THE UNIVERSITY OF ALBERTA

Demonstration of Quantitative Risk Assessment to Some Municipal Water Treatment Plant Processes

by

Shauna Mercer

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES AND RESEARCH

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE

OF Masters of Science

IN

Civil Engineering

EDMONTON, ALBERTA

Spring, 1988

ISBN 0-315-52764-1

THE UNIVERSITY OF ALBERTA

RELEASE FORM

NAME OF AUTHOR Shauna Mercer

TITLE OF THESIS Demonstration of Quantitative Risk Assessment to Some Municipal Water Treatment Plant Processes

DEGREE FOR WHICH THESIS WAS PRESENTED Masters of Science

YEAR THIS DEGREE GRANTED Spring, 1988

Permission is hereby granted to THE UNIVERSITY OF ALBERTA LIBRARY to reproduce single copies of this thesis and to lend or sell such copies for private, scholarly or scientific research purposes only.

The author reserves other publication rights, and neither the thesis nor extensive extracts from it may be printed or otherwise reproduced without the author's written permission.

(SIGNED) Shauna Mercer

PERMANENT ADDRESS:

#806 10101 Sask. Dr.
Edmonton, Alta.
T6E 4R6

DATED April 26 1988

THE UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research, for acceptance, a thesis entitled Application of Quantitative Risk Assessment to a Municipal Water Treatment Plant submitted by Shauna Mercer in partial fulfilment of the requirements for the degree of Masters of Science in Civil Engineering.

....

Supervisor

....

Daniel W. Smith

Date April 22, 1988

DISCLAIMER

This work represents an academic exercise for the purpose of evaluating a risk assessment methodology as part of the graduate degree requirements of the author. The specific findings of this investigation are provided for information only. The specific findings are not to be relied upon as the primary basis for implementing change or maintaining the status quo.

The author accepts no legal responsibility for any actions or inactions, whatsoever, founded upon the information provided in this thesis. Permission to use the material in this thesis is governed by the above conditions.

Dedicated to my father

John E. H. Mercer

ABSTRACT

Quantitative risk assessment has developed as a design tool for identifying hazards and managing risk. Risk consists of three separate elements: a scenario, the probability of the occurrence of the scenario, and the consequences of the scenario.

The first element of a risk assessment, developing the scenario, is a hazards identification stage [illegible] wing each element of a system in its operating and failed state, potential deviations in the system response are highlighted.

The probability of a failure scenario's occurrence requires the development of the failure rates for these elements through general data sources, plant operating data of similar facilites and plant specific data. The individual failure rates from each of these data sources are then combined using Bayes Theorem.

The consequence analysis considers the impact a particular scenario would have on employees or the public. By considering all three of these elements the risk for the facility can be compared with target values. For those events which have risk values exceeding target values, one of three elements must be altered so that the risk is reduced to below the target value.

Quantitative risk assessment was used to evaluate two aspects of a municipal water treatment plant. The first aspect was the risk the chlorine storage and feed unit posed to occupational health and safety. The second aspect was the risk of chlorination failing and resulting in an inadequately disinfected water being distributed to the public.

Potential hazards and corresponding scenarios were developed using the hazards and operability studies (HAZOP) technique. Established codes of practice, manufacturer's information and plant specific data were all combined using Bayes Theorem to develop the probability of occurrence for identified scenarios. The consequences of the scenarios were evaluated by considering exposure levels and times.

The application of the risk assessment technique to a municipal water treatment plant was useful. Although there were not any unexpected scenarios identified, the separation of a scenario into its elemental events identified inefficient or unacceptable procedures. The probability analysis verified the operating record of the plant. The consequence analysis indicated several practical methods which would considerably reduce the risk with minimal cost.

Acknowledgements

I am indepted to the operations and maintenance staff of the Rossdale Water Treament Plant. Their assistance, cooperation and honesty was appreciated.

I thank my supervisor, Dr. Hrudey, for his guidance and critical assessment of the study. I also thank Don Noot and Bob Andrews for their assistance with the graphics.

Lastly, I thank my family for their support during the course of this degree.

Table of Contents

Chapter Page

DISCLAIMER iv

ABSTRACT vi

Acknowledgements viii

List of Tables xv

List of Figures xvi

1. INTRODUCTION 1

2. QUANTIFYING RISK 4

2.1 Definitions 4

2.1.1 Risk and Hazard 4

2.1.2 Risk and Uncertainty 5

2.1.3 Probability and Frequency 5

2.1.4 Risk Analysis and Hazard Analysis 7

2.2 Quantitative Risk Analysis 7

2.3 Hazard Identification 8

2.3.1 Comparative Methods 9

2.3.2 Failure Modes and Effects Analysis (FMEA) 9

2.3.3 Hazard and Operability Studies (HAZOP) ..10

2.3.4 General Aspects of Hazard Identification 11

2.3.5 Members of the Hazard Identification Team 13

2.3.6 Components of the Hazard Identification .13

2.4 Scenario Development 14

2.4.1 Initiating Events and Damage States 15

2.4.2 Event Trees 15

2.4.3 Fault Trees 16

2.4.4 Comparing Event Trees and Fault Trees ...19

2.5 Frequency Analysis 21

2.6 Data Collection 22

2.6.1 Handling the Uncertainty in the Data 25

2.6.2 Combining the Data with Bayes Theorem ...26

2.7 Consequence Analysis 30

2.8 The Human Factor 32

2.8.1 Types of Errors 33

2.8.2 Predicting Human Errors 39

2.8.3 Determining the Error Rate 42

3. MANAGING RISK 44

3.1 Occupational Risks and Hazards 45

3.1.1 Fatal Accident Rate (FAR) 45

3.1.2 Cost/Benefit Analysis 47

3.2 Risks to the Public 48

3.2.1 Voluntary and Involuntary Risk 48

3.2.2 Cost/Benefit 49

3.2.3 Determining an Acceptable Level of Risk .50

3.3 Applying Target Values and Decision Making 56

3.3.1 Controlling Human Error 58

4. BENEFITS AND LIMITATIONS OF A QUANTITATIVE RISK ASSESSMENT 60

4.1 Data 61

4.1.1 Reliability of Data 61

4.1.2 Inaccuracy of Results 62

4.1.3 The Human Factor 63

4.1.4 The Necessity of a Full Assessment 64

4.2 Summary 65

5. APPLICATION OF A QUANTITATIVE RISK ASSESSMENT TO A WATER TREATMENT PLANT 66

5.1 Why do a Quantitative Risk Assessment? 66

5.2 Review of Water Treatment Plant 67

5.2.1 Raw Water Supply 68

5.2.2 Overview of the Water Treatment Plant ...70

5.2.3 Treatment Processes 70

6. CHLORINE FEED UNIT 86

6.1 Hazard Identification for the Chlorine System .86

6.2 Chemical and Physical Properties of Chlorine ..87

6.2.1 Volume-Temperature Effects 87

6.2.2 Density 89

6.2.3 Chemical Reactions 89

6.2.4 Toxicity 89

6.3 Equipment 90

6.3.1 The Chlorine Storage and Feed Unit 93

6.4 Review of Accidents 94

7. DEVELOPMENT OF SCENARIOS 98

7.1 Occupational Safety 98

7.1.1 Inititiating Events and Damage States ...98

7.1.2 The Hazardous Scenarios 100

7.1.3 The Injury Scenarios 121

7.2 Water Supply Contaminated 125

8. FREQUENCY ANALYSIS 131

8.1 Data Collection 131

8.1.1 Developing the Prior 131

8.1.2 Updating the Prior 133

8.1.3 Combining the Failure Rates 134

8.1.4 Example of Method 134

8.2 Frequency Analysis for Damage State Injury ...134

8.3 Contolled Release 135

8.3.1 Chlorine Headers Full of Liquid Chlorine 135

8.3.2 Handling Liquid Chlorine in the Lines ..146

8.4 Eductor Fouled 146

8.5 Chlorinator Flooded 148

8.5.1 Final Distribution for a Controlled Release Causing Injury 149

8.6 Injury From an Uncontrolled Release 149

8.6.1 Tonner Rupture 154

8.6.2 Tonner Valve Break 154

8.6.3 Fusible Plug 156

8.6.4 Header Break, Flexible Connectors and PVC Break 156

8.6.5 Uncontrolled Release Summary 156

8.6.6 Warning System 156

8.6.7 Injury Summary 162

8.7 Water Contamination Frequency Analysis 162

8.7.1 Major Leak, No Alarm 164

8.7.2 Liquid Chlorine in Headers, No High Vacuum Alarm 164

8.7.3 Chlorinator Floods, No Low Vacuum 165

8.7.4 Chlorine Solution Line Breaks 166

8.7.5 Run out of Chlorine 167

8.8 Summary of Frequency Analysis for Water Quality 168

8.9 Exterior Force 169

8.9.1 Airplane Crash 169

8.9.2 Environment 170

9. CONSCEQUENCE ANALYSIS 173

9.1 Exposure to Chlorine Gas 173

9.1.1 Controlled Release 173

9.1.2 Uncontrolled Release 175

9.2 Water Not Chlorinated 180

9.3 Exterior Force 182

10. MANAGING THE RISK 183

10.1 Injury Scenario 183

10.2 Contaminated Water Supply Scenario 187

11. DISCUSSION 190

11.1 Modifications Which Have Reduced Risk 192

11.2 Application of Risk Analysis at the Design Stage 200

12. CONCLUSIONS 203

REFERENCES 209

APPENDIX A.1 213

APPENDIX B.1 227

APPENDIX B.2 248

APPENDIX B.3 255

APPENDIX B.4 268

APPENDIX B.5 274

APPENDIX C.1 275

APPENDIX C.2 288

APPENDIX C.3 290

APPENDIX C.4 292

APPENDIX D.1 296

APPENDIX D.2 301

APPENDIX E.1 303

APPENDIX E.2 304

APPENDIX F 305

APPENDIX G 328

List of Tables

Table	Description	Page
2.1	Deviations and Application of HAZOP guide words..	12
2.2	The differences between fault trees and event trees..	20
2.3	Error rates for simple routine actions........	35
2.4	Expected error rates for operator action......	40
2.5	Expected error rates for operator intervention	41
3.1	Probability of death for involuntary risks....	51
3.2	Probability of death for commonly accepted risks..	52
3.3	Probability of death per person per annum.....	53
5.1	Maximum and reliable pumpage rates for plants 1, 2 & 3..	71
6.1	Physical and chemical properties of chlorine..	88
6.2	Recommended exposure limits for chlorine......	92
8.1	The expected failure rate o, with the prior and posterior density functions..................	141
8.2	The tabulation of o, p(o), L(E/o) used to calculate the posterior distribution p(o,L/E).....	142
B.1.1	Plants 1 and 2 combined flow rates..........	233
B.1.2	Extreme minimum and mean temperatures for Edmonton..	238
F.1.1	Activated carbon feeding rates.............	308

List of Figures

Figure	Description	Page
2.1a	A simplified event tree	17
2.1b	A simplified fault tree	18
2.2	The three formats used to express probability.	23
2.3	The effect of stress on operator performance..	43
5.1	Process diagram of the municipal water treatment plant	69
6.1	Process diagram of the chlorine storage and feed unit	91
7.1	Event tree diagram for a partial or complete loss of vacuum	104
7.2	Fault tree diagram for a partial or complete loss of vacuum	105
7.3a	Event tree for a vacuum line break between injector or storage room	106
7.3b	Event tree for a vacuum line break between injector or storage room	107
7.4	Fault tree diagram for a vacuum line break....	108
7.5	Event tree for the chlorine pressure falling in headers	111
7.6	Fault tree for chlorine pressure falling in headers	112
7.7	Event tree for a plugged chlorinator	116
7.8	Fault tree for a plugged chlorinator	117
7.9	Fault tree for liquid chlorine in the headers.	118
7.10	Event tree for an uncontrolled release	119
7.11	Fault tree for an uncontrolled release	120
7.12	Fault tree for a tonner rupture	122
7.13	Fault tree for the failure of a tonner valve.	123

7.14 Fault tree for the failure of a fusible plug. 124

7.15 Fault tree for a header break................ 126

7.16 Fault tree for a controlled release.......... 127

7.17 Fault tree for an uncontrolled release....... 129

7.18 Fault tree for the water not receiving chlorine.. 130

8.1 Prior distribution for a broken tonner eductor 139

8.2 Prior and posterior probability distributions for a broken tonner eductor...................... 145

8.3 Probability distribution for liquid chlorine in the headers.................................... 147

8.4 Probability distribution for a fouled injector 150

8.5 Probability distribution for a flooded chlorinator.. 151

8.6 Probability distribution for injury from a controlled release............................... 152

8.7 Probability distribution for an uncontrolle release.. 153

8.8 Probability distribution for a tonner rupture. 155

8.9 Probability distribution for a tonner valve break.. 157

8.10 Probability distribution for a fusible plug leak... 158

8.11 Probability distribution for a header break.. 159

8.12 Probability distribution for a flexible connector break................................. 160

8.13 Probability distribution of an injury from and uncontrolled release......................... 161

8.14 Probability distribution of the water not receiving chlorine.............................. 163

8.15 Probability distribution of complete plant destruction...................................... 172

9.1 Fault tree of improper isolation resulting in a leak.. 176

A.1 Construction of a tonner...................... 214

A.2 Construction of a chlorinator................. 222

B.1.1 Probability distribution for one tonner valve plugged.................................... 229

B.1.2 Probability distribution for the chlorine demand greater than four tonners.................. 234

B.1.3 Probability distribution for the chlorine demand greater than three tonners................. 235

B.1.4 Probability of an operator leaving three valves open during tonner change.................. 243

B.1.5 Probability of an operator connecting the flexible connector to the wrong valve............. 246

B.2.1 Probability of an explosion from cleaning chlorinators or piping with alcohol............... 249

B.2.2 Probability that an operator would expose himself to chlorine during a controlled release... 253

B.3.1 Probability of a water supply line rupture.. 256

B.3.2 Probability of the injector plugging........ 258

B.3.3 Probability of the discharge line plugging.. 259

B.3.4 Probability of the pressure regulating valve jamming open.............................. 262

B.3.5 Probability of the relief valve being jammed closed.. 264

B.3.6 Probability of the maintenance personnel not wearing breathing equipment during repairs........ 266

B.4.1 Probability of failing to close the isolation valve.................................. 272

C.1.1 Probability for failure of the hoist........ 275

C.1.2 Probability of a tonner collision........... 278

C.1.3 Probability of a tonner with a corroded valve being delivered to the plant................ 281

C.1.4 Probability of welding occurring in the storage room.................................. 285

C.3.1 Probability of a fusible plug melting....... 290

D.1.1 Probability of the failure of the leak alarm 296

F.1.1 Process diagram for the activated carbon feed unit.................................... 309

F.1.2 Process diagram for the addition of water to the activated carbon storage tank................. 310

F.1.3 The air sparger unit in the storage tank.... 311

F.1.4 Alarms and automatic shut down points for the activated carbon storage tank................. 313

F.1.5 Event tree describing the storage tank operation.................................... 319

F.1.6 Event tree diagram for the operation of the activated carbon pumps............................ 322

1. INTRODUCTION

The technique of quantitative risk assessment has become a popular tool for designers and reviewers to improve the safety and efficiency of modern, highly technical facilities. Whether it is used only to identify hazards or is fully developed to the stages of frequency and consequence analyses, it provides a mechanism for managing risk.

For most engineering designs, risk has been compensated for by applying safety factors. However complex systems with many interactions may end up with factors of safety below intended levels. In these instances, a quantitative risk analysis can provide a continuous review which can help to identify these hazards, and determine if adequate protection has been provided.

Risk is a term which has many different connotative definitions. Generally, it is associated with the chance of either being exposed to or harmed by a hazard. The exposure to the hazard may result in psychological, economic or physical damage. The technique of quantitative risk analysis provides an organized method by which hazards can be identified and solutions for the elimination or reduction o these hazards evaluated. This process, which has been developed for the nuclear and chemical process industries was evaluated for application to a water treatment plant process.

Risk analysis has often been associated with the detection of rare events that would have devastating consequences should they occur. The identification and prevention of a catastrophic accident makes the benefits of risk analysis clear. However, there are additional ways in which the technique can benefit the overall design and operational procedures within a system. A risk analysis forces the designer to consider the system under every conceivable operating condition. This type of exhaustive review can highlight weak spots or design deficiencies whether the consequences would be catastrophic or not. The assessor can then determine if the cost of either reducing or eliminating the consequences of these deficiencies is worth the benefit. The generation of alternate procedures or new processes to reduce these hazards is encouraged and often results in overall increases in plant efficiency.

There are three distinct stages of a quantitative risk analysis including: the identification of hazards, a frequency analysis and a consequence analysis. There are differing opinions on how detailed each of these stages should be. However for an experienced and knowledgable asessment team, the detail is determined by the complexity of the design and the type of risk posed by the hazard, rather than by a preset policy. In some instances, only the first stage is required. However for some sections of a facility, a full examination with all three stages may be performed.

The technique of quantitative risk analysis was reviewed and then applied to a municipal water treatment plant. The effectiveness of the technique for identifying and reducing potential hazards which affect employee safety and the quality of water produced was evaluated.

2. QUANTIFYING RISK

2.1 Definitions

When any topic is to be discussed it is important that the definition of each descriptive word used be clearly understood. This is particularly true for the process of risk analysis since many of the descriptive words are often used as synonyms in everyday language, or have strong connotative meanings which are normally substituted for their denotative meanings.

2.1.1 Risk and Hazard

Much of the confusion begins with the words 'risk' and 'hazard'. The denotative definition of risk is, 'the possibility of loss or injury', and hazard is, 'a source of danger' (Funk and Wagnall, 1980). The confusion arises from the close link between the two words. Kaplan and Garrick (1981) indicate that risk can be related to hazards since risk is the chance or probability of being harmed or suffering loss from the source of danger. The chance of being harmed can be varied by the degrees of protection provided. Kaplan and Garrick (1981) refer to the degree of protection as 'safeguards' and present the following relationship between risk, hazard and safeguards;

$$\text{risk} = \frac{\text{hazards}}{\text{safeguards}}$$

As the authors indicate, this equation implies some important features about risk. Unless an infinite number of flawless safeguards are introduced, risk can never be equivalent to zero. Intuitively, people know this is true, but the equation clearly states this.

Safeguards include the concept of awareness. The awareness of a potential hazard or how a hazard can cause an injury may reduce the risk through simple avoidance (Kaplan and Garrick, 1981). The introduction of safeguards and reduction of risk brings associated with a cost because safeguards are rarely free.

2.1.2 Risk and Uncertainty

Along with hazards, the concept of uncertainty is closely connected with risk. The denotative definition for risk includes, 'the probability'. Intuitively probability implies uncertainty. Where there cannot be a definite solution or answer, we express our degree of belief in a particular outcome in the form of probability. However, on its own, this uncertainty does not equate to risk. Risk is the uncertainty associated with some type of loss or injury. Kaplan and Garrick (1981) have proposed the following relationship:

$$\text{risk} = \text{uncertainty} + \text{damage}.$$

2.1.3 Probability and Frequency

While probability and frequency are often used interchangeably, for risk analysis they are not equivalent terms. Frequency is used to express the results of an experiment. The results are generated by repeating an experiment a number of times and then reporting the outcome. The results are measurable numbers.

Probability is not a hard, measurable number, but indicates a state of knowledge or belief. Given an uncertain event, it allows for the expression of one's belief in the occurrence of that event. Given two events, probability can express the likelihood of occurrence of each event allowing for a comparision between the two events (Kaplan and Garrick, 1981).

Probability Scale

Where confusion often arises is in the numerical expression of probability since it is defined by the frequency scale. 'If an event is certain to occur, it is defined as having a probability equal to 1.0. If the event is certain not to occur, it is given a probability of 0.0. If a person believes that an event has an equal chance of occurring as not occurring, it is assigned a probability of 0.5' (Kaplan, 1986). The remainder of the scale is defined using an example of Kaplan and Garrick's (1981). Tickets are numbered 1 to 1000. When asked if a number drawn is numbered 632 or less, a person has a certain degree of confidence about this event's occurrence. This would normally be expressed as a probability of 0.632. Using this form of frequency, the probability scale is defined from 0.0 to 1.0.

2.1.4 Risk Analysis and Hazard Analysis

Although these two titles appear to refer to the same type of analysis, many authors draw definite distinctions between them. After reviewing the definitions and distinctions made by various authors, it appears that hazard analysis is the qualitative portion of risk analysis.

Lowe (1984) discusses the merits of hazard analysis over risk analysis. He observes hazard analysis to involve the identification of hazards and the assessment of control measures or safeguards. However, he determines that risk analysis, which only serves to give a number indicating total risk is not useful and wastes resources. Joschek (1983) also identifies quantitative risk analysis as a waste of resources and manpower. Both authors suggest that the initial stage of a risk analysis, which is hazard identification and scenario development, should be the most important part of the review. Other authors agree that a complete analysis is not often required (Kletz, 1982; Kaplan, 1986). However, there are instances where a quantitative evaluation of the risk is necesary to allow comparisons so that the risk can be managed.

2.2 Quantitative Risk Analysis

For all risk assessments, there are three questions answered about a proposed design or existing plant. (Kaplan and Garrick, 1981; Kletz, 1982; Kazarians et al., 1985). These are:

1. What can go wrong?
2. How likely is it to happen?
3. If it does occur, what are the consequences?

The technique used to solve these questions generates a solution set consisting of: a set of scenarios, their probability of occurrence and the consequences of the scenarios. Kaplan and Garrick (1981) define risk as being equivalent to the solution set $\{s_i, p_i, x_i\}$ where;

s_i = scenario of event i

p_i = probability of event i

x_i = consequence of event i

2.3 Hazard Identification

Identification of hazards is commonly accepted as the most important stage of a quantitative risk assessment. However, identifiying a hazard does not necessarily control the hazard. 'Having the knowledge does not always equate to use of the knowledge' (Pasman, 1985).

Over the last ten years, several organized formal techniques have been developed to assist designers in the identification of hazards. These techniques are an attempt to ensure that the list of hazards will be complete. These techniques include comparative methods, failure mode and effect analysis, and hazard an operability studies (HAZOP) (Pasman, 1985). With these methods, an existing facility or proposed design is reviewed on a line by line, item by item basis.

2.3.1 Comparative Methods

This technique of hazard idenfification is actually the manner in which all designers have historically developed new facilities. Engineering codes, design standards and accepted engineering practice are used as guides during the design phase and then as examples for comparison with the final design. With new technologies, some of these standards and codes must be questioned during the design to determine if they will apply under new circumstances (Pasman, 1985).

Comparative methods employs historical resources by using checklists. The checklists represent known failure modes for a particular design, which the design under review must be checked against (Cullen, 1985). These checklists have been used to develop Hazard Indices which are a ranking of the hazards with a comparison to established Hazard Indexes such as those developed by DOW Chemical and MOND (Cullen, 1985). This method ensures that company standards and practices have been upheld and followed adequately. Comparative methods are often used as a starting point for hazard identification, and they may be used in conjunction with other methods.

2.3.2 Failure Modes and Effects Analysis (FMEA)

This technique is a rather informal approach to the identification of hazards. As the analysis progresses through each item, all possible failure modes and their consequences are identified (Cullen, 1985). Under normal operating conditions, the system is assumed to be responding in its intended manner. Each item is then presumed to be under a stressful condition, and its expected response is evaluated.

ıure modes and effects analysis usually results in an extremely detailed analysis so it is normally performed only on critical aspects in the design that have been identified by other methods as potential hazards.

2.3.3 Hazard and Operability Studies (HAZOP)

Hazard and operability studies were initially developed by Imperial Chemicals Industries (Lawley, 1974). HAZOP is a formal, structured method which systematically reviews a system based on the premise that problems arise only under stressful or abnormal operating conditions. In order to identify hazards, six guide words are used to analyse each section of a proposed or existing design. The guide words are intended to inspire questions and allow free thinking within the analysis team, while maintaining an organized and comprehensive review of the design. Maintaining this systematic approach is important to ensure all of the hazards are identified.

The six guide words used to stimulate thoughts within the HAZOP team are, NONE, MORE OF, LESS OF, PART OF, MORE THAN, and OTHER THAN (Kletz, 1986). Each word represents a stressful or abnormal condition which the process or system could be exposed to. The application of the guide words is shown in Table 2.1.

Proper application of the guide words ensures that all conditions are reviewed including deviations in normal plant operations, start-up and shut-downs, plant materials and equipment, and provisions for safety and maintenance (Lawley, 1974). As these deviations are generated, potential causes and consequences of these events are also considered. For problems that can be easily and obviously corrected, the solution can be implemented and the study is considered complete. Kletz (1986) and Lawley (1974) both provide detailed examples of the HAZOP process.

2.3.4 General Aspects of Hazard Identification

Both HAZOP and FMEA describe or highlight hazards that will occur under a stressful situation. They assume that proper engineering standards and codes will have been used and followed. Therefore, they really incorporate the technique of comparative methods into their structure. To ensure that all hazards are recognized as such, it is important that the Hazard Identification team have members who are knowledgeable about the process under evaluation.

Table 2.1 Deviations and Applications of the HAZOP guide words.

(modified from Kletz, 1986)

Guide Word	Deviation
NONE	No flow in the designed direction (e.g. no forward flow)
MORE OF	More of any relevant physical property (e.g. higher temperature)
LESS OF	Less of any relevant Physical Property (e.g. lower temperature)
PART OF	System compostion different than it should be (e.g. ratio of components)
MORE THAN	More components present in the system (e.g. impurities)
OTHER THAN	Events which occur apart from normal operation (e.g. start up or shut down)

2.3.5 Members of the Hazard Identification Team

Depending on whether an existing plant or a proposed design is being analysed, the hazard identification team will vary slightly. For both types of analyses all aspects of the facility must be covered. In the case of a process plant there should be representatives from the design team, operations, maintenance, instrumentation, a chemistry representative, and an independent chairman to oversee the progression of the analysis (Kletz, 1986). By having a broad knowledge base, each area within the facility is covered and biases are eliminated.

2.3.6 Components of the Hazard Identification

Hazards will arise from two areas, either the materials or the new equipment being used. For any type of process plant, it is critical that all pertinent information about all of the chemicals used at the facility be known and understood. This includes the physical and chemical properties, toxicological and biological data, reaction parameters, thermodynamics, flammability and explosion limits and any other kinetic properties (Pasman, 1985; Kazarians et al., 1985). This information provides the basis for the hazard identification.

All details of the operating equipment, the operating conditions and layout of the equipment must be known. Because a hazard in one area could potentially create a hazard in an adjacent area these interactions must be considered (Kazarians et al., 1985). The effect of outside forces on the equipment must also be considered. These forces include severe storms, seismic activity, airplane crashes and other external forces.

2.4 Scenario Development

Once a hazard has been identified, whether it be through the approach of HAZOP or one of the other methods, the possible mechanisms by which the hazardous situation can be realized must be investigated (Kazarians et al., 1985). All of the approaches rely on the imagination of the review team. There can be a temptation to eliminate a potential scenario because of the extremely low likelihood that it would occur. This temptation should be resisted, because other stages of the assessment will indicate the importance of the scenario.

Scenarios can be formally developed using logic diagrams. These diagrams take the form of event trees or fault trees. For very complex analysis, a combination of the diagrams is often used with one diagram giving the overall system interaction and the more detailed sections being described by the alternate technique. To begin the diagra both the initiating events and damage states must be defined.

2.4.1 Initiating Events and Damage States

From the identification of hazards, events which alter the normal operating routine within a system are identified. As the event is propagated throughout the system each section has a particular response. If the event has been planned for in the design, the response usually involves the activation of a safety device or an alternate mechanism is tripped to handle the stressful condition.

If the e\ent has not been planned for, the abnormal condition would continue through the system until some kind of end state has been reached. An event which alters the normal operating routine or creates the stressful condition is an initiating event (Kazarians et al., 1985). The final condition that the system ends up in, depending on how the initiating event has affected the system, is the damage state.

The damage states are defined prior to beginning an analysis and cover all possible ranges from a stable system to complete destruction. defining the initiating events and damage states, the beginning and end points of the logic diagrams are defined (Kazarians et al., 1985).

2.4.2 Event Trees

Event trees begin with an initiating event and systematically follow the effects of the induced stress on the system (Fig. 2.1a) (Schrieber, 1982). Each event that occurs in response to the initiating event is clearly defined in two conditions. The first condition is a successful response, when it has reacted in its designed and intended manner. The second condition is a failure response, in which case the correct response has not occurred. These two separate conditions result in two new pathways in which the next event for each pathway can be analysed in a similar manner. The process of considering each subsequent response in both its success and failed condition continues until one of the damage states has been reached.

2.4.3 Fault Trees

Fault trees provide an alternate way of organizing the logical sequence of events in a scenario. This type of logic diagram differs from an event tree in that it starts with the damage state and then progresses backwards through all possible events which could have resulted in the preceding event. The process continues until the initiating event has been found (Fig. 2.1b) (Schrieber, 1982).

The fault tree is set up using Boolean logical 'AND' and 'OR' gates. The 'AND' gate signifies that the probabilities for the events involved in that gate are to be multiplied. The 'OR' gate signifies that the probabilities for the events involved are to be added. This logic can be continued throughout the fault tree until the final probability distribution for a particular event has been calculated.

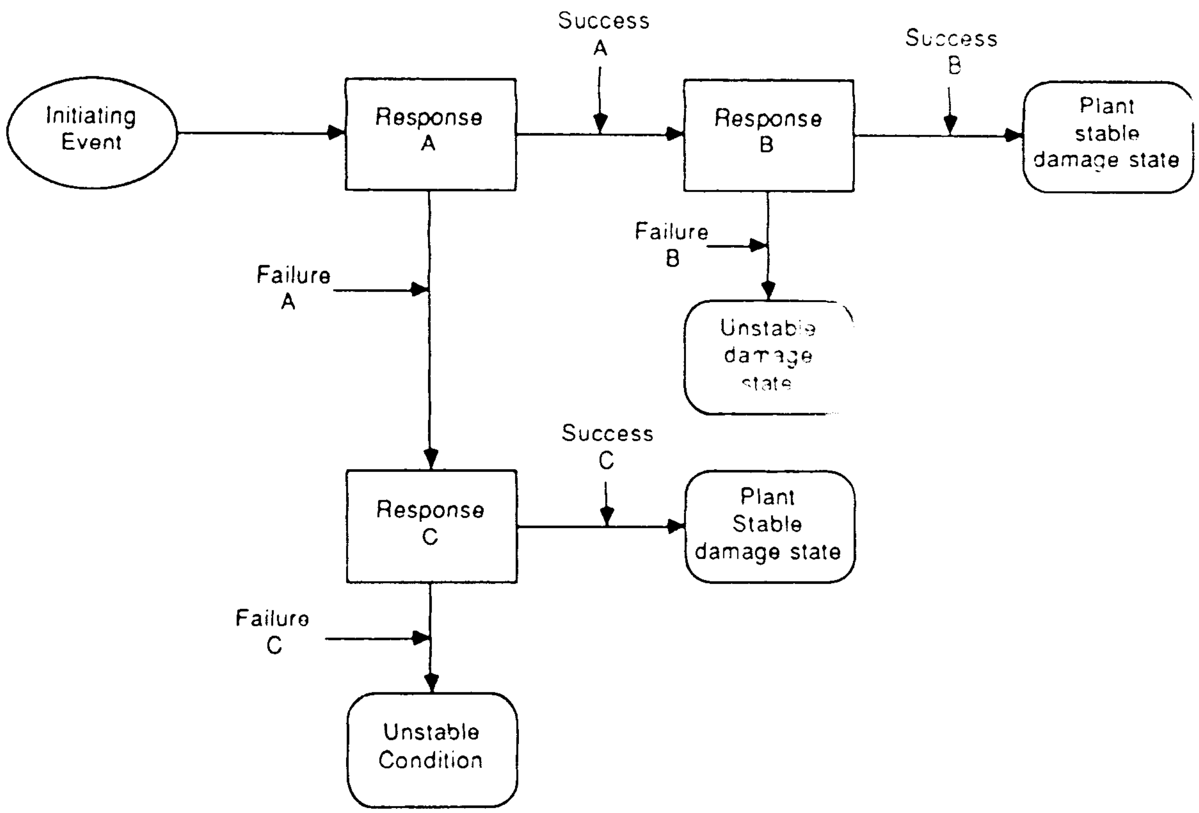
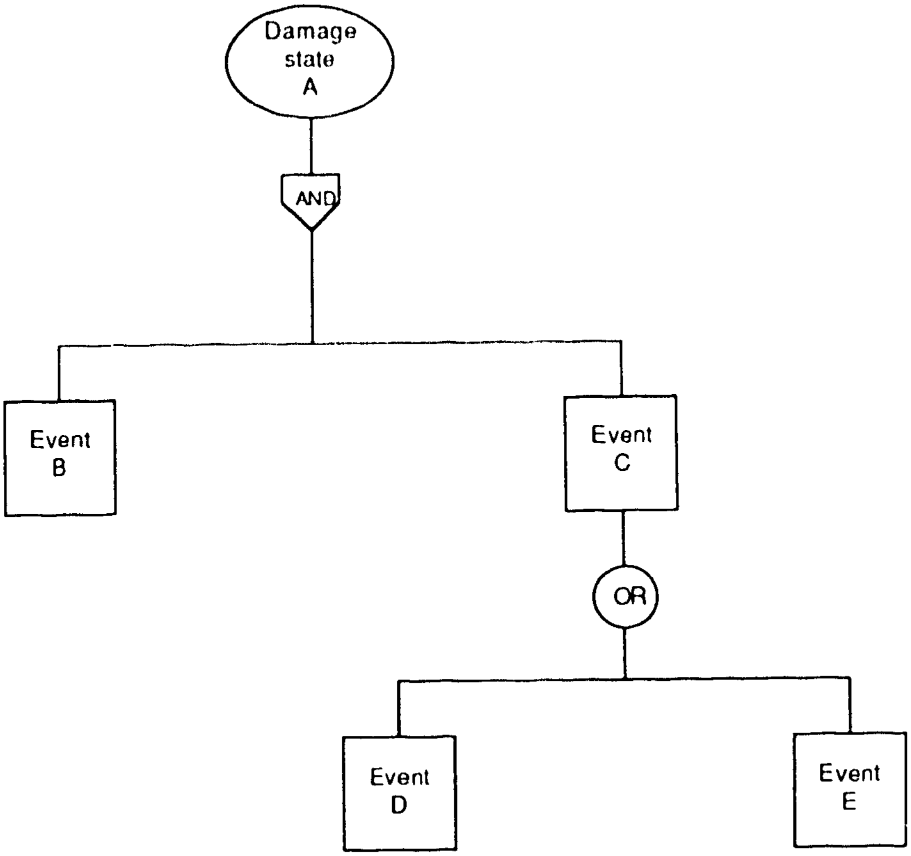


Figure 2.1a A simplified event tree



P(A) = P(B) x P(C)

where: P(C) = P(D) + P(E)

Figure 2.1b A simplified fault tree

2.4.4 Comparing Event Trees and Fault Trees

In essence, fault trees and event trees should produce the same logical scenarios. However, there are differences in the development of the two trees which may make one preferable to the other. Table 2.2 presents a comparison of the two logic diagrams.

Kaplan (1985) clearly prefers the event tree particularly for its implied time dimension. The tree ends with the damage states which seemingly makes the analysis more complete since both stable and complete destruction scenarios are developed. A clear pathway from the initiating event, through subsequent events resulting in a particular damage is clearly shown. Each pathway for each damage state is obvious.

The fault tree logic is used by most advocates of the HAZOP and hazard analysis (HAZAN) technique (Kletz, 1985). By using a fault tree only damage states which are of concern need to be considered. This can be a much more effective use of time and resources.

While some authors advocate one approach over the other, within a complex analysis a combination of both fault trees and event trees is usually necessary to clearly represent the possible sequences of events.

Table 2.2 The differences between fault trees and event trees (modified from Kaplan, 1986).

Fault Tree	Event Tree
Single end state	All end states
Proceeds backward from end state	Proceeds forward from initiating event
Scenarios not visible	Scenarios visible as paths
Does not have time dimension	Includes time dimension
Uses Boolean logic	Logic controlled by user

2.5 Frequency Analysis

The second stage of clearly defining the risk within a system is developing the frequencies and probabilities for the scenarios developed in the hazard indentification stage. The frequency analysis is important for it gives the analyst the first indication of which scenarios have a higher likelihood of occurrence, and therefore which may require greater attention.

Frequencies and probabilites have been clearly defined as two distinct ideas. This distinction allows the development of three different formats by which the likelihood of an event can be expressed. The first format is in the form of a probability number representing the state of confidence about the likelihood of the event's occurrence. The graphical distribution which represents this probability (p_i) is indicated in Figure 2.2. The second format is used when there is more information about the event, and in particular the frequency of occurrence of the event is known. Therefore the state of confidence is expressed as a frequency or $p_i = f_i$. The final format develops the idea of having uncertainty about the frequency which was known in format 2. The state of confidence can be shown as $p_i(f_i)$. These three formats allow for an expresson of confidence in the data collected (Kaplan, 1986).

2.6 Data Collection

There are three basic sources from which data can be collected and then developed. Type I data is from operational experience. This data is only applicable in an analysis of an existing plant. Type II data is gathered from operating experience at similar plants. Finally type III data makes use of expert judgement and equipment design (Mosleh et al., 1986). All of the data sources provide information on failure rates and exposure or success rates.

Potential causes of component failure include: testing, maintenance, human error, and environmental factors such as storms, earthquakes etc. (Kazarians et al., 1987). There should be some failure rate data from types I and II data on the dependent and independent component, testing and maintence failures. More judgement is required in predicting the effects of human error and the environment which use type III data.

Type I Data

Collection of applicable plant specific data can be the most difficult stage of data collection, however the results it provides are the most meaningful. An ideal plant specific data base would consist of failure and success rate data for all systems, parts of systems and equipment within the plant. The success data is in the form of total exposure or operating time before a failure occurs (Mosleh et al., 1986). This data is hard to collect and evaluate, because it

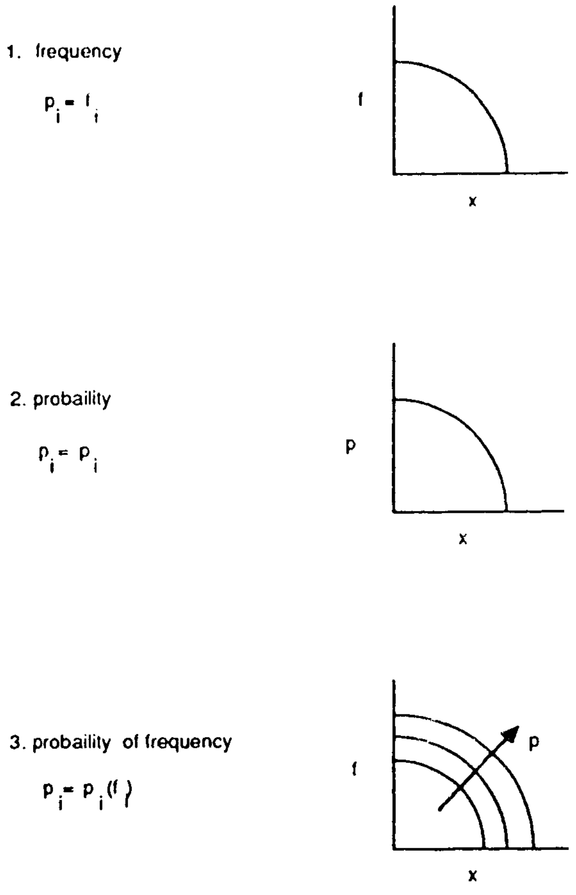


Figure 2.2 The three formats used to express probability (modified from Kaplan, 1986).

does not exist in many plants. What does exist is usually found within the maintenance records which usually give the minimum information about the work performed. For duplicated or even triplicated systems, the total operating time for each unit will vary. Meters may be changed or reset without the cumulative time being recorded (Mosleh et al., 1986). The difficulties in determining the failure rates also exists for the total operating exposure time. When small component changes are performed, they are often not recorded. Judgement is often required to determine if some maintenance work even constitutes a failure.

Within an operating plant the lack of data can be compensated for through the knowledge and memories of the operating personnel. The analyst must be very objective about this source of data, and look for a correlation amongst the information gathered from the various personnel (Mosleh et al., 1986).

Type II and Type III Data

These data sources should be considered together, because they are often developed at the same time. Type II data is normally much easier to collect, however it is often difficult to evaluate the applicability of the information. For those industries which have rigorously employed quantititative risk assessment in their designs, the information on system and equipment failure and success rates is being steadily collected. This data must then be reviewed for its applicability to the particular assessment being performed. Such factors as operating conditions, variations in environment and the definition of a failure, must all be considered by the analyst (Mosleh et al., 1986).

Type III data can determine the applicability of the type II data. Through the application of engineering knowledge, the effects of the operating condition on the failure rate can be judged. This additional information can then be applied to the operating knowledge of existing plants and the data from other similar plants to determine what probability values should be used to describe the particular success or failure rate.

2.6.1 Handling the Uncertainty in the Data

One of the main criticisms of a quantitative risk assessment is that the frequency values generated are only estimates and they often vary by an order of magnitude in both directions (Joschek, 1983). Because of the difficulties in data collection the uncertainty is not surprising. However there are methods within the risk assessment process which can handle this uncertainty (Kaplan, 1986).

Initially it must be determined which sources of data are available for the particular system. For many systems it is necessary to break the system into small sections for which there is data of some form. These smaller sections are referred to as elemental events. Elemental events consist of hardware failures, maintenance actions, human errors, and the initiating events (Kaplan, 1986).

Once the data for the elemental events has been collected, probability values describing failure frequencies can be developed. These values are developed using the third format (Fig. 2.2) for expressing the likelihood of a failure. The data collected will give some indication of the failure frequency, however there is uncertainty as to the precise value of this frequency. A probability distribution is assigned to this frequency. This initial distribution varies from a uniform distribution to a normal distribution depending on the confidence the analyst has in the data. In this way, a quantitative risk assessment expresses the uncertainty associated with the system whether the uncertainty is large or small.

2.6.2 Combining the Data with Bayes Theorem

For each elemental event, there will be either two or three sets of data developed, one from each source. Not only may the failure frequencies developed from each source vary, but the uncertainty associated with each data set may also vary. The technique which has been developed to combine this data into meaningful and useful information is Bayes Theorem.

Bayes Theorem

Bayes Theorem is a mathematical approach which allows for the addition of new information to an existing probability distribution representing our current state of knowledge. The existing probability distribution is termed the 'prior'. When new information is provided, the prior must be updated, which is done with a correction factor to give the 'posterior' distribution (Kazarians et al., 1985).

$$P(A/B) = \frac{P(A)\,P(B/A)}{P(B)}$$

$$P(\phi_i\,,\,L(E/\phi_i) = \frac{P(\phi_i)\,L(E/\phi_i)}{\sum_{i=1}^{N} P(\phi_i)\,L(E/\phi_i)}$$

$P(\phi)$ = prior distribution

$P(\phi, L/E)$ = posterior distribution

L/E = likelihood function

ϕ , I=1,2,...,N possible discrete values of ϕ

Bayes Theorem is based on the theory of conditional probabilities. Conditional probabilities are read in the following manner;

p(A)=probability of A

p(B)=probability of B

p(A/B)=probability of A given B

p(B/A)=probability of B given A

Applying Bayes Theorem

The initial step in applying Bayes Theorem is to develop a prior distribution. For the elemental events, the prior distribution is normally established from type II and III data. Depending on the confidence the analyst has in the data, the prior can take on many forms. If there is absolutely no information on the failure rate for an elemental event, then it is appropriate that the prior be represented as a uniform distribution, going from 0.0 to 1.0, and having an area of 1.0. The form of the numerical scale derived for probability requires that the area described by the curve must always be equal to 1.0.

If there is some information which is consistent throughout the literature and data collected, a normal distribution may be appropriate to describe the prior. The standard deviation represents the consistency of different data sources. If the information is inconsistent and varies considerably, a log-normal distribution may be more appropriate (Mosleh et al., 1986).

Updating the Prior

When there is additonal information available from a source other than that used to determine the prior, Bayes Theorem is implemented to update the prior. The additional information often called evidence, is placed in the form of either a poisson distribution or a binomial distribution depending on the nature of the elemental event being considered.

Definitions:

Poisson Distribtion

'if an event occurs with a constant rate R, the probability of observing K events in the time interval T is given by a Poisson distribution' (Kazarians et al., 1985);

$$P(K/T,R) = \frac{(R \times T)^{K}}{K!} \times e^{-KT}$$

Binomial Distribution

'if an event occurs with constant probability P on each trial, the probability of observing K events in N trials is given by a binomial distribution(Kazarians et al., 1985);

$$P(K/N,P) = \frac{N!}{K!\,(N-K)!} \times P^{K} \times (1-P)^{(N-K)}$$

Therefore the poisson distribution is used for those events that are continuous over time, such as a pump that runs continuously. The binomial distribution is used for events that are discontinuous such as the start up of a pump or disconnection of a hose.

The prior distribution determines the range over which R or P is considered. Evaluating the posterior distribution then only involves mathematical calculations. The prior is subdivided into small areas, each being associated with a particular R or P. Using the appropriate equation, either the binomial or poisson, the probability of observing a failure, knowing the evidence, at the particular R or P is calculated. This is equivalent to calculating the probability of B given A in a conditional probability. To complete Bayes Theorem, the P(R) and P(K/T,R) (or P(P) and P(K/N,P)) are multiplied and then summed over all R (or P). Each multiplied value is then divided by this summation. The final probabilities represent the posterior probability distribution for the given R or P (Mosleh et al., 1986).

Combining the Probabilities of Elemental Events

Once the posterior distributions have been established for the elemental events, they must be combined to give the final liklelihood values. In order to properly combine the probability distributions, a fault tree rather than an event tree is necessary to describe the combination of elemental events which can lead to the outcome of interest.

2.7 Consequence Analysis

This is the stage in the risk analysis which often determines how the risk will be managed. While the frequency of occurrence of a scenario is very important, if the consequence of that scenario is relatively insignificant, the analyst may choose to accept the risk even if the frequency is high. Freeman et al. (1986) recommends that consequence analysis should follow the identification of hazards and scenerio development. The frequency analysis should only be developed if the consequences warrant. As the authors recognized, an important part of doing a consequence analysis initially is determining which events are possible. Without a strict definition to limit the scope of the analysis, time and resources could be wasted on determining the consequences for imaginary and impossible events (Freeman et al., 1986).

Whether the consequence analysis is done at the initial stage or after the development of the scenarios and frequencies the key factors in determining the effects on people and the environment are the same. In the case of a chemical release, several factors must be clearly defined. The chemical's condition including toxicity, pressure, temperature, physical state, vapour pressure, and the expected quantity of chemical released must be known. Whether the release originates from a spill or a point source must also be defined. A clear representation of the release area should be given so that dispersion conditions can be determined. This includes the presence of dykes or retaining walls, ventilation units, or other chemical storage units. The possibility of one hazard interacting with other units in the area should have been developed as one of the hazards, however a complete review during the consequence analysis ensures that this type of event is not overlooked (Freeman et al., 1986).

Once the release has been defined, the potential for injury to either operational personnel or a member of the public must be evaluated. Injury to an operator could result from asphyxiation from a gas cloud or toxic fumes, a flammable chemical exploding or burning, or the collapse of a structure that was inadequately designed or weakened by the chemical release. The presence of the operator within the affected area must be predicted. This may reflect the regular inspection routine of the operator, or it may be an emergency response situation. In either case, the operator or other personnel who are at greatest risk must always be the individuals considered (Lawley et al., 1985).

For the public at large, most scenarios that result in a toxic cloud or an explosion and fire situation will produce consequences of concern. For these scenarios, downwind dispersion analysis must be conducted to determine the full impact of a release (Freeman et al., 1986). Several sophisticated modelling programs have been developed. However all would require a complete description of the problem to fully evaluate the downwind effects.

2.8 The Human Factor

Gathering reliable, applicable failure rate data is one of the difficulties in developing a quantitative risk assessment. Some critics believe that this factor alone destroys the credibility of a quantitative risk assessment. They would argue that established engineering practice should adequately account for safety. 80 to 90% of all accidents or errors are usually attributed to human error which the designer cannot control according to Joschek

(1983).

However, there has been a shift in the responsbility for accidents from the operational level to the design level. This shift has resulted from a realization that it is natural for human beings to make mistakes. Consequently, designers must compensate for this reality rather than trying to change the nature of the human being. Quantitative risk assessment is useful for identifying those areas which cannot tolerate human error. Initially risk assessment must determine where errors can occur, so that corrective design steps can be taken if necessary.

2.8.1 Types of Errors

Forgetfulness

By reviewing accidents that have been attributed to human error, analysts have developed different categories which describe why human errors occur. The first category of errors is usually attributed to a moment of forgetfulness (Kletz, 1987). These errors result from boring or repetitive tasks (Rasmussen, 1987). This type of error occurs when a person becomes too familiar with the particular job. The routine becomes automatic and the human being no longer concentrates on the task allowing his body to proceed without concentrating on each stage of the task. Many of these mundane repetitive tasks have been replaced by machines. Unfortunately, for some procedures this solution is not possible. Designers may suggest that better training would reduce these errors. On the contrary, these errors occur because the person is well trained and finds the action routine (Kletz, 1987). The errors will always occur, so it is up to the designer to determine if the system can tolerate the error. If not, system changes may be necessary.

To determine the error tolerance of the system the techniques developed for hazard identification can be used. Scenarios which require operational input can be reviewed, and the consequences of incorrect action or no action can be determined. For standard, routine events, human error rates have been developed (Table 2.3). These rates are assumed to be caused by a lapse in concentration.

Accidents from Lack of Training

Accidents which are the result of a loss of concentration cannot be removed through training, but some accidents can be reduced by training. These types of accidents are related to the increase in technology and machinery within industries. Automation has altered the role of the operator, removing some of the routine repetitive tasks, and replacing them with problem solving, decision making jobs (Rasmussen, 1987). Accidents or mistakes often occur because of an incorrect diagnosis.

Table 2.3. Error rates for simple, routine actions.

(modified from Kletz, 1986).

Failure Rate	Task
1 in 1	Complex Action Required
1 in 10	Busy Control Room with other alarms
1 in 100	Quiet Control Room
1 in 1000	Valve to be closed immediately below the alarm

'Human variability in problem solving may allow a stable situation to deviate outside acceptable limits or the human adaptability may not be able to cope with variations or abnormal occurrences in the routine' (Rasmussen, 1987).

The present method of dealing with these errors is to prepare a procedure outlining the steps to be taken in the event of a particular scenario. Initially the scenario must be recognized from the particular initiating event and there may be several scenarios which result in the same event. Without a correct understanding of the event, carefully prepared procedures are useless because they may be incorrectly applied (Kletz, 1987).

There are three ways an operator can assess and then correct a developing situation. One way is by having proper training and an understanding of the system so that a correct diagnosis is made (Kletz, 1987). The second method is from experience. This situation can be both positive and negative but the accurate diagnosis of the event depends on the event being the same as the previous one. The third way is through a trial and error process which is usually the most common one (Rasmussen, 1987).

The trial and error process is really the testing of a hypothesis about the cause of a deviation in the system. As with any experimental hypothesis, it can be wrong, which may result in an accident which is attributed to human error. Rasmussen (1987) points out that designers are placing the operator in an unrealistic situation, since they are required to perform a thought experiment, then diagnose the hypothesis and consequences correctly. Often this is performed without difficulty, however in crisis situations undesirable diagnosis and response can arise.

Since there will always be deviations in the normal operation of the plant, operational personnel will continue to make operating decisions. To ensure the maximum accuracy in these decisions, there must be adequate training and a system that is sufficiently error tolerant to allow for corrections should an incorrect decision be made. A quantitative risk assessment can be used to ensure that there is a complete understanding of the system, and that those indicators used to diagnose the operating condition of the plant are not misleading, redundant, or confusing. Making an error or mistake is often the most effective way of learning and a very natural way of learning. Therefore, systems must be able to tolerate an incorrect decision so that it is not a deadly one (Rasmussen, 1987).

Accidents caused by Lack of Ability

These types of human errors are the direct result of ignoring the functional limits of a human being. An operator may be required to perform a task that is beyond either his physical or mental ability (Kletz, 1987). This does not imply that the person is below average in either aspect, but rather the request requires a performance far beyond what an average person can handle.

Physical accidents are usually a result of poor design that does not consider a human's limits. Obvious situations involve inadequate lifting apparatus or poorly positioned benches and piping. Bell (1987) has developed an analytical technique, referred to as task analysis, to determine the effects of the environment, organization, economic, management and ergonomics on a particular job. The analyst performs the task himself as part of the task analysis. This type of personal experience would be very valuable to a designer, however it is not always practical. The hazard identification stage should pinpoint these types of potential accidents (Kletz, 1987).

Exceeding the mental capacity of an individual is easy , particularly with the use of computers. While an accident scenario is developing, warning signals begin to sound. If the scenario develops very rapidly, these indicators may all be sounding at once. This can cause an information overload for the operator. For a system with computer alarms, the effect can be overwhelming. A natural response under such a condition is to do nothing, since the operator cannot determine what needs to be done (Kletz, 1987). While safety systems and warning systems are important, the effect of a major accident and the reaction to these systems must be evaluated.

2.8.2 Predicting Human Errors

Operator responses can be classified as an action or intervention response. There are different factors affecting the error rate associated with each type of reponse. An operator action response, involves a task which the person performs as part of his daily routine. Errors coming under operator action would be redundancy errors or errors from excessive demand on the person. Operator intervention, requires that the operator assess a particular situation and then take corrective action. Failure because of inadequate training usually occur with an operator intervention scenario.

Operator action errors depend on the type of task required (Table 2.4) (Parvin, 1985). For these types of errors, it is assumed that there are not any time constraints and that stress is at a minimum.

Operator intervention errors are directly related to the time allowed for response, and the degree of stress the person experiences (Table 2.5). Factors which affect the stress level include the anxiety, time, quantity of information and distractions. Anxiety may result from a physical danger, or perhaps the fear of making a mistake resulting in a reprimand. Time is a key factor, with the relationship of response time being directly related to the time available. If too much information is provided, a person may seek confirmation, or become confused.

Table 2.4. Expected error rates for operator action. (modified from Parvin, 1985).

Error Rate	Operator Action
1 in 4	Complicated, non-routine
1 in 10	Non-routine, other duties at same time
1 in 100	Routine, requires care
1 in 1000	Routine, simple
1 in 10,000 to 1 in 100,000	Simplest possible action

Table 2.5. Expected error rates for operator intervention. (modified from Parvin, 1985).

Time for Action (min)	Probability for Failure to Act
less than 5 min	75 -100
less than 5 min*	10 - 25
30	5 - 20
60	5 - 10

*important instrument operator has been instructed to watch

If there are two alarms sounding it is very difficult for the operator to respond to both. Figure 2.3 shows the role of stress in determining the ability of a individual to perform (Parvin, 1985). All of the preceding factors must be established when attempting to judge the failure rate for human beings.

2.8.3 Determining the Error Rate

Tables 2.4 and 2.5, provide the average error rate that can be expected for operator action and intervention errors. These values are only estimates which require a more detailed analysis for a particular industry. By considering all of the factors that affect the response of an individual under normal and abnormal situations, a failure rate can be estimated. These values can then be used in the logic diagrams to develop the overall failure rates.

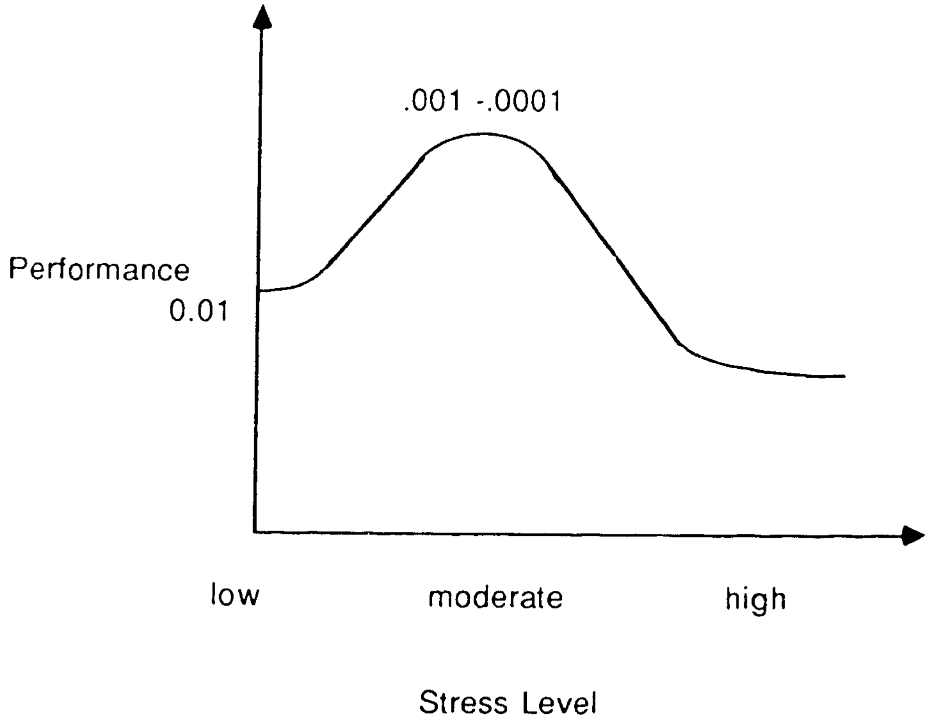


Figure 2.3 The effect of stress on operator performance (modified from Parvin, 1985).

3. MANAGING RISK

The main purpose of performing a comprehensive quantitive risk assessment, is to identify and manage areas of unacceptably high risk. The assessment provides a consistent basis for making decisions.

Upon completion of a risk assessment there are three options available to the analyst or manager. These are:

1. accept the risk and do nothing,
2. prepare further studies to reduce the uncertainty,
3. redesign the area of unacceptable risk

(Kazarians et al., 1985).

Before making any of the preceding choices, several factors are considered. The risk associated with a particular system must be judged in the different ways it affects the employee, the general public, individuals and the profits of the plant. A manager uses not only professional judgement, but considers the cost and benefits of the risk, public preferences and acceptance of risk, compares the risk to background risk and reviews the risk analysis of other alternatives before accepting the risk for a particular system (Kazarians et al., 1985).

When a risk analysis is developed, there are the three questions answered: what will happen?, how likely is it to happen?, and what are the consequences? Certain consequences will dominated the concerns of the risk manager. In particular, the manager is usually concerned with preventing or reducing the frequencies of those scenarios which result in deaths of either employees or the public.

3.1 Occupational Risks and Hazards

The Alberta Occupational Health and Safety regulations state that;

'Every employer shall ensure, as far as it is reasonably practicable for him to do so, the health and safety of

(a) workers engaged in the work of that employer, and

(b) those workers not engaged in the work of that employer but present at the work site at which that work is being carried out' (OHSA, 1976).

For a system with a particular risk, the manager must determine if it is necessary and/or reasonable to reduce that risk for the health and welfare of the worker. This question of reasonable or acceptable risk has been analysed in different ways. The European countries have established a target fatal accident rate (FAR) that is based on operational experience. The North American approach generally uses cost/benefit analysis to judge the acceptibility of risk.

3.1.1 Fatal Accident Rate (FAR)

The FAR is the, 'number of fatalities which occur in 10^{-8} person hours of exposure in an occupation' (Bulloch, 1984). The value of 10^{-8} person hours, is equivalent to the combined working lifetime of 1000 people (Kletz, 1982). Imperial Chemicals Industries Limited (ICI) has developed a target FAR based on the safest ten consecutive years of operation (Bulloch, 1984). This target value is 4 fatalities per 10^{-8} working hours (Ketz, 1982). The types of accidents resulting in this criteria were reviewed, and it was found that about half of the accidents were the result of road accidents, falling, tripping and other incidents unconnected with materials handling (Kletz, 1982). The developers of the target FAR considered these types of accidents to be a background risk that could not be improved through a process risk analysis (Bulloch, 1984). Consequently the target FAR was taken as 2 deaths per 10^{-8} man hours. This target value was further qualified by restricting the risk associated with any particular section or process within the plant. An individual chemical or process shall not have an FAR greater than 0.4. This restriction attempts to consider some of the risks that may not be adequately identified, and assumes that there are less than 5 chemicals with a significant risk value in the plant (Kletz, 1982). These target values are all applied to the employee who is at greatest risk in the plant.

The FAR has been widely accepted in European countries where it was developed. Kletz (1982) outlines two reasons for its acceptibility. The first is related to the philosophy behind the FAR. By attempting to reduce risks below the average risks that have been experienced, there is the concept of improving on the past. Secondly, the target values given have been attainable without being unreasonably costly. 'A ten fold decrease in the given FAR would in most cases not be feasible either economically or technically' (Kletz, 1982).

3.1.2 Cost/Benefit Analysis

This type of risk management is more widely accepted in the United States. Kaplan and Garrick (1981) indicate that risk cannot be considered in isolation but must be considered with the costs and benefits of the risk. Intuitively this is the same decision-making process an individual undertakes every day. One determines the benefit one will receive if a particular risk is taken, understanding what the consequences may be if the risk is realized. An employee is expected to be at higher risk because of the benefit received from being employed. If an activity providing only marginal benefit had a probability of a fatality 10^{-7} per annum for members of the public, then it is usually expected that an acceptable risk could be three to four orders of magnitude higher for the employees, because they are receiving the benefit of the full time employment (Starr, 1969).

The technique of cost/benefit analysis does not provide a fixed number that is considered acceptable, but it is constrained by two factors. The first is the onus placed on the employer to reasonably protect the employees by the Occupational Health and Safety Act. Secondly, within a cost/benefit analysis, a risk that may meet a target value is not acceptable if the same benefit can be obtained through another method that has less risk (Kaplan and Garrick, 1981).

A drawback of the cost/benefit analysis, is that it c n be used to rationalize those systems with higher risk (Bulloch, 1984). For the risk manager, the importance of professional judgement in these instances is essential.

3.2 Risks to the Public

An acceptable risk value for a group in society is difficult to develop, because there are so many individual ideas of what acceptable risk is. There are two concepts which define how society and individuals accept risk: involuntary versus voluntary risks, and the cost/benefit aspects of risk.

3.2.1 Voluntary and Involuntary Risk

When individuals voluntarily choose to perform an activity, they are using their own set of values to judge the experience (Starr, 1969). Whether the evaluation process is made consciously or unconsciously, the individual considers the potential risk and benefit associated with the activity. If the benefit outweighs the risk, the individual gains something.

For involuntary risk it is not the individual, but a controlling body which determines what benefits outweigh the risks, and therefore which activities the individual and public, will be exposed to (Starr, 1969). While there are many differences between the voluntary and involuntary risks, one of the key features is how the individual accepts these risks. Certainly individuals and society will accept a voluntary risk that is several orders of magnitude higher than an involuntary risk. Most individuals like to make their own choices about which risks are worth the perceived benefit (Starr, 1969).

3.2.2 Cost/Benefit

With every risk or chance that is taken, there is a cost and a benefit associated with that risk. Individuals and societies take risks because of the benefit they receive and under most circumstances, the greater the risk, the greater the benefit. Since individuals view risk differently and tolerate different levels of involuntary risk, it is difficult to determine the acceptable relationship between benefit and risk. Starr (1969) found that the relationship between the acceptance of risk and the number of people affected by the risk was inversely proportional. This finding correlates with the different perceptions individuals have of risk. With more individuals involved, there is a correspondingly wider range of opinion on what is acceptable risk.

Because of the different perceptions of acceptable involuntary risk, controlling bodies have tried to use cost/benefit analysis to aid in the management of risk. They calculate the benefit an individual will receive from the activity, and the cost of the risk. Both calculations are difficult since they require nonmonetary items to be expressed in monetary terms. If an industry is providing an improved quality of life, the dollar value of that improvement is subjective and varies for each individual. Generally a proportional relationship is used between the increased salary or spending of an individual to the dollar value of the quality of life.

Evaluating the cost of the risk is even more difficult since the risk is usually expressed as the number of fatalities per year. This requires a dollar value being placed on a human life. These quantitative difficulties have resulted in cost/benefit analysis being used as support for risk values generated by alternated techniques.

3.2.3 Determining an Acceptable Level of Risk

In order to develop a target value for public risk, managers have tried to use the two concepts individuals have of risk. Most managers use those involuntary risks that society is presently accepting as a guide. Risk associated with involuntary exposure, are summarized in Table 3.1 and risk asociated with voluntary exposures are summarized in Table 3.2. These tables can then be used as a guideline for developing an acceptable risk value.

Table 3.1. Probability of death for involuntary risks. (modified from Bulloch, 1984)

Event	Probability of Death per Person per Annum
Falling Meteorite	6×10^{-11}
Cosmic Rays	$10^{-11} - 10^{-10}$
Explosion of a pressure vessel	5×10^{-8}
Falling Aircraft	1.8×10^{-8}
Release from U.K. Atomic power station at 1 km	1×10^{-7}
Lightening (U.K.)	1×10^{-7}
Major Storm (U.S.)	8×10^{-7}
Falling Aircraft (close to airport)	10^{-6}
California Earthquake	1.7×10^{-6}
U.S. Midwest tornado	2.2×10^{-6}
U.S. Flood	2.2×10^{-6}
Run over by a motor vehicle	8.8×10^{-5}
Leukemia	7.0×10^{5}
Influenza	1.8×10^{-4}

Table 3.2. Probablity of death for commonly accepted risks (modified from Bulloch, 1984)

Event	Probability of death per person per year
Travelling by car	5.2×10^{-3}
Travelling by air	2.1×10^{-4}
Lung cancer	4.4×10^{-4}
Travel by train	4.4×10^{-4}
Average for British Industry	3.5×10^{-4}
Travel by Bus	2.6×10^{-4}
Stay at Home	2.6×10^{-4}
Taking Oral contraceptives	$1.8\ 10^{-5}$
Accidental Poisoning by Aspirin	1.8×10^{-6}

Table 3.3. Probability of death per person per annum. (modified from Kletz, 1986).

Event	Probability of death per person per year (x 10^{-5})
All Causes	
Whole population	1200
Man Age 30	100
Woman Age 30	60
Man Age 60	2000
Woman Age 60	1000
Cancer	250
All Accidents	34
Road Accidents	14
Falls	11
Fires	1.8
Drowning	1.1
Electrocution	.24

The philosophy of this reasoning, is to prevent the involuntary risk posed by an industry from exceeding the level the public is already exposed to (Rasbash, 1985). While the philosophy has been agreed upon, the exact number which represents this involuntary risk has not been defined and agreed upon by all risk analysts. Some set an upper limit of 10^{-4} per person per year while others only permit a risk value of 10^{-7} per person per year (Lowe, 1984). The variance in these numbers can be related to the cost/benefit relationship, and how the analyst views the relationship of an additional industrial risk to those involuntary risks which already exist.

In Table 3.3 Kletz (1981) indicates the overall risk to particular segments of the population depending on age and sex. For a man of age 30, there is a probability of death of 1 in 1000 per year from all of the involuntary risks he would be exposed to in that year. An industry that poses an individual risk of 10^{-5} fatalities per year would be increasing that man's probability of death by 1%. For a risk of 10^{-6}, the probability is increased by 0.1%. On this basis a risk of 10^{-5} to 10^{-6} is acceptable to Kletz (1981).

Other analysts do not rely on numbers alone, but justify the additional risk a person is exposed to through the benefit they receive. Rasbash (1984) uses a risk benefit curve developed from Starr (1969). The curve approaches the limit of 10^{-6} which is the probability of death from disease for an average person. Rasbash (1981) indicates that an individual should not be exposed to more risk than is warranted by benefit provided. From this philosophy, a limit of 10^{-7} per individual per year was established for circumstances providing only marginal benefit. This risk benefit curve, suggests that higher risks are tolerated up to 10^{-6} as long as there is a corresponding benefit.

Both Kletz (1981) and Rasbash (1984) give risk numbers for the individual. The issue of how to handle scenarios where the consequences represent multiple fatalities has not been discussed. Rasbash (1984) handles multiple fatalities from a fire by reducing the acceptable risk from 10^{-6} per year to 10^{-7} to 10^{-8} per year where over 100 people could be killed. Gibson (1976) argues that if a scenario causing 1 death per 100 years is acceptable, and has an FAR that is equivalent to 100 deaths per 10,000 years, then the second scenario which is 100 times less probable, should also be acceptable. Bowen (1976) indicates that if the analysis for an individual is done properly and considered acceptable, then that analysis can be applied as many times as necessary to compensate for more people being affected.

Kletz (1981) and Bowen (1976) draw attention to this problem by posing the following question:

'(A) is 100 deaths once in 100 years worse than
(B) one death per year for 100 years?'

Both scenarios A and B result in the same number of deaths, however scenario A which represents a catastrophic accident demands and receives more attention from the public and government. Because of the greater economic and social disruption there may be some justification for giving scenario A priority. However, when only the number of fatalities is considered, scenario B should be given equal consideration if not priority. Over a ten year period, event B is certain to happen ten times resulting in ten fatalities. However, over the same ten year period, scenario A only has a 1 in 10 chance of occurring. When there is a fixed allocation of resources the prevention of a certain death is more worthwhile (Kletz, 1981). However when the probability of an event that can kill 100 people is equivalent to that of an event which can kill 1, the total possible number of deaths must be considered. Therefore, an accident fatality number representing the total possible killed must also be considered (Kletz, 1981).

3.3 Applying Target Values and Decision Making

There are several factors which the analyst must consider when judging how to handle a particular scenario. From the assessment, the likelihood of occurrence and consequences for several scenarios within the plant will have been predicted. The manager must determine which scenarios require improvement, which can remain as they are, and which should be eliminated completely. If the manager accepts the basis and the development of the FAR, then he can compare the results of the risk analysis for occupational and public saftey and determine where improvements are required. For those analysts who do not agree with or want to use the FAR comparison, they must determine their own target values. Kaplan and Garrick (1981) consider a risk level acceptable only if the same benefit cannot be achieved in another way with less risk at a small cost. This definition of acceptable risk allows for higher risk levels if the benefit is correspondingly high.

When evaluating the risk to employees and the public the individual who will be at greatest risk should always be considered. For public risk, this removes the temptation to take the total risk value and divide it among the population, to give an average risk which appears to be an acceptable individual risk (Kletz, 1981).

Once the acceptable risk limits have been set by the manager, the review of the risk assessment can begin. In some instances, the risk will be unacceptable or perhaps only marginally acceptable. To reduce the risk a complete redesign may be required, or perhaps just a slight adjustment in one of the processes may reduce the risk. By going through the fault tree or event tree, the process which has the greatest impact on the final risk value can be identified. By reducing the risk for the critical section of the process the overall risk is reduced.

Once the risk is deemed to be acceptable for employees and the public, the manager must determine if the economic risk is acceptable. The cost of a potential scenario along with cost of its consequences can be compared with the cost of improvements which reduce the risk (Lawley et al., 1985).

By evaluating the risk before and after a potential change, and knowing the cost of the change, the dollar value of the life saved can be estimated (Bulloch, 1984). This technique has been used to ensure a consistent allocation of funds for improvements.

Other methods of evaluating an improvement involve a simple economic calculation. The annual cost of the proposed change should be less than the annual cost caused by the incident which will be prevented (Lawley et al., 1985). By using a risk assessment effectively, all goals and objectives of the manager can be maintained. The occupational and public safety can be ensured with reasonable and appropriate economic expenditures.

3.3.1 Controlling Human Error

When the probability of a scenario occurring is too high the designer must alter or redesign the situation so that it meets the target values. When the target values are exceeded because of human unreliability, some designers prefer to avoid this human error by using using machines, resulting in fully automated plants. While it may appear that a fully automated plant does not have any human error, the error has been shifted from the operator to the designer and manufacturer (Kletz, 1987). The appropriate solution is neither one extreme nor the other, but a mixture of men and machines.

Machines can improve safety when they are used in tasks that are boring or redundant, or when there is an uncomfortable hazardous situation that would create an abnormally high stress level then humans (Swain, 1987). There is no doubt that equipment which is working in its intended manner, and that has been adequately designed to successfully handle deviations in the system, will be safer and more reliable (Swain, 1987).

Human beings have a distinct advantage in that they are able to take actions outside of their programming. Although some consider this characteristic to be a disadvantage, properly trained human beings are desirable and necessary for a adaptive operating systems.

4. BENEFITS AND LIMITATIONS OF A QUANTITATIVE RISK ASSESSMENT

There is a general agreement amongst designers, engineers, and managers, that there is a need for an organized comprehensive approach for managing risk. As industries have been quickly advancing, larger facilities using new technologies are being developed. Sophisticated competition means that the capabilities of the facilities are often pushed to their physical limits. Although there is a general agreement about the need to identify risks, there is some discrepancy about the usefulness of quantitative risk assessments.

The main difficulties with quantitative risk assessments are the lack of a universally accepted set of definitions and an inadequate understanding of how probabilistic risk assessments are used. Some critics dispute the usefulness of the assessment because they feel only the hazard identification section of an assessment is useful. These critics are correct, for in some instances that is all that is required, but the power of the assessment is that it can be used to further quantify the risk if it is necessary. These criticisms of a quantitative risk assessment shall be reviewed.

4.1 Data

4.1.1 Reliability of Data

A major criticism of a quantitative risk assessment is the inaccuracy of the results produced from inadequate and inapplicable data. Reliability data used to develop failure rates for various pieces of equipment can only have meaning if a large number of identical pieces of equipment are examined (Joschek, 1983). The equipment must be manufactured, operated, tested and maintained in exactly the same manner if data from one plant is used for the assessment of the performance of similar equipment in another plant. 'For the process industries where each facility is almost completely unique, this set of data is almost impossible to collect because it does not exist' (Joschek, 1983).

While this criticism is valid, the method of data analysis and subsequent generation of probability values using Bayes Theorem has been designed to not only consider this problem, but to indicate how it affects the results or the present state of uncertainty about a particular system. Failure rate data collected from similar plants are not used in isolation. The failure rates can be adjusted by utilizing the alternate data sources available.

4.1.2 Inaccuracy of Results

The accuracy of results produced in a quantitative risk assessment are also questioned. Predicted values can vary by an order of magnitude in both directions (Joschek, 1983). However, a probabilistic risk assessment should express the designer's uncertainty.

The risk of a particular process or system cannot be a single number as is often cited. Rather the risk is a probability distribution expressing the confidence which the analyst has that the event will occur with a particular consequence (Kaplan, 1986). The uncertainty surrounding an event should be indicated and communicated. A quantitative risk assessment provides the means for this communication. If the uncertainty varies over an order of magnitude then that uncertainty is expressed in the probability distribution.

Another criticism of a risk assessment is that the inaccuracy of the final numbers makes the results meaningless. This criticism would be valid if the analysts claimed the results were absolute and definitive, but a competent analyst does not. If the assessment was done in a comprehensive and consistent manner, the analyst only needs to use the numbers as a relative measure of risk to aid in identifying the major areas of concern (Lowe, 1984). The assessment allows for the communication of uncertainty and puts that uncertainty in relative terms so that it can be managed responsibly.

4.1.3 The Human Factor

Joschek (1983) assigns 80 to 90% of all accidents to human fault and error. He does agree that the man machine interface can be predicted with some accuracy, and that it can be expressed through a risk assessment. He questions however, the ability to predict the occasional loss of concentration, or incorrect reaction to a particular emergency. The variance in management, administration, operator training and safety objectives at each plant make the results pertaining to human input meaningless according to Joschek (1983).

The human factor is always difficult to predict. However an initial assumption of a risk assessment is that the facility will be properly operated and maintained in the manner the designer intended. This includes the training and management of operations. The occasional loss of concentration for any individual must always be expected (Kletz, 1987). Instead of ignoring this factor as being beyond the designer's control the quantitative risk assessment can pinpoint areas where an occasional lapse will cause failure. Such areas will inevitably have accidents unless redesigned. Rather than accepting such situations as inevitable, designers must consider the human factor and build tolerance for humans into their design (Kletz, 1987).

4.1.4 The Necessity of a Full Assessment

Many of the criticisms about a quantative risk assessment pertain to the quantitative portion of the assessment. All designers agree that there is a need for the identification of hazards but rather than wasting resources, time and effort on attempting to quantify the risk, the critics believe that the effort should be focused on identifying all possible hazards (Joschek, 1983).

There is no doubt that the most important stage of an assessment is the identification of hazards. This is where the emphasis of the assessment should be. In some instances it is not necessary to develop the assessment any further since the solutions to reducing the risk are obvious. However, in other instances the designer may not be sure if the system is acceptable. This is particularly true for new systems and for procedures that do not have any guidelines for their use. The development of the failure frequencies provides a mechanism by which the analyst can judge the system and the safety procedures taken to reduce the risk. A well trained analyst does not waste resources on developing a quantitative analysis when the solution is obvious.

The analyst may prefer to complete the consequence analysis before developing the probabilities of the scenarios so that only those scenarios with intolerable consequences are analysed for frequency (Freeman et al., 1986). Although this type of analysis may be incomplete, where the allocation of resources is very restricted this is a possible solution.

4.2 Summary

The important feature of the quantitative risk assessment technique is that it has been developed in a manner so that it is flexible enough to meet the requirements of many different facilities and industries. An assessment can be as broad or detailed as required. Only some sections of a facility may require a detailed analysis, in which case that is all that should be done. The purpose of the assessment is to help manage the risk. If the risk is known and acceptable, an assessment may not be necessary.

A quantitative risk assessment is a tool for handling uncertainty and expressing it. Final single risk numbers do not represent anything to the public or the manager (Lowe, 1984). However, when considered in a relative manner with the other risks that the public can understand and relate to, the numbers may have meaning. The numbers are only a method of communication which may need some explanation.Quantitative risk assessment clearly has a role if correctly used.

5. APPLICATION OF A QUANTITATIVE RISK ASSESSMENT TO A WATER TREATMENT PLANT

5.1 Why do a Quantitative Risk Assessment?

The technique of quantitative risk assessment, was developed, because designers found that the established codes of practice were not always adequate to ensure an acceptable level of safety for either employees or the public. By performing a quantitative risk analysis, designers had a way of evaluating the risk associated with a particular plant, and could determine if the risk was acceptable.

The treatment of water for human consumption is not a new industry. Since Roman times man has recognized the health benefits of treating water for public use, but it was not until the discovery of bacteria that the reasons for water treatment were understood. Within the water treatment industry, there has been very little change in the chemicals used to treat water since the early 1900's. There may have been some improvements in efficiency, but the basic processes have remained unchanged (Hopkins, 1936).

The technique of quantitative risk assessment was designed to highlight the risk from hazards. While it has only been applied within the chemical, nuclear and space industries, the technique was designed to be general enough so that its application was not limiting. There are several ways in which this technique can be used to analyse the various risks associated with a municipal water treatment plant.

There are hazards posed by the variety of chemicals used in modern plants. These hazards affect employees, the environment and the public. This is particularly true in the latter case since most municipal treatment plants are located near or within large concentrated populations. There is an additional risk posed to the public which is associated with the product. Mor specifically, the hazard would be from consuming contaminated or inadequately treated water. As water sources have become more contaminated, there is some degree of uncertainty about the adequacy of established techniques and the reliability of new techniques to provide safe water. Quantitative risk assessment is a tool which designers can use to measure and deal with that uncertainty. The usefulness of a quantitative risk assessment for determining the adequacy of established standards and proposed designs will be evaluated by analysing an existing municipal water treatment plant.

5.2 Review of Water Treatment Plant

The water treatment plant which was reviewed is located in Edmonton, Alberta a community that has a population of approximately 700,000. The water supply for the plant is a river which has a highly variable quality depending on the time of year. To provide a treated water of acceptable quality, this facility uses several chemicals and physical processess (Fig.5.1). The plant was built in the late 1940's. Various parts have been added or have been upgraded by automation. However because of its age, there is still a high degree of human involvement in plant operation. There are automatic analysers throughout the facility, and the newer equipment can be started, stopped or altered remotely. Many of these controls are not employed. Those that are used regularly, are manually checked to ensure that the operation is continuing correctly.

5.2.1 Raw Water Supply

The water su[illegible] the North Saskatchewan River has a flow rate of approximately 200 m³/s in the summer and 130 m³/s in the winter months (IWD, 1986). During the spring runoff the water quality is the poorest with high organic loadings and high turbidity values. The plant has two possible intakes, one located at the north river bank and the other 30 m from the north bank. This allows for a limited flexibility in controlling the quality of the raw water source.

Because this facility is located within the center of the city, there is relatively high organic loading which must be dealt with on a continuing basis. During storm events this organic loading increases dramatically because of storm sewer outfalls located upstream of the raw water intakes (Hrudey, 1986). Minor oil spills and other types of contamination occur throughout the year. During 1985,

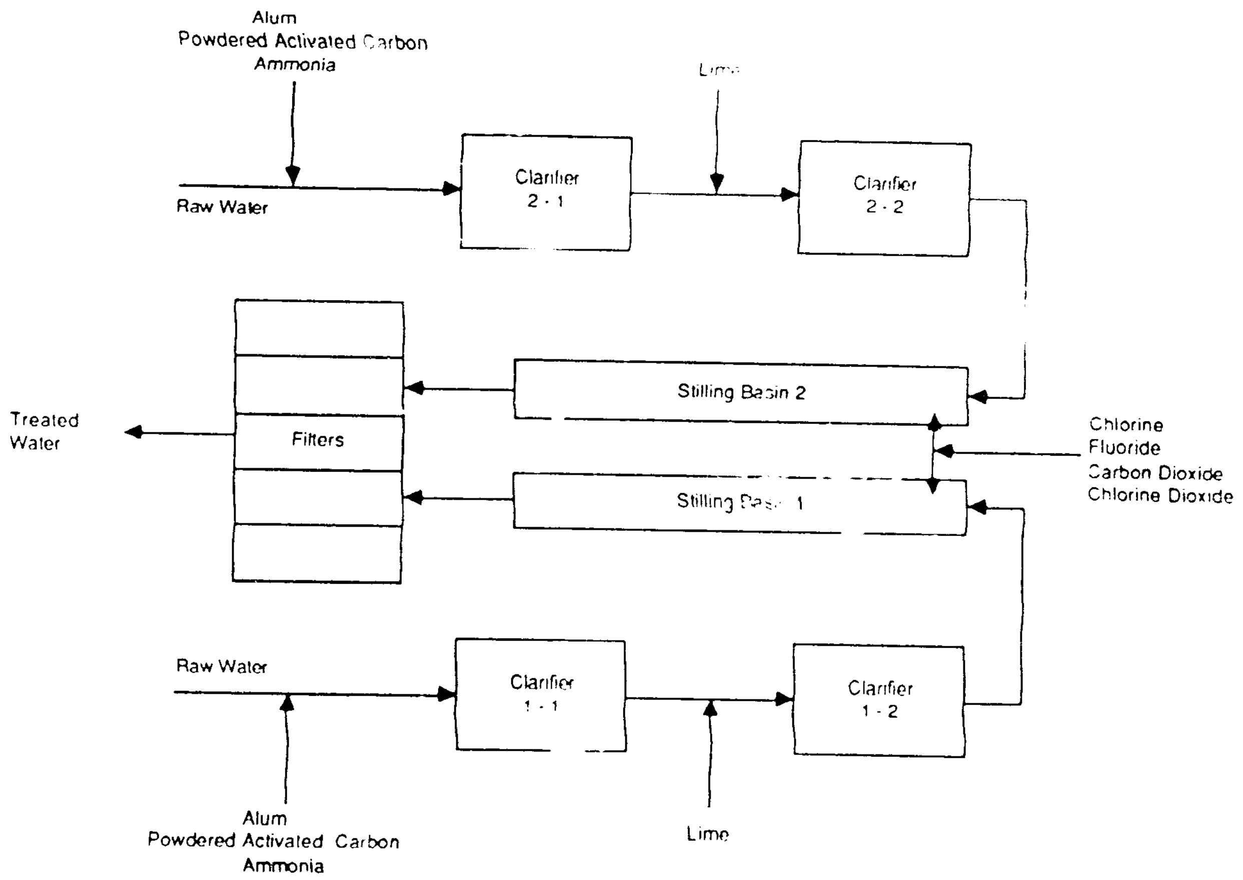


Figure 5.1 Process diagram of the municipal water treatment plant (modified from Hrudey, 1986).

seventeen oil spill incidences were reported, and fourteen in 1984 (Annual Report, 1984, 1985). These variations can create numerous difficulties in attempting to produce a potable water.

5.2.2 Overview of the Water Treatment Plant

The treatment facility consists of three separate plants. Their maximum reliable capacities and peak capacities are indicated in Table 5.1. Plant 3 which is much smaller than Plant 1 or Plant 2, was designed as a peaking plant, used only when the demand exceeded the capacity of plants 1 and 2. This plant now operates continuously, although it cannot perform softening. The main plants are normally operated as one unit with the treated water produced by all three plants being combined. The two main plants share the same chemical storage areas, differing only in their respective feed rates. Having two main plants allows for more flexibility when maintenance work or upgrading is to be performed.

5.2.3 Treatment Processes

This treatment facility relies on many different chemicals to provide drinking water of adequate quality. Most of these chemicals are part of a standard treatment process and are not considered to be classified as advanced treatment processes (Hopkins, 1936).

Table 5.1. Maximum and reliable pumpage rates for plants 1, 2, & 3.
(modified from Annual Report, 1985).

Capacity (MLD)	Plant 1	Plant 2	Total for 1 and 2	Plant 3	Total for all three plants
Maximum Reliable	80	120	200	35	235
Peak	120	170	290	80	370

The various chemicals will be considered in the order that they are normally added in the treatment process at this particular installation (Fig 5.1). In an emergency, each clarifier can be isolated and operated as a separate plant with the necessary chemicals being rerouted to the appropriate applications points.

Chemicals

Aluminum Sulphate (ALUM)

Alum is used in the process of coagulation. This chemical is added into the raw water via a rapid mixer. Proper mixing of the alum with the water is important for adequate flocculation and sedimentation. The feed rate which varies depending on the raw water turbidity, is determined through a jar test (APHA,1980).

Since the middle of 1986, there has been a switch from dry alum to liquid alum. This has reduced the direct hazard to the operators because they no longer need to prepare an alum slurry for feed to the raw water. By eliminating direct contact with the chemical substance the risk posed by this chemical has been reduced. However, even though the risk from handling the substance has been reduced, the risk from liquid alum is greater than dry alum should a spill occur

Dry alum is classified as a low hazardous subtance. Fires, leaks or larger spills can be controlled by adding water although a dry chemical fire extinguisher is preferred (Emergency Manual, 1987).

Liquid alum is a poisonous corrosive acid. Consequently, extreme care must be taken in the event of a fire or spill. Fumes capable of causing severe injury or death can be produced upon exposure to heat or water. As with dry alum, a water spray can be used to contain fires or reduce vapours, but foam or a dry chemical fire extinguisher is preferred (Emergency Manual, 1987).

<u>Activated Carbon (PAC)</u>

Along with the addition of alum, activated carbon is added into the raw water via the rapid mixer. Activated carbon is used to adsorb dissolved organics which can affect the taste and odor of the treated water. The removal of organics is also important for the prevention of harmful organic oxidation products that may occur when chlorine is added.

Activated carbon is added to the water by preparing a slurry which can be pumped to the rapid mixer. A new system was installed in 1986 which reduces the direct manual handling of the PAC by the operators, thereby reducing the direct risk of inhaling the carbon dust. The activated carbon is delivered in tanker trucks, which can be directly emptied into the storage tank while make up water is added to prepare an activated carbon slurry of the correct concentration (approximately 4%). This is far superior to the original system which required the manual preparation of the slurry from 25 kg bags. The direct exposure to PAC dust created in the process presented a hazard which the operational staff had to deal with. The dust was also found to be irritating when it came in contact with clothing. By storing the carbon in a slurry form the fire hazard from dry activated carbon powder was eliminated.

Ammonia (NH_3)

In order to form chloramines for disinfection ammonia is also added at the rapid mixer. The ammonia is added early in the treatment process to ensure adequate mixing before the chlorine is added.

The type of ammonia system employed, has been changed from a dry system which used ammonium sulphate ($(NH_4)_2SO_4$) to a liquid system using ammonium hydroxide (NH_4OH), also called aqua ammonia. The new system went into operation in February 1988. The new system also removes the need for direct contact between the operator and the chemical.

When dry alum was used, the $(NH_4)_2SO_4$ was mixed directly with the alum slurry by the manual addition of 25 kg bags to the slurry tank. The new system eliminates worker exposure to dusts and direct skin contact. However, there is an increase in risk posed by the storage of the liquid form rather than the dry form.

Aqua ammonia is considered to be poisonous and corrosive. Exposure to fire or water can produce poisonous and corrosive gases that can cause severe injury or death. The containment area for the liquid form must have adequate ventilation because of the volatile nature of the chemical. In the event of a spill vapours can be controlled with a water spray. Proper breathing equipment is essential when dealing with an emergency spill or leak (Emergency Manual, 1987).

Calcium Oxide (Lime, CaO)

After the water has passed through the initial flocculating and clarification chambers, it has a pH approximately 5.2 to 7.1 and an average hardness of 180 mg/L as $CaCO_3$. Calcium oxide is added to precipitate hardness. The quantity of lime fed depends on the hardness of the raw water. The lime storage and feed area has also recently been altered. The lime is delivered in 26 to 32 tonne shipments, and is transferred into a storage silo with a capacity of 120 tonnes.

The lime slurry is prepared by feeding the lime through a hopper into a lime slaker where it is mixed with water. A 2:1 ratio of lime to water is used. This paste is then transferred to a lime slurry tank where it is diluted to a consistency that is readily pumped to the injection points. This entire process requires a high degree of maintainence. The slaker and slurry tank is normally cleaned once every 12 h, by draining both units and then hosing them down. Additionally, the lime feed lines must be cleaned once every 12 h, by mechanically forcing a small scouring unit through the pipes with high velocity water. Even with this intensive maintenance program, the lines must be acidized once every six months (Operator Training Manual, 1984).

Because of the high degree of maintenance and the preparation technique used, there are numerous instances when operators are directly exposed to the lime. Lime is considered to be poisonous and corrosive. When it comes into contact with skin it is highly irritating and if not immediately rinsed off, it can cause severe burns (Emergency Manual, 1984). Eye protection, coveralls and gloves must be worn at all times. However, in emergency situations, these protective measures are often forgotten (personal observation, 1986).

In a fire situation, care must be taken to prevent the direct addition of water to the silo. Such an event would cause a major explosion from the heat produced by the chemical reaction between the hydrated lime and water.

Carbon Dioxide (CO_2)

After a period of clarification which allows the calcium carbonate and magnesium carbonate to precipitate and be removed from the water, the water enters the stilling basins where a number of chemicals are added. If the pH of the water is above 9.2, carbon dioxide is added. The CO_2 combines with noncarbonate alkalinity to produce the carbonate radical.

$$2OH^- + CO_2 \rightleftharpoons CO_3^{-2} + H_2O$$

The carbonate radical can the precipitate remaining calcium ions (Montgomery, 1985). The natural gas burners are used to generate the carbon dioxide. The units automatically monitor the pH, adjusting the quantity of carbon dioxide added accordingly. The unit is completely closed, only requiring an occasional manual check to ensure that the system is operating correctly.

Chlorine (Cl_2)

After clarification and softening chlorine is added for several reasons. At this stage most of the suspended matter that would create a chlorine demand has been removed. Likewise, by adding chlorine after the activated carbon, some of the dissolved organics will also have been removed. The dissolved organics create a chlorine demand or form potentially harmful oxidation products. If the chlorine were added with the activated carbon it would react and lose chlorine residual. Finally the late addition of chlorine ensures that the ammonia is completely mixed so the chlorine will oxidize the ammonia forming chloramines rather than forming trihalomethanes and other chlorinated organic compounds (Montgomery, 1985).

Chlorine is considered to be poisonous, corrosive and a strong oxidant. It can be fatal if inhaled at a concentrations greater than 25 ppm. At concentrations greater than 1 ppm it can be readily smelled (ETSI, 1984). Care must be taken in a fire situation, since the direct addition of water to the chlorine will form hydrochloric acid. A spill can involve gaseous or liquid chlorine, however a liquid leak is normally much more serious since every litre of liquid chlorine will form 454 L of gaseous chlorine (Hjalmar, 1978). If a large quantity of liquid chlorine is rapidly exposed to the atmosphere, the liquid may flash off creating an explosive situation. In the event of a leak, guidelines prohibit entry into the area unless appropriate breathing apparatus is worn.

The chlorine feed unit in place was upgraded in 1976. New chlorinators, piping and storage facilities were installed and the plant switched from using liquid chlorine and evaporators, to using gaseous chlorine.

Sodium Chlorite ($NaClO_2$)

The other disinfection process used in this particular treatment process is chlorine dioxide. By combining chlorine with sodium chlorite, chlorine dioxide is formed under acidic conditions:

$$Cl_2 + 2NaClO_2 \rightleftharpoons 2ClO_2 + 2NaCl$$

Chlorine dioxide is a preferred disinfectant since it does not react to form haloorganic compounds (Montgomery, 1985). However chlorite, an unreacted and decomposition product of the reaction, has known deleterious health effects. Because of this risk, careful monitoring of residual concentrations of chlorine dioxide and chlorite must be done. Currently the maximum allowable combined level is 1.0 mg/L. This is intended to restrict the chlorite concentration to 0.5 mg/L (Hrudey, 1986).

Sodium chlorite was originally shipped in solid form, but is now ordered in the liquid form. For this chemical, the switch to the liquid form has improved the safety of the operator from a materials handling point of view. Sodium chlorite solid is an explosive material which can under go spontaneous combustion under pressure or when in contact with organic materials. If the material came in contact with skin, severe burns could result. In the event of a fire, the fumes produced are poisonous.

The solid form required the manual preparation of a 25% solution. This was prepared in a 900 L mixing tank, and was then transferred to either of two 5500 L holding tanks (Operator Training Manual, 1984).

By switching to liquid soduim chlorite there is no longer any direct contact between the operator and the chemical. While sodium chlorite liquid is considered to be both poisonous and corrosive it is not explosive. By using a CO_2 fire extinguisher or a water spray, the fire can be contained (Emergency Manual, 1987).

Hydrofluorosilicic Acid (Fluoride, F)

In the silling basins, fluoride is added. Fluoride is the only chemical in the treatment process which does not directly affect the process. It is added only as a health benefit to the public. The addition of fluoride has caused some controversy, since opponents to its addition claim there are either not any beneficial health effects provided by this chemical or that fluoride itself is harmful. This controversy is ongoing, but there has been no epidemiological evidence obtained to demonstrate harmful health effects when fluoride is used in water systems. The addition of fluoride up to 1 mg/L is known to prevent dental caries (Weber, 1972).

Fluoride is shipped as hydrofluorosilicic acid. An underground holding tank with a capacity of 90,000 kg is used for storage. Feed rates are controlled from a day tank which has a capacity of 1000 kg. The fluoride is added to the chlorine headers which run to the stilling basins. The feed rate is determined by evaluating the concentration of fluoride from a 24 hour sampler. If it is not between 0.9 to 1.05 mg/L, a trimmer pump is automatically activated to adjust the concentration.

The acid form of fluoride used, is corrosive and poisonous. Using a liquid form of the compound eliminates direct contact with the material, unless there is a spill. Excessive heat from a fire can produce poisonous fumes. A CO_2, foam, or dry chemical fire extinguisher should be used to contain a fire in the vicinity of the hydrofluorosilicic acid (Emergency Manual, 1985).

Polymers

The removal of suspended and dissolved materials from the water naturally produces a large quantitiy of waste sludges. Alum sludge is produced fom the first clarifier. A $CaCO_3$ sludge, which is relatively pure, is wasted from the second clarifier.

The alum sludge is generally drained from the clarifier at regular intervals into the river by gravity. There is a recycle capacity however it is not normally used unless lime has been added in this first stage. The $CaCO_3$ sludge however, cannot be drained to the river, and must be thickened and removed for disposal. In order to promote the thickening process, an anionic polymer is used. This polymer which is delivered as a liquid, is prepared as a 33% solution. The solids content of the sludge is monitored hourly until the concentration is above 15 to 17% for plant 2 and 12 to 18% for plant 1. Once it is concentrated, the sludge is drained to the recalcination building where thickening occurs via a thickener and centrifuge. The sludge is then transferred to hopper trucks which transport the thickened sludge to landfill.

There is direct contact by the operator with both the polymer and sludge. The hazards associated with the sludge are similar to those of the lime. At one time the $CaCO_3$ sludge was dewatered and recycled back to the lime silo. However, the additional process of recalcination was more expensive than the purchased lime. In addition, the lime produced was not flaky but in the form of hard pellets. Some of the pellets were known to explode when suddenly exposed to water in the slaker.

General

At this point, all of the chemicals have been added to the water. After passing through the stilling basins which provides approximately 30 to 45 min residence time depending on the flow rate, the water passes down through sand filters. At this point the water from the two separate plants along with the third plant is combined and sent to the reservoir or to distribution.

Physical Processes

Most of the physical processes have already been alluded to in the discussion on chemicals. This facility does not use any type of presedimentation, drawing its raw water directly from the river. The mixing prior to the first clarifier promotes coagulation and flocculation. Both flow-through sedimentation and tube settlers are used to promote clarification. The second clarifier operates in exactly the same manner as the first only the lime is added in the flume. The stilling basin provides further clarification and increases the contact time for the disinfectants. The last treatment stage is filtration which is the only purely physical treatment method used. These sand filters are used to reduce the final turbidity to 0.1

to 0.2 NTU.

Operations

While the role of the operator in water treatment has changed over time, there will always be a need for human judgement and involvement in the production of potable water. This is mainly caused by the variance in the source water. While the different treatment processes could be completely automated, the design would be complex and expensive. For a variable source water, it would also be difficult to program for every circumstance, and the possible consequences of missing a particular scenario could be extremely serious.

The source water for this particular treatment facility is extremely variable. Reviewing turbidity alone, it can vary from 1 NTU to 300 NTU within a matter of hours (Annual Report, 1986). The variability partly explains the high degree of operator involvement in the plant. The lack of automation within the plant also requires operator involvement.

Until two years ago all of the chemicals were dry feed units requiring direct contact between the operator and chemicals. The switch to aqueous solutions has reduced the direct contact however there is still only manual control for most of the valving and feed mechanisms.

Manual involvement is also required for emergency responses. While there are a few automatic shut down systems, most of the systems rely on operator intervention to isolate the situation, neutralize it, and activate standby response mechanisms to maintain the treatment process. In order to understand how routine jobs and emergency actions are performed, a brief description of operator duties and the organization of the personnel on the shifts follows.

Of the twenty six full time operators, twenty work 12 h rotating shifts, while the other six work [illegible] day shifts or as replacement staff for the shift workers. There are four shifts with five operators per shift. The responsibility and decision making authority is delegated in the following way. There is one shift foreman, one or two level 2 operators and two or three level 1 operators.

A level 1 operator is directly involved with the chemicals. He is responsible for monitoring the water at different stages within the treatment process. From the tests performed the operator determines if any adjustments are required in the feed rates, and if so, makes them. Even if adjustments are not required, the chemical feed rates and quantities of chemicals consumed are monitored every two or three hours to ensure the equipment is performing as expected. A level 1 operator is also responsible for draining sludge from the clarifiers, transferring sludge to disposal trucks when required, helping in the unloading of the various chemicals, and washing filters.

A level 2 operator must be prepared to perform any of the level 1 operator duties should there be a shortaqe of manpower. This operator also requires knowledge of the distribution system since he is mostly involved in monitoring and adjusting the raw and treated water pumpage rates. Should the shift foreman not be on duty, the level 2 operator is also responsible for his duties.

The shift foreman is ultimately responsible for all of the decisions and actions which are performed on his shift. He is responsible for making all operational decisions. This includes the appropriate pumpage rates to attain the appropriate chemical feed rates. While the other two levels of operators can make the necessary feed rate adjustments on their own, the shift foreman is normally informed.

All personnel have been trained in the appropriate responses for the various alarms which are activated in the plant. At the sounding of an alarm, personnel closest to the area will respond, however the normal procedure is to first contact the shift foreman and determine if their assistance is required.

6. CHLORINE FEED UNIT

Rather than developing a complete risk analysis for the entire water treatment facility, a quantitative risk assessment was performed only on the chlorine storage and feed unit. This particular unit was chosen since it could demonstrate two applications of the technique. Following the traditional application of a quantitative risk assessment the occupational health risks resulting in injury or death were evaluated. Chlorine is the most acutely toxic chemical at the plant, requiring the most safeguards. The other application focused on the quality of the water produced, and evaluated the public health risk from ingesting inadequately disinfected water.

6.1 Hazard Identification for the Chlorine System

This particular chlorine system is designed to provide disinfection for up to 200 ML of pumped water per day. It is used for the production of chlorine dioxide which is the main oxidizing agent and for the formation of chloramines which are used to maintain an adequate disinfectant residual for the distribution system. The two main plants consume between 155,000 to 170,000 kg of chlorine yearly (Annual Report, 1985, 1986).

6.2 Chemical and Physical Properties of Chlorine

Chlorine is a greenish yellow gas at standard temperature and pressure (White, 1986). Chlorine is normally shipped as liquefied gas, therefore properties of its liquid state are presented along with its gaseous state in Table 6.1. In its gaseous form, chlorine has a specific gravity of 2.48, which reflects its tendency to collect in low lying areas. The gas has a characteristic pungent, irritating, easily recognizable odor (ETSI, 1984).

6.2.1 Volume-Temperature Effects

A certain degree of care must be exercized when designing storage or transportation containers for liquid chlorine because of its characteristic volume-temperature relationship. As the temperature increases, the volume of liquid chlorine will increase. Because of the potential for a rupture of a chlorine container under appropriate circumstances, designs have been developed to compensate for this factor. All containers have at least 15% of their volume allocated for vapour space. Fusible plugs are designed to melt at the same temperature which would cause the liquid chlorine to fill this space, so that a rupture is prevented (White, 1986).

Table 6.1. Physical and chemical properties of chlorine. (modified from ETSi, 1984)

State (15 °C, 1 atm)	gas
Shipping State	liquid
Boiling Point	-34.6 °C
Melting Point	-100.98 °C
Flammability	Noncombustible
Vapour Pressure	
25 °C	759.1 kPa
21 °C	589.2 kPa
Density (liquefied chlorine)	
0 °C	1.46 kg/L
STP	3.21 g/L
Solubility (in water) 20 °C	7.3 g/L
Odor threshold	0.3 to 0.5 mg/L
Vapour Density (Dry gas)	2.48
$Cl_2 + Fe \rightleftharpoons FeCl_2 + \Delta h$	

6.2.2 Density

Pressure has the greatest effect on chlorine vapour density. The temperature effect is negligible by comparison. For liquid chlorine the density decreases as the temperature increases.

6.2.3 Chemical Reactions

Dry chlorine, whether it is in the liquid or gaseous form is not corrosive to ferrous metals. However, it is almost impossible to have either form 100% free of moisture, therefore some corrosion results. Moist chlorine gas will readily corrode all ferrous metals, with only lead, gold, silver and platinum being inert (White, 1986). Aqueous solutions of chlorine accentuate this corrosivity. Therefore, handling materials must be made of PVC, polyethylene, fibreglass, or teflon except liquid chlorine readily attacks PVC or rubber materials. Therefore, in a closed system where PVC is used for aqueous chlorine solutions, these materials must be protected from the liquid chlorine (White, 1986).

6.2.4 Toxicity

Physiological responses to varying concentrations of chlorine gas are shown in Table 6.2. The inhalation of chlorine gas will affect the individual in one of two ways, depending on whether the gas is dry or moist. When dry chlorine is inhaled, the victim immediately experiences an irritating choking sensation. At this point, the victim should evacuate the area. Moist chlorine gas initially appears less harmful to victims because they do not experience the choking sensation. However, this reduces the sense of urgency and may cause victims to inhale a larger quantity of gas, which can result in a pulmonary edema that results in asphyxiation (White, 1986).

Liquid chlorine causes local irritation and severe burns. If it comes in contact with eyes, burning and possible loss of sight can result (ETSI, 1984). Liquid chlorine vaporizes so quickly that these effects are also applicable to high concentrations of chlorine gas. There is no doubt that the severity of injury is directly proportional to the quantity of gas inhaled.

6.3 Equipment

Chlorine is both extremely toxic to nearly all forms of life, and potentially corrosive to most metals. Both of these undesireable characteristics can be controlled through properly designed and maintained transfer, storage, and injection equipment. The containers must be of suitable sizes to meet the requirements of the particular industry. All materials which will be in contact with the chlorine must be suitable for the particular phase and moisture content of chlorine.

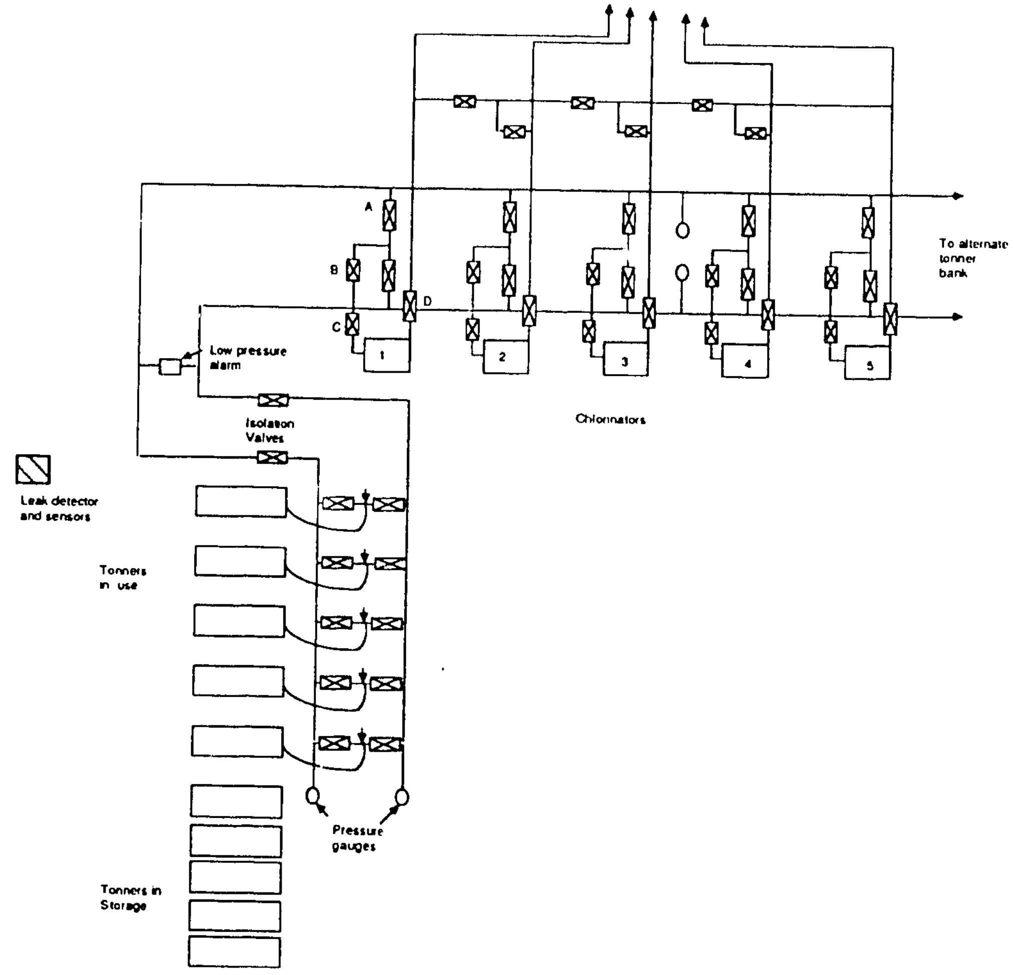


Figure 6.1 Process diagram of the chlorine storage and feed unit

Table 6.2. Recommended exposure limits for chlorine. (modified from ETSI, 1984)

Guideline (Time)	Recommended Level
Time weighted Averages (TWA)	
TLV (8 h)	1 ppm (3 mg/m^3)
TWA (8 h)	1 ppm (3 mg/m^3)
MIC	0.3 ppm (1 mg/m^3)
TWA	0.5 ppm (1 mg/m^3)
Short term exposure limits	
STEL (15 min)	3 ppm (9 mg/m^3)
Ceiling (15 min)	1 ppm
PEL (15 min)	0.5 ppm (1.5 mg/m^3)
Other Human Toxicities	
IDLH	25 ppm (75 mg/m^3)
LCLO (30 min)	873 ppm
TCLO	15 ppm

TLV - Threshold Limit Value
MIC - Maximum Immision Concentration
STEL - Short Term Exposure Limit
PEL - Permissible Exposure Limit
IDLH - Immediately Dangerous to Life and Health
LCLO - Lethal Concentration Low Value
TCLO - Toxic Concentration Low Value

6.3.1 The Chlorine Storage and Feed Unit

The chlorine storage and feed unit at this facility are located in a separate building (Fig. 6.1). The chlorine is stored in liquid form in one tonne containers (tonners). The capacity of a tonner is approximately 1000 kg. A duplicate steel piping manifold connects the tonners, which are oriented to provide chlorine gas rather than liquid, to the chlorinators. Five tonners are used at one time, with the alternate bank on standby.

The chlorinators control the chlorine gas flow rate with a variable v-notch orifice. A vacuum, which is created by the solution feed water at the injector, opens a diaphragm regulating valve within the chlorinator, allowing the chlorine gas to flow. The gas is added to the solution feed water at the injector. This chlorine solution then travels to the east end of the stilling basin where it is injected into the water (Fig. 5.1).

The chlorine storage room has duplicate leak detectors which activate an audible alarm and a ventilation unit. A low pressure alarm signifies a lack of chlorine gas in the piping up to the chlorinator. Two of the chlorinators have a high/low vacuum alarm which indicates a problem with the chlorinator or injection unit. A more detailed description or the chlorine unit is provided in Appendix A.1.

6.4 Review of Accidents

When trying to identify possible hazards it is very useful to review previous releases and consequences. This car give insight into possible release mechanisms control measures, and the success or failure of these measures. Only one tonne container releases have been reviewed in detail since this is the type of equipment used.

The causes of chlorine releases have been listed in order of frequency as reported by the Chlorine Institute (White, 1986). These are:

1. fire
2. flexible connection failure
3. fusible plug failure
4. Carelessness and Ignorance
5. valve packing failure
6. gasket failure
7. piping failure
8. equipment failure
9. collision
10. container failure.

Because of the volume-temperature relationship of chlorine, the enormous expansion in the volume of liquid clorine resulting from the heat of a fire could cause the rupture of a container. The 1 tonne containers and 68 kg cylinders have fusible plugs designed to melt at 70°C to prevent rupture. But, in any event, a major release would occur whether the container ruptures or the plugs melt. A ruptured container is considered worse because the sudden release of a large quantity of liquid chlorine greatly increases the size of the vapour cloud produced (Laubusch, 1962).

The flexible connectors which join the tonners or cylinders to the manifold are copper annealed lines which must be attached and detached whenever a new tonner is required. Their life expectancy depends on the number of connections made. When disconnected they are exposed to the air which promotes corrosion from within the tube. Regular inspection and maintenance can reduce the potential for a release by this route (White, 1986).

Fusible plugs have been found to melt without any direct cause. Corrosion and loss of screw length in the plug have also been causes of releases. From the numerous emissions via this route, there have been suggestions that fusible plugs be eliminated (White, 1986).

Ignorance of chlorine's behavior has resulted in accidents and increased severity of releases. A release involving tonne containers in Vancouver, illustrates how an undesirable situation became extremely hazardous to both the public and emergency response teams (ETSI, 1984).

Six tonners from a shipment of twelve fell off a transport truck in downtown Vancouver. One tonner was struck by a car, while another developed a leak at the welded seam. Firemen and police evacuated the immediate area and called an emergency response team. To try and control the chlorine vapours, the firemen sprayed a fog over the cylinders. However they were advised to stop because of the formation of hydrochloric acid which could increase the leak. After 1.5 h the emergency response team arrived. However their repair equipment could not seal the leaking seam. After 2 h a tarpaulin placed over the containers along with a water fog greatly reduced the vapours. After 3 h the chlorine was neutralized with caustic soda (NaOH), and finally after 5 h, the area was cleaned up and evacuees were allowed to return (ETSI, 1986).

This incident resulted in 77 people being taken to hospital. The number of people affected and the severity of the incident could have been reduced if several factors had been known. The equipment of the repair crew was inadequate. The quantity of vapour could have been reduced if the leaking container had been turned so that only gas was released. The emergency personnel were not aware of the dangers of combining water and chlorine. These factors all could have been prevented or the response improved with proper education.

Four other types of failures which have resulted in chlorine releases are all related to equipment failures, and they are relatively rare (White, 1986). Valve packing and gasket failures usually result in a slow release that can be quickly and readily repaired. Piping failures may be the result of corrosion, collision, or carelessness. Events causing such failures are dictated by the magnitude of the impact.

Most people have a high respect for the extremely toxic nature of chlorine and therefore are extra cautious in its vicinity. As used container failures are rare because high standards are maintained to ensure the safety of the public.

7. DEVELOPMENT OF SCENARIOS

7.1 Occupational Safety

There are several methods which can be used to identify hazards. Each of these methods begins with the premise that the system under normal routine operating conditions, is performing correctly. The initial assumption is that stress must be induced into the system for a problem to be created. This philosophy was used for the identification of hazards in the chlorine feed unit.

Initially the identification of the hazards was done in a very general way on the entire system. This provided an overview of the process and gave an indication of how the different scenarios would interact. Once the overview and main scenarios were complete, those areas which required a more detailed review could be analysed.

7.1.1 Inititiating Events and Damage States

The defining of boundaries is important so that each scenario can be developed equally. The initiating events were developed by using the HAZOP guide words on each of the main sections in the feed unit. By developing the initiating events, the scenario in the form of an event tree was created, resulting in the previously defined damage state. This provided the initial hazard scenarios. Once developed, the causes of the initiating events could be reviewed. In some instances entirely new scenarios were developed, with the initiating events becoming an end state. Some sections in the scenarios were found to require more detailed development than others. These precipitating scenarios were developed through the use of a fault tree.

Once the scenarios were complete, they were separated into the events which resulted in particular damage states. This provides a simpler frequency analysis, since only those damage states of concern needed to be developed.

Damage States

The damage states identified were: a major chlorine gas or liquid release, chlorine vented to the atmosphere, injury, plant shut down due to inadequate chlorination, and plant stable with chlorination continuing. These initial damage states provided broad enough end states so that each scenario could be terminated by one of the damage states.

For occupational safety, the damage state of interest was that defined as injury. Those events which would lead to a possible injury were removed from overall scenarios and reviewed to find common areas which would lead to the injury. Frequency and consequence analyses were then performed on these sections.

Initiating Events

Using HAZOP guide words NONE, MORE OF, LESS OF, PART OF, MORE THAN and OTHER THAN, and the standard codes of practice, initiating events were identified. Each initiating event and scenario for the various parts of the feed unit have been represented by an event tree. These initial scenarios represented the complete response to a stress induced in the system. These intiating events in some cases directly related to the damage state injury, and in other instances only small sections resulted in that state. These overall scenarios will be reviewed, followed by combining of specific events which could lead to injury.

7.1.2 The Hazardous Scenarios

Injection Unit

The injection or eductor unit provides the mechanism for applying the chlorine. The water that passes through the injector creates the vacuum which is critical for the correct operation of the chlorine unit. Using the different HAZOP guide words, possible stress induced on the system through variances in the operation of the vacuum was analyzed.

The first scenario was developed using the guide words NONE and LESS OF. Both guide words were used in developing the scenario, since the response of the system to either a no vacuum or partial vacuum situation would be the same, when the situation is induced at the eductor. The event tree was structured so that the system response which would be considered correct is written horizontally, whereas a failure response is written vertically. Therefore by following the first horizontal line, the correct system response or designed system response should be achieved (Fig. 7.1). For either a partial or no vacuum situation, the first system response was the closing of the diaphragm and in line check valves in the PVC line. This prevents backflow of water from the injector to the chlorinators. The next system response is the closure of the pressure regulating valve. This stabilizes the chlorine gas up to the chlorinator, and prevents chlorine gas from continuing to flow and ultimately contaminating the injection water line, or causing a leak scenario if maintenance work required access to this line. If the check valves do not close, and the injector water is still available, the chlorinator may be flooded. This is particularly true for the partial vacuum situation in which there may be enough of a vacuum to keep the two check valves open.

The main damage from this scenario would be from the problem not being recognized quickly enough. When the vacuum is reduced to below 100 mm of water the low vacuum alarm should sound for chlorinators 1 and 2. For the other three chlorinators, the loss of the vacuum would have to be discovered through inspection.

The damage state of injury could occur, if the pressure regulating valve remains open. The gas should vent if this occurs. However, if the gas did not vent and continued flowing in the piping, an injury could occur if the proper isolation procedures were not followed by the maintenance staff. The complete scenario with the different possible combinations of successes and failures is shown in Figure 7.1.

While the complete or partial loss of the vacuum can be termed as an initiating event, there are different ways by which this situation can be developed. To represent the combination of events which would result in the loss of the vacuum, a fault tree was used, in which the final result is the initiating event or the loss of the vacuum (Fig. 7.2). Since each event can independently cause the loss of the vacuum, they are connected through 'OR' gates.

Vacuum Line Breaks

The next initiating event considered, was a vacuum line break. Again it was developed through the HAZOP guide word NONE. This scenario was developed separately since the consequences of the scenario could be influenced by the location of the break along with the failure of different parts of the system. The set up of the event tree is similar to that of the injector scenario in that a horizontal movement in the tree represents a successful response (Fig. 7.3a and 7.3b).

There are three possible locations for the break, either the injector room, the storage room, or between the injector and storage room. The critical response is the closure of the inline check valve and the pressure regulating valve if a break occurs. The diaphragm check valve may remain open, sucking in air since the water would still be available to apply the vacuum. These closures result in the isolation of the water and chlorine gas. The separate consideration of the three locations is important for the length of time before discovery. Both the injector and storage rooms have detectors which are sensitive enough to be activated by the level of residual which would be released from the vacuum line in such an event. If the break occurs between the two rooms, then the discovery of the event is dependent on inspection. The main damage state from this scenario is the prevention of chlorination. Injury can occur if there is a failure of the pressure regulating valve.

The development of causes of the break were depicted through a fault tree (Fig. 7.4). Because any of these events can result in the initiating event they are combined using 'OR' gates.

Falling Chlorine Pressure

The NONE and LESS OF guide words were then applied to the storage room so that the scenario of no or partial chlorine flow was developed. The tonners must be replaced about once per week. The progression of the scenario depends on a series of actions taken by the operator to shut off the empty tonner bank and open the full tonner bank (Fig. 7.5). There are several actions which could prevent the damage state of a plant stable with plant chlorination continuing. Most of the actions involve leaving a valve closed which

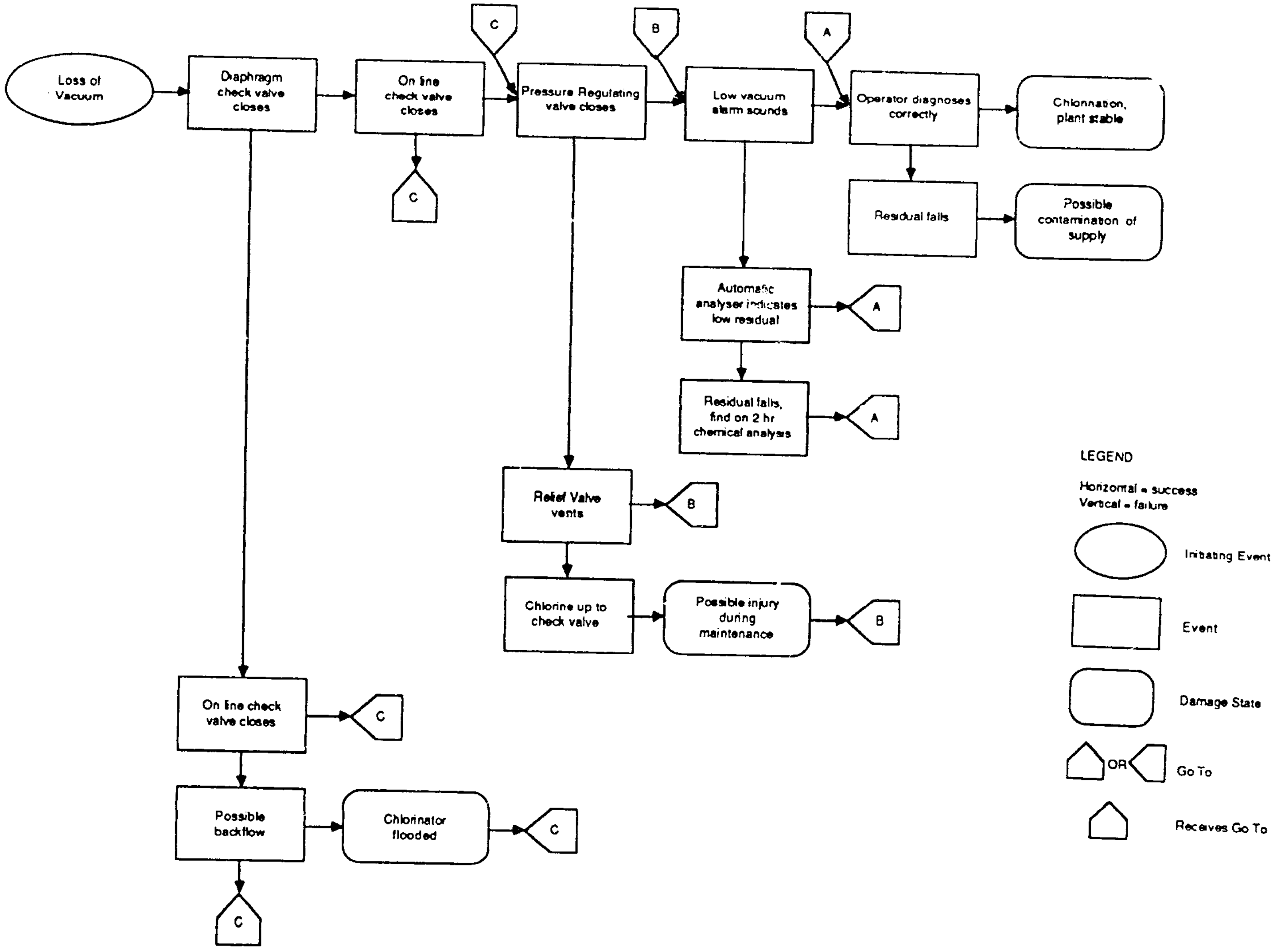

Loss of Vacuum
Diaphragm check valve closes
On line check valve closes
C
Pressure Regulating valve closes
B
Low vacuum alarm sounds
A
Operator diagnoses correctly
Chlorination, plant stable
C
Residual falls
Possible contamination of supply
Automatic analyser indicates low residual
A
Residual falls, find on 2 hr chemical analysis
A
Relief Valve vents
B
Chlorine up to check valve
Possible injury during maintenance
B
On line check valve closes
C
Possible backflow
Chlorinator flooded
C
C
LEGEND
Horizontal = success
Vertical = failure
Initiating Event
Event
Damage State
OR
Go To
Receives Go To

Figure 7.1 Event tree diagram for a partial or complete loss of vacuum

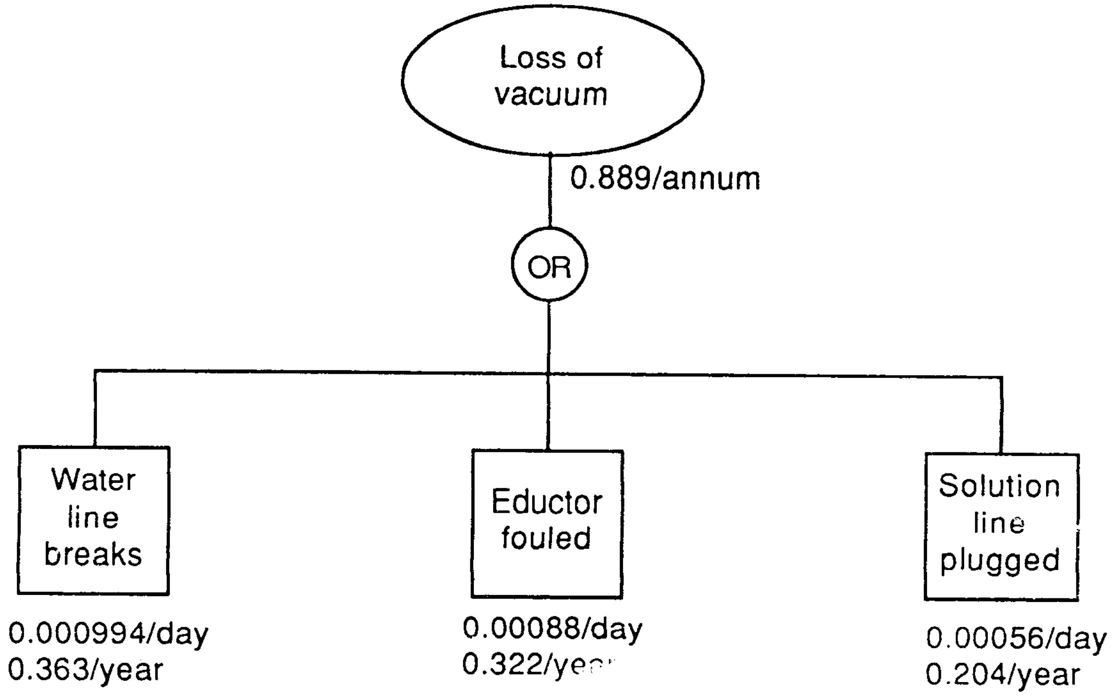
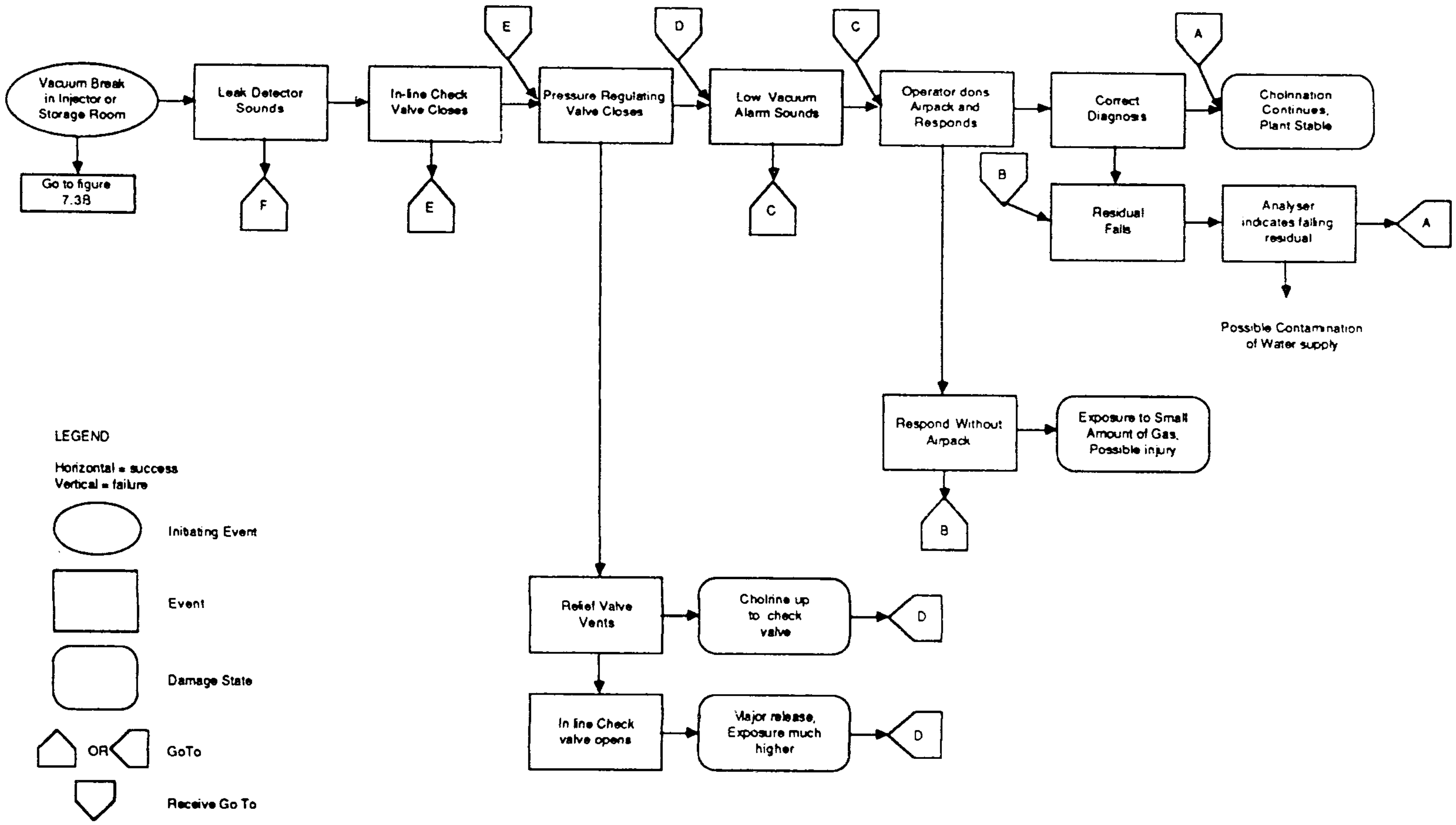


Figure 7.2 Fault tree diagram for a partial or complete loss of vacuum



E
D
C
A
Vacuum Break in Injector or Storage Room
Go to figure 7.3B
Leak Detector Sounds
F
In-line Check Valve Closes
E
Pressure Regulating Valve Closes
Low Vacuum Alarm Sounds
C
Operator dons Airpack and Responds
Correct Diagnosis
Cholrination Continues, Plant Stable
B
Residual Fails
Analyser indicates failing residual
A
Possible Contamination of Water supply
Respond Without Airpack
Exposure to Small Amount of Gas, Possible injury
B
Relief Valve Vents
Cholrine up to check valve
D
In line Check valve opens
Major release, Exposure much higher
D
LEGEND
Horizontal = success
Vertical = failure
Initiating Event
Event
Damage State
OR
GoTo
Receive Go To

Figure 7.3a Event tree for a vacuum line break between injector or storage room

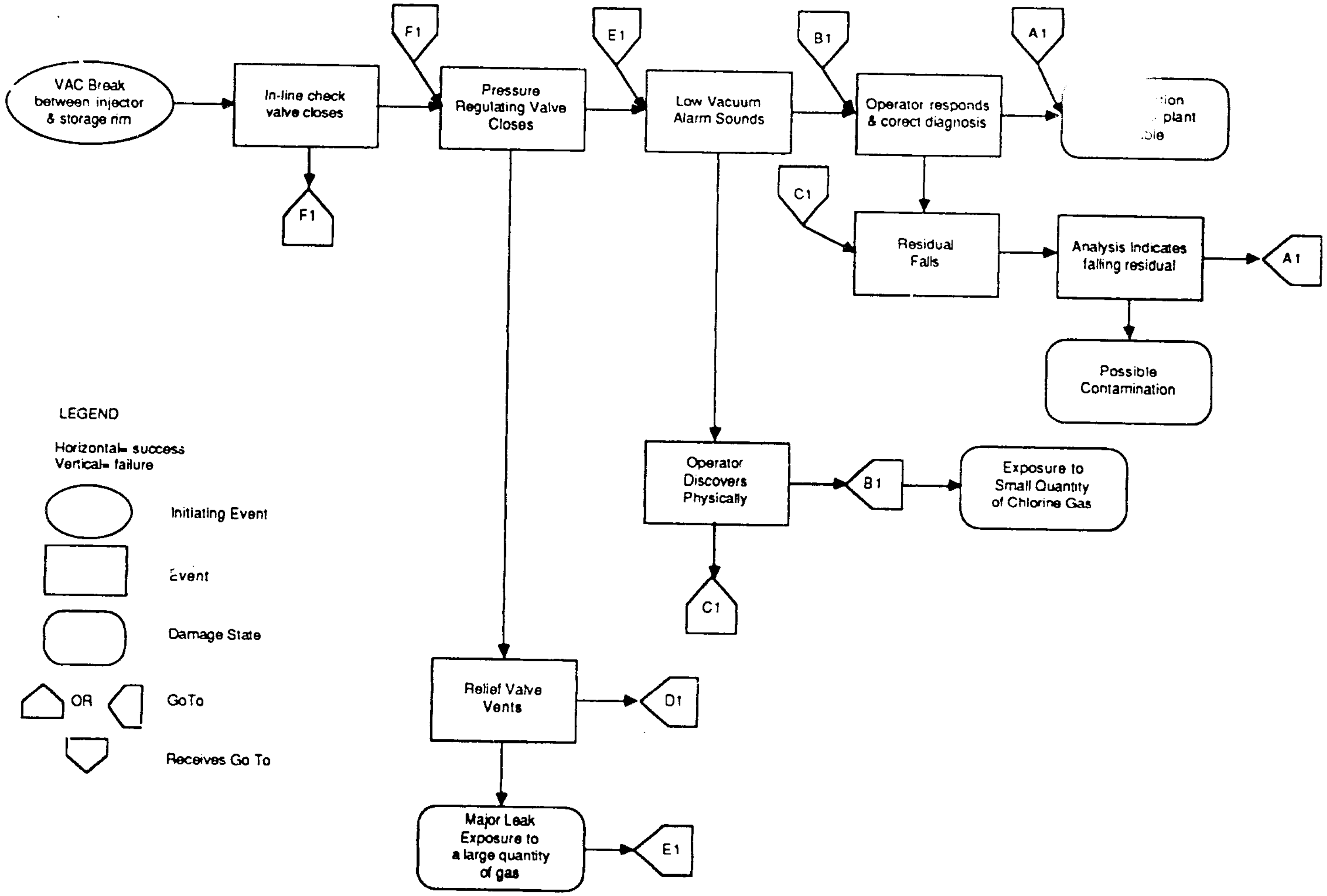

VAC Break between injector & storage rm
In-line check valve closes
F1
F1
Pressure Regulating Valve Closes
E1
Low Vacuum Alarm Sounds
B1
Operator responds & corect diagnosis
A1
ion plant ble
C1
Residual Falls
Analysis Indicates falling residual
A1
Possible Contamination
Operator Discovers Physically
B1
Exposure to Small Quantity of Chlorine Gas
C1
Relief Valve Vents
D1
Major Leak Exposure to a large quantity of gas
E1
LEGEND
Horizontal= success
Vertical= failure
Initiating Event
Event
Damage State
OR
GoTo
Receives Go To

Figure 7.3b Event tree for a vacuum line break between injector or storage room

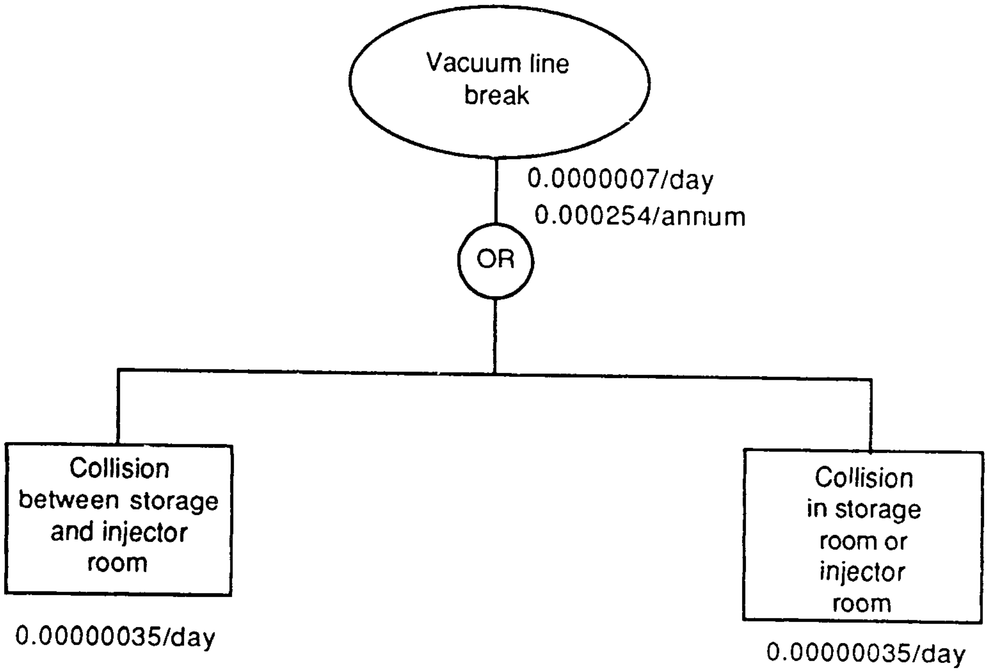

Vacuum line break
0.0000007/day
0.000254/annum
OR
Collision between storage and injector room
0.00000035/day
Collision in storage room or injector room
0.00000035/day

Figure 7.4 Fault tree diagram for a vacuum line break

prevents the chlorine from reaching or leaving the chlorinators. Once the operator adjusted the flow rate, the lack of chlorine would be recognized and the problem rectified. The section of the scenario that would create the most serious situation requires the operator to leave three valves open. The chlorine gas could then pass from the full tonner bank to the empty tonner bank. The extreme pressure difference and rapid velocity of the gas would cause the lines to freeze forming liquid chlorine. This would result in a plant shut down.

The possible causes for a no or partial chlorine flow situation which would create the falling chlorine pressure are represented by the fault tree shown in Figure 7.6. These events are also combined using 'OR' gates.

Chlorinator Plugged

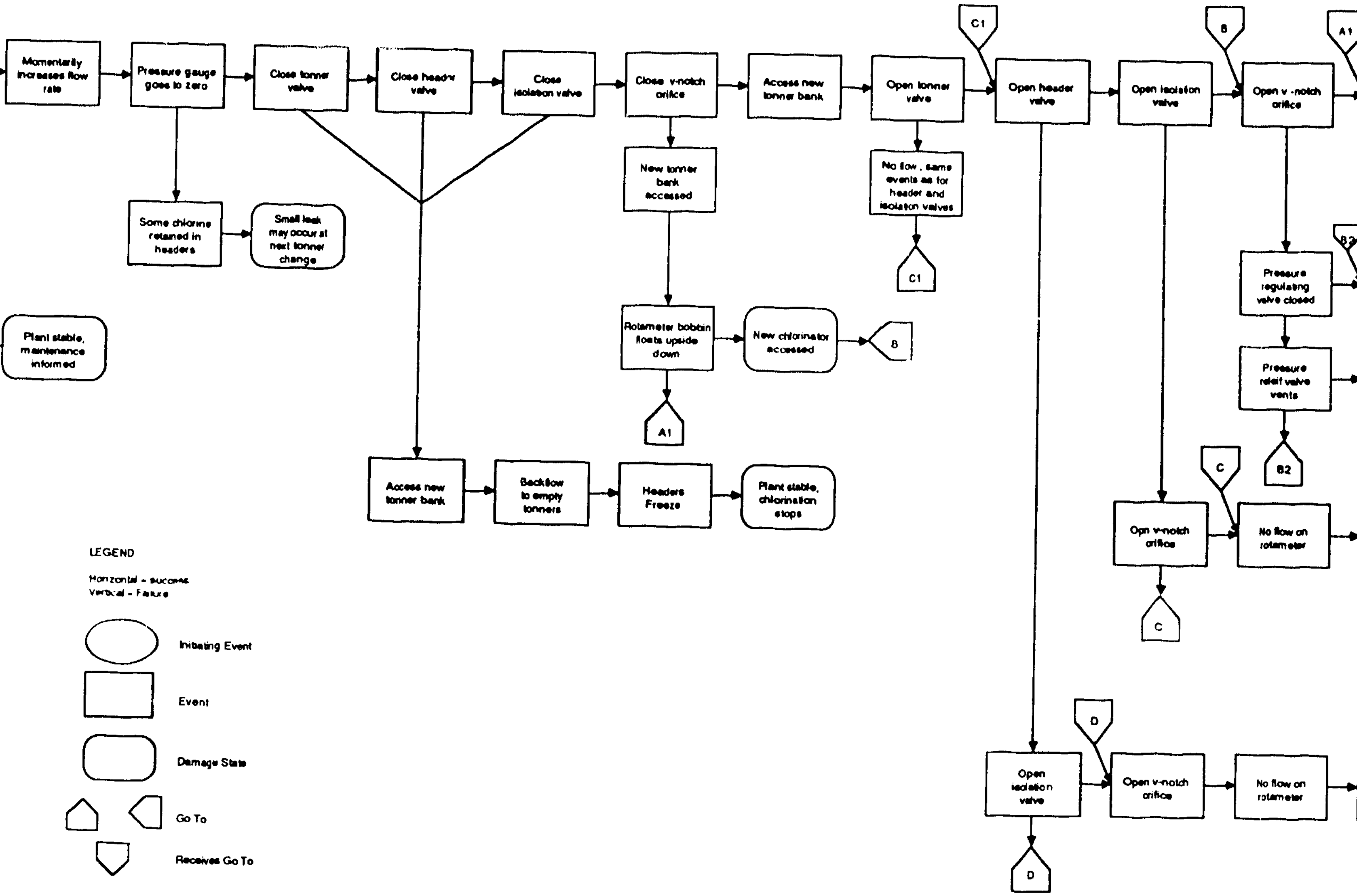
The situation of no chlorine flow could also be a result of the chlorinator being plugged. This scenario is really a response or extension of the no vacuum scenario when the check valve in the injector room does not hold and allows water to pass into the chlorinator. It is also a response to the scenarios which result in liquid chlorine filling the pipes and the chlorinator. This particular scenario involves the procedure the maintenance personnel would follow in the event the chlorinator was plugged (Fig. 7.7). This scenario may not follow the same type of development as the previous scenarios, but it does involve actions which can be expressed as successes or failures that result in a particular outcome.

The event tree shown in Figure 7.7 represents the scenario of a plugged chlorinator. Critical stages in this scenario involve the correct isolation of the chlorinator and that the valves and pressure gauges are not faulty. If these individual events were all performed incorrectly, there is the possibility of a major chlorine leak and injury.

The fault tree which represents the development of this initiating event is made up of the other senerios chlorinator flooded or liquid chlorine in the headers. The flooding of the chlorinator does not occur from a single action but follows a sequence of events. This is also true for the scenario representing liquid chlorine in the headers (Fig. 7.8).

Liquid Chlorine in Headers

HAZOP allows the review to consider different phases of the material with the guide word MORE THAN. Having liquid chlorine in the pipes is an initiating event for the plugged chlorinator scenario (Fig. 7.7). The damage states from this scenario result in a controlled release of the chlorine to the atmosphere, or a possible injury should the scenario not follow the success route. The isolation of the various piping sections and chlorinators is critical for controlling the quantity of chlorine gas released.



the chlorine pressure falling in headers

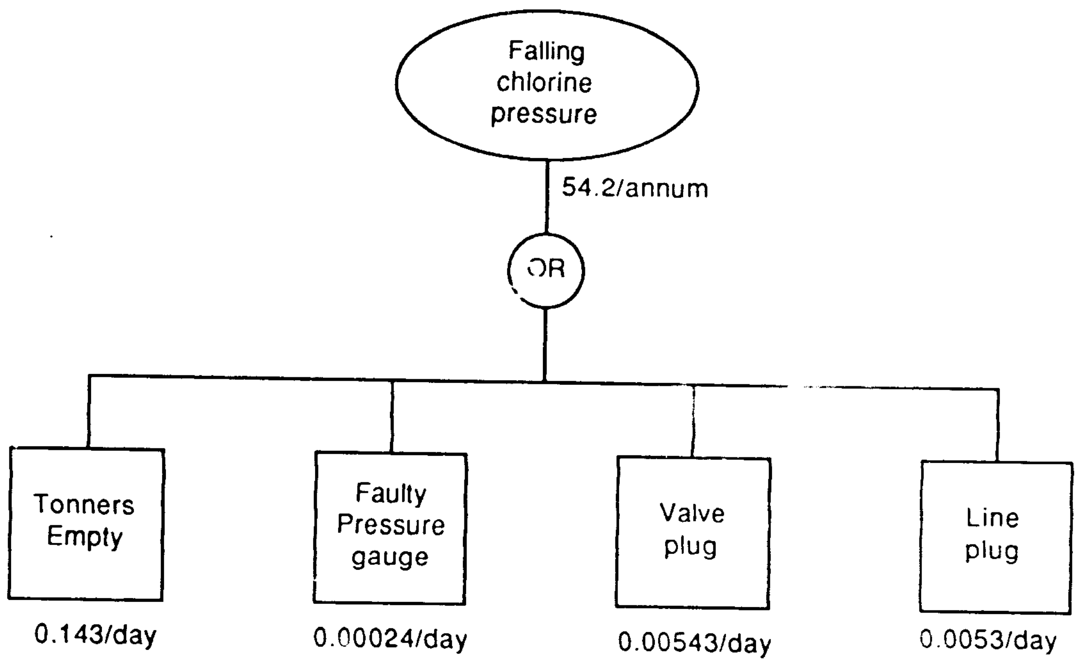


Figure 7.6 Fault tree for chlorine pressure falling in headers

This intitiating event has a rather complex fault tree since there are many ways in which this event can be reached (Fig. 7.9). These different sections of the fault tree are separate scenarios in themselves. These separate scenarios are combined with 'OR' gates since they can independently cause the liquid chlorine scenario.

Tonner Valve Plugged

If the demand rate is greater than the evaporation rate, the available chlorine gas no longer flows naturally under its own pressure, but is forced or sucked from the tonners. By applying the HAZOP guide word PART OF, the scenario of having one or more tonner valves plugged so that there is not enough chlorine gas to meet the demand is considered. When this occurs, the rapid flow of chlorine causes the chlorinator and pipes to freeze, resulting in the formation of liquid chlorine in the lines.

Heater Failure

The HAZOP guide word LESS OF was applied to the heating unit in the storage room. The initiating event is the failure of the main heating unit. The impact of this failure depends on the outside temperature. The impact of a heater failure depends on how quickly the room cools compared with how quickly the situation is discovered. The greatest damage occurs from liquid chlorine in the pipes. This damage state results in the temporary shut down of the plant so repairs can be made.

Other

The other two possible mechanisms for having liquid chlorine in the lines do not have scenarios associated with them, but are the result of an equipment failure and a human error. A broken eductor would be accessing liquid rather than gaseous chlorine. If the operator attaches the flexible connector to the wrong valve then, liquid chlorine rather than gaseous chlorine is being provided.

Major Leak

This scenario is similar to the plugged chlorinator and the liquid chlorine in pipes scenarios, because it is a response scenario. It considers the procedures that have been developed in the event a major leak occurs (Fig. 7.10). Critical to handling such a scenario is the activation of the leak detector and sounding of the alarm. This gives an immediate warning to personnel. Injury would most likely occur if the personnel were in the room when the incident creating the leak occurred. Preventing a serious incident depends both on the cause of the leak and the response time to the leak. There are different scenarios which could create a major leak scenario. Each of these shall be considered as a fault tree (Fig. 7.11).

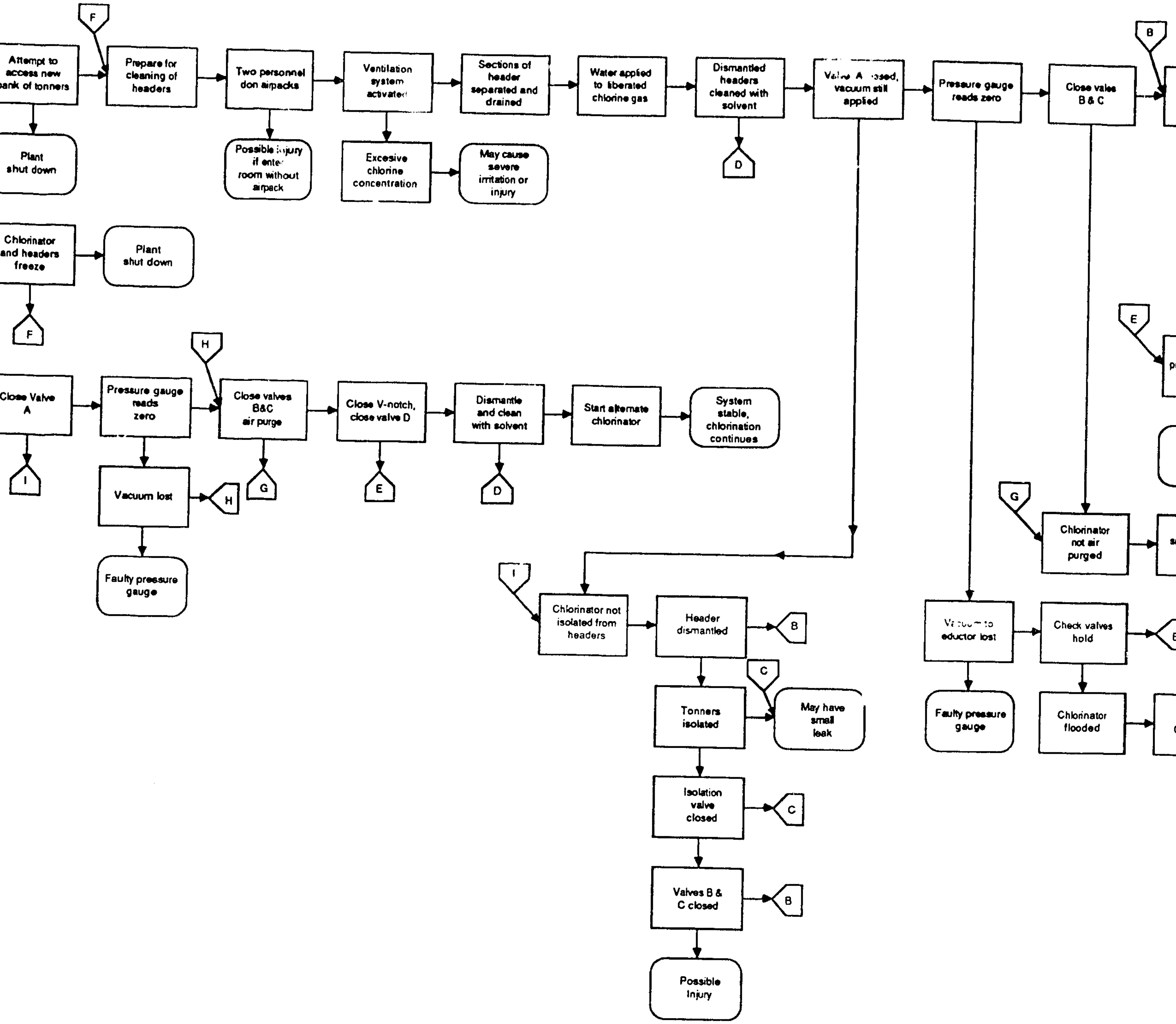
Tonner Rupture

The scenario for a tonner rupture has been developed as a fault tree (Fig. 7.12). There is no doubt that such an event would result in a major chlorine leak. The development of causes for a possible tonner rupture was performed using the HAZOP guide words MORE OF and OTHER THAN. The MORE OF guide word considers the possible scenario of excess heat causing the chlorine gas to liquefy. For a tonner rupture to occur, the fusible plugs must fail by not melting.

The OTHER THAN guide word considers the many movements a tonner undergoes. It is transported from the truck to the storage platform, and then onto one of the feeding banks. Failure of the hoist, storage platform or a collision during any one of these movements could cause a rupture.

Tonner Valves and Fusible Plugs

Both of these par s of tonner would contribute to a major chlorine release in the event of their failure (Figs. 7.13, 7.14). The MORE OF guide word considers the possibility of additional heat. Such a situation is bound to create a chlorine release whether it is from the fusible plugs melting or from a tonner rupture. There are three possible mechanisms by which this situation could occur. The first is a fire which affects the storage room. The second is related to the loss of the main heating unit. If auxilary units are brought into the room they must be positioned carefully so they are not directly aimed at the tonners. The


F
Attempt to access new bank of tonners
Prepare for cleaning of headers
Two personnel don airpacks
Ventilation system activated
Sections of header separated and drained
Water applied to liberated chlorine gas
Dismantled headers cleaned with solvent
Valve A closed, vacuum still applied
Pressure gauge reads zero
B
Close vales B & C
Plant shut down
Possible injury if enter room without airpack
Excesive chlorine concentration
May cause severe irritation or injury
D
Chlorinator and headers freeze
Plant shut down
F
E
H
Close Valve A
Pressure gauge reads zero
Close valves B&C air purge
Close V-notch, close valve D
Dismantle and clean with solvent
Start alternate chlorinator
System stable, chlorination continues
I
G
E
D
Vacuum lost
H
Faulty pressure gauge
G
Chlorinator not air purged
I
Chlorinator not isolated from headers
Header dismantled
B
C
Tonners isolated
May have small leak
Isolation valve closed
C
Valves B & C closed
B
Possible Injury
Vacuum to eductor lost
Check valves hold
Faulty pressure gauge
Chlorinator flooded

tree for a plugged chlorinator

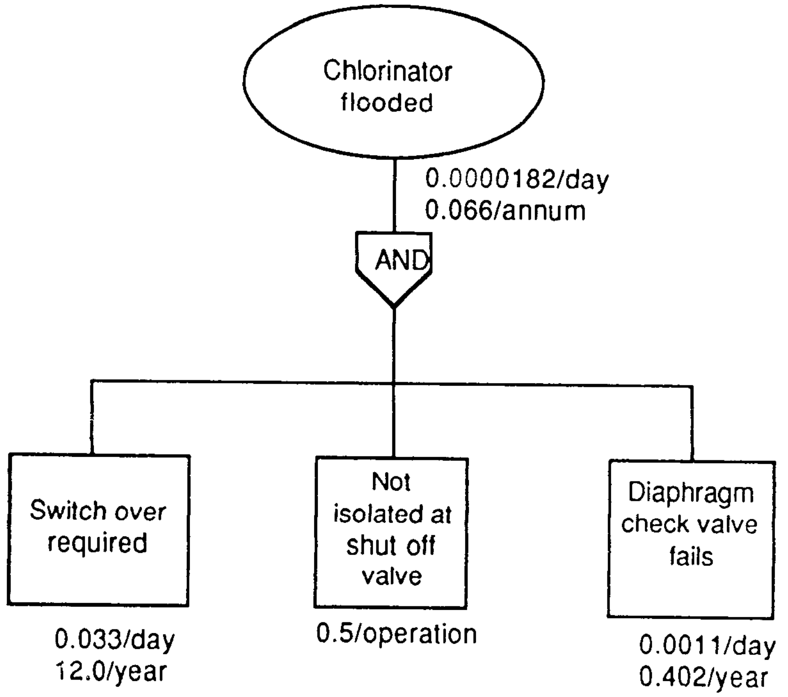


Figure 7.8 Fault tree for a plugged chlorinator

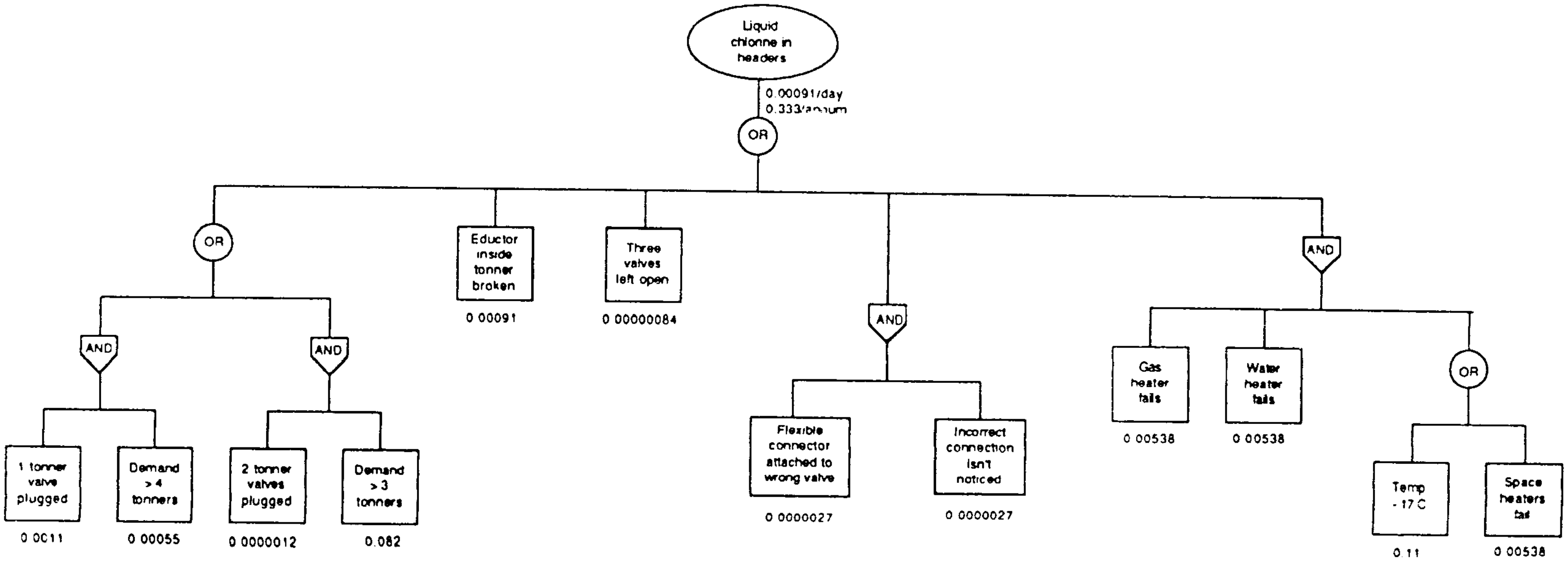


Figure 7.9 Fault tree for liquid chlorine in the headers

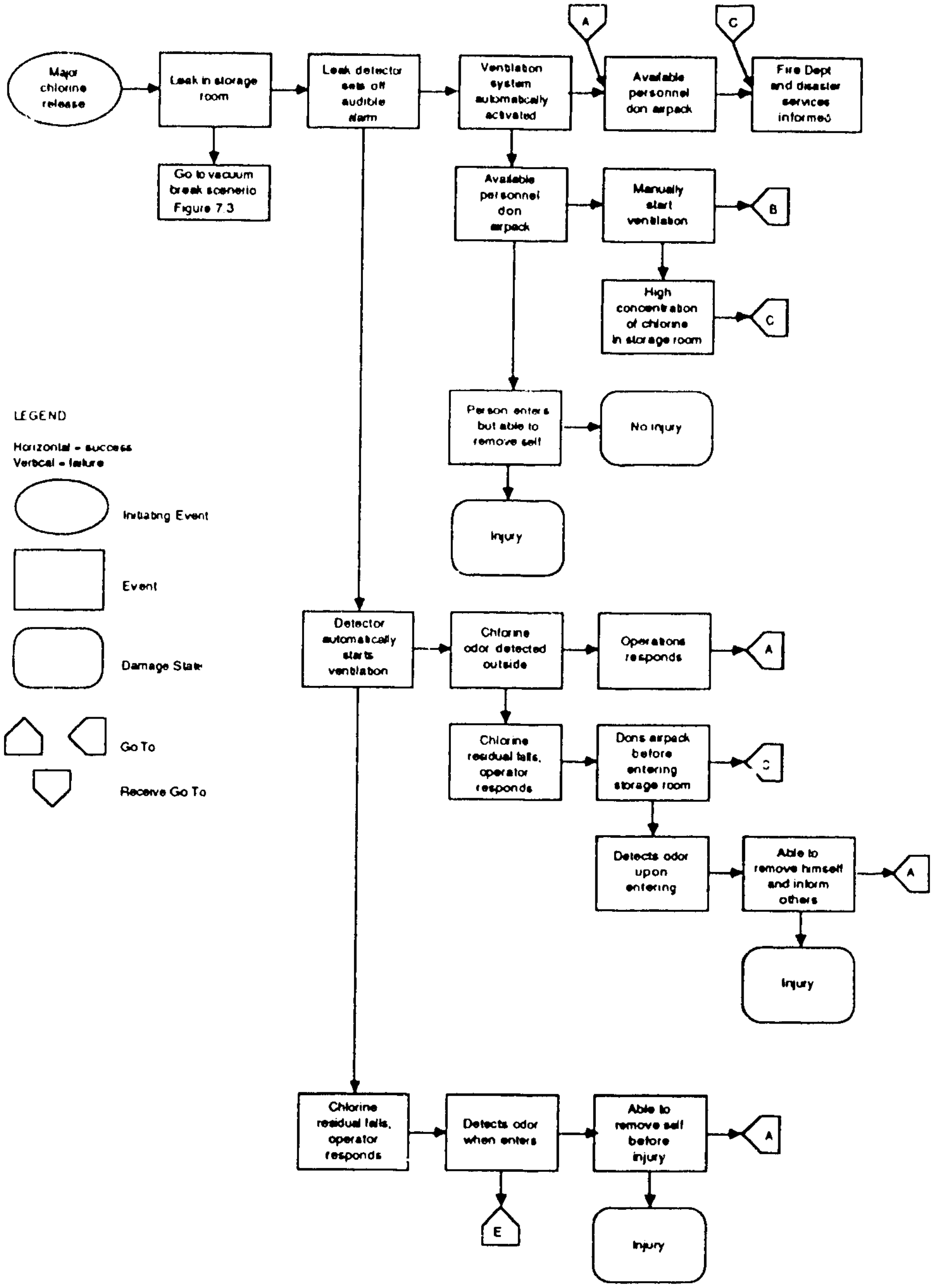

A
C
Major chlorine release
Leak in storage room
Go to vacuum break scenario Figure 7.3
Leak detector sets off audible alarm
Ventilation system automatically activated
Available personnel don airpack
Fire Dept and disaster services informed
Available personnel don airpack
Manually start ventilation
B
High concentration of chlorine in storage room
C
Person enters but able to remove self
No injury
Injury
LEGEND
Horizontal = success
Vertical = failure
Initiating Event
Event
Damage State
Go To
Receive Go To
Detector automatically starts ventilation
Chlorine odor detected outside
Operations responds
A
Chlorine residual fails, operator responds
Dons airpack before entering storage room
C
Detects odor upon entering
Able to remove himself and inform others
A
Injury
Chlorine residual fails, operator responds
Detects odor when enters
Able to remove self before injury
A
E
Injury

Figure 7.10 Event tree for an uncontrolled release

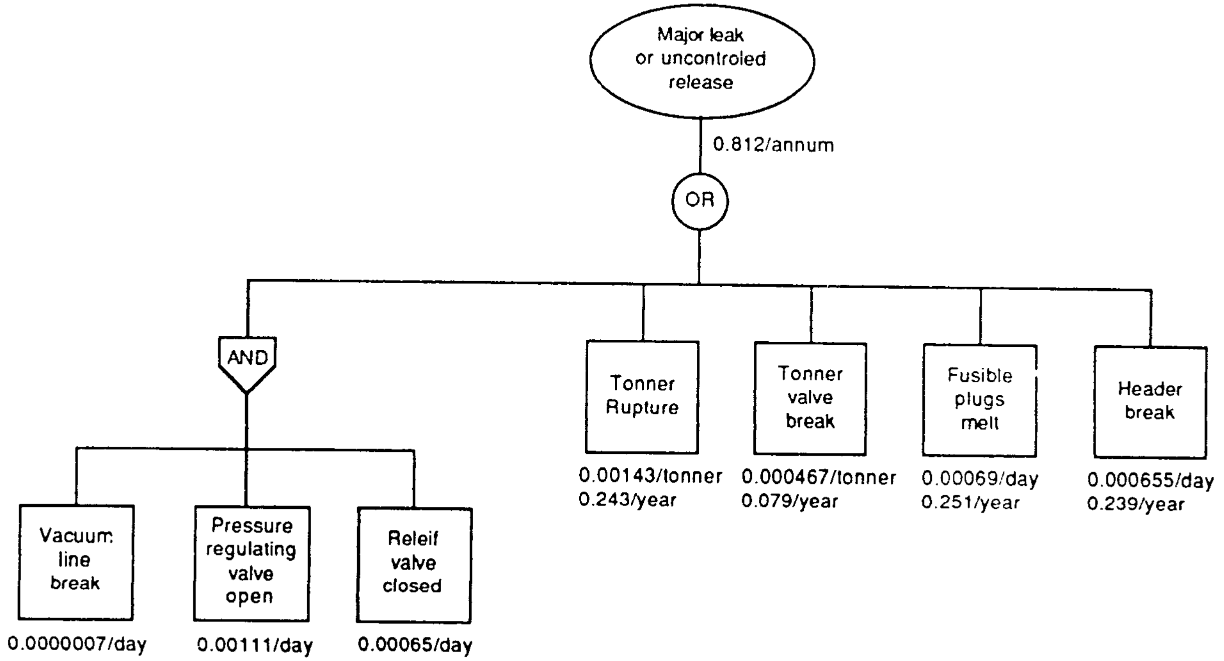


Figure 7.11 Fault tree for an uncontrolled release

BLANK PAGE INSERT.̄D

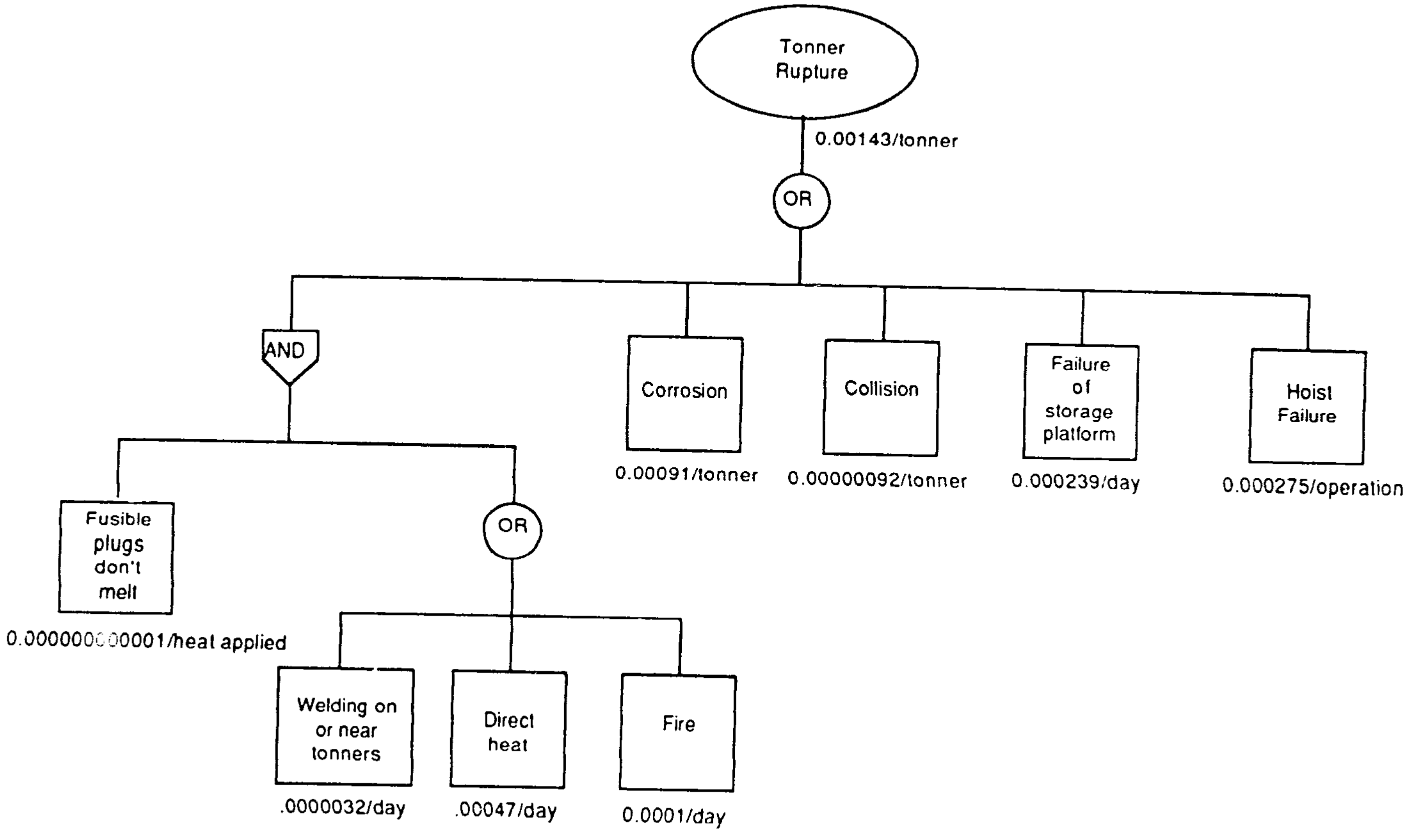


Figure 7.12 Fault tree for a tonner rupture

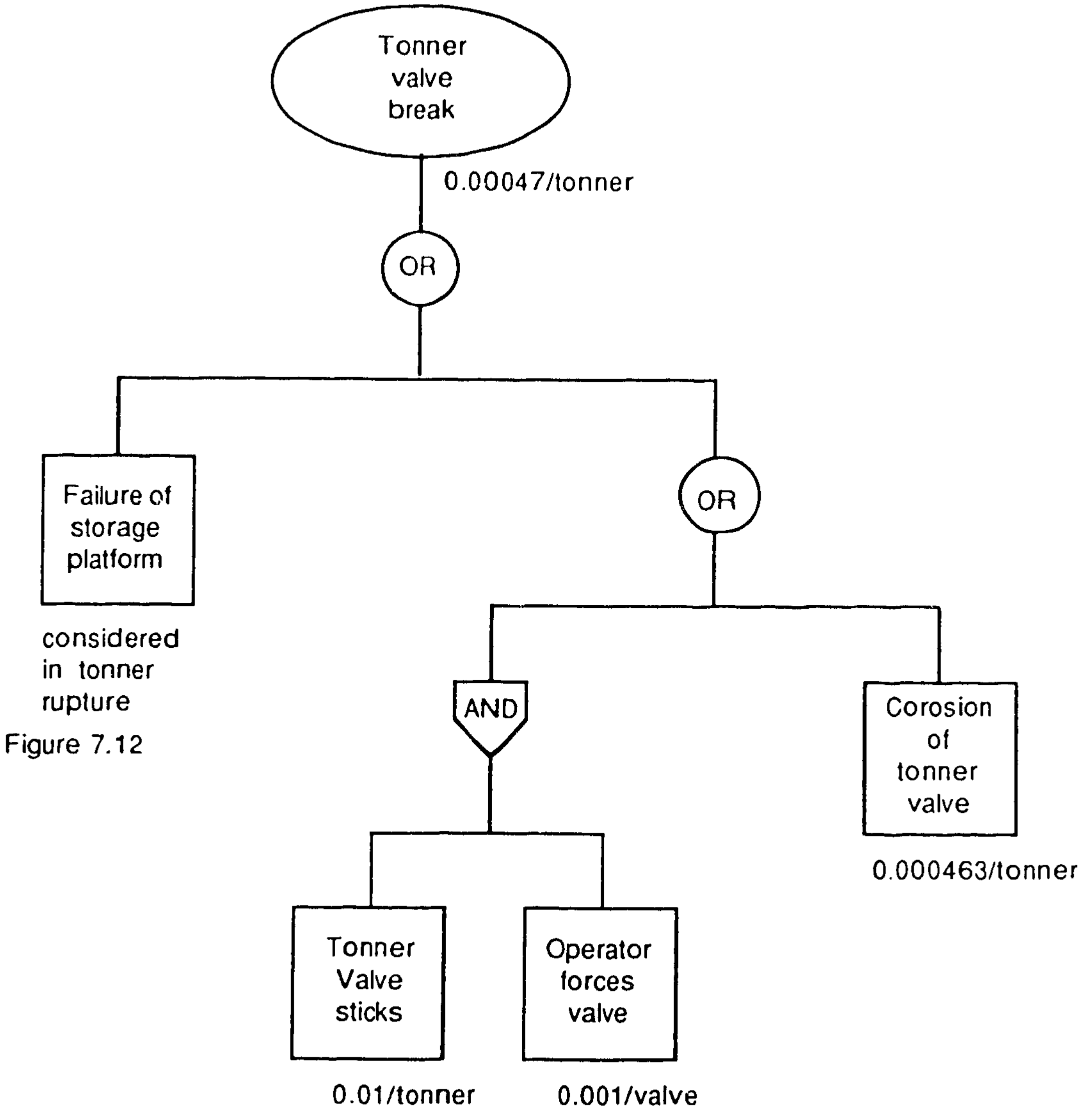


Figure 7.13 Fault tree for the failure of a tonner valve

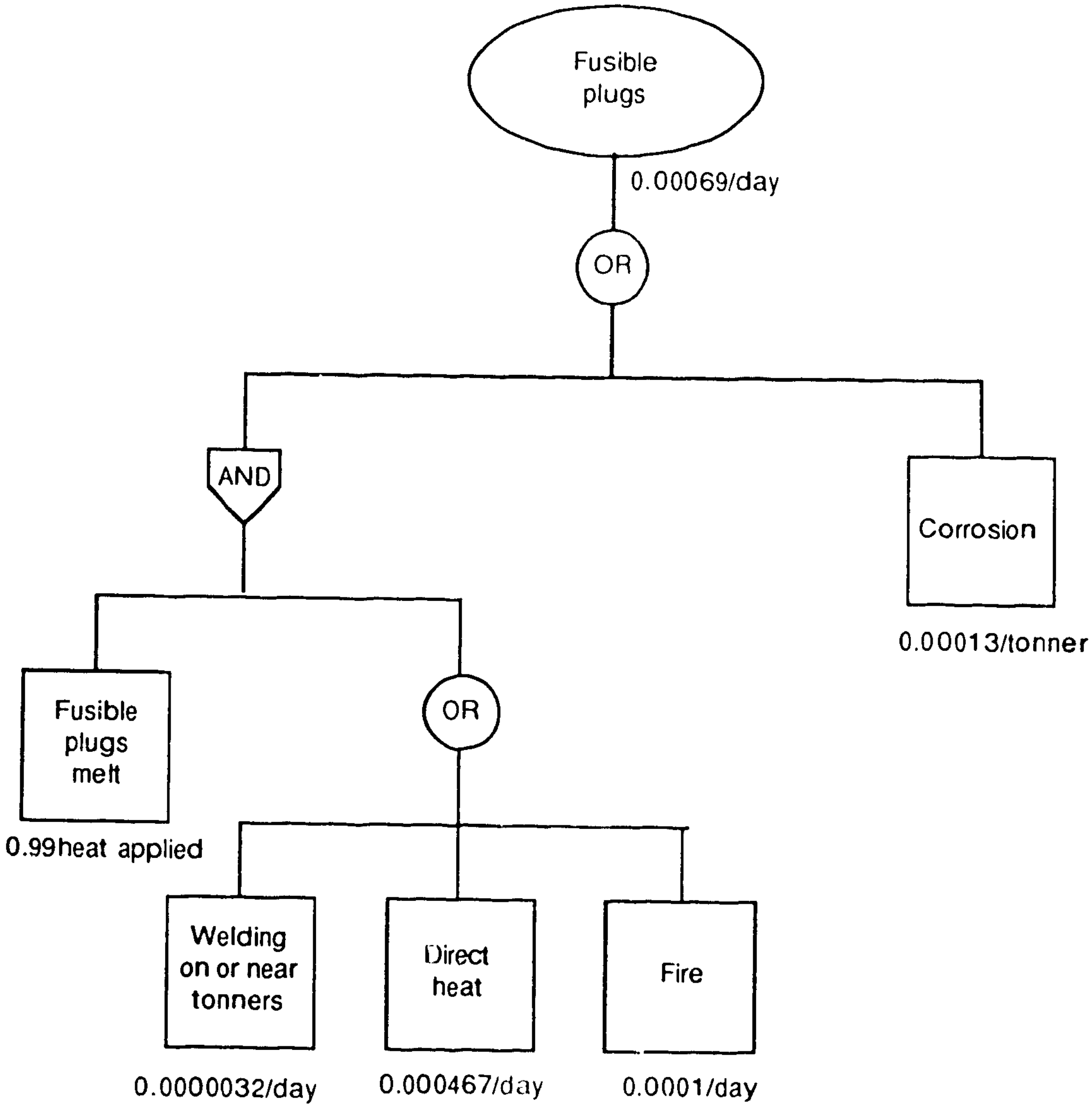


Figure 7.14 Fault tree for the failure of a fusible plug

damage state occurs if the proper corrective procedures are not followed. Those scenarios which result in liquid chlorine in the headers, the chlorinator being plugged or a loss of vacuum would create a controlled release (Fig. 7.16).

The other type of scenarios which result in injury would be from an uncontrolled release. These scenarios result in the immediate release of chlorine gas or liquid (Fig. 7.17). Injury occurs when an operator unable to remove himself is exposed to the gas for an extended period of time. Those events resulting in a major chlorine leak can all be considered under this heading. The preceding fault trees all focused on the final damage state of injury. From the main event trees, those smaller scenarios which could eventually result in an injury were combined into fault trees. For the latter stages of the frequency and consequence analysis, this refinement greatly simplified the results.

7.2 Water Supply Contaminated

The damage state of plant shut down because of inadequate chlorination was also reviewed. The damage state was further developed to evaluate the impact on water quality. The objective of this analysis was to judge the risk associated with an inadequately disinfected water. It does not address the adequacy of the chemical as a disinfectant or the risk posed by reaction products as a

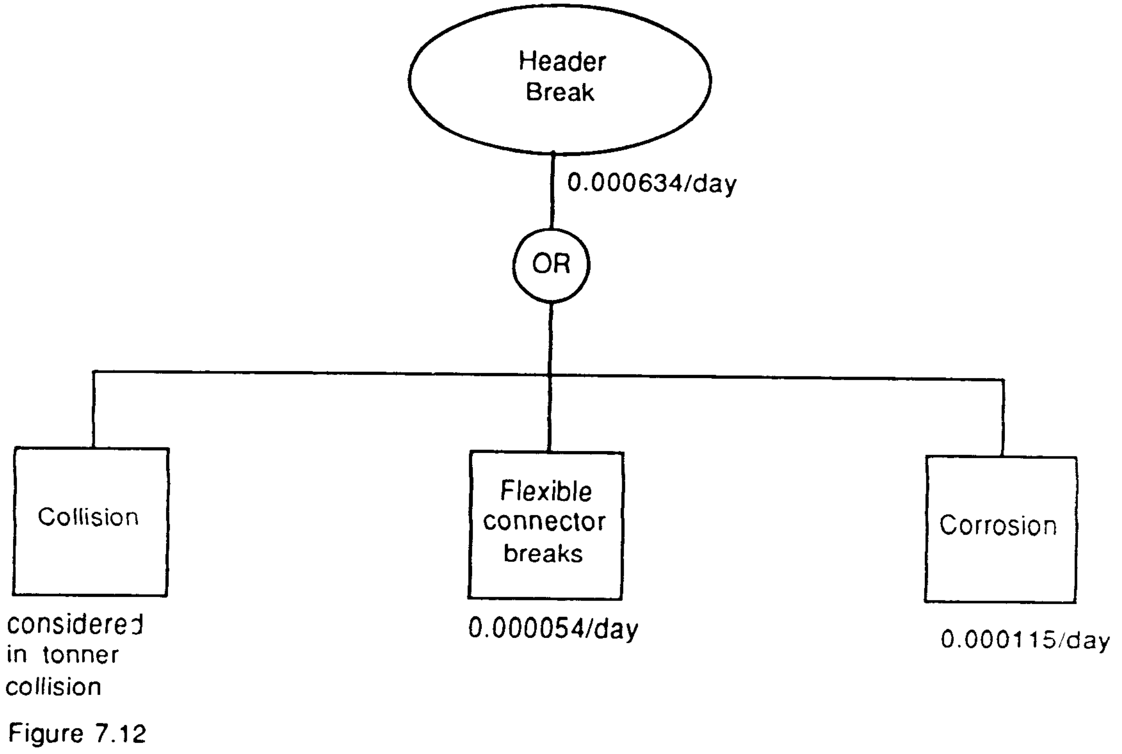


Figure 7.15 Fault tree for a header hreak

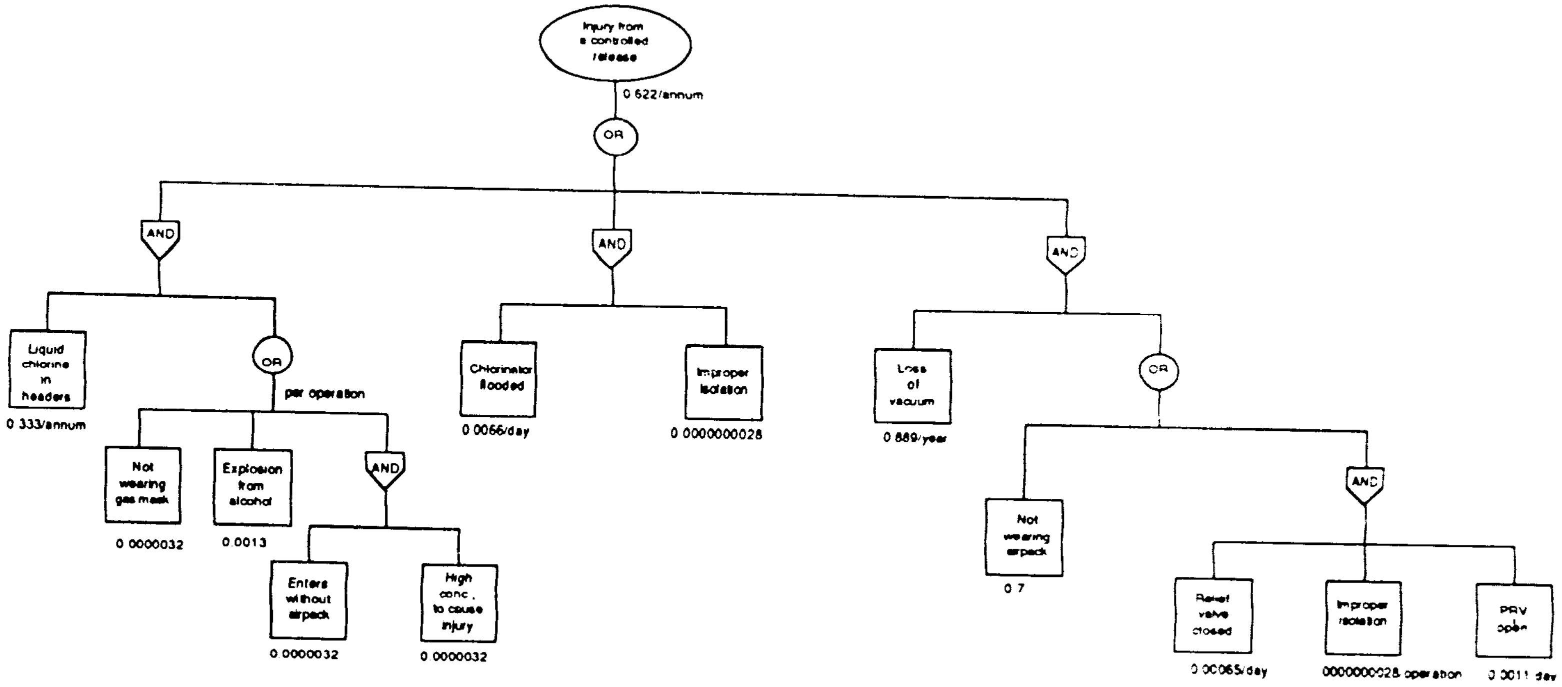


Figure 7.16 Fault tree for a controlled release

result of the disinfection. This analysis only considers the adequacy of the existing feeder equipment and the warning systems which are presently in place.

The main event trees developed in the general hazard identification were used to develop a fault tree which had as its damage state the water not being adequately disinfected (Fig. 7.18). These fault trees are similar to those developed for the injury damage states in which all scenarios resulting in an injury damage state were combined for the frequency and consequence analysis.

For the fault tree scenario representing the water not chlorinated damage state, each event represents some mechanism by which the chlorine flow to the injector has been stopped, and the appropriate warning system has not been activated (Fig. 7.18). While each event would stop chlorination, the combined inactivation of the alarm system is critical for the water to be of unacceptable quality. The warning system indicates to the operator that an event has occurred which affects the chlorination. He can then determine if the event can be rectified so that chlorination can continue, or in the event that it cannot, that a plant shut down is required. If the operator is unaware of the situation, there is the possibility that inadequately disinfected water could be distributed.

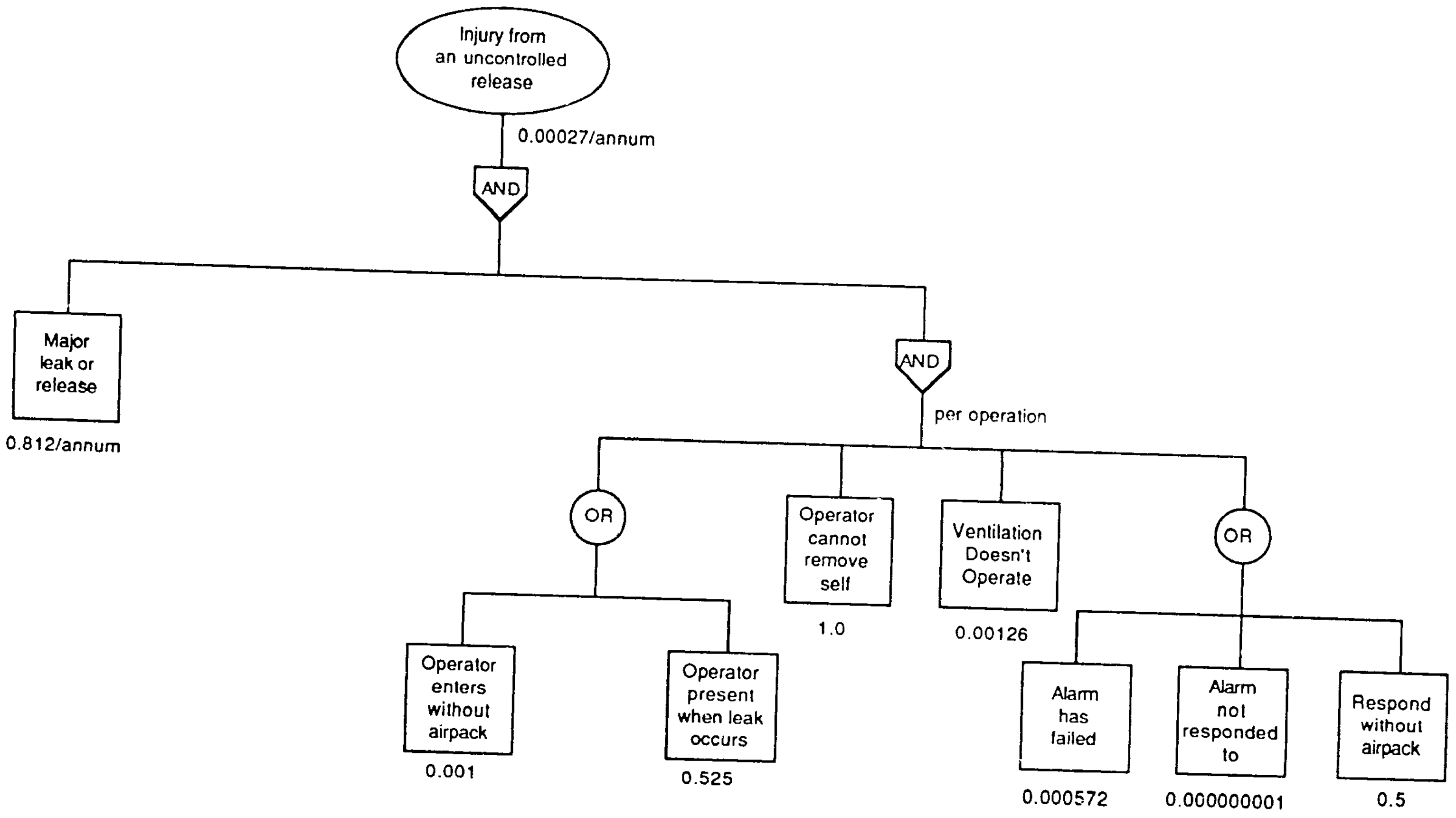
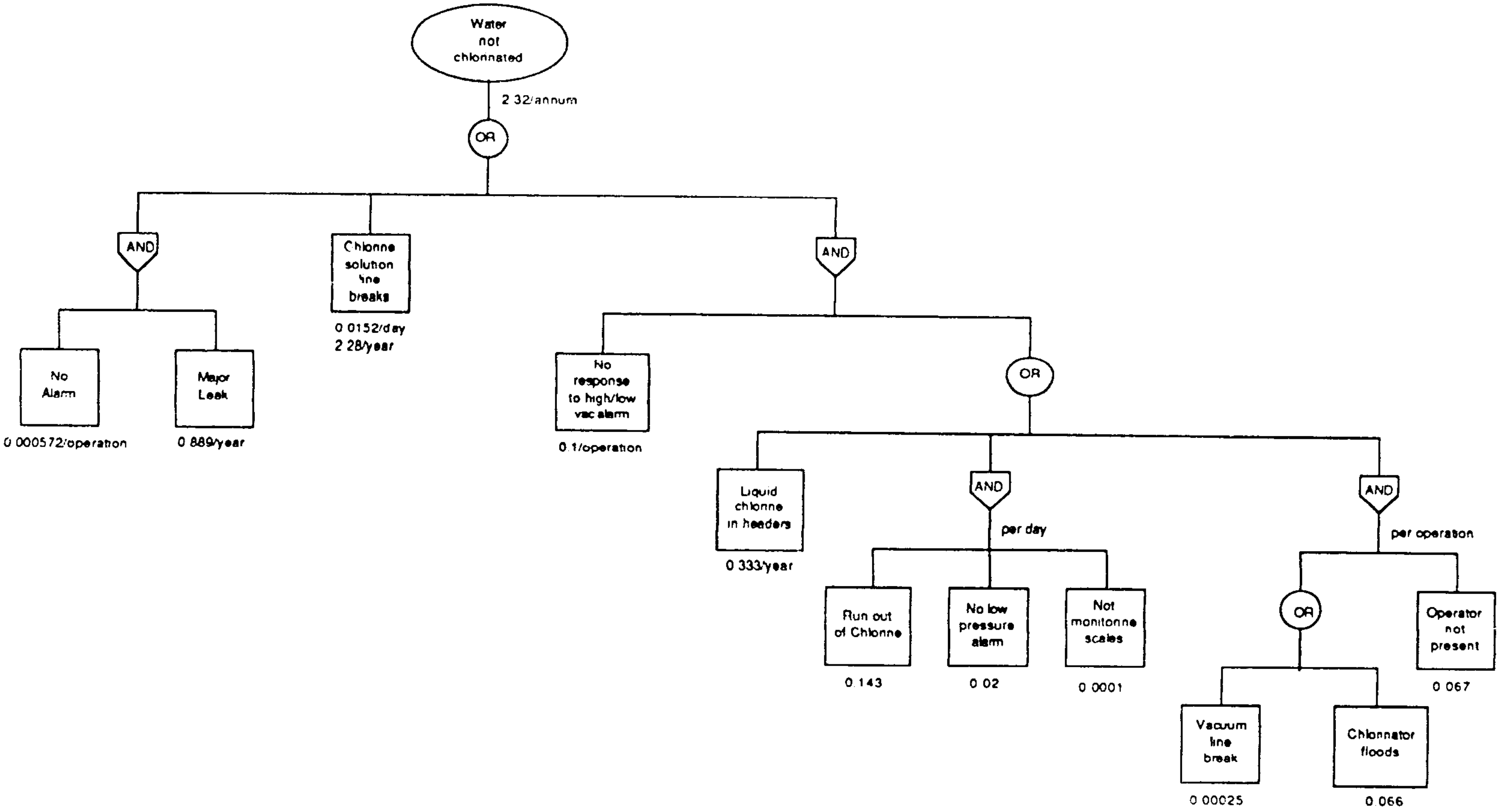


Figure 7.17 Fault tree for an uncontrolled release



F:gure 7.18 Fault tree for the water not receiving chlorine

8. FREQUENCY ANALYSIS

The frequency analysis can be developed once the hazards have been identified and the corresponding scenarios developed. The probability values generated are described by either of three notations, p_i, $F_i = f_i$, or $p_i(f_i)$. The notation representing the uncertainty in a frequency distribution $p_i(f_i)$ was used for this analysis.

8.1 Data Collection

For most of the events, two data sources were used in developing the probability distributions for the failure rates. One source was plant specific data which was derived from maintenance records and interviews with the operations and maintenance personnel. The other data source was generic in nature. Design books and the manufacturing companies of various equipment sections indicated expected failure rates. The probability distributions were developed using, this latter data source for the prior distribution. Bayes Theorem was then implemented to combine the plant specific data with the prior distribution.

8.1.1 Developing the Prior

The prior was developed from the generic data sources. Several design books and manufacturer's information sources, were reviewed to define the ranges over which a failure rate may exist. In some instances the reported failure rate was consistent. For these failure rates, a normal probability distribution was used for the prior. When fairly good agreement exists among reported failure rates, the analyst can be confident that the expected failure rate should be described by a normal distribution. The mean failure rate was equated to the most frequently reported number. The standard deviation chosen depended on the variance in the reported numbers. The closer the agreement in numbers, the smaller the standard deviation.

Because many of the failure rates were close to 0, the theoretical normal distribution which described these failure rates sometimes had negative values. The negative portion of the distribution does not have any physical meaning for failure rate data. Therefore this portion of the graph was not considered in succeeding calculations, which resulted in a truncated normal prior distribution. The shape of the prior distribution is arbitrary. A normal distribution expresses a higher degree of confidence in the failure rate, but it does not represent statistical data which takes the form of a normal distribution.

For some events, the reported failure rates were very different and varied over an extremely wide range. For these instances, a log-normal distribution was chosen for the prior. This type of distribution expresses a lower degree of the confidence the analyst has in the reported data. Where the log-normal prior was used, the two extreme upper and lower values were equated to the 95% and 5% confidence levels. The mean and standard deviation were then calculated.

Along with events for which there was excellent and reproducible generic failure rate data, there was also the other extreme for which there was either no data or very inconsisitent data. In these instances a generalization about the failure rate could not be developed. To express this lack of knowledge about the failure rate, a uniform distribution was used for the prior. If there was a small amount of information about the failure rate a slightly biased the uniform distribution was used.

8.1.2 Updating the Prior

Once the prior was established, the knowledge derived from maintenance records and the operating and maintenance personnel could be applied. The maintenance records have been maintained in an organized and rigorous fashion for only the past three years. Those failures which occur frequently can be adequately represented by such a short time period. However those events which occur infrequently are not represented by this time frame. Therefore, interviews which probed the knowledge of the staff were critical for establishing representative failure rates.

Once the plant specific data was gathered, Bayes Theorem was used to apply this additional knowledge to the prior. To express the plant specific failure rates, either the poisson or binomial distributions were used. All of the events considered in the various scenarios could be described by either of these distributions.

8.1.3 Combining the Failure Rates

Once the posterior distribution has been derived, it can be fitted into the fault tree or event tree. Following the logical rules for each diagram the probabilities can be combined developing the probability of the next event occurring. This method was propagated through the tree until the final damage states had a probability distribution which describes the confidence the analyst has that the event would occur with the particular frequency given. For each scenario and elemental event within that scenario, the preceding methodolgy was applied.

8.1.4 Example of Method

A detailed example of the approach is provided in section 8.3.1.

8.2 Frequency Analysis for Damage State Injury

The first series of scenarios that were analysed are those that contributed to the damage state of injury. This damage state was recognized in the hazard identification and scenario development stage as being propagated through two different kinds of releases, a controlled or an uncontrolled release. The frequency analyses for each of these scenarios were developed separately and then combined to give the final probability distribution for the damage state of injury.

8.3 Contolled Release

From the hazard identification stage, a controlled release will be required when the chlorine headers are full of liquid chlorine and they must be cleaned, when the eductor is fouled and gas remains in the PVC vacuum lines or when the chlorinator is fouled and gas remains in the headers. These latter two scenarios do not really require a controlled release. However, they do represent a situation where the water is no longer receiving chlorine and maintenance must be performed. If the isolation is not performed correctly, injury can result. Each of the frequencies for the events indicated in the fault tree will be considered and, where applicable, fault trees for the individual events will also be developed.

8.3.1 Chlorine Headers Full of Liquid Chlorine

From the fault tree developed for this scenario, there are five basic scenarios which can result in liquid chlorine being formed (Fig. 7.9). These are: the demand rate exceeding the evaporation rate due to one or more tonner valves being plugged, loss of heat, a broken eductor, switching tonner banks from an empty line to a full one when three valves are left open, or the flexible connector may be attached to the wrong valve. The scenario of a broken eductor was developed to demonstrate the method used for the frequency analyis. The remaining scenarios are discussed in detail in Appendix B.1.

Example Calculation

The scenario of a tonner eductor tube failing and allowing liquid chlorine to enter the headers, will be used to demonstrate the application of Bayes Theorem for data analysis. The following form of Bayes Theorem was used:

$$P(\o_i , L(E/\o_i) = \frac{P(\o_i) L(E/\o_i)}{\sum_{i=1}^{N} P(\o_i) L(E/\o_i)}$$

$p(\emptyset_i) =$ prior

$L(E/\emptyset_i) =$ evidence

$p\{(\emptyset_i), L/E\} =$ posterior

The development of the prior and the evidence to calculate the posterior disribution follows.

Developing the Prior

The prior distribution can be developed from manufacturer's information, similar plant's operating information or from general engineering knowledge. The prior may be a normal, log-normal or uniform distribution, depending on the availability and reliability of the information. Manufacturer's information and engineering knowledge were used to develop the prior for the tonner eductor.

The tonners are inspected, filled with the liquid chlorine and shipped out, all from the same company. This company was not able to supply information on the number of eductor failures which occur in a year. Through engineering knowledge it may be possible to predict the corrosion rate of the eductors, however the corrosion rate alone does not determine the failure rate of the eductors. A strict inspection routine is performed on every tonner prior to filling and distribution (Appendix C.1). Although the corrosion and therefore failure rate of the eductors may be quite high, regular inspection should identify the faulty eductors. Therefore the distribution of a tonner with a faulty eductor depends on an inspection failure.

The inspection procedure (Appendix C.1) can be classified as an operator action duty (section 2.7.2). Table 2.4 indicates that a routine simple action has an error rate of 1 in 1000 (0.001). This error rate is also given by Parvin(1985). Because of the consistency in this error rate, a normal distribution was established for the prior. The uncertainty which exists in the failure is expressed through the standard deviation.

The equation of a normal prior distribution was used to establish the prior. The expected failure rate was equated to the mean of a normal distribution. For this example the mean equals one undetected eductor failure per 1000 tonners (0.001). To express the uncertainty which exists in this railure rate, one standard deviation was equated to 0.00075.

This standard deviation, represents an undetected eductor failure rate varying from 1 in 500 tonners to 1 in 4000 tonners. The equation of a normal distribution is :

$$f(\text{ø}) = \frac{1}{\sigma\sqrt{2\pi}} e^{[-0.5(\frac{\text{ø} - \mu}{\sigma})^2]}$$

where:

ø = expected failure rate

μ = mean

σ = standard deviation

f(ø) = probability density function of the expected failure rate.

Table 8.1, indicates the values of ø and f(ø) where f(ø) was generated through the equation:

$$f(\text{ø}) = \frac{1}{0.00075\sqrt{2\pi}} e^{[-0.5(\frac{\text{ø} - 0.001}{0.00075})^2]}$$

Figure 8.1, is the graphical representation of the function. This distribution does not necessarily go to 0 at a failure rate of 0. The distribution is not a true normal distribution but a truncated normal distribution (section 8.1.1). The prior distribution is arbitrary depending only the quantity and consistency of the generic failure rate data.

Once the prior distribution has been established, the probability of each expected failure rate (ø) must be calculated. The calculation was done through a discontinuous

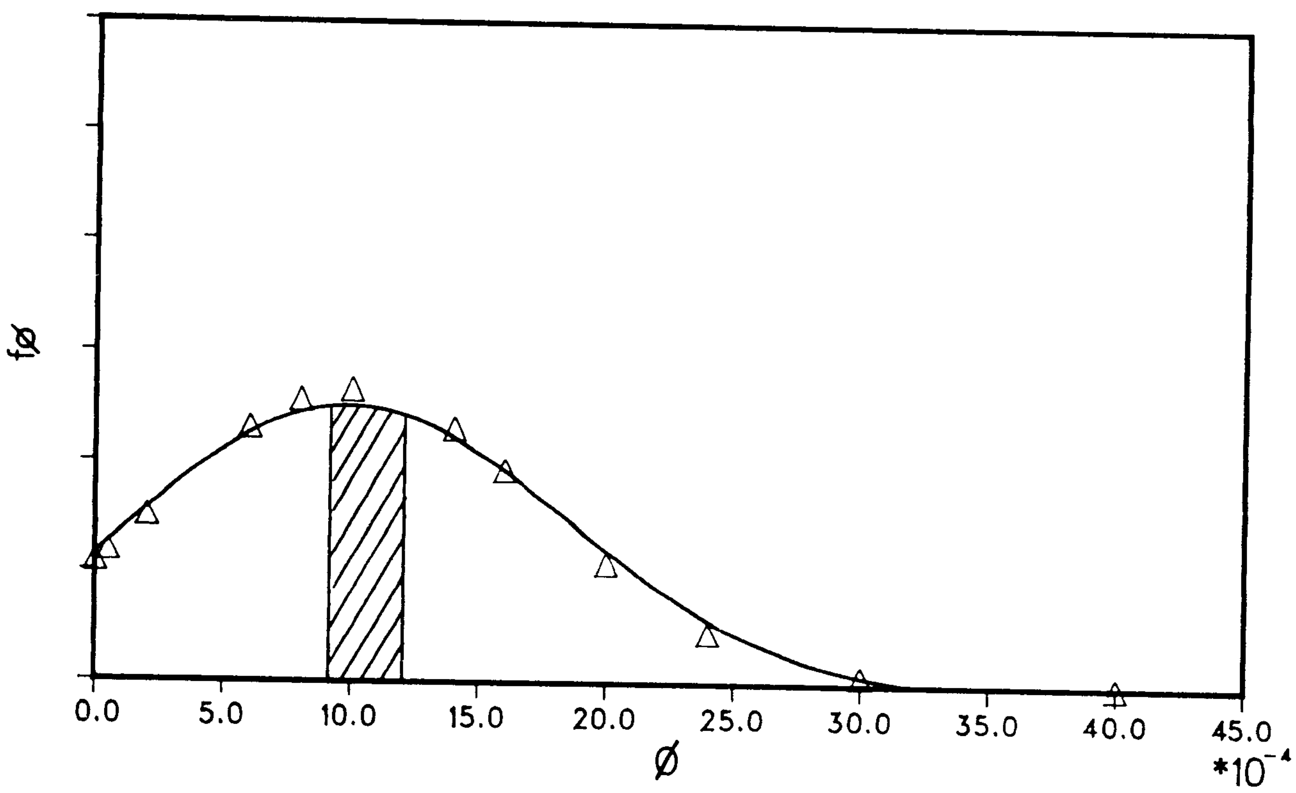


Figure 8.1 Prior distribution for a broken tonner eductor

method. The probability density function was divided into rectangles (Figure 8.1). The boundaries of each rectangle along the x axis were set by calculating the midpoint of each ∅. The y axis boundary was set by the f(∅) function. The probability of each ∅ was then approximated by calculting the area of the rectangle. The probability of each ∅ is given in Table 8.2.

Applying the Evidence

Bayes Theorem is used to apply the evidence to the prior distributions. Maintenance records and operator recollection were used to establish the evidence. Over ten years of operating time, only one tonner eductor has failed. This information was used to update the prior.

Table 8.1. The expected failure rate ϕ, with the prior and posterior probability density functions.

ϕ (x 10^{-3})	$f(\phi)$ prior	$f(\phi)$ posterior
0.05	0.002	65.7
0.1	259.0	209.3
0.2	301.2	368.1
0.30	344.2	510.2
0.40	386.4	653.9
0.50	426.0	736.8
0.7	491.2	809.3
0.90	527.3	769.4
1.20	513.5	534.2
1.40	461.5	381.4
1.80	301.3	150.0
2.20	147.9	26.1

Table 8.2 The tabulation of ϕ, $p(\phi)$, $L(E/\phi)$ used to calculate the posterior distribution $p(\phi, L/E)$

												Σ
ø (x10 [illegible])	.025	.125	.4	.7	.9	1.2	1.5	1.8	2.2	2.7	3.5	
P(ø)	.011	.040	.152	.097	.104	.198	.085	.121	.062	.032	.008	
L(E/ø)	.041	172	.34	.36	.33	.26	.20	.14	.09	.05	.02	
(ø) x L(E/ø) (x10 [illegible])	04	.69	5.2	3.5	3.5	5.3	1.7	1.7	55	.15	01	22.1
P(ø / L(E/ø) (x10 [illegible])	.21	3.1	2.3	1.6	1.5	2.4	7.5	7.7	2.5	.67	05	

$$P(\text{ø} / L(E/\text{ø}) = \frac{P(\text{ø}) \times L(E/\text{ø})}{\sum P(\text{ø}) \times L(E/\text{ø})}$$

e.g. $$P(\text{ø}_1 / L(E/\text{ø}_1) = \frac{P(\text{ø}_1) \times L(E/\text{ø}_1)}{\sum_{i=1}^{13} P(\text{ø}_i) \times L(E/\text{ø}_i)}$$

$$P(\text{ø}_1 / L(E/\text{ø}_1) = \frac{0.011 \times 0.041}{0.224}$$

$$= 0.002$$

The Likelihood Function

The likelihood function calculates the probability of observing the evidence given the established failure rate of the prior distribution. The Poisson or the Binomial equations may be used to calculate the likelihood function. (section 2.5). The binomial equation was used to calculated the likelihood function because the scenario represents a discontinous event over time. Each tonner may be considered as a success or failure event depending on if the eductor has failed.

$$L(E/ø) = \frac{N!}{K!(N-K)!} ø^{K} \; (1 - ø))^{(N - K)}$$

K represents the failure, which is equivalent to 1 for this scenario. N represents the total number of events. If approximately 170 tonners are used per annum, the N value would be equivalent to 1700 for ten years. These values can then be substituted into the equation:

$$L(E/ø) = \frac{1700!}{1!(1700 - 1)!} ø^{1} \; (1 - ø)^{(1700 - 1)}$$

The likelihood function can then be calculated for each ø established in the prior distribution (Table 8.2).

Combining the Evidence

Once the prior and the evidence have been calculated the posterior distribution is calculated. The probability for each expected failure rate is multiplied by the likelihood function for each failure rate (Table 8.2). The denominator of Bayes Theorem is calculated by summing the values.

The posterior distribution is then calculated by dividing the multiplication of the prior and likelihood function by this summation. The posterior distribution represents the probability of each expected failure rate given the evidence.

The probability density function for the posterior distribution can then be calculated. The midpoints between each o were calculated for the prior probability distribution. For each o the posterior probability distribution can be divided by the difference between each midpoint. This results in the posterior probability density function (Figure 8.2).

The mean and standard deviation for the posterior distribution can then be calculated by:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N} (\varnothing - \mu)^{2}}{n-1}} \qquad \mu = \frac{\sum_{i=1}^{N} \varnothing_i f(\varnothing_i)}{\sum_{i=1}^{N} f(\varnothing_i)}$$

The value of the mean for the posterior distribution was then placed into the fault tree.

All of the data analysis was performed using this technique. The information used to establish the prior of each scenario, whether it was a uniform, normal or log-normal distribution is given in the appropriate section.

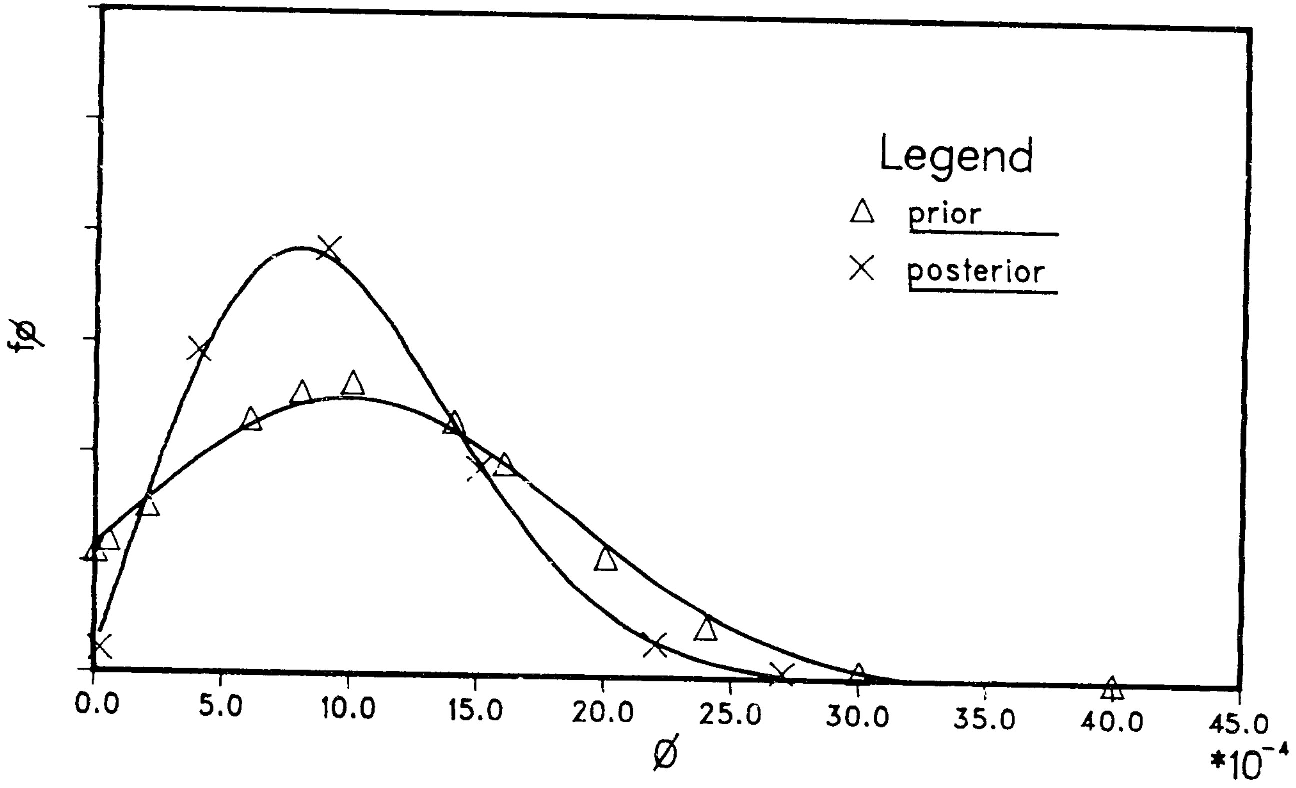


Figure 8.2 Prior and posterior probability distributions for a broken tonner eductor

The plant specific operating information was then used to update the prior through either a Poisson or Binomial likelihood function. The failure and success rate evidence along with the particular likelihood function is also given for each scenario. The mean failure rate developed for each posterior distribution are then placed into the appropriate fault tree.

8.3.2 Handling Liquid Chlorine in the Lines

When a chemical is stored in a liquid phase but fed in the gas phase there is always a risk of the liquid form entering the system. In order to prevent an injury in the event of liquid chlorine in the headers, it is critical that the emergency equipment be available to handle the situation. Those circumstances which could contribute to an injury are considered in detail in Appendix B.2. The probability distribution for having liquid chlorine in the headers is given in Figure 8.3.

8.4 Eductor Fouled

When there is a loss of vacuum, it is impossible for the chlorination of the water to continue. When this does occur, there must be an immediate switch to another eductor. Since the manipulation of the valving to switch the eductor for a particular chlorinator is fairly complicated, the normal procedure is to completely switch chlorinators, with each chlorinator using its own eductor unit. The valving

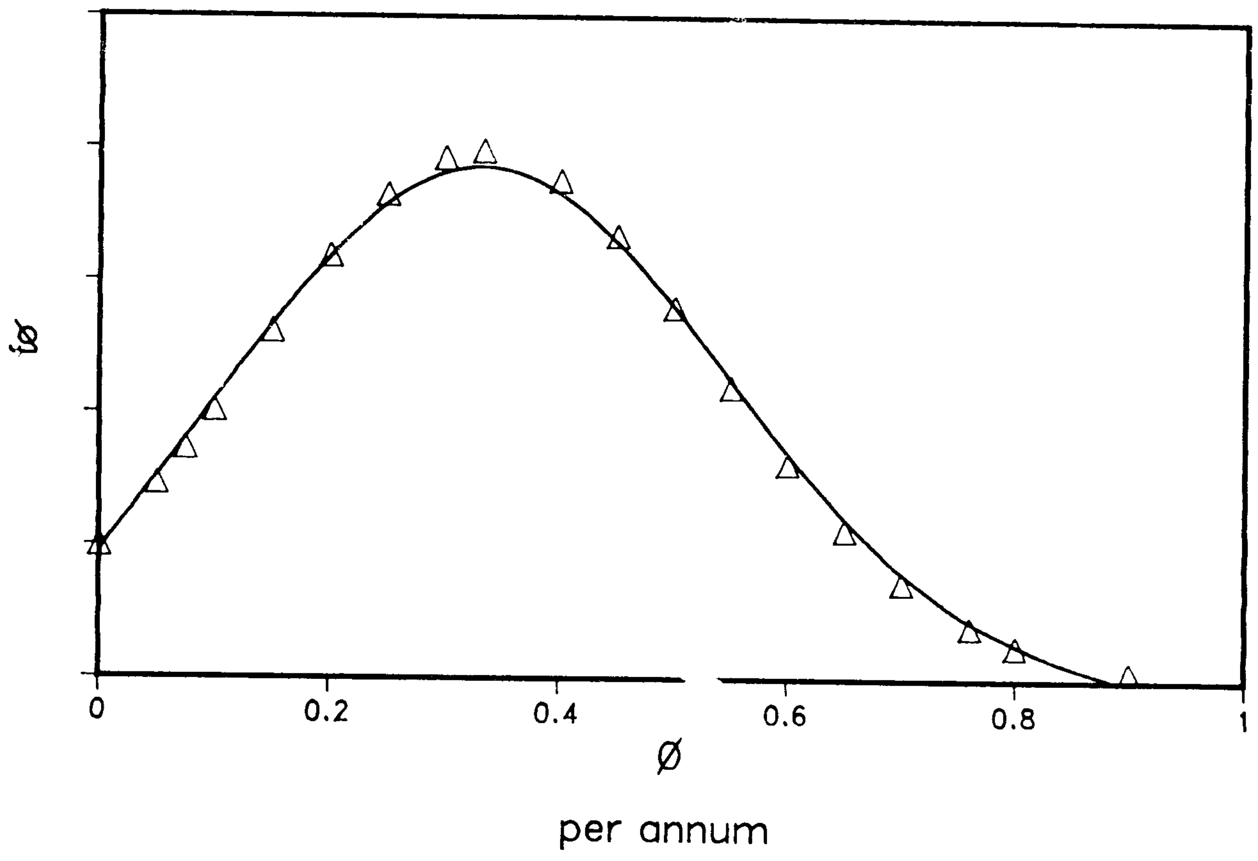


Figure 8.3 Probability distribution for liquid chlorine in the headers

after the eductor can then be changed to maintain the same feeding point.

The eductor should be able to supply a vacuum of at least 250 mm Hg, and above 900 mm Hg the high vacuum alarm sounds. There are three possible reasons why there could be a reduction in the vacuum at the injector including; loss of supply water pressure, partial plugging of the eductor from debris or manganese and iron build up, or blockage of the discharge line (Fig. 7.1). These are discussed in detail in Appendix B.3. The probability distribution for a fouled eductor occurring is given in Figure 8.4.

8.5 Chlorinator Flooded

Another scenario requiring the maintenance personnel to perform repair work which could potentially result in injury, is the flooding of the chlorinators (Fig. 7.8). The chlorinators are flooded when there is an excess back pressure from the injector and both check valves do not hold allowing the water to pass. The back pressure results from a partial fouling of the eductor or a slight loss of the vacuum when the chlorinators are to be changed. In the former case, little can be done to protect the chlorinators, however in the latter case isolation valves have been installed which stop the water from entering the chlorinator, even if the line floods. The frequency analysis for five events which can result in a flooded chlorinator are discussed in Appendix B.4. The probability distribution for a flooded chlorinator is given in Figure 8.5.

8.5.1 Final Distribution for a Controlled Release Causing Injury

As the probability values were generated they could be combined through the appropriate logic gates (Fig. 7.16). This final distribution for an injury from a controlled release can then be combined with the injury from an uncontrolled release. The probability distribution representing the probability of injury from a controlled release is given in Figure 8.6.

8.6 Injury From an Uncontrolled Release

When the final damage state of injury is considered, the initiating event of an uncontrolled release is usually necessary. For the controlled release, events which could lead to the damage state were often operational problems that had been designed for. For an uncontrolled release, the events leading to the injury are from rare, unexpected events that immediately result in a chlorine release. While failure of either a mechanical or human action can increase the hazard from the release, the situation is not stable and must be immediately attended to.

When the major leak occurs, the damage state of injury arises when personnel who are not warned of the situation are unable to leave the affected area and are overcome by the toxic gas. The events resulting in a major leak are

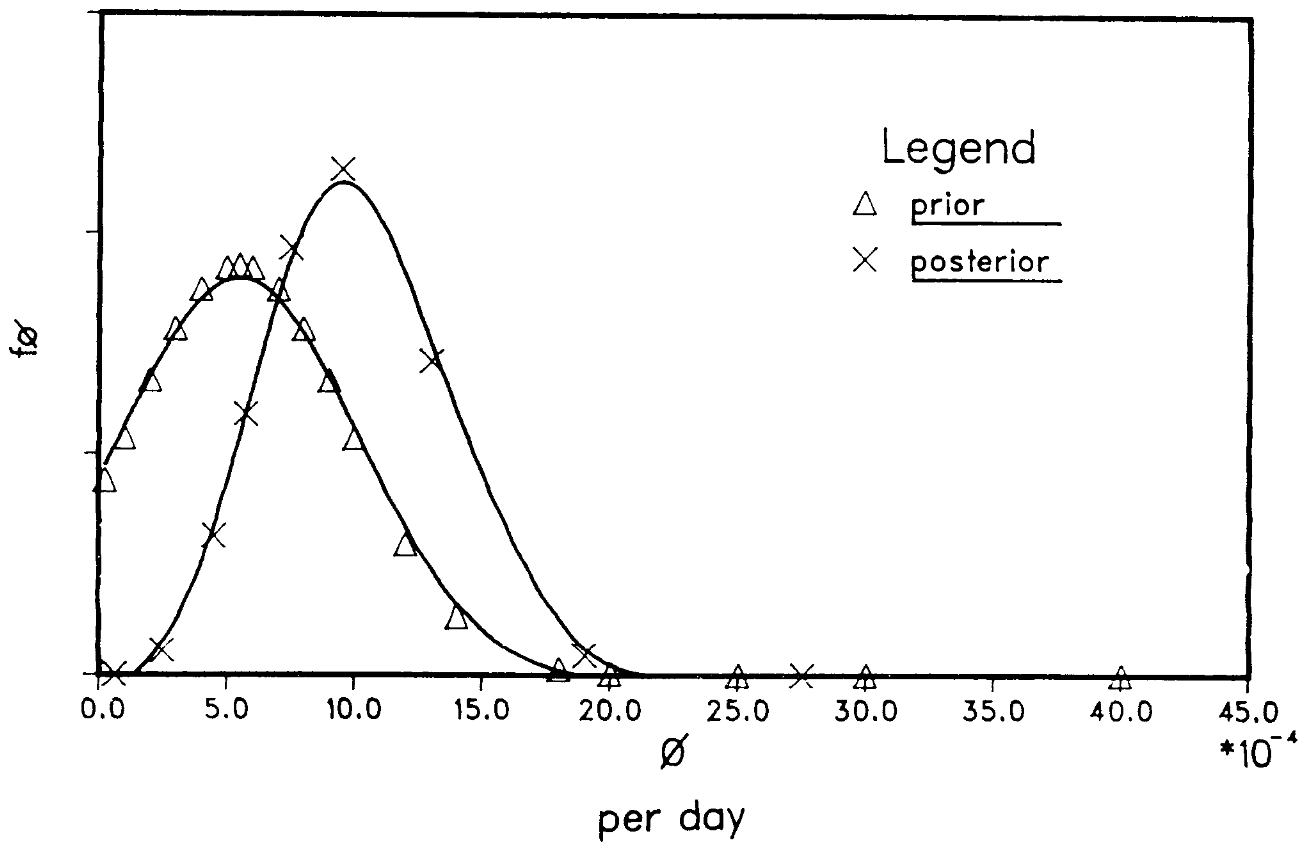
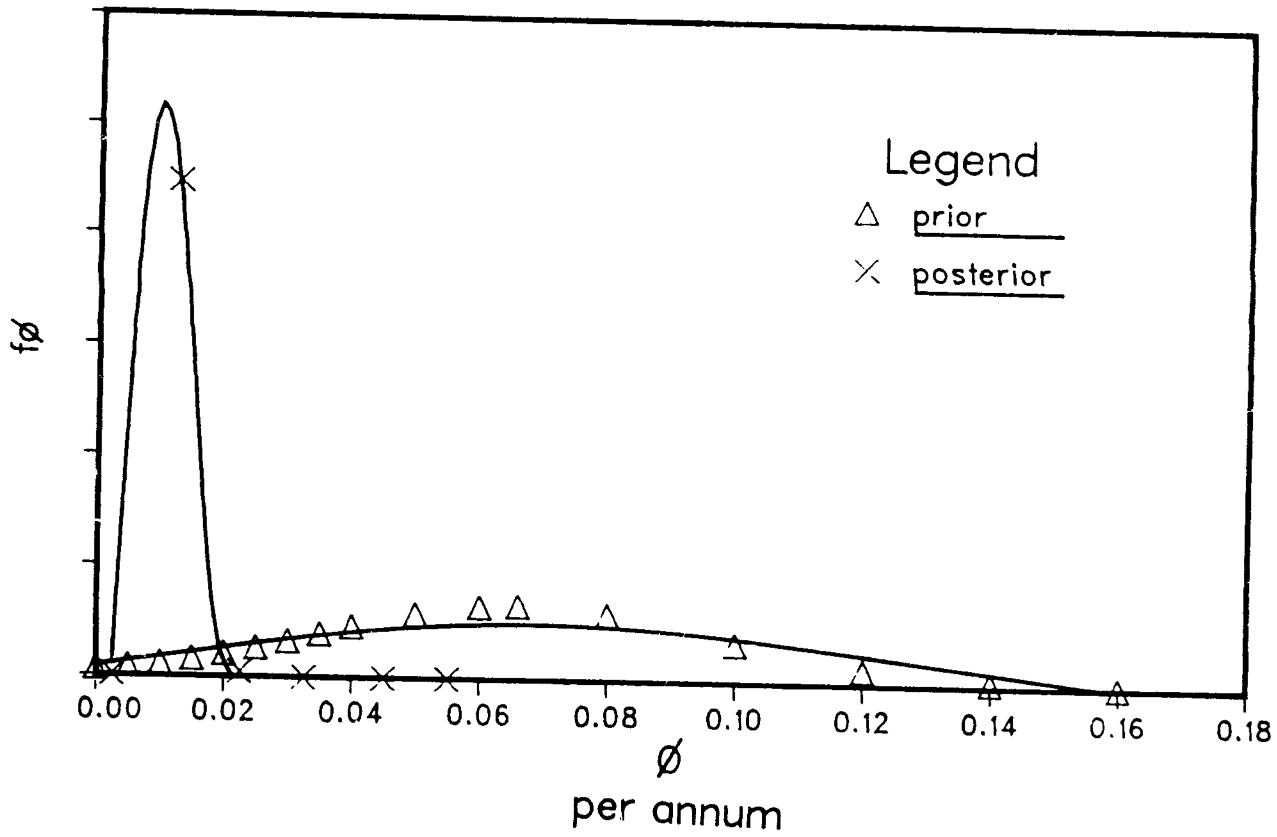


Figure 8.4 Probability distribution for a fouled injector



'igure 8.5 Probab:lity distribution for a flooded chlorinator

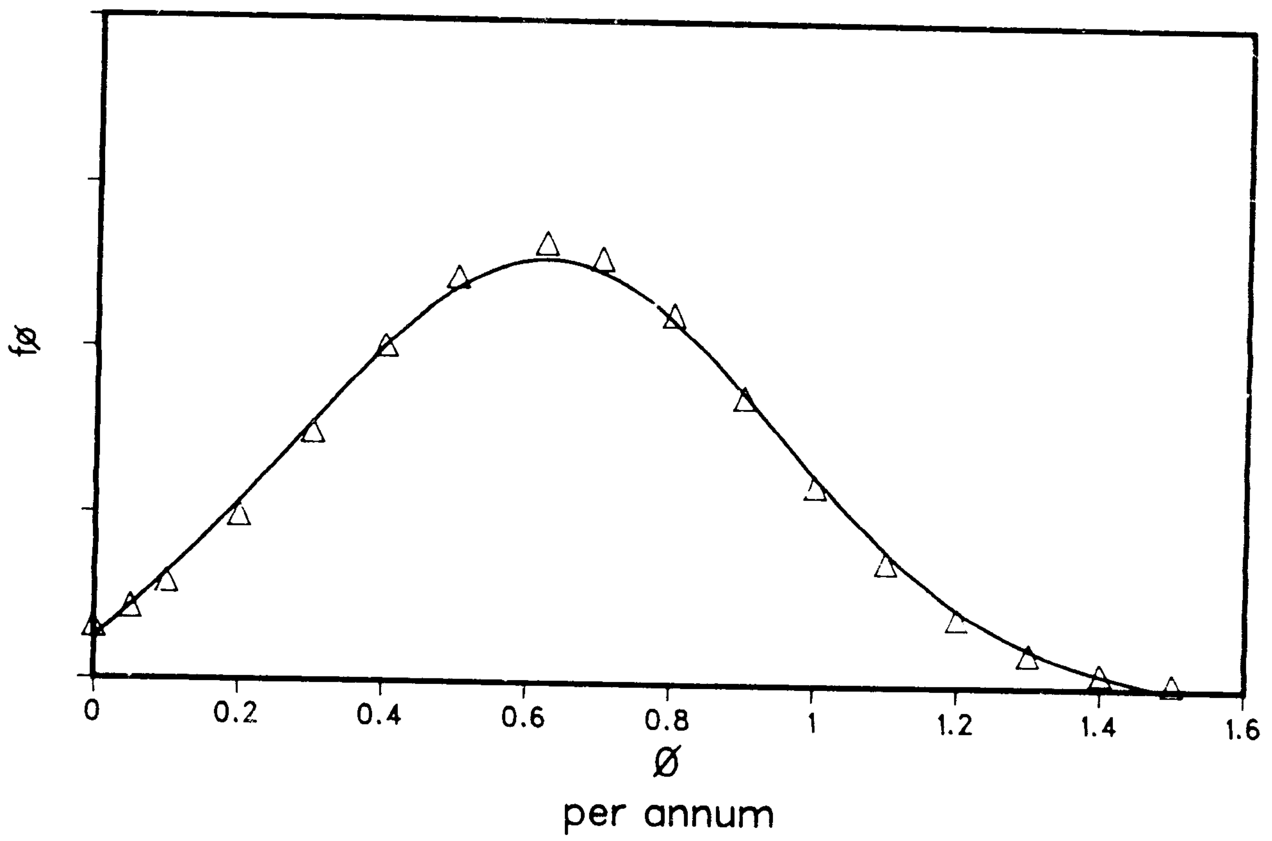
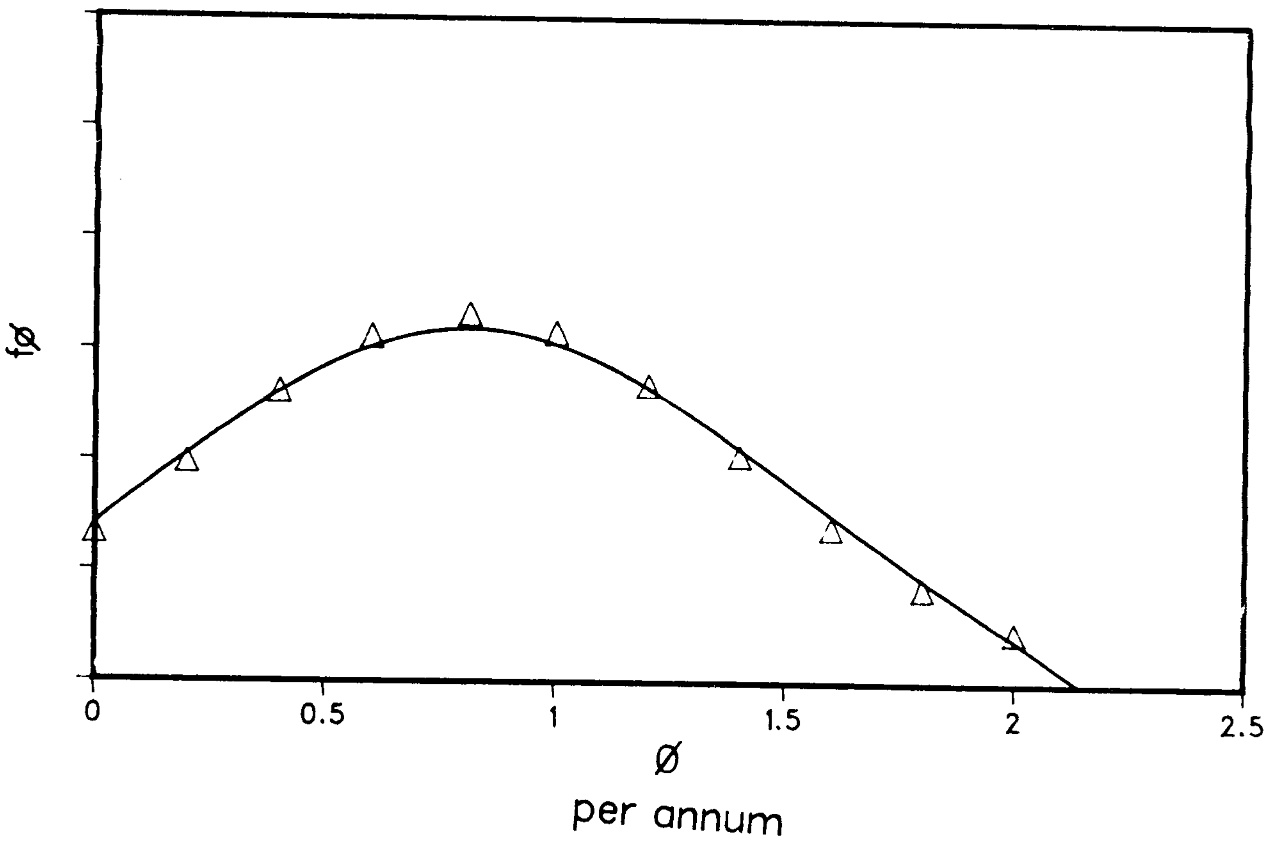


Figure 8.6 Probability distribution for injury from a controlled release



gure 8.7 Probability distribution for an uncontrolled release

expressed by separate fault trees.

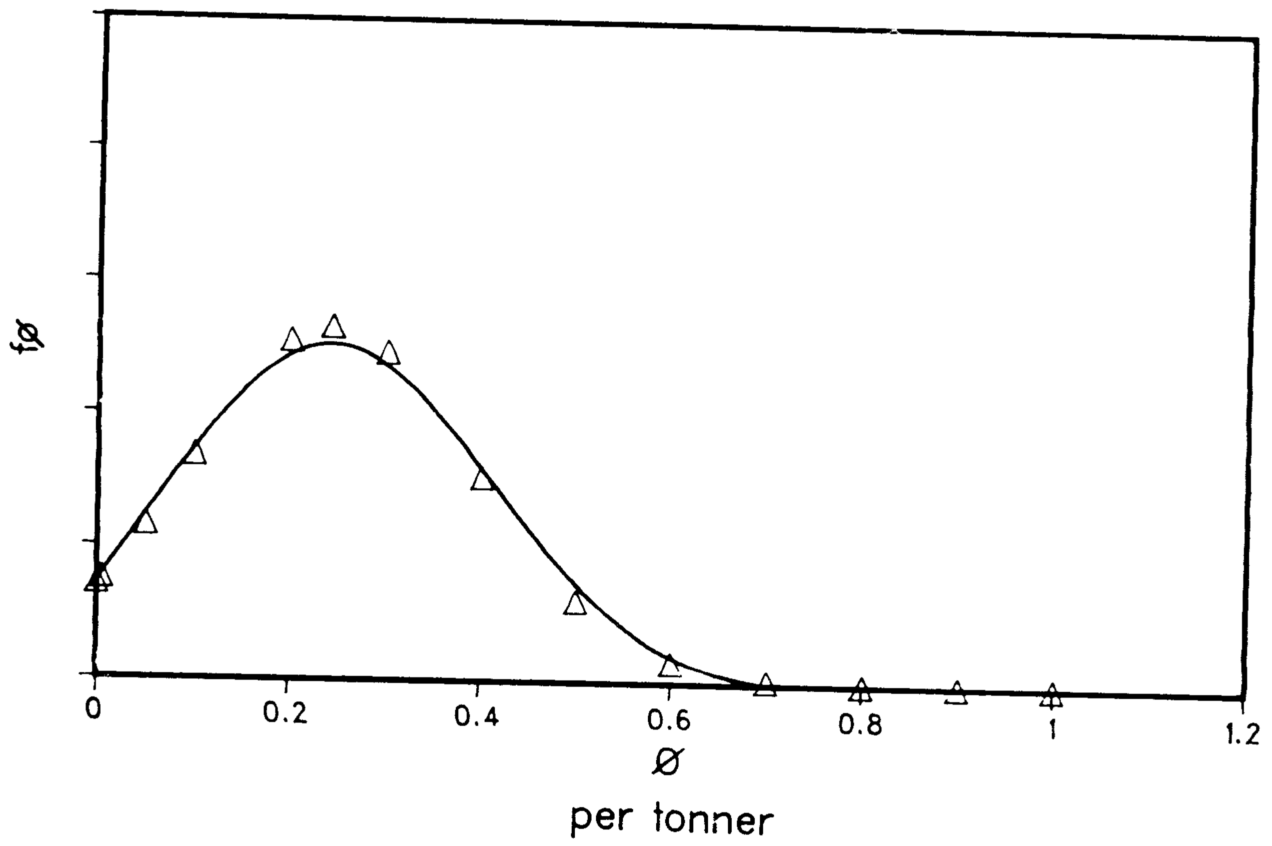
The event of an uncontrolled release occurs when either the tonners or the feed equipment has a failure resulting in a rupture. Fault trees were developed representing the events that can result in these ruptures (Figs. 7.12, 7.13, 7.14, 7.15). The probability distribution for an uncontrolled release is given in Figure 8.7.

8.6.1 Tonner Rupture

There are six routes which can cause a tonner rupture. These are represented by Figure 7.12. The routes represent the application of some type of excessive force, or excessive heat to the tonner except for the corrosion event. These events are discussed in detail in Appendix C.1. The probability distribution of a tonner rupture is given in Figure 8.8.

8.6.2 Tonner Valve Break

The only incident that would be specific to the tonner valve that was not considered by a tonner rupture, is the corrosion of the valve. The details of the frequency analysis for this event are given in Appendix C.2. The probability distribution of a tonner valve break is given in Figure 8.9.



igure 8.8 Probability distribution for a tonner rupture

8.6.3 Fusible Plug

Much of the development for a leak from the fusible plugs has already been done in Appendix C.1. The leak could be caused by corrosion or from the valves melting. The frequency analyses for these events are detailed in Appendix C.3. Figure 8.10 indicates the probability distribution for a leak from the fusible plugs.

8.6.4 Header Break, Flexible Connectors and PVC Break

The frequency analyses for an uncontrolled relases from a header break a flexible connector or a PVC vacuum line, have been developed in Appendix C.4. The probability distributions for the header and flexible connectro break are given in Figures 8.11 and 8.12 respectively.

8.6.5 Uncontrolled Release Summary

For each of the events listed in the uncontrolled release fault tree an expected likelihood of occurrence has been developed. These individual probabilities were then combined through logical OR gates to give the expected probability of an uncontrolled release.

8.6.6 Warning System

When an uncontrolled release of the chlorine occurs, the activation of the warning and ventilation system is crucial for the prevention of an injury. When an uncontrolled release occurs in the storage room, the leak

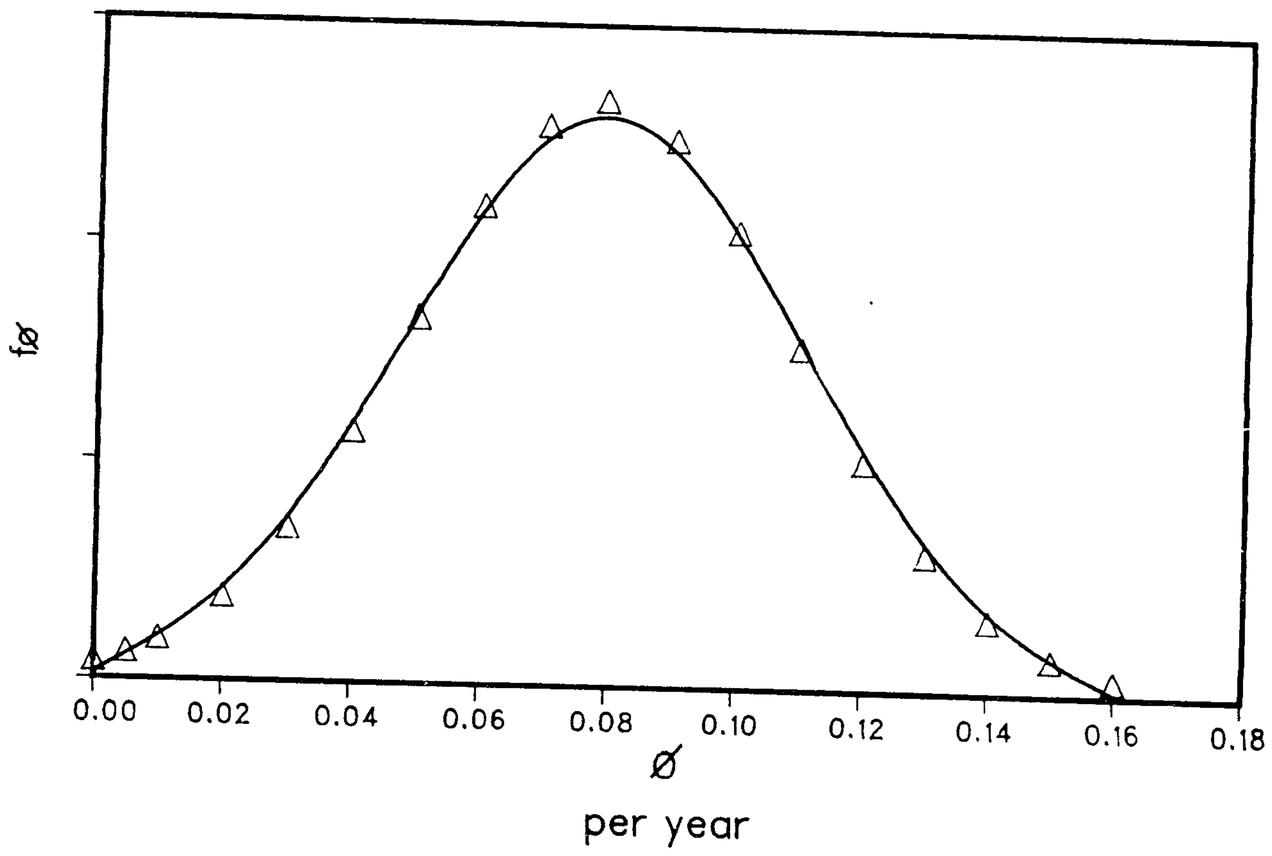


Figure 8.9 Probability distribution for a tonner valve break

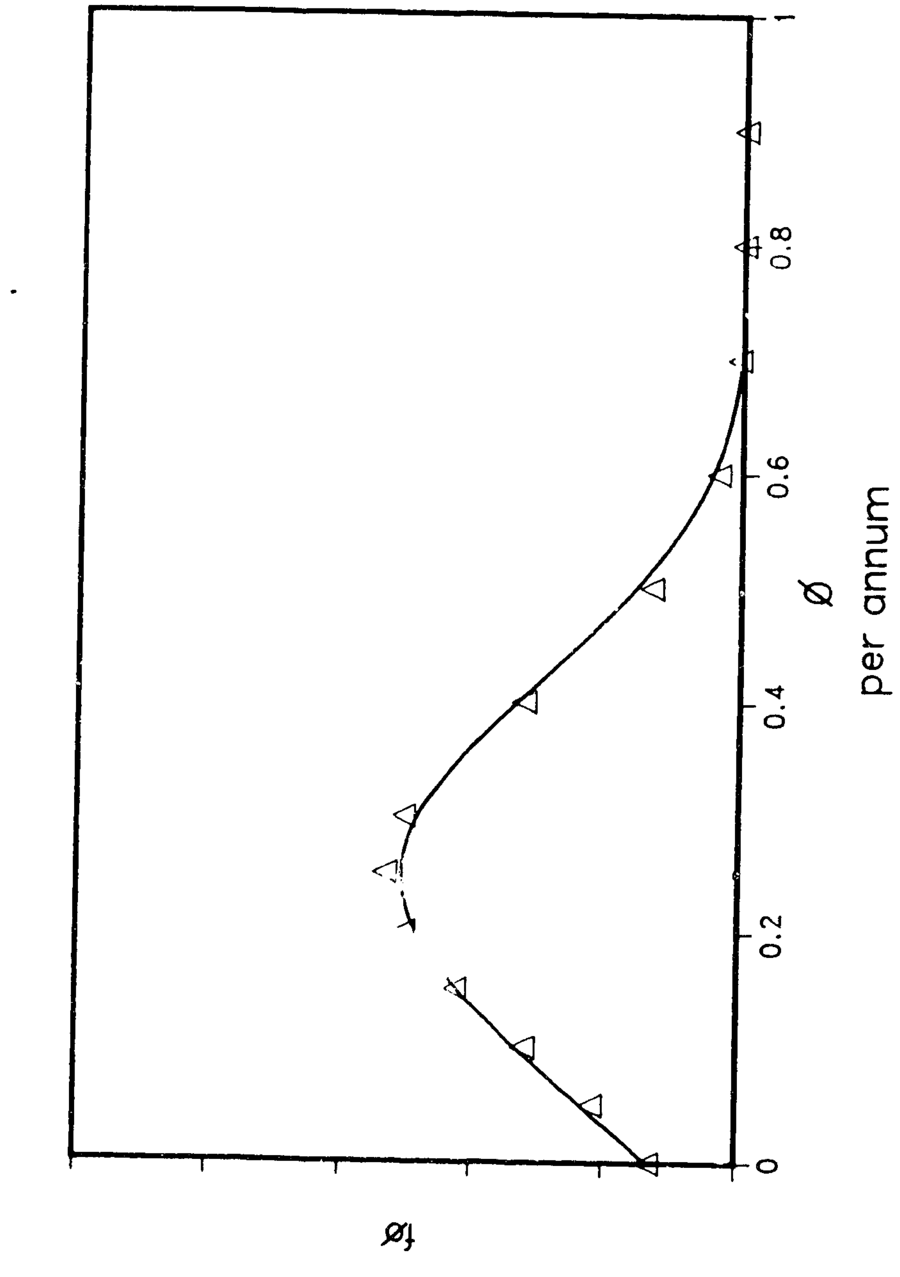


Figure 8.10 Probability distribution for a fusible plug leak

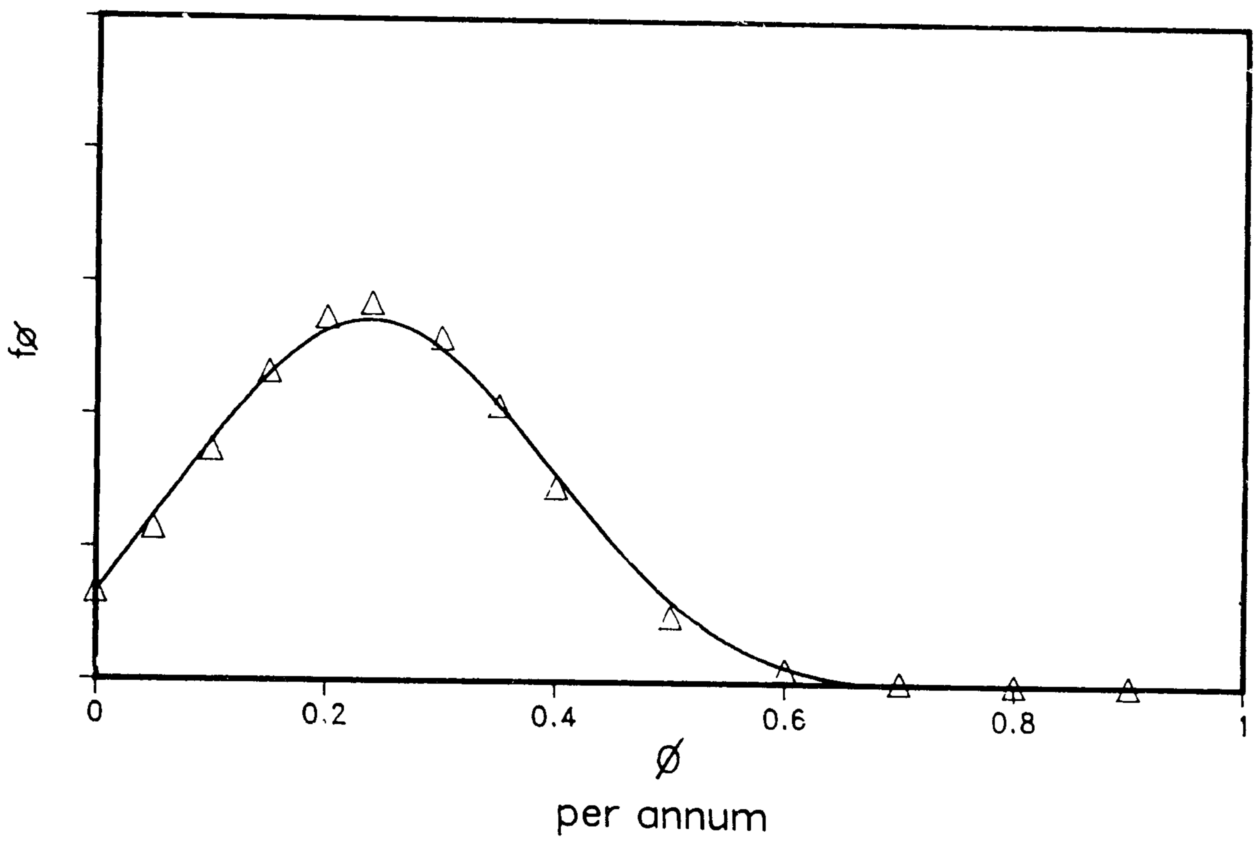


Figure 8.11 Probability distribution for a header break

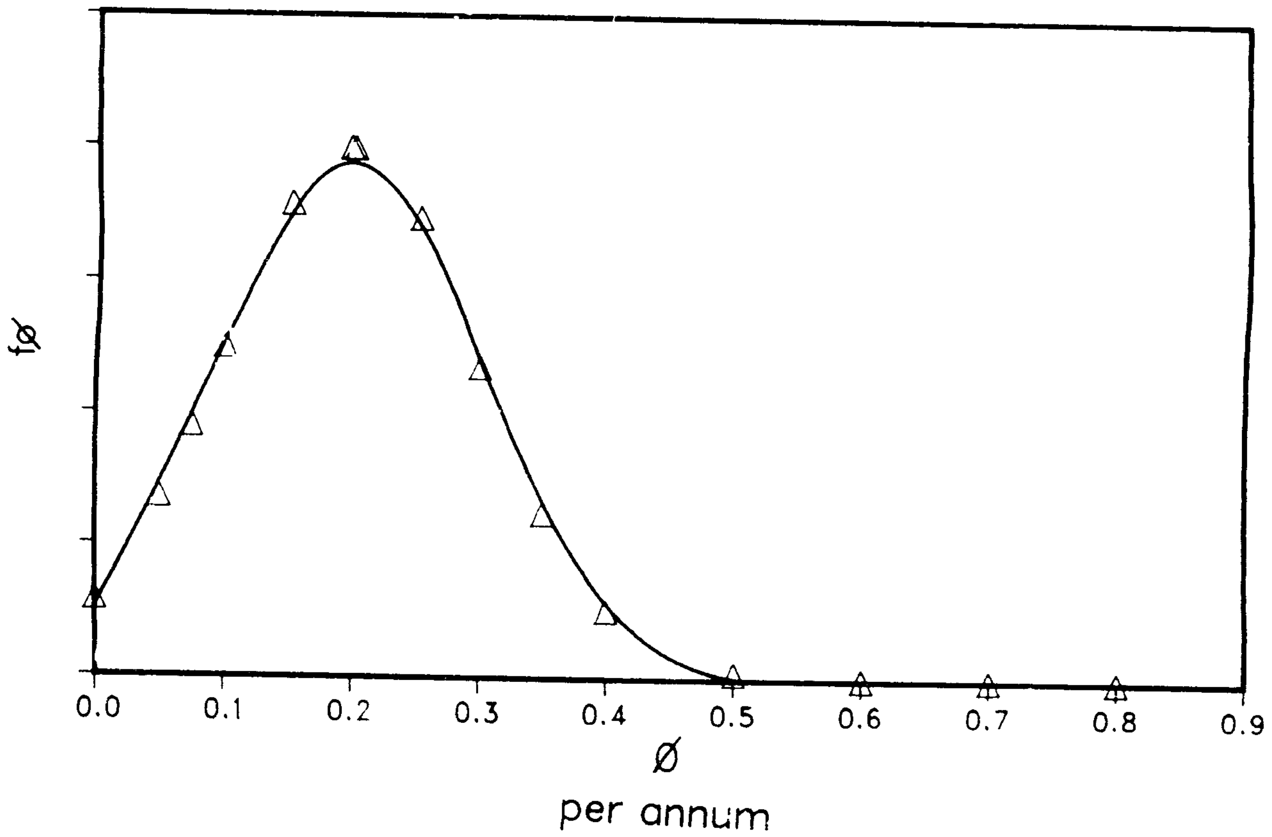


Figure 8.12 Probability distribution for a flexible connector break

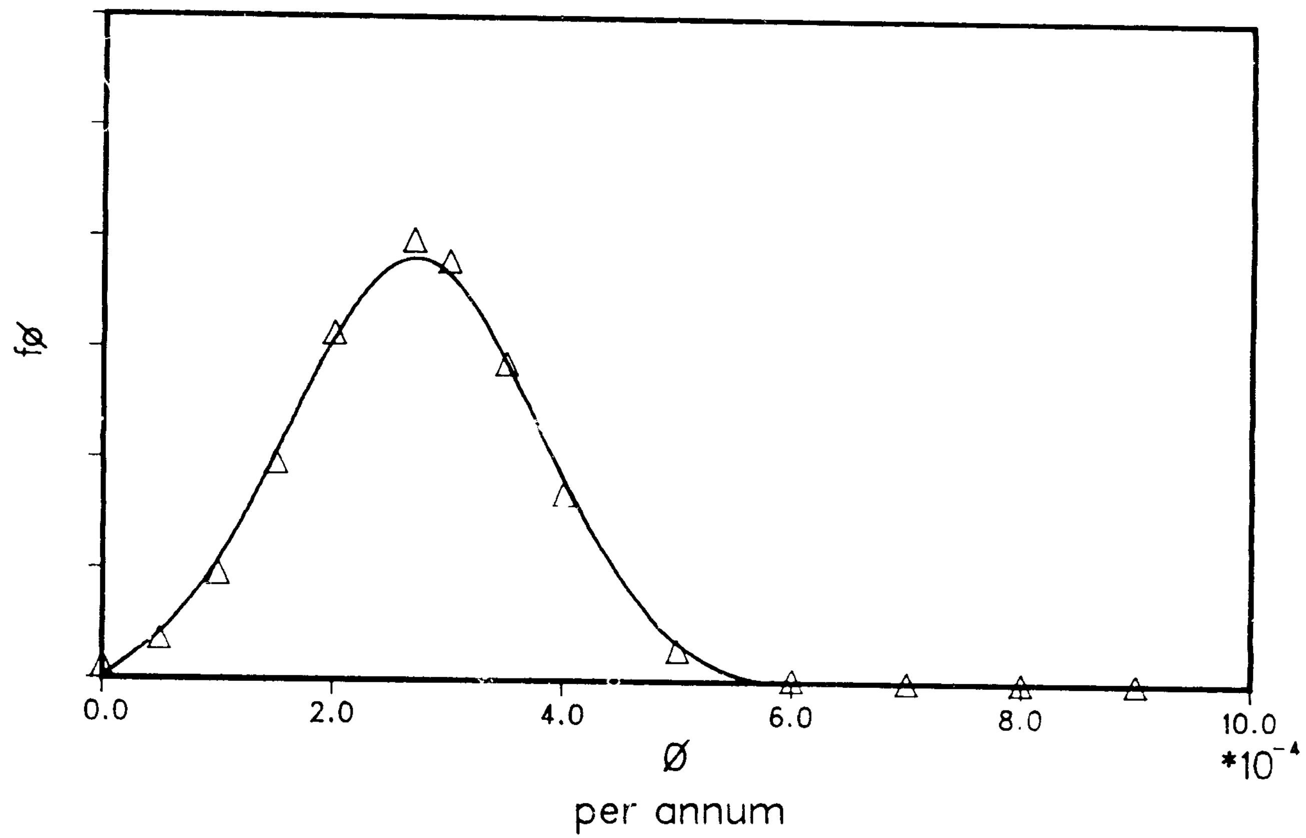


Figure 8.13 Probability distribution of an injury from an uncontrolled release

detector should sense the presence of chlorine, activate an audible alarm, the ventilation unit and a red light outside the northwest door will flash on and off. When this alarm sounds, the personnel closest are to don the appropriate breathing apparatus and investigate the cause of the alarm. The failure rate for this warning system and the failure of operators to respond to this system are given in Appendix D.1.

8.6.7 Injury Summary

The fault tree which represents an injury from an uncontrolled release, can be combined with the controlled scenario to arrive at the total probability of injury from exposure to chlorine gas. To understand the severity of the injury a closer examination of the events in the fault tree and their projected consequences must be done. The probability distribution describing the expected frequency of an injury from an uncontrolled release is given Figure 8.13.

8.7 Water Contamination Frequency Analysis

Many of those scenarios developed which could result in the injury damage state would also result in the water not receiving chlorine. The effect these events have on the water quality, depend on how long inadequate chlorination continues. Each of the scenarios is combined with the failure of the particular warning signal, since there must

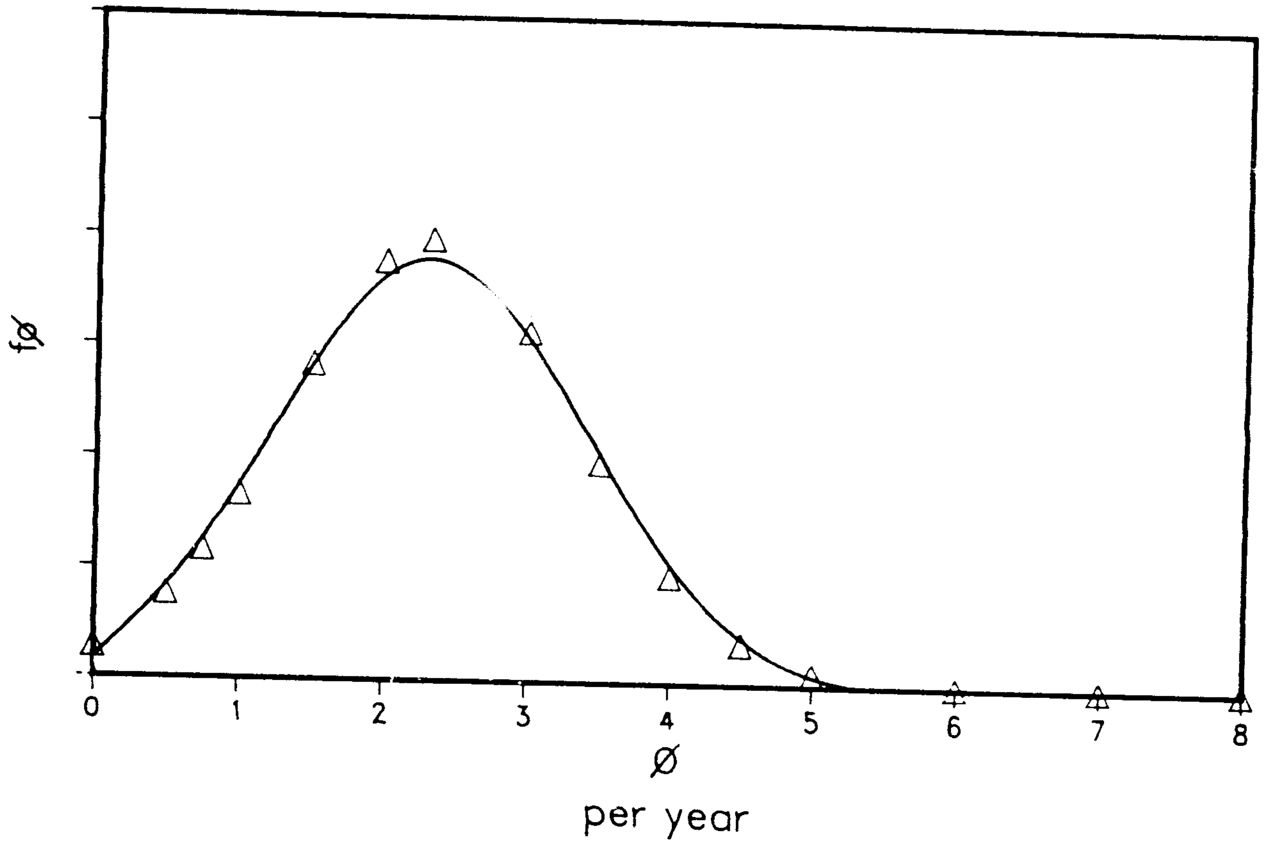


Figure 8.14 Probability distribution of the water not receiving chlorine

be a time lapse for the stoppage of chlorination to have an effect (Fig. 7.18). The flow rate affects the degree of damage to the water quality. Lower water flow rates will allow a longer retention time permitting a greater chance for the error to be corrected on any particular cubic meter of water.

8.7.1 Major Leak, No Alarm

Both of these events have been fully developed for the injury scenario.

8.7.2 Liquid Chlorine in Headers, No High Vacuum Alarm

The scenarios which would result in liquid chlorine in the headers were developed in the frequency analysis for a controlled release. Given that there is liquid chlorine in the lines, the flow of chlorine, would stop creating an excess vacuum which should sound the high vacuum alarm. This alarm is not tested regularly as the leak detectors are. It is an audible alarm which sounds on the alarm panel.

An additional problem with this alarm, is not whether or not it will sound, but whether or not it would be responded to. Of the fourteen operators interviewed, only six were aware of the alarm, and why it would be activated. Given the low level of understanding, the response to the alarm may be to simply reset it. Only when resetting becomes impossible would the alarm be investigated.

The probability distribution describing this response to the high vacuum alarm was developed using a normal distribution with a mean of 0.1 and a standard deviation of 0.05. This represents the probable lack of response to the alarm rather than failed operation. This type of information cannot be updated with additional knowledge since the situation is unique to this facility. Therefore only the prior form is represented.

8.7.3 Chlorinator Floods, No Low Vacuum

The scenario for the chlorinator flooding was developed in the controlled release section. The most frequent cause of this event is from the switching of the chlorinators. Therefore it is quite likely that an operator would be present. If the operator is present, he can quickly adjust the valving so that chlorination can continue. Those events which cause flooding of the chlorinators without the staff being aware may adversely affect the water quality. The probability of an operator not being present was calculated by combining the independent events which could cause the chlorinator to flood without the operator in attendence

The only warning of the chlorinator flooding, should the operator not be present, is from the low vacuum alarm. Unfortunately, this alarm which sounds on the same panel with the same flashing light as the high vacuum alarm is dealt with in the same manner. The presence of both alarms on the same panel creates confusion. Not only are many of the staff unsure of how the alarm may be activated, but it appears completely contradictory for a situation to cause both a low and a high vacuum. The same probability distribution wa used for the no response to the low vacuum scenario. A normal distribution with a mean of 0.1 and a standard deviation of 0.05 were used.

8.7.4 Chlorine Solution Line Breaks

The breakage of a chlorine solution line could occur from either freezing in the cold weather or from impact. Most of the solution lines follow relatively protected pathways. They travel close to walls and underneath overhangs. There is very little information on the probability of a chlorine solution line being impacted, so a uniform prior distribution was used. This prior was updated with a poisson distribution which had an incidence value of 0 and an event time of 10 years.

The possibility of a break from freezing is much greater. The chlorine solution lines are insulated, but they are not heat traced. As breaks occur, drains and valves are installed so that the lines may be air purged. From plant specific data there are, on average, two breaks during the winter months. Using this information on a uniform prior distribution, the updated prior was developed from a poisson distribution with an incidence rate of 2 and an event rate of 5 months (150 days).

8.7.5 Run out of Chlorine

Approximately once per week, a tonner bank will empty and must be changed over to a full bank. A normal probability distribution was developed for this event with a mean of 7 days and a standard deviation of 2 days. To ensure that there are no interruptions in chlorination there are two precautions taken. A low pressure alarm will sound at 25 kPa, when the tonners are nearly empty and the weights are monitored every 12 h so that the change of the tonner bank would be anticipated. When the tonners are almost emptied the operator responsible for the changeover begins to closely monitor their weights. The low pressure alarm is actually used as a verification mechanism rather than a signalling mechanism.

For the tonners to run dry, the operator would have to be involved in another task, but they are usually aware of the impending event. Human error described as a momentary forgetfulness could account for an operator failing to change the tonners. This type of failure rate would be approximately 0.0001. This value was used as a mean to develop a probability distribution with a standard deviation of 0.00005.

In the event the operator is not monitoring the tonner weights, the low pressure alarm should sound, signifying his forgetfulness. As the alarm continues, it would eventually be investigated. However, if the alarm did not sound, it could be some time before the situation was discovered.

The low pressure alarm must be switched to monitor the particular tonner bank in use. It is possible that the alarm could be monitoring the wrong bank preventing its activation. Interviews with the staff indicated this has happened once in the past two years. With 35 tonner changes per year, an error rate of 1/50 (0.02) gives a conservative estimate.

The low pressure alarm is not regularly tested so there was not any failure rate data on this alarm. As with the failure rate for the leak detector, it can be expected that the mechanical failure rate of this alarm would be insignificant when compared witn the effect of the human error rate. Therefore a normal distribution with a mean of 0.02 shall be used to represent the failure of the low pressure alarm. This is mostly influenced by the failure to switch the alarm to the appropriate bank. A standard deviation of 0.01 shall be used.

8.8 Summary of Frequency Analysis for Water Quality

The possibility of chlorination stopping is relatively high when compared with the release scenarios. The prevention of the water contamination damage state relies on the discovery of the event by the operational staff. In nearly all of the instances there was an alarm mechanism which indicated this problem. The response of the operator to this alarm had the greatest impact on the amount of chlorination lost. The probability distribution for the water not receiving chlorine is given in Figure 8.14.

8.9 Exterior Force

An incident that is unrelated to plant activity, and yet is powerful enough to cause the rupture of the chlorine tonner or the the headers is classified as an exterior force. The incident may be man made, as in an air plane crash, or from natural forces as in the weather. The frequency of these events is relatively small. Up to a particular level, weather incidences strong enough to cause damage are compensated for in design but economics will limit this protection. Therefore, there is always a hazard posed by these catastrophic types of events. The risk posed by these hazards is the background risk which the public normally accepts without complaint (section 3.2.3.). The types of events which are relevant to this facility will be considered here to give a standard by which to compare the other risks developed and evaluate what may be considered an acceptable risk. The probability distribution of complete plant destruction from these events is given in Figure 8.15.

8.9.1 Airplane Crash

This water treatment facility is located within the five mile radius of a municipal airport. The largest airplanes allowed to land at the airport are small jets carrying approximately 100 people (Transport Canada). It is a relatively busy airport with approximately 140,000 landings and takeoffs per annum. From studying the accident report information for airplane crashes, most occur during landings and takeoffs, within a few hundred meters of the runway. The distance between this facility and the airport, is great enough that the increased accident rate from landings and take offs should not affect it. The probability of being killed by a falling aircraft is given by Bulloch(1984) as 10^{-6} per person per year. Gibson (1976) gives a value of 10^{-8}. This study used the value of Bulloch (1984) at 10^{-6} per annum. A standard deviation of 5 x 10^{-7} was used to develop a normal distribution.

8.9.2 Environment

Environmental events are always difficult to predict, and can range from storm events to seismic events. For this particular facility, the probabilty of an earthquake is negligible. However storm events do pose a level of risk that should be considered. The most serious of these events is a tornado.

Newark(1983) studied the frequency and strength of tornadoes within Canada and predicted the probability of occurrence of a particular tornado for particular regions. From his development, the probability of being hit by a tornado that is capable of serious structural damage is 0.02% per 1 km^2 per year. This particular facility has an area of approximately 1 km^2 which results in an annual predicted frequency of 0.02% which is equivalent to a 1 in

5000 year chance.

Wallace (1987) indicated that this frequency may actually be low for the particular area being studied, because of a lack of data. Therefore, the probability distribution represents this inaccuracy by having a standard deviation .00005.

These two events have been considered since they would have enough force to cause serious structural damage. There would not be any reason to try and design a system which could handle such an exterior force since such an event would result in the entire plant being shut down from other structural damage. The probabilities of theses destructive events give baseline values below which it would be unreasonable to reduce other risks.

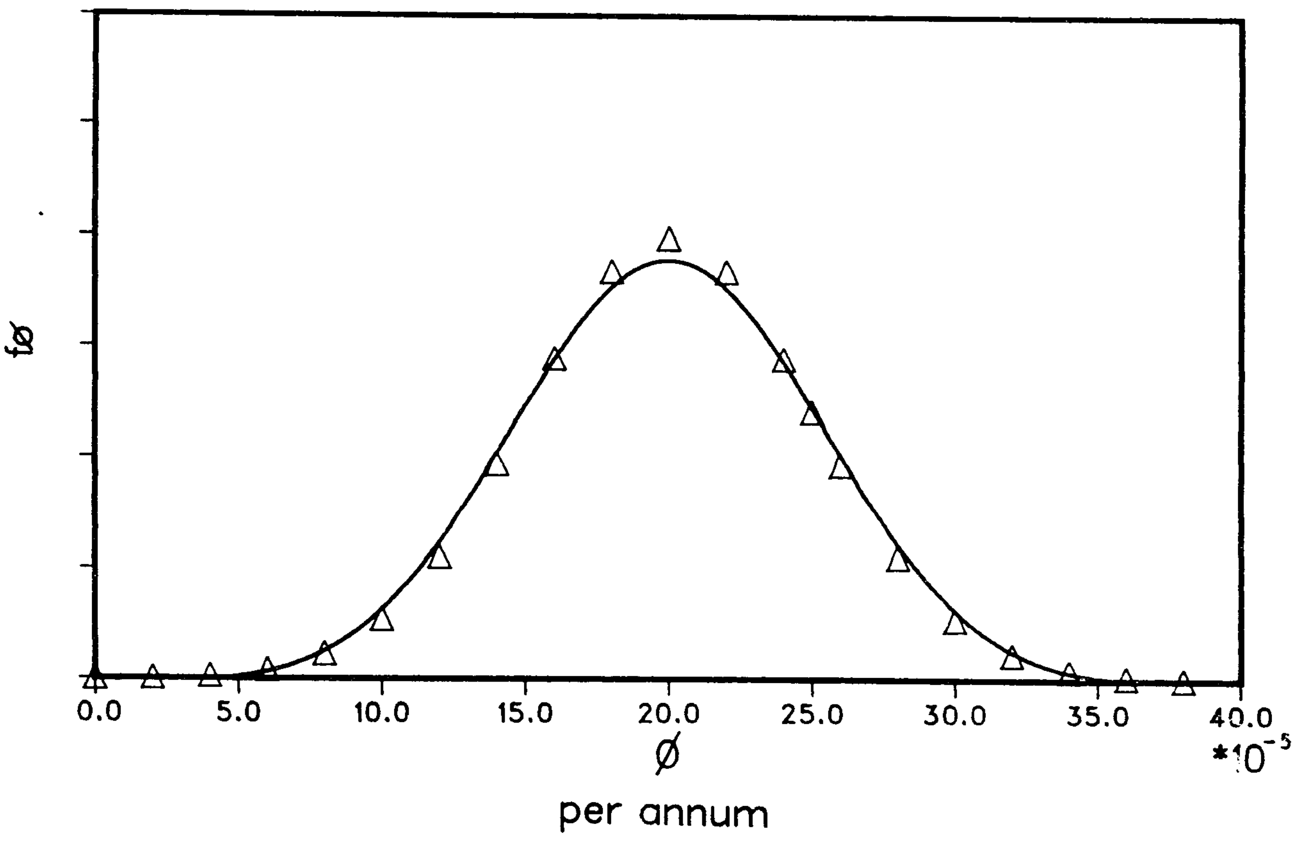


Figure 8.15 Probability distribution of complete plant destruction

9. CONSCEQUENCE ANALYSIS

The damage states which were developed in both the hazard and frequency analysis defined an undesireable consequence which was to be prevented. There were two damage states considered, the first was an exposure to chlorine gas and the second was the water not receiving chlorine. The consequence analysis considers these damage states and determines how they will directly affect the employee in the former case and the water quality in the latter case.

9.1 Exposure to Chlorine Gas

9.1.1 Controlled Release

For this damage state, the severity of the injury will depend on the quantity of gas the person is exposed to and the length of time of exposure. From the controlled release scenario, the most likely route of exposure was from a fouled eductor and a small quantity of gas remaining in the lines (Fig. 7.16). This would result in a brief exposure to approximately 0.2 L of less of concentrated gas. This small quantity of gas would immediately disperse in the atmosphere of the storage room. Although would still be very concentrated and may cause some discomfort, it should not cause any long term problems. However, for a person with respiratory problems such exposure could produce a mild pulmonary edema. The severity would depend on factors such as how close the workers face was to the opening, if he was wearing a protective face shield and whether he was breathing in or out at the time. All of these factors are difficult to determine, but they do indicate simple measures which can reduce the chance of exposure.

Demanding that all workers wear a breathing apparatus is not realistic. Even when tonners are being changed and there is a great chance for exposure to chlorine remaining in the flexible connectors, the staff do not wear breathing masks. There is not any point in setting unrealistic regulations that will be broken. Rather, it is better to have regulations which are truly necessary to protect the individual and will be followed.

The scenario for handling liquid chlorine in the headers indicates there is a chance for exposure to the gas, however the workers are wearing appropriate breathing apparatus and protective clothing. The technique used to handle the liquid chlorine may be questionable. The application of water to the chlorine vapours would control them, however hydrochloric acid which is very corrosive will also form which may have a destructive effect on the ventilation flumes and fans, and other equipment.

This scenario would most likely result in severe skin irritation. Protective clothing must be worn to prevent a possible chlorine burn.

An open vacuum line or chlorinator without correct isolation could be devastating, particularly if the pressure regulating valve was stuck open. Chlorine gas under 240 kPa would pour out of the line or chlorinator. There is no doubt inhalation would occur but the severity would depend on the persons ability to remove himself. A frequency analysis (Fig. 9.1) indicateds that it is highly unlikely that a worker would not remember to perform the necessary isolation steps or that the valves would fail.

When maintenance is required on a line or chlorinator, the unit is isolated by the operator, so that chlorination continues. Once isolated, a work order is placed for the necessary repairs. The maintenance staff then recheck the isolation before performing any work. To have a severe consequence which would be death or critical injury, both operational and maintenance staff would have to forget to isolate the equipment. If there was no isolation, a severe injury could occur. The important factor in reducing the consequences is the awareness all the workers have about the hazards of chlorine. They must all take care to protect themselves and other workers.

9.1.2 Uncontrolled Release

Since an uncontrolled release occurs unexpectedly, the consequences of such an event are more severe. Prevention of a death or critical injury in these instances depends mostly on the warning system and response of the individuals to that warning system. An uncontrolled release from the piping or a tonner valve would result in chlorine gas at a pressure of 240 kPA at 20°C and flowing at 1.8 g/s being discharged.

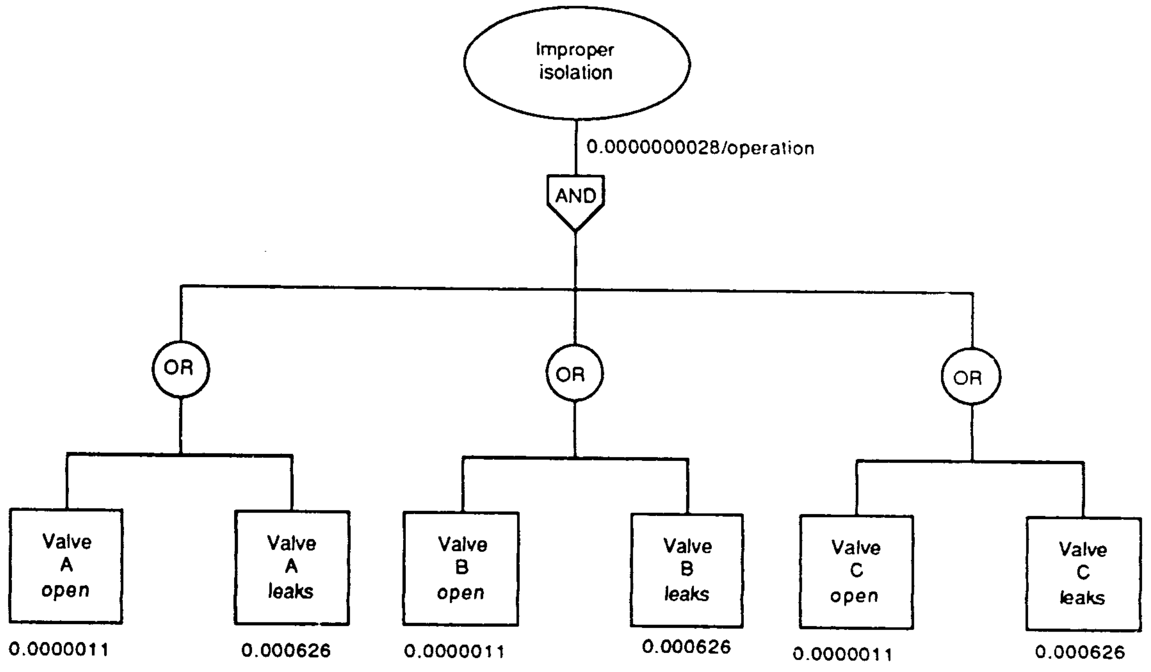


Figure 9.1 Fault tree of improper isolation resulting in a leak

In the case of a tonner rupture the entire contents could be released which is equivalent to 907 kg of liquid chlorine. When a chlorine leak occurs, the gas will hug the ground. The first meter of ai. closest to the ground would have the highest concentration which after 3 min would be approximately 9.4 mg/L at the extreme edges of the cloud, but could be completely concentrated at the source of the leak. The health limits indicate that 25 mg/L is the toxic limit (Table 6.2.).

Given an uncontrolled release occurs, the ventilation unit should be activated within 2 to 3 s. The response time to the alarm given that the operator takes time to don a breathing apparatus should be no more than 3 min. At a flow rate of 6.9 kg/hr, out of a 25 mm valve, three minutes would allow 340 g of chlorine to escape (Appendix E.1).

If the ventilation unit is automatically activated, the entire volume of air within the storage room can be exchanged in approximately 3 min with the waste air vented to the atmosphere. The chlorine gas would be diluted by the mixing action from the suction. From the large quantity of air drawn into the flume the concentration of gas released from the vent would not exceed 1 mg/L. This concentration can be verified from the controlled release event which occurred when liquid chlorine had filled the headers. As the gas was released, the air surrounding the building was monitored for chlorine gas. The concentration never rose above 1 mg/L (Operator Interview).

From the frequency analysis there is a high probability that the warning system and the ventilation unit will be activated. However, the response to the leak alarm would more than 50% of the time be an operator without an airpack (Fig. 7.17). If there was a person injured, collapsed within the room, an operator without an airpack would require an additional 3 to 4 min to get a breathing apparatus. This would allow an additional 340 g of chlorine to be released. For an injured person collapsed on the floor, th [illegible] additional 3 min of exposure to the chemical. The injured operator would be in the worst possible position, close to the leak source and lying on the floor, he would be exposed to the highest concentration in the room.

The forcing of a corroded valve would have an operator present when the release occurred. Otherwise the presence of the operator would have to be coincidence, during their two hour routine inspection. For the latter instance the operator would not be directly affected by the release, therefore serious injury could be prevented by the operator removing himself.

Of those scenarios which would result in an uncontrolled release, the collsion scenarios would all have a man present at the instance of release. These scenarios could result in a critical injury or death, since there is the potential for a direct contact from the chlorine.

If a PVC vacuum line break occurred, the consequences should be a loss of chlorination. However, the correct combination of a failure of valves could result in a major leak, that does not have a leak detection system nearby (Fig. 7.11). Such a break would occur in the presence of an operator or another person who would have been responsible for the break. Therefore this person should inform the shift foreman and take corrective action within minutes.

Such a break would release a quantity of chlorine even if the pressure regulating valve closed, since there would be residual chlorine gas in the line. Approximately 20 L of gas would be released if two lines were carrying chlorine and both were broken (Appendix E.2). The direct application of 20 L of chlorine gas could cause a serious injury however, the collision would probably be caused through movement of some type of machinery. Therefore the person would be clear of a direct blast relatively quickly. This gas is not under pressure so the flow rate would be low. Serious injury in this scenario is not likely to occur, however the exposure to the gas could cause discomfort. This type of incident would create more overall discomfort since lingering fumes would affect the entire plant. There are not any ventilation fans or alternate methods for clearing a release in this area.

Operator impact would cause a vacuum line break in the storage room. If the break did result in a major leak, the consequences would be the same as those from the other collision scenarios resulting in an uncontrolled release.

9.2 Water Not Chlorinated

The consequences of the water not being chlorinated can range from the contamination of the water supply so that there is no longer an assurance of virus or pathogenic bacterial inactivation to a slight drop in residual chlorine that still remains above the lower limit of the guidelines. The contamination of the supply does not necessarily equate to public illness since there is the option of either shutting down the plant until chlorination can be restored or warning the public of the problem so that they can take precautions.

The time of discovery is a key factor for preventing a loss of chlorination. If the incident which prevented chlorination was not discovered, the first indication of a loss of chlorination would be the drop in the residual chlorine analyser. This automatic analyser records the residual chlorine in the flume continuously. As soon as the residual began to drop significantly, the operator in the control room would investigate.

The length of time before action depends in part on the reliability of this instrument. From maintenance records this particular analyser needs adjustment at least once per month. While this may indicate an unreliability, it shows that a discrepancy in the results between the manual residual analysis and automatic residual analysis is immediately investigated.

The average length of time the water would not be chlorinated would be approximately 0.5 h. If the analyser failed and did not indicate the falling residual, the length of time increases to a maximum of two hours, which is the time between the manual analysis and chemical feed rate checks.

The consequences of the water not receiving chlorine for two hours would in part depend on the flow rate. At higher flow rates, the retention time is reduced allowing more water to pass that would not have been disinfected.

The normal procedure for determining the adequacy of the disinfection is through bacteriological tests including total coliform, fecal coliform, and streptococci. The total coliforms are limited to a maximum of 10 coliforms per 100 mL treated water sample with no more than 2 consecutive samples for the same sample indicating the presence of the organisms (Annual Report, 1986). This facility consistently has kept this value at less than 2 per 100 mL. While the coliform test does offer a relatively quick analysis of the water quality it does not give an accurate representation of the presence of viruses or cysts. Even at optimumm efficiency, with consistent total coliform counts of 0 organisms per 100 mL, there has been some doubt as to the ability of this facility to provide adequate disinfeciton against viruses and cysts (Hrudey, 1986). Therefore, even 0.5 h of lost disinfection could pose a threat to public health. The maximum two hour time length could allow contaminated water into the distribution system.

9.3 Exterior Force

The frequency analysis indicated that the probabilitv of the facility being struck by either a natural weather disaster such as a tornado or by an air plane crash was less than 0.0002. The consequence of such an event would be destruction of the plant. Should such an event occur, it would be highly unlikely that there would be water being pumped into the plant, therefore chlorination would not be required. This analysis represents a natural disaster that the designer cannot protect the system against. Therefore it represents a lower limit below which it would be unreasonable to reduce other risks.

10. MANAGING THE RISK

The risk for both the injury and water quality damage states is defined once the three elements of risk, the scenarios, frequencies and consequences are developed. The frequency and consequences of each scenario can then be compared with target values set by the risk managers. The risk is only acceptable if both the frequency and consequences are below the target value. If one of these elements does not comply with its target value, that element is reviewed to determine if it must be changed. An element that exceeds its target value may be tolerated if the other element reduces its effect and therefore the risk.

10.1 Injury Scenario

Initially, a target probability distribution for the injury damage state was set by developing the probability of a catastrophic event affecting the facility. The catastrophic events were developed by analysing the probability of destruction from a tornado or an air plane crash. The combined probability distributions for these events had a mean probability of occurrence of 0.00023 per annum. The FAR guidelines used by ICI set a limit for the probability of death from an individual chemical at 0.000035 per annum. The ICI limit is an order of magnitude lower that the limit used in this study.

The higher limit was considered acceptable because of the relative severity of the consequences which were being dealt with at the water treatment plant. None of the scenarios contained credible events which would definitely result in death for the injury damage state. Only an uncontrolled release, when an operator was unable to remove himself may have resulted in death. The response time of the personnel and whether or not they were wearing appropriate breathing apparel affected the probability of a fatality occurring.

The probability analysis indicated the frequency of of an uncontrolled release causing injury was 2.7 x 10^{-4} per person per annum. The results of this probability analysis were close enough to the target value (2.3 x 10^{-4} per annum) to be acceptable, however the probability of injury could be reduced even further through a simple modification. The addition of breathing equipment closer to the storage room would reduce the exposure time, resulting in a lower probability of injury.

The consequences for the scenarios resulting in injury from a controlled release varied from no exposure to a brief but direct exposure. The latter consequence had a high frequency of occurrence (.622 exposures per annum). This value represents plant conditions which are currently accepted by management.

The most frequent exposure to chlorine was from a small quantity of chlorine gas remaining in the flexible connector. The high frequency of this scenario is currently accepted because the initiating event is an operator not completely draining the flexible connector which is attributed to human error. Many managers consider such "human errors" to be unavoidable and unchangeable. Training seminars and penalties have been employed but judging from the high rate of occurrence of these exposures neither training nor penalties are working. To reduce the risk for this scenario either the frequency of occurrence or the consequences must be reduced.

When the tonners empty on a night shift the operator must switch tonner banks when he is tired and not as alert. This mental fatigue contributes to the occasional event when the connector is not completely emptied of chlorine.

Because the elimination of this scenario would be difficult, reducing its consequences, while accepting its frequency of occurrence may be an alternative. White (1986) has suggested that if there is a possibility of exposure to the gas, a breathing apparatus should be worn. At this particular facility, this has not been a practical solution because workers are reluctant to wear breathing equipment for minor consequences. The breathing equipment currently used is awkward and bulky which likely contributes to the current attitude. Also, there are only three units located in the main plant. If two were used for changing tonners, only one would be available if an alternate chemical emergency occurred.

To reduce the direct exposure, procedures must be suitable so that they will be followed and will not create an alternate hazardous situation. Rather than a full breathing apparatus, a small breathing mask or a face shield would be more appropriate. If the equipment were not awkward and uncomfortable the staff would be more receptive to wearing the breathing equipment during tonner changes. Additional breathing equipment would also be useful at the facility. If this type of equipment was not suitable, a face shield would protect the face from any direct contact with the chemical in the event of a release. A face shield is not bulky and provides adequate vision.

Activation of the ventilation unit should also be part of the tonner change procedure. Some operators already do this as part of their routine. In the event of a small release, chlorine gas would be quickly and immediately dispersed. These procedures do not prevent the event from occurring, but protect the operator by introducing safeguards that reduce the consequences and therefore the risk.

For scenarios which could lead to the exposure of a maintenance person to a small quantity of gas, a small gas mask or face shield should also be worn. A gas mask provides both respiratory and skin protection. A face shield would prevent the direct contact of the gas with the face. By implementing these small changes in procedure and equipment locations the likelihood of injury from a controlled release would meet the target values.

10.2 Contaminated Water Supply Scenario

The contamination of the water supply damage state had a slightly lower target value for an acceptable level of risk. Because the final consequences of a contaminated water supply would affect the public, the probability of death from background risks which society readily accepts everyday was used (section 3.2.3). Kletz (1981) developed an acceptable social risk was used for the target value (10^{-5} per annum). The probability of death for a man age 30, is 1 in 1000. An event with a probability of occurrence of 10^{-5} increases that risk by 1%. A 10^{-6} probability of death increases the risk by 0.1% The 10^{-5} value was used rather than the 10^{-6} value because the consequences for the contaminated water supply would not necessarily result in death. Some of the consequences of a stoppage of chlorination are unknown because they depend on the quality of the water immediately preceding the disinfection stage.

The breaking of a chlorine solution line had the highest probability of occurrence. Freezing of the pipes in the winter is responsible for the high failure rate. This event does not have any warning alarms. The automatic residual analyser would be the first indication of a loss of chlorination.

The frequency of occurrence for this event (2.32 breaks per annum) is much higher than the limit of 10^{-5} per annum. Therefore, either the consequences or frequency of this event must be reduced. The consequences could be reduced by installing alarms at the diffusers which would signal an interruption in the flow. The frequency could be reduced by heat tracing the solution lines or providing insulation.

The choice between these two methods would depend on cost. Heat tracing all the pipes is a preventative solution however it would have a higher initial cost. Savings in overtime salary to maintenance personnel may eventually offset the additional cost. Reducing the number of breaks rather than giving a warning of their occurrence, directly reduces the frequency for the water not receiving chlorine. It does not rely on predicting the reliability of personnel response to the alarm.

The remaining probability distributions developed for the water quality damage state were well below the target values. Each event which could lead to a loss of chlorination had a corresponding alarm or alarms which give adequate warning of the event. Other than a review of the alarm systems, little can be done to reduce this risk.

This assessment does not judge whether this facility provides adequate disinfection, it only represents the effects of a loss of chlorine in the system. The ability to provide adequate disinfection depends on the complete treatment process including turbidity reduction, organics removal, pH adjustment, mixing and settling conditions. While the warning systems are adequate to prevent a loss of chlorination, the remaining processes should also be reviewed. The risk to the public from an inadequately disinfected water supply could then be evaluated from the combined results.

11. DISCUSSION

The technique of quantitative risk assessment was developed for industries in which the failure of equipment or humans, would result in severe plant damage or a fatal accident. These industries recognized the severe impact they could have on employees and the public, so they devised methods which would help them to communicate among themselves, to the government and society how they were controlling that possible impact.

Risk analysis has traditionally focused on facilities which the public and government would view as threatening, but it also is a suitable technique for those facilities which are not viewed with the same reverence. The flexibility of the technique allows for an analysis which is only as detailed as the designer wants and requires. It can focus on quality control as well as safety, for both employees and the public. With the increase in litigation that has become a routine occurrence for some professions, the assessment can provide a detailed and documented account of how and why decisions were made.

An additional aspect of quantitative risk assessment is the potential for improved efficiency which follows improved safety up to a practical economic level. Some sections or processes within the plant may be marginally tolerable or inefficient. In these areas, an assessment can provide new information because it dissects the process into small enough elements so the origin of the problem can be determined and hopefully solved.

The application of this technique to a municipal water treatment plant considered the impact on employee safety and water quality with specific reference to the chlorine unit. To consider the risk analysis as essential, areas which contained unacceptable risk should have been exposed. For a facility which uses processes that have remained unchanged for nearly sixty years, it was not expected that there would be many unacceptable risks exposed. Discovery of inefficient or marginally acceptable areas was expected.

The only scenarios which did not meet the target risk values for the injury damage state, were those which resulted in a brief exposure to chlorine gas. Because a reduction in the frequency of these events could not be easily achieved, a reduction of the consequences through procedure modifications was suggested.

The rate of occurrence of these scenarios was not new information to the managers or staff. They were aware of and tolerated the occurrence rate of the events. The low frequency values for the other injury scenarios and most of the contaminated water scenarios were also expected by the cperations staff.

The risk analysis verified the safety record of the particular chlorine unit studied. Standards which have been set by the industry have been proven acceptable. Where accepted practice has not been followed, the risk associated with deviations from the standard practice is currently accepted by management staff. Both the exposure of personnel to small quantities of chlorine and the lack of adequate breathing equipment are examples.

These conclusions were made about the current chlorine storage and feed unit. Accidents and some close calls have resulted in changes and modifications to the storage and feed unit. These modifications reduced the risk to its present level.

11.1 Modifications Which Have Reduced Risk

The heating unit analysed was installed and operated for the first time in the winter of 1987 - 88. Prior to this new unit being installed, a gas fired heater was used with only the five small electric heaters as back-up. This gas heater would be inoperable at least three or four times during the winter months. The maintenance staff indicated that the problem was related to a pilot light that was extinguished under extreme wind and cold. Those weather conditions occur when the heater would be required the most. Because this event occurred regularly, a large propane heater was permanently left in the storage room. During one of the gas heater failures the propane heater was aimed directly at a tonner. Fortunately, the operations staff corrected the positioning of the heater before any serious damage occurred.

The chlorinators are manifolded to parallel headers. There were two additional valves on the manifold identical to valve A (Fig. 6.1). These duplicated valves were located approximately 150 mm to the right of the A valves for chlorinator 4. The valves opened to a header system which discharges into the raw water rapid mixer for plant 1. The purpose of the valves was to provide a waste route for the air which used to purge the chlorine gas remnants out of the chlorinators after they had been taken out of service. On one occasion when chlorinator 4 was being put on line, the operator watching the manifold pressure gauge had turned his head. He inadvertantly opened this waste air line. The result was connecting a low pressure line to chlorine gas at 240 kPa.

A large dose of pure chlorine went to the plant 1 rapid mixer. The odor was immediately detected by the operator and the valve was closed. The lack of adequate ventilation outside of the storage room allowed chlorine gas fumes to linger throughout much of the work day. This condition caused many of the daytime employees to experience nausea and headaches. The operator involved also experienced nausea, but was able to immediately close the valve and remove himself. This scenario resulted in the offending valves being permanently closed and the handles removed.

Several factors become clear when this incident is reviewed. The lack of adequate ventilation caused several employees to be affected by the lingering fumes. The release of the gas under pressure for three to five seconds would have released 9 to 10 g of chlorine which is equivalent to approximately 3 to 4 L of gas. This quantity of gas created discomfort for most of the plant personnel once it was distributed throughout the plant air ducts. Should a PVC vacuum line break occur outside of the storage room, an estimated 10 to 20 L could be released without adequate ventilation. This could cause a temporary plant shut down.

This type of accident is one which could easily have been avoided. As Kletz (1986) indicates, there are several examples of this type of mix up caused by identical valving, that designers can easily avoid. These types of situations are accidents waiting to happen.

There has been one serious chlorine accident at this facility which occurred at plant 3. Improperly sized and unreliable equipment were the causes of the uncontrolled release. Chlorinators which regulated and indicated the flow rate of the chlorine out of the tonners were attached directly to the tonner valve. When the tonner was empty, a flag indicator attached to the tonner should have switched from green to red.

This particular chlorinator was over sized, so that it often did not register the flow rate. The flag mechanism on the valve was also faulty so that the staff no longer relied on it. These factors combined so that an operator opened a full tonner which he believed to empty. The operator wearing a face shield, received a full blast of chlorine at 240 kPa pressure in the chest. He removed himself only to return seconds later without proper breathing equipment to shut off the valve. This entire incident could have been avoided if the equipment had not been faulty and improperly sized.

Flooding of the chlorinators with the supply water has become so routine at this facility, that drain valves have been installed to provide easier and safer maintenance procedures. When the chlorinator floods, the water will contain residual chlorine gas that was in the vacuum line. The chlorine concentration is high enough to set the leak detectors off when the water is drained from the line. Drain lines have been installed from the PVC line before it enters the chlorinator down to the floor. The fumes produced during draining are now sucked up by the ventilation unit. This reduces direct exposures to the gas.

The ventilation unit has recently been upgraded. The older unit consisted of only one fan with two flumes located in the north end of the building. This upgrading was completed during the winter of 1987-88. The capacity of the older unit was not available, however most of the staff expressed their doubts about the adequacy of this unit. The new unit will provide ventilation that meets the recommended guidelines.

All of these changes resulted in a safe, reliable chlorine storage and feed unit. Through trial and error the system was improved so that the risk analysis on the current system indicated a low risk facility. However, there are still some areas in which the risk could be reduced through minor modifications

The chlorine unit has several alarms which indicate that an undesireable situation has occurred in the chlorination equipment. Operator interviews demonstrated that there was confusion among the staff about the purpose of some alarms and how they are activated. The chlorine leak alarm and low pressure alarm were both clearly understood, however the high/low vacuum was not well understood.

The design for the high/low vacuum alarm is very poor. Both alarms activate a single slot on the alarm panel audibly and by a flashing panel light. When both a high and a low vacuum condition activate the alarm there is no way of knowing which event has occurred. A separate alarm location for each alarm would eliminate much of the confusion. By removing this confusion and providing proper instruction, the response to these alarms would be increased.

The activation of the leak alarm may be a relatively common occurrence. This has lead to a lapse in the response routine. The facilities policy is to don a breathing apparatus immediately and investigate a leak alarm. This is rarely done. Only those operators in the control room who are aware of the events in the storage room follow the established procedure.

Managerial staff are responsible for ensuring safety policies are followed. This may require a biannual review or even quarterly review of safety procedures. Management would likely be held responsible for an accident if they did not insure that safety procedures were followed regardless of the difficulty in obtaining cooperation by operational staff. Documentation of management efforts to insure safe safe practices by operational staff would likely be required if management were to hold a staff member responsible for an accident caused by poor practice.

When safety policies and procedures are reviewed it cannot be done in isolation. All of the operations and maintenance staff are aware of the required safety response procedure to a chlorine leak alarm. However, the staff do not follow this procedure. This situation would be difficult to correct with more rules and regulations. If the existing rules are not being followed, additional rules would not be either. Enforcement of the policy may be increased through drills and penalties, but this may create some animosity from the operators having to follow regulations they believe are unnecessary. Increased enforcement would also create a situation where the rules would only be followed when management was in attendance.

Not withstanding these difficulties, the current situation cannot be ignored. The lapse in following the recommended standard procedures has occurred because the plant has a good saftey record. The operators have switched their procedure to one of investigating first and then donning breathing equipment if required. Given this experience, the facility should correct current practice. There are three air packs available to the operators that are all presently located on the second floor of the plant.

At least one air pack should be located on the bottom level to increase accessibility and reduce the time required to obtain an air pack.

In the event of a leak, those personnel located on the second floor will not be directly threatened. The air packs are located outside of rooms in which the staff would most likely be. The intent is that prior to going down into an environment possibly filled with chlorine they have time to put on an air pack. While this is a reasonable scenario, there are instances where operators are on the first level. They must go upstairs to get an air pack. This is undesirable, so there is clear justification for at least one or two air packs located on the ground level, with one reasonably close to the storage room.

In the event of a major release there are not enough air packs for all of the personnel. There are three for the operations personnel, one for maintenance, another for the instrumentation personnel and one for the lab staff. If it is judged to be too expensive to supply air packs for all personnel in the area, there must be a practical plan which all personnel will follow in the event of a release. Action plans should also be developed for the other chemicals which can be spilled or released.

The switch for the ventilation unit can only be reached from inside the storage room. Should a leak occur without the alarms being activated, the ventilation unit would not be activated either. To disperse the chlorine, an operator must enter the storage room and manually switch on the ventilation. By having a switch outside the room, the ventilation could be activated immediately rather than waiting for a person with a breathing apparatus.

The brief exposure of personnel to small quantities of gas has been mentioned. Face shields and activation of the ventilation unit can reduce the consequences of a small release. In addition to maintenance personnel wearing face shields during repairs on chlorine equipment, a mechanism for draining and neutralizing the chlorine gas would eliminate the possibility of an exposure. Emptying the line into a caustic solution may be sufficient.

The current method of reducing chlorine gas vapours applying ammonia should be reconsidered. The reaction between the chlorine and ammonia can form monochloramine, dichloramine or nitrogen trichloride depending upon the molar ratios of ammonia and chlorine. Nitrogen trichloride is a volatile and very irritating chemical which could create an alternate inhalation hazard.

Cleaning of the chlorinators and chlorine headers with alcohol is a hazard. The maintenance staff have indicated that they would not use the alternate solvent trichloroethylene, because there is some experimental evidence of a link to cancer. Consequenty they use alcohol. However, White (1986) describes two cleaning procedures in which neither alcohol nor trichloroethylene are used (Appendix G.1). These two methods would take more time and therefore are more expensive, however they offer a very reasonable solution to this cleaning problem.

An improved preventative maintenance program would greatly reduce some failure rates. With a chlorine unit, it is not acceptable to install new equipment only when there is a breakage or failure. Both the chlorination manual (1977) and White (1986) give daily, weekly, monthly and yearly maintenance schedules which are not currently being practiced.

There should be a complete review of the current system to ensure that correct and consistent action is taken in the event a failure occurs. All of the operators have taken training courses, but each system has unique sections which demand this type of review.

Understanding the disinfection mechanism and purpose of chlorine addition is also important. How the chlorine interacts with the other chemicals within the water must be understood by the operators so that deviations in the analysis on the water can be explained and as a result corrected. For protection of the water quality and personnel safety this basic knowledge is essential.

11.2 Application of Risk Analysis at the Design Stage

Rather than using ten years of trial and error to provide a safe and reliable facility, performing a quantitative risk assessment on new designs would be beneficial. A risk assessment questions and anticipates many design faults prior to implementation. Changes on paper are simpler and more cost effective. Savings at this stage can justify the expense of a risk assessment.

The current activated carbon feed system represents an example of where a risk assessment may have been beneficial at the design stage. The new unit was installed and operational in June 1986. Stachowski (1987) estimates that $50,000 in renovations are required to make the unit operationally reliable.

The activated carbon storage and feed unit was analysed using the quantitative risk assessment technique (Appendix F). Many of the design flaws could have been discovered at the design phase prior to implementation. The pump and required slurry concentrations would certainly have been reviewed to ensure that the quantity of carbon required for treatment would be met. Many of the valves between the pumps and storage tank are unable to provide adequate isolation. The carbon plugs the pumps preventing them from starting upon demand. Even when the flushing procedures are followed the pumps often fail to start when required. The adequacy of these valves could have been verified from either type II or III data.

A computer is used to regulate the addition of water by opening and closing a valve. This allows a small amount of freedom for the operator. However, the rest of the operation requires manual movement of the valves, so this small amount of automation does not reduce the human input or reduce water addition errors.

12. CONCLUSIONS

Risk consists of three separate elements: the scenario, the probability of occurrence of the scenario and the consequences of the scenario. By altering anyone of these three elements, the risk may bn increased or reduced.

This particular risk assessment did not identify any scenarios which had not been already recognized or experienced. However, by breaking each scenario into its elemental events, the causes of these scenarios could be examined. The scenarios which are presently tolerated in the system, have initiating events which are attributed to human error. Those events which were not tolerable have been changed.

The probability analysis did not produce any unexpected results. The mean probability values generated were below the target values set, except for the failure rate of the chlorine solution line and the brief exposure of personnel to small quantities of gas. Although both of these scenarios had frequencies higher than the target value set in this study, they are currently accepted by management with knowledge of the consequences.

There were several scenarios which could have a reduced risk by an alteration of the consequences. The recommendations which follow, all focus on altering the consequences which reduce the risk. Consequences which are currently accepted, can be easily and economically adjusted so that the offending scenarios will result in insignificant consequences.

Although this assessment may not have provided any startling information about potential hazards, the assessment has been useful. The results validated operational experience which indicated that the current chlorine facility is safe and reliable. By considering each of the three elements of risk, the overall risk can be reduced through minor alterations which affect the consequences. A risk analysis on the original design of this unit should have indicated the required modifications which were discovered through trial and error. The risk assessment technique can be beneficial as a design tool or as a system review for a municipal water treatment plant.

General Conclusions

Most of the chemicals and chemical addition processes used in municipal water treatment plants have not been fundamentally changed for at least sixty years. Facilities are designeed from conventional, well established techniques. Other than verifying the adequacy of the techniques a probabilistic risk assessment would not provide any new information about water treatment plants that has not been discovered through experience. For existing plants or proposed designs that follow these coventional methods, a quantitative risk assessment would likely not be a useful design tool.

For many existing and proposed facilities there are sections which deviate from these conventional practices. These deviations may result from new designs, or from cost-reducing modifications in designs. For both of these areas, a probabilistic risk assessment would be useful. The hazard identification and scenario development stages of the assessment may be sufficient because municipal water treatment plants are relatively uncomplicated. The frequency and consequence analysis stages can be used to clarify any uncertainty about the acceptability of a hazard or scenario. As research leads to the adoption of new water treatment processes, such application may find wider utility.

The technique of quantitative risk assessment can be used in areas other than design. A quantitative risk assessment can be used as an educational tool within a municipal water treatment plant. The design team must have a complete understanding of the system to conduct the hazard identification stage. The system is considered under every conceivable condition. This is a very instructive method of understanding how a system will respond and how safety measures protect the system and facility. New employees and designers could perform HAZOP's on existing facilities to increase their understanding of system interactions.

A quantitative risk is an excellent communication tool. When the assessments are performed in a consistent and comprehensive manner, risk values can be compared. When a risk is judged to be unacceptable based on emotion, a quantitative risk assessment can be used to compare the risk to other well known risks. This provides a more rational approach to managing and identifying acceptable risks. This aspect of a quantitative risk assessment would be useful for educating employees on risks which exist for different chemicals and procedures within the plant.

The technique of quantitative risk assessment would be beneficial in the preceding areas. Although a complete quantitative risk asessment will not generally be required for municipal water treatment plants, there are aspects of the technique which would be useful.

RECOMMENDATIONS

As a result of the risk analysis process, several specific recommendations can be made which will reduce one or more element of risk.

1. A comprehensive and accurate collection of success and failure rate data should be maintained for future reference. This would help in the diagnosis of results.
2. An emergency response plan for chlorine and the other chemicals should be prepared and practiced so that all personnel are comfortable with their role in the plan.
3. Management should take measures to ensure that necessary procedures and regulations are followed. These measures should be documented so that management can verify their efforts at seeking good practice.
4. Preventative maintenance of the chlorination unit should be increased in accordance with the recommendations of White (1986).
5. A complete review of the chlorine system and the corresponding alarms should be performed.
6. All of the staff should review the chlorine chemistry and reactions with ammonia and with other substances in the water to insure a sound understanding of what processes are occurring.
7. The procedure for tonner changes should include: a. activation of the ventilation unit, b.donning of face shields or alternative breathing equipment.
8. Additional air packs should be provided, with one

located next to the chlorine storage room on ground level.

9. Ventilation fans should be installed in hallways which may be exposed to a chlorine release.
10. A ventilation switch should be located outside of the storage room.
11. The high/low vacuum alarms should be separated on the alarm panel to reduce confusion.
12. A draining and neutralization procedure should be prepared for accessing a chlorine line. The gas can be neutalized by bubbling through caustic (NaOH).
13. A cleaning solvent for the chlorinators and chlorine headers other than alcohol must be introduced.

REFERENCES

APHA (American Public Health Association) (1980). Standards Methods for the Examination of Water and Wastewater. 15th Edition, Washington, D.C. 349 - 356.

Annual Report, Water Treatment (1986). The City of Edmonton, Alberta. 46 - 61.

Annual Report, Water Treatment (1985). The City of Edmonton, Alberta. 46 - 61.

Annual Report, Water Treatment (1984). The City of Edmonton, Alberta. 46 - 61.

Bowen, J.H. (1976). Individual Risk vs. Public Risk Criteria. Chemical Engineering Progress, 72 (1), 63 - 67.

Bulloch, B.C. (1984). The Development of Quantitative Risk Criteria and their Application to Chemical Process Analysis. In: Risk Assessment in the Chemical Process Industries, American Society for Cemical Engineers, Minneapolis, Minnesota. 4.1 - 4.13.

The Chlorine Manual (1986). The Chlorine Institute, Washington, D.C. 36 p.

Cylinder Ton Container Procedure for Chlorine Packaging. (1980). Chlorine Institute, Pamphlet 17, Washington, D.C. 36 p.

Cotruvo, J.A. (1987). Risk Assessment and Control Decisions for Protecting Drinking Water Quality. In: Organic Pollutants in Water, Sampling Analysis and Toxicity Testing, Ed. I.H. Suffet and M. Malaiyandi, American Chemical Society, Washington, D.C. 693 - 733.

Cullen, E.J. (1985). Nomenclature for Hazard and Risk Assessment in the Process Industries. The Institution of Chemical Engineers, Rugby, England. 48 p.

Emergency Manual, Edmonton Water and Sanitation (1987). The City of Edmonton, Alberta. 1 - 17.

ETSI (Enviro Technical Spills Information for Problem Spills, Chlorine) (1984). Environment Canada, Beauregard Press Ltd., Ottawa, Ontario. 122 p.

Freeman, R.A., Schroy, J.M. and Wilson, J.D. (1986). Assessment of Risks from Acute Hazards at Monsanto. In: Society for Risk Analysis Annual Meeting, Boston, Massachusetts. 2.4 - 2.12.

Funk and Wagnalls Standard Dictionary (1985). Lippincott and Crowell, New York. 358, 693.

Gibson, S.B. (1976). Risk Criteria in Hazard Analysis. Chemical Engineering Progress, 72 (1), 59-62.

Hjalmar, S.S. (1978). Handling, Storage and Feeding of Chlorine, Proceedings of the Twentieth Public Water Supply Conference, Water Treatment Part III, University of Illinios, 53-64.

Hopkins, E.S. (1936). Water Purification Control. The Williams and Wilkins Company, Baltimore.

Hrudey, S.E. (1986). A Critical Assessment of the Safety and Quality of Water in Edmonton. Steve Hrudey and Associates Ltd., Edmonton, Alberta. Volume 1, p 41, 50 - 60.

IWD (Inland Waters Directorate) (1986). Surface Water Data for Alberta, Environment Canada, Ottawa, Ontario. 172.

Joschek, (1983). Risk Assessment in the Chemical Industries. Plant/Operations Progress, 2 (1), 1 - 5.

Kaplan, S. (1986). Dealing With Uncertainty in PRA. In: American Institute of Chemical Engineers, Summer Meeting, Boston, Massachusetts.

Kaplan, S. and Garrick, B.J. (1981). On the Quantitative Definition of Risk. Risk Analysis, 1 (1), 11 - 27.

Kaplan, S. (1985). On the use of data and judgement in probabilistic risk and safety analysis. Nuclear Engineering and Design, SMIRT 8 Conference, Brussels, Belgium.

Kazarians, M., Bradford, W.J. and Abrams, M.J. (1985). Risk Assessment of a Process Facility. American Institute of Chemical Engineers, Annual Technical Meeting, Washington, D.C. 5.1 - 5.36.

Kletz, T.A. (1985). An Engineers View of Human Error. Institute of Chemical Engineers.

Kletz, T.A. (1982). Hazard Analysis, A Review of Criteria. Reliability Engineering, 3, 325 - 338.

Kletz, T.A. (1986). HAZOP and HAZAN, Notes on the Identification and Assessment of Hazards. The Institution of Chemical Engineers, Rugby, England.

Laubusch,E.J. (1962). Chlorine: It's Development , Characteristics and Utility for Disinfection and

Oxidation, In: Disinfection and Chemical Oxidation in Water and Wastewater Treatment, Proceedings of the Third Sanitary Engineering Conference, University of Illinois, Urban, Illinois, 6 - 17.

Lawley, H.G. (1974). Operability Studies and Hazard Analysis, Chemical Engineering Progress, 70 (4) 45 - 56.

Lawley, H.G., Parvin, R., Notman, J., and Bullock, C.J. (1985). Practical Quantitative Hazard Assessment, University of Durham, Institution of Chemical Engineers, University, of Durham, England.

Leplat, J. and Rasmussen J. (1984). Analysis of Human Error in Industrial Incidents and Accidents for Improvement of Work Safety. Accident Analysis and Prevention, 6 (2) 77-88.

Lowe, D.R.T. (1984). The Hazards of Risk Analysis. Reliability Engineering, 1, 243 - 256.

Mann, R.D. (1962). Feeding, Handling and Storage of Chlorine, Disinfection and Chemical Oxidation in Water and Wastewater Treatment. Proceedings of the Third Sanitary Engineering Conference, University of Illinois, Urban Illinois, 18 - 28.

Mehta, H., Augustus, M., and Chen, C.L. (1987). Planning a Chemical Handling System. Operations Forum, 4 (2), 15 - 20.

Montgomery, J.M. (1985). Water Treatment Principles and Design. John Wiley and Sons, New York, New York. 379 - 381.

Mosleh, A., Kazarians, M., and Gekler, W.C. (1986). Development of a Risk and Reliability Data Base for Chemical Facilities. Amer'can Institute of Chemical Engineers, Summer Meeting, Boston, Massachusetts.

Newark, M.J. (1983). Tornadoes in Canada for the Period 1950 - 79. Environment Canada, Downsview, Ontario. 70 p.

OHSA (Occupational Health and Safety Regulations) (1976). The Occupational Health and Safety Regulations of Alberta. Government of Alberta, Edmonton, Alberta.

Parvin, R. (1985). Operator Intervention - A Guide for Hazard Analysis. In:Practical Quantitative Hazard Assessment, University of Durham, Institution of Chemical Engineers, University of Durham, England. 1 - 10.

Pasman, H.J. (1985). Risk Analysis In the Process

Industries. European Federation of Chemical Engineering Publ. Series no. 45, The Institution of Chemical Engineers. 95 p.

Pfaffenberger, R.C. and Patterson, J.H. (1987) Statistical Methods. Irwin Inc., Homewood, Illinois. 268 - 288.

Rasbash, D.J. (1984). Criteria for Acceptibility for Use with Quantitative Approaches fo Fire Safety. Fire Safety Journal, (8), 141- 158.

Rasmussen, J. (1987). Approaches to the Control of the Effects of Human Effor on Chemical Plant Safety. Presented at: The International Symposium on Preventing Major Chemical Accidents, Washington, D.C. 6.1 - 6.24.

Schreiber, A.M. (1982). Using Event Trees and Fault Trees. Chemical Engineering , 89, (20) 115 - 120.

Seddon, F. and O'Key, P. (1985). Safety in the Use of Chlorine, Water Services, 89, p 106.

Stachowski, Woytek (1987). Activated Carbon Feed System Upgrading Proposal. The City of Edmonton, Alberta. 29 p.

Starr, C. (1969). Social Benefit vs. Technological Risk. Science, 165, 1232 - 1238.

Swain, A.P. (1987). Relative Advantages of People and Machines in Process Industries. Presented at: The International Symposium on Preventing Major Chemical Accidents, Washington, D.C. 6.97 - 6.128.

Vaughn, J.C., Turre, G.J. and Grines, B.L. (1971). Chemicals and Chemical Handling, In: Water Quality and Treatment, (ed.) H.B. Crawford and D.N. Fischel, American Water Works Association, pp 541 - 553.

Vinnem, J.E. (1983). Quantitative Risk Analysis in the Design of Offshore Installations. Reliability Engineering, 6 (1), 1 - 12.

Water and Wastewater Operators Chlorination Manual (1977). Alberta Environment, Pollution Control Division, Edmonton, Alberta. 40 p.

Weber, W.J. (1972). Physiochemical Processes for Water Quality Control. John Wiley and Sons, New York. 426 - 442.

White, G.C. (1986). The Handbook of Chlorination. Van Nostrand Reinhold Company, Inc., New York, New York. 1070 p.

APPENDIX A.1

Chlorine Storage and Feed Equipment

Containers

There are three main sizes of chlorine container, 68 kg, 1 tonne and single unit railway cars (ETI, 1984). All of them are intended to contain liquid chlorine under pressure. The liquid chlorine should be between 99.5 to 100% pure to prevent any corrosion, since the tanks are normally made of steel. The choice of container size depends on the average daily consumption. Variations in temperature must be considered and used as a safety factor when choosing how many containers to use.

The smallest industrial-sized container, the 68 kg cylinders, are made of seamless steel construction. They are used in smaller installations and provide only gas chlorination. The name of the cylinder (68 kg) indicates the quantity of chlorine the cylinder contains.

The next size of container is a one tonne cylinder normally referred to as a tonner. Tonners are welded steel tanks that can provide as the name suggests, one tonne or 1000 kg of chlorine. These tonners differ from the smaller-sized cylinders because they are capable of providing either liquid or gaseous chlorine. Figure A.1 represents the construction of a tonner. They have a length of approximately 2 m and a diameter of 0.762 m. The ends are normally concave, and the edges are specially crimped to facilitate lifting (Operator Training Manual, 1984). At one

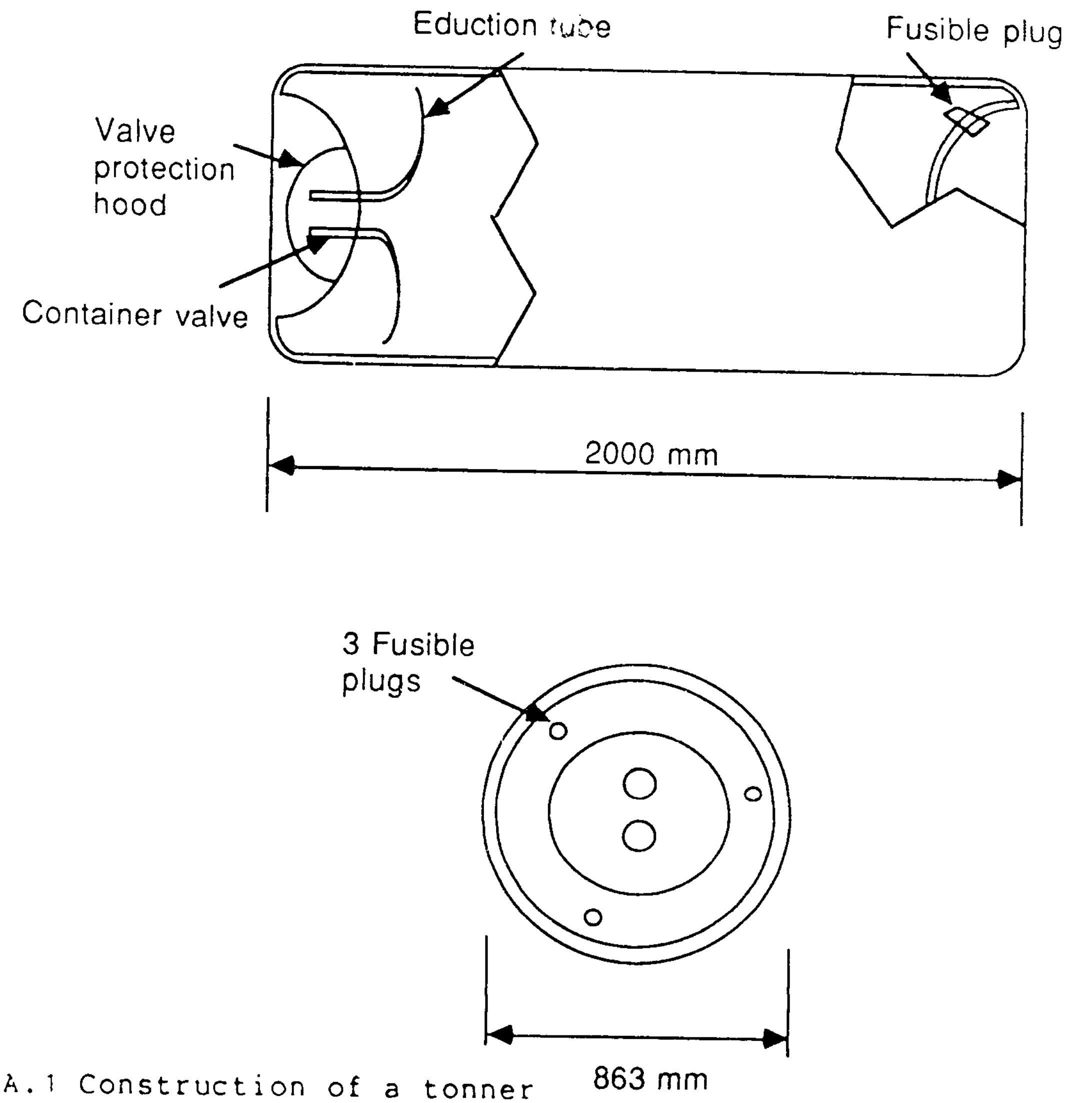


Figure A.1 Construction of a tonner

end of the tonner there are two identical valves which are opened with a wrench. These valves are each connected to an eduction tube. When the valves are aligned vertically, one eduction tube will draw gas, and another will draw liquid. Both ends also have three evenly spaced fusible plugs which are designed to melt at 70°C (ETI, 1984).

The particular municipal plant which has been reviewed uses a gas withdrawal from five one tonne containers. At 20°C and a maximum capacity of 180 kg/day per tonner, this system has a maximum capacity of 900 kg/day.

Transporting and Unloading

The one ton containers are transported by specifically designed trucks. The trucks have properly sized support cradles which prevent any movement of the tonners. A steel protective hood that fits over the valves should always be in place when the tonners are not in use (Whit 986).

Because of the much larger weight of the tonners, much more sophisticated loading and unloading equipment is required (White, 1986). The tonners are unloaded via a monorail system which provides a continuous path from one side of the storage room to the other. The I-beam support should be capable of handling the full tonner weight, the electric hoist and lifing bar. The hoist capacity should be 2000 kg to account for the weight of the empty tonner plus the chlorine. Appropriate height and width clearance for the piping, chlorinators, tonners, and the truck bed must be considered when the monorail is positioned within the storage room. Trunnions support the tonner when in position for use. These trunnions which are properly spaced rollers, allow for easy positioning of the tonner valves and should prevent movement of the tonner in the event of collision.

Feed Rate and Injection Control

Because the system which was analysed uses a gas withdrawal from one tonne containers to apply the chlorine, the system used to control feed and injection rates for a gas system shall be the only system described. If this system was found to be inadequate other systems would be considered and reviewed.

Storage Room

In a properly designed chlorine storage room, the area should contain only chlorine equipment and the chlorine tonners. The area should only be accessible from the outside. This helps to confine and contain the chlorine to one particular area in the event of a spill or leak (Mann, 1962). Doors providing access to the area should open to the outside, and have a panic bar on the inside.

The storage room being reviewed is a reasonably well organized room (Fig. 6.3). The room is actually a separate building which shares two walls with the main plant. There is not a direct access route to the room except from outside doors. The chlorine tonners and chlorinators are both located within the room. The only part requiring comment is the location of the monorail. When full tonners are moved from the east storage platform to the west header bank, the tonners are move northward around the semicircle track. When this maneuver is being performed there is approximately 20 to 30 mm clearance between the edge of the tonner and the piping (headers). As it passes the chlorinator, the tonner must be held parallel since there is not enough room for the tonner to pass.

Proper ventilation within the storage room is essential. Exhaust fans with intakes at floor level should be powerful enough to exchange the volume of air in the room within 2 to 3 min. To prevent a negative pressure within the room, louvres above the doorways should also be provided (Mann, 1962). This storage room has two large exhaust fans with four flumes of dimensions 600 by 600 mm extended to just above floor level. Two are located in each corner of the north end of the building, and there is one halfway along the length of the building on each side. The combined capacity of the two fans is 600 L/s which can theoretically provide a complete air exchange in 3.25 min. Louvres are located above both doorways.

An adequate heating system is particularly important in a northern community. The heating unit should be able to maintain the storage room at 20°C. The effects of the environmental temperature and the loss of heat from vaporization must both be considered. Heaters, windows and the piping layout should be reviewed, so that efficiency in heating is maintained, liquefaction of the gaseous chlorine is avoided and piping is not overheated (Hjalmar, 1978).

The present layout of piping, tonners and chlorinators is relatively efficient, but there are trouble spots. Large folding doors providing loading and unloading access are a major loss of heat. Piping passes near an access door which could create problems in the winter. The storage room has two walls 15.8 m by 5.8 m and a roof 9 m by 15.8 m which are exposed to outside temperatures. Heating has been a problem for this large area, but in November of 1987, a new natural gas heater and two new water unit heaters were installed. The unit heaters are to reduce the impact of opening the main doors when new chlorine tonners must be unloaded. There are also five small thermostatically controlled space heaters, which are only required on very cold days or if one of the other units fail.

Piping

The chemical and physical properties of chlorine dictate the piping material. Dry chlorine in the liquid or gas form is does not corrode ferrous metals, so that seamless carbon steel is recommended. If the chlorine does become moist however, it will readily attack ferrous metals. Therefore, prior to use, it is important that any steel sections exposed to chlorine be adequately dried. After the chlorinators, there is a relatively small chance of liquid chlorine passing into the piping, however there is a much higher chance of the piping being flooded with water. If steel was used between the chlorinators and the eductors, the piping would quickly corrode, so PVC piping is used. Aqueous solutions of chlorine do not attack PVC, even though liquid chlorine will (White, 1986; ETSI, 1984). This type of piping layout is used by the facility being reviewed.

A flexible connection is used between the tonner and the rigid steel piping system, since it must be attached and detached frequently. Either flexible Monel hose or copper tubing can be used for this connection. The plant under review uses a copper alloy tubing.

Valves and Pressure Guages

While the valving set up for this chlorine feed unit is not overly complex, it has been developed so that in the event of a spill, leak or plugged line, the appropriate isolation can be achieved, so that chlorination of the water would not be interrupted. The valves located in the steel section of the piping are mostly needle valves. Where the PVC piping begins, ball valves are used. Pressure gauges are also installed on the steel lines. These gauges are corrosion resistant, diaphragm protected, with the diaphragms being constructed from silver or tantalum (White, 1986).

Most joints within the piping system are welded. This connection is definitely preferred, but where a threaded joint must be used, it is important that the clean, sharp threads are used to ensure a pressure tight joint (ETSI, 1984).

Chlorinators

The chlorinators which are presently used are Wallace and Tiernan's v-notch manual control chlorinators. Remote vacuum type injection is used to diffuse the chlorine into the carrier water which is ultimately applied to the drinking water. These chlorinators have slowly developed through trial and error, but this has resulted in instruments which provide practical and safe operation for a particularly hazardous chemical.

The chlorinator consists of two pressure regulating valves with the unit itself, and a remote injection unit (Fig. A.2). The chlorine gas enters the chlorinator under pressure. Initially, the gas enters the gas pressure regulating valve which is a diaphragm valve. As the vacuum is applied, the diaphragm is sucked in causing the attached spring to contract and allowing the chlorine gas to bypass the valve. After this valve, the gas is no longer under pressure, but is maintained at a constant negative pressure. The gas then passes through a rotameter, which provides a visual indicator of the gas flow rate for the operator. This flow rate can be manually adjusted through a v-notch variable orifice. When the gas passes the orifice it goes through a vacuum regulating valve which maintains the constant negative pressure at tne orifice. Should the vacuum at the injector be eliminated, this valve does not close, but is actually fully open. This valve prevents an excessive vacuum being applied. This unit is also attached to another diaphragm valve which acts as a pressure and vacuum relief valve. At a vacuum of 900 to 1000 mm of water, the diaphragm will be opened to the vent, and air will be sucked into the system. If the vacuum has been stopped, but the chlorine gas continues to flow, the pressure relief valve will be opened. At 25 to 50 mm water pressure the diaphragm will be opened to the vent, releasing the chlorine gas. The loss of vacuum should close the initial gas pressure regulating valve, so this relief vent would only be activated in the event that the regulating valve was stuck open.

Once the gas leaves the chlorinator it travels under vacuum to the injection room. This line has a manual shut off valve and a check valve which should close under a no vacuum condition. The injector the vacuum by passage of a water supply. Another diaphragm valve is opened by the application of the vacuum, allowing the vacuum to be transmitted back to the chlorinator, causing the chlorine gas to pass. The size of the injector is regulated by the quantity of chlorine to be fed since there is limited solubility of the chlorine gas in the water. The limiting concentration under this vacuum condition is 3500 mg/L. Above this concentration the solution which should be a mix of hypochlorous acid (HOCl) and molecular chlorine (Cl_2) has

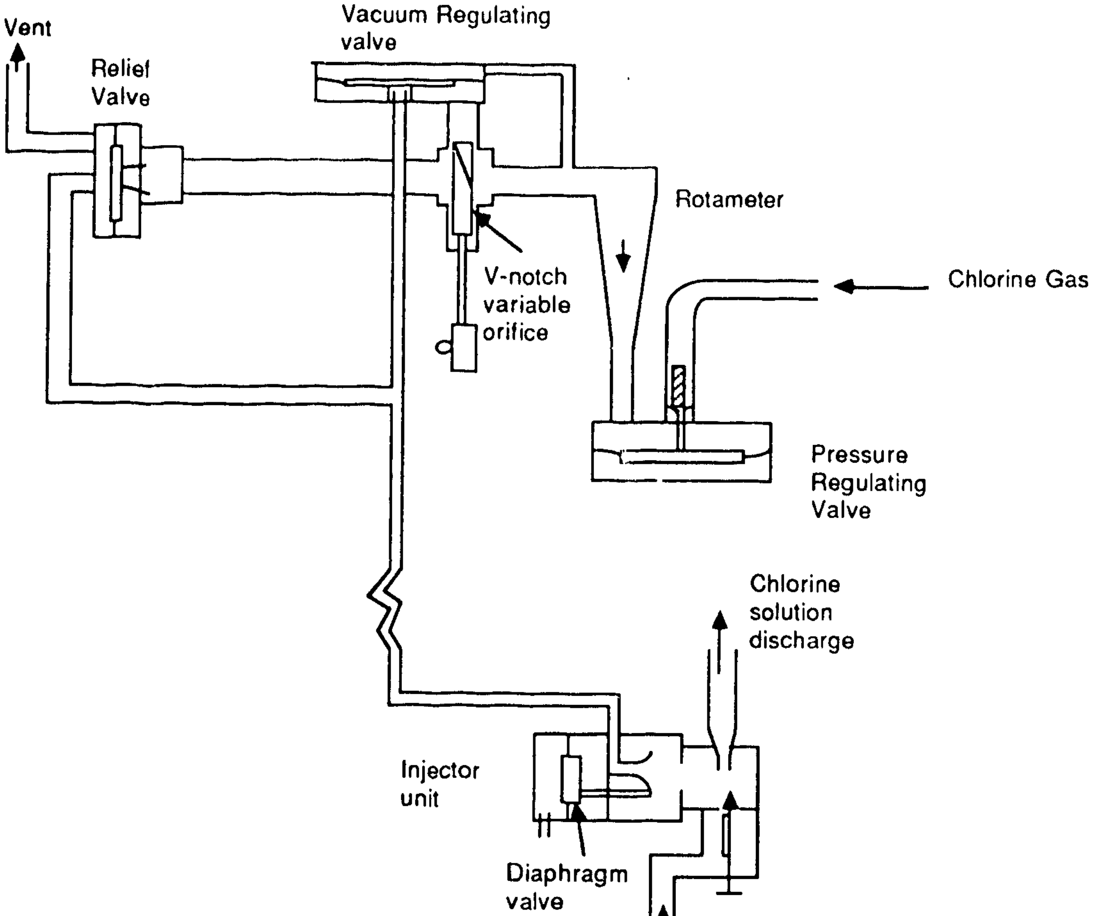


Figure A.2 Construction of a chlorinator

an excess quantity of (Cl_2) which will come out of solution at the application point. Approximately 70 L of water are required per kg of chlorine per day (White, 1986).

This type of vacuum injection chlorination system is extremely advantageous. Not only is the chlorine easier to handle in the aqueous form, this method is the most effective way of dissolving chlorine in water. The application of the vacuum not only provides an accurate method for measuring the chlorine flow, but also offers a much safer mechanism for transporting the chlorine. A break in the vacuum line only causes air to be sucked in rather than having chlorine gas pouring out as in a pressure line.

The Role of the Operator

The facility which is being reviewed, relies heavily on manual actions and reactions to effectively monitor and control the chlorination procedure. The operator is involved in unloading tonners, connecting and disconnecting tonners, adjustment of line valving for correct feed locations, monitoring of water to determine feed rates, and then the adjustment of flow rates on the chlorinator to maintain the correct residual. They are also responsible for responding to and correcting any of the alarms which may be activated. When this type of situation occurs, all personal normally check with the shift foreman to determine if their response is required.

Alarms

The importance of chlorine as a disinfectant in the treatment process and the xtreme corrosivity and toxicity it possesses are both reflected in the number of alarm systems this feed unit contains.

Leak Alarm

To reduce the hazard posed by its toxicity, the storage room has two independent leak detectors. These detector's sensors are placed near floor level and set to alarm at 1 ppm, so that even the smallest leak is detected. The alarms are tested once per week to ensure they are working properly. When the alarm is set off, an audible alarm sounds with the storage room and within the distribution or control room. A red light above the doorway flashes on and off. The ventilation system is automatically activated if it is set locally on automatic. There are not any automatic shut downs or isolations on the chlorinators, eductors or tonners when this alarm is activated.

Low Pressure Alarm

This alarm is used as an operational tool for the verification of readings the operator should have been taking. The alarm is attached to both header systems running from the tonner banks to the chlorinators As the tonner bank empties, the pressure will begin to fall and at 25 kPa or less the alarm sounds. Normally the operator is expecting the alarm since he would have been monitoring the scales which indicate the tonner weights. As standard operating procedure the operator normally waits until the alarm sounds before switching over to the alternate tonner bank. If this alarm sounds unexpectedly, the operator is immediately aware of some type of deviation in the system, whether its a faulty alarm or a plugged line. The alarm is activated only in the control room and is only a flashing panel light without an audible alarm. The alarm can be switched off by having it set on the alternate tonner bank.

High/Low Vacuum Alarm

This alarm signifies problems with the chlorinator or injection system. If one of [illegible] valves immediately preceding the chlorinator were to plug, [illegible] excess vacuum would develop which sounds the alarm. Should the injector or some other section become fouled reducing or eliminating the vacuum the low vacuum alarm sounds.

These alarms are dealt with together because they are activated on the same flashing light panel on an alarm board. The other three chlorinators do not have this alarm. Both the flashing panel light and an audible alarm are sounded. The audible alarm is the same alarm used for a chlorine leak, however upon investigation it would be apparent which alarm had been activated. The audible alarm in the storage room is not activated, which provides an additional verification as to which alarm has been activated.

APPENDIX B.1

Liquid Chlorine in the Headers

Demand Greater than Supply

The demand rate will exceed the supply rate, if one or more of the valves is plugged and the chlorine requirement is greater than the number of tonners available.

One or More Valves Plugged

The cause of a plugged tonner valve would be from the corrosion of the tonner and the valve allowing particles to jam the valve. After each shipment is returned the valves are carefully inspected for signs of corrosion and wear. When there are less that five full threads showing on the valve or if there are obvious nicks or cuts, the valve should be replaced (Chlorine Inst., 1980). There was not any generic information available on either the failure rates of these valves or on their replacement rate. The packaging company follows strict inspection guidelines to ensure the tonners are in adequate condition (Chlorine Inst., 1980). The inspection team would have to miss a damaged valve for a deteriorated valve to pass. This event is similar to a failed eductor. An error rate of 1 in 1000 (0.001) with a standard deviation of 0.00075 was used for a normal prior distribution.

A binomial distribution using plant specific information was used to update the prior. The operations personnel estimate that one tonner per year would have a plugged valve. The facility uses approximately 170 tonners per year. Using the binomial distribution and Bayes theorem, the prior was updated giving the posterior distribution shown in Figure B.1.1.

The tonners are shipped out individually. This is important for the independence of the event. If a certain group of tonners was always kept together during cleaning and testing, the probability of more than one tonner valve being plugged in the tonner bank would be higher. Because the probability of a plugged tonner valve is an independent event, the probability of occurrence for more than one plugged tonner valve, was found by multiplying the probability of each independent event together.

Demand Greater Than Available Tonners

When one or more tonner valves plug liquid chlorine does not necessarily enter the headers. The demand rate must exceed the available supply causing the chlorine to flow at a high rate. The chlorine then liquefys in the chlorinator and at the flexible connectors. This is a result of the high rate of evaporation required to meet the demand. After a short time, the heat transfer required for vaporization would not be able to keep pace with the evaporation rate. This reduction in temperature, causes the liquefaction of the chlorine. It initially would appear as frost on the flexible connectors and the glass tubing in the rotameters.

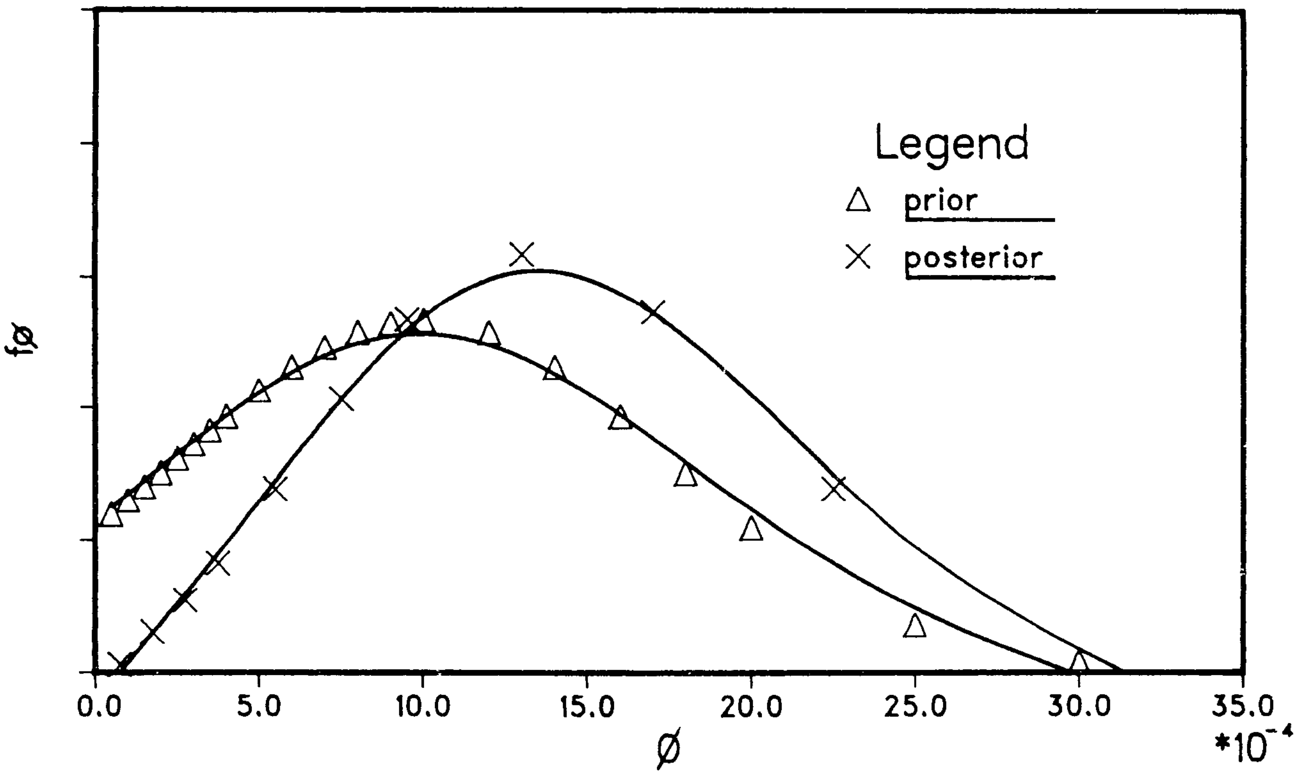


Figure B.1.1 Probability distribution for one tonner valveplugged

The demand rate is a function of pumpage. The chlorine dose usually varies between 2 and 3 mg/L depending on the demand rate within the water. It is only on those days of very high demand that all five tonners would be required (Annual Report, 1985, 1986). For much of the year, three or four tonners is normally adequate. Knowing the capacity of the five tonners, the pumpage would never be increased passed the point where adequate disinfection could be provided. Even at the peak capacity for both plants, which is equivalent to 290 ML per day, the five tonners, at 20°C could provide chlorine at a rate of 3.1 mg/L.

The available chlorine from two, three, four and five tonners can also be calculated. These availabilities were then compared with the average demand rate over a year. Four tonners can provide 30 kg/hr given that each tonner is supplying 7.5 kg/hr assuming an air temperature of 20°C. At higher temperatures more chlorine would be available, however the storage room is normally maintained within a few degrees of 20°C even in the summer.

Reviewing the annual reports, there were on average two days out of the year when the demand would be greater than 30 kg/hr (Annual Report, 1986). There was some variation to this number which over the last four years, has gone from one to three days when demand was greater than four tonners.

A normal distribution was used to represent the uncertainty in the average demand of two days. Since the data base only covered four years, the variance in the numbers were used as the standard deviation. This ensures that 66% of the time a demand of greater than four tonners would occur between one and three days out of the year. For this distribution the prior was not updated (Fig. B.1.2). Generic data does not exist for this type of information.

The same type of analysis was performed for the other feed rates. For two tonner valves plugged, the demand only needs to be greater than three tonners or 22.5 kg/hr. This is an adequate feed rate for a plant flow rate of approximately 180 ML per day. During the year, the plant flow rate is greater than 180 ML per day for approximately one month per year (Table B.1.1). A normal distribution with a mean of 30 days per annum was used for this event since there was excellent correlation for the data. A standard deviation of 15 days per annum was used (Fig. B.1.3).

For the scenario of having three tonners plugged, there would be a supply of 15 kg/hr which can supply enough chlorine for a flow rate of 120 ML per day.

Table B.1.1. Plants 1 and 2 combined flow rates in ML per day.
(Annual Reports, 1985, 1986)

Month	1986	1985
Jan	124	147
Feb	117	141
Mar	135	155
Apr	119	143
May	139	147
Jun	170	132
Jul	133	187
Aug	180	141
Sep	119	123
Oct	119	120
Nov	123	112
Dec	150	115

For most of the year, except during one of the plant shutdowns, this is the minimun plant flow rate (Table 5.1). Therefore if three valves plugged, the demand rate at any time during the year would be great enough so that a freezing of the system would occur.

Frequency of Demand Greater than Supply

The logic diagram lo liquid chlorine in the headers (Fig. 7.9), combines the event of a tonner valve plugging and the demand being greater than the supply with a logical 'AND' gate. Plant specific data can then be used to update the event of the lines freezing. From operational experience, the plugging of one valve has never caused the headers to freeze. However, there was one event during the 40 years of operation where the lines did freeze because of the scenario when two valves were plugged. The event of three valves causing the lines to freeze has never happened.

A binomial distribution was used. The N value in the equation varies from that used in the updating of one tonner valve being plugged. In one year approximately 170 tonners are used. If five tonners are used at one time, there are 35 'banks' of tonners per year. It is within that bank that there may be one or more valves plugged. Over forty years, 1400 banks of tonners are used. The event of one valve plugging and causing freezing has not occurred so the K value is 0. Two valves plugging has caused freezing once, therefore the K value is 1. The event of three valves

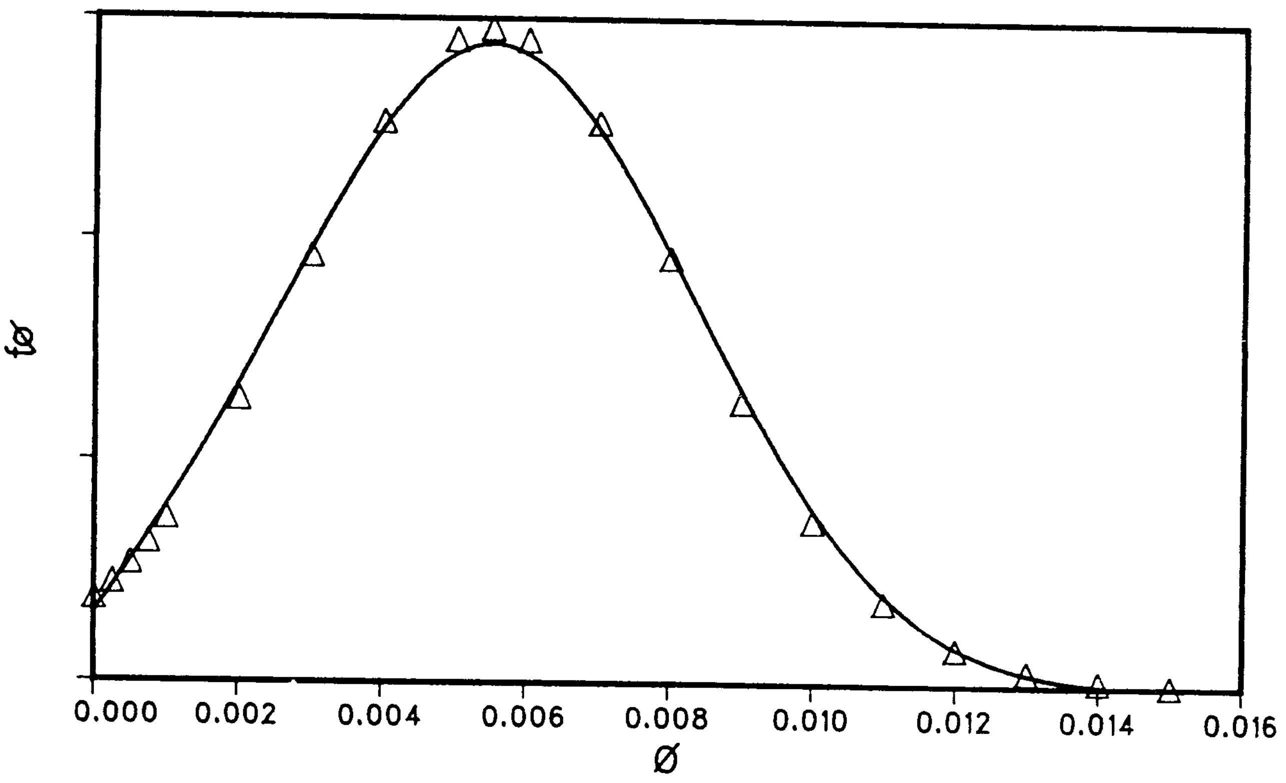


Figure B.1.2 Probability distribution for the chlorine demand greater than four tonners

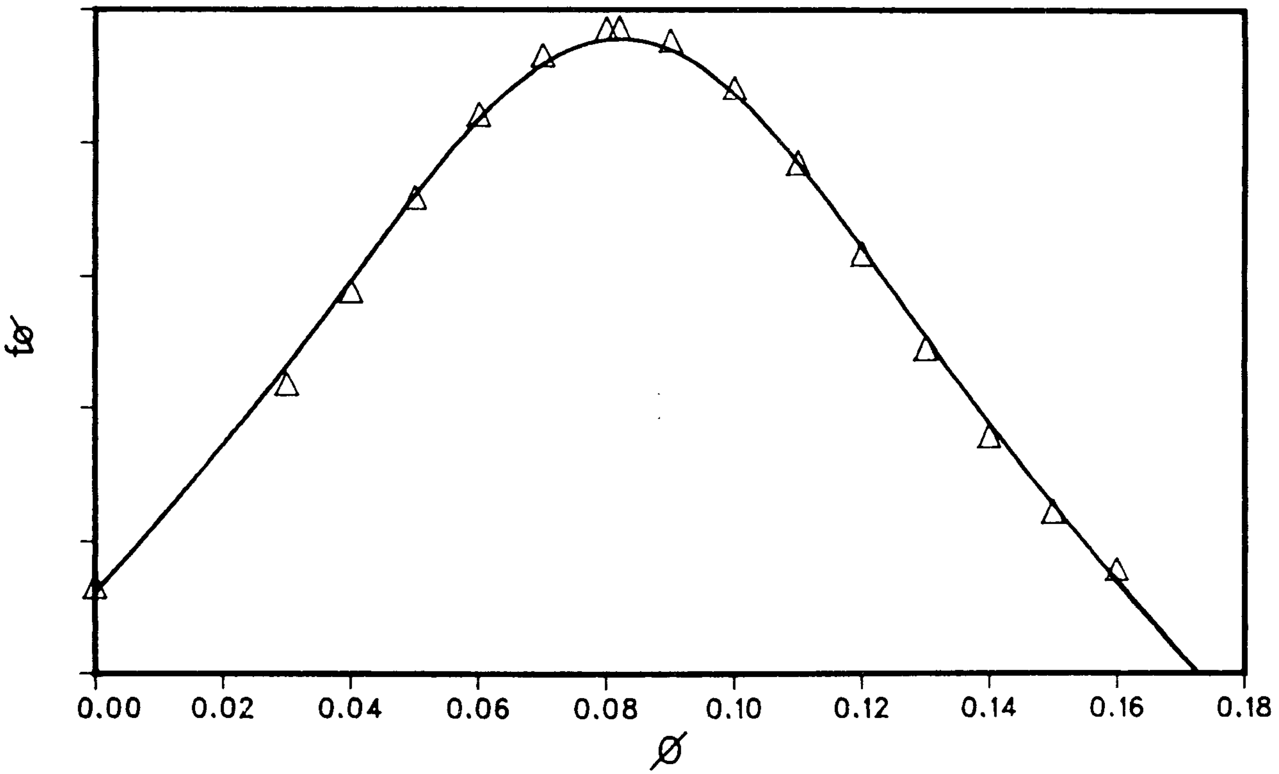


Figure B.1.3 Probability distribution for the chlorine demand greater than three tonners

plugging resulting in liquid chlorine in the headers has never happened, so K is 0. By applying Bayes Theorem the final updated, posterior distribution for each event has been found.

Loss of Heat

Loss of heat in the storage room would be created by the failure of three sets of heating systems, or by failure of the 2 main heating units and the temperature drops to below -17°C.

Direct Fired Gas Heater

This heater was installed and became operational in December, 1987. The unit is a natural gas, direct fired heater with a heating output of 109 kW. It has an air supply of 1723 L/s which is distributed through six vent ducts. The main duct (600 x 400 mm) travels the length of the storage room.

Water Heater

To supplement the main heater, two new hot water heaters located at the south end of the building near the main access doors for unloading tonners are used to supplement the main heater.

Electric Fans

There are five wall mounted electric heaters which operate as air circulators and local heaters. These units are intended to prevent a critical drop in temperature in the storage room should the other units fail. They have been found to be effective up to -17°C.

Temperature

The local conditions for this northern community are quite variable from summer to winter. The mean maximum and minumum temperatures as well as the extreme maximum and minimum temperatures are indicated in Table B.1.2. These values are the averages over ten years (Env. Canada, 1975). Since chlorination must continue, regardless of the temperature, it is critical that the heating unit be able to maintain at least 10 to 15°C within the storage room even during the minimum temperatures.

There was not any generic information on the failure rates of these units. Using the procedure established for this situation, a uniform distribution was used for the prior. The prior was updated with the limited operating information available through a poisson distribution. The K value was 0 since there have not been any failures of the unit and the T value was 180 days. This same distribution was used for all three units.

The distributions could then be placed into the fault tree (Fig. 7.9). They were combined through logial AND gates.

Table B.1.2. Extreme minimum and mean temperatures for Edmonton.
(Environment Canada, 1975)

Month	Mean Minimum	Extreme Minimum
Jan	-19.4	-44
Feb	-15.5	-46.1
Mar	-10.3	-36.1
Apr	-1.6	-25.6
May	4.7	-12.2
Jun	8.9	-1.11
Jul	11.5	0.6
Aug	10.1	0.6
Sep	5.0	-11.7
Oct	-.22	-25.0
Nov	-8.4	-32.8
Dec	-15.0	-48.3

The frequencv of the drop in temperature below -17 °C was included with the small space heaters since they are unable to maintain adequate heat above this temperature. An OR gate was used for the loss of the space heaters or the drop temperature since either event represents a failed situation.

Eductor Broken in Tonner

This event was fully developed in section B.3.1.

Three Valves Left Open

If this scenario occurred the headers would fill with liquid chlorine, and chlorination would cease. The event of leaving the three valves open would create such a pressure difference that gaseous chlorine would flow rapidly to the empty tonners, causing the chlorine to liquefy. To understand the development of the probability for this action, a review of the changeover process is required. Referring to Figure 7.5, the series of events which precede the valve switches are indicated. When the low pressure alarm sounds, the operator is aware that the banks need switching. Prior to switching, the feed rate is boosted slightly to compensate for the one or two min that the system will be without chlorine. Once the pressure gauge (Fig. 6.1) goes to zero, the operator begins to close valves. Starting at the tonners, the operator closes the tonner valves . Some operators crack this valve open briefly to air purge the line. The header valves and finally the isolation valve for the entire header are then closed. The chlorinators v-notch orifice should be closed to prevent the rotameter ball from flipping from a sudden pressure surge when the new bank is accessed. The operator can now begin to open the set of tonner valves on the full bank. The new bank will have been connected to the flexible connectors during the tonner change.

For this scenario to occur, the operator, once having emptied the line would have to immediately go and open the other bank. During this time he must open three valves and remain oblivious to his error. The prediction of the human failure rate depends on the type of error. This error could be due to a moments abberation. These types of errors are usually created from a well trained automated response. The switching of tonner banks is performed only 34 times per year which is less than once per week. Because of the rotating shifts, an operator may not have to perform this task for up to six months. Therefore the operator must think about what he is doing rather than shifting into automatic. In addition, this procedure is always performed by two operators. They can check each other which reduces the chance of a mistake.

From these facts it appears that such an error should not occur from familiarity but would be caused by a lack of training. However as part of a questionnaire, the staff were asked to critically consider their competence in having to perform the task. All were extremely confident that they could do so without any mishaps or difficulty.

Another possible explanation for such an event could be from the operator being called away during the change. This possibility is extremely unlikely since during this brief interval, the water is not being chlorinated. There is the utmost urgency that the switch should be done quickly and efficiently, to continue chlorinating.

In Table 2.4, an operator action which is routine but requires care would have an error rate of 1 in 100. Because this event is precipitated by the low pressure alarm, it may also be considered to be an operator intervention. When the alarm is one which the operator has been instructed to watch and there is less than 5 min to react, the error rate is about 10 to 25% (Table 2.5). This latter information is for a process plant where the sounding of an alarm, and failure to correctly respond to that alarm, may create an explosion. There is a definite threat to the plant and personnel.

When the low pressure alarm sounds, it is normally a verification of information for the operator. There would probably be more stress if the alarm did not sound. The effect of no response would be the loss of chlorination, and while the operator realizes that this situation must be prevented, their stress level is less than when bodily harm may be involved.

When stress level, frequency of the action, consequences to the operator if there was no action and the use of pairs are all considered, the error rate drops to 1 in 1000 or 1 in 10,000. A log normal distribution shall be used for the prior distribution. The error rate per operation varied from a 5 % of 10^{-6} to a 95 % of 10^{-2}. A binomial distribution can be used to update the value, with an incidence value K equal to 0 and the number of events N equal to 1360 (Fig. B.1.4). The posterior distribution's mean value was then entered into the liquid chlorine in headers fault tree (Fig. 7.9).

Pigtail Attached to Wrong Valve

This event can also be attributed to human error, however the circumstances affecting the likelihood of this event are much different than those for the preceding event. The reconnection of flexible connector follows the unloading of empty tonners from the tonner scale, and reloading of full tonners. While the tonners are being moved about, the operators experience a relatively high level of stress, particularly when the tonners are moved on the inside semicircle portion of the overhead track during winter. The tonners pass precariously close to headers and chlorinators when on this portion of the track.

Several of the staff take special precautions during such maneuvers. These include, turning on the automatic ventilation fans, leaving one door open, planning an escaped route with their partner, breathing out when disconnecting a flexible connector and checking all connections with ammonia

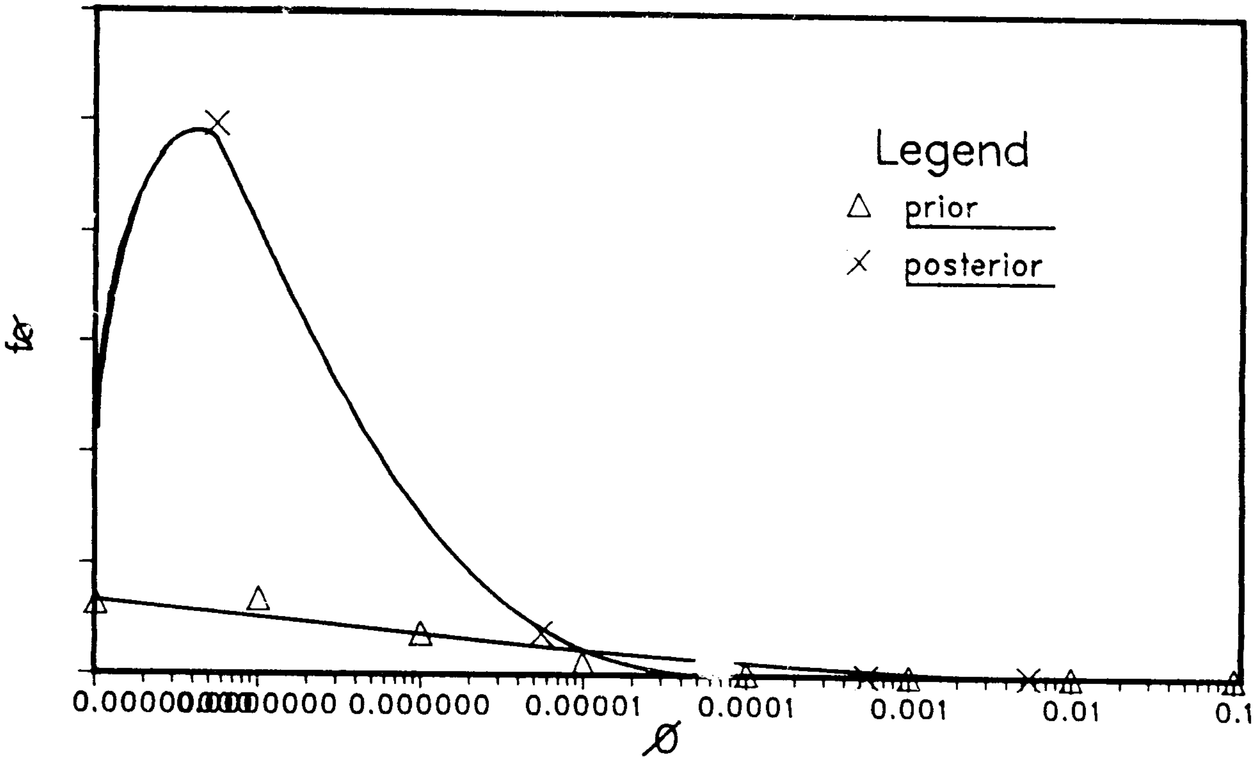


Figure B.1.4 Probability of an operator leaving three valves open during tonner change

to ensure tight seals. The latter two techniques deal solely with the connection aspect of the task.

These precautions suggest that, there is a high level of awareness about the possible dangers of the task. However, connecting the flexible connector to the wrong valve could happen even when great care is taken, because once the connection is made some of the stress is gone, the danger has been partly removed. As the five connections are made, it would be possible for the operator to have a momentary loss of concentration.

This task is normally performed by the day shift operators. This can create some familiarity with the task which increases the chance of error. Combining these factors, the error rate for this task could be expected to be between 1 in 100 and 1 in 1000.

Because of the uncertainty involved in this type of human action, the error rate will be described by a log normal distribution. The 5 % will be 10^{-5} and the 95 % 10^{-1} (Fig. B.1.5).

The incorrect attachment of the flexible connector does not result in liquid chlorine in the headers. There is a different operator who accesses the chlorine tonner to put it on line. When the tonner banks are switched from the empty side to the full side, the operator usually rechecks all connections with ammonia to ensure they are tight. The operator is under a higher stress level during the changing of tonner banks because chlorination has stopped during this time. This higher stress level could increase his awareness causing him to notice the incorrect attachment, or perhaps in his rush to continue chlorination would bypass the error.

The uncertainty which exists for this event has been expressed with a log normal distribution. A wide range for the 5 and 95 % were chosen, being 10^{-6} and 10^{-1} respectively.

Practical plant experience with this event can be used to update the combined effect of these two events. The final event of liquid chlorine in the headers from the incorrect connection of the valves has never occurred. Therefore a binomial distribution with an incidence value of K equal to 0 and event value of N equal to 1700 was used to update the combined distribution.

Expected Probability of Liquid Chlorine in Headers

The fault tree Figure 7.9 shows, the sequence of events which can result in liquid chlorine in the headers. All of the elemental events have had their probability of occurrence calculated. These probabilities can now be combined through logical 'OR' gates since any one of the events can create the damage state of liquid chlorine in the lines. This final probability can now be considered in the general fault tree which has the damage state of injury.

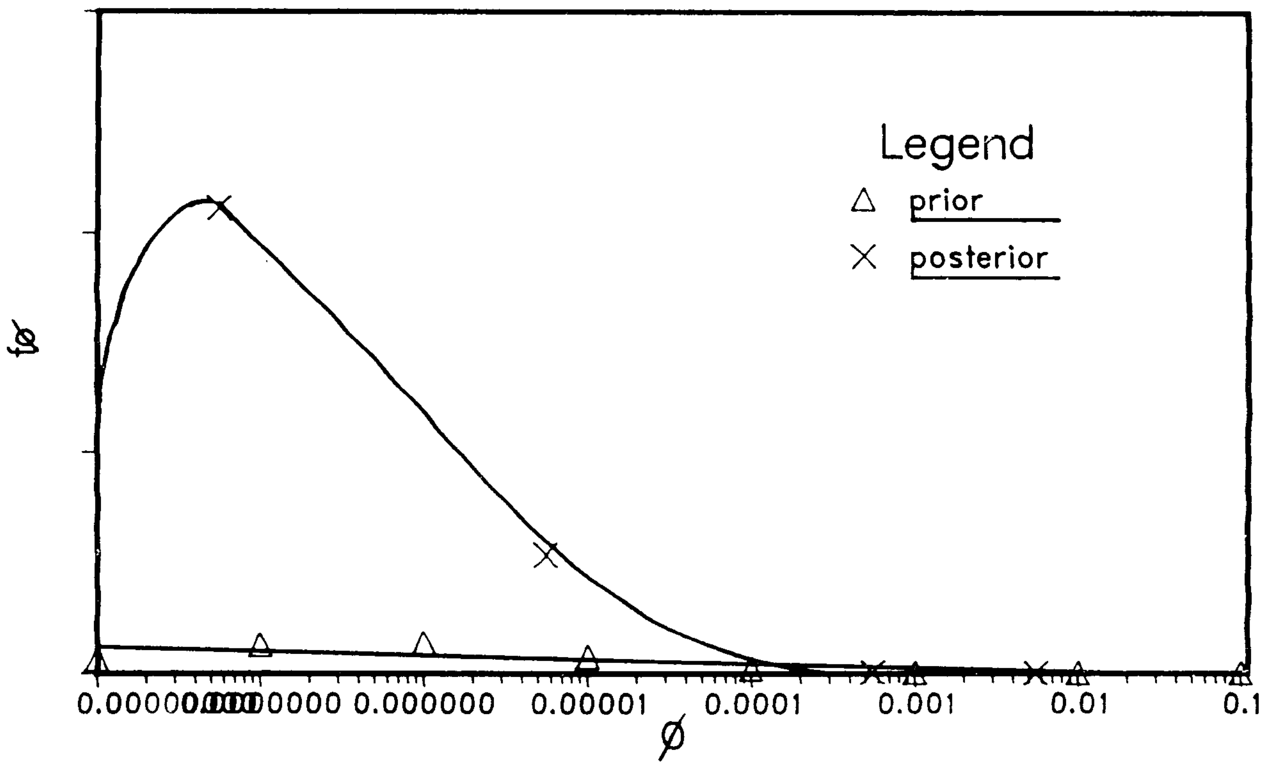


Figure B.1.5 Probability of an operator connecting the flexible connector to the wrong valve

APPENDIX B.2

Handling Liquid Chlorine in the Headers

Cleaning with Alcohol

The headers must be cleaned is they have been exposed to liquid chlorine. A solvent capable of removing the corrosion products of the chlorine and any residual chlorine compounds should be used. The solvents which are recommended for use are trichloroethylene (Hjalmar, 1978) and carbon tetrachloride (Mann, 1962). Alcohol will remove the corrosion products, but this solvent is not recommended under any circumstances, because of the explosive reaction which can occur between chlorine and alcohol (Vaughn et al., 1971).

The maintenance personnel were questioned about their cleaning techniques. They indicated that alcohol was used on a routine basis rather than the other suggested solvents. They chose alcohol over the other solvents because there has been experimental evidence of both trichloroethylene and carbon tetrachloride causing cancer in mice.

Under most circumstances, there would not be any chlorine remaining in the lines only ferric chloride. There could be a reaction between the alcohol and chlorine when the system was exposed to the chlorine gas if alcohol was remaining in the headers.

The chlorine gas would be at room temperature but reasonably high pressure due to the new series of tonners being opened (240 kPa). The possibility of an explosion exists, but there is a high degree of uncertainty about the value of the probability of occurrence. Therefore, a uniform distribution was used for the prior. From the maintenance records, cleaning of the chlorinators or piping with alcohol would be done approximately 15 times per year and has been done over the last 10 years. This gives an event occurrence number of 150. Using a binomial distribution with an incidence number K of 0, an event number N of 225, the prior can be updated (Fig. B.2.1).

Concentration High Enough to Injure

Although liquid chlorine may have filled the headers, the system is still stable. The chlorine is contained even though it is under pressure. The total length of carbon steel piping within the storage room is approximately 9.3 m. During chlorination, not all of the headers are in use which reduces the total quantity of pipe to an active number which varies from 2.4 to 2.9 m. The diameter of the piping is 25.4 mm. Therefore in the event that one of these lines was filled with liquid chlorine, the volume would be 1.2 L. However, when the clean up does occur, the entire length of pipe and therefore volume of liquid chlorine is not release at once, but rather the piping is taken in smaller sections between the valves. The longest section would be approximately 1.5 m in length resulting in a volume of 0.76 L (Appendix B.5).

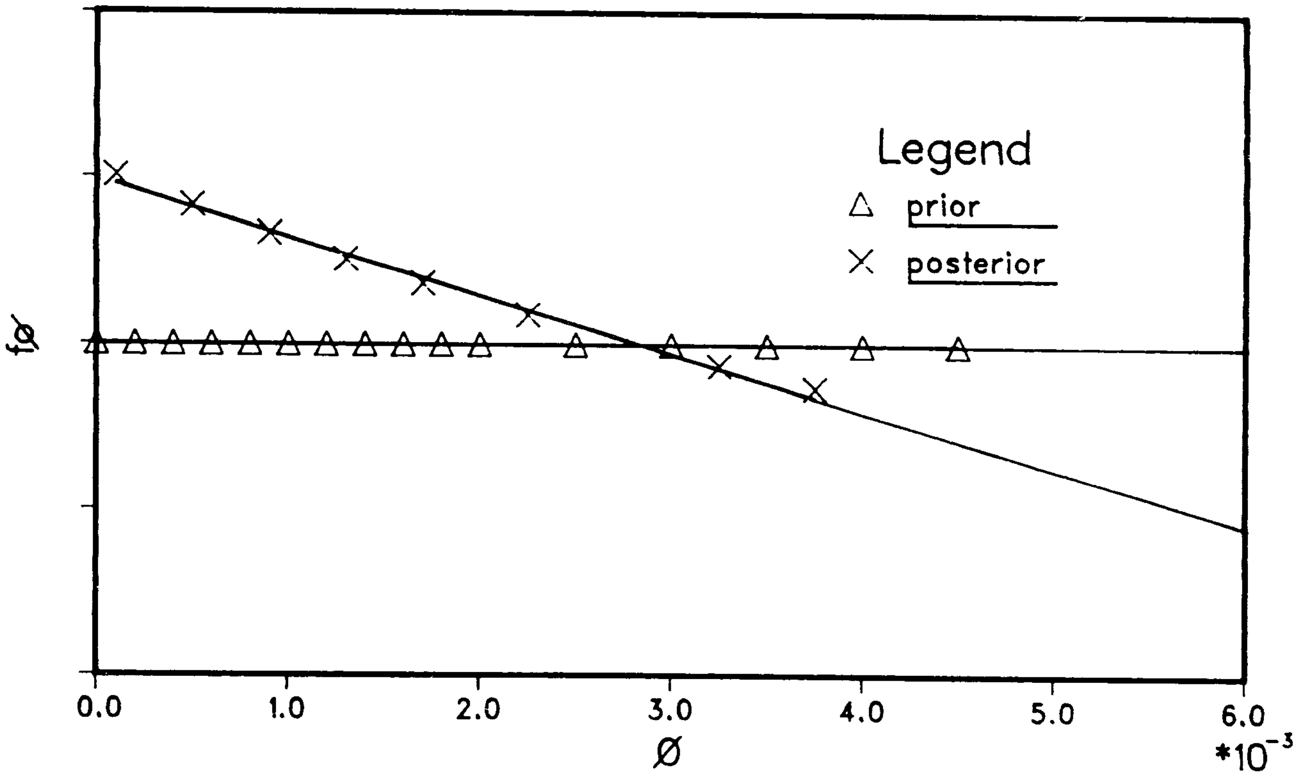


Figure B.2.1 Probability of an explosion from cleaning chlorinators or piping with alcohol

After breaking the pipe into manageable sections, the liquid chlorine is discharged, water is sprayed onto it, and it is removed via the ventilation unit. The application of water would enhance the formation of hydrochloric acid which may corrode the ventilation shaft.

There is no doubt that the release of the gas would affect personnel who were not wearing appropriate breathing apparatus and clothing. This is really a feature of training and awareness. Personnel involved in the release that were not wearing appropriate clothing would soon have severe skin irritation forcing them to leave the area. Breathing apparatus would be essential particularly when water is applied creating the moist chlorine condition.

The interviews with the operators indicated that, they were all very aware of the potential danger which exist with chlorine. All of them had a high degree of respect for the chemical and would consider any situation in which chlorine was involved very seriously. Therefore, providing that the proper warning precautions were taken, it is very unlikely that a person would enter the room without proper clothing or breathing equipment in a controlled release event. During a properly managed controlled release a person would have to be completely ignorant of the potential danger within the release area. This event can be prevented through proper warning signs and and the training of personnel. It has been indicated that the operational personnel have all been trained in the hazards of chlorine. Therefore in this controlled situation, a logarithmic distribution with a 5 % of 10^{-7} and a 95 % of 10^{-4} shall be used. There was not any operational evidence which can be used to update this value (Fig. B.2.2).

Ventilation Inadequate

During the release of the liquid chlorine, the ventilation unit may not remove all of the chlorine. The ventilation unit consists of two ventilation fans. The larger fan is capable of moving 4305 L/s, and the smaller, 1723 L/s. This is a total of approximately 6000 L/s. At this rate, the entire volume of air within the storage room should be changed within 3.25 min. This is certainly within the recommended guidelines given by White (1986).

With any type of exhaust system there are going to be currents and eddies set up which could cause pockets of chlorine to remain. The present unit was recently changed from two exhaust flumes on the north wall to the four flumes. This will improve the thoroughness of the air exchange.

The point at which a worker would consider the area safe enough to remove his mask would depend on how seriously the person viewed the circumstances. As previously indicated all personnel respect the hazards associated with chlorine. This situation is similar to that of the person entering the room without protective clothing. Therefore the same probability distribution will be used to describe this event, which is a log normal distribution with a 5 % of 10^{-7} and a 95 % of 10^{-4}.

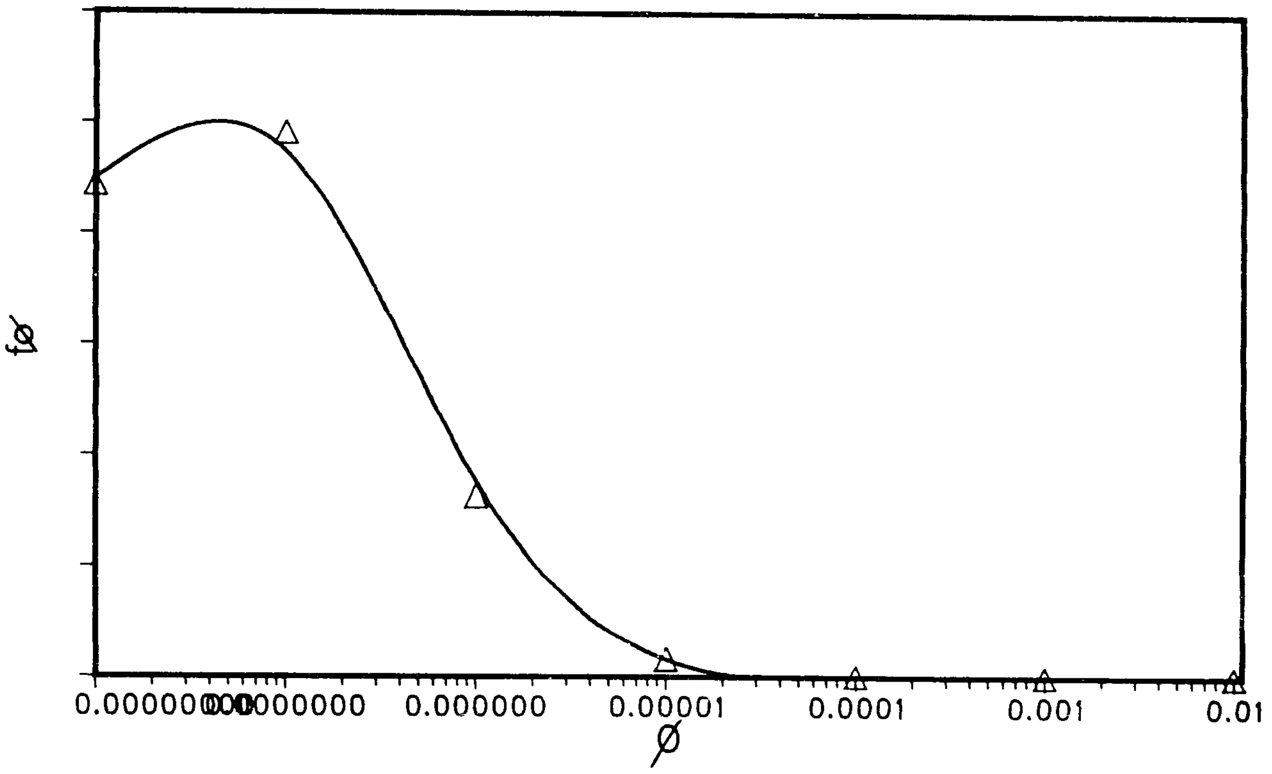


Figure B.2.2 Probability that an operator would expose himself to chlorine during a controlled release

APPENDIX B.3

Eductor Fouled

Loss of Supply Water Pressure

There are two possible explanations for the loss of the water pressure. There may be a loss of water from a pipe breakage, or there may be a large enough demand on the supply line so there is not enough water to create the vacuum.

Pipe Breakage

Generic information on the failure rate of a pipe is very difficult to collect because there are many unique factors affecting the failure rate of a pipe. The operating environment operating pressures, and temperature changes all contribute. For this particular plant, which is relatively old, some sections of piping have been replaced, while some sections remain unchanged. The new pipe, which is PVC, can withstand higher pressures. When there are pressure surges, or simply through wearing out, older sections of the pipe break. This has occurrred twice over the last seven years.

Because there was not any generic data, and there is a high degree of uncertainty as to the actual failure rate of the piping, a uniform prior distribution was used. The uniform prior was updated by a Poisson distribution (Fig. B.3.1).

Too Much Demand

A loss of vacuum would also occur from lack of pressure because of too many demands being placed on the system. Water is required throughout the plant for preparation of chemical slurries and cleaning up spills. There was a problem with the lack of injector water however three years ago a new 150 mm line was attached to a main water pipe which provided a constant and steady supply source. Now the only mechanism by which there would be a lack of water from this cause would be from a plant shut down, in which case the chlorine would not be required. Therefore this scenario was not given a frequency distribution in the fault tree.

Eductor Plugged

The loss of all or part of the vacuum may also be due to the eductor plugging. Impurities may partially clog the diaphragm valve within the eductor or foul up the discharge line. Generic information provided by White (1986) suggests a recommended life span of two years for these valves. This time limit is suggested because of possible impurities which plug the valve, and also from the corrosion which occurs because of the formation of hydrochloric acid as the chlorine passes into the water. The prior distribution was developed from this information by assuming the replacement rate represents a 5% chance of failure. The mean failure rate could then be calculated. A normal distribution with a mean of once every five years and a standard deviation of

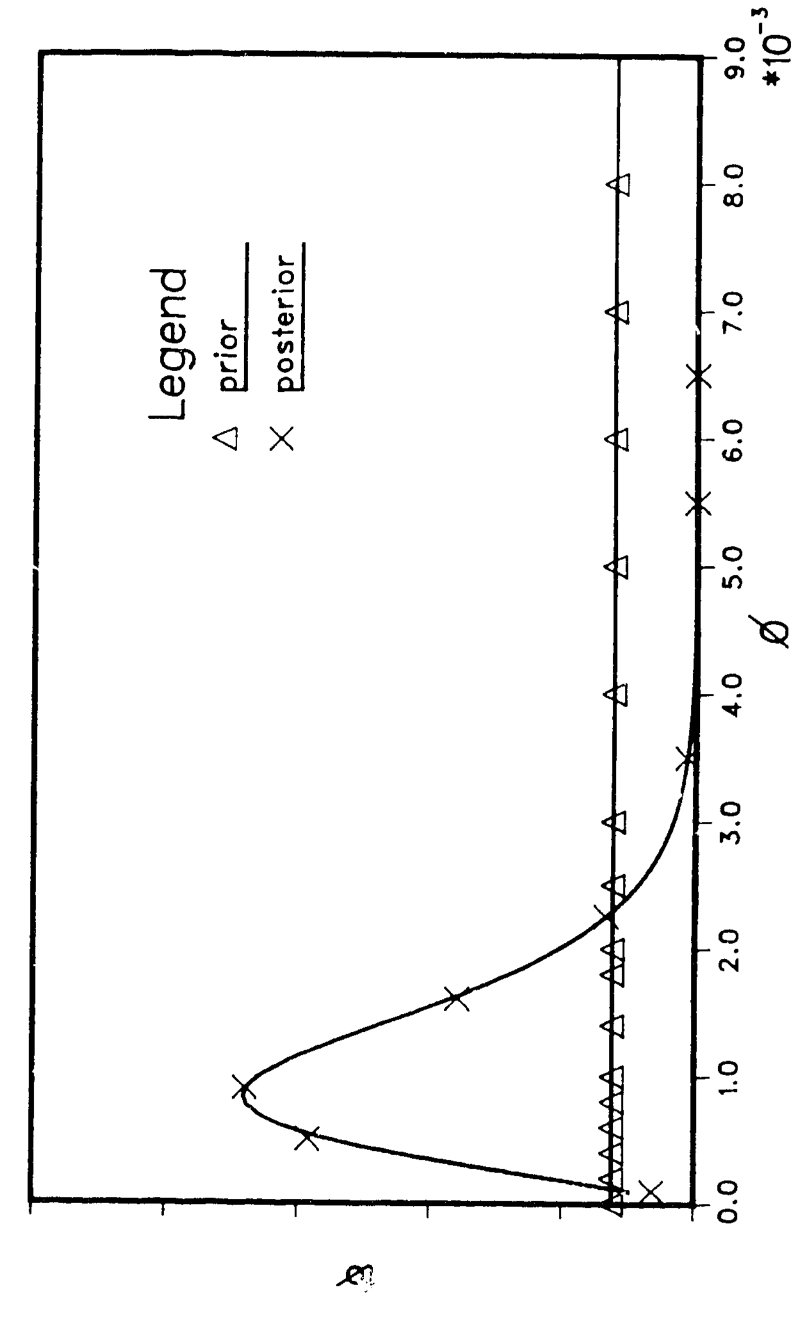


Figure B.3.1 Probability of a water supply line rupture

once every six and a half years was develcped.

From the maintence records kept since 1984 there have been four incidences when fouling of the diaphragm check valve at the eductor caused a loss of vacuum.

Within the records there is not any distinction made between which injectors had caused the problems. Generally, injectors 1 and 2 are used which provide chlorination to the east end of the stilling basins. Therefore, to update the uniform prior distribution, a poisson distribution with an event time of 3 years and an incidence of 2 shall be used. The error rate was considered to be equal for both eductors (Fig. B.3.2).

Discharge Plugged

A uniform distribution was used for the prior. This event has not occurred during the last three years. Therefore, a poisson distribution will be used to update the prior, only the incidence rate will be 0 for an event time of 3 years (Fig. B.3.3).

Improper Isolation

The chlorine system should automatically stabilize when there is the total loss or partial loss of vacuum. Within the chlorinator the pressure regulating valve should close stabilizing the chlorine gas supply. The vacuum section of piping should be isolated by closure of the check valve in the line and closure of the diaphragm check valve at the

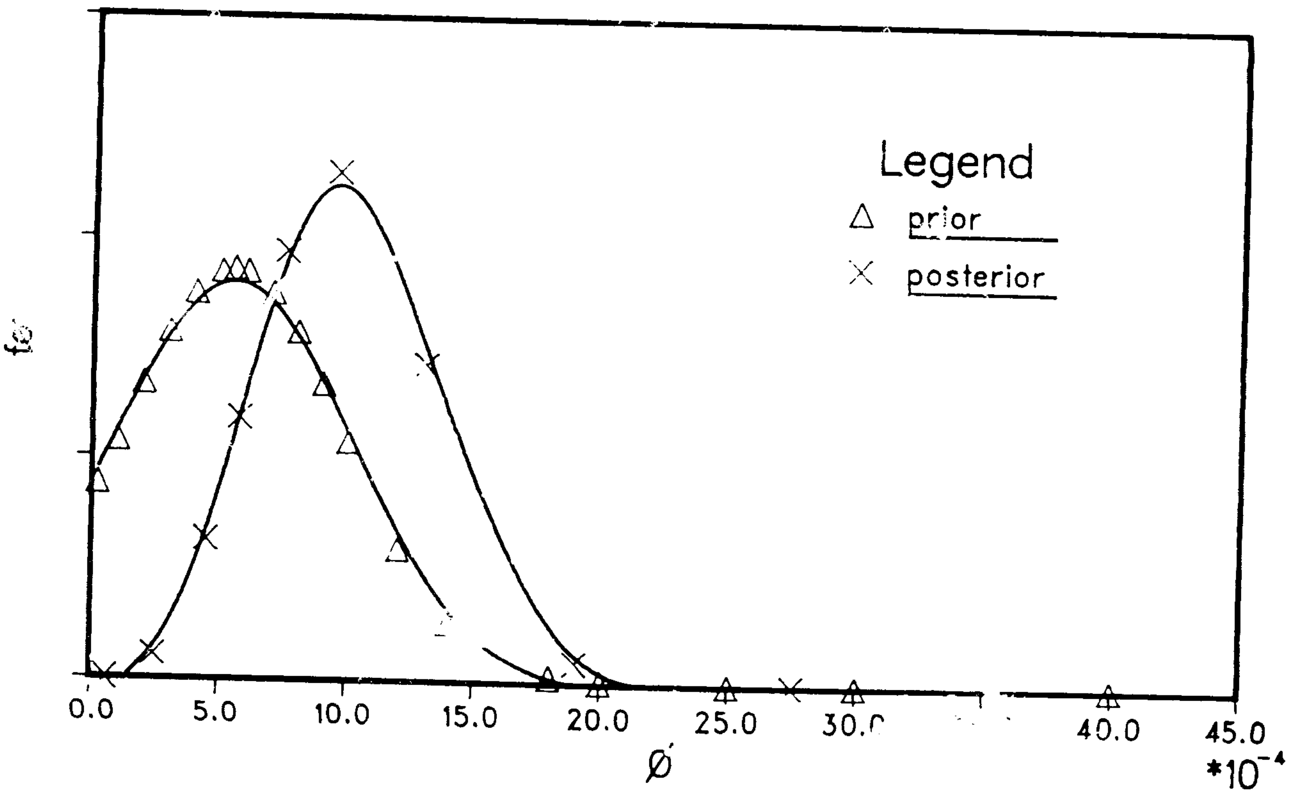


Figure B.3.2 Probability of the injector plugging

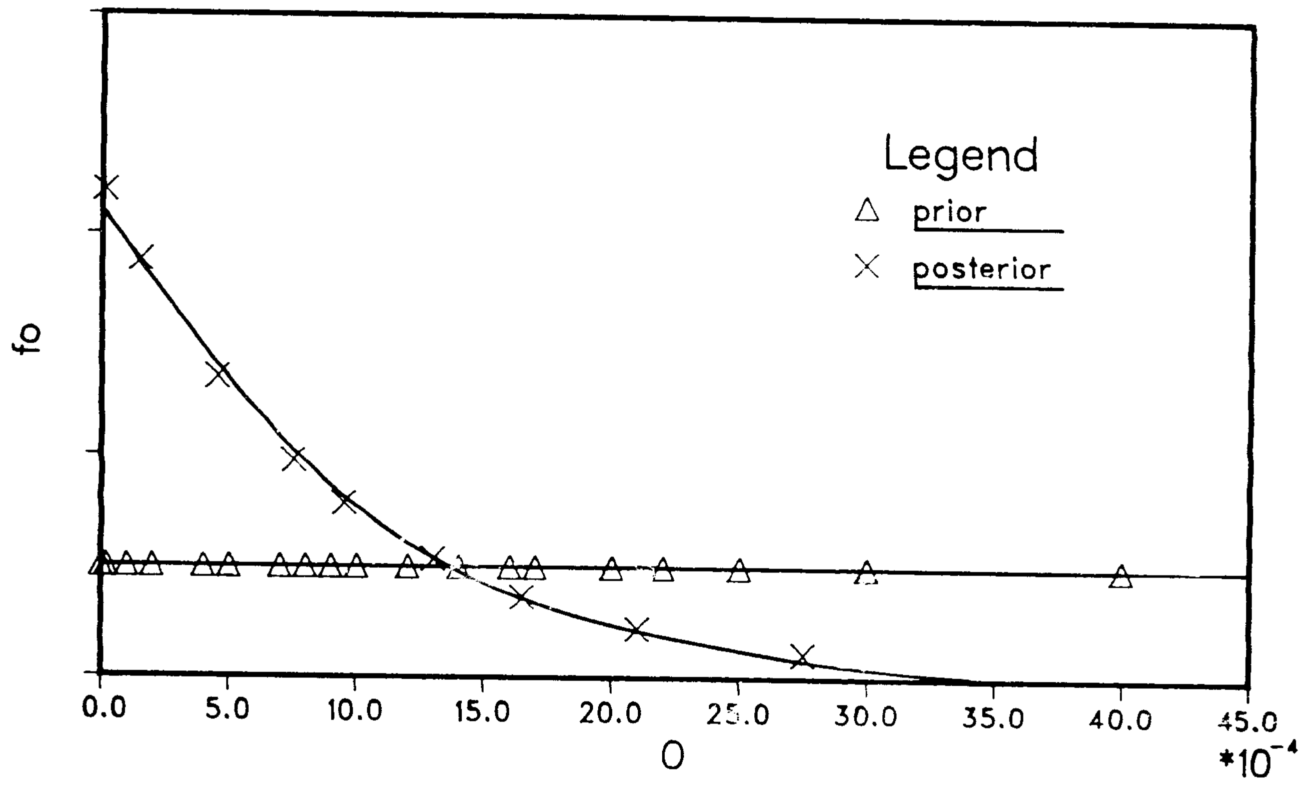


Figure B.3.3 Probability of the discharge line plugging

eductor. The low vacuum alarm should sound. The low pressure alarm should indicate to the staff the problem condition. The operational response, would be the changing of chlorinators and eductors, so that chlorination could continue. Prevention of injury requires that each automatic closure and the switching of the chlorinators occur correctly.

Closure of the Pressure Regulating Valve

The pressure regulating valve is opened and closed by applying a vacuum. When the vacuum is applied, a diaphragm depresses a spring which opens the valve. When the vacuum stops the spring is released closing the valve. A large pressure drop occurs at this valve. As a result, impurities within the chlorine gas tend to collect at this valve and may jam it open Generic information recommends the replacement of springs every two years and complete inspection of the unit every five years. The replacement rate was considered to be representative of a 5% failure rate. Using a normal distribution, the prior distribution was established. A mean of once every five years, with a standard deviation of once every six and a half years was used.

The updating of the prior with plant specific information was difficult for these valves because they operate for different lengths of time. The maintenance records were not always clear which chlorinator valve had been repaired. This was specified in only a few instances. The chlorinators which feed into the stilling basins are operating nearly continuously, and when the repairs were specified it was normally for these two chlorinators. Therefore those records which do specify the chlorinator repaired were used. The pressure regulating diaphragm valve of chlorinator 1 has undergone five repairs since 1984. Chlorinator 2 has had three repairs performed since 1984. Using the average of these valves the incidence rate was 4 over an event time of three years. The evidence was applied with a Poisson distribution (Fig. B.3.4).

Vent Does Not Lift

If the pressure regulating valve does not close, and there is no vacuum, the relief valve should lift, releasing the chlorine to the atmosphere via the exhaust fan. If this relief valve does not vent, the chlorine gas may continue along the PVC vacuum line under its own pressure. Depending on the cause of the loss of vacuum there could be varying results. If there is a water line break, the chlorine could eventually be released out of the break. If the eductor fouled and closed, the chlorine would remain under pressure in the lines. However, if isolation of the vacuum line or the chlorinator was not performed correctly there could be a major release when the eductor was dismantled for repair.

Because the relief valve is a diaphragm spring valve, the generic information suggests the same maintenance program as for the pressure regulating valve. The prior distribution that was developed for the pressure regulating valve has been used here as well; a normal distribution with a mean of once in five years and a standard deviation of once in six and a half years.

The failure rate evidence for this valve was different. There was only one repair incident required for a vent valve over the last three years. The lower failure rate may be due to the smaller number of times this valve is required to operate. It may also be due to the difficulty in determining if the valve is operating as it should. There are no alarm mechanisms to indicate if the valve is operational or not. However, the maintenance data are the only records which are kept for such equipment. This data was used to update the prior with a Poisson distribution. The event time used was 3 years with an incidence rate of 1 (Fig. B.3.5).

Gas Remaining in Line

When the pressure regulating valve closes the chlorine gas is contained under pressure up to the chlorinator. The closure of the diaphragm and in line check valves in the PVC vacuum line should prevent reverse flow of the injector water into the chlorinator. Even when these systems operate correctly, chlorine gas remains in the vacuum line between the chlorinator and the injector. There is not any mechanism to remove the gas in the line. The exposure of personnel to this gas depends on how the vacuum was interrupted. If there

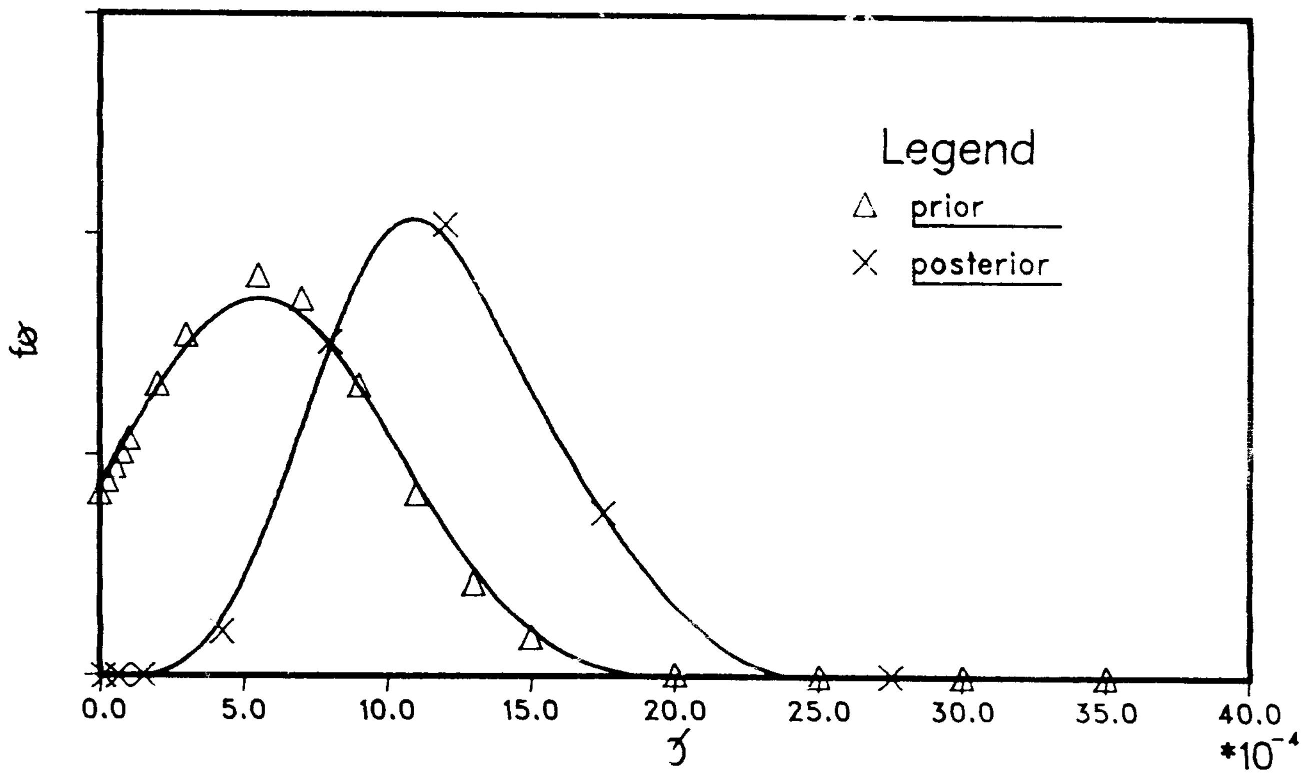


Figure B.3.4 Probability of the pressure regulating valve jamming open

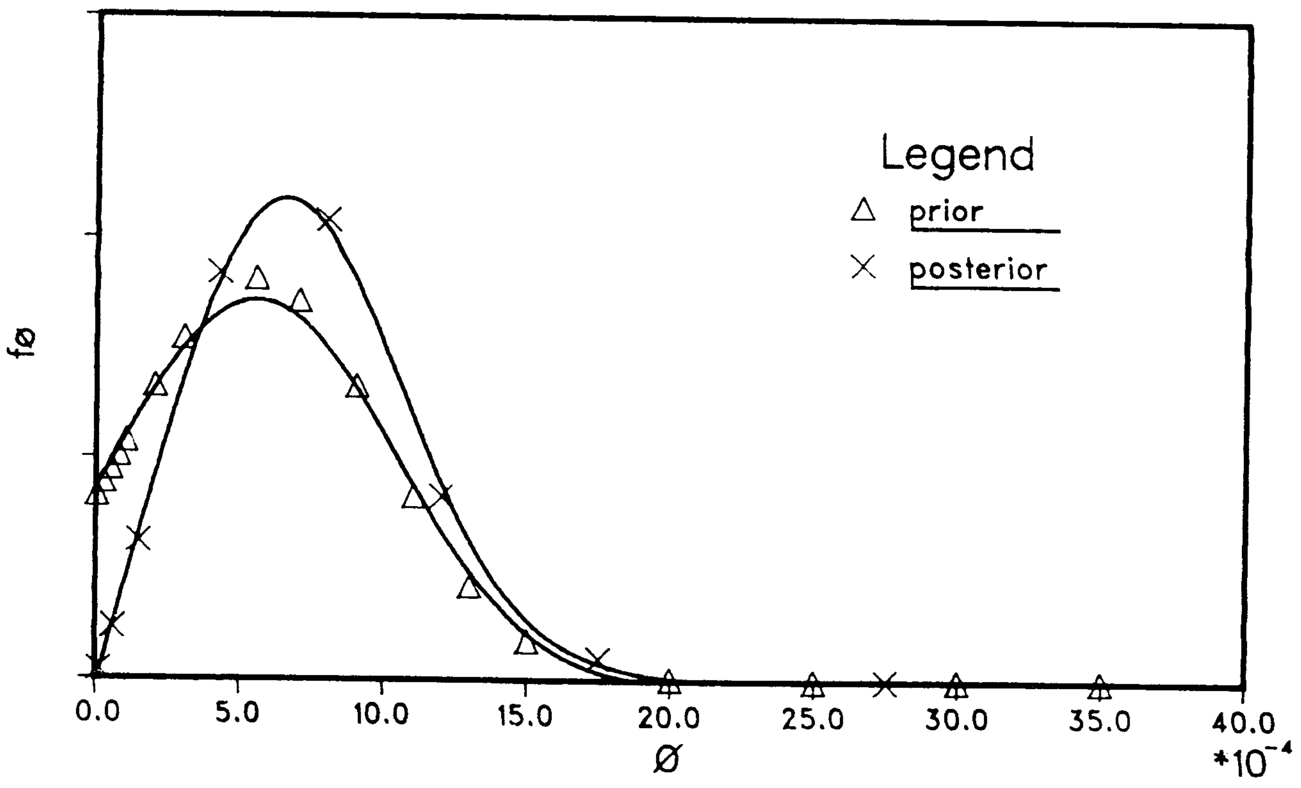


Figure B.3.5 Probability of the relief valve being jammed closed

was a loss of the water supply there would not be any exposure to the gas. If the loss of vacuum was due to a fouling of the eductor or a plugged vacuum line maintenance work would require the removal of, or access to the eductor.

The scenario of a loss of vacuum, results in a controlled release of a small quantity of chlorine gas. Because the tolerance to chlorine for each individual is different, the effect of such an exposure will vary. Only if the person was wearing an appropriate breathing apparatus would there be no effect.

Generic information cannot be applied to this type of problem. The probability of an individual donning a breathing apparatus depends on company policy, the enforcement of that policy and how threatened the individual is under the circumstances. Interviews with the maintenance staff, indicated the staff would not wear a breathing apparatus when repairing the system. They either did not view the quantity of chlorine as dangerous, or in some cases were not aware of the potential release. The probability that they would not be wearing their gas mask was represented by a normal distribution with a mean of 0.7 and a standard deviation of 0.1 (Fig B.3.6).

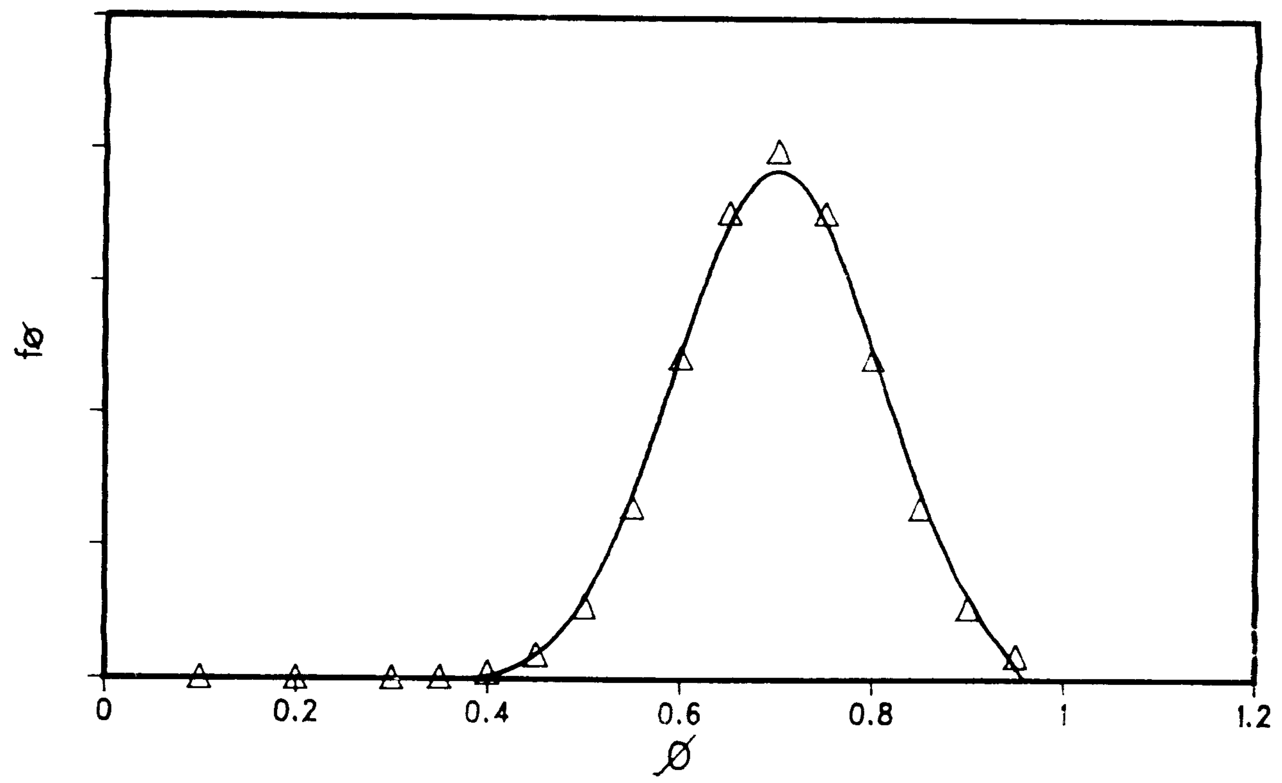


Figure B.3.6 Probability of the maintenance personnel not wearing breathing equipment during repairs

APPENDIX B.4

Chlorinator Flooded

Diaphragm Check Valve Fails

The probability of this valve failing and causing a fouled eductor was developed in Appendix B.3. Either the valve being corroded or its being jammed opened would allow water to pass and could eventually result in a flooded chlorinator.

In line Check Valve Fails Open

This check valve is unique to this system. Other feed units may or may not have such a valve. This valve does not need to be failed open for it to allow the passage of the water. Because the valve is opened by the application of a vacuum a slight vacuum may be strong enough to hold the valve open while the water passes in the opposite direction. This is the result of a design problem rather than a mechanical failure. The frequent presence of water in this line causes the valve to deteriorate from exposure to moist chlorine. A distribution for the valve was not developed. Rather it was assumed that under the conditions when the diaphragm check valve would create a partial vacuum but allow water to pass, this valve would also allow water to pass.

Switch Over of Chlorinators

The other event which may cause flooding of the chlorinator is an operational procedure. The chlorinators must be isolated at the isolation ball valve D(Fig. 6.1) when they are switched. If this is not done and the pressure fluctuates, the line and chlorinator may be flooded.

The probability of forgetting to close this valve is quite high. The valves have only recently been installed. The procedure of switching chlorinators is a rare event. There is the possiblity that even if the valve is left open the chlorinator may not flood. There is not any real hazard that results from forgetting to close this valve. The lack of stress along with the unfamiliarity all contribute to a high frequency of failing to close this isolation valve.

The expected frequency of changing the chlorinators has been estimated at once every 30 days. This value shall be used as the mean for the normal distribution with a standard deviation of one out of 45 days. This wide distribution represents the variability in the occurrence of this event.

The probability that the operator will close the valve can be estimated at 0.5 or once in every two chlorinator switches. This value shall be used for the mean with the standard deviation being set at 0.25.

The frequency of the back pressure being high enough to flood is also difficult to estimate. It depends largely on the eductor being fouled open which has been calculated and included in the fault tree. A conservative estimate of this frequency would be to assume that it always floods given the other conditions. The frequency for this event shall be assumed to be 1.0.

Updating the Prior

The fouling of the eductor or the switch over scenario combined with the failure of both check valves results in the probability distribution for the flooding of the chlorinator (Fig. 8.5). Plant data was used to update this initial distribution. A poisson distribution with an incidence value of 10 and an event value of 3 years was used to arrive at the final distribution.

Improper Isolation

When a chlorinator floods, maintenance work is required. The vacuum has been lost which indicates that the pressure regulating valve should be closed. If this valve remains open, the combination of the chlorine with the water would form a strong solution of hydrochloric acid, which is very corrosive. The probability of this valve remaining open was established in Appendix B.3.

The correct isolation of the chlorinator is critical when maintenance is required on a flooded chlorinator. The isolation procedure of the chlorinator requires the closure of three valves. Any one of these valves will isolate the chlorinator (Fig. 6.1). The procedure for isolation follows the following routine:

1. valve A is closed while the pressure gauge 2 drops to zero,
2. valves B and C are closed,
3. if there is still a vacuum, plug on chlorinator is pulled for an air purge,
4. close V-notch orifice,
5. close valve D.

If the chlorinator is flooded,the same order of valve closure is followed, however small pockets of gas will remain in the lines because step 3 would be omitted. Improper isolation would arise from either the valves leaking, a mechanical failure or from forgetting to close the necessary valves for complete isolation.

Closure of Valves

The procedure for isolation of a chlorinator is not performed frequently. Normally the isolation of valve A would be performed by the operations staff so that chlorination continues. The maintenance staff complete the remaining stages of the isolation.

The personnel all have a high degree of respect for the dangers associated with chlorine so the isolation procedure is performed with extreme care. Since these features of this procedure are very similar to the change of a tonner bank the same values for the prior distribution shall be used. A log-normal distribution with a 5% of 10^{-6} and a 95% of 10^{-2} was used. There was not an accurate value of the occurrence rate of this event. The prior was not updated because there was no indication of the number of isolations performed per annum (Fig. B.4.1).

Valves Leaking

The other possibility for injury, would be from the leaking of the three valves. If only one or two valves leak, the other valve will prevent the release of any gas. The generic information on the failure rate of these valves was limited. Most leak information is concerned with an exterior release rather than an isolation failure. Because of the lack of information, a uniform prior distribution was used.

Plant specific data was also limited because this failure would only be noticed when a chlorinator was dismantled. The maintenance records indicated, one isolation needle valve on the bottom, east header line, plugged once. In another instance, valve A was leaking. From this data a log normal distribution was developed. A 5% value of 10^{-6} adn 95% value of 10^{-1} were used. The K value was 2 and the event time was five years.

The different combinations which could lead to the release of chlorine gas from improper isolation were combined in the fault tree shown in Figure 9.1.

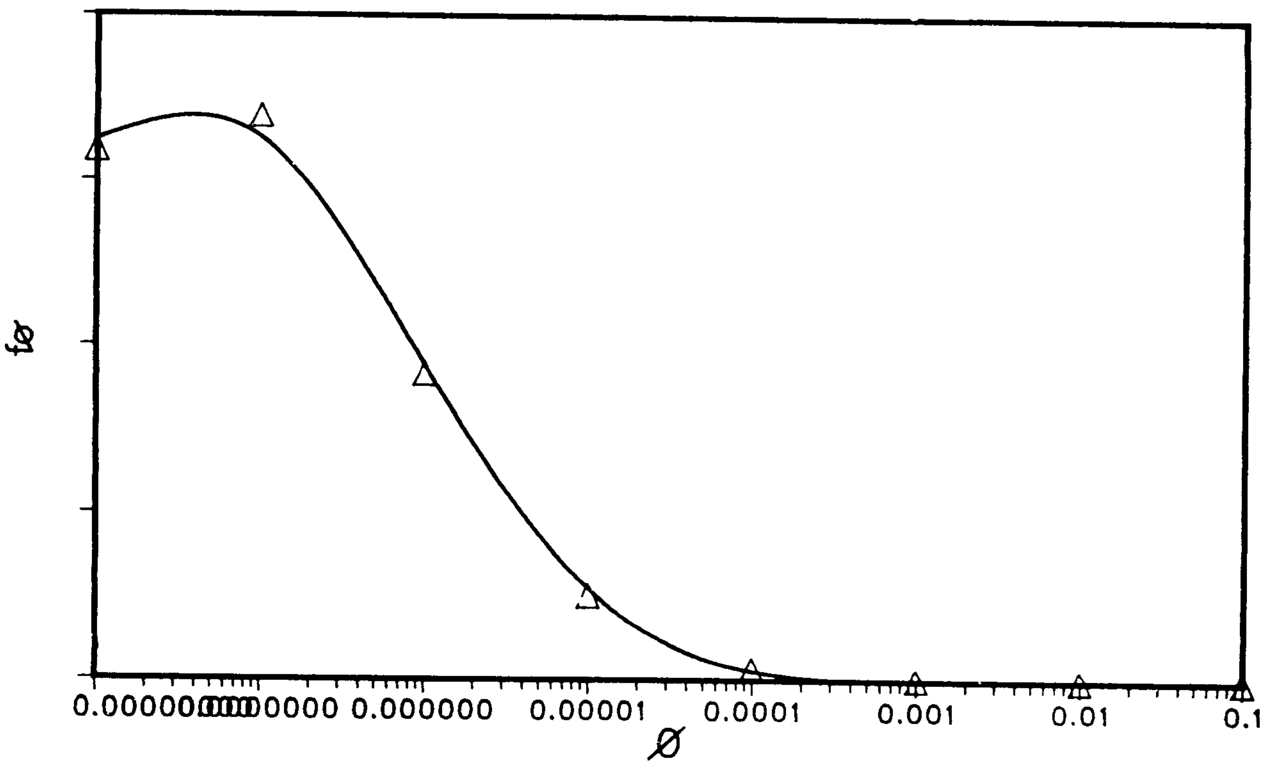


Figure B.4.1 Probability of failing to close the isolation valve

APPENDIX B.5

Quantity of Chlorine released from headers when full of liquid chlorine.

area of pipe = PI x r^2= 3.14 x (12.5 mm)^2 = 491 mm^2 longest section of pipe released = 1500 mm

Therefore total volume = 491 mm^2 x 15000 mm = 7.6 L

APPENDIX C.1

Tonner Rupture

Hoist Failure

For the existing unit, the lifting system meets its required capacity. There is the possibility that a failure of this mechanism could occur from excessive use. With a preventative maintenance program and routine checks, a serious failure should be averted. However there has been no routine maintenance program for this unit and there has never been an overhaul of any part of the lifting apparatus

A uniform prior distribution was used to describe the failure rate because of the limited generic data. There has only been one incident related to a potential hoist failure. This involved some loose screws in a section of the monorail. While this event did not constitute a complete failure it is indicative of the potential failure rate. Over 10 years, there are approximately 1700 tonners used. If each tonner is unloaded onto a storage platform, moved to a tonner bank, then onto the empty storage platform, and then reloaded, the lifting mechanism must be used four times per tonner. Therefore, over 10 years, the event number would be 6800, and the incidence rate 1. This evidence was applied with a binomial distribution (Fig. C.1.1).

Failure of Storage Platform

The two storage platforms are capable of holding ten tonners each. The east side holds full tonners each weighing

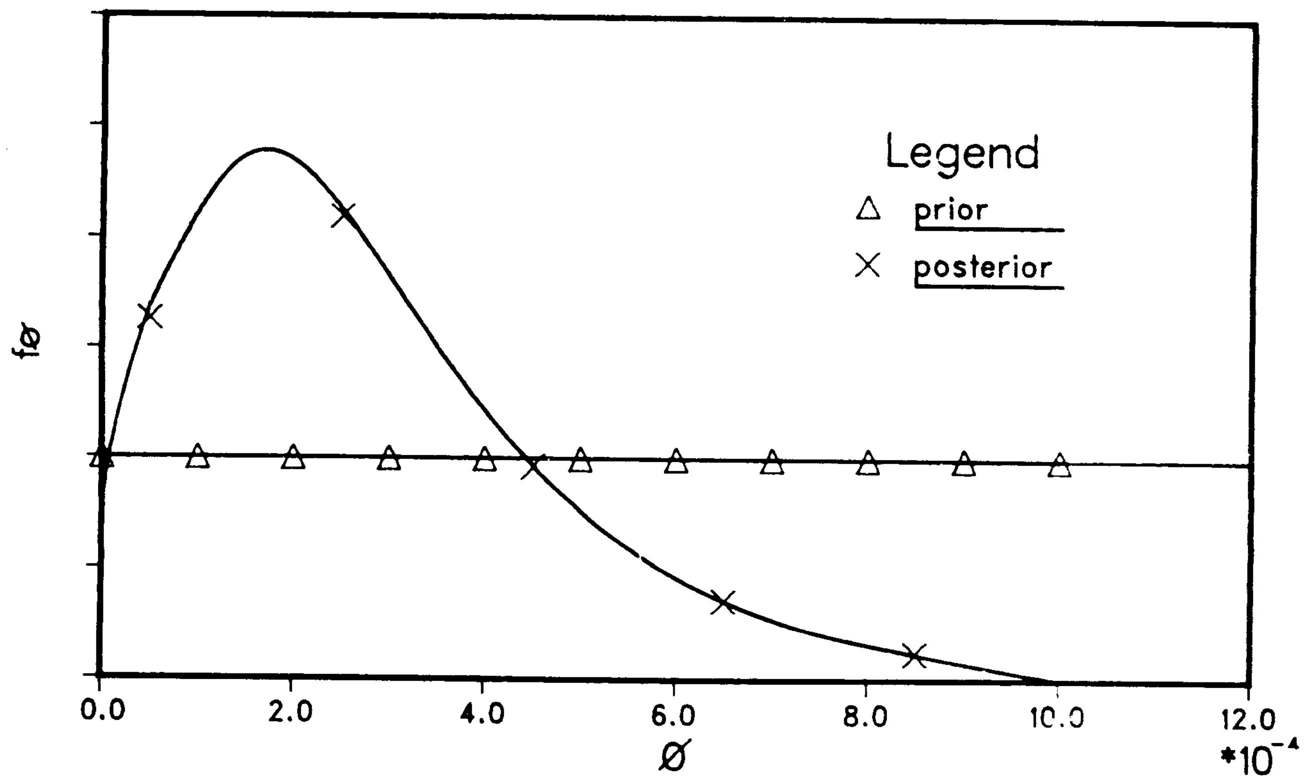


Figure C.1.1 Probability for failure of the hoist

approximately 2000 kg, and the west side holds empty tonners each weighing approximately 1000 kg. These tonners are stored in two layers. The bottom layer of tonners are supported by rotating trunnions with the second layer of tonners sitting on top. The failure of the platform, without being caused by an exterior force, would require the failure of two outside trunnions that are both held in position by two 20 mm diameter threaded bolts.

Over the past ten years, these trunnions have not shown any signs of fatigue, nor have they been exposed to any excessive forces. Because of a lack of generic data, the prior was represented by a uniform distribution. The updating of the prior was done with a Poisson distribution where the incidence value was 0, and the time interval 10 years.

Collision

There are two types of collisions which would cause a tonner rupture. The first would be during the movement of the tonner, when the tonner could hit one of headers, a chlorinator or another tonner. The second type of collision would be from an external source such as a truck or fork lift.

Collision with a Tonner

When tonners are being moved inside the storage room from the east to the west side, the clearance between the moving tonner and the headers or chlorinators is only 20 to

30 mm. If the tonner began to rock or swing, serious damage of either the chlorinators, headers or tonners could occur. During this procedure the staff are very aware of the potential hazard. This high level of stress may increase the potential for error, however there is not any time restriction for moving tonners. Even with extreme caution, there is always the potential for an accident, such as an operator tripping.

This information was used for the development of the prior. A log normal distribution was used to express the uncertainty which exists with this operation. A 5% of 10^{-6} per operation and a 95% of 10^{-2} were used. These values were updated with a binomial distribution. The incidence value was 0. Only half of the tonners are moved this way during the year. Over ten years this is equivalent to 850 tonners. Therefore the event value was 850 (Fig. C.1.2).

Collision with an Exterior Element

Only a person completely unaware of the presence of the tonners could cause a tonner rupture from an exterior force. Therefore the collision with a fork lift is extremely unlikely since only operations and maintenance personnel who work at the plant operate this equipment. For such an event to occur, the action would have to be intentional, which is impossible to evaluate with a risk assessment. Because of this, the prediction of a frequency distribution for the event was not deemed worthwhile.

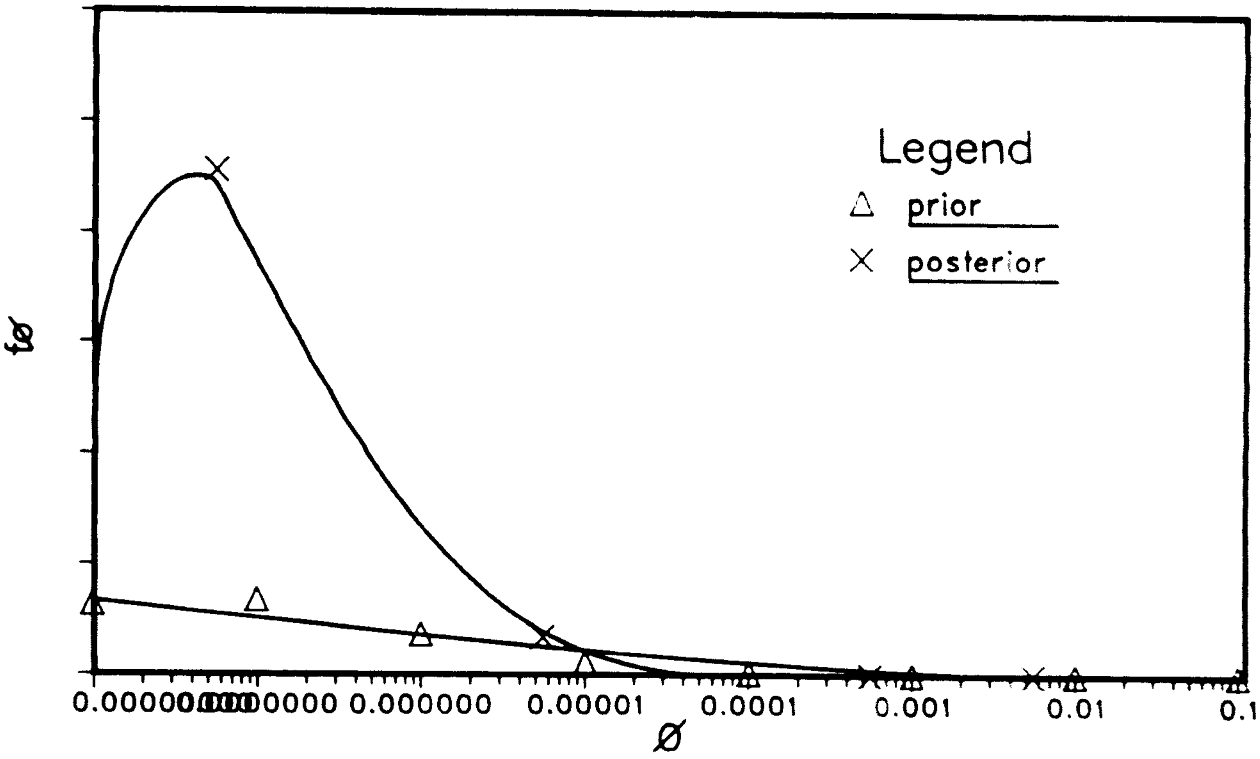


Figure C.1.2 Probability of a tonner collision

Collision from a truck backing up is a more reasonable scenario, because the driver may be unaware of the presence of chlorine, and there are many trucks backing up and turning in the storage room area. Such an incident can only be prevented by ensuring the drivers are well informed about the hazards, and that all areas are well signed. If a driver makes an error and backs into the chlorine room, he would impact the unloading doors before entering the room. This should give him adequate warning. The prior distribution shall be described by a uniform distribution. To update, the plant experience shall be used in a binomial distribution. An average of two trucks back up in this area per day giving an event value N of 7300 over the last 10 years. The incident value K is 0.

Corrosion

The physical and chemical properties of chlorine indicate that chlorine in the presence of water will corrode steel. Since the formation of 100% pure chlorine is impossible, there will always be a small amount of moisture within the tonners. Because this corrosion is inevitable, the supply and packaging companies of the tonners follow strict guidelines to prevent a possible leak from a tonner wall, or seam.

When each tonner is returned to the supply company, it is emptied of any excess chlorine and then weighed. If the weight is less than 95% of the original weight, the tonner is no longer usable. The inside and outside walls are inspected for dents, pitting, bulging and visible corrosion. The wall thickness is checked and if the thickness falls below one half the allowable thickness of the container it is condemned. If there are any crevices or lines exceeding 80 mm the tonner is no longer used. Dents should not exceed 6.5 mm at welds or 13 mm anywhere else. Obvious bulges which alter the diameter more than 25 mm make the tonner unusable (Chlorine Inst., 1980).

By following these guidelines it is unlikely that a tonner would remain in use if it was no longer in suitable condition. There is the possibility that a corrosion crack or a weld crack may be missed. Such a crack would produce a small slow leak.

The reasoning behind human errors and faults have been used to predict this error rate. The checking of tonners for the cracks and dents can be associated with jobs that are routine and mundane. It is a routine task that could be susceptible to a moment of forgetfulness. This type of job could be described as one which is routine and simple but which requires care. These routine tasks have an error rate of approximately 1 in 1000 (Table 2.3). For the prior distribution, a normal distribution with a mean of 1 in 1000 and a standard deviation of 1 in 5000 shall be used. To update this prior, a binomial distribution with an event rate of 1700 and an incidence rate of 0 shall be used (Fig. C.1.3).

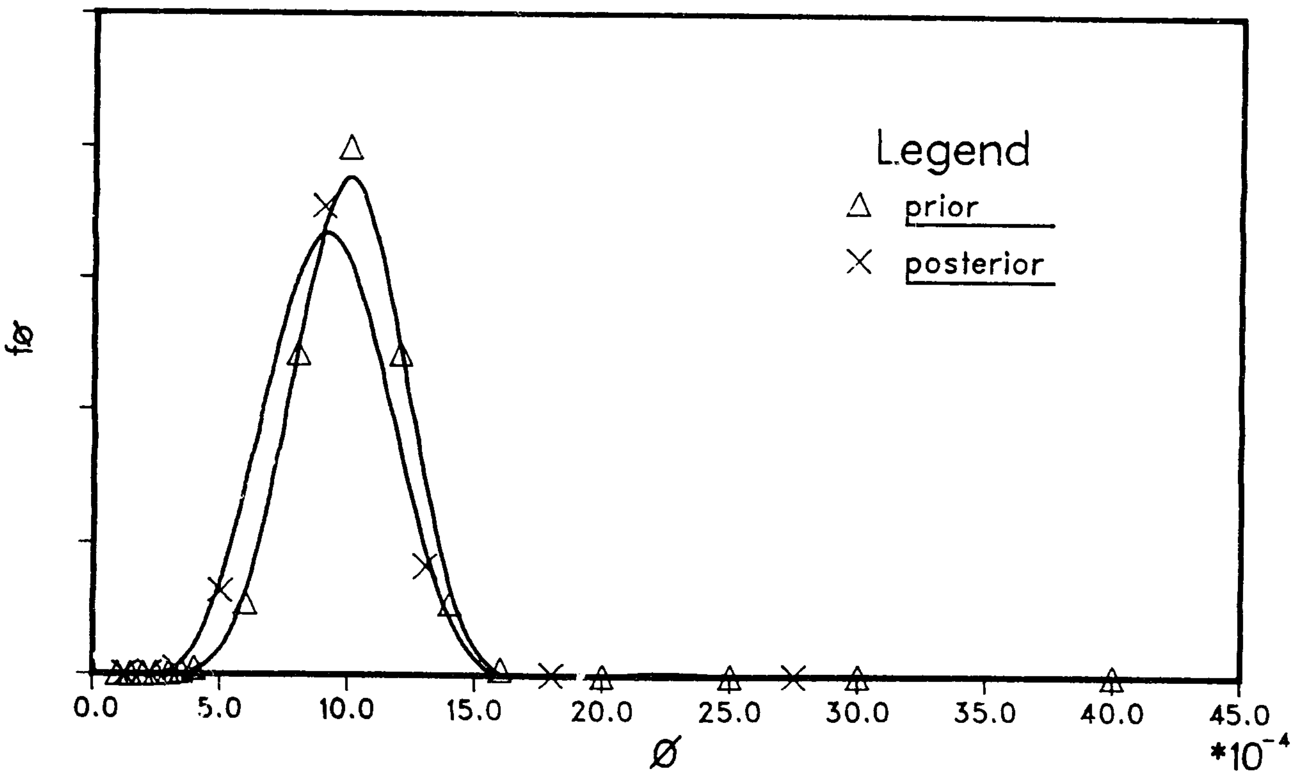


Figure C.1.3 Probability of a tonner with a corroded valve being delivered to the plant

Tonner Rupture

A tonner would rupture from the application of excessive heat. This could be in the form of a fire or an alternate mechanism which results in a direct application of heat. To prevent a tonner rupture, six fusible plugs which melt at 70°C , are installed in the ends of the chlorinator.

Fire

A fire event in any facility is always serious, but within a facility that has many chemicals which react violently when exposed to heat the result can be disastorous. Chlorine does not burn or explode under heat, however, increased temperature causes the liquid volume to expand.

This water treatment plant is composed mainly of concrete. The chlorine storage room is entirely concrete, except for the access doors which are metal. The interviews with operational and maintenance personnel indicated that, there have been only two fires in the last 10 years. Both were immediately controlled. The first was from welders igniting the tube settlers in a drained clarifier, and the second was from a plugged sodium chlorite pipe. When attempting to unplug the line, excessive force caused the chemical to spontaneously combust.

There are chemical fire extinguishers through out the plant, and all personnel have been well trained in their use. Because of the training and structural material, the probability of chlorine release from a fire is very small. A lognormal distribution with a 5 % of 10^{-6} and a 95 % of 10^{-2} was used. The plant specific data used to update the prior with a Poisson distribution were an incidence value of 0 and an event value of 10 years. The two fires that did occur were not considered since they did not affect the chlorine area.

Application of Heat

The application of heat which could cause a temperature of 70 °C may be from welding or an extra heater unit in winter. The welding situation is particularly dangerous since chlorine will support the combustion of steel. Given this information, an informed person would not attempt any welding within the storage room or on a live line carrying chlorine. This is where an error could occur from lack of training, or a moment of forgetfulness. Using a log-normal distribution developed from interviews with the maintenance personnel a prior distribution with a 5% of 10^{-7} per operation and a 95% of 10^{-4} was established. There was not any plant specific information to update this prior (Fig. C.1.4).

The application of direct heat by an alternate means could take the form of an extra heater. On one occasion a heater unit was placed in the storage room because the main heater had gone out. When the room was checked, it was noticed that the heater was directly facing one tonner, and that the tonner had become very hot. The heater was then immediately relocated. Since this event has occurred it is unlikely that the same mistake would be made again. However, this one event shall be used to develop the probability of other similar events.

A uniform prior distribution was used with a poisson distribution applied to update. A K value of 1 and a T value of ten years (3650 days) were used.

Fusible Plugs

Only if all six fusible plugs remained intact when the heat is applied, would a tonner rupture occur. The probability of each individual plug not melting is independent, so the probability of all of them not melting is the probability of each plug not melting multiplied together. There is little generic information on the failure rate of these plugs. Even if the failure rate was fairly high such as 1 in 100, when this value is raised to the six power, the probability of all of them not melting would be 10^{-12}. Because this is such a low value, and the estimate of 1 in 100 is a conservative value it shall be used for the fusible plugs not melting. A standard deviation of 1 in 500 shall be used for this normal distribution. There was not any plant specific information on this data, so the prior distribution was not updated.

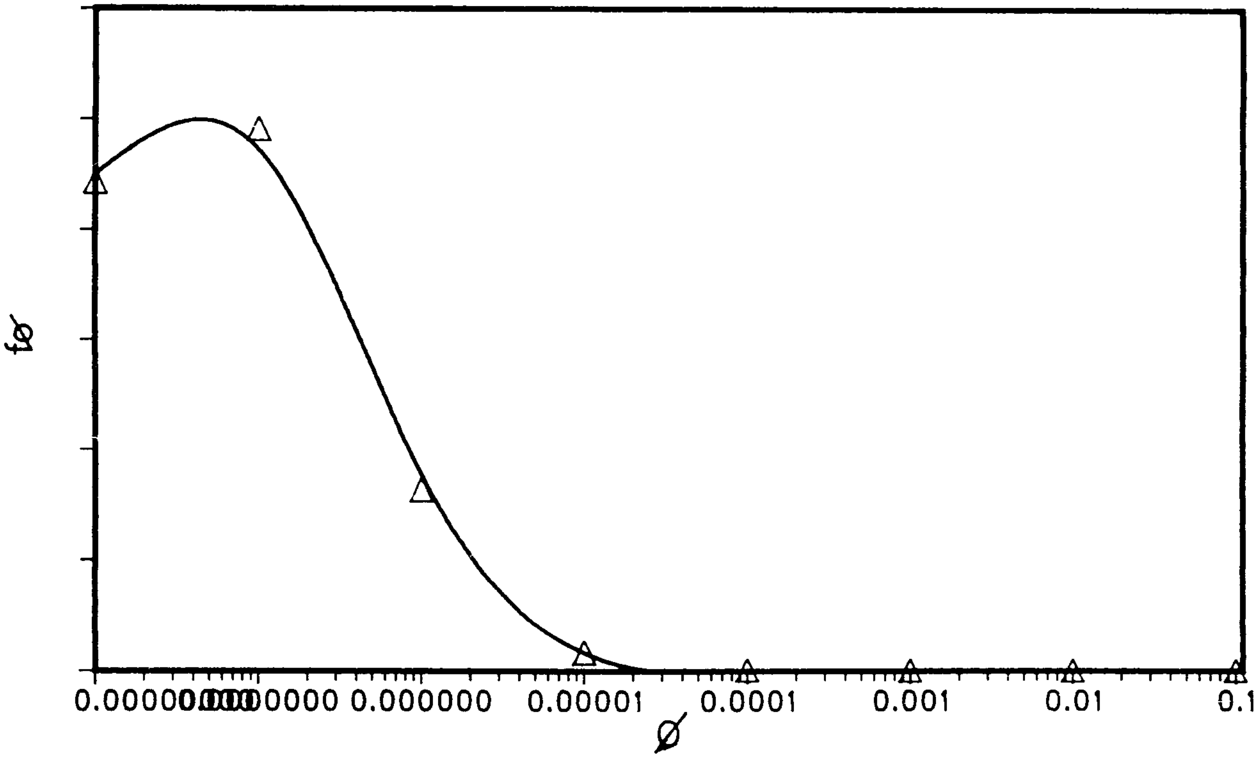


Figure C.1.4 Probability of welding occurring in the storage room

Combining the Events

For a tonner rupture the application of heat plus the failure of all six fusible plugs must occur. Therefore the events causing the excess heat situation were combined with OR gates and then combined with the failed fusible plugs by an AND gate.

APPENDIX C.2

Tonner Valve Corrosion

A corroded tonner valve could cause a leak. The valve could break off, or if it was sticking and the operator forced the valve, it could break. The valves are examined as part of the general inspection performed on the tonners. When installed, the valves should be free of any dirt, rust or other foreign matter (Chlorine Institute, 1980). The gasket seating surface is also inspected along with the valve packing. Any visible wear indicates that a new ring or packing should be installed. Replacement of the gasket rings and valve packing are very important for the prevention of leaks, since the valve packing represents the leading cause of valve leaks (White, 1986). White (1986) recommends the replacement of these valves at least once per year.

There was not any generic information on the failure rate of these valves. White (1986) indicated the expected valve replacement rate, he did not indicate the number of these which may be missed on inspection. Maintaining the same philosophy established for the monitoring and control of corrosion in a tonner, the same human failure rate will be used to estimate the failure rate of the valve. The prior value used for the mean was 0.001 and the standard deviation was 0.0005. If 200 tonners are used each year, this corresponds to a valve leak once every five years. There has never been a leaking valve on one of the tonners which gives a binomial distribution with an incidence value of 0 and an event value of 1700 for the updating of the prior.

The corrosion may not directly cause the leak but only cause the valve to stick. The probability for the valve sticking was given a prior distribution the same as that for just a leaking valve, since the same inspection failure rate would apply. It is more difficult to predict the operator response to a sticking valve. The policy in the facility was not to force a sticking tonner valve, but to simply detach it and employ an alternate tonner. Given their operating instructions and the awareness all of the staff have for chlorine, an estimate of 0.01 was used for the mean. To emphasize the uncertainty about this value a wide standard deviation of 0.005 was used.

These two distributions were then combined through an AND gate which signifies that the valve must stick and the operator must try to force it open before a leak scenario can occur from just a sticking valve. This gave a probability distribution which could then be updated by plant specific data, because the event has never happened. A binomial distribution with an incidence rate of 0, and an event value of 1700 was used.

APPENDIX C.3

Fusible Plug Corrosion

The corrosion scenario for a fusible plug, follows the same development as for a corroded valve. Fusible plugs are to be replaced if there are any cracks or signs of separation from the tonner end. Even if the plug appears to be in satisfactory condition, they are to be replaced once every five years. For a corrosion failure, the same values developed for the tonner valve will be used which was a mean of 0.001 and a standard deviation of 0.0005 for a normal prior distribution. A binomial distribution with a K value of 0, and a N value of 10200 valve connections for the last 10 years, was used to update the prior. When developing the scenario for the melting of the plugs there must first be a sufficient application of heat. The probability of an external heat source being directly applied to the tonner was devloped in Appedix C.1. The desired reaction is that the plug will melt. The probability of the plug melting was given a mean value of 0.99 in the tonner rupture scenario. For this scenario only one plug needs to melt to meet the requirements of an uncontrolled chlorine leak.

The probability that the plug would melt along with the probability of the direct application of heat were combined to give a prior distribution. The prior was then updated with a binomial distribution with a K value of 0 and a N value of 1700 (Fig. C.3.1).

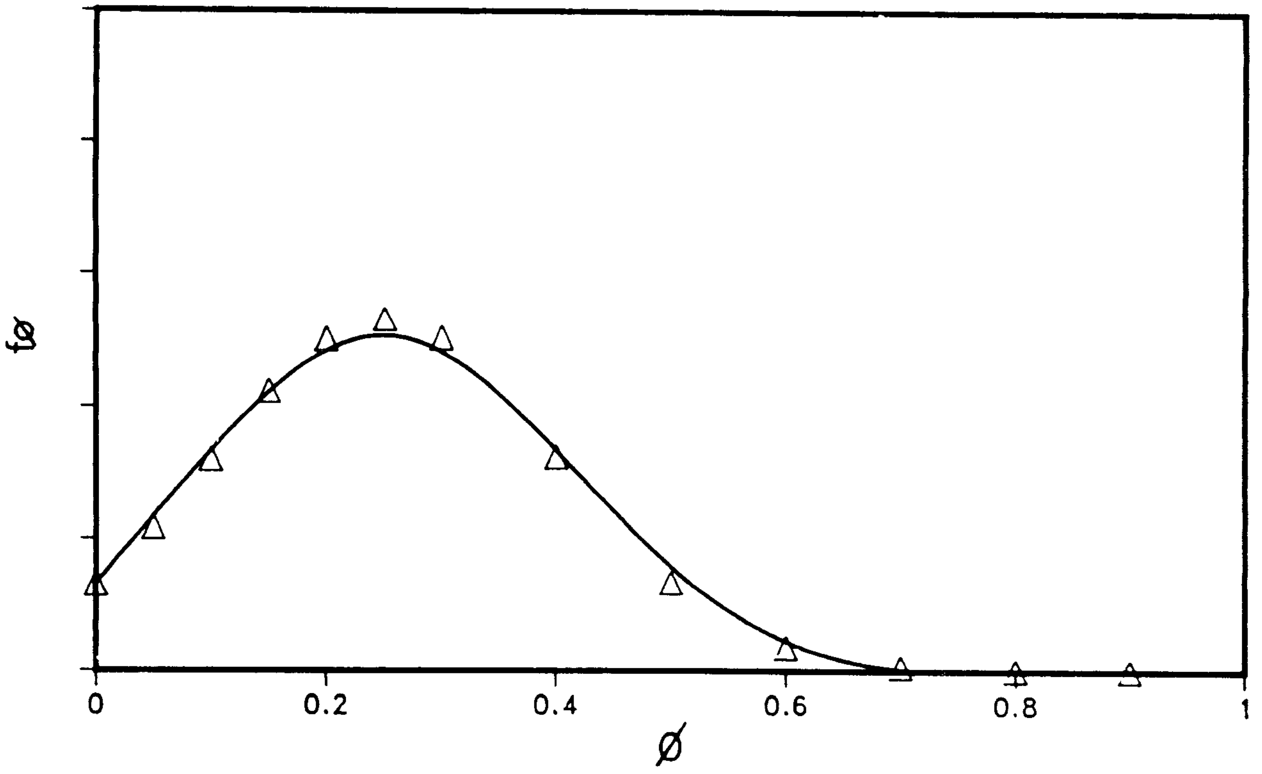


Figure C.3.1 Probability of a fusible plug melting

APPENDIX C.4

Header Break

Many of the scenarios which could result in a header break have already been considered. A collision from either a tonner or a ground force was considered in the collision section for a tonner rupture.

Corrosion is a possible mechanism which could cause a header leak. Corrosion can occur undetected for long periods of time within steel piping particularly in the the joints. To detect such a leak, discoloration of the piping and moisture droplets should be watched for. On brightly painted yellow piping, rust spots should be readily visible if corrosion is occurring.

These header systems have a recommended replacement rate of once every five years (Chorination Manual, 1977). Unlike the tonners which are routinely checked for possible signs of wearing out, this piping system has not been replaced or inspected on a regular basis. This recommended replacement rate was considered indicative of the failure rate. Following the procedure used for the other generic data sources, a one in five year failure rate was equated to a 5% probability of failure. The mean was then set at 1/15 years. The standard deviation was 1/15 years.

The maintenance records indicated there has never been a leak associated directly with the header system. Using this information a poisson distribution was used to update the prior with an K value of 0, and a N value of 3 years.

Flexible Connectors

The flexible connectors are recognized as being a weak section within the piping system. These pieces of piping are continually exposed to the moisture in the atmosphere causes corrosion. White (1986) recommended a replacment rate for these lines of once per year. Within tne Chlorination Manual (1977) a two year replacement rate was recommended. In the present facility, the flexible connectors have never been the cause of a chlorine leak, however these connectors are only changed when there is a complaint from one of the operating personnel. This results in these connectors being left on for an average of two years. The expected failure rates were developed Following the same procedure used for suggested replacement rates. Using the replacement rate of once per annum as the 5% probability value, the mean was developed. A normal prior distribution with a mean of once per five years andard deviation of once every two and a half years were used for the prior. This prior distribution was then updated using a poisson distribution, with a 0 incidence rate over 2 years or 730 days.

PVC Break

A breakage of the PVC vacuum line would only result in a leak if the pressure regulating valve dic not close upon loss of vacuum, and the relief valve did not vent. The probability values for these events were established in section 8.3 and have been recorded in the fault tree

(Fig.7.11).

A PVC line could break from collision with a forklift or other piece of moving equipment, or from the failure of a support during the change of piping routes immediately succeeding the chlorinators. The former scenario could happen in either the area between the storage room and the injector room or in the storage room. A collision in the storage room follows the same scenario as that for the collision of a tonner causing rupture. However the likelihood of the vacuum lines being struck is even less since they are located between the chlorinators and the building wall which provides fairly good protection. This is also true for the injector room, which is isolated from high traffic areas. A uniform prior distribution was used. This was updated using a Poisson distribution with a K of 0 and a N value of 3650 days.

The collision scenario between the storage room and injector room is much higher. The five chlorine vacuum lines run virtually unprotected along a low ceiling up to the injector room. An awareness of their presence does reduce the potential hazard. These particular pipes have never been hit according to plant experience. However, an alum line and a water line have been broken from this type of collision during the last ten years. This type of error may be considered to be a human error arising from an operator momentarily forgetting the presence of the chlorine lines. This type of relationship shall be used for the development of the prior, which was a log-normal distribution, with a 5% of 10^{-7} and a 95% of 10^{-2}. To update the prior, a poisson distribution shall be used. The incidence rate is 0, and the event time is 10 years (3650 days).

Sticky PVC ball valves could also result in a PVC vacuum line break. When chlorinators are switched the valving succeeding the chlorinators must be changed. Large 80 mm ball valves must be rotated to close or open the line to the particular chlorinator. The operational staff has indicated that improper support when these valves are changed could possibly cause a line to break. Rather than attempting to predict this failure rate it is suggested that a step ladder be permanently assigned to the room to ensure that this type of accident does not happen.

APPENDIX D.1

Alarm Systems

Within the storage room there are two identical Wallace and Tiernan leak detectors which are set to detect a concentration of 1 ppm of chlorine. This system represents a duplicated, but independent warning system. The fractional dead time which represents the proportion of time the detectors can be expected to be inoperable from random, testing and common mode errors has been calculated at 0.002 (Appendix D.2). By reviewing the contribution each individual type of error makes to the total fractional dead time, the human error and common mode errors contribute the most to the down time. The failure rate of the detectors does not significantly contribute to this dead time mostly because of the duplicated system and the frequent testing that is done. Because the human error rate, evaluated at one in 1000 operations can vary there is a degree of uncertainty that exists for the fractional dead time. This uncertainty can be expressed as a probability distribution. A normal distribution, with a mean of .001 and a standard deviation of .0005 shall be used for the prior distribution.

This value shall be updated with a poisson distribution. There has been one instance within the plant when both detectors were inoperable. Information can be used for the poisson distribution with an incident rate of 1 and an event time of 10 years (3650 days) (Fig. D.1.1).

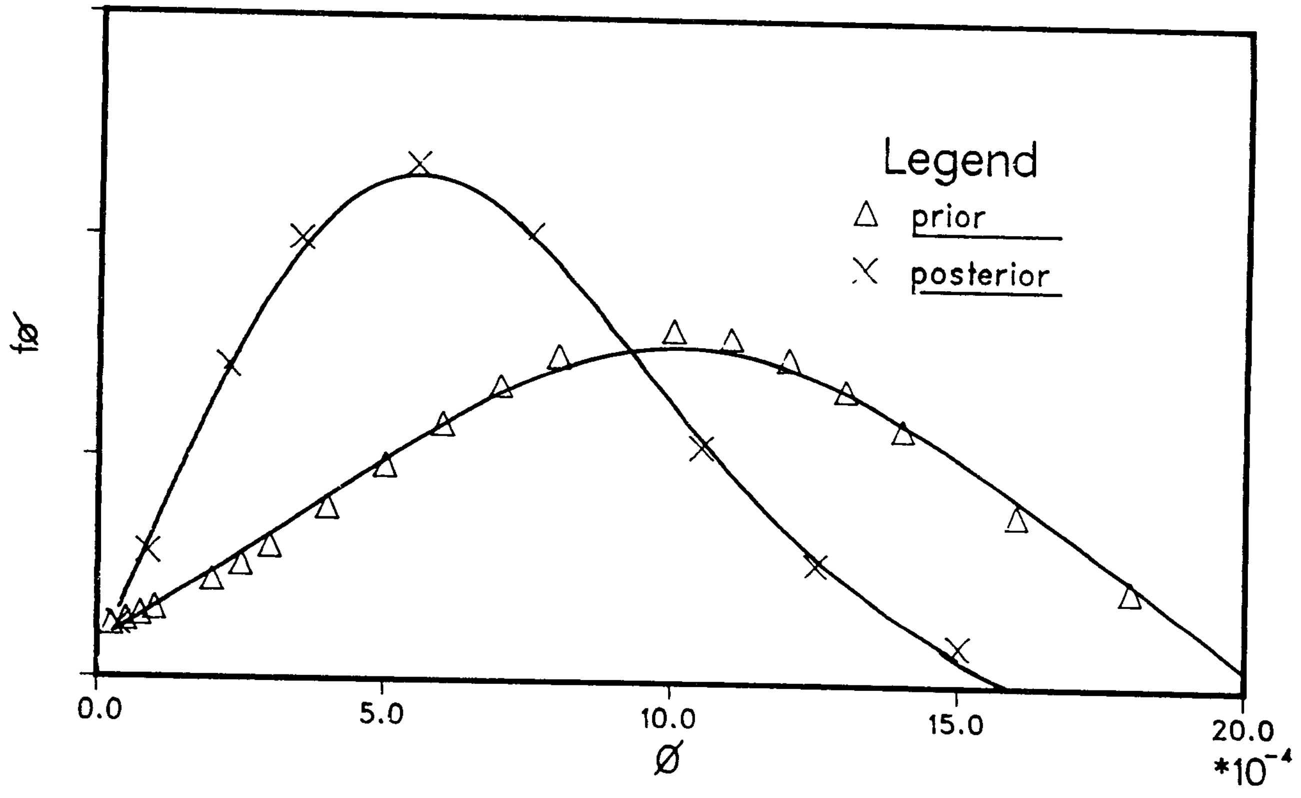


Figure D.1.1 Probability of the failure of the leak alarm

No Response to Warning System

There has only been one uncontrolled chlorine release which occurred in plant 3. There has never been a major uncontrolled release in the storage room of plants 1 and 2. Therefore, when the chlorine detector sounds the alarm, the automatic response is to assume that the leak is minor,

aps from a small quantity of gas left in a flexible connector during a tonner change.

Whenever there is to be work carried out in the storage room, the operator in the control room is notified. He is aware of any unusual circumstances which may cause the alarm to be set off, and therefore also knows when an unexpected leak may be occurring.

An interview with the operators indicated that upon hearing the alarm, they did not assume it was a major leak. Of fourteen operators interviewed, only three would immediately don a breathing appratus and investigate. Three would phone for instructions and eight would conduct an initial investigation without a breathing apparatus. All three who would immediately don the breathing equipment were level 2 operators who would usually be in the control room and therefore would know of any potential accidents. A probability distribution was developed for personnel responding without airpacks. A normal distribution with a mean of 0.5 and a standard deviation of 0.25 was used.

The probability that there would be no response to the alarm is negligible when compared to the response without an airpack. When the alarm sounds it must be turned off locally, so it cannot be reset without an investigation.

Ventilation

The ventilation units are automatically activated when the leak detector sets off the alarm, as long as the switch is set locally on automatic rather than manual position. If the switch is in the manual position the ventilation unit would be operating. The automatic start of the ventilation unit is checked once per week with the test of the chlorine leak detectors. Human error in testing would be the main cause of the ventilation unit's inactivation. A mean value for the failure of the ventilation unit to start, was set at 0.001 using the fractional dead time calculation for the leak detector. This was used for a normal distribution with a standard deviation of 0.0005. This prior distribution was updated with a binomial distribution. The ventila unit has never failed to start during the weekly test over the last three years. Therefore an event value of 156 and an incidence value of 0 shall be used to update the prior.

Person Enters Without a Breathing Apparatus

The odor threshhold of chlorine for a human being is 0.3 to 5.0 ppm. On the average, most people can readily smell chlorine gas at a concentration of 1 ppm which is the recommended exposure limit over eight hours (Table 6.2). The short term limit of fifteen minutes allows an exposure to 3 ppm. The IDLH is set at 25 ppm, and extreme discomfort is caused by 15 ppm. Because chlorine has a strong odor at low concentrations, it provides its own warning system should there be a leak without the leak detector sounding.

This strong odor would warn people who enter the storage room of the leak. When a operator arrives at the storage room and discovers the leak, it is unlikely that they would enter the room without an appropriate breathing appratus. From the interviews carried out on the personnel, there was a 100% agreement that a person would not enter a room with a leak without wearing an appropriate breathing appratus. However, if the operator were to discover a collegue collapsed, it is difficult to predict a person's response. There was a leak at plant 3 in which the operator after receiving a blast of chlorine gas, returned to the room to shut a valve, without first donning an air pack. All of this information was used to develop a probability distribution. A log-normal distribution with a 5% of 10^{-5} and a 95% of 10^{-1} were used. The number of leaks that have occurred at the plant have not been recorded to develop an updated prior distribution.

APPENDIX D.2

Fractional Dead Time Calculation

This calculation is for a system with 2 identical warning systems.

1. Total possible failure time;

random fractional dead time (fdt) + common mode failure fdt.

2. Calculate Random fdt.

(A)Estimated failure rates:

bell in alarm fails -	0.1 per year
detector fails -	0.1 per year
total	0.11 per year (F)

(B) testing Time

3 min per channel per test (t)

test frequency - once per week (T)

(C) Other Errors

Independent errors at trip test - 1/1000 tests

spurious trips - 1/100 tests

common mode errors at test 1/1000 tests

(D)Calculate fdt random for the combined warning system:

$$\text{fdt(combined)} = (\text{Avg. fdt 1 out of 2}) \frac{(T-2t)}{T} + (\text{Avg. fdt 1 out of 1})\frac{2t}{T}$$

$$\text{fdt (1 out of 1)} = \frac{F^n T^n}{n+1} = 0.5\ (\ .11T) + 0.001 = 0.55T + 0.001$$

$$\text{fdt (1 out of 2)} = 4/3\ (0.055T)^2 + (0.055T)(0.002)$$

After substituting these equations into the fdt combined equation, and the values given for the variables the final solution is found:

$$\text{fdt(random)} = 1.6 \times 10^{-5}$$

$$\text{Total fdt} = \text{fdt(random)} + \text{fdt(common mode test error)} + \text{fdt(common mode error)}$$

$$\text{Therefore the total fdt} = 1.6 \times 10^{-5} + 0.001 + 0.00001 = 0.00103$$

APPENDIX E.1

Chlorine Concentration in Storage Room

Flow rate of chlorine under 240 kPa = 1.8 g/s

Total release time considered = 3 min (180 s).

Total quantity of chlorine released = 1.8 g/s x 180 s
= 324 g

Total area of storage room floor = 15.8 m x 9.0 m = 142.2 m^3

- considering 1/4 of the storage room up to a 1 m height,

there is a total volume of 35.5 m^3

The concentration of chlorine after 3 min would be:

concentration = 340 g / 35.5 m^3 = 9.6 g/m^3

APPENDIX E.2

Quantity of Chlorine Released from a Broken Vacuum Line

Diameter of pipe = 50.8 mm

Area of pipe = PI x r^2 = 3.14 x $(25.4)^2$ = 2032 mm^2

Total length of pipe = 500 cm= 5000mm

Total volume per pipe = 2032 mm^2 x 5000 mm

= 10.2 L

If 2 pipes carry the chlorine,

the total volume of chlorine released = 2 x 10.2 L = 20.4 L

APPENDIX F

Activated Carbon

Hazard Identification for Activated Carbon Applied to Water Quality

The risk considered for the activated carbon system did not focus on operational safety but on the risk to the public from the production of drinking water that does not meet specified requirements. The health risk posed directly by activated carbon as a chemical will not be considered, therefore the toxicological properties of activated carbon do not need to be emphasized as they were for chlorine. The important areas for this type of review will be the reliability of feeding equipment and analyses that are performed to indicate when the carbon is required.

The Use of Activated Carbon

Activated carbon is used for the removal of many types of compounds which affect the quality of drinking water in different ways. Historically it has been used for the removal of taste and odor causing compounds, both manmade and natural (Hopkins, 1936). Natural taste and odor causing sources are usually related to algae, decaying plant matter, and spring runoff. Manmade taste and odor compounds may be either inorganic or organic. Inorganic compounds can usually be removed through alum addition and pH adjustment. Organic compounds that create undesirable taste and odors include: pesticides from agricultural runoff, and oil and gasoline from street runoff (Montgomery, 1985).

The removal of organic compounds has received more attention in recent years for reasons other than the prevention of taste and odor. Chlorine, which has been used by most water treatment plants for disinfection was found to be useful in reducing taste and odor. Because chlorine is an extremely powerful oxidizing agent, the process of superchlorination, in which the water was overdosed with chlorine and then dechlorinated to remove the residual, was used to oxidize taste and odor compounds to tasteless and odorless compounds (Hopkins, 1936). While this may have effectively reduced taste and odours, some of the byproducts of this oxidation such as trihalomethanes are suspected carcinogens. In addition to these serious health effects, some compounds produced through the oxidation are not tasteless and odorless but have a very strong disinctive odor (Montgomery, 1985).

These factors have made the removal of organics one of the most important reasons for using activated carbon. By reducing the dissolved organics, the possibility of producing chlorinated hydrocarbons and objectionable taste and odor compounds is reduced.

Feading Activated Carbon

When a water treatment facility draws its raw water source from a river that flows through a city, the addition of activated carbon is critical. Not only must naturally occurring organics be removed, but manmade compounds from street runoff must also be contended with.

The system under review uses powdered activated carbon for the removal of organics and taste and odor causing compounds. Unlike other chemicals in the facility, activated carbon is not used continuously. Both rain and snow melt creating urban and rural runoff are conditions which require the addition of activated carbon. Advanced warning of an oil spill or the observance of a surface film in the plant are conditions for the addition of activated carbon. If odor is detected from an unknown source, carbon is also added. The required dose of carbon varies from 5 mg/L to 20 mg/L depending on the circumstances. The carbon may actually be hand applied to surface films, although there are absorbent pads and booms which can be used. These feeding requirements are summarized in Table F.1.1.

Carbon Feed Unit

Vaughn et al. (1971) has provided some guidelines for the construction of a powdered activated carbon (PAC) storage and feed unit. These guidelines, while being general do indicate the basic requirements a facility should meet. The facility should be able to feed carbon continuously in a constant proportion and volume. The mixing device should ensure complete wetting of the carbon and be able to maintain an even distribution of the carbon slurry. The unit should also have a suitable dust collector.

Table F.1.1. Activated carbon feeding rates.

(Annual Report, 1986)

Condition	Quantity
—	
Urban Runoff	
From Rain	Feed at 5 mg/L
From Snow Melt	Feed at 5 mg/L for forecast above freezing temperatures
Spring Runoff, Urban and Rural	
Due to snow melt	Feed at 10 to 20 mg/L
Oil or Chemical Spill	
Due to overturned truck or unknown sources	Feed at 10 mg/L , may require plant shutdown
Odour	Feed at 20 mg/L
Precautionary	Feed at 5 mg/L

The carbon slurry is prepared in a storage - mixing tank. Four pumps are available to transport the slurry to the three plants. The feed unit is represented by the process diagram in Figure F.1.1.

Transporting and Unloading

A truck load of activated carbon may vary from 10000 to 12000 kg. The material comes in a dry form and is mixed into a slurry within the storage tank as it is unloaded. Prior to unloading, the quantity of carbon must be known, so the corresponding volume of water can be added.

The addition of the water is done semi-automatically. The operator chooses the quantity of water to be added and programs this volume into the 'BATCH WATER CONTROL' panel (Fig. F.1.2). Supply valve A is then manually opened. The automatic addition of the preprogrammed quantity of water is manually started by pushing a start button. The motorized solenoid valve C then automatically opens and the addition of water begins. This valve automatically closes when the programmed quantity of water has been added.

Once the water has started, the carbon can be unloaded from the truck. Most trucks are capable of unloading themselves. If the truck unloading unit is inoperable, there is a vacuum eductor unit that can be used to unload the carbon.

Figure F.1.3 indicates that there are two routes the make up water can be added by. The first route is through

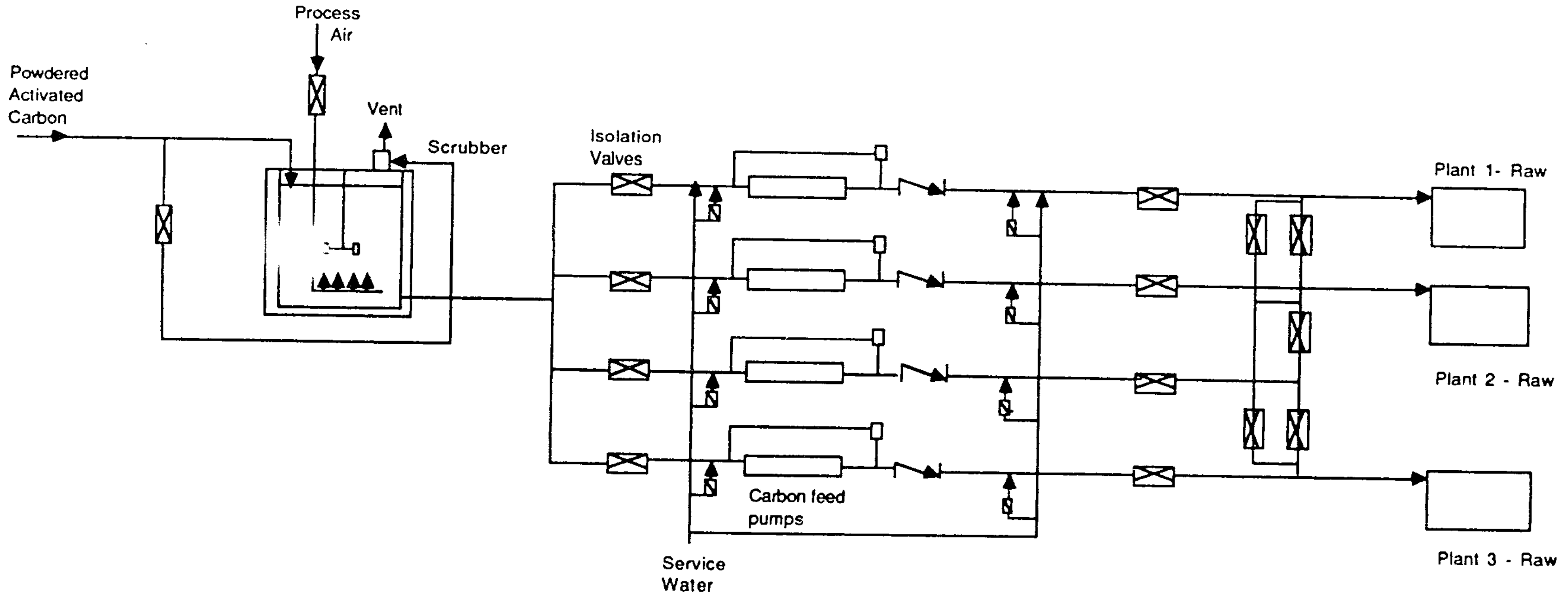


Figure F.1.1 Process diagram for the activated carbon feed unit

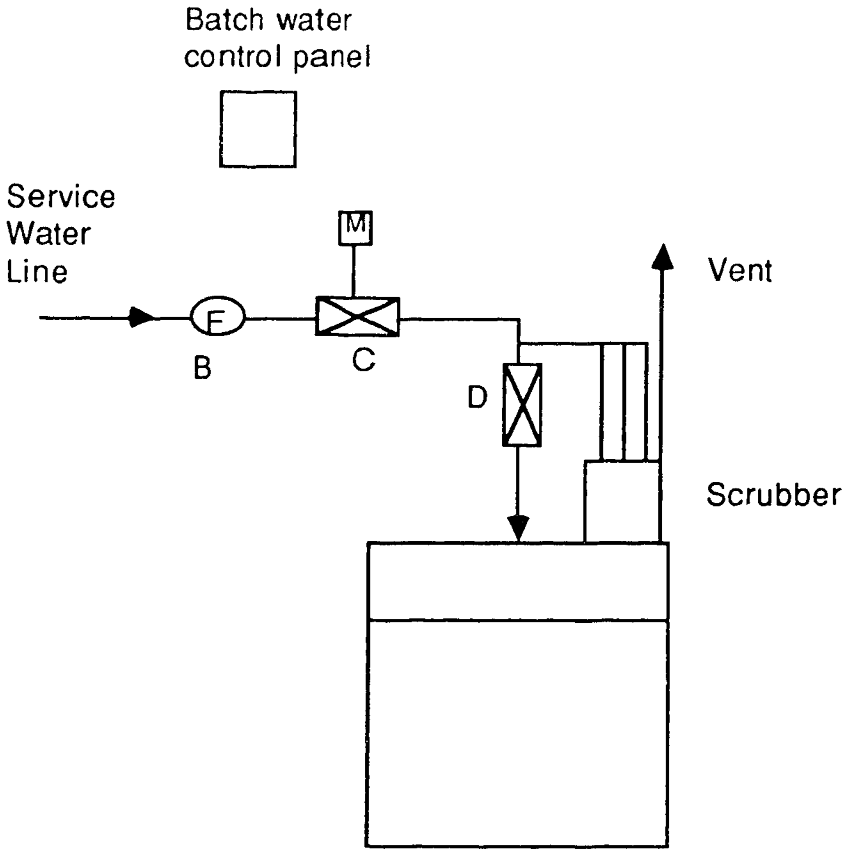


Figure F.1.2 Process diagram for the addition of water to the activated carbon storage tank

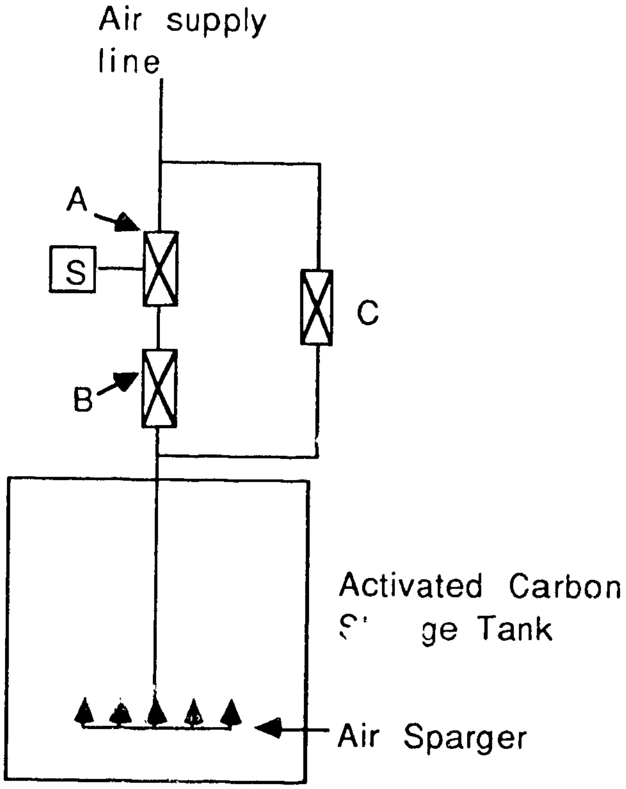


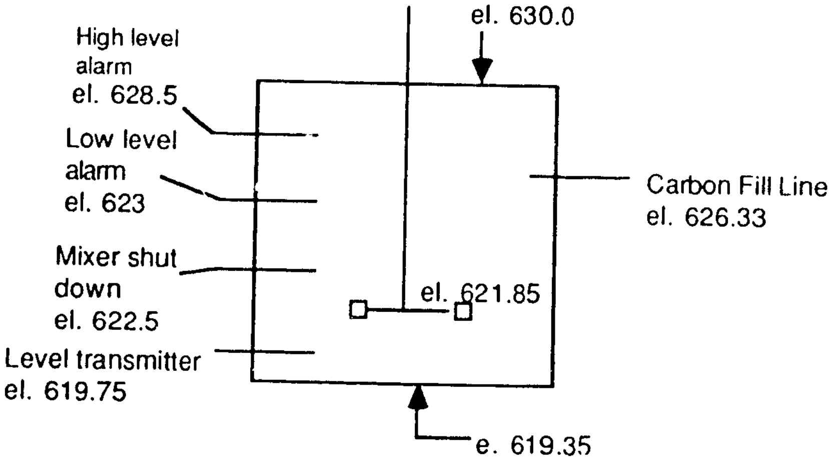
Figure F.1.3 The air sparger unit in the storage tank

valve D, and the alternate route is through the scrubber. Standard procedure is to use the scrubber during unloading of the carbon and then switch to valve D. The scrubber reduces the quantity of dust during unloading.

Storage Tank and Mixing Unit

The storage tank has a volume of 835.6 m^3, but a usuable volume of 573 m^3. There are two mixing units used to maintain an even suspension throughout the tank consisting of a mechanical mixer and an air sparger unit. Depending on the quantity of carbon in the tank, the mixing unit used will vary. When there is more than 263 m^3 of carbon slurry, Mode 1 is used. Mode 1, which is set on a chemical control panel uses the mechanical mixer continuously. The air sparger is used during the mixer start up. Even though the mixer will continue operating to a storage level of 263 m^3, the mixer cannot be started unless there is at least 315 m^3 of carbon in storage. Mode 2 is the second mixing method, used when the storage is below 270 m^3. It involves only the air sparger as the mixing unit. The switch over to mode 2 requires a manual adjustment at the control panel, and manual start up of the air sparger.

To start the air sparger unit when it is used with the mixer, valve B is opened and valve C is closed (Fig. F.1.4). The air compressor may need to be activated if there is not enough air. Once the mixer is started at a local control panel, the solenoid valve A automatically opens after a 2



1. High level alarm el. 628.5	$835.6\ m^3$
2 Low level Alarm el. 623.0	$310.4\ m^3$
3. Low level mixer and pump shut down el. 622.5	$262.6\ m^3$
4. Transmitter Elevation el. 619.75	0 m

Figure F.1.4 Alarms and automatic shut down points for the activated carbon storage tank

min delay. The valve then automatically closes after an additional 2 min. When Mode 2 is in operation, the bypass valve C is used, with valve B closed.

Pumps and Piping

The activated carbon storage unit supplies all three plants on site with the necessary quantities of activated carbon. There are four pumps and three piping systems to supply the different requirements of each plant. The extra pump acts as an emergency or standby pump (Fig. F.1.1). In Mode 1, the pumps are automatically shut down with the mixer. When the manual switchover to the air sparger is performed, the pumps must also be restarted locally. For the pumps to be restarted, the carbon level must be above 30 m^3 of the shut down point (263 m^3).

The four pumps are all of the same model; Moyno 214 two stage metering feed pumps. The pumps are air hardened tool steel with chrome lining and a natural rubber stator. The extra lining helps protect against the abrasive carbon. The piping lines are 32 mm diameter PVC pipes.

The pumps are isolated and flushed out before start-up or shutdown. Isolation valves are located between the storage tank and the pumps to prevent the pumps from clogging with the carbon slurry. This valve must be opened when pumping commences. Carrier water is added immediately after the pumps to ensure smooth flowing of the carbon slurry. The carrier water is always applied unless the pump is being flushed either before or after use. Because the carbon slurry is maintained at a constant concentration, and the pumps have a limited capacity, there may be instances when the raw water pumpage rate would create a demand that the present system could not meet. Standard operating procedure reduces the raw water pumpage rate so the required concentration of carbon would be applied.

Role of the Operator

The operators are a very important link in ensuring the unit performs correctly. The addition of activated carbon is one of the few chemicals which has a preset feed concentration (Table F.1.1). The operator must initially determine that a condition exists which requires the addition of carbon. Knowing the pumpage rate of the raw water and that the carbon slurry is at 4%, the feed pumps can be set accordingly. A calibration chart is used to relate pump settings to pump rates.

When turning on the pumps, the operator is responsible for flushing out the pump, getting the pump started and then setting the feed rate. The feed rates can be checked at sample locations prior to the injection point to ensure the correct concentration and flow rate.

The operators are also important for unloading the carbon into the storage tank. They manually open water and air valves, determine the correct quantity of water to add and program the water controller. The quantity of water added is also monitored to ensure that the correct amount is added. Operations also monitors the level of carbon within the tank.

Alarms

With the possibility of an automatic shutdown on various pieces of equipment, it is important that the operations staff be warned of such an event. Prior to the mechanical mixer automatically shutting down at 263 m^3 storage, there is a low level alarm which sounds when there is 310 m^3 of storage left (Fig. F.1.4). When the storage volume drops to 263 m^3, another alarm sounds which is the low low level alarm. This signifies that the mixer and pumps have been shut down in Mode 1. There is also a high level alarm which sounds at 835.6 m^3. This would sound if the automatic water controller continued to fill the tank after its preprogrammed quantity. The tank could also be overfilled if a shipment was ordered and unloaded when there was not enough room for it in the storage tank.

Development of Scenarios

The focus of the risk assessment for the activated carbon unit, was the risk to water quality from an inadequate supply of activated carbon. The efficiency and effectiveness of powdered activated carbon or the mixing equipment which disperses carbon throughout the water was not reviewed. Only the ability of the storage and feed equipment to provide carbon on demand was considered. In a more complete review, mixing studies of the rapid mixer, effects of alum addition, and the risk associated with granular activated carbon versus powdered activated carbon would be compared.

Damage States

Damage states and initiating events must be defined to develop the hazard scenarios. The damage states were general enough to provide an ending point for each scenario. These general damage states included: plant shut down with supply stable, plant shut down with supply contaminated, or supply stable and continuing.

Initiating Events

The initiating events focused on the system supplying an adequate quantity of carbon. The initiating events could have been the list of situations which indicate to the operator that the carbon was required. Rather than developing the initiating events in this manner, the various possibilities for a carbon demand were considered separately. The remaining initiating events represented a loss of carbon feed. They were developed from the HAZOP guide words which provided a systematic method for inducing stress on the system. These scenarios shall now be considered.

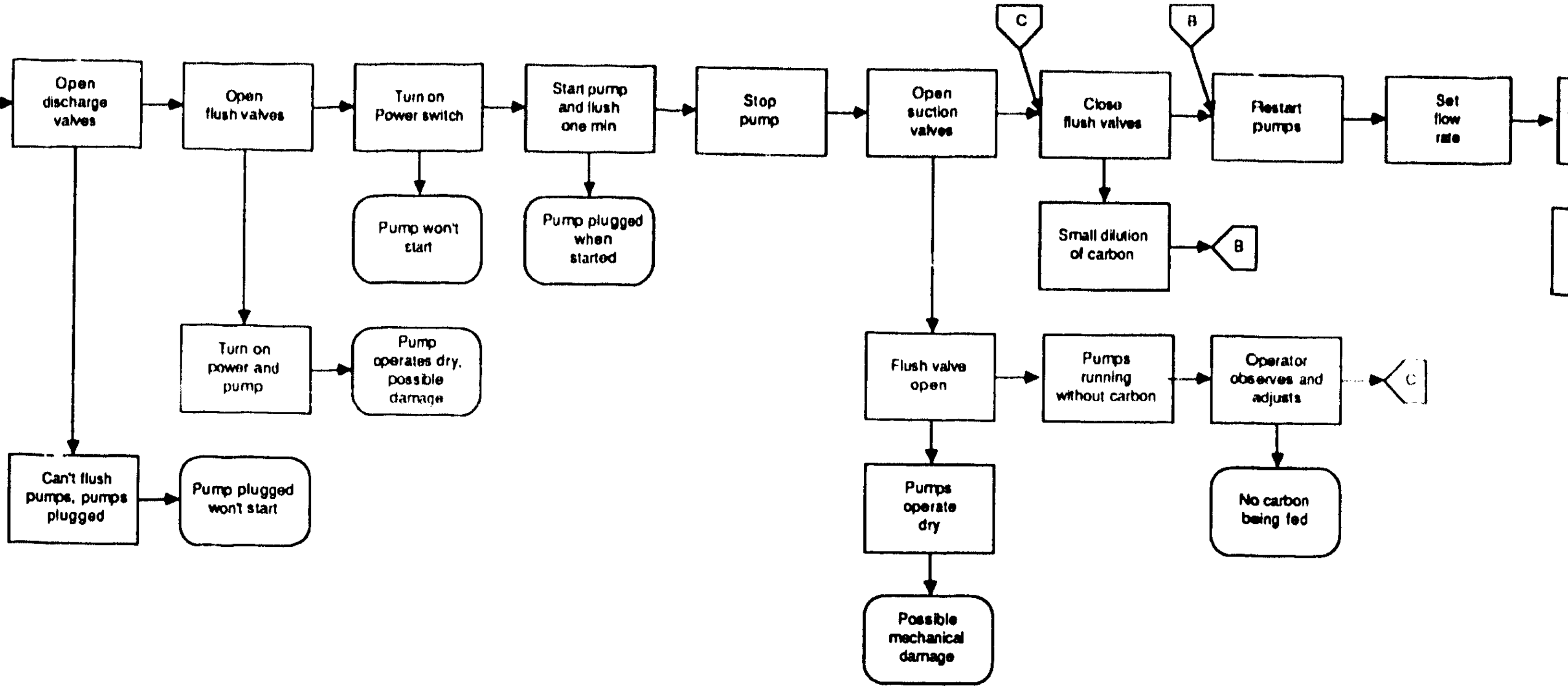
Storage Tank

The HAZOP guide word NONE can be applied in several ways to the carbon unit. It can refer to no carbon, no make-up water, no flow, no carrier water, or no flush water. Beginning with the storage tank, each of these events will be considered. The situation of no carbon may occur from either a physical lack of carbon in storage or from the system being plugged so that pumping is prevented. These scenarios were developed using an event tree (Fig. F.1.5.). The success responses appear horizontally while the failures are vertical.

When carbon is demanded, the first possibility is that there is not enough carbon in storage. There are several circumstances which could explain the lack of carbon. The personnel who order the shipments may forget, they may order the shipment late, or the shipment may arrive late even though it was ordered on time.

If the carbon does begin to run low there are the two low level alarms which should indicate to the staff that the carbon storage is inadequate. There are two explanations for the alarms not sounding, either the control switch was left in Mode 2, or the alarm may have failed. After each 12 h period, the quantity of carbon is totaled and compared to the usage rate. A lack of carbon should be discovered at this point.

The other NONE situation for the storage tank is no make-up water. A mechanical failure or a human failure could



e describing the storage tank operation

cause a no make-up water scenario. The mechanical failure would be from a burst pipe or the automatic solenoid valve not opening. The human failure would be from either forgetting to add the water on the batch controller or forgetting to open the manual valve. The carbon concentration within the tank would be incorrect if there was inadequate make-p water. A local digital read out gives the carbon concentration. The manual and solenoid valves are checked periodically to ensure they are in the correct position.

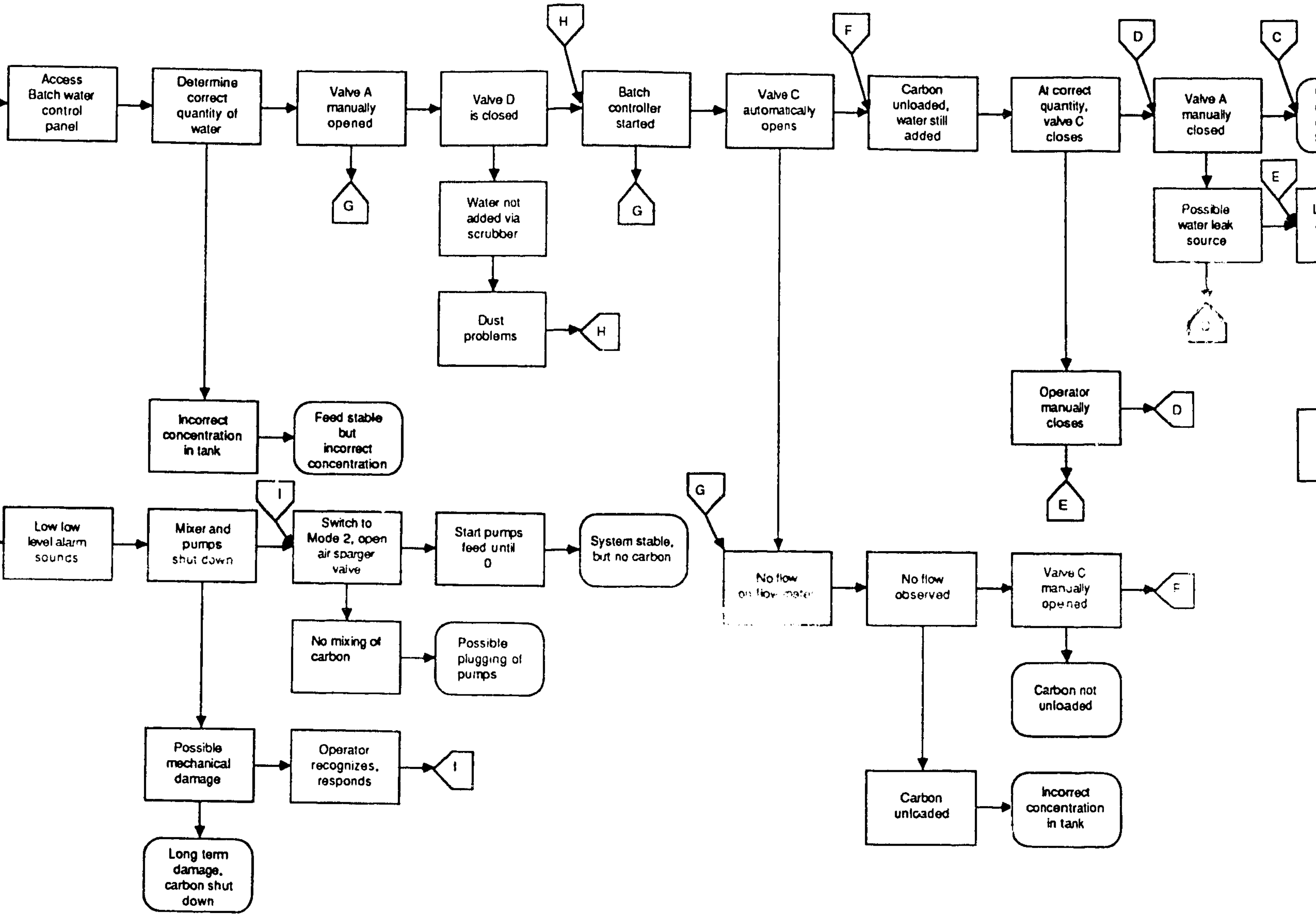
The result of an incorrect carbon slurry concentration when erred on the high side, is that the pumps or piping would eventually clog. This would result in plant shut down. A slurry which is too dilute could result in a contaminated water supply.

The HAZOP guide word MORE OF, was applied to the storage tank to generate scenarios considering more make-up water. This could cause an overflow of the tank, or alter the concentration of the carbon slurry. The event could occur from either mechanical or human failure. A faulty valve, leak, or a failure in the automatic batch water control, could all be causes of a more make-up water scenario. A human failure such as the incorrect programming of the batch water control or leaving a valve open could also result in this scenario.

Both the digital read out of the slurry concentration, and the high level alarm should give warning of such an event. However, if the overflow were to occur there would be plant damage since carbon would contaminate the sludge dewatering tank as well as create a severe cleaning problem. The carbon slurry would be very dilute, resulting in feed rate problems. The final damage state from such an event would be a water supply safe or plant shut down with supply safe. The former damage state would depend on how quickly the situation was discovered and then rectified.

Pumps

The no flow scenario can be associated with the pumps or pipes (Fig. F.1.6). There are several reasons for a no flow situation caused by the pumps. Suction or discharge valves may be closed, the pump may be clogged with carbon, or the pump may be worn out from the abbrasive material it must pump. When the pumps are stopped or started a rather complicated series of valve maneuvering occurs so that the system is flushed on line. When the pump is not pumping during start up, the operator is on hand to try and rectify the problem. Should the pump stop during operation, the situation would not be found until a routine check is made on the system, or the lack of carbon was noticed in the system. A plugged pipe would also be manually discovered through investigation. Once the no flow situation is discovered there are several courses of action. The stand by pump if available can be started. A blocked pump or pipe could be flushed clear with high pressure water.


Access Batch water control panel
Determine correct quantity of water
Valve A manually opened
Valve D is closed
H
Batch controller started
Valve C automatically opens
F
Carbon unloaded, water still added
At correct quantity, valve C closes
D
Valve A manually closed
C
G
Water not added via scrubber
G
E
Possible water leak source
Dust problems
H
Operator manually closes
D
E
Incorrect concentration in tank
Feed stable but incorrect concentration
I
Low low level alarm sounds
Mixer and pumps shut down
Switch to Mode 2, open air sparger valve
Start pumps feed until 0
System stable, but no carbon
G
No flow on flow meter
No flow observed
Valve C manually opened
F
No mixing of carbon
Possible plugging of pumps
Carbon not unloaded
Possible mechanical damage
Operator recognizes, responds
I
Carbon unloaded
Incorrect concentration in tank
Long term damage, carbon shut down

gram for the operation of the activated carbon pumps

The damage state for the no flow event depends on the time of discovery. If discovered immediately, plant shut down maybe required, but the water supply should remain intact. However if the stoppage was not discovered until there was analysis of the water, the water may be contaminated.

HAZOP also generates the scenarios of no carrier water and no flush water. Either of these events would only add to a higher probability of the pipes plugging creating the no flow scenario. Therefore these events are part of the elementary events responsible for the no flow situation. Both of the events may be the result of mechanical or human failure. The supply lines may break, cutting off the source, or the operator may forget to open one of the valves.

The guide words LESS OF, PART OF,and MORE THAN are all variations of the NONE and MORE OF guidewords. The NONE and MORE OF guidewords re the extreme scenarios for the former guidewords. Both the LESS OF and MORE THAN guide words would result in a change in the ratio of carbon to water, so changes in this ratio shall be examined.

When there is more carbon than water, there will be distribution problems. Pumps and lines will plug preventing the addition of activated carbon to the water. The effects of this scenario are the same as the no water condition. The events which would create an improper ratio are also either mechanical or human. Errors in the quantity of water added would be from an incorrect programming of the batch water controller, or the batch water controller failing. The solenoid valve may close prematurely or the manual valve may be closed before the addition of the make up water is finished.

The condition of less carbon to water is in effect considered by the more make-up water scenario developed through the MORE OF guide word.

Other Than

The OTHER THAN guide word is intended to generate those scenarios which occur during abnormal operations such as start up or shut down. These events are part of the event trees developed for both the storage tank and pumps (Figs. F.1.5, F.1.6). For the first scenario, the storage tank is running out of carbon so that the low level alarm sounds. The mixer and pumps eventually shut down, so that start-up is required. The second scenario represents only the procedure for the start-up of the pumps whether the shut down was manual or automatical. Many of the smaller events developed through the other guide words are represented in these event trees. This indicates the relationship between the different procedures.

Water Quality, Application of Activated Carbon

The same techniques were used for the frequency analysis of the activated carbon unit as for the chlorine unit. Design manuals and design guidelines were reviewed to develop possible failure rates for the equipment. Plant specific information from maintenance records and interviews with the operations and maintenance staff was also gathered.

When the preliminary investigation of the frequency analysis was completed, it was determined that the frequency analysis would not provide any useful information to the managerial, operations, or maintenance staff. The purpose of the frequency and consequence analysis is to provide a method for quantitatively comparing the risks and benefits of one or more proposed or existing designs. The technique was designed to highlight or emphasize areas which may have been considered completely improbable but are actually very realistic.

Many of the hazard scenarios are dealt with on a routine day to day basis. The failure rate of the pump starting is an important factor when trying to ensure the feeding of the carbon. The pumps fail to start nine times out of ten on the first try. Lines are continuously plugged. At least fifty percent of the time, the fixed PVC piping is bypassed with fire hoses so that feeding can continue.

The automatic batch water controller is unreliable up to forty percent of the time and must be continuously monitored to ensure that the correct quantity of water is added. The storage tank has been slowly filling from a water leak. This extra water changes the concentration of the carbon slurry.

The pumps chosen for the distribution are improperly sized. The pumps were designed for a higher carbon slurry concentration than is presently used (10%). However for the raw water pumpage flow rates, this concentration is too high for the minimum pump rates. Therefore a lower concentration of 4% is used. Chemical Detergent Method;
The pumps now wear out at a tremendous rate, with seventeen new stators being required in five months. The sampling points which are meant for the checking of the carbon concentration are used to verify that there is carbon flowing.

Obviously, a frequency analysis will not provide any new information. The basic assumption of a quantitative risk assessment is that the system is operating for its designed purpose. This system does not operate in its designed manner. Therefore, the frequency and consequence analyses were not performed on the hazard scenarios.

APPENDIX G

Alternate Cleaning Procedures for the Chlorine Feed System

1. Degrease with caustic, trisodium phophate, sodium metasilicate and a sufactant. Circulate mixture of chemicals through piping for two hours at 82 - 88°C.
2. If there are leaks, drain system and repair.
3. Recharge system with chlorine and hold at operating pressure for 24 h.
4. Drain gas, flush with fresh water.
5. Flush system with steam followed by air at 60°C. Continue air flush until air is at zero relative humidity at 1028 kPa.
6. Pressure test system with air or nitrogen at 2058 kPa.
7. Flush piping until pH is neutral.
8. Descale with inhibited hydrochloric acid at 65 to 70°C.
9. Flush system with citric flush.
10. Blow dry with nitrogen.

Pickling Method

1. If piping is assembled with welded steel fittings flush with strong caustic.
2. Pressurize with air to 2057 kPa, soap test and repair leaks. During pressure test isolate pressure gauges, pressure valves, rupture disks and pressure switches.
3. If air pressure is not suitable, a hydrostatic test can be don.
4. Pickle system by charging it with chlorine to normal

operating presure then check for leaks with ammonia.