENCE THE OVERALL SAFETY OF PROFILE OF THE FACILITY.

X. NRC VIEWS OF RISK-BASED LICENSING AND SAFETY GOALS.

A. THE MANY ADVANTAGES OF PRA ARE SUCH THAT THE COMMISSION ALMOST ALWAYS WANTS THE BENEFIT OF PRA-BASED PERSPECTIVES ON ANY MAJOR NUCLEAR SAFETY REGULATORY DECISION.

B. THE NRC HAS CONSIDERED AND REJECTED USING PRA AS A CENTERPIECE OF LICENSING DECISION MAKING IN THE FOLLOWING WAY:

1. ESTABLISH THRESHOLDS OF ACCEPTABLE RISK THROUGH POLICY

OR RULEMAKING.

2. EMPLOY PRA RISK PREDICTIONS TO MEASURE COMPLIANCE OF INDIVIDUAL LICENSE APPLICANTS.

THIS APPROACH HAS BEEN REJECTED PRIMARILY BECAUSE IT IS FAR TOO VULNERABLE TO THE BROAD UNCERTAINTIES AND POOR QUANTITATIVE REPEATABILITY OF THE BOTTOM LINE RISK PREDICTIONS OF PRA'S.

IN ADDITION, THRESHOLDS OF ACCEPTABLE RISK FAIL TO ADDRESS THE PROBLEM OF ALLOCATION: HOW DO YOU INFER STANDARDS OF, E.G., OPERATOR TRAINING OR SEISMIC DESIGN MARGINS FROM AN INTEGRAL STANDARD OF ACCEPTABLE RISK?

C. THE NRC HAS ISSUED A SAFETY GOAL POLICY, BUT ITS USE IS RESTRICTED TO THE REGULATORY BACKGROUND, E.G., STANDARDS DEVELOPMENT, NOT CASEWORK REGULATION.

XI. PRA HAS BEEN FOUND TO BE AN OUTSTANDING DESIGN TOOL.

A. EVEN IN CONCEPTUAL DESIGN, DESPITE LITTLE QUANTITATIVE PRECISION, THE PICTURE OF SEVERE ACCIDENT VULNERABILITIES PRODUCED BY PRA MODELS FURNISHES VERY USEFUL INSIGHTS INTO CONCEPTUAL DESIGN TRADEOFFS.

B. IN DETAILED DESIGN AND PROCUREMENT, THE PARALLEL DEVELOPMENT AND USE OF PRA MODELS AS DESIGN DECISIONS ARE MADE FURNISH USEFUL FEEDBACK ON DESIGN OPTIONS AND AN EFFECTIVE MULTI-DISCIPLINARY DESIGN REVIEW TOOL.

C. IN SITE CHARACTERIZATION AND DETAILED DESIGN OF ANY PROPOSED REPOSITORY, THE PARALLEL DEVELOPMENT AND USE OF PERFORMANCE ASSESSMENT MODELS SHOULD FURNISH VERY USEFUL INSIGHTS TO EVALUATE AND FOCUS ATTENTION ON DEVELOPING DESIGN AND SITE RESEARCH ISSUES.

XII. PARADIGMS FOR RESPONSIBLE USE OF PRA, DRAWN FROM THE NUCLEAR POWER PLANT EXPERIENCE.

A. PRA SHOULD BE USED BY THOSE RESPONSIBLE FOR THE DEVELOPMENT, DESIGN AND OPERATION OF A NUCLEAR FACILITY TO IDENTIFY SUBTLE VULNERABILITIES, DEBUG AND REFINE SAFETY DESIGN AND OPERATIONAL PRACTICES, FOCUS SAFETY RESEARCH, AND GUIDE IN THE ALLOCATION OF RESOURCES. [THE NRC EXPECTS THIS OF NEW APPLICANTS FOR NUCLEAR POWER PLANT LICENSES, AND — INCREASINGLY — OF LICENSE HOLDERS.]

EVEN IF PERFORMANCE ASSESSMENT DID NOT HOLD THE PROMINENT PLACE IT DOES IN 40 CFR 191 AND 10 CFR 60, REACTOR EXPERIENCE SUGGESTS THAT IT SHOULD BE ONE OF THE - IF NOT THE - PRINCIPAL METHODS TO EVALUATE AND DIRECT THE INVESTIGATIONS OF SITE CHARACTERIZATION, ETC.

B. PRA MAY BE USED AS A SUPPLEMENT TO DETERMINISTIC SAFETY REGULATIONS — WHICH REMAIN THE PRIMARY BASIS FOR REACTOR LICENSING — TO CATCH SAFETY PROBLEMS THAT MIGHT OTHERWISE BE MISSED IN REGULATORY REVIEWS, EVALUATE APPLICATIONS FOR EXEMPTIONS FROM THE REGULATIONS, AID IN THE CALIBRATION OF THE STRINGENCY AND FOCUS OF THE REGULATIONS, AND TO APPORTION RESOURCES TO ENFORCEMENT. [THE NRC DOES THIS WITH REACTOR REGULATION.]

C. PRA MIGHT BE MOVED TO CENTER STAGE IN LICENSING DECISION-MAKING, PROVIDED CHECKS AND BALANCES ARE FURNISHED TO KEEP THE PROCESS FROM BEING TOO VULNERABLE TO PRA UNCERTAINTIES.

AMONG THE WAYS THESE CHECKS AND BALANCES MIGHT BE STRUCTURED ARE:

1. DEFENSE-IN-DEPTH: DETERMINISTIC AND/OR

RELIABILITY PERFORMANCE CRITERIA MIGHT BE SET FOR INDIVIDUAL, INDEPENDENT LAYERS OF SAFETY FUNCTIONS. [10 CFR 60 IS AN EARLY EXAMPLE.]

2. USE OF INDEPENDENT, DIVERSE AND REDUNDANT LICENSING DECISION INDICATORS, PERHAPS WITH A "PREPONDERANCE OF EVIDENCE" OR "N OUT OF M" OVERALL DECISION LOGIC.

   EXAMPLES OF DIVERSE LICENSING DECISION INDICATORS:

   a. ESTABLISH A HIGH LEVEL OF CONFIDENCE THAT THE RISKS ARE NOT COMMANDINGLY HIGH, AND A MODERATE CONFIDENCE THAT THE RISKS ARE NOT MORE THAN MODERATE, AND LOW CONFIDENCE THAT THE RISKS ARE VERY SMALL. [GIVEN THE BROAD UNCERTAINTIES IN NUCLEAR RISK ASSESSMENT, SUCH EVALUATIONS MIGHT BE QUITE DISTINCT AND

INDEPENDENT, THOUGH ONLY IF THE CRITERIA ARE MORE DISTINCT THAN THE TWO PROBABILISTIC STANDARDS USING THE TABLE OF SOURCE TERMS IN THE 40 CFR 191.]

b. DEVELOP DIVERSE WAYS OF ASSESSING THE COMPARATIVE IMPORTANCE OF THE FACILITY RISKS COMPARED WITH ALTERNATIVE AND COMPETING RISKS.

c. SUPPLEMENT THE PRIMARY PROBABILISTIC CRITERIA WITH DETERMINISTIC LICENSING CRITERIA.