Probabilistic Safety Assessment in the Chemical and Nuclear Industries

Ralph R. Fullwood
Probabilistic Safety Assessment in the Chemical and Nuclear Industries

Ralph R. Fullwood
Disclaimer

The information in this book is collected from published and unpublished literature. Responsibility for the accuracy of this material is disclaimed, however, responsibility is accepted for the selection, organization, and presentation. The vastness of the information necessitates selectivity in the attempt to make a comprehensive and cohesive presentation. The material is selected to illustrate a procedure or principle not advocacy. Every effort toward objectivity was made to balance human health and safety, environment, economic welfare, and civilization.

Neither I, Brookhaven National Laboratory from which I am retired, nor the publisher are responsible for the materials presented here.

RALPH R. FULLWOOD

Upton, NY
October 1998
## Contents

Chapter 1  Protecting the Public Health and Safety ................................................................. 1
  1.1 Historical Review ................................................................. 1
    1.1.1 Beginnings ............................................................... 1
    1.1.2 Industrial Revolution ................................................. 2
    1.1.3 This Century ............................................................ 3
  1.2 Risk Assessment Objectives .................................................. 5
  1.3 Risk, Hazard, and other Terms ............................................ 6
  1.4 Quantitative Aspects of Risk ................................................ 6
    1.4.1 Actuarial or Linear Risk ............................................ 6
    1.4.2 Shortcomings of Linear Risk ....................................... 7
    1.4.3 Presentation of Risk ................................................ 8
    1.4.4 Public Perception of Risk ......................................... 12
  1.5 Safety Goals ................................................................. 13
  1.6 Emergency Planning Zones ................................................ 15
  1.7 Use of PSA by Government and Industry .................................. 17
  1.8 Regulation of Nuclear Power ............................................... 18
    1.8.1 Regulations ........................................................... 18
    1.8.2 Regulatory Structure ............................................... 18
    1.8.3 Licensing Process ................................................ 19
    1.8.4 Public Participation ............................................... 20
    1.8.5 Advisory Committee on Reactor Safety (ACRS) ................. 20
    1.8.6 Inspection .......................................................... 21
    1.8.7 Decommissioning ................................................... 21
    1.8.8 Accident Severity Criteria ....................................... 21
    1.8.9 PSA Requirements ................................................ 22
  1.9 Regulation of Chemical Processing and Wastes ......................... 22
    1.9.1 Environmental Law ................................................ 22
    1.9.2 Occupational Risk Protection: the PSM Rule ................. 27
  1.10 Summary ................................................................. 33
  1.11 Problems ................................................................. 34

Chapter 2  Mathematics for Probabilistic Safety ............................................................... 35
  2.1 Boolean Algebra ............................................................ 35
  2.2 Venn Diagram and Mincuts ................................................ 37
  2.3 Probability and Frequency ................................................ 39
  2.4 Combining Probabilities ................................................ 41
    2.4.1 Intersection or Multiplication .................................. 41
    2.4.2 Union or Addition ................................................ 41
    2.4.3 M-Out-of-N-Combinations ....................................... 42
  2.5 Distributions ............................................................. 42
    2.5.1 Discrete Distributions ............................................ 43
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3 Database Preparation</td>
<td>160</td>
</tr>
<tr>
<td>4.3.1 How to Estimate Failure Rates</td>
<td>160</td>
</tr>
<tr>
<td>4.3.2 Making a Database</td>
<td>160</td>
</tr>
<tr>
<td>4.3.3 Test Reports and Procedures</td>
<td>161</td>
</tr>
<tr>
<td>4.3.4 Maintenance Reports</td>
<td>162</td>
</tr>
<tr>
<td>4.3.5 Operating Procedures</td>
<td>162</td>
</tr>
<tr>
<td>4.3.6 Control Room Log</td>
<td>162</td>
</tr>
<tr>
<td>4.3.7 Information Flow in Plant Data Collecting</td>
<td>163</td>
</tr>
<tr>
<td>4.3.8 Data Sources Used in Past PSAs</td>
<td>163</td>
</tr>
<tr>
<td>4.4 Human Reliability Analysis</td>
<td>163</td>
</tr>
<tr>
<td>4.4.1 Human Error in System Accidents</td>
<td>163</td>
</tr>
<tr>
<td>4.4.2 Lack of Human Error Considerations</td>
<td>166</td>
</tr>
<tr>
<td>4.4.3 Cases Involving Human Error</td>
<td>168</td>
</tr>
<tr>
<td>4.5 Incorporating Human Reliability into a PSA</td>
<td>173</td>
</tr>
<tr>
<td>4.5.1 Human Reliability Analysis Models</td>
<td>173</td>
</tr>
<tr>
<td>4.5.2 Quantifying Human Error Probabilities (HEPs)</td>
<td>175</td>
</tr>
<tr>
<td>4.5.3 Human Factors Data</td>
<td>179</td>
</tr>
<tr>
<td>4.5.4 Example of Human Error Analysis</td>
<td>180</td>
</tr>
<tr>
<td>4.5.5 HRA Event Tree (NUREG/CR-1278)</td>
<td>181</td>
</tr>
<tr>
<td>4.5.6 Comparison of Human Factors in PSAs</td>
<td>183</td>
</tr>
<tr>
<td>4.7 Summary</td>
<td>184</td>
</tr>
<tr>
<td>4.8 Problems</td>
<td>184</td>
</tr>
</tbody>
</table>

Chapter 5 External Events

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Seismic Events</td>
<td>185</td>
</tr>
<tr>
<td>5.1.1 Overview</td>
<td>185</td>
</tr>
<tr>
<td>5.1.2 Richter Magnitude - Frequency of Occurrence Distribution</td>
<td>188</td>
</tr>
<tr>
<td>5.1.3 Ground Coupling with Attenuation</td>
<td>190</td>
</tr>
<tr>
<td>5.1.4 Shaking Model of the Plant</td>
<td>190</td>
</tr>
<tr>
<td>5.1.5 Fragility Curves</td>
<td>192</td>
</tr>
<tr>
<td>5.1.6 System Analysis</td>
<td>194</td>
</tr>
<tr>
<td>5.2 Fires</td>
<td>195</td>
</tr>
<tr>
<td>5.2.1 Introduction</td>
<td>195</td>
</tr>
<tr>
<td>5.2.2 Procedures for Fire Analysis</td>
<td>196</td>
</tr>
<tr>
<td>5.2.3 Screening Analysis</td>
<td>197</td>
</tr>
<tr>
<td>5.2.4 Fire Frequencies</td>
<td>197</td>
</tr>
<tr>
<td>5.2.5 Fire Growth Modeling</td>
<td>198</td>
</tr>
<tr>
<td>5.2.6 Fragility Curves</td>
<td>199</td>
</tr>
<tr>
<td>5.2.7 Systems Analysis</td>
<td>199</td>
</tr>
<tr>
<td>5.3 Flood</td>
<td>200</td>
</tr>
<tr>
<td>5.3.1 Overview of Internal Flooding</td>
<td>200</td>
</tr>
<tr>
<td>5.3.2 Internal Flooding Incidents</td>
<td>200</td>
</tr>
<tr>
<td>5.3.3 Internal Flood Modeling</td>
<td>202</td>
</tr>
</tbody>
</table>
5.3.4 External Flooding .......................................... 203
5.4 Summary ......................................................... 204

Chapter 6 Analyzing Nuclear Reactor Safety Systems ...................... 205

6.1 Nuclear Power Reactors ............................................. 205
  6.1.1 U.S. Light Water Reactors .................................... 206
  6.1.2 Pressurized Water Reactors ................................ 208
  6.1.3 Boiling Water Reactors ...................................... 211
  6.1.4 Advanced Light Water Reactors ................................ 213
6.2 TMI-2 and Chernobyl Accidents ....................................... 221
  6.2.1 The TMI-2 Accident ......................................... 221
  6.2.2 The Chernobyl Accident ...................................... 223
6.3 Preparing a Nuclear Power Plant PSA .................................. 227
  6.3.1 Overview of the Probabilistic Safety Process Using Event Trees ....... 228
  6.3.2 Preparing for the PSA ........................................ 228
  6.3.3 PSA Construction ........................................... 236
6.4 Example: Analyzing an Emergency Electric Power System .................. 238
  6.4.1 The Problem: Emergency Electric Power ......................... 239
  6.4.2 Overview of FTAPSUIT ...................................... 239
6.5 Summary ......................................................... 243
6.6 Problems ......................................................... 243

Chapter 7 Analyzing Chemical Process Safety Systems .............................. 245

7.1 Chemical Process Accidents ........................................... 245
  7.1.1 The Nature of Process Accidents ................................ 245
  7.1.2 Some Deadly and Severe Chemical Accidents ..................... 247
7.2 Chemical Processes ................................................. 261
  7.2.1 The Topography of Chemical Processes ......................... 261
  7.2.2 Inorganic Chemicals ........................................ 262
  7.2.3 Fertilizer Production ....................................... 264
  7.2.4 Halogens and Their Compounds ................................ 266
  7.2.5 Organic Chemicals .......................................... 269
  7.2.6 Explosives ................................................ 272
  7.2.7 Plastics and Resins ........................................ 276
  7.2.8 Paints and Varnishes ........................................ 283
  7.2.9 Petrochemical Processing ..................................... 286
7.3 Chemical Process Accident Analysis .................................... 293
  7.3.1 Scoping Analysis ............................................ 295
  7.3.2 Performing a Detailed Probabilistic Safety Analysis ............... 299
7.4 Example: Analyzing a Chemical Tank Rupture ........................... 304
  7.4.1 Defining the Problem with Fault Tree Analysis .................. 304
  7.4.2 Applying FTAPSUIT to Chemical Process Tank Rupture .......... 305
7.5 Summary ......................................................... 307
List of Figures

1.4.2-1 Curve Enveloping Accident Data and a Linear Envelope for a Looser Straight-Line Bound ................................................................. 7
1.4.2-2 Exceedance Probability (accidents 1-6) and composite envelope ................... 8
1.4.3-1 Fatality Frequency for Man-Caused Events (from WASH-1400) ...................... 9
1.4.3-2 Confidence Intervals: CCDF for Latent Cancer Fatalities Internal and External Seismicity .............................................................. 10
1.4.3-3 Latent Cancer Risk at Indian Point site if the Reactor were one of the five types shown 10
1.4.3-4 Early fatality risk if the Indian Point Plant had been at one of these sites .......... 10
1.4.3-5 Risk compared as volumes or masses .............................................. 11
1.4.3-6 Relative contributions to the Zion and ANO-1 core melt frequencies ............ 12
1.4.4-1 Revealed and risk-benefit relationships ........................................ 13
2.2-1 Venn diagram of two sets .................................................................. 37
2.2-2 Mincut Explanation by Venn Diagrams .............................................. 39
2.3-1 Probability of Scores in Craps .............................................................. 40
2.4-1 Venn Diagram of Sets A and B ............................................................... 41
2.5-1 The discrete distribution of probability of crap scores has impressed on it a continuous distribution with quite a different meaning .......................... 43
2.5-2 Conceptual Life-Cycle of a Component ................................................ 46
2.5-3 Transitions between States ................................................................. 48
2.7-1 ERMA simulation of a low pressure coolant injection system ......................... 59
2.7-2 Histogram of probability distribution generated by Monte Carlo simulation .... 60
2.8-1 Risk worth ratios with respect to core melt for Sequoyah safety systems ....... 65
2.8-2 Risk worth ratios with respect to core melt for Oconee safety systems ......... 65
2.10-1 Control Rod Pattern ............................................................... 66
3.1.3-1 Example of a Block Flow Diagram .................................................. 68
3.1.3-2 Process Flow Diagram ................................................................. 69
3.3.1-1 Hydrogen Fluoride Supply System .............................................. 76
3.3.1-2 Cooling Tower Water ................................................................. 77
3.3.4-1 The HAZOP Process ................................................................. 88
3.4.1-1 Illustrative Cooling Systems ........................................................... 98
3.4.3-1 Reliability Block Diagram of Figure 3.4.1-1 ..................................... 100

The first number is the chapter number, the second number is the section number and the third number (if present) is the subsection number. The number after the dash is the figure number.
3.4.4-1 Symbols of Fault Tree Analysis .............................................. 101
3.4.4-2 Sketch of an Internal Combustion Engine .................................. 102
3.4.4-3 Fault Tree of Engine ............................................................. 103
3.4.4-4 Example Fault Tree ............................................................... 104
3.4.4-5 Mincut Fault Tree of Figure 3.4.4-4 ......................................... 105
3.4.4-6 Simple injection system .......................................................... 109
3.4.4-7 Failure to Inject Fault Tree ..................................................... 109
3.4.4-8 Boolean Reduction of "Failure to Inject Fault Tree" ....................... 109
3.4.4-9 Fault Tree from the Mincut Representation of Figure 3.4.4-8 Fault Tree 110
3.4.4-10 Success Tree Transformation of Figure 3.4.4-9 Fault Tree .................. 110
3.4.5-1 Event Tree Scenario Depiction ................................................. 111
3.4.5-2 Large LOCA as a Function Event Tree .................................... 113
3.4.5-3 Fault Trees at the Nodes of an Event Trees to Determine the Probability 114
3.4.5-4 Large LOCA as a System Event Tree ...................................... 115
3.4.5-5 Large LOCA Event Tree in the LESF style .................................. 116
3.4.5-6 Containment Event Tree .......................................................... 119
3.5.7-1 Fault Tree diagram of the emergency electric power system .............. 127
3.6-1 The Saphire Main Menu and the Fault Tree Editor Menu ....................... 139
3.7-1 Fault Tree of a doubly redundant ECCS ..................................... 148
3.7-2 Time-sequential testing ............................................................. 149
3.7-3 Staggered testing ........................................................................ 149
4.3-1 Plant Data Processing for PSA ..................................................... 163
4.4-1 Releases based on plant status ..................................................... 165
4.4-2 Releases based on cause code ...................................................... 165
4.4-1 Venn Diagram of Error Cause ..................................................... 167
4.5-1 Phases of Human Reliability Analysis ........................................ 172
4.5-2 General incorporation of HRA into the PSA process ........................ 174
4.5-3 Failure vs Problem-Solving Time .................................................. 180
4.5-4 HRA Event Tree ........................................................................ 180
4.5-5 HRA Event Tree for Actions Outside the Control Room .................... 181
4.5-6 Example of Spread in HEPs from IPE for BWRs .............................. 183
5.1-1 Procedures for Analyzing External Events ..................................... 187
5.1-2 Comparison of the world frequency-magnitude shape with data from the CMMG 189
5.1-3 Seismic hazard curves for a hypothetical site .................................. 191
5.1-4 Plan view of nuclear steam supply system ..................................... 191
5.1-5 Nodal diagram of a nuclear steam supply system .............................. 191
5.1-6 Large LOCA Seismic Event Tree for a PWR .................................. 195
5.3.1 Fault Tree Identification of Flood-Critical Equipment ...................... 202
5.3-2 Flood data plotted lognormally .................................................... 204
6.1-1 Sketch of a Pressurized Water Reactor (PWR) ................................ 207
6.1-2 Sketch of a Boiling Water Reactor (BWR) .................................... 212
6.1-3 The In-Containment Passive Safety Injection System .......................... 215
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1-4 AP500 Passively Cooled containment</td>
<td>216</td>
</tr>
<tr>
<td>6.1-5 Sketch of the PIUS Principle</td>
<td>218</td>
</tr>
<tr>
<td>6.1-6 SWBR LOCA Response</td>
<td>219</td>
</tr>
<tr>
<td>6.2-1 The Damaged TMI-2 Core</td>
<td>221</td>
</tr>
<tr>
<td>6.2-2 Schematic of the RBMK-1000</td>
<td>224</td>
</tr>
<tr>
<td>6.3-1 Overview of the PSA process</td>
<td>227</td>
</tr>
<tr>
<td>6.3-2 Possible PSA Organization Chart</td>
<td>229</td>
</tr>
<tr>
<td>6.3-3 Core Damage Master Logic Diagrams for Indian Point 2 and 3 Nuclear Power Stations</td>
<td>233</td>
</tr>
<tr>
<td>6.3-4 Organizing the Analysis via Event Tree</td>
<td>236</td>
</tr>
<tr>
<td>6.3-5 Relative core melt contributions</td>
<td>238</td>
</tr>
<tr>
<td>6.4-1 Emergency Electric Power</td>
<td>238</td>
</tr>
<tr>
<td>6.4-2 Procedure for Using FTAPSUIT</td>
<td>240</td>
</tr>
<tr>
<td>6.4-3 Menu for FTAPSUIT</td>
<td>241</td>
</tr>
<tr>
<td>6.4-4 FTAPlus Menu</td>
<td>241</td>
</tr>
<tr>
<td>6.4-5 Post Processor Menu</td>
<td>241</td>
</tr>
<tr>
<td>7.1-1 Increasing Cost of Process Accidents per 4 Year Period</td>
<td>246</td>
</tr>
<tr>
<td>7.1-2 Average Loss by Type of Plant</td>
<td>246</td>
</tr>
<tr>
<td>7.1-3 Average Loss by Loss Mechanism</td>
<td>246</td>
</tr>
<tr>
<td>7.1-4 Average Loss by Loss Cause</td>
<td>246</td>
</tr>
<tr>
<td>7.1-5 Average Loss by Type of Equipment</td>
<td>246</td>
</tr>
<tr>
<td>7.1-6 Temporary Repair at Flixborough</td>
<td>250</td>
</tr>
<tr>
<td>7.1-7 Common Headers to the MIC Storage Tanks at Bhopal</td>
<td>252</td>
</tr>
<tr>
<td>7.1-8 MIC Storage Tank</td>
<td>253</td>
</tr>
<tr>
<td>7.2-1 Fertilizers and Uses</td>
<td>264</td>
</tr>
<tr>
<td>7.2-2 Uses for Benzene</td>
<td>269</td>
</tr>
<tr>
<td>7.2-3 Unsaturated Hydrocarbons from Petroleum</td>
<td>270</td>
</tr>
<tr>
<td>7.2-4 Diagram of a Fractional Distillation Column</td>
<td>287</td>
</tr>
<tr>
<td>7.2-5 Schematic of a Catalytic Cracking Unit</td>
<td>289</td>
</tr>
<tr>
<td>7.3-1 Process Scoping Steps</td>
<td>296</td>
</tr>
<tr>
<td>7.3-2 A Detailed PSA</td>
<td>299</td>
</tr>
<tr>
<td>7.4-1 Fault Tree for Tank Rupture</td>
<td>304</td>
</tr>
<tr>
<td>7.4-2 FTAP Input file</td>
<td>305</td>
</tr>
<tr>
<td>7.4-3 FTAP Punch output</td>
<td>305</td>
</tr>
<tr>
<td>7.4-4 Appearance of File</td>
<td>305</td>
</tr>
<tr>
<td>7.4-5 Edited Output of IMPORTANCE</td>
<td>306</td>
</tr>
<tr>
<td>7.4-6 Monte Carlo Calculation of the Chemical Process Tank Rupture</td>
<td>307</td>
</tr>
<tr>
<td>8.1-1 Decay Heat from a 3000 MWe Core</td>
<td>310</td>
</tr>
<tr>
<td>8.1-2 Total heat evolved from fuel and absorbed by concrete</td>
<td>310</td>
</tr>
<tr>
<td>8.1-3a Molten droplets and rivulets begin to flow downward</td>
<td>311</td>
</tr>
<tr>
<td>8.1-3b Formation of a local blockage in colder rod regions</td>
<td>311</td>
</tr>
<tr>
<td>8.1-3c Formation of the molten pool</td>
<td>312</td>
</tr>
<tr>
<td>8.1-3d Radial and axial growth of the molten pool</td>
<td>312</td>
</tr>
</tbody>
</table>
List of Tables

1.4.3-1 Illustrative Cutset Listing ................................................. 9
1.4.3-2 Expected Annual Consequences (risk) from Five LWR Designs if Sited at Indian Point ........................................................... 11
1.4.3-3 Estimated Frequencies of Severe Core Damage ............................... 11
1.6-1 Chronology of Federal Emergency Regulations ........................................ 15
1.6-2 Emergency Action Levels and Responses ............................................. 17
1.8-1 Some Federal Regulations Governing the Environment .......................... 18
1.9-1 List of Highly-Hazardous Chemicals, Toxics, and Reactives (Mandatory) ............ 28
2.1-1 Comparison of Ordinary and Boolean Algebra ........................................ 36
2.5-1 Values of the Inverse Cumulative Chi-Squared Distribution in terms of percentage confidence with M failures ............................................. 47
2.5-2 Mean Variance and Moment-Generating Functions for Several Distributions 49
2.6-1 Bayes Conjugate Self-Replication ............................................... 52
2.6-2 Effect of Bayes Conjugation on a Gamma Prior ................................ 52
2.8-1 Relationships between Importance Measures ..................................... 64
3.3.1-1 Possible Checklist Main Headings ........................................... 77
3.3.1-2 Possible Headings and Subheadings ........................................... 78
3.3.1-3 Simplified Process Hazards Analysis Checklist ................................ 79
3.3.1-4 Checklist Analysis of Dock 8 HF Supply ................................ 80
3.3.1-5 Checklist of Cooling Tower Chlorination .................................. 80
3.3.1-6 Estimated Time for a Checklist ............................................... 81
3.3.2-1 What-If Analysis of Dock 8 HF Supply System ................................ 82
3.3.2-2 What-If Analysis of the Cooling Tower Chlorination System .............. 83
3.3.2-3 Estimated Time for a What-If .............................................. 84
3.3.3-1 Estimated Time for a What-If/Checklist ........................................ 85
3.3.3-2 What-If/Checklist Analysis of Dock 8 HF Supply System .................. 85
3.3.3-3 What-If/Checklist Analysis of Cooling Tower Chlorination System ........ 85
3.3.4-1 Guide Words for HAZOP ..................................................... 90
3.3.4-2 HAZOP Process Parameters and Deviations .................................. 91
3.3.4-3 HAZOP of the Cooling Tower Chlorination System ............................ 92

b The first number is the chapter number, the second number is the section number and the third number (if present) is the subsection number. The number after the dash is the figure number.
Foreword

The last three decades have seen the development of a new science to help us better understand the risk of events about which there is often very little information. The reason there is interest in such a science is that there are a great many societal benefits from activities that involve risk; risk that if properly managed through better understanding can greatly benefit the quality of all life on the planet earth, both plant and animal. That science is quantitative risk assessment, also known by such names as probabilistic risk assessment and probabilistic safety assessment, the latter being the preferred name for this text. Probabilistic safety assessment divides the risk question into three questions "What can go wrong?" "How likely is it?" and "What are the consequences?"

Probabilistic safety assessment has had its greatest push in relation to the assessment of risk associated with nuclear power plant operation as documented in the author's previous book. This new book, besides updating and reorganizing the nuclear portions of the previous text, ventures into the safety assessment of chemical facilities, another important industry driver of probabilistic safety assessment methods and applications.

As expected, the nuclear sections of this book have much greater scope (breadth and depth) than the chemical sections. This is a direct result of the difference in the experience of the two industries in the development and application of PSA methods. The great appeal of extending the text to the chemical field is that it indicates not only the growth of the discipline, but the contribution to PSA that can come from different industries applying such methods. For example, the chemical field is extremely cost and competitively driven and has been very innovative in coupling safety assessment with plant performance considerations, a factor not nearly as visible in nuclear safety analysis. Other advantages of adding the chemical industry safety assessment practices to this text is the extensive operating experience base involved and the efforts of the chemical safety experts to employ more abbreviated probabilistic safety assessment methods.

This book, for the most part, is a stand-alone text. It addresses not only the fundamentals of PSA as a science, but insights on the regulatory framework affecting its development and application. In particular, it provides the basic methods of analysis that can be employed, available databases, an excellent set of examples, software resources, chapter summaries that facilitate comprehension, and problem sets that are very well connected to the theory. While much has been written about probabilistic safety assessment over the last three decades, this is the most comprehensive attempt so far to provide a much needed college level textbook for the education of risk and safety professionals. It also provides a valuable reference for any individual curious enough about the risk and safety sciences to want to become much more informed.

B. John Garrick, Ph.D, P.E.
Preface

This book aims at a unified presentation of probabilistic safety assessment as it is applied to the chemical processing and nuclear electrical generation industries. As John Garrick points out in the foreword, probabilistic safety assessment has developed over the latter part of this century to assess and thereby enhance safety in industries that have a remote possibility of affecting many people. PSA's genesis was in the space industry to achieve better equipment reliability. Its application to safety came with the U.S. government's "Plowshare" program for peaceful use of nuclear energy for electric power generation. The electric utility industry was reluctant to adopt this energy source because of the unknown liabilities. The Price-Anderson Act provided the insurance to protect the industry from an unknown risk. A worst case analysis (WASH-740) indicated a large potential hazard with unknown probability of occurrence.

There had been small-scale probabilistic risk studies, but the first in-depth study was initiated by the U.S. Atomic Energy Commission in September 1972 and completed by the Nuclear Regulatory Commission (NRC). This was known as the "Reactor Safety Study," (WASH-1400, October 1975) that set the pattern for subsequent PSAs not only nuclear, but chemical and transportation. PSA had it beginnings in nuclear power because of the unknown risk and the large amounts of funds for the investigation.

There is a close kinship between the chemical process industry and the nuclear electric power industry. In fact once the physics of nuclear reaction was established the rest is chemistry and heat transfer. The word "reactor" is from chemistry for the location the reaction takes place. A nuclear reactor consists of a vessel in which a nuclear reaction heats water to make steam to drive a turbine to generate electricity. Thus the primary components are pipes, valves, pumps heat exchangers, and water purifiers similar to the components found in a chemical plant. Following the success of WASH-1400, PSA was used to analyze the chemical processing of nuclear fuel and waste preparation for disposal.

A leader in applying PSA to other parts of the chemical process industry has been the AIChE's Center for Chemical Process Safety. A major difference between PSA for nuclear power and PSA for chemical processing has been the lack of government regulations that require risk analysis for chemical processes. A primary impetus has been the Occupational Safety and Health Administration's (OSHA) PSM rule that defines the application of PSA to the chemical industry for the protection of the public and workers. In addition, the Environmental Protection Agency (EPA) regulates waste disposal.

This book describes the evolution of PSA.

WASH-1400 provided the first comprehensive estimate of the risk of two nuclear power plants which were assumed to be generic, hence, taken to represent the industry in the U.S. The NRC, the agency responsible for the regulation of nuclear power in the U.S. used and extended WASH-1400 for regulating the plants and making decision on retrofitting, inspection, maintenance and other purposes. Thus, the legal requirements for a nuclear power plant license drives the use of PSA for this purpose. While not an NRC licensee, the Department of Energy applied PSA to its nuclear power plants and process facilities and adopted many of NRC's safety criteria.

Considerations for preparing this book were:
• Show the long historical usage of PSA by government and industry for protecting health safety, environment and the infrastructure of civilization. PSA has only been known recently by this term, but its processes have long been practiced.
• Present risk from its basis in insurance. This is the natural basis that says that risk is the product of probability and consequences.
• Show the complex iterations between government laws and regulations and the PSA response to not only comply but to protect the process industry. The real impact of the accident at the Three-Mile Island nuclear plant was not radiation, which was within regulations but financial losses to the utility and the acceptance of nuclear electrical power in the United States. The effects of the Bhopal accident were in human life but it also had a profound effect on the chemical industry: financially, and its acceptability and growth.
• Present the mathematics used in PSA in one chapter to be skipped, studied, or referred to according to the readers needs.
• Provide the reader with a computer disk containing programs that I have found useful and to provide FTAP and its associated programs. Computer codes that calculate fault trees are either proprietary or expensive or both. FTAP and associated codes are the only code suite that is in the public domain. The disk proves them grouped as FTAPSUIT as a "bat" file in association with the FTAPLUS program to aid in formatting. FTAPSUIT is a sophisticated set of programs that finds the cutsets, calculates their probabilities, handles dependencies, and calculates importances and uncertainties. It was written long ago before user-friendly interfaces but this fact may assist understanding and learning.
• As far as I know, this is the only book that merges nuclear and chemical PSA. Although both processes are similar, nuclear PSA places emphasis on reliability and the probabilistic calculation other than the consequence calculation. Chemical PSA places more emphasis on the consequences than on the probability. Chapter 3 presents methods used by both to determine the reliability of systems and the probability of failure. It begins with OSHA's PSM rule that outlines process for use in analyzing PSA. Qualitative methods are presented before quantitative. The chapter ends by describing computer codes to aid in the calculations and results presentation. Chapter 4 presents data and human factors analysis that are used by both industries. Chapter 5 outlines methods for analyzing the effects of "externalities" on plants. These include earthquake, wind, fire and flood. Chapter 6 describes nuclear reactors, and how they are analyzed to determine the probability of an accident. The only major accidents: Three-Mile Island and Chernobyl are described as to cause and response. Chapter 8 describes how the consequences of such an accident are calculated. Chapter 7 describes the scope of the chemical process industry, major recent accidents that have occurred, including Bhopal. It goes on to describe hazardous chemical processes and how to analyze the probability of an accident. Nuclear reactors and how they are analyzed to determine the probability of an accident; Chapter 9 describes how the consequences of such an accident are calculated by hand and computer codes that are available for more detailed calculations. Chapter 10 describes how the accident probabilities and consequences are

---

These codes are provided by Dr. Howard Lambert of LLNL and FTA Associates, 3728 Brunell Dr., Oakland CA 94602.
assembled for a risk assessment. Chapter 11 describes how PSA is applied in both industries. More examples of nuclear than chemical applications are given because many of the chemical applications are proprietary. Chapter 12 describes codes on the distribution disk. Chapter 13 is an extensive glossary to define acronyms for the reader that is unfamiliar with them and allows me to use them as shorthand for those that are familiar to them. Chapter 14 provides references from which some information was extracted and some references are provided for further study by the reader. Chapter 15 provides answers to the problems that are at the end of some of the chapters. These problems are not so much exercises as providing an extension of the text. My answers are not simply stated but are worked out to show the reasoning.

I am a physicist who switched to nuclear engineering for my Ph D. My introduction to PSA was as an original participant in the Reactor Safety Study in 1972. Material for this book was first gathered in 1974 for a workshop on what to expect in WASH-1400 (the results of the Reactor Safety Study). Materials were gathered over the years for EPRI, Savannah River Laboratory, and other workshops. A culmination was in 1988 with "Probabilistic Risk Assessment in the Nuclear Power Industry" with Robert Hall as coauthor. This book updates these materials and adds material on PSA in the chemical process industry. I prepared the material for printing using a word processor.

Ralph Fullwood
Brookhaven National Laboratory, retired, 1998.
This Page Intentionally Left Blank
Acknowledgments

I am greatly indebted to many people over the years who have taught and advised me. To Professor Rasmussen who introduced me to the subject and colleagues on the Reactor Safety Study: Dr. William Vesely, John Kelly, Fred Leverenz, and Abel Garcia. To Dr. Robert Erdman for whom I worked at Science Applications International Corporation and other friends in that organization including Kartik Majumdar, Eugene Hughes Dr. Edward Burns, and Dr. Bryce Johnson. To Professor N. J. McCormick at the University of Washington whose book was an inspiration for this one.

At Brookhaven National Laboratory, I wish to acknowledge the support, assistance, discussions and suggestions with Robert Hall (coauthor on the first book), and Drs. Robert Bari, Ali Azarm, Robert Bari, John Boccio, Lewis Chu, John Lehner, Semyon Shteyngart, and Trevor Pratt. Helen Todosow was very helpful for library assistance.

I am particularly indebted to Dr. Howard Lambert of Lawrence Livermore Laboratory and FTA Associates for providing the PC computer codes FTAP (fault tree code), POSTPR (post processor), IMPORT (importance calculation), MONTE (Monte Carlo error determination), and supporting documentation and instructions.

Dr. Richard Walentowicz provided the EPA CD-ROM disk entitled “Exposure Models Library and Integrated Model Evaluation System” with other reference material. Lester Wittenberg of the Center for Chemical Process Safety, AIChE was particularly helpful in providing a chemical industry perspective and reference material as was Dr. Steven Arendt of JBF Associates, Inc. Drs. David Hesse of Battelle Columbus Laboratories and Vinod Mubayi of Brookhaven National Laboratory were very helpful in providing material on the chemical consequence codes.

For the foreword, I would like to thank Dr. John Garrick, who began PSA work in the 1960s and innovated many of the procedures.

Lastly, I wish to thank my publisher Butterworth-Heinemann and staff for their patient, accurate and prompt work in preparing the manuscript.

Ralph R. Fullwood
Chapter 1
Protecting the Public Health and Safety

Probabilistic Safety Assessment (PSA) is an analytic method for protecting the public health and safety. The institutional methods are traced from early times to the present to show a progressive understanding of risk, related terms and methods for anticipating safety concerns before they are manifest as death and injury. Besides presenting common definitions of terms related to safety, mathematical representations of risk are presented for calculating risk. Short-comings of the mathematical forms are discussed as well as differences between calculated risk and public perception of risk. Safety goals for nuclear power are discussed as well as the regulatory bases for nuclear power and chemical processing.

1.1 Historical Review

1.1.1 Beginnings

State intervention in man's activities to protect the health of the inhabitants goes back to prehistory. The motivation may not have been altogether altruistic; the king acted to protect his subjects because he regarded them as his property. Public health protection began for disease control. With industrialization, came the need for control of even more hazardous forces and substances. This extended protection became technological in accident analysis and response. Present efforts in controlling risk, such as from nuclear power, are a continuation of this development.

Safety, as it relates to public protection from disease, has a history extending to early history. Ruins in the Indus Valley reveal that as early as 400 B.C., building codes and sanitary engineering was in effect. The Egyptians from the middle kingdom (approximately 2000 B.C.) had bathroom and sewage facilities, as did the Incas. The Greeks formulated principles of hygiene and attempted to show a causal relationship between environmental factors and disease. Indeed, the basic text on epidemiology for 2,000 years was "Air, Waters, and Places" from the Hippocratic collection. The Romans perceived a relationship between swamps and malaria and drained many swamps. They also devised dust respirators for workers, built sewage systems, public baths and great aqueducts. Officials were empowered to destroy impure foodstuffs and regulate public baths, brothels and burial grounds. Justinian I of Byzantine, to combat one of the worst plagues in history (532 A.D.), set up quarantine posts and required certificates of health for admission to Constantinople.
Protecting the Public Health and Safety

Health protection is a very old concept that has also been incorporated into state religion. The Biblical books: Leviticus and Numbers established dietary laws, rules of hygiene, precautions against contagious diseases and prohibitions against consanguineous marriages. These rules are similar to those imposed by modern states concerning food preservation, epidemic control, and hereditary diseases.

While health care declined after the fall of the Roman Empire, England used the common-law concept of public nuisance to protect the public from flagrant cases of polluting the waters. In France, Germany, and Italy, tanners were prohibited from washing skins in the water supply. London, from 1309, had ordinances regulating cesspools and sewers. The Florentines forbade the sale of meat on Monday that had been slaughtered on Friday.

National health legislation came into being in the 19th century primarily in the form of laws that governed the conditions of child labor and eventually prohibited it. In Germany, medical police were organized to make and enforce health and safety regulations. Both France and Germany became committed to the proposition that government had a positive duty to provide for the health, safety and welfare of workers and citizens.

The coming of industrialization intensified existing problems and created new ones. With the Clearances in England, came migration of farm labor to the cities as well as improvements in agricultural productivity to support the increasing urban population and consequent increase in communicable diseases. Smallpox was the most widespread disease in the 18th century. Peak years in London occurred between 1723 and 1796, with a periodicity of about five years. Each outbreak took over three thousand lives. In the 1740s, 75% of London’s infants died before the age of five. The diseases of typhus and scarlet fever were also major contributors.

Victorian England led the world to better health by actions improving nutrition and working conditions. The Public Health Act of 1848, established Local Boards of Health specifying educational levels of the district health officers and empowering them to enforce sanitation requirements.

1.1.2 Industrial Revolution

The other effects on safety brought by industrialization resulted from new and more powerful energy sources. Although water and wind power was used in the Middle Ages, these forces were "natural" and believed to be understood. However, the steam engine was something new. The original condensation engine was sub-atmospheric, but with Watt’s invention and Carnot’s theory, the quest for higher steam pressure and temperature began.

The original steam generators were simple pressure vessels that were prone to catastrophic failures and loss of life. Due to better boiler design, tube-fired boilers, and boiler inspections, the incidence of catastrophic failure is now to a rare event (about once every 100,000 vessel-years). In Great Britain in 1866, there were 74 steam boiler explosions causing 77 deaths. This was reduced to 17 explosions and 8 deaths in 1900 as a result of inspections performed by the Manchester Steam User Association. In the United States, the American Society of Mechanical Engineers established the ASME Pressure Vessel Codes with comparable reductions.
The development of steam and later the internal combustion engine made possible transportation by rail, road and air at speeds never before experienced. In all cases, the regulations, inspections, and design standards were imposed after the hazards had been exhibited by many deaths and injuries. Nuclear power has attempted, rather successfully, to anticipate the risks before they occur and avoid them through design, control and regulation. PSA is an essential analytical tool for accomplishing this result.

1.1.3 This Century

The discovery of nuclear fission made possible a far more concentrated energy source than ever before. Its hazards were recognized from the beginning, and for the first time, a commitment by government, to safely bring a technology on line without the deadly learning experiences that occurred to safely use earlier technologies. During World War II, experience was acquired in the operation of plutonium production and experimental reactors. Shortly after passage of the Atomic Energy Act of 1948, the Reactor Safeguards Committee was formed (1947) which was to merge with the Industrial Committee on Reactor Location Problems (1951) to become the ACRS (Advisory Committee on Reactor Safeguards). The Atomic Energy Act of 1954 made industrial nuclear power possible, and the first plant began operation at Shippingport, PA, in 1957. The risk posed by a nuclear power plant at this time was unknown, hence the Price-Anderson Act was passed to limit the financial risk.

The first report on nuclear power plant accidents, WASH-740, was issued by Brookhaven National Laboratory (1957). The consequences predicted were unacceptable, but it was believed that the probability of such an accident was very small. This report and the technically untenable Maximum Credible Accident method in licensing gave rise, during the 1960s, to probabilistic approaches to siting (Farmer, 1967; Otway and Erdmann, 1970) and to accident analysis (Garrick et al., 1967; Salvatori, 1970; Brunot, 1970; Otway et al., 1970; Crosetti, 1971; and Vesely, 1971). The most ambitious of the pre-Reactor Safety Studies was Mulvihill, 1966, which consisted of a fault tree probability analysis followed by consequence analysis of the postulated accidents at a nuclear power plant.

Reactor Safety Study

The Reactor Safety Study (RSS) directed by Professor Norman Rasmussen of MIT may have had its beginnings in a letter from Senator Pastore to James Schlesinger, AEC Chairman, requesting risk information for the Price-Anderson renewal. The RSS study began in September 1972 with Saul Levine, full-time staff director assisted by John Bewick and Thomas Murley (all AEC).

A significant development of the study was the use of event trees to link the system fault trees to the accident initiators and the core damage states as described in Chapter 3. This was a response to the difficulties encountered in performing the in-plant analysis by fault trees alone. Nathan Villalva and Winston Little proposed the application of decision trees, which was recognized by Saul Levine as providing the structure needed to link accident sequences to equipment failure.

The Reactor Safety Study was the most important development in PSA because it:
Protecting the Public Health and Safety

- Established a pattern for performing a PSA of a nuclear plant;
- Provided a basis for comparison;
- Identified transients and small LOCAs as the major risk contributors, rather than the previous emphasis on a large LOCAs;
- Showed that the radiological risk of a nuclear power plant is small compared with other societal risks;
- Originated the event tree for linking initiators, systems, and consequences, and introduced the fault tree to a large audience;
- Compiled a database;
- Showed that human error is a major contributor;
- Showed the impact of test and maintenance; and
- Showed the importance of common mode interactions.

The work was published as draft WASH-1400 in August 1974 and extensively reviewed. The revised report was published as WASH-1400 (FINAL) in October 1975.

Following the release of WASH-1400, the techniques were disseminated by the authors and interpreters through publications, lectures, and workshops. Many organizations set up in-house PSA groups, and the nucleus of the organization that had produced the Reactor Safety Study continued at the NRC.

Critique of the Reactor Safety Study (RSS)

WASH-1400 (FINAL), Appendix XI presents comments and responses on the draft report. Some of these resulted in changes that were incorporated in the final report. Only a few critiques of the final report have been published. Two of these are NUREG/CR-0400 (Lewis Report) and Kendall, 1977. Of these, the Lewis Report’s comments are the most objective (Leverenz and Erdmann, 1979, provide a review of the Lewis review). Some comments are summarized:

1. Despite its shortcomings, WASH-1400 provides at this time (1978) the most complete single picture of accident probabilities associated with nuclear reactors. The fault tree/event tree approach coupled with an adequate database is the best method available to quantify these probabilities.
2. The Committee is unable to determine whether the absolute probabilities of accident sequences in WASH-1400 are high or low, but it is believed that the error bounds on those estimates are, in general, greatly understated. This is due in part to an inability to quantify common cause failures, and in part to some questionable methodological and statistical procedures.
3. It should be noted that the dispersion model for radioactive material developed in WASH-1400 for reactor sites as a class cannot be applied to individual sites without significant refinement and sensitivity tests.
4. The biological effects models should be updated and improved in the light of new information.
5. After having studied the peer comments about some important classes of initiating events, we remain unconvinced of the WASH-1400 conclusion that they contribute negligibly to the overall risk. Examples include fires, earthquakes, and human accident initiation.
6. It is conceptually impossible to be complete in a mathematical sense in the construction of event trees and fault trees. What matters is the approach to completeness and the ability to demonstrate with reasonable assurance that only small contributions are omitted. This inherent limitation means that any calculation using this methodology is always subject to revision and to doubt as to its completeness.

7. The statistical analysis in WASH-1400 suffers from a spectrum of problems, ranging from lack of data on which to base input distributions to the invention and the use of wrong statistical methods. Even when correct, the analysis is often presented in so murky a way as to be very hard to decipher.

8. For a report of this magnitude, confidence in the correctness of the result can only come from a systematic and deep peer review process. The peer review process of WASH-1400 was defective in many ways and the review was inadequate.

9. Lack of scrutability is a major failing of the report, impairing both its usefulness and the quality of possible peer review.

These criticisms only are partially addressed in subsequent work.

1.2 Risk Assessment Objectives

The assessment of risk with respect to nuclear power plants is intended to achieve the following general objectives:

- Identify initiating events and event sequences that might contribute significantly to risk,
- Provide realistic quantitative measures of the likelihood of the risk contributors,
- Provide a realistic evaluation of the potential consequences associated with hypothetical accident sequences, and
- Provide a reasonable risk-based framework for making decisions regarding nuclear plant design, operation, and siting.

One of the products of a nuclear power plant PSA is a list of plant responses to initiating events (accident starters) and the sequences of events that could follow. By evaluating the significance of the identified risk contributors, it is possible to identify the high-risk accident sequences and take actions to mitigate them.

Although the consequences of the high-risk accident sequences may vary from one PSA to another, all PSAs attempt to evaluate realistically, the consequences of hypothetical accident sequences. Depending on the scope of the PSA, these evaluations may include an estimation of the number of latent cancers, the number of immediate fatalities, the probability of core damage, or a number of other consequence measures.

When used to identify and evaluate significant risk contributors, as well as to assess the consequences of accident sequences, the PSA provides a comprehensive framework for making many types of decisions regarding reactor design, operation, and siting. These and other applications can be facilitated by the rational evaluation of the risks associated with a particular installation.
1.3 Risk, Hazard, and other Terms

This text is concerned with quantified risk. To treat any subject mathematically, precise definitions are necessary for a common understanding. Risk is related to safety, danger, hazard, loss, injury, death, toxicity, and peril but it has two meanings that may cause confusion. The first definition concerns "hazard, peril, and exposure to injury or loss," which suggests an unrealized potential for harm. If the danger becomes real, then it is no longer risk but becomes "injury, loss, or death." The second definition is more explicit: "Risk is the chance of loss, injury, or death." Chance, likelihood, and probability are all related words for a random process.

1.4 Quantitative Aspects of Risk

Risk is a nebulous concept, but when low risk equipment leads to major consequences, the public feels that something is wrong - especially after the media perform their work. Putting risk on a mathematical foundation is a first step in setting a number to risk.

1.4.1 Actuarial or Linear Risk

To convert the words of the second definition of risk into mathematics, let "chance" be probability, "loss" be consequences, and "of" be multiplication. Expressed in words, this is: Risk = Probability times Consequences which is expressed by equation 1.4-1, using \( R \) for risk, \( p \) for probability, and \( C \) for consequence.

\[ R = p \times C \] (1.4-1)

A useful example of equation 1.4-1 is insurance, which was invented by the 15th century Genoese to protect against individual catastrophic shipping losses by sharing the risk. To derive the risk equation, suppose the insurer collects premium \( R \) for insuring \( N \) ships per year of which \( n \) are lost and an award \( C \) is paid for each lost ship. The insurance company receives \( N \times R \) in premiums; it pays out \( n \times C \) and breaks even (neglecting insurance company expenses) when these are equal (equation 1.4-2). Solving equation 1.4-2 for risk gives equation 1.4-3. As \( N \) becomes very large, the ratio, \( n/N \), approaches probability, \( p \) (Section 2.3). Thus, \( R = p \times C \), as stated in equation 1.4-1.

To illustrate, if you are in an age group with 1% probability of dying per year and the insurance pays $10,000, your annual premium must be at least $100 for the insurance company to break-even without considering the insurance company’s expenses.

A risk equation for nuclear power may be derived by imagining a world with a very large nuclear power plant population. All plants are identical with the same demography and meteorology. The plants are separated such that one does not affect the other. Each year, \( n_i \) plants fail in the \( i \)th failure mode, causing a population dose \( d_i \). If the effects are additive, the population dose (other risk measures could be used) is linearly proportional to the number failing (Equation 1.4-4), where \( c_i \) is...
a proportionality constant that is interpreted as the average population dose per plant caused by the \(i\)th failure mode. The total population dose \(D\) is the sum over the doses from \(M\) failure modes (equation 1.4-5). The probability of occurrence of the \(i\)th failure mode in the limit of large \(N\) is equation 1.4-6. The population dose per year per plant, and hence the plant risk, is given by equation 1.4-7 which says that risk is the expected consequence in the same sense that an insurance premium is the expected consequence of the awards.

In conclusion, risk is probability times consequences which is the expectation value of the consequences. In analogy to insurance, risk is the premium paid by society for the use of a technology.

### 1.4.2 Shortcomings of Linear Risk

Equation 1.4-7 is unsatisfactory because the risk from a large number of small accidents is the same as from a small number of large accidents if the total number of effects, say fatalities, is the same for each case. It is hypothesized that the perceived risk of a large accident is greater than the equivalent risk from many small accidents because of human nature and the emphasis of the news services on the unusual (50,000 traffic deaths per year is not newsworthy, but a single accident killing 50,000 is very newsworthy).

To address this nonlinearity, it has been proposed that the risk equation be modified as shown in equation 1.4-8 where the consequences are raised to the \(v\)-power to account for the effects of perception. Unfortunately, a physical basis for the value of \(v\) has not been established, but a suggested value is 1.2 (NUREG-0739). If \(v\) were set to 1, then risk would be linear and not allow for perception.

The perception problem may be avoided if risk is considered to be an ordered pair composed of probability and consequences without a relationship between the members of the pair. Figure 1.4.2-1 illustratively shows points representing the probability and consequence of accidents, associated with an activity plotted as a log-log graph. Encompassing the points are a smooth curve through the maximum points, and a tangent to this curve that defines at the maximum risk (\(p \cdot C\) product). Notice that neither curve bounds the total risk they bound the \(p, C\) ordered pair combinations. That is, given \(p\), the curves will indicate the maximum consequence with the curve giving a tighter (less conservative) bound than the straight line. The linear curve has the equation: \(p \cdot c = k\), where \(k\) is the constant risk value. (The slope of the constant risk curve will be 45° if the abscissa and ordinate have equal size decades.)
Although discussion up to this point has treated probability and consequences as precise quantities, there are uncertainties associated with both. It is common practice to present uncertainties as a "bell-shaped" curve called a probability distribution, probability density function (pdf), or just distribution (Figure 2.5-1). Such bell-shaped curves, however, are not probability but are the rate of change of probability (probability density). Probability is obtained by integrating over portions of the probability density. An exceedance probability (CCDF - complementary cumulative distribution function) is the integral from \( x \) to \( \infty \) (equation 1.4-9). This is the way that WASH-1400 presents most of its results. The next section discusses several ways of presenting PRA results and this method in particular. Figure 1.4.2-2 illustrates this type of presentation. Instead of showing the accident (\( p, C \)) combinations as dots, the accidents are presented as exceedance plots, i.e., the probability that a consequence \( x \) will be exceeded.

As a final comment on inadequacies of mathematical representations of risk, those who bear the risk are not necessarily those who receive the benefit. While unequal distribution of risk and benefit may not be fair, it is difficult to redress the inequity.

1.4.3 Presentation of Risk

Abstract calculations of risk have meaning only when their meaning is understood by people. Their significance may be communicated quantitatively and qualitatively.

1.4.3.1 Qualitative Results

System models, even unquantified, provide valuable insight into the robustness of the plant design. Because of the uncertainties in the data used to quantify the PSA, some people say that information in the cutsets is the most valuable result of a PSA. The cutsets are the groupings of things that must fail for an undesirable event to occur. Such an event could be some degree of core melt or it could be some system failing to perform its design function. Table 1.4.3-1 shows a typical cutset listing, grouped according to the order of combinations of failed components (single, double, triple, etc.) that must fail to cause system failure. For example, if failures A and D ("\(*\)" is the symbol for logical "AND"), occur concurrently, the system will fail. Furthermore, paired failures G*H, I*J, etc. will fail the system as will the triple combinations \( P*R*S \), \( P*R*T \), etc. Clearly, singlet components are more important than doublet which are more important than triplet.
components. Prioritization of test, maintenance and inspection activities may be prioritized according to their order in a cutset listing. A cutset listing also indicates systems that may be taken out for repair when the system is operating. For example, G may be taken out as long as H is functioning, but if L is taken out, the failure of M, N or O will fail the system, thus giving L a higher importance than G.

This ordering by singles, doubles and triples takes added meaning when the failure rates of the active and passive components (Table 1.4.3-1) are included. A doublet has a failure frequency that is the product of the two failure rates; a triplet is the product of three failure rates.

Another qualitative result, obtained from quantitative analysis, is the ordering of accident sequences, according to their fractional contribution to the risk. The order of the sequences is insensitive to data uncertainties (unless they are extreme).

The uncertainties in the data should be carried through the analysis and sensitivity studies performed. It is important to recognize that results can be useful despite large uncertainties because the order of importance may not be strongly affected by the uncertainties.

An important product of the analysis is the framework of engineering logic generated in constructing the models. The numerical estimates of frequencies need only be sufficiently accurate to distinguish risk-significant plant features.

The patterns, ranges, and relative behavior obtained can be used to develop insights into design and operation - insights that can be gained only from an integrated, consistent approach such as PSA. These insights are applicable to regulation and minimizing regulation impact.

Thus, PSA techniques serve as a valuable adjunct to the methods currently used in decision making by both industry and government. Although not yet developed to the point where they can be used without caution, they provide a framework of integrated engineering logic that can be used to identify and evaluate critical areas that influence economics and safety.
1.4.3.2 Quantitative Results

Figure 1.4.3-1 from WASH-1400 compares the risk of 100 nuclear plants with other man-caused risks. This is a CCDF that gives the frequency per year that accidents will exceed a value on the abscissa. For example, for 100 fatalities, the frequency that 100 nuclear power plants could do this is 1E-4, air crashes to persons on the ground: 1E-2, chlorine releases: 1.1E-2, dam failures: 7E-2, explosions: 8E-2, fires: 1.1E-1, air crashes (total): 5E-1, and total man-caused: 9E-1.

Some comments regarding Figure 1.4.3-1 are:

1. CCDF plots are difficult for many people to interpret.
2. Many activities are presented but the benefits of each are not the same. For example, there is no viable alternative to air travel, but there are alternatives to producing electricity with nuclear power plants. A better comparison would be between alternative methods for producing the same quantity. This was not done because the authors of WASH-1400 wanted to relate the risk of national nuclear power usage to risks with which the public is more familiar.
3. CCDFs may be compared if they have the same shape. If not, a line of constant risk may be drawn (Figure 1.4.2-1) and the comparison made by comparing the envelopes of constant risk.
4. Figure 1.4.3-1 does not reflect the uncertainties in the analysis; Figure 1.4.3-2 addresses this deficiency by presenting envelopes at the 5, 50, and 95% confidence levels. Of course, including confidence intervals on all curves, e.g., Figure 1.4.3-1 would be confusing.

Figure 1.4.3-3 is an example from the Indian Point hearings showing an effective use of CCDF. The purpose of this presentation was to assure that the reactor at the Indian Point site is about as safe as any that could be sited there; hence, comparisons are made of the risk
posed by other reactors at the same site. Figure 1.4.3-4 is presented to show that the Indian Point site is reasonable by comparison with some other sites. This figure illustrates the point that CCDFs cannot be compared if the curves have different shapes.

Logarithmic scales are frequently used in presenting risk results but most of the public do not understand logarithmic scales. Fullwood and Erdman, 1983 circumvent this problem by comparing risk as cubes in which linear dimensions are the cube root of the volume/risk. Figure 1.4.3-5 compares the risks associated with nuclear fuel reprocessing, refabrication and waste disposal with non-nuclear risks.

Presenting information as a cumulative integral (CCDF) may be confusing. Tables 1.4.3-2 and 1.4.3-3, corresponding to the preceding figures, present considerably more information in terms of expected effects (probability times consequences). Table 1.4.3-2, also from the Indian Point hearings, compares the PSA-assessed probabilities of severe core damage for various reactors.

Perhaps the most readily perceived type of presentation is a "pie" chart of the major contributors as determined in the Zion and Arkansas Nuclear One (ANO)-1) PSAs and presented in Figure 1.4.3-6.
1.4.4 Public Perception of Risk

The preceding section shows the rather abstract, mathematical methods used to present the results of PSA. While the "public" is a very diverse group, the majority do not receive information in this fashion but receive it through the news media. It is not the nature of news to attempt a balanced presentation but to emphasize the unusual. To illustrate, the fact that 50,000 people die each year in traffic accidents, involving a few deaths at a time, is not newsworthy. Furthermore the latency of a hazard greatly affects risk perception. If smoking resulted in immediate death, however unlikely, the public attitude would be greatly changed because the cause-effect relationship would be apparent. There is similarity between the risk of smoking and that of a nuclear power accident in that both result in an increase in the probability of cancer developing with a latency period of about 20 years, yet the hazard of nuclear power is perceived quite differently from that of smoking.

Equation 1.4-7 showed that as long as consequences are small enough, that effects are linear, i.e., not so catastrophic as to affect the perpetuation of civilization, the number of injuries or fatalities in either case are the same whether or not there are many small accidents or a few large accidents. But the public, either because of information sources or for more fundamental reasons does not see it this way. Since the public affects government, public perception is a concern.

The literature on this subject is so large that it cannot be encompassed in a brief review. NUREG/CR-1930 (1981) is a bibliographical survey of 123 references; Covello, 1981 lists 148 references. Since no risk should be tolerated if it has no benefits, most of the papers address the question "How safe is safe enough," by comparisons with acceptable risks. (In many cases these "acceptable" risks are really "tolerated" risks in that the cost of reduction does not seem to be warranted.)

Starr, 1969 approached this by investigating the "revealed preferences exhibited in society as the result of trial and error. (Similar to the "efficient market theory" in the stock market.) Starr conjectured that the risk of death from disease appears to determine a level of acceptable voluntary risk but that society requires a much lower level for involuntary risk. He noted that individuals seem to accept a much higher risk (by about 1000 times) if it is voluntary, e.g., sky-diving or mountain climbing, than if it is imposed, such as electric power or commercial air travel, by a correlating with the perceived benefit. From this study, a "law" of acceptable risk was found concluding that risk acceptability is proportional cube of the benefits. Figure 1.4.4-1 from Starr, 1972 shows these relationships. One aspect of revealed preferences is that these preferences do not necessarily remain constant (Starr et al., 1976). In Starr et al., 1976, it is shown that while nuclear power has the least risk of those activities compared, it also has the least perceived benefit. Clearly the public thinks that
alternative ways of producing electricity have less risk despite risk comparisons of various ways of electric power production such as Inhaber, 1979, Okrent, 1980 or Bolten, 1983.

Another approach to public perception of risk is to simply ask the public. This was the approach of Fischhoff et al., 1977 in which a survey of the League of Women Voters in Eugene, Oregon was taken. Later studies covered 40 college students at the University of Oregon, 25 Eugene businessmen and 15 national experts in risk analysis. Thomas, 1981 reports a survey of 224 selected Austrians.

Cross-comparing the risks of various activities is difficult because of the lack of a common basis of comparison, however Cohen and Lee, 1979 provide such a comparison on the basis of loss of life expectancy. Solomon and Abraham, 1979 used an index of harm in a study of 6 occupational harms - three radiological and three nonradiological to bracket high and low estimates of radiological effects. The index of harm consists of a weighting factor for parametric study: the lost time in an industry and the worker population at risk. The conclusions were that the data are too imprecise for firm conclusions but it is possible for a radiation worker under pessimistic health effects assumptions to have as high index of harm as the other industries compared.

To conclude, this sampling of the literature of risk perception, the comments of Covello, 1981 may be summarized. Surveys have been of small specialized groups - generally not representative of the population as a whole. There has been little attempt to analyze the effects of ethnicity, religion, sex, region age, occupation and other variables that may affect risk perception. People respond to surveys with the first thing that comes to mind and tend to stick to this answer. They provide an answer to any question asked even when they have no opinion, do not understand the question or have inconsistent beliefs. Surveys are influenced by the order of questions, speed of response, whether a verbal or numerical response is required and by how the answer is posed. Few studies have examined the relationships between perceptions of technological hazards and behavior which seems to be influenced by several factors such as positive identification with a leader, efficacy of social and action, physical proximity to arenas of social conflict.

1.5 Safety Goals

During the 1970s, a number of safety requirements were imposed that required backfitting existing nuclear power plants that increased the costs of new plants. It was believed that codifying
Protecting the Public Health and Safety

a level of safety would stabilize the licensing and possibly aid in the public acceptance of nuclear power. The Three Mile Island-2 accident gave further impetus to establishing safety goals because the requirements of 10CFR100 (accidents must be less than 25 rem whole body or 300 rem thyroid dose to any individual) were not even closely approached. Nevertheless the public response essentially invalidated the rule. The NRC, in responding to the President's Commission on the Accident at Three Mile Island, stated that it was "prepared to move forward with an explicit policy statement on safety philosophy and the role of safety-cost tradeoffs in the NRC safety decisions." The objective of the policy statement was to establish goals defining a acceptable level of radiological public accident risk imposed on the public by the operation of nuclear electric power plants. Hearings on both coasts were held and suggestions were solicited. Some of the papers that were published in response to this request were: Mattson et al., 1980; Starr, 1980; Salem et al., 1980; O'Donnell; 1982 and Cox and Baybutt, 1982. The NRC issued a "Discussion Paper on Safety Goals for Nuclear Power Plants" (NUREG-880, 1983) with qualitative goals and a suggested a quantitative goal of less than one core melt per 10,000 years.

Discussions continued and in August 1986 the formal statement was issued by the NRC (Federal Register 51.162 p30029 - 30033). The two qualitative safety goals are:

- "Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.
- "Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks."

The statement goes on to acknowledge the contribution of the Reactor Safety Study (WASH-1400) to risk quantification but points out that safety goals were not the study objectives and that the uncertainties make it unsuitable for such a purpose. After pointing out that the death of any individual is not "acceptable," it states two quantitative objectives:

- "The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed 0.1% of the sum of prompt fatality risks from other accidents to which members of the U.S. population are generally exposed."
- "The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed 0.1% of the sum of cancer fatality risk resulting from all other causes."

The fraction 0.1% is chosen to be so low that individuals living near a nuclear plant should have no special concern because of the closeness. Uncertainties in the analysis of risk are not caused by the "quantitative methodology" but are highlighted by it. Uncertainty reduction will be achieved by methodological improvements; mean values should be calculated. As a guideline for regulatory implementation, the following is recommended:
"...the overall mean frequency of a large release of radioactive materials to the environment should be less than 1 in 1,000,000 years of reactor operation."

These safety goals are not meant to supersede any of the present conservative design and operational practices such as, defense in depth, low population zone siting or emergency response capabilities. The goals may be considered as a factor in the licensing decision. Commissioner Asselstine of the USNRC provided an additional view by saying that the nuclear industry has been trying to distance itself from the Chernobyl accident on the basis of containment performance (the Russian plant had no containment structure) and recommended "a mean frequency of containment failure in the event of a severe core damage accident should be less than 1 in 100 severe core damage accidents." Commissioner Asselstine also recommends that the large release criterion of less than once per 1,000,000 reactor years be adopted with clarification as to the meaning of a "large release."

Commissioner Bernthal, felt that the statement does not address the question "How safe is safe enough?" or assure the public concerning the Chernobyl accident, while preserving the nuclear power option. A fool-proof containment, while protecting the public would not satisfy this last requirement. He furthermore decries the absence of population density consideration in the 0.1% goals which would allow a plant to be located in "New York’s Central Park." Furthermore he points out that the 0.1% incremental societal health risk standard that is adopted is a purely subjective assessment of public acceptance.

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1970</td>
<td>10CFR50.34 required a discussion of plans for coping with emergencies.</td>
</tr>
<tr>
<td>1975</td>
<td>The format and content of onsite emergency plans was given in Reg. Guide 1.101. Offsite emergency planning was required for licensing purposes for a low-zone (EPZ) within a 3 mile radius about the plant.</td>
</tr>
<tr>
<td>1978</td>
<td>NUREG-0396 defined two EPZ at radii of 10 miles to provide protection from direct radiation by evacuating or sheltering the public and at 50 miles within which food and water interdiction would protect from this dose pathway.</td>
</tr>
<tr>
<td>1979</td>
<td>President Carter directs the Federal Emergency Management Administration (FEMA) responsibility of offsite emergency planning. The NRC retained jurisdiction over plant licensing and operation with respect to onsite emergency preparedness.</td>
</tr>
<tr>
<td>1980</td>
<td>NUREG-0654/FEMA-REP-1 and 10CFRS0 Appendix E gave bases for both onsite and offsite emergency planning. It requires joint utility, state and local participation in an annual simuated accident exercise as a condition for an operating license.</td>
</tr>
<tr>
<td>1981</td>
<td>The NUREG-0654, etc., requirements were modified such that the annual exercise is needed only for operation above 5% power.</td>
</tr>
<tr>
<td>1983</td>
<td>FEMA relaxed the rule for offsite exercises to every two years. The onsite exercise frequency remains the same.</td>
</tr>
</tbody>
</table>

1.6 Emergency Planning Zones

The philosophy of public health protection used by the AEC and pursued ever since, is the use of multiple independent barriers, each a significant shield for the public. The last barrier involves the removal of people from the area over which the radioactive plume is expected to pass, interdiction of food supplies and the use of prophylaxis to reduce the iodine dose. Blood
transfusions have also been used to save the lives of people lethally exposed. Emergency planning to protect the public in case of a nuclear power accident is in a much more advanced state than the emergency planning for more likely and potentially more dangerous accidents such as poisonous chemical releases or dam failure because it is required by law. It does present some vexing problems regarding legal responsibilities. The Atomic Energy Act of 1954 made the Federal Government responsible for nuclear power but emergency actions may require the participation of several states and many local jurisdictions. The lack of cooperation from any of these may be used to oppose Federal policy.

Table 1.6-1 from Buzelli, 1986 gives a chronology of the Federal regulations.

Evacuation in case of a nuclear accident had always been considered a possibility to be considered on an ad hoc basis much as it is for releases of hazardous material that could affect the public. The Reactor Safety Study (WASH-1400, 1975) showed the possibility of some immediate fatalities, and set in motion the regulatory process shown in the table. The TMI-2 accident, during which Governor Thornburg, concerned about the possibility of a hydrogen-bubble explosion, recommended an evacuation, did much to increase the concern for emergency planning.

In the aftermath of TMI-2, NUREG-0654 and regulations were promulgated that strongly codified the emergency planning process. NUREG-0654 presents bases for emergency planning and its relationship to the EPZ. Sixteen standards are presented to be used in evaluating the plant's emergency plan. The criteria for emergency response are presented in Table 1.6-2.

The nuclear power industry has generally opposed these emergency planning requirements partially on the basis of cost but primarily because of the poor public image it gives these plants by involving the public in the drills not required for any other industry. Reducing the size of the EPZ is much to their liking. The technical basis for the size of the EPZ was WASH-1400 which was a basis for the criteria presented in NUREG-0396. Besides demonstrating an evacuation, TMI-2 also demonstrated that the quantities of radioactive releases used in WASH-1400 were grossly conservative for many isotopes. The industry response was the IDCOR program and the NRC response to a reexamination of the "source terms" is contained in NUREG-0956 (discussed in Section 7.2). Hazzan and Warman, 1986 using these and other sources recommend that the EPZ be reduced to 2 miles as does Kaiser, 1986. Solomon and Kastenburg, 1985 reviewed 4 PSA studies of the Shoreham plant - one of the most affected plants by emergency planning and concluded that plant features would allow a reduction to 10 miles.

In concluding this brief discussion on emergency planning, it may be pointed out that the planning criteria are not dependent on the size of the plant nor on special plant features. For example, a plant could have such a strong containment that nothing could escape, even in the most severe accident, and the EPZ would be the same as it is for any other plant. Another anomaly is that the 50 mile ingestion pathway from the Canadian nuclear power plants reach into the U.S. without the same requirements being applied.

---

1 Immediate in emergency planning means a death within a year of exposure. Long-term deaths are a different problem because of the indistinguishability of a cancer death initiated by radiation and other causes, e.g., smoking. The effect of a nuclear accident would be a very small contributor to a large background of other causes.
<table>
<thead>
<tr>
<th>Emergency class</th>
<th>Plant criteria</th>
<th>Release of activity</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unusual event (UE)</td>
<td>Indication of potential plant degradation</td>
<td>None</td>
<td>Notification and information</td>
</tr>
<tr>
<td>Alert (A)</td>
<td>Actual or potential degradation of plant safety</td>
<td>Minor</td>
<td>Notification and information, partial activation of EOC</td>
</tr>
<tr>
<td>Site area emergency (SAE)</td>
<td>Actual or likely failure of plant safety</td>
<td>Small - within Federal guidelines</td>
<td>Activation of EOC, deployment of emergency monitoring and communication teams</td>
</tr>
<tr>
<td>General emergency (GE)</td>
<td>Actual or imminent substantial core degradation loss of containment possible</td>
<td>Releases reasonably expected to exceed Federal guidelines</td>
<td>Recommendations to evacuate/shelter for a 2-mile radius, shelter downwind expected to sectors to five miles</td>
</tr>
</tbody>
</table>

### 1.7 Use of PSA by Government and Industry

Interpreting PSA as any risk assessment using accident probabilities and consequences, government and industry have prepared many examples. These are discussed as: Public Risk, Specialized Analyses, and Performance Improvement.

Initially PSAs were used, primarily, to evaluate risk imposed on the public or workers. This includes the use of PSA in licensing and/or review procedures to assure protection of public health and safety. Examples by user are:

- Department of Defense - requires that a PSA be performed according to MIL-STD-882A for any major activity or undertaking, e.g., analyses of the transportation of nuclear weapons and deactivation of chemical weapons.
- Environmental Protection Agency - has sponsored work on the risk of chemical manufacture and transportation, the risk of reprocessing nuclear fuel, and the risk of nuclear waste disposal.
- Department of Transportation - has sponsored work on air, ground, rail, and water transportation, using PSA methods.
- Department of Energy - has sponsored analyses of its reactors and process facilities, the risks of the breeder reactor, the risk of nuclear material transportation and disposal, and the risks of several fuel cycles.
- Chemical Industry - has risks comparable to or possibly greater than those of the nuclear power industry, but no risk studies of chemical plants in the U.S. have been published. Great Britain, on the other hand, has been active in this area, e.g., the Canvey Island Study (Section 11.4.1 and Green, 1982).
Protecting the Public Health and Safety

- Nuclear Regulatory Commission - has been a prime mover in the use of PSA and in requiring its use by applicants. Although the Reactor Safety Study (RSS) originated under the Atomic Energy Commission, it was completed by the NRC. Its initial purpose was to provide information for the, at that time, forthcoming Price-Anderson renewal hearings regarding the risk of commercial nuclear power plants.

1.8 Regulation of Nuclear Power

1.8.1 Regulations

The regulations concerning nuclear installations in the United States are governed by the Atomic Energy Act of 1954 as amended, and the Energy Reorganization Act of 1974, as amended (which created the NRC, and the DOE). The NRC administers statutes on the licensing of nuclear installations in the United States. In addition, other applicable statutes are given in Table 1.8-1

Nuclear installations in the United States must be licensed by the NRC, but some Federal government facilities are exempt from licensing such as the Department of Energy.

<table>
<thead>
<tr>
<th>Table 1.8-1 Some Federal Regulations Governing the Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>- National Environmental Policy Act of 1969</td>
</tr>
<tr>
<td>- Resource Conservation and Recovery Act (RCRA) of 1976</td>
</tr>
<tr>
<td>- Toxic Substances Control Act; Clean Air Act of 1977</td>
</tr>
<tr>
<td>- Clean Water Act (CWA) of 1977</td>
</tr>
<tr>
<td>- Uranium Mill Tailings Radiation Control Act of 1978</td>
</tr>
<tr>
<td>- Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) of 1980</td>
</tr>
<tr>
<td>- Federal Facilities Compliance Act of 1990</td>
</tr>
<tr>
<td>- West Valley Demonstration Project Act of 1980</td>
</tr>
<tr>
<td>- Nuclear Waste Policy Act of 1982</td>
</tr>
<tr>
<td>- Administrative Procedure Act</td>
</tr>
<tr>
<td>- Coastal Zone Management Act</td>
</tr>
<tr>
<td>- Endangered Species Act</td>
</tr>
<tr>
<td>- Federal Advisory Committee Act Federal Water Pollution Control Act</td>
</tr>
<tr>
<td>- Freedom of Information Act</td>
</tr>
<tr>
<td>- Government in the Sunshine Act</td>
</tr>
<tr>
<td>- National Historic Preservation Act</td>
</tr>
<tr>
<td>- Privacy Act</td>
</tr>
<tr>
<td>- Wild and Scenic Rivers Act</td>
</tr>
</tbody>
</table>

1.8.2 Regulatory Structure

The NRC delegates the authority for reactor licensing to its Office of Nuclear Reactor Regulation (NRR). Fuel facility, nuclear waste storage and disposal are delegated to the Office of Nuclear Material Safety and Safeguards (NMSS). In cases where public hearings are required, the decision to license, and the condition of the license, rest with an Atomic Safety and Licensing Board (ASLB). For a construction permit, the ASLB decides all issues; in operating license proceedings, the ASLB decides controversial matters. These decisions are subject to review by an Appeal Board
and the NRC Commissioners. In these cases, the NRC staff cannot communicate directly with the Board and the Commission on the merits of the proceedings until a final Commission decision is rendered. Applications for a license to construct and operate an enrichment facility are handled by NMSS; if public hearings are held on such applications, decisions are subject to review by the Commission. Thus, in the United States, it is necessary to distinguish between actions, positions and decisions of the NRC staff, the Boards, and those of the Commission itself. Additional support for the licensing activities of NRR and NMSS comes from the Office of Nuclear Regulatory Research and Regional Offices.

1.8.3 Licensing Process

The licensing process consists of two steps: construction and operating license that must be completed before fuel loading. Licensing covers radiological safety, environmental protection, and antitrust considerations. Activities not defined as production or utilization of special nuclear material (SNM), use simple one-step, Materials Licenses, for the possession of radioactive materials. Examples are: uranium mills, solution recovery plants, UO₂ fabrication plants, interim spent fuel storage, and isotopic separation plants.

An applicant for a construction permit files a Preliminary Safety Analysis Report (PSAR) presenting design criteria and preliminary design information, hypothetical accident analyses, safety features, and site data. An Environmental Report (ER) must be submitted to evaluate the environmental impact of the proposed facility, and information must be submitted to the Attorney General and the NRC staff for antitrust review.

The application is subjected to an acceptance review to determine whether it contains sufficient information for a detailed review, if insufficient, additional information may be requested. When minimum material is submitted, the application is docketed in the Public Document Room, near the project, and an announcement is published in the Federal Register with appropriate officials being informed. When the PSAR is submitted, a substantive review and inspection of the applicant's quality assurance program, covering design, construction and procurement is conducted. The NRC staff reviews the application for undue risk to the health and safety of the public. If such is found, plant modifications may be requested. Additional information for the review are: demography, site characteristics, engineered safety features, design, fabrication, testing, response to transients, accident consequences, PSA conduct of operations, and quality assurance. The NRC staff and its consultants conduct this review over about two to three years using previous evaluations of other licensed reactors.

When the review progresses to the point that the staff concludes that the documentation is acceptable, a Safety Evaluation Report is prepared that represents a summary of the review and evaluation of the application by the staff.

The National Environmental Policy Act (NEPA) review is performed concurrently by the staff. After completion, a Draft Environmental Statement (DES) is issued and circulated for review and comments by the appropriate Federal, State and local agencies, individuals and public. After receipt of comments and their resolution, the Final Environmental Statement (FES) is issued.
When the final design information and plans for operation are ready, a Final Safety Analysis Report (FSAR) and the operating Environmental Report are submitted. The final design of the facility, and the operational and emergency plans are given in the FSAR. Amendments to the application and reports may be submitted from time to time. Each license for operation of a nuclear reactor contains Technical Specifications (Tech. Specs.) and an Environmental Protection Plan assuring the protection of health and the environment.

For an early site permit, the application must describe the number, type, thermal power level, and contain a plan for site restoration if the site preparation activities are performed, but the permit expires without being used. The application must identify physical characteristics that could pose a significant impediment to the development of emergency plans. The issues presented in an early site permit proceeding are mostly environmental, but if they involve significant safety issues, they are reported to the ACRS on the permit application.

Certified Standard Designs allow preapproval of the NSSS to reduce the time required for power reactor licensing. Applications for certification of a design must contain a level of detail comparable to that required for a final design approval. Combined Construction Permits and Conditional Operating Licenses streamline the licensing process by referencing a standard design and early permitted site.

1.8.4 Public Participation

Public hearings are required at the construction permit stage; the ASLB may grant a public hearing at the operating stage if requested by: the NRC, applicant, or a member of the public. The public hearing is conducted by a three-member Atomic Safety and Licensing Board (Board) appointed from the NRC's Atomic Safety and Licensing Board Panel. The Board is composed of a lawyer (chairman), and two technically-qualified persons. The Safety Evaluation, its supplements and the Final Environmental Statement are offered as evidence by the staff at the public hearing. The hearing may be a combined safety and environmental hearing or separate hearings can take place. If the initial decision regarding NEPA and safety matters is favorable, a construction permit is issued to the applicant by the Director of NRR. The Board's initial decision is, in the case of a reactor license application, subject to review by an Atomic Safety and Licensing Appeal Board.

1.8.5 Advisory Committee on Reactor Safety (ACRS)

The ACRS is an independent statutory committee that advises the Commission on reactor safety, and reviews each application for a construction permit or an operating license. It is composed of a maximum of fifteen members appointed by the Commission for terms of four years each.

As soon as an application for a construction permit is docketed, copies of the PSAR are provided to the ACRS for assignment to a project subcommittee consisting of four to five members. During the Staff review, the ACRS is kept informed of requests for additional information, meetings and potential design changes. If the plant is a "standard design" and the site appears acceptable, the subcommittee review does not begin until the staff has nearly completed its detailed review. Otherwise, the ACRS subcommittee begins its formal review early in the process. The Staff's Safety
1.8.6 Inspection

Construction inspections encompass all safety-related construction activities at the facility site. They consist of observation of work performance, quality assurance, testing, examination, inspection, records and maintenance. Inspection of pre-operational testing and operational readiness verifies the operability of systems, structures and components related to safety and whether the results of such tests demonstrate that the plant is ready for operation as specified in the SAR. It also verifies that the licensee has an operating organization and procedures consistent with the SAR; it verifies whether the tests conducted under both transient and operating conditions are consistent with the SAR. It also verifies that licensee management controls for the test program are consistent with NRC requirements and commitments.

Operations phase inspections verify, through direct observation, personnel interviews, and review of facility records and procedures that the licensee's management control system is effective and the facility is being operated safely and in conformance with the regulatory requirements. The NRC inspection program assigns resident inspectors at power reactors that are under construction or already operating. The licensee must give any resident inspector immediate, uninhibited access to the facility. In addition to regular inspections, staff members from several NRC offices investigate any significant incident and determine any hazards. Enforcement involves plant shutdowns, corporation and individual fines, and incarceration.

1.8.7 Decommissioning

The regulations require, before a license can be terminated, that the NRC must determine that the licensee's decommissioning activities have been carried out in accordance with the approved decommissioning plan, and the NRC order authorizing decommissioning with a final radiation survey demonstrating that the premises are suitable for release for unrestricted use. The regulations require licensee funding and completion of the decommissioning in a manner that protects public health, safety and environment.

1.8.8 Accident Severity Criteria

10 Code of Federal Regulations (10CFR) part 100 provides reactor siting criteria. It specifies that the fission product release calculated for major hypothetical accidents shall produce a whole
body dose less than 25 rem or thyroid dose less than 300 rem to the public (people outside of the site boundary fence). These criteria are not accepted limits but are intended as reference values.

### 1.8.9 PSA Requirements

There are no PSA requirements for licensing the current generation of nuclear power plants. Nevertheless PSA (PRA to the NRC) has been a tool for regulatory decisions by the NRC and has been used for compliance demonstration and modification justification by licensees.

10CFR50.54(f) states that the licensee must submit individual plant examinations (IPE) of significant safety issues to justify continuing operation of a reactor facility. The NRC issued Generic Letter stating that utilities with existing PSAs or similar analysis use these results, provided they are updated and certified that they reflect the actual design, operation, maintenance and emergency operations of the plant. The methodologies allow the user to determine dominant accident sequences and to assess the core damage preventive and mitigative capabilities of their plant. The IPEs are needed to confirm the absence of any plant unique vulnerabilities to severe accidents. This is to confirm vulnerabilities, identified by PRAs that were not previously identified by traditional methods.

The Generic Letter does not specify methodology or contents of an acceptable PSA. A satisfactory analysis is to be determined by the NRC staff, although NUREG-1560, volume 2 part 4 lists attributes of a quality PSA.

### 1.9 Regulation of Chemical Processing and Wastes

Chemical regulation is primarily concerned with the consequences to the public that may result from chemical releases to the environment. Note there is less concern with the probability than with the consequences of release. The major U. S. environmental laws are as follows.

#### 1.9.1 Environmental Law

**1.9.1.1 Clean Air Act (CAA) 42 U.S.C. s/s 7401 et seq. (1970)**

The Clean Air Act is the comprehensive Federal law that regulates air emissions from area, stationary, and mobile sources. This law authorizes the U.S. Environmental Protection Agency (EPA) to establish National Ambient Air Quality Standards (NAAQS) to protect public health and the environment. The goal of the Act was to set and achieve NAAQS in every state by 1975. This setting of maximum pollutant standards was coupled with directing the states to develop state

---

`b` Author’s note - The accident at TMI-1 released radioactivity far below 10CFR criteria but still the licensee was subject to severe regulatory action and suffered severe financial loss.

`c` 10CFR52 requires a PSA for the next generation of nuclear power plants.
Regulation of Chemical Processing and Waste

Implementation plans (SIPs) applicable to appropriate industrial sources in the state. The Act was amended in 1977 to set new goals for achieving NAAQS, since many areas of the country had failed to meet the deadlines. The 1990 amendments to the Clean Air Act in large part were intended to meet unaddressed or insufficiently addressed problems such as acid rain, ground level ozone, stratospheric ozone depletion, and air toxics.

1.9.1.2 Clean Water Act (CWA) 33 U.S.C. s/s 121 et seq. (1977)

The Clean Water Act is a 1977 amendment to the Federal Water Pollution Control Act of 1972, that set the basic structure for regulating discharges of pollutants to waters of the United States. This law gave the EPA the authority to set effluent standards on an industry-by-industry basis and continued the requirements to set water quality standards for all contaminants in surface waters. The CWA makes it unlawful for any person to discharge any pollutant from a point source into navigable waters unless a permit (NPDES) is obtained under the Act. The 1977 amendments focused on toxic pollutants. In 1987, the CWA was reauthorized and again focused on toxic substances, authorized citizen suit provisions, and funded sewage treatment plants (POTWs) under the Construction Grants Program. The CWA provides for the delegation by EPA of many permitting, administrative, and enforcement aspects, of the law to state governments. In states with the authority to implement CWA programs, EPA still retains oversight responsibilities.

1.9.1.3 Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA or Superfund) 42 U.S.C. s/s 9601 et seq. (1980)

CERCLA (pronounced “serk-la”) provides a Federal "Superfund" to clean up uncontrolled or abandoned hazardous waste sites as well as accidents, spills, and other emergency releases of pollutants and contaminants into the environment. Through the Act, EPA was given power to seek out those parties responsible for any release and assure their cooperation in the cleanup. EPA cleans up orphan sites when potentially responsible parties (PRPs) cannot be identified or located, or when they fail to act. Through various enforcement tools, EPA obtains private party cleanup through orders, consent decrees, and other small party settlements. EPA also recovers costs from financially viable individuals and companies once a response action has been completed. It is authorized to implement the Act in all 50 states and U.S. territories. Superfund site identification, monitoring, and response activities in states are coordinated through the state environmental protection or waste management agencies.

1.9.1.4 Emergency Planning & Community Right-to-Know Act (EPCRA) 42 U.S.C. 11011 et seq. (1986)

This is also known as Title III of SARA, EPCRA was enacted by Congress as the national legislation on community safety. This law was designed to help local communities protect public health, safety, and the environment from chemical hazards. To implement EPCRA, Congress required each state to appoint a State Emergency Response Commission (SERC). The SERCs were
required to divide their states into Emergency Planning Districts and to name a Local Emergency Planning Committee (LEPC) for each district. Broad representation by firefighters, health officials, government and media representatives, community groups, industrial facilities, and emergency managers ensures that all necessary elements of the planning process are represented.


The Endangered Species Act provides a program for the conservation of threatened and endangered plants and animals and the habitats in which they are found. The U.S. Fish and Wildlife Service (FWS) of the Department of Interior maintains the list of 632 endangered species (326 are plants) and 190 threatened species (78 are plants). Species include birds, insects, fish, reptiles, mammals, crustaceans, flowers, grasses, and trees. Anyone can petition FWS to include a species on this list or to prevent some activity, such as logging, mining, or dam building. The law prohibits any action, administrative or real, that results in a "taking" of a listed species, or adversely affects habitat. Likewise, import, export, interstate, and foreign commerce of listed species are all prohibited.

EPA's decision to register a pesticide is based in part on the risk of adverse effects on endangered species as well as the environmental fate (how a pesticide will affect the habitat). Under FIFRA, EPA can issue emergency suspensions of certain pesticides to cancel, or restrict their use if an endangered species will be adversely affected. Under a new program, EPA, FWS, and USDA are distributing hundreds of county bulletins which include habitat maps, pesticide use limitations, and other actions required to protect listed species.

In addition, EPA enforces regulations under various treaties, including the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES). The U.S. and 70 other nations have established procedures to regulate the import and export of imperiled species and their habitat. The Fish and Wildlife Service works with U.S. Customs agents to stop the illegal trade of species, including the Black Rhino, African elephants, tropical birds and fish, orchids, and various corals.

1.9.1.6 Federal Insecticide, Fungicide and Rodenticide Act (FIFRA) 7 U.S.C. s/s 135 et seq. (1972)

The primary focus of FIFRA provides Federal control of pesticide distribution, sale, and use. EPA was given authority under FIFRA not only to study the consequences of pesticide usage but also to require users (farmers, utility companies, and others) to register when purchasing pesticides. Through later amendments to the law, users also must take examinations for certification as applicators of pesticides. All pesticides used in the U.S. must be registered (licensed) by EPA. Registration assures that pesticides will be properly labeled and that, if used in accordance with specifications, will not cause unreasonable harm to the environment.
1.9.1.7 Freedom of Information Act (FOIA) U.S.C. s/s 552 (1966)

The Freedom of Information Act provides specifically that "any person" can make requests for government information. Citizens who make requests are not required to identify themselves or explain why they want the information they have requested. The position of Congress in passing FOIA was that the workings of government are "for and by the people" and that the benefits of government information should be made available to everyone. All branches of the Federal government must adhere to the provisions of FOIA with certain restrictions for work in progress (early drafts), enforcement, confidential information, classified documents, and national security information.

1.9.1.8 National Environmental Policy Act (NEPA) 42 U.S.C. s/s 4321 et seq. (1969)

The National Environmental Policy Act was one of the first laws written to establish the broad national framework for protecting the environment. NEPA's basic policy is to assure that all branches of government give proper consideration to the environment prior to undertaking any major Federal action which significantly affects the environment. NEPA requirements are invoked when airports, buildings, military complexes, highways, parkland purchases, and other Federal activities are proposed. Environmental Assessments (EAs) and Environmental Impact Statements (EISs) that assess the likelihood of impacts from alternative courses of action, are required from all Federal agencies and are the most visible NEPA requirements.

1.9.1.9 Occupational Safety and Health Act 29 U.S.C. 61 et seq. (1970)

Congress passed the Occupational and Safety Health Act to ensure worker and workplace safety. Their goal was to make sure employers provide their workers a place of employment free from recognized hazards to safety and health, such as exposure to toxic chemicals, excessive noise levels, mechanical dangers, heat or cold stress, or unsanitary conditions. In order to establish standards for workplace health and safety, the Act also created the National Institute for Occupational Safety and Health (NIOSH) as the research institution for the Occupational Safety and Health Administration (OSHA). OSHA is a division of the U.S. Department of Labor which oversees the administration of the Act and enforces Federal standards in all 50 states.

1.9.1.10 Pollution Prevention Act 42 U.S.C. 13101 and 13102, s/s 6602 et. seq. (1990)

The Pollution Prevention Act focused industry, government, and public attention on reducing the amount of pollution produced through cost-effective changes in production, operation, and raw materials use. Opportunities for source reduction are often not realized because existing regulations, and the industrial resources required for compliance, focus on treatment and disposal. Source reduction is fundamentally different and more desirable than waste management or pollution control. Pollution prevention also includes other practices that increase efficiency in the use of energy, water,
Protecting the Public Health and Safety

or other natural resources, and protect our resource base through conservation. Practices include recycling, source reduction, and sustainable agriculture.


RCRA (pronounced "reck-rah") gave EPA the authority to control hazardous waste from "cradle-to-grave" including generation, transportation, treatment, storage, and disposal of hazardous waste. RCRA also set forth a framework for the management of non-hazardous solid wastes. The 1986 amendments to RCRA enabled EPA to address environmental problems that could result from underground tanks storing petroleum and other hazardous substances. RCRA focuses only on active and future facilities and does not address abandoned or historical sites (see CERCLA).

The 1984 Federal Hazardous and Solid Waste Amendments (HSWA, pronounced "hiss-wa") to RCRA requires phasing-out land disposal of hazardous waste. Some of the other mandates of this law include increased enforcement authority for EPA, more stringent hazardous waste management standards, and a comprehensive underground storage tank program.


The Safe Drinking Water Act protects the quality of drinking water in the U.S. This law focuses on all waters actually or potentially designated for drinking use, whether above or below ground. The Act authorized EPA to establish safe standards of purity and required all owners or operators of public water systems to comply with primary (health-related) standards. State governments, that assume this power from EPA, also encourage attainment of secondary standards (nuisance-related).

1.9.1.13 Superfund Amendments and Reauthorization Act (SARA) 42 U.S.C. 9601 et seq. (1986)

The Superfund Amendments and Reauthorization Act of 1986 reauthorized CERCLA to continue cleanup activities around the country. Several site-specific amendments, definitions, clarifications, and technical requirements were added to the legislation, including additional enforcement authorities. Title III of SARA also authorized the Emergency Planning and Community Right-to-Know Act (EPCRA).


The Toxic Substances Control Act of 1976 was enacted by Congress to test, regulate, and screen all chemicals produced or imported into the U.S. Many thousands of chemicals and their compounds are developed each year with unknown toxic or dangerous characteristics. To prevent tragic consequences, TSCA requires that any chemical that reaches the consumer market be tested for possible toxic effects prior to commercial manufacture. Any chemical that poses health and