

Spring 2005

Quantifying Vulnerability to Critical Infrastructure

Barry Charles Ezell
Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/emse_etds

 Part of the [Infrastructure Commons](#), [Operational Research Commons](#), and the [Systems Engineering Commons](#)

Recommended Citation

Ezell, Barry C.. "Quantifying Vulnerability to Critical Infrastructure" (2005). Doctor of Philosophy (PhD), dissertation, Mechanical Engineering, Old Dominion University, DOI: 10.25777/588y-yd09
https://digitalcommons.odu.edu/emse_etds/71

This Dissertation is brought to you for free and open access by the Engineering Management & Systems Engineering at ODU Digital Commons. It has been accepted for inclusion in Engineering Management & Systems Engineering Theses & Dissertations by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

QUANTIFYING VULNERABILITY TO CRITICAL INFRASTRUCTURE

by

Barry Charles Ezell

B.S. May 1988, University of Southern Mississippi

M.S. May 1998, University of Virginia

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirement for the Degree of

DOCTOR OF PHILOSOPHY

ENGINEERING MANAGEMENT

OLD DOMINION UNIVERSITY

May 2005

Approved by:

Charles B. Keating (Director)

Andres Sousa-Poza (Member)

Resit Unal (Member)

Willie J. McFadden II (Member)

ABSTRACT**QUANTIFYING VULNERABILITY TO CRITICAL INFRASTRUCTURE**

Barry Charles Ezell
Old Dominion University, 2004
Director: Dr. Charles Keating

Military and civilian leaders have the responsibility to protect our Nation's critical infrastructure, communities, and symbols of American power from terrorists, home and abroad, as well as from natural disasters. To this end, assessments are conducted to reduce vulnerability. The literature offers multiple definitions of vulnerability and measurement has not been adequately addressed. Thus, the purpose of this research has been to develop and deploy a systems-based model that quantifies vulnerability to critical infrastructure. This research defines critical infrastructure vulnerability as a measure of the susceptibility of critical infrastructure to threat scenarios. Vulnerability is a function of 1) threat scenario, 2) protection and 3) importance. Critical infrastructure vulnerability is measured by a system's 1) deterrence, 2) detection, 3) delay and 4) response capabilities. Importance implies that some subsystems are more critical to overall system performance than other subsystems. A value model was used as the logic construct for quantifying vulnerability. Subject-matter experts were queried to establish the shapes of value functions and importance (weights) in the model. Another set of subject-matter experts are queried to assess a notional clean water system with respect to each protection measure within the vulnerability value model. To accomplish this, two simulations are executed in the model. The first simulation aggregates expert assessments into one assessment. The results are then used as inputs into the vulnerability value portion of the model for use in the second simulation where vulnerability is quantified. Results of this

research demonstrate that vulnerability can be quantified and that quantifying vulnerability is useful to decision-makers who prefer quantification to qualitative treatment of vulnerability. This research is a novel contribution to the body of scholarly work by: 1) providing a rigorous method to quantify vulnerability to critical infrastructure, 2) introducing the theory of vulnerability, and 3) specifying the theoretical relationship between risk and vulnerability. Subject matter experts conclude that there is value in the approach put forward in this body of research as it is applied to clean water systems, so it may be useful in other critical infrastructures. The research closes with directions for further research.

This dissertation is dedicated to the men and women who protect our Homeland.

ACKNOWLEDGEMENTS

My inspiration to complete this dissertation and achieve a Ph.D. comes from God and I am thankful He guided me through some very tough times to see this thing through. Without His grace, the entire effort would have been futile.

Thank you Mike McGinnis who reminded me that Ph.D. stood for patience, humility, and discipline. Chuck Keating, my advisor has been a superb mentor, teaching me how to conduct rigorous research. Greg Parnell, thank you for being my friend and role model. Daniel Pinto, thank you for being my friend and believing in me. Martha McRavin-Oliver my leader in The Army School System (TASS) was tremendous support; thank you. Danny, Michael and Reagan, you are my sons and I wanted to set a good example. Never forget that dad's report card went up on the refrigerator right beside yours. Thank you for your support and understanding. Mom, I am grateful for you teaching me the value of hard work early in life. It served me well in this endeavor. I know dad would have been proud and I am sure he is pleased with my achievement in heaven. Sarah, my beautiful bride and friend, I will always appreciate how you stood by my side and supported me working the crazy hours and odd places (hotels, airplanes and airports) to get through this journey. You provided inspiration and helped me focus. You are a very bright light in my life.

PREFACE

Having been a part of the effort to protect our infrastructure for 18 years as a service member of the US Army and nine years of academic research directly related to finding ways to harden water and Supervisory Control and Data Acquisition (SCADA) systems, the author became interested in researching ways to quantify vulnerability to water systems. The author fully understands the sensitivity of addressing vulnerability in water and has proceeded in a responsible manner.

Whereas many vulnerability studies identify vulnerable points in the system, most are without quantifiable rigor. The author has seen first hand the frustration of military leaders who needed a way to quantify vulnerability to water systems to help make better force protection decisions. Sousa-Poza (2003) makes the point explicit in his socio-technical systems course that decision-makers in general prefer quantification.

Chapter I summarizes the purpose, questions, and significance of the research. Limitations and delimitations are presented to establish the context for this inquiry. Key concepts and definitions are also presented in Chapter I. Chapter II surveys the literature on vulnerability synthesizing definitions, methodologies and key concepts. The literature is partitioned into three literature domains: 1) risk, 2) vulnerability, and 3) critical infrastructure. The important point made in Chapter II is the gap in the literature with respect to quantifying vulnerability to critical infrastructure.

With the research context set and the gap in the literature identified, the dissertation focuses Chapter III on the research methodology and design. Chapter III is the centerpiece of the dissertation as it discloses the manner in which the research purpose is accomplished and the control measures in place to ensure validity. The

research methodology explains the manner in which data is linked, collected and validated, as well as how data may be aggregated for use in the vulnerability value model. Chapter IV is an application of the model to a water system. The results are presented in this chapter. Chapter V documents the contribution of the research to theory and practice. In addition, it describes many future concepts and examples of how this research may be used in other areas. This chapter provides examples of how the research might be used in conjunction with an index score for Homeland Security. The author hopes that Chapter V inspires future researchers to develop the ideas presented in this chapter. The consolidated references list is an additional benefit for the future researcher on vulnerability, infrastructure, and risk.

This research contributes to the body of knowledge in the discipline of risk analysis and infrastructure systems. By quantifying vulnerability using the value model described in this research, decision-makers will have a meaningful measure of vulnerability built upon the decision-makers' system of values.

TABLE OF CONTENTS

ABSTRACT.....	ii
ACKNOWLEDGEMENTS.....	vi
PREFACE.....	vii
LIST OF FIGURES.....	xi
LIST OF TABLES.....	xii
LIST OF TABLES.....	xii
LIST OF EQUATIONS.....	xiii
LIST OF EQUATIONS.....	xiii
CHAPTER I INTRODUCTION.....	1
Purpose of the Study.....	2
Research Questions.....	2
Definition of Key Concepts and Variables.....	4
Study Limitations and Delimitations.....	6
Significance of the Study.....	7
Summary.....	8
CHAPTER II LITERATURE REVIEW.....	10
Vulnerability Definitions, Concepts and Assessments.....	12
Classic Risk Assessment and the Concept of Vulnerability.....	18
Critical Infrastructure.....	20
Summary.....	23
CHAPTER III RESEARCH METHODOLOGY.....	26
Research Design.....	29
<i>Expert Elicitation</i>	31
<i>The Relationship: Vulnerability and Risk</i>	34
<i>Vulnerability Value Model Construction</i>	37
<i>Value Function Construction</i>	38
<i>Model Calibration</i>	42
<i>Model Sensitivity, Verification and Validation</i>	50
<i>Assessing (Scoring) the Clean Water System</i>	51
<i>Notional Medium Clean Water System</i>	52
Summary.....	54
CHAPTER IV RESULTS.....	57
Relative Importance Data.....	58
Value Functions.....	60
Scoring (Assessing) the Clean Water System.....	62
Aggregation of Scores.....	63
Sensitivity Analysis.....	71
Face Validity.....	75

Summary	76
CHAPTER V CONCLUSION.....	78
Significance.....	79
Discussion of Future Research.....	81
Vulnerability Index Score	82
Threat Scenarios.....	84
Summary	87
APPENDIX A (Glossary of Terms)	95
APPENDIX B SME-1 Interview Template and Notes	97
APPENDIX C SME-2 Establishing the Importance Weights	98
APPENDIX D SME-2 Establishing the Value Function.....	101
APPENDIX E SME-1 and -2 CWS Assessment	109
APPENDIX F SME-3 Weighting Factors (SME-1 and -2).....	113
APPENDIX G Face Validity of The Model	114
APPENDIX H Aggregation Assessments SME-1 and -2.....	115
APPENDIX I Vita.....	157

LIST OF FIGURES

Figure 1. Framework for Inquiry	4
Figure 2. Interaction Matrix among Critical Infrastructures.....	7
Figure 3. Streams of Literature	11
Figure 4. Extensive Size of US Water System	21
Figure 5. Function Flow Diagram of Water System.....	22
Figure 6. Research Design	30
Figure 7. Universe of Risk, A	36
Figure 8. Universe of Vulnerability, A	36
Figure 9. Value Model Structure	40
Figure 10. Deterrence Value Function Example.....	41
Figure 11. Protection Value Function Example.....	41
Figure 12. Delay Value Function Example.....	41
Figure 13. Response Value Function Example.....	41
Figure 14. Notional Clean Water System	56
Figure 15. Deter value function from SME-1	60
Figure 16. Detect value function for SME-1	60
Figure 17. Delay value function for SME-1	61
Figure 18. Response value function for SME-1.....	61
Figure 19. Sample from inner loop aggregation of SME-1 and SME-2.....	64
Figure 20. Ideal and Actual System Value	67
Figure 21. Source Subsystem Value	67
Figure 22. Transmit Subsystem Value.....	68
Figure 23. Treatment Subsystem Value.....	68
Figure 24. Storage Subsystem Value	69
Figure 25. Distribution Subsystem Value	69
Figure 26. Control Subsystem Value	70
Figure 27. System Distribution of Vulnerability (Ω).....	70
Figure 28. Latin Hyper-cube simulation of 15,000 trials.....	71
Figure 29. Output Sensitivity to Input Parameters.....	72
Figure 30. Vulnerability Index Score Model	83
Figure 31. Vulnerability Index Score.....	84

LIST OF TABLES

Table 1. Summary of Vulnerability Definitions	16
Table 2. System Functions	23
Table 3. Literature Review Matrix.....	25
Table 4. Determining Research Approach (Leedy and Ormrod 2001).....	28
Table 5. Value Model Structure.....	43
Table 6. Vulnerability Value Model Inputs and Calculation Matrix	45
Table 7. Model variables and parameters	47
Table 8. Relative Importance and Weights.....	58
Table 9. Summary of assessments for SME-1 and SME-2.....	62
Table 10. Input-output Data for the Vulnerability Value Model	65
Table 12. Sensitivity of Simulation Runs: Monte Carlo vs. Latin Hyper-cube.....	71
Table 13. Location of Sensitive Measures in the Model	73

LIST OF EQUATIONS

Equation 1. Additive Value Form	42
Equation 2. River Component Value (1.1.1)	48
Equation 3. River Component Vulnerability (1.1.1).....	48
Equation 4. Source Subsystem Value (1.1)	48
Equation 5. Source Subsystem Vulnerability (1.1).....	49
Equation 6. Overall Clean Water System Value Assessment.....	49
Equation 7. Expected Value of vulnerability.....	49

CHAPTER I

INTRODUCTION

Critical infrastructure protection is a very serious mission of the government with many civilian and military stake-holders. The customer is ultimately the people. This research concentrated on vulnerability to water systems, which is one of six infrastructures identified as absolutely critical in the 1998 government report entitled *Critical Foundations*. The report made explicit: 1) telecommunications, 2) energy, 3) banking and finance, 4) transportation, 5) water systems and 6) emergency services as *critical infrastructures*.

This research documents the confusion of terms and definitions of terms such as vulnerability, risk, hazard, assessment, and analysis. Vulnerability means different things to different people and organizations. This gap in the literature concerning vulnerability quantification was the motivation for the research questions: (1) What is vulnerability as it applies to critical infrastructure systems?, (2) How does risk and systems theory apply to critical infrastructure vulnerability?, (3) How can critical infrastructure vulnerability be quantified?, and (4) What results from the deployment of a systems-based model that quantifies vulnerability to a critical infrastructure such as a water system?

Chapter I is organized into six sections. The first section covers the study purpose. It makes the point that systems theory is used to inform the thinking in the research design but is not a literature stream in the research. Section two presents the research questions that will guide the inquiry. Section three introduces key concepts and variables that are germane to the research. Section four describes the research limitations

and delimitations. In essence, this section helps define the scope of the research. Section five presents the significance of the research. It shows just how important the research is by describing the original and significant contributions of the research. Chapter I concludes by summarizing the content of the chapter.

Purpose of the Study

The purpose of the study was to develop and deploy a systems-based model that quantifies vulnerability to critical infrastructure. Develop and deploy implies that a model was created and then applied to an existing infrastructure. The model is systems-based in its design because critical infrastructures are large-scale complex systems. Systems-based implies that systems theory was used to inform the vulnerability model development. However, systems theory as a body of literature is not being surveyed as a stream in the literature review. Instead, systems theory was used to support the perspective taken for model development. Furthermore, critical infrastructures are richly interconnected with society. Therefore, appreciation and understanding of the nature and relationships of the components, entities, and boundaries along with other system properties was critical to the research. Systems theory helps to understand the system in focus so that meaningful vulnerability quantification can be accomplished. To accomplish the study purpose, the research was guided by the research questions presented in the following section.

Research Questions

Figure one shows the framework inquiry for the study. There were two primary objectives guiding the research. The objectives were divided into two categories: *develop* and *deploy*. Under *develop* there were three questions. The first question was what is vulnerability as it applies to critical infrastructure systems? Based upon the literature

review the research developed the concept and definition of vulnerability as a key first step in exploration of the phenomenon. The research synthesized the known vulnerability literature as well as supplementing and complementing it with perspectives drawn from systems theory and the discipline of risk analysis. Response to the first research question clearly establishes the perspective, definition, and foundation of vulnerability necessary to deepen further exploration of the questions related to the phenomenon.

The second research question is how does risk and systems theory apply to critical infrastructure vulnerability? This study demonstrated and made explicit the utility of systems theory in modeling vulnerability as well as its relationship to risk. The relationship to risk was guided by the risk literature of Kaplan (1997); Kaplan, Zlotin, Zussman, and Vishnipolski (1999); and Kaplan, Haimes, and Garrick (2001).

The third research question is how can critical infrastructure vulnerability be quantified? Quantifying vulnerability was built upon the research of Keeney, R.L. (1992); Keeney, R.L. and Raiffa, H. (1993); and Parnell, G.S., Jackson, J.A., Jones, B.L., Lehmkuhl, L.J., Conley, H.W., and Andrew, J.M., (1998). Model decomposition is inspired by systems theory, guided by the research of Sage and Armstrong (2000), Haimes (1998) and Gibson (1991).

Deploy has one supporting question: what results from the deployment of a systems-based model that quantifies vulnerability to a critical infrastructure such as a water system? After applying the model to an infrastructure as a case application, the usefulness of the model is measured. The application of the model provides for a critical examination of the ability of the model to be employed in establishing vulnerability of

critical infrastructure. Although this model deployment is limited, it does serve as an initial attempt to build credibility for the model's utility.

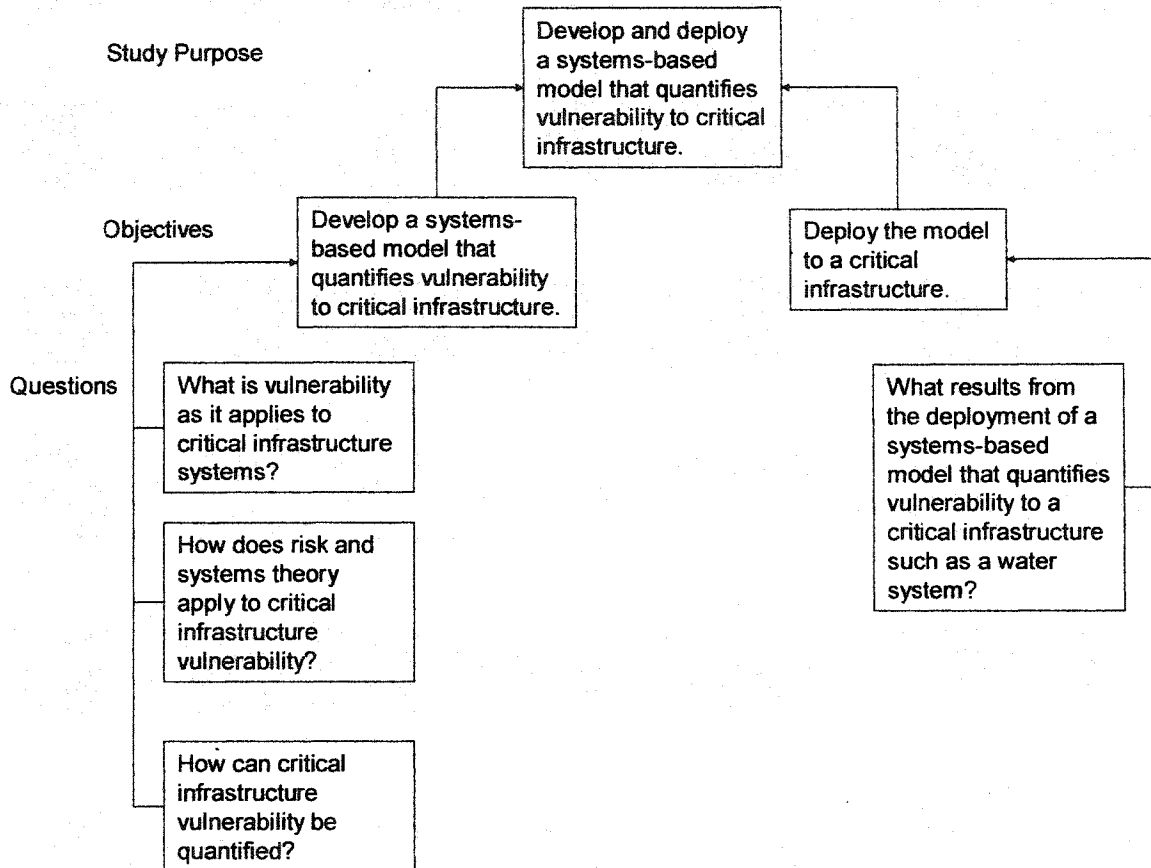


Figure 1. Framework for Inquiry

Definition of Key Concepts and Variables

While many definitions of infrastructure are explored in Chapter II, this research was guided by the definition provided in the Presidential Decision Directive 63 (p. 1, 1998) as “those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both

governmental and private”. Of these six critical infrastructures the scope of this research focuses exclusively on water systems.

In a similar fashion, vulnerability is defined in many different ways and those definitions are explored in Chapter II. For the purpose of this research, critical infrastructure vulnerability was defined as a measure of the susceptibility of critical infrastructure to threat scenarios. Furthermore, this research asserts that critical infrastructure vulnerability is a function of threat scenario, protection, and importance. Threat scenarios are guided by the research of Kaplan (1997); Kaplan, Zlotin, Zussman, and Vishnipolski (1999); and Kaplan, Haimes, and Garrick (2001). Vulnerability is measured by a system’s deterrence, detection, delay and response capabilities. Importance implies that some subsystems are more critical to overall system performance than other subsystems.

A key concept of this research is the relationship between risk and vulnerability. Exploring this concept became apparent due to the confusion of terms in the academic literature. This research asserts that the threat scenario is the link between risk and vulnerability. Chapter III describes these relationships in detail. Kaplan’s (1997) foundational paper on the quantitative definition of risk defines a risk triplet (scenario, likelihood, consequence) and his work guided the development of the vulnerability triplet: threat scenario, protection, and importance.

Omega (Ω) is the output variable of interest in this research. Omega (Ω) is the vulnerability value calculated by the vulnerability value model described in Chapter III. Model parameters are variables that are assigned by subject-matter experts: threat scenarios (s), protection (p), and importance (w).

Study Limitations and Delimitations

The major limitation of this research is that it addresses one critical infrastructure, water supply. Therefore, extension of this research beyond water systems to other critical infrastructures cannot be directly established from the research. Another limitation to this research is that it focuses on a medium sized clean water system. In addition, the generalizability of research findings beyond a water supply system must be questioned because the study was not based on a large population (Palmquist 2003; Creswell 1994). This implies that if a future researcher attempts to generalize the results of this research beyond the original context, the research findings may have questionable applicability. The implication of this limitation suggests that this research will not show generalizability beyond the chosen critical infrastructure of water supply. The transferability of the research methodology, methods, and model is an important aspect of this study, but cannot be directly established beyond applicability to contextually similar water systems. The value model developed for this research represents the values of the subject-matter expert who assigned the weights and shape of value functions. Great care was taken in validating the parameter settings for the model, to account for subject-matter expert values expressed in the model. The qualifications of subject matter experts were rigorously established for this research to minimize the impact of this limitation.

This research did not apply the model to every type of infrastructure. Instead, the research confines itself to one water supply case study and known decomposition supported by the literature (American Water Works Association 2002). The research does not present a new methodology. In addition, the research does not address the interaction between the infrastructures but acknowledges interaction exists (figure 2). In

addition, the model does not address interdependencies within the structure or between infrastructures.

	1.0 Water	2.0 Energy	3.0 Emergency Service	4.0 Banking & Finance	5.0 Telecommunication	6.0 Transportation
1.0 Water		+	+	-	+	-
2.0 Energy			+	-	+	-
3.0 Emergency Service				-	+	-
4.0 Banking & Finance					+	-
5.0 Telecommunication						-
6.0 Transportation						

Figure 2. Interaction Matrix among Critical Infrastructures

Although threat scenarios are shown to be the link between risk and vulnerability, this research does not inject threat scenarios into quantifying vulnerability. This was deemed beyond the scope of this research and not required to quantify vulnerability of a clean water system. A rich discussion on how future researchers might accomplish this is presented in Chapter VI.

In summary, this section presented the limitations and delimitations in the research. The limitations and delimitations have been considered, were reasonable, and did not affect the ability to respond to the research questions.

Significance of the Study

Quantifying vulnerability to clean water systems is a significant contribution because the US alone has 54,000 systems providing water to 263 million customers (American Water Works Association (AWWA) 2002). This research contributed to the body of

knowledge by reviewing and then synthesizing the limited literature on vulnerability. Contributions were organized into two domains: academic and practical (DOD, governments, and private industries). Academic contributions include a systems-based vulnerability model that quantifies vulnerability for a critical infrastructure, new theory of vulnerability, and the relationship of risk and vulnerability made explicit. This is significant because up to this point, no one has quantified vulnerability. This research fills that gap using the value model as the construct for quantifying vulnerability, discussed in chapter III as the Omega Value. This research shows how one can assess the system and measure its performance compared to the ideal system Omega value of vulnerability. Practical implications of the research include providing decision-makers with a model to help them understand system vulnerability so that resources can be allocated in a meaningful way. The Omega value of vulnerability accomplishes this need because as the user makes changes, the model can be ran multiple iterations to see first hand how vulnerability may be reduced. Practitioners will be provided with the model and the references that allow them to conduct their own analysis.

Summary

Chapter I identified the framework and the supporting research questions: 1) what is vulnerability as it applies to critical infrastructure systems?; 2) how does risk and systems theory apply to critical infrastructure vulnerability?; and 3) how can critical infrastructure vulnerability be quantified? Next, the significance of the research was identified by the fact that quantifying vulnerability in a rigorous manner was missing from the literature. Limitations and delimitations were presented that narrowed the scope to water systems. In addition, chapter I outlines the content and flow of the dissertation. Chapter I makes explicit the relationship between risk and vulnerability. Chapter I

concluded by detailing the novel contributions of theory and vulnerability quantification and summarizing the chapter. In the following chapter, the literature review is presented.

CHAPTER II

LITERATURE REVIEW

The purpose of this chapter is to review, synthesize, and criticize the literature that describes what is known regarding vulnerability. The first section explores the many definitions and conceptual idea and definitions on vulnerability, vulnerability assessment, and quantification of vulnerability. Section two provides a brief overview of critical infrastructure and a working definition of critical infrastructure. Section three describes classic risk analysis and the manner in which the term vulnerability is viewed. Section four discusses the use of systems theory in the representation of critical infrastructure using foundational concepts to guide the construction of a critical infrastructure from a systems point of view. The final section summarizes the chapter, and the significance of the literature review.

Building a model to quantify critical infrastructure vulnerability involves the literature domains of risk, infrastructure, systems, and decision science. Chapter II systematically navigates through the literature streams of vulnerability and critical infrastructure to understand the current state of knowledge for vulnerability. The discipline of quantitative risk analysis is explored to understand the literature concerning the relationship between risk and vulnerability. This is important because literature review of infrastructure indicates significant differences in the definition of vulnerability. Systems, decision sciences, and risk literature are used in Chapter III to support model construction. Using expert elicitation and aggregation involves the decision sciences (Chytka 2003). Value models in their design and deployment are also a part of the decision science and systems literature. Chapter III uses decision sciences, risk, and

systems literature in the construction of the vulnerability value model. Government literature is also important because most of what is actionable in the study of vulnerability is in the government literature. As indicated in Figure 3, no significant research has been published on quantifying vulnerability. Also, the risk literature provides no research on the operational definition of vulnerability. Although critical infrastructure literature describes studies on infrastructures, this literature is silent when it comes to quantifying vulnerability. The current literature is poised to fill the gap (as indicated by the dotted line in Figure 3) between vulnerability, critical infrastructure, and risk.

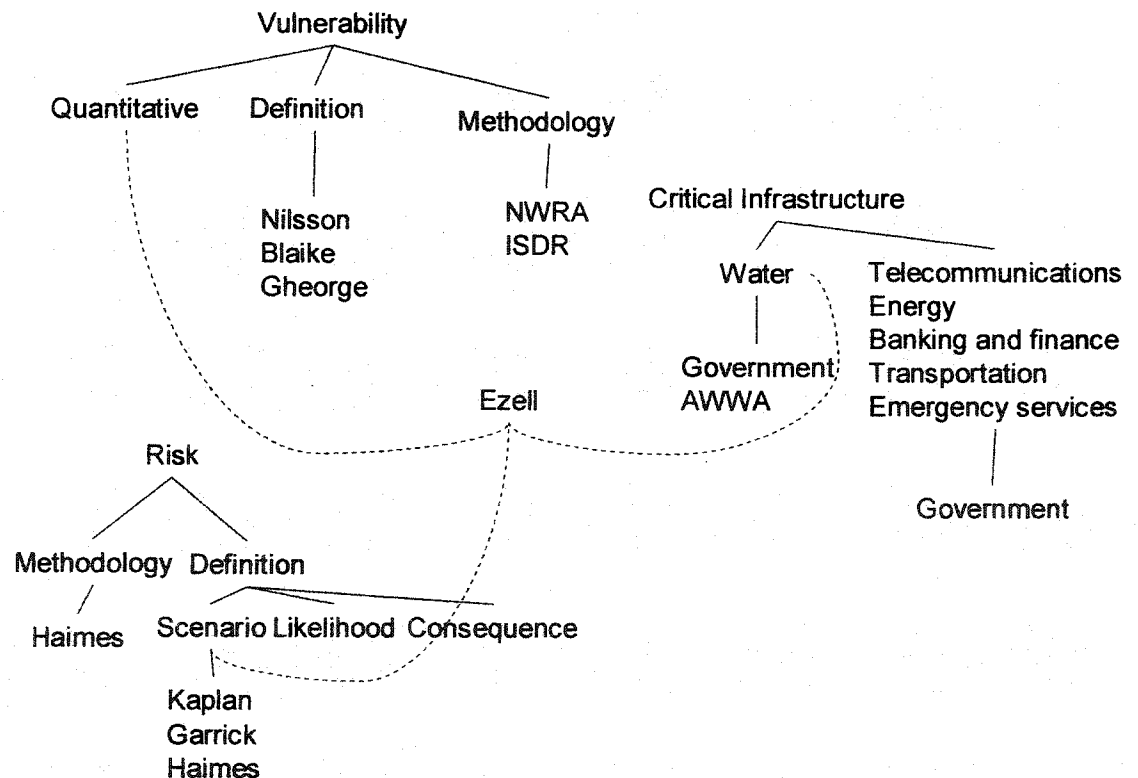


Figure 3. Streams of Literature

Vulnerability Definitions, Concepts and Assessments

Literature review indicates many views on vulnerability. There is significant confusion in the use and meaning of terms such as vulnerability, risk, hazard, assessment, and analysis. Buckel (2000) contends that work must be done to clear up the definition of vulnerability with respect to risk. For example, Emergency Management Australia (1998) defines vulnerability as the degree of susceptibility and resilience of the community and environment to hazards. Likewise, the Emergency Management Australia (1998) glossary of terms interchanges the terms vulnerability analysis with hazard *analysis* or vulnerability *assessment*. NWRA (2002) defines a vulnerability assessment as the identification of weaknesses in security, focusing on defined threats that could compromise its ability to provide a service. Blaike et al. (p. 4, 1994) defines vulnerability as “the characteristics of a person or group in terms of their capacity to anticipate, cope with, resist, and recover from the impact of a natural hazard”. The National Oceanic and Atmospheric Administration (2002) views vulnerability as “susceptibility of resources to negative impacts from hazard events”. Nilsson et al. (2001) contend that vulnerability is the collective result of risks and the ability of a society, local municipal authority, company or organization to deal with and survive external and internal emergency situations. Gheorghe (2001) defines vulnerability as the susceptibility and resilience/survivability of the community / system and its environment to hazards. Vulnerability is a function of susceptibility, resilience and the environment. International Strategy for Disaster Reduction (2002) defines vulnerability to disasters is “a status resulting from human action. It describes the degree to which a society is either threatened by or protected from the impact of natural hazards”. NSTAC- National

Security Telecommunications Advisory Committee (1997) is credited for claiming that vulnerability is really a function of access and exposure, whereas dictionary.com (2000) views vulnerability as susceptibility to attack.

Other uses of vulnerability can be found in the literature. The National Security Telecommunications Advisory Committee (NSTAC) (1997) presents a view stating that vulnerability may be viewed as access and exposure. Nilsson, Magnusson, Hallin, and Lenntorp (2000) investigate and present methods suitable for analyzing and auditing municipal vulnerability. Nilsson, Magnusson, Hallin, and Lenntorp (2000) propose models by which it may be possible to distribute financial support to municipalities for their work on reducing vulnerability in the most cost-effective way. Vulnerability exists as a result of a collection of risks and the ability of a society, local municipal authority, company or organization to deal with and survive external and internal emergency situations. In both definitions and uses above, vulnerability is not anchored to any literature. In the following paragraph, references are found in the literature that begin to measure vulnerability or at a minimum, suggest a scale or direction of attainment. Buckle (2000) says that vulnerability is a broad measure of the susceptibility to suffer loss or damage. The higher the resilience, the less likely damage may be, and the faster and more effective recovery is likely to be. Conversely, the higher the vulnerability, the more exposure there is to loss and damage. Andreas, Wenger and Dunn (2002) developed a handbook compiling risk analysis strategies used by eight countries for critical infrastructure protection. Organizations such as Association of State Drinking Water Administrators National Rural Water Association (2002) have developed self-assessment vulnerability checklists as well as American Water Works Association

(AWWA). In a similar fashion, academic literature and government reports address vulnerability as a step in risk assessment.

Sandia National Laboratories presents a high-level discussion on water system vulnerability for local, state and federal risk practitioners. However, Sandia National Laboratory has not shared its vulnerability assessment methodology to date. Hierarchical Holographic Modeling (Haimes 1981) was used to identify sources of risk and indirectly imply systems vulnerabilities (Ezell, Haimes and Lambert 2000). The Infrastructure Risk Analysis Model (IRAM) introduced by Ezell, Farr, and Wiese (2000a) mathematically modeled vulnerability as simply a function of access and exposure, building upon NSTAC's (1997) ideas of access and exposure. For instance, in water systems, exposure was equivalent to visibility. Water towers, treatment plants, and pump stations are examples of highly visible components. There have been few attempts to address vulnerability either by defining or developing checklists within the context of its use. Ezell, Farr, and Wiese (2000a) introduce the Infrastructure Risk Analysis Model and apply it in a companion paper to a small community's water supply system. It is the first documented attempt in the literature to quantify vulnerability. The focus of this research centered on systems decomposition to facilitate subjectively rank ordering vulnerability based on exposure and access control. For example, a water system may be described in terms of components, elements, modes, or human interactions that satisfy an array of functions such as gather, transmit, and deliver. Within the current context of IRAM a system is decomposed into components and subjective ad hoc decisions are made concerning what sources vulnerabilities to model (Ezell 2000a). Vulnerabilities are a function of access α_i and exposure γ_i , where vulnerability of a component or subsystem

is defined as $v_i = \alpha_i \gamma_i$, where α_i and γ_i are subjectively scaled $0 < \alpha_i < 1$ and $0 < \gamma_i < 1$.

A low vulnerability score for a component is an advantage. The total vulnerability of the system is a simple summation of all systems vulnerability scores. The total vulnerability

of the system is $V = \sum_{i=1}^n v_i$. This expression, however, fails to account for the various

differences in system size, complexity, and number of components. It does not include

many other factors such as people or context. The system boundary for the IRAM model

omits many items that touch the system. Also, IRAM does not address the relative

differences between systems. For instance, any large system's vulnerability score will

always be larger than a smaller system due to the number of components. Additionally,

there exist issues with the boundary of critical infrastructure if the boundary simply lies

around components from the perspective of access and exposure. With the exception of

IRAM, no paper quantifies vulnerability and yet IRAM fails to consider many attributes

available in the literature.

In conclusion, IRAM inability to account for relative scores from an idealized score or assessments between systems seriously diminishes its contribution to quantify

vulnerability in a manner that can be useful beyond the system it was applied to. And,

given that there is no upper bound on score, prevents the user from comparing scores

between systems of different sizes and complexities.

The definitions given in the literature addressing vulnerability appear to fall into

one category: nominal. Babble (2001) distinguishes three types of definitions: real,

nominal, and operational. "Real" definitions are difficult because one tries to develop a

concrete statement that captures the essential and pure elements and attributes of

something real. For many, an attempt to view an abstraction as if it had material

existence is unattainable. Therefore, concepts in scientific inquiry rely upon nominal and operational definitions. The literature does not support the conclusion that an operational definition of vulnerability exists and therefore it is presently [un]measurable. The problem with nominal definitions as Babbie (2001) explains is that the definition is one that is assigned to a term without any claim that the definition represents a real entity. Simply put, nominal definitions are arbitrary. Definitions of vulnerability in the literature review appear to fall in the nominal category. Operational definitions are nominal and not real. Yet, operational definitions achieve clarity about the meaning of the concept and in the context of a given study (Babbie 2001). It is important to note that the various definitions of vulnerability presented in this chapter do not share the same underlying context. Each definition has been tailored for a particular concept in mind and within a certain context. Table 1 below summarizes the definitions from the literature review.

Table 1. Summary of Vulnerability Definitions

Author	Vulnerability Definition and Uses in the Literature
Blaike et al. (1994)	A characteristics of a person or group in terms of their capacity to anticipate, cope with, resist, and recover from the impact of a natural hazard
Association of State Drinking Water Administrators National Rural Water Association (2002)	Developed self-assessment vulnerability checklists as well as American Water Works Association (AWWA)
Buckle (2000)	A broad measure of the susceptibility to suffer loss or damage. The higher the resilience, the less likely damage may be, and the faster and more effective recovery is likely to be. Conversely, the higher the vulnerability, the more exposure there is to loss and damage
Dictionary.com (2000)	susceptibility to attack
Emergency Management Australia (1998)	The degree of susceptibility and resilience of the community and environment to hazards.

Author	Vulnerability Definition and Uses in the Literature
Gheorghe (2001)	The susceptibility and resilience/survivability of the community / system and its environment to hazards. Vulnerability is a function of susceptibility, resilience and the environment.
International Strategy for Disaster Reduction (2002)	A status resulting from human action. It describes the degree to which a society is either threatened by or protected from the impact of natural hazards.
National Oceanic and Atmospheric Administration (2002)	Susceptibility of resources to negative impacts from hazard events.
Nilsson et al. (2001)	The collective result of risks and the ability of a society, local municipal authority, company or organization to deal with and survive external and internal emergency situations.
Nilsson, Magnusson, Hallin, and Lenntorp (2000)	Vulnerability exists as a result of a collection of risks and the ability of a society, local municipal authority, company or organization to deal with and survive external and internal emergency situations.
National Security Telecommunications Advisory Committee (1997)	A function of access and exposure. NSTAC (1997) argues that vulnerable systems are systems that are exposed and, accessible and therefore susceptible to natural hazards as well as willful intrusion, tampering, or terrorism.
National Waterworks of Rural America (2002)	Vulnerability assessment is the identification of weaknesses in security, focusing on defined threats that could compromise its ability to provide a service.
Ezell et al. (2000)	The Infrastructure Risk Analysis Model (IRAM) mathematically modeled vulnerability as a function of access and exposure, building upon NSTAC's (1997) ideas of access and exposure.

Seven references: Buckle (2000), Dictionary.com (2000), Emergency Management of Australia (1998), Gheorghe (2001), International Strategy for Disaster Reduction (2002), National Oceanic and Atmospheric Administration (2002), and the National Security Telecommunications Advisory Committee (1997) use the adjective “susceptibility to...” to define vulnerability. Four references: Blaike et al. (1994),

Nilsson et al. (2001), Nilsson, Magnusson, Hallin, and Lenntorp (2000), and the National Waterworks for Rural America (2002) use the adjectives cope and deal with to define vulnerability. Two definitions provided by Nilsson et al. (2001) and Nilsson, Magnusson, Hallin, and Lenntorp (2000) view vulnerability as a collection of risks. Ezell et al (2000a) builds upon NSTAC (1997) notion of access and exposure and identify that some subsystems and components are not equally important. Subsystems and components can be assessed by their relative importance and protected. The literature on vulnerability does not support the notion that definitions build upon one another. But from what is in the literature a theme begins to emerge in the attributes that describe vulnerability: susceptibility to “what”; weakness in the system; a target with respect to a threat or risk; exposure to hazard. These concepts are more completely defined in the risk literature presented in the following section.

Classic Risk Assessment and the Concept of Vulnerability

Risk assessment methodologies are often employed to help understand what can go wrong, estimate the likelihood and the consequences, and to develop risk mitigation strategies to counter risk. One critical component of risk assessment methodology is determining the vulnerability of a system (Ezell et al. 2000a, 200b). Blaike (1994), Buckle (200a,b), NOAA(2002) indicate a link the concept of vulnerability and risk. However, foundational definitions such as Lowrance’s (1976), defines risk as a measure of the probability and severity of adverse effects whereas Blaike (1994), Buckle (2000a, 2000b), NOAA (2002) suggests vulnerability is *susceptibility* to risk. Kaplan (1997) said that risk was a triplet of scenario, likelihood, and consequences. The difference between Lowrance (1976) and Kaplan (1997) is the notion of scenario(s) as a euphemism for

“what can go wrong”. NSTAC (1997) argues that vulnerable systems are systems that are exposed and, accessible and therefore susceptible (NOAA 2002) to natural hazards as well as willful intrusion, tampering, or terrorism. Therefore, a relationship emerges from the literature between vulnerability and risk. Vulnerability highlights the notion of susceptibility to a scenario whereas risk focuses on the severity of consequences to a scenario. The following paragraph discusses scenarios and Chapter III formalizes the relationship between vulnerability and risk.

Scenario appears in risk and vulnerability literature. A scenario is defined as an outline, script, or sequence of events (dictionary.com, 2003). In the discipline of risk analysis, scenarios were made explicit by Kaplan and Garrick (1981); Kaplan, Zlotin, and Vishnipolski (1999); and refined by Kaplan, Haimes and Garrick (2001).

Fundamental to the theory of scenario structuring is the requirement that scenarios be (1) complete, (2) finite, and (3) disjoint. In Kaplan and Garrick (1981) the authors point out that scenario was loosely defined as “What can go wrong?” In Kaplan, Haimes and Garrick (2001) the authors attempt to bridge Hierarchical Holographic Modeling (HHM) Haimes (1981) with the theory of uncertainty. The approach focuses on using the philosophy of HHM to holistically identify sources of risk from multiple perspectives: functional, temporal, and geographical. The authors then introduce rate and weight methodologies to arrive at a subset of scenarios from which to proceed. However, the authors do not address how one explicitly defines a scenario, nor the limit of the universal set of all risks and scenarios. In fact, even if one satisfies the criteria above, the essential components of the scenario remain an open question in the literature.

Literature review indicates that vulnerability is not defined explicitly in the risk literature, yet there are similar themes of scenario used in risk and vulnerability. Vulnerability emphasizes susceptibility to a scenario and risk highlights the severity of consequences to a scenario. The literature also highlights that certain subsystems and components are relatively more important to other components and subsystems performance of its overall purpose. Last, the literature shows that these susceptible components and subsystems need protection from threat scenarios. In the following section, the infrastructure literature is reviewed to understand what is meant by critical infrastructure with an emphasis on water systems.

Critical Infrastructure

Military and civilian leaders (i.e. decision makers) have the responsibility to protect our Nation's critical infrastructure, communities, and symbols of American power from terrorists, home and abroad, as well as from natural disasters. For the purpose of this research critical infrastructure is defined as "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private" (PDD 63, p. 1, 1998).

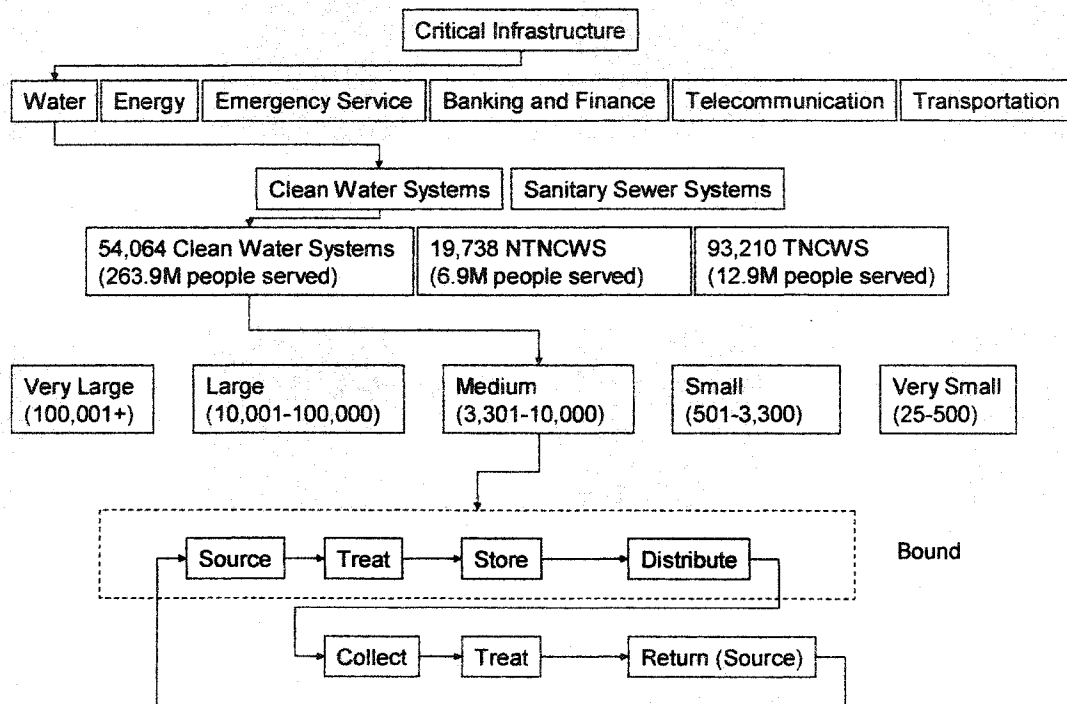


Figure 4. Extensive Size of US Water System

This research focuses on the water system as a critical infrastructure. To understand the magnitude of this critical infrastructure, consider the number of utilities and customers per infrastructure sector. There are 54,064 clean water systems in the United States, serving 264 million Americans (CDI 2002). Figure 4 provides a sense of the scope of water systems as an extraordinarily large critical infrastructure. A water system can be decomposed into two distinct systems, clean water and sanitary sewer systems. A clean water system has seven main functions in the process flow (AWWA 2002b): 1) water arrives from a source; 2) pumped from a well, river, etc. to a treatment plant; 3) treatment plant removes impurities; 4) clean water is stored in tank; 5)

distribution mains carry clean water to industry and service lines; 6) service lines carry water to homes; and 7) from industry and homes, water enters the sanitary sewer system. The sanitary sewer system sewer lines carry water to a sewage treatment plant. After cleansing, water is returned to the source such as river where the Earth continues the cleansing process (AWWA 2002b). In conclusion, Figure 5 and the section above explains the size of the critical infrastructure and its significance in this research.

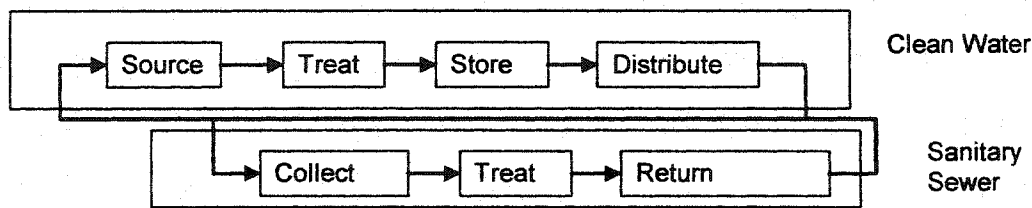


Figure 5. Function Flow Diagram of Water System

Table 2 summarizes the functions of a water system and a brief description of each function (AWWA 2002b and Reynolds 2004). These functions become important in Chapter III, as the decomposition readily identified and understood in the literature in used in the research design in Chapter III. Table 3 is a matrix of literature that summarizes the contributions of authors and the subject which each author addressed. Along the left column of the table research questions are listed. Along the top of the matrix, authors are listed. Within the body of the matrix, an “X” indicates that the author’s research and that characteristic/element addressed in their work. An “X” under Ezell (2004) indicates the areas in which this research supplemented and complimented the body of scholarly research. In the case research has not been previously conducted, this research fills the following gaps: 1) vulnerability is defined explicitly; 2) the application to critical infrastructure is shown; 3) vulnerability is quantified; 4) a theory of

vulnerability is presented; 5) the relationship between vulnerability and risk is made explicit; and 6) an application of the model's ability to quantify vulnerability to a critical infrastructure is presented.

Table 2. System Functions

Number	Name	Description
1.1	Clean Water System	Source, Transmission, Treatment, Storage, Distribution, Use, Communication, and Control
1.1.1	Source water	Watersheds and surface water sources, Reservoirs and dams, Groundwater sources, Wells and galleries
1.1.2	Transmission system	Intake structures, Aqueducts, Pump stations, Pipelines, Valves
1.1.3	Treatment facilities	Facility structures (buildings, basins, and tanks), Controls (manual and computer), Equipment (feeder, pumps, and piping), Treatment chemicals and storage
1.1.4	Finished water storage	Clearwells, Tanks, Elevated tanks, and Reservoirs
1.1.5	Distribution system	Pipelines, valves, fire hydrants; Pump or pressure-reducing stations; Materials (extra pipe, valves, hydrants, etc.); Meters, meter boxes, and pits; Cross-connection-control and backflow-prevention devices
1.1.6	Use	Home, Industry
1.1.7	Communications	Telephone, Radio, Internet/intranet
1.1.8	Control	SCADA or Telemetry

Summary

This chapter has shown the gap in the literature on vulnerability defined operationally (Babbie 2001) and the lack of any model to quantify vulnerability. In addition, the literature shows the significance of critical infrastructure and the massive size of just one infrastructure: water supply. Although there have been attempts to quantify vulnerability, they have not been as robust or rigorous in their formulation as this research. Ezell and Farr (2000a, 2000b) attempted to quantify vulnerability, yet the approach omits many of the attributes of vulnerability pointed out by NSTAC (1997),

NOAA (2002), Baike (1994) and Buckle (200a,b). Kaplan (1997), Kaplan and Garrick (1981); Kaplan , Zlotin, and Vishnipolski (1999) and Kaplan, Haines and Garrick (2001) research on the quantitative definition of risk and specifically the notion of scenario is very significant to this research because scenario is identified in Chapter III as the link between risk and vulnerability. For the remainder of this dissertation, critical infrastructure vulnerability is defined as the susceptibility of the infrastructure to threat scenarios. This research filled the gap in the vulnerability literature. Specifically, this research defined and quantified vulnerability with a systems perspective and in a manner that can was modeled and measured. Second, the vulnerability model was applied to a critical infrastructure (clean water system). Third, vulnerability theory was induced from the literature that made explicit the relationship between risk and vulnerability. In Chapter III, the research methodology is presented. It provides the research design and manner that data will be collected, analyzed and interpreted.

Table 3. Literature Review Matrix

	Blaike (1994)	ANRU (2002)	EMA (1998)	Ezell (2000a)	Ezell (2000b)	Gheorghe (2001)	Haines (1981)	ISDR (2002)	Nilsson (2002)	NOAA (2002)	NSTAC (1997)	NWRA (2002)	Sandia (2001)	Ezell (2004)
Definition of Vulnerability	x		x	x		x		x		x	x		x	x
Vulnerability Assessment Methodology			x		x							x	x	
Application to Critical Infrastructure		x			x		x		x				x	x
Quantification of Vulnerability					x									x
Vulnerability Quantification Model Deployment														x
Theory of Vulnerability														x
Vulnerability and Risk Analysis				x	x					x				x

CHAPTER III

RESEARCH METHODOLOGY

The purpose of this chapter is to detail the research methodology and design. The chapter is comprised of six sections. The first section is the research design. It explains the form of the design and how the author arrived at the type of research. The chapter transitions to expert elicitation in the second section and how experts were used in the design. In this section, the details for how experts' assessments are combined to facilitate data for the modeling of vulnerability are explained. In the third section of the chapter, the relationship between risk and vulnerability is disclosed. The threat scenario is shown to be the relationship and the link between risk and vulnerability. The fourth section describes the construction of the vulnerability value model. The components of the construction and value functions are discussed. In addition, the section describes how the model calculates vulnerability. In the final section, model calibration, verification and validation are explained.

This research was not exclusively qualitative. For research question number three (How can critical infrastructure vulnerability be quantified?) it was determined that a quantitative approach was more appropriate to answer this question, based on the analysis in Table 4 below. Also, qualitative designs are more focused on process (Creswell, 1994) and in this research, the outcome of the model was more important as identified as a gap in the literature from Chapter II. The design explained further in the chapter dictated quantification. Sensitivity analysis was required to understand parameter and model

sensitivity. In addition, aggregation of subject-matter experts scoring required quantification because many of the scores were of the form consistent with the work of Chytka (2003): pessimistic, most likely, and optimistic; and modeled using the triangle distribution. Qualitative research methodology was used in the inductive process of developing a model for vulnerability and a critical step in the development of a theory of critical infrastructure vulnerability.

Chapter III describes the mixed research methodology that was used during this research. As the methodology is explained, literature was used to support the design decisions that were made concerning the details of the approach. The entire research design is outlined in Figure 6. The research design explains the research approach that guided the inquiry. It includes concepts and details and required steps in the execution of the research. Creswell (p. 146, 1994) maintains that “one of the chief reasons for conducting a qualitative study is that the study is exploratory; not much has been written about the topic or population being studied, and the researcher seeks to listen to informants and to build a picture based on their ideas”. In the pursuit of defining critical infrastructure vulnerability, it became obvious that exploration was needed. Leedy and Ormrod (2001) provided guideline questions about research and then two columns for quantitative and qualitative approach, Table 4. The author’s analysis is indicated by an asterisk (*) and the mix of qualitative and quantitative becomes apparent for this research. Although Creswell (1994) advises that one should avoid a mixed approach, Rogers (2002) maintains that one should allow the problem type to drive the approach. The first question: “what is the purpose of the research?” the literature was used qualitatively to describe and explain vulnerability’s definition and relationship to risk.

Although a complete theory of vulnerability was not accomplished, the literature and model development discussed later in the chapter begins to infer a theory to build upon in future research. The second question “what is the nature of the research?” the literature combined with the author’s systems engineering and risk analysis background concluded that the research was holistic, included context, and held personal view due in large part to research conducted in Ezell et al. (2000a, 2000b). The third question from Table 4 was “what are the methods of data collection?” Given that most of what is known on vulnerability as indicated in Chapter II was in the literature, observations and interviews became apparent to further understand vulnerability. The form of reasoning was both inductive to build the relationship of vulnerability and risk, as well as the definition and model of vulnerability, whereas the output from the model was studied by deductive analysis. Finally, the findings were communicated in two ways, through interviews and literature as well as the quantified output from the model. For these reasons, a mixed approach was necessary and appropriate.

Table 4. Determining Research Approach (Leedy and Ormrod 2001)

Question	Quantitative	Qualitative
What is the purpose of the research?	<ul style="list-style-type: none"> • To explain and predict • To confirm and validate • To test theory 	<ul style="list-style-type: none"> • To describe and explain* • To explore and interpret • To build theory*
What is the nature of the research process?	<ul style="list-style-type: none"> • Focused • Known variable • Established guidelines • Static design • Context free • Detached view 	<ul style="list-style-type: none"> • Holistic* • Unknown variables • Flexible guidelines • Emergent designs • Context-bound* • Personal view*
What are the methods of data collection?	<ul style="list-style-type: none"> • Representative, large sample • Standardized instruments 	<ul style="list-style-type: none"> • Informative, small sample* • Observations, interviews*

<u>Question</u>	<u>Quantitative</u>	<u>Qualitative</u>
What is the form of reasoning in the analysis?	<ul style="list-style-type: none"> • Deductive analysis* 	<ul style="list-style-type: none"> • Inductive Analysis*
How are the findings communicated?	<ul style="list-style-type: none"> • Numbers* • Statistics, aggregated data* • Formal voice, scientific style 	<ul style="list-style-type: none"> • Words* • Narratives, individual quotes* • Personal style, literary style

Research Design

This research focused on using the literature to qualitatively infer the definition of vulnerability, then transitioned to quantifying vulnerability to a clean water system. This research design was type one holistic, single case design (Yin 1984) where the unit of analysis was one medium-sized clean water system. The research design was holistic in that it considered an entire water system. The research was a single case in that it focused on one application to a clean water system to demonstrate the model's ability to quantify vulnerability. To achieve this design, critical infrastructure vulnerability was defined in an operational way as described in the previous section.

In the following sections of chapter III, interview and survey instruments, data collection and analysis plan, and interpretation are described. The research design used the literature as the basis for choices made. The following sections identify expert criteria used and the manner in which subject-matter experts are employed in the research. Critical infrastructure vulnerability is defined showing that the conceptual and mathematical relationship of vulnerability and risk is the threat scenario. The final section in this chapter details the barriers to the research and what was done to mitigate those barriers. Each step in the design is shown in Figure 6 and described in each corresponding section.

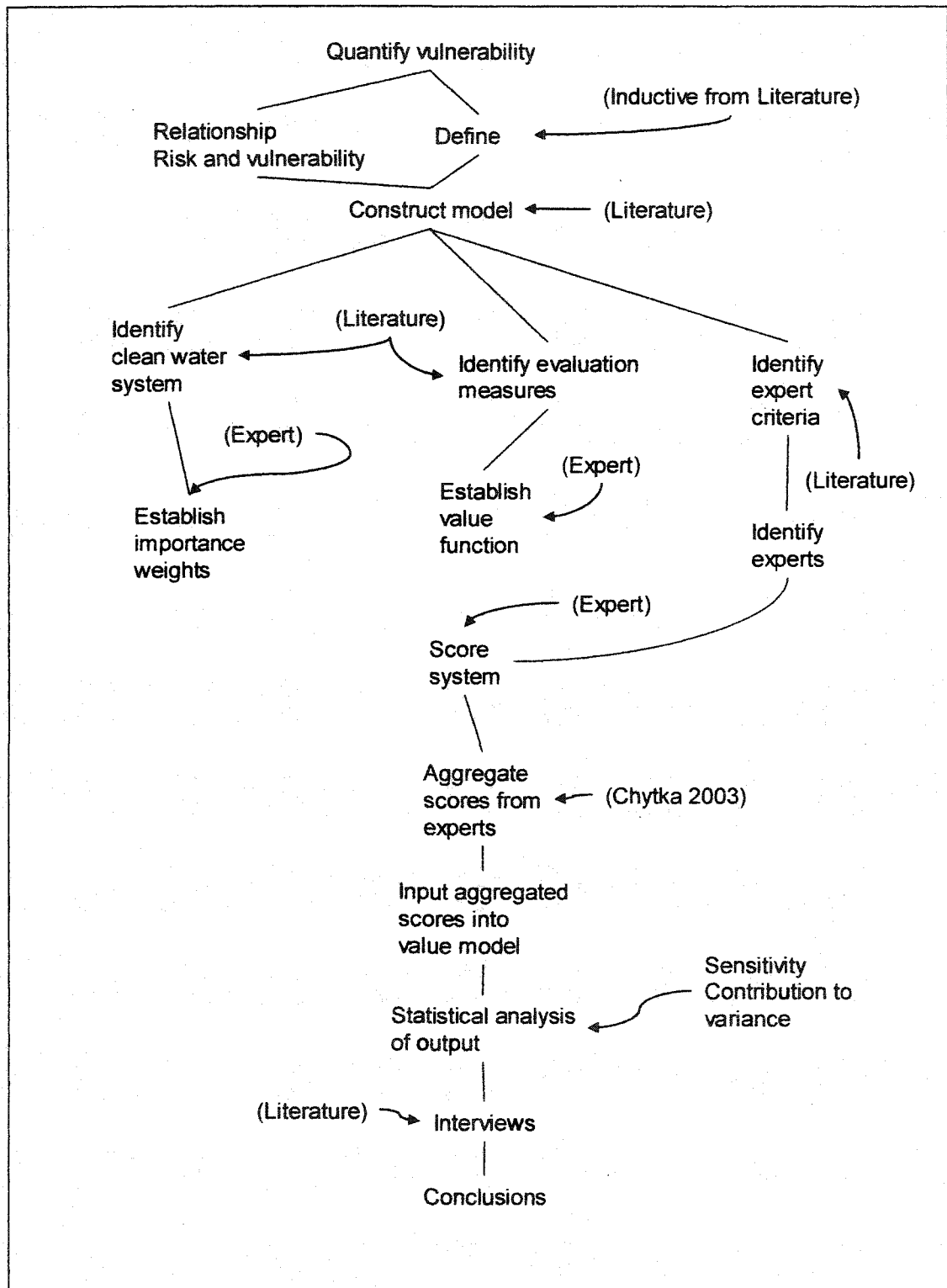


Figure 6. Research Design

Expert Elicitation

Validating model construction, setting the parameters of the model and scoring the performance of the clean water system with respect to each threat scenario required the use of experts. The criteria used for selecting experts are guided by the research of Chytka (2003): 1) years of experience in water systems as an engineer, manager, Supervisory Control and Data Acquisition Systems (SCADA) design; 2) educational background in engineering (civil, environmental, chemical); and 3) appropriate expertise for discipline specific tasks such as water storage, treatment, distribution, and control.

This research included three subject-matter experts (SME). SME-1 was interviewed to validate the decomposition of the system into functions. The interview worksheet is located in Appendix B. SME-2 was asked to establish the relative importance of each of the components of the decomposed system shown below in Figure 9. The Microsoft Excel ® (Microsoft Corporation, 2004, Version 2003 SR-2) workbook used to collect the data is located in Appendix C. SME-2 was asked to establish the shape of the value functions in the model. The Microsoft Excel workbook used to collect the data is located in Appendix D. SMEs-1 and 2 were next interviewed to assess the vulnerability a notional clean water medium-sized system. SME-3 was used to weight the assessments of SME-1 and 2. SME-3 was exceptionally qualified as his experience was 28 years (1.5 to 2 times greater than SME-1 and 2) in the clean water treatment and production system. In addition, his education was equal to both SME-1 and 2. In addition, SME 1,2,and 3 were each asked to gage the face validity of the final model as discussed in Appendix F. (Chytka, p. 50, 2003) states in her research: “the linear opinion

pool is the most straightforward method of combining the opinions of experts". Chytka (2003) points out that for the cases where hard data is negligible or non existent, one must rely upon subject matter experts to quantify uncertainty, making mathematical aggregation such as the linear opinion pool appropriate choice to mathematically aggregate uncertainty scores among subject matter experts. This research utilized the aggregation methodology and process model of Chytka (p. 45, 2003):

1. Who is doing the aggregation: a normative model, a decision-maker or a group?
2. What is the form of the information elicited and the response the decision-maker generates?
3. What is the nature of events that are relevant to aggregation epistemically uncertain or aleatory?
4. Are there any inherent characterizations that can be made about the information pattern or information sources such as biases or redundancy in information?
5. What combination rule is to be utilized?

For question one: who is doing the aggregation this research design culminated in a model to quantify vulnerability therefore the answer to this question was a normative model using Microsoft Excel ® (Microsoft Corporation, 2004, Version 2003 SR-2) and the add-in simulation software Crystal Ball ® (Decisioneering 2004, Version 5.0). Chytka's (2003) second question: what is the form of the information elicited and the response the decision-maker generates? This research design indicated qualitative using semi-structured interviews and then quantified using Chytka (2003) Aggregation Process

Model. For question three, what is the nature of events that are relevant to aggregation epistemically uncertain or aleatory? This research modeled aleatory or uncertain answers using the triangle distribution because how an expert scores or assesses a system cannot fully be known. Question four asked are there any inherent characterizations that can be made about the information pattern or information sources such as biases or redundancy in information? Chytka (2003) identifies the research of Conway's (2003) use of the calibration function to account for redundancies in information, but this work is not part of the aggregation algorithm itself and is beyond the scope of this research. In question five, Chytka (2003) asks: what combination rule is to be utilized? Chytka (2003) presents no best or dominant choices and states that there is no clear best answer in the literature and that the ultimate choice reverts to the researcher. For this research, the weighted linear opinion pool method was chosen. The linear opinion pool was used to combine scores when scores were uncertain, using the triangle distribution (Chytka 2003). Microsoft Excel ® (Microsoft Corporation, 2004, Version 2003 SR-2) and the add-in simulation software Crystal Ball ® (Decisioneering 2004, Version 5.0) was used to collect the data. The instructions and scoring table sample is located in Appendix E. SME-3(S) was used to determine the weighting factor reflecting the perceived credibility for each SME based on expert criteria already mentioned above and comparing each SME resume of experience. The assessment is provided in Appendix F. The case application, a clean water medium-sized system, was provided from the research of Ezell and Farr (2000b).

The Relationship: Vulnerability and Risk

In Chapter II, the literature review revealed many concepts and definitions on vulnerability and risk. The following paragraphs summarize vulnerability, risk and the attributes that define and describe each. The first paragraph highlights vulnerability and risk. Next, scenarios are shown to be the link between vulnerability and risk. The final paragraph of this section describes the mathematical relationship of vulnerability and risk.

To recap vulnerability, Buckle (2000), Dictionary.com (2000), Emergency Management of Australia (1998), Gheorghe (2001), International Strategy for Disaster Reduction (2002), National Oceanic and Atmospheric Administration (2002), and the National Security Telecommunications Advisory Committee (1997) use the adjective “susceptibility to...” to define vulnerability. Blaike et al. (1994); Nilsson et al. (2001); Nilsson, Magnusson, Hallin, and Lenntorp (2000); and the National Waterworks for Rural America (2002) use the adjectives “cope and deal with” to define vulnerability. Two definitions provided by Nilsson et al. (2001) and Nilsson, Magnusson, Hallin, and Lenntorp (2000) view vulnerability as a “collection of risks”, thus establishing a relationship between vulnerability and risk in the literature. Careful study of the literature disclosed the attributes that describe vulnerability: susceptibility to “what”; weakness in the system; a target with respect to a threat or risk; exposure to hazard. Kaplan (1997) said that risk was a triplet of scenario, likelihood, and consequences. The difference between Lowrance (1976) and Kaplan (1997) was the notion of scenario(s) as a euphemism for “what can go wrong”. *Vulnerability highlights the notion of susceptibility to a scenario whereas risk focuses on the severity of consequences to a*

scenario. Scenario appears in risk literature as an outline, script, or sequence of events. In the discipline of risk analysis, scenarios were made explicit by Kaplan and Garrick (1981); Kaplan, Zlotin, and Vishnipolski (1999); and refined by Kaplan, Haines and Garrick (2001). Fundamental to the theory of scenario structuring was the requirement that scenarios be (1) complete, (2) finite, and (3) disjoint. Kaplan, Haines and Garrick (2001) used scenario as the initiating event. Ezell (2000) and Ezell and Farr (2000a, 2000b) use scenario in a similar way with event trees. Scenarios were used in the development of alternatives and performance is assessed. In Kaplan and Garrick (1981), the authors point out that scenario was loosely defined as: "What can go wrong?" In Kaplan, Haines and Garrick (2001), the authors attempted to bridge Hierarchical Holographic Modeling (HHM) Haines (1981) with the theory of uncertainty. The approach focused on using the philosophy of HHM to holistically identify sources of risk from multiple perspectives: functional, temporal, and geographical. The authors then introduced rate and weight methodologies to arrive at a subset of scenarios from which to proceed. However, the authors did not address how one explicitly defines a scenario, nor the limit of the universal set of all risks and scenarios. In fact, even if one satisfied the criteria above, the essential components of the scenario remain an open question in the literature. In summary, this research has shown that vulnerability emphasizes susceptibility to a scenario (sometimes referred to as threat scenario) and risk highlights the severity of consequences to a threat scenario. Whereas risk is a function of threat scenario, likelihood of occurrence, and consequence, critical infrastructure vulnerability was shown to be a function of threat scenario, protection, and importance. Importance implied that some subsystems are more critical to overall system performance than other

subsystems (Ezell 2000a). Threat scenarios typified the classic risk question: what can go wrong? This research used the notion of importance (Ezell 2000a) and AWWA (2002b) measures of deterrence, detection, delay and response capabilities and to measure protection and quantify system vulnerability.

From the research of Kaplan and Garrick (1981), mathematically risk is $(R_A) = \{s_a, l_a, x_a\}A$. In words, risk is the universal set of the triplet: scenario (s_a), likelihood (l_a) and (x_a) consequence shown below.

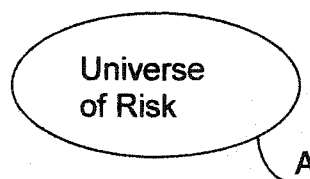


Figure 7. Universe of Risk, A

Building upon Kaplan and Garrick (1981) definition and the relationship of scenario pointed out in Chapter II, vulnerability is the universal set of the triplet: scenario (s_a), protection (p_a), and importance (w_a) shown below. Mathematically vulnerability is $(\Omega_a) = \{s_a, p_a, w_a\}A$.

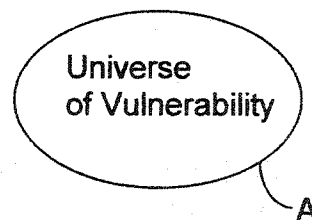


Figure 8. Universe of Vulnerability, A

To measure system vulnerability this research assessed protection by measuring deterrence (d_1), detection (d_2), delay (d_3) and response (r) protection measures (Sandia 2000).

In summary, as developed and inferred from the literature synthesized in Chapter II and amplified here in Chapter III, the definition of critical infrastructure vulnerability was shown to be the susceptibility of the infrastructure to threat scenarios, where vulnerability (Ω) is a function of threat (s_a), protection (p_a), and importance (w_a). Threat scenario is akin to the risk question: what can go wrong (Kaplan and Garrick 1981)? This is the relationship between risk and vulnerability. And, vulnerability was quantified by a system's protection measures evaluated as deterrence, detection, delay and response capabilities (AWWA 2002b). Chapter IV includes a section that discusses concepts on applying threat scenarios for future researches. The following section describes the value model as the logical construct for quantifying critical infrastructure vulnerability.

Vulnerability Value Model Construction

The critical infrastructure clean water system vulnerability value model was built upon the mathematics of multi-attribute value theory and structured as a value model. The research was guided by the work of Keeney, R.L. (1992), Keeney, R.L. and Raiffa, H. (1993), and Parnell, G.S., Jackson, J.A., Jones, B.L., Lehmkuhl, L.J., Conley, H.W., and Andrew, J.M., (1998). Model decomposition was inspired by systems theory and guided by the research of Sage and Armstrong (2000), Haines (1998) and Gibson (1991). The model was targeted to a medium-sized clean water system as a large-scale complex system (Ezell 2000a). Taken as an entire system, functional decomposition of a clean water system was guided by the research of AWWA (2002b) and shown in figure 9. This decomposition served as the structure of value model.

The next step in model construction was to add the protection level of evaluation measures to the model. For each of the lowest levels of the model, protection measures

of deterrence (d_1), detection (d_2), delay (d_3) and response (r) were added. Deterrence (d_1) was defined by Garcia (2001) as those measures implemented that are perceived by adversaries as too difficult to defeat. Detection (d_2) was defined as the probability of determining that an unauthorized action has occurred or is occurring including sensing, communicating alarm to control center, and assessing the alarm. Delay (d_3) was defined as the time, measured in minutes that an element of a physical protection system designed to impede adversary penetration into or exit from the protected area (Garcia 2001). Response (r) was defined as time (minutes) to respond to a threat (Garcia 2001). The next step in establishing the model was constructing the value functions. This step is covered in the next section.

Value Function Construction

The model used four evaluation measures of protection. These measures were deterrence (d_1), detection (d_2), delay (d_3), and response (r). The definitions of the measures were guided by the research of Garcia (2001), Sandia (2000) and AWWA (2002b). Figures 10-13 show four samples representing each of the four protection measures. A value function has five components: 1) definition and source, 2) x-axis description, 3) function, and 4) the subject-matter expert who determined the relationship between the x-axis and the associated value. The rationale behind subject-matter expert criteria and selection are presented later in the chapter. To recap, Garcia (2001) defined deterrence measures implemented that are perceived by adversaries as too difficult to defeat. In Figure 10, the value function x-axis has a description for each on an ordinal scale of one to five. On the $V(x)$ axis, the subject-matter expert decided that for a given subsystem, the value he placed on the level of increasing deterrence. Figures 11 through

13 are samples for detect, delay and response. All 14 sets (56 individually) of the actual value functions are listed in Appendix D.

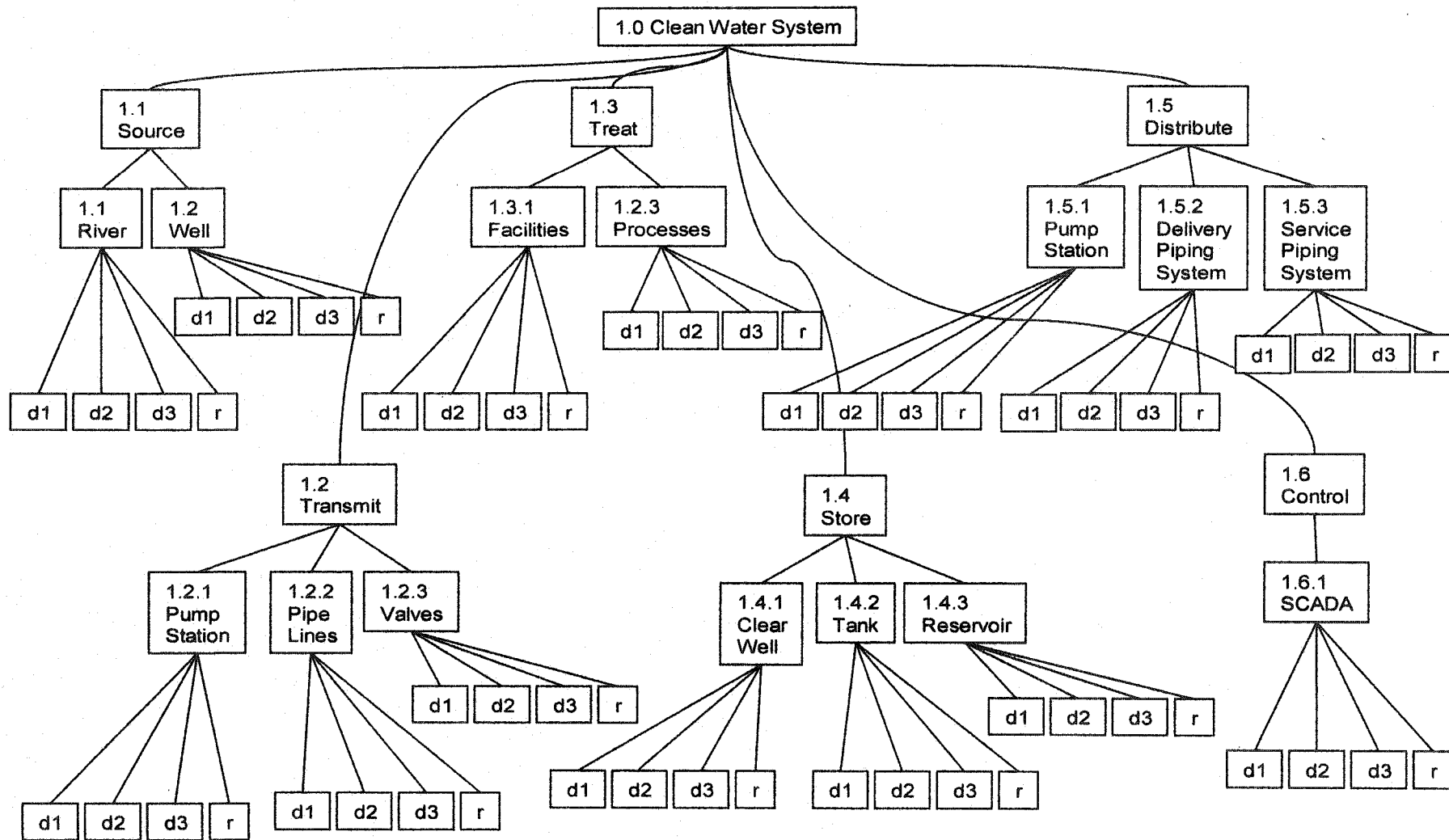


Figure 9. Value Model Structure

Deterrence value function		x	v(x)
	None	0	1
	Posting signs	1	20
	Posting signs and night lighting	2	40
	Posting signs, night lighting and fencing	3	60
	Posting signs, night lighting and multiple barriers	4	80
	Posting signs, night lighting, multiple barriers and audible warnings	5	100
The measures implemented that are perceived by adversaries as too difficult to defeat.			

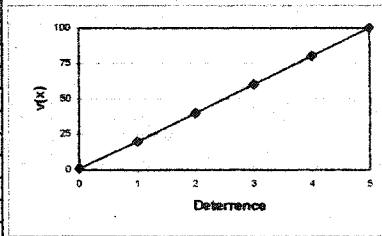


Figure 10. Deterrence Value Function Example

Detection value function		x	v(x)
	none	0	0
	very low	0.2	20
	low	0.4	40
	medium	0.6	60
	high	0.8	80
	very high	1	100
Probability of determining that an unauthorized action has occurred or is occurring.			

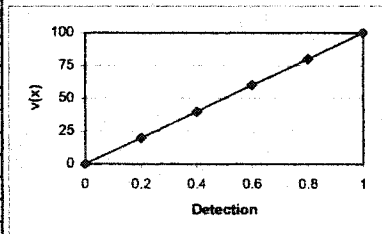


Figure 11. Protection Value Function Example

Delay value function		x	v(x)
	No delay	0	0
	One minute delay	1	20
	Five minute delay	5	40
	15 minute delay	15	60
	30 minute delay	30	80
	60 minutes delay	120	100
Time (minutes) that an element of a physical protection system designed to impede adversary			
Evaluation measure source		Garcia, 2001	

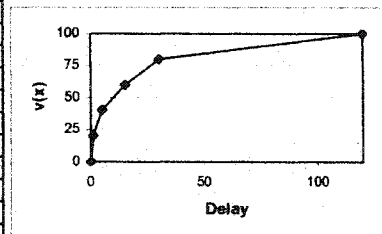


Figure 12. Delay Value Function Example

Response value function		x	v(x)
	Respond within seconds	0	100
	Respond within one minute	1	80
	Respond within five minute	5	60
	Respond within 15 minute	15	40
	Respond within thirty minute	45	20
	Respond within 60 minutes	90	0
Time (minutes) to respond to a threat			
Evaluation measure source		Garcia, 2001	

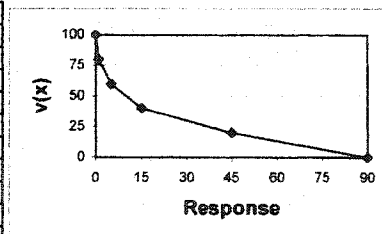


Figure 13. Response Value Function Example

In summary, the figures shown above represented the basic value functions that subject matter expert used to determine the shape of each function for every component in the system. Each function contained a definition, reference source and a graph that showed the subject matter expert where his or her value increased or decreased monotonically or both. In the next section the manner in which the model was calibrated is discussed in the research design.

Model Calibration

Raw data and weights, represented by the scores and relative importance of elements were assigned by subject-matter experts. The critical infrastructure clean water system vulnerability value model is an additive preference model in that it assigns value to each attribute measurement on a scale 0-100, using value assignment methodology. Value functions were built through subject-matter expertise assignment and have the following form:

$$V(x) = \sum_{m=1}^n w_m v_m(x_m)$$

Equation 1. Additive Value Form

where m is the evaluation measure, x_m is the level of the m th measure, $v_m(x_m)$ is the value of the value function at level x_m , and w_m is the product of the weights for each level up the hierarchy (Parnell, Conley, Jackson, Lehmkuhl, and Andrew, 1998).

Subject-matter experts were discussed in earlier sections of this chapter. The benefits of a value model are that it avoids arbitrary scaling or aggregation and makes the

model flexible for a variety of users. Flexibility was apparent because a value model allowed the user to rate possible levels of evaluation measures with different scales to one scale: *value* ranging from zero as worst to 100 as the best value. Raw data-to-value score was simply a piecewise linear interpolation obtained from the value function. The form of the function was monotonically increasing, decreasing, or both. A generic value model works in the following way: 1) raw data is entered; 2) value is calculated with respect to value functions; and 3) a global weight is applied. The model used a sufficiently large number of 15,000 trials of Monte Carlo simulation to aggregate uncertainty scores from experts and simulated again within the value model itself. Although the research could have calculated the minimum required number based on the desired standard error and confidence interval, the research design simply accepted very large sampling size because the simulation time was not an issue in this research. This accounts for uncertainty in scores used for calculating the distribution of values for vulnerability. The triangle distribution is an appropriate distribution to be used for such cases (Chytka 2003). The model used Monte Carlo simulation to generate the output for vulnerability by generating a sufficiently large number of trials (15,000 trials). Table 5 provides a summary of the output measures for the vulnerability value model. The measures column indicates the lowest level within the model.

Table 5. Value Model Structure

Measure	Component	Subsystem	System
Deter (.1)	River (1.1.1)	Source (1.1)	Clean Water System
Delay (.2)			
Detect (.3)			

Measure	Component	Subsystem	System
Respond (.4)	Well(1.1.2)		
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Pump Station (1.2.1)		
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Pipelines (1.2.2)	Transmit (1.2)	
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Valves (1.2.3)		
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Facilities (1.3.1)	Treat (1.3)	
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Processes (1.3.2)		
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Clearwell (1.4.1)		
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Tank (1.4.2)	Store (1.4)	
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Reservoir (1.4.3)		
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)	Pump Station (1.5.1)	Distribute (1.5)	
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)			

Measure	Component	Subsystem	System
Deter (.1)	Del Piping System (1.5.2)		
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Svc Piping System (1.5.3)		
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	SCADA (1.6.1)	Control (1.6)	
Delay (.2)			
Detect (.3)			
Respond (.4)			

In the adjacent columns, component, subsystem and system show the remaining levels from lowest to the top of the model. The numbering system also indicates the location in the system. For example, 1.1.1 indicates the Rive component, whereas 1.1.1.2 indicates the delay measure at the lowest level in the model. Table 6 is table of outputs and calculations from the model. Table 6 was used to collect all data from experts as well as the calculations from the Vulnerability Value Model discussed in Chapter V.

Table 6. Vulnerability Value Model Inputs and Calculation Matrix

Evaluation Measure	wt	x	v(x)	Comp	wt	x	v(x)	Ω	Sub-sys	wt	x	v(x)	Ω	V(X)	Ω
1.1.1.1				1.1.1					1.1					1	
1.1.1.2															
1.1.1.3															
1.1.1.4															
1.1.2.1				1.1.2					1.2						
1.1.2.2															
1.1.2.3															
1.1.2.4															
1.2.1.1				1.2.1											
1.2.1.2															

Evaluation Measure	wt	x	v(x)	Comp	wt	x	v(x)	Ω	Sub-sys	wt	x	v(x)	Ω	V(X)	Ω		
1.2.1.3																	
1.2.1.4																	
1.2.2.1				1.2.2													
1.2.2.2																	
1.2.2.3																	
1.2.2.4																	
1.2.3.1				1.2.3													
1.2.3.2																	
1.2.3.3																	
1.2.3.4																	
1.3.1.1				1.3.1						1.3							
1.3.1.2																	
1.3.1.3																	
1.3.1.4																	
1.3.2.1				1.3.2													
1.3.2.2																	
1.3.2.3																	
1.3.2.4																	
1.4.1.1				1.4.1					1.4								
1.4.1.2																	
1.4.1.3																	
1.4.1.4																	
1.4.2.1				1.4.2													
1.4.2.2																	
1.4.2.3																	
1.4.2.4																	
1.4.3.1				1.4.3													
1.4.3.2																	
1.4.3.3																	
1.4.3.4																	
1.5.1.1				1.5.1					1.5								
1.5.1.2																	
1.5.1.3																	
1.5.1.4																	
1.5.2.1				1.5.2													
1.5.2.2																	
1.5.2.3																	
1.5.2.4																	
1.5.3.1				1.5.3													
1.5.3.2																	
1.5.3.3																	
1.5.3.4																	

Evaluation Measure	wt	x	v(x)	Comp	wt	x	v(x)	Ω	Sub-sys	wt	x	v(x)	Ω	V(X)	Ω	
1.6.1.1				1.6.1					1.6							
1.6.1.2																
1.6.1.3																
1.6.1.4																

Table 7 below summarizes the variables and parameters used in the Vulnerability Value Model. The left most column describes the variable. In the next two columns, description and type of notation is provided. In the last column, the form of the variable is shown as discrete or continuous.

Table 7. Model variables and parameters

Notation	Description	Type	Form
X	Protection measure assessment	Variable	Continuous
v(x), V(X)	Value associated with x measure, Total value score	Variable	Continuous
Ω	Vulnerability	Variable	Expected Value (Continuous)
M	Location in model	Parameter	Discrete
W	Global Weight	Parameter	Discrete
L	Local Weight	Parameter	Discrete
D	deterrence (d_1), detection (d_2), delay (d_3) and response (r)	Variable	Continuous
N	Number of Trials	Parameter	Discrete

Calculations for the model are in the form $V(x) = \sum_{m=1}^n w_m v_m(x_m)$. For example, to

calculate component value and vulnerability for the river component, the weight of each

protection measure is multiplied by the corresponding value of x from the value functions and summed together for the river component.

$$v_{1.1.1}(x_{1.1.1}) = w_{1.1.1.1} * v_{1.1.1.1}(x_{1.1.1.1}) + w_{1.1.1.2} * v_{1.1.1.2}(x_{1.1.1.2}) + w_{1.1.1.3} * v_{1.1.1.3}(x_{1.1.1.3}) + w_{1.1.1.4} * v_{1.1.1.4}(x_{1.1.1.4})$$

Equation 2. River Component Value (1.1.1)

River component (1.1.1) vulnerability would be the ideal v^* or max possible value score, $v^*(x)$ minus the assessed value score, $v(x)$. The difference becomes river component vulnerability: $\Omega_{(1.1.1)}$.

$$\Omega_{1.1.1} = v^*_{1.1.1}(x) - v_{1.1.1}(x)$$

Equation 3. River Component Vulnerability (1.1.1)

Subsystem value score is the sum product of all component value scores and their associated weight. For the case of the source subsystem (1.1) the value score is given by equation 4.

$$v_{1.1}(x) = w_{1.1.1} * v_{1.1.1}(x) + w_{1.1.2} * v_{1.1.2}(x)$$

Equation 4. Source Subsystem Value (1.1)

Vulnerability of the source (1.1) subsystem is the difference of the ideal or maximum possible value score for the subsystem and the assessed value score given in equation 5.

$$\Omega_{1.1} = v^*_{1.1}(x) - v_{1.1}(x)$$

Equation 5. Source Subsystem Vulnerability (1.1)

Overall system value score is the product sum of all subsystems given in equation 6.

$$V(X) = w_{1.1} * v_{1.1}(x) + w_{1.2} * v_{1.2}(x) + w_{1.3} * v_{1.3}(x) + w_{1.4} * v_{1.4}(x) \\ + w_{1.5} * v_{1.5}(x) + w_{1.6} * v_{1.6}(x)$$

Equation 6. Overall Clean Water System Value Assessment

In the discrete form, overall vulnerability, Ω is the max value (100) minus the overall assessed value given in equation 6, above. In the continuous form, the expected value of vulnerability, $E[\Omega]$ is given by equation 7 below.

$$E(\Omega) = \int_0^{+\infty} \omega f(\omega) d\omega$$

Equation 7. Expected Value of vulnerability

The output from the model simulation is a distribution of vulnerability, Ω . The expected value of the distribution is the integration from the min to max value as shown in equation 7, above.

In summary, this section has provided the details that were used to develop the Vulnerability Value Model. The section showed how relative importance among the different components and subsystems would be assessed and collected. Value function assessment by subject matter experts were discussed as well as examples. Tables were presented to demonstrate how data was organized for the model.

Model Sensitivity, Verification and Validation

Model sensitivity was accomplished by evaluating the influence of each assumption within the model to the model's output (Decisioneering 1996). In Crystal Ball ® (Decisioneering 2004, Version 5.0), the influence of each assumption was accomplished by analyzing each assumption's contribution to variance and by measuring the relative importance of each assumption to the model's output. A positive coefficient indicates that an increase in an assumption is associated with an increase in the model's output. A negative coefficient implies the reverse. The larger the absolute value of the coefficient, the stronger the relationship. In addition, the Monte Carlo simulation (more random number generation) was run at 15,000 trials and 150,000 trials to observe if there was change in the output. Also, Latin-Hypercube (more even random number sample) runs were simulated to observe output at 15,000 and 150,000 trials (Chytka 2003; Decisioneering 2004).

Model verification consisted of the logic and math checks in the model. At every level within the model, the sum of the weights must equal one, $\sum_{i=1}^m w_m = 1$. In addition, the value at the component level product sum must equal the value of the product sum at the subsystem level, $\sum_{i=1.1}^{1.6} w_m v(x_m) = \sum_{i=1.1.1}^{1.6.1} w_m v(x_m)$. The assessed value of the system must always be less than or equal to the ideal or max possible score of the system. Finally, the x , $v(x)$, w must be greater than or equal to zero. By following the research design for sensitivity and verification, it was assured that that the model performed in its intended

design. Last, sensitivity as it was designed helped to see what places within the model had the greatest impact on the model output.

Model validity was accomplished by using the decomposition of a clean water system given by the research of AWWA (2000a) and through interviews with SME-2 and SME-3. As stated earlier in the chapter, value model validity was assured by the research of Keeney, R.L. (1992); Keeney, R.L. and Raiffa, H. (1993); and Parnell, G.S., Jackson, J.A., Jones, B.L., Lehmkuhl, L.J., Conley, H.W., and Andrew, J.M., (1998). This research design rigorously followed the manner in which values models are developed as addressed in the preceding sections. For example, the model was decomposed into generally agreed to independent components and subsystems and validated with the literature of AWWA (2002). To the greatest extent possible, measures were used that held no dependence and supported by the literature from Sandia (2000). Face validity of the decomposed medium sized clean water system was validated by the research of (Ezell 2000a) and AWWA (2002). In the following section, the methodology for scoring and the notional system description used by the subject matter experts is presented.

Assessing (Scoring) the Clean Water System

SME-1 and SME-2 scored the notional clean water system described below using the scoring matrix provided in Appendix E. The deterrence measure was discrete and detect, delay and response measures were assessed with uncertainty modeled with the triangle distribution following the expert elicitation work of Chytka (2003). In the next section, the notional clean water system

description used by the subject matter experts is introduced below. The system served as a case for application of the Vulnerability Value Model.

Notional Medium Clean Water System

The notional city and corresponding water system was an amalgamation of previous work from Ezell (1998); Ezell, Farr and Wiese (2000b); and Ezell, Haimes, and Lambert (2001). The City was a medium-sized municipality comprised of 10,000 customers. It has a water treatment and distribution system that supplies approximately 2 million gallons per day (MGD). The community is mainly residential with some light industrial facilities. Water Treatment Plant A (WTPA) is primarily responsible for the uninterrupted flow of water to its customers. The primary means of water-flow is gravity. WTPA receives water from a large lake that is shared with another small community to the south. The treatment processes are relatively simple, involving chlorinating (for disinfecting), addition of fluoride (dental health), and treatment with alum (clarification). The treatment plant has some simple gauges monitoring inflows and outflows, and some fault lights that alert the operator to pump failures. There is no sophisticated computer-based control of the treatment plant. The SCADA system uses a master-slave relationship, relying on the total control of the SCADA Master. Remote terminal units are dumb. They accept instructions and perform their functions in accordance with their programming. The water from the treatment plant is pumped to Tank 1 from where it supplies Area A. Area A has approximately 2/3 of the total number of customers during the day. WTPB is primarily used during the summer time to support the added demand in a seasonal resort area. WTPB also shares a lake with an

adjacent city, east of the reservation. WTPB has similar treatment processes to WTPA, and primarily supplies Area D, although it can also supply Area C. There are 4 tanks and 1 pumping station as shown in Figure 14. Tank 1 serves 2/3 of customers in the most densely populated low-level area (the community is on the side of a mountain valley). The capacity of Tank 1 is 0.5 MG. The remaining tanks serve relatively fewer customers in the high-level zone comprised of Areas B, C, and D.

Pump Station 1 is controlled from the levels in Tank 2, using simple float balls and RTU as well as a landline modem connection between the two sites to transmit a control signal. The control is based on level control using a pump cut-in level and a pump cutout level. The tank capacity has two component segments. One is reserve storage that allows the tank to operate over a peak week when demand exceeds pumping capacity. The other component is control storage. This is the portion of the tank between the pump cutout and cut-in levels. Visually, the control storage is the top portion of the tank. If demand is less than pump rate, (low demand periods) the level will rise until it reaches the pump cut-out-level. When the water level falls to the tank cut-in-level the pump will begin to operate. The cut-in-level refers to a level in the tank that water reaches and triggers the pump to start. If the demand is greater than the pump rate, the level will continue to fall, until it reaches reserve storage. The tank level will stay in this area until the demand has fallen for a sufficient time to allow the level to recover. The reserve storage is sized according to demand (e.g., a tank with larger reserve storage serves more customers).

Tank 2 supplies customers in Area B by gravity. The arrangement of providing supply to customers directly from the tank rather than from the connecting pipeline ensures a constant pressure is supplied. Water also gravitates from Tank 2 to Tank 3. An Altitude Control Valve (ACV) closes when Tank 3 is full to prevent it overflowing. It will open when the tank is emptied to a predetermined level, allowing the tank to refill. Tank 3 then supplies customers in Area C by gravity. During low demand periods (mainly non summer) water gravitates from Tank 2 to Tank 4, and from there is gravity fed to customers in Area D. An Altitude Control Valve regulates the flow into Tank 4. During the peak summer months WTPB supplies Tank 4 instead of the gravity supply from tank 2. When WTPB is to be brought into operation for the peak summer period, a valve is closed to prevent flow from Tank 2 to Tank 4. There is an interconnection between Tank 4 and Tank 3, which allows Tank 3 also to receive water from Tank 4.

This section presented a notional water system based on the research of Ezell (1998); Ezell, Farr and Wiese (2000b); and Ezell, Haines, and Lambert (2001). The description served as the vignette to apply the Vulnerability Value Model to quantify vulnerability.

Summary

Chapter III comprised the research design. The chapter began with an explanation of the methodology and the logic behind why a mixed design of qualitative and quantitative was necessary to answer the research questions. A qualitative approach was used to infer the definition of vulnerability and the relationship of risk and vulnerability from the literature. From this definition, a relationship emerged that

vulnerability is a function of scenario, protection, and importance. The qualitative design showed from the literature synthesis that the scenario (threat scenario) is the link between vulnerability and risk. Vulnerability highlights the notion of susceptibility to a scenario whereas risk focuses on the severity of consequences to a scenario. The centerpiece to the chapter was figure 6 as it detailed the research design and graphic form. The figure shows how the design is laid out as well as the order in which the design was executed. Chapter III showed how user input from subject matter experts was aggregated using the weighted linear pool method. It showed how data was collected for weights, value function assignment, and system assessment by subject matter experts. Specifically, this chapter showed how subject matter experts were used and how their scores were aggregated into a consensus input distribution for each measure in the vulnerability value model. Next the chapter detailed the design and development of the vulnerability value model. System decomposition of a clean water system was presented and the justification for the decomposition from the literature and the experts. An example clean water system validated from the literature was presented as the example subject matter experts would use to assess the system. The design in Chapter III highlighted how the model was verified and validated. Finally, the chapter provided the equations for calculating vulnerability as well as a table that was used to represent the data collected from the model. In Chapter IV, the results of the model are provided as well as the supporting analysis.

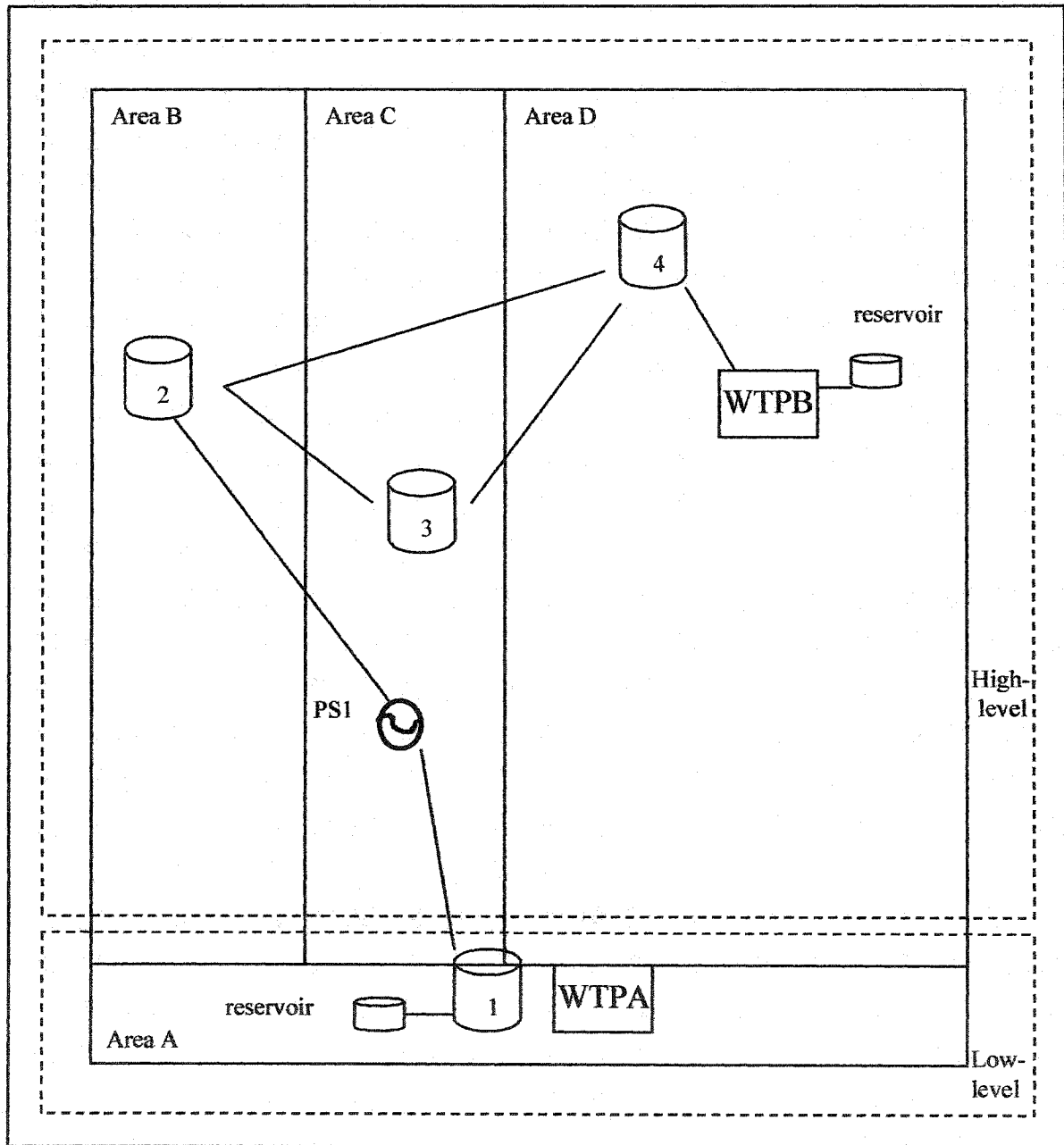


Figure 14. Notional Clean Water System

CHAPTER IV

RESULTS

The purpose of this chapter is to provide a summary of the data collected and an analysis from the vulnerability value model of a clean water system, presented in Chapter III. Using the research design detailed in Chapter III, Chapter IV carefully employed the design to answer the research questions presented in Chapter I. This chapter begins with a summary of the data collected from the subject matter expert for the relative importance of system components and subsystems and the determination of the shapes of each value function in the model. Next, two subject matter experts reviewed the notional clean water system and then scored (assess) the x value for each measure within the model. A third subject matter expert was interviewed to assess the level of expertise of subject matter experts one and two. The weighted inner loop aggregation simulation was run and the resulting distributions are summarized in the chapter and all input distributions are provided in Appendix G. The vulnerability value model simulation was executed. The results are presented in table 10 followed by explanation and analysis. In addition, the chapter shows the major output graphs comparing an ideal system's performance with the performance of the notional system as scored by the subject matter experts. Last, sensitivity analysis is discussed and the implication of the sensitivity of the model is examined.

Relative Importance Data

Subject Matter Expert One was asked to rate the relative importance of each subsystem and component within the clean water system. Table eight summarizes the assessment of relative importance.

Table 8. Relative Importance and Weights

Measure	Rel. Imp.	wt	Component	Rel. Imp.	wt	Sub system	Rel. Imp.	wt
1.1.1.1	10	0.263	1.1.1	9	0.75	1.1	3	0.09
1.1.1.2	10	0.263						
1.1.1.3	9	0.237						
1.1.1.4	9	0.237						
1.1.2.1	7	0.259	1.1.2	3	0.25			
1.1.2.2	8	0.296						
1.1.2.3	6	0.222						
1.1.2.4	6	0.222						
1.2.1.1	9	0.265	1.2.1	9	0.43			
1.2.1.2	9	0.265						
1.2.1.3	8	0.235						
1.2.1.4	8	0.235						
1.2.2.1	9	0.237	1.2.2	8	0.38	1.2	9	0.26
1.2.2.2	10	0.263						
1.2.2.3	9	0.237						
1.2.2.4	10	0.263						
1.2.3.1	9	0.273	1.2.3	4	0.19			
1.2.3.2	9	0.273						
1.2.3.3	8	0.242						
1.2.3.4	7	0.212						
1.3.1.1	10	0.256	1.3.1	10	0.53	1.3	9	0.26
1.3.1.2	10	0.256						
1.3.1.3	9	0.231						
1.3.1.4	10	0.256						
1.3.2.1	10	0.278	1.3.2	9	0.47			
1.3.2.2	10	0.278						
1.3.2.3	8	0.222						
1.3.2.4	8	0.222						
1.4.1.1	10	0.263	1.4.1	9	0.36	1.4	6	0.17
1.4.1.2	10	0.263						
1.4.1.3	9	0.237						

Measure	Rel. Imp.	wt	Component	Rel. Imp.	wt	Sub system	Rel. Imp.	wt
1.4.1.4	9	0.237						
1.4.2.1	9	0.281	1.4.2	6	0.24			
1.4.2.2	8	0.250						
1.4.2.3	8	0.250						
1.4.2.4	7	0.219						
1.4.3.1	10	0.250	1.4.3	10	0.40			
1.4.3.2	10	0.250						
1.4.3.3	10	0.250						
1.4.3.4	10	0.250						
1.5.1.1	8	0.267	1.5.1	6	0.55			
1.5.1.2	8	0.267						
1.5.1.3	7	0.233						
1.5.1.4	7	0.233						
1.5.2.1	7	0.304	1.5.2	3	0.27	1.5	3	0.09
1.5.2.2	6	0.261						
1.5.2.3	5	0.217						
1.5.2.4	5	0.217						
1.5.3.1	4	0.286	1.5.3	2	0.18			
1.5.3.2	4	0.286						
1.5.3.3	3	0.214						
1.5.3.4	3	0.214						
1.6.1.1	9	0.265	1.6.1	10	1.00	1.6	5	0.14
1.6.1.2	9	0.265						
1.6.1.3	8	0.235						
1.6.1.4	8	0.235						

At the protection measure level, the relative importance of measures varied little. The SME noted that these measures were always important regardless of the component being assessed. At the component level of the system, relative importance became more evident. At the subsystem level, the greatest differences in importance were observed. The subject matter expert assessed the importance of the source and control subsystems very low, 1/3 the importance of the transmission and treatment system, reasoning that the source is larger and more robust.

Value Functions

Subject matter expert one set the shape of each of the 56 value functions. Four value functions are shown below for deter, detect, delay and respond, corresponding to the river source subsystem. All value functions are included in Appendix D.

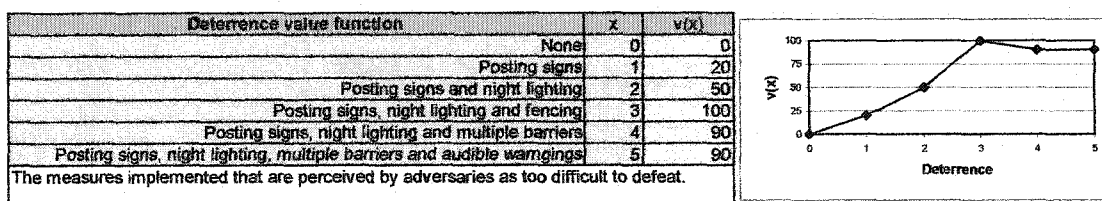


Figure 15. Deter value function from SME-1

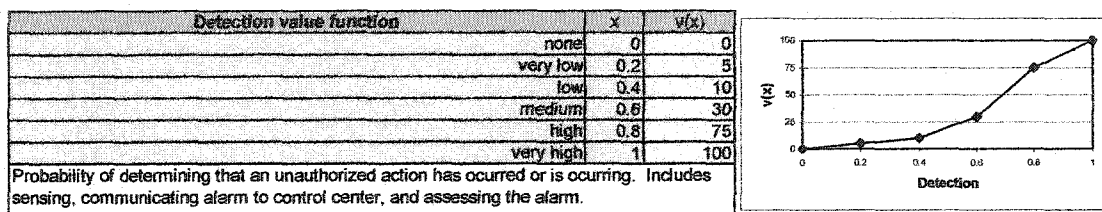


Figure 16. Detect value function for SME-1

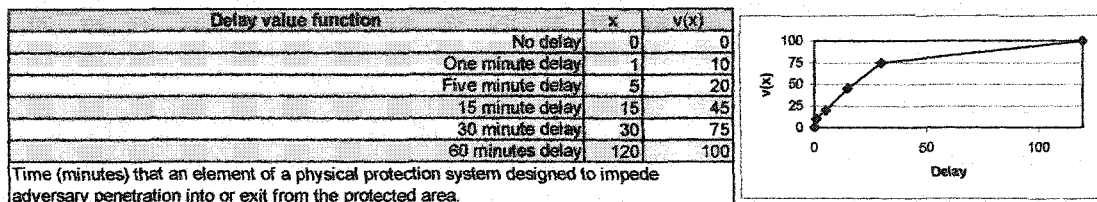


Figure 17. Delay value function for SME-1

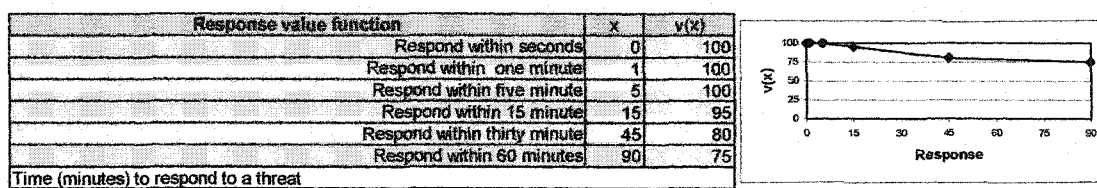


Figure 18. Response value function for SME-1

In figure 15 SME-1 valued deterrence as a monotonically increasing function to the point where posted signs, lights, and fencing were in place, putting 100 percent of the value here. Beyond that, SME-1 felt a diminishing return for greater deterrence measures, hence the monotonically decreasing function. In figure 16, SME-1 placed very little value for a medium and below detection probability. Value jumped to 75 percent of total value for a detection probability of high (0.8). SME-1 placed 100 percent of value on a perfect detection probability. For the delay value function in Figure 17, SME-1 placed about 50 percent of the value at a 15 minute delay. The remaining value was spread in a linear fashion from 15 minutes to 120 minutes, with 120 minutes receiving 100 percent of the value.

Scoring (Assessing) the Clean Water System

SME-1 and SME-2 scored the clean water system based on the notional clean water system presented in the previous chapter. A summary of their scores are presented below in table 9.

Table 9. Summary of assessments for SME-1 and SME-2

Comp	SME-1(.6)			SME-2 (.4)		
	Min	ML	Max	Min	ML	Max
1.1.1.2	5.00	30.00	60.00	15.00	25.00	60.00
1.1.1.3	0.10	0.40	0.75	0.20	0.25	0.50
1.1.1.4	10.00	30.00	60.00	1.00	10.00	60.00
1.1.2.2	10.00	20.00	60.00	10.00	20.00	45.00
1.1.2.3	0.40	0.75	1.00	0.20	0.80	1.00
1.1.2.4	5.00	30.00	60.00	5.00	10.00	15.00
1.2.1.2	15.00	30.00	60.00	20.00	35.00	60.00
1.2.1.3	0.50	0.80	0.90	0.50	0.80	1.00
1.2.1.4	1.00	10.00	20.00	5.00	15.00	25.00
1.2.2.2	1.00	5.00	15.00	1.00	5.00	8.00
1.2.2.3	0.40	0.80	1.00	0.50	0.80	1.00
1.2.2.4	2.00	10.00	20.00	5.00	15.00	25.00
1.2.3.2	5.00	20.00	60.00	15.00	25.00	40.00
1.2.3.3	0.20	0.60	1.00	0.20	0.70	0.90
1.2.3.4	5.00	20.00	60.00	5.00	10.00	15.00
1.3.1.2	15.00	30.00	60.00	10.00	20.00	60.00
1.3.1.3	0.50	0.80	1.00	0.50	0.70	1.00
1.3.1.4	5.00	50.00	60.00	10.00	25.00	45.00
1.3.2.2	1.00	10.00	15.00	5.00	15.00	20.00
1.3.2.3	0.40	0.80	1.00	0.10	0.30	0.70
1.3.2.4	2.00	10.00	20.00	5.00	10.00	25.00
1.4.1.2	5.00	30.00	60.00	15.00	35.00	60.00
1.4.1.3	0.40	0.70	0.90	0.50	0.80	1.00
1.4.1.4	5.00	20.00	60.00	5.00	10.00	30.00
1.4.2.2	5.00	20.00	60.00	10.00	30.00	45.00
1.4.2.3	0.50	0.80	1.00	0.40	0.60	0.70
1.4.2.4	0.00	5.00	10.00	1.00	10.00	15.00
1.4.3.2	10.00	30.00	60.00	5.00	20.00	30.00
1.4.3.3	0.00	0.10	0.30	0.00	0.10	0.30
1.4.3.4	2.00	10.00	20.00	5.00	15.00	25.00
1.5.1.2	20.00	45.00	90.00	20.00	55.00	90.00

Comp	SME-1(.6)			SME-2 (.4)		
	Min	ML	Max	Min	ML	Max
1.5.1.3	0.40	0.80	0.90	0.10	0.40	0.70
1.5.1.4	5.00	20.00	60.00	5.00	25.00	45.00
1.5.2.2	5.00	30.00	60.00	15.00	40.00	60.00
1.5.2.3	0.50	0.70	0.95	0.40	0.80	0.90
1.5.2.4	5.00	30.00	60.00	10.00	20.00	45.00
1.5.3.2	5.00	15.00	40.00	10.00	20.00	45.00
1.5.3.3	0.60	0.80	0.90	0.70	0.75	0.80
1.5.3.4	10.00	20.00	45.00	10.00	30.00	45.00
1.6.1.2	2.00	10.00	20.00	5.00	20.00	25.00
1.6.1.3	0.50	0.75	0.80	0.60	0.75	0.90
1.6.1.4	5.00	10.00	15.00	10.00	15.00	20.00

Aggregation of Scores

SME-3 was interviewed to determine the weighting factors for SME-1 and SME-2. After reviewing resumes and using the criteria developed in chapter 3, SME-3 concluded that SME-1 should receive 0.6 of the total weight and SME-2 receive 0.4 weight. The major contributing factor was experience in water. SME-3 judged SME-1's experience as more direct and precise, although each had similar educational experiences. That said, the experience of SME-2 was considerable and had no impact on the research. Using the weighted inner loop aggregation simulation technique advocated by the research of Chytka (2003), SME-1 and SME-2 scores were combined into a new distribution for use in the clean water system vulnerability value model. A sample of that aggregation from 150,000 trials is presented in figure 19 below and the remaining figures in appendix G. Figure 19 depicts the assessments of SME-1 and SME-2, modeled as a triangle distribution with a minimum score, most likely score and maximum score. Crystal Ball ran 150,000 trials multiplying a weight of 0.6 times SME-1 random variable

plus 0.4 times SME-2 random variable. Each random variable was generated with respect to each SME triangle distribution. What resulted was a beta distribution with parameters: 6.73 min, 62.16 max, 5.49 alpha and beta of 6.39.

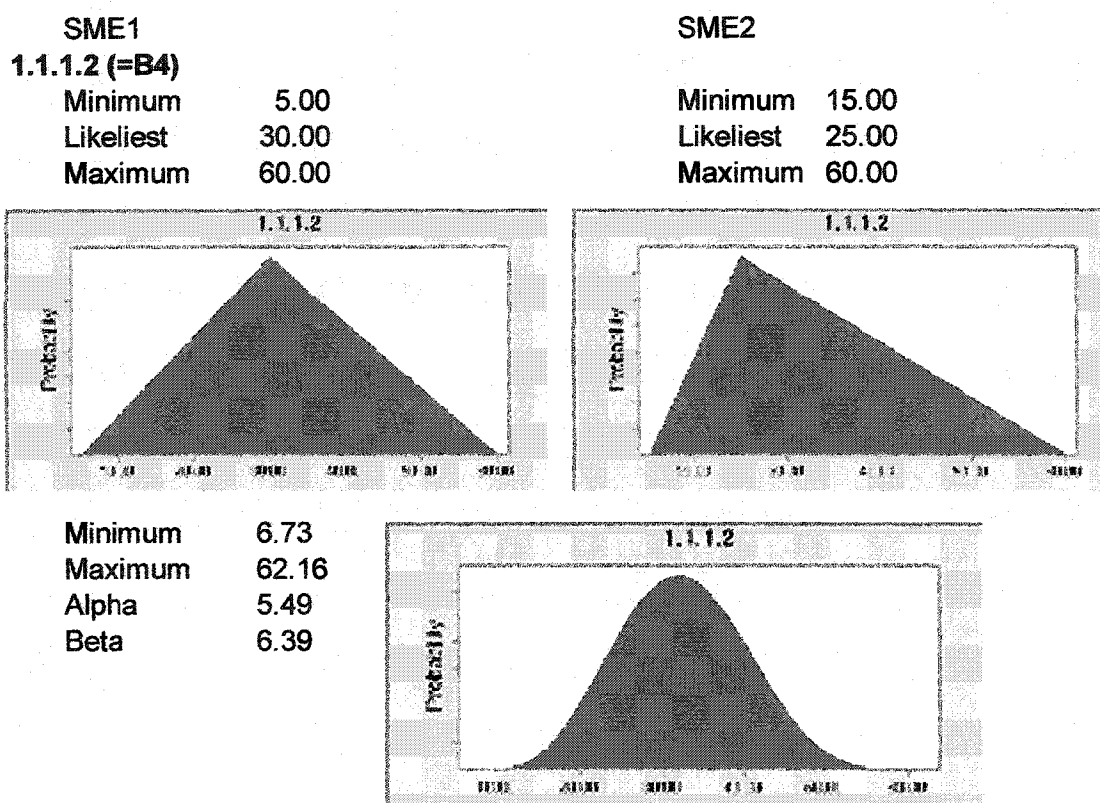


Figure 19. Sample from inner loop aggregation of SME-1 and SME-2

Once the aggregation was completed, all input data was supplied to the clean water system vulnerability value model. Data is provided in table 10.

Table 10. Input-output Data for the Vulnerability Value Model

	wt	x	v(x)	Comp	wt	v(x)	Ω	Sub sys	wt	v(x)	Ω	V(X)	Ω
1.1.1.1	0.26	3.00	1.69	1.1.1	0.75	4.96	1.47	1.1	0.09	6.22	2.35	68.1	31.9
1.1.1.2	0.26	28.65	1.10										
1.1.1.3	0.24	0.70	0.87										
1.1.1.4	0.24	35.10	1.29										
1.1.2.1	0.26	3.00	0.56	1.1.2	0.25	1.27	0.88						
1.1.2.2	0.30	6.34	0.11										
1.1.2.3	0.22	0.60	0.19										
1.1.2.4	0.22	32.98	0.41										
1.2.1.1	0.26	3.00	1.75	1.2.1	0.43	6.72	4.30						
1.2.1.2	0.26	10.00	0.84										
1.2.1.3	0.24	0.75	1.84										
1.2.1.4	0.24	28.33	2.29										
1.2.2.1	0.24	0.40	0.04	1.2.2	0.38	4.67	5.12	1.2	0.26	14.92	10.79		
1.2.2.2	0.26	26.64	1.63										
1.2.2.3	0.24	0.58	0.74										
1.2.2.4	0.26	34.41	2.26										
1.2.3.1	0.27	3.00	1.20	1.2.3	0.19	3.53	1.37						
1.2.3.2	0.27	22.04	0.70										
1.2.3.3	0.24	0.71	0.73										
1.2.3.4	0.21	33.32	0.89										
1.3.1.1	0.26	4.00	3.47	1.3.1	0.53	10.90	2.63						
1.3.1.2	0.26	22.99	1.90										
1.3.1.3	0.23	0.75	2.18										
1.3.1.4	0.26	12.42	3.34										
1.3.2.1	0.28	4.00	3.38	1.3.2	0.47	9.72	2.46	1.3	0.26	20.62	5.10		
1.3.2.2	0.28	21.10	1.55										
1.3.2.3	0.22	0.75	2.18										
1.3.2.4	0.22	12.39	2.61										
1.4.1.1	0.26	2.40	0.49	1.4.1	0.36	3.43	2.74	1.4	0.17	10.30	6.84		
1.4.1.2	0.26	21.00	0.83										
1.4.1.3	0.24	0.69	0.81										
1.4.1.4	0.24	26.99	1.30										
1.4.2.1	0.28	3.00	0.87	1.4.2	0.24	2.92	1.19						
1.4.2.2	0.25	26.99	0.71										
1.4.2.3	0.25	0.70	0.54										
1.4.2.4	0.22	26.35	0.80										

	wt	x	v(x)	Comp	wt	v(x)	Ω	Sub sys	wt	v(x)	Ω	V(X)	Ω
1.4.3.1	0.25	3.00	1.71	1.4.3	0.40	3.95	2.91	1.5	0.09	4.99	3.59		
1.4.3.2	0.25	10.02	0.56										
1.4.3.3	0.25	0.38	0.16										
1.4.3.4	0.25	28.01	1.52										
1.5.1.1	0.27	3.00	0.31	1.5.1	0.55	3.07	1.60						
1.5.1.2	0.27	12.22	0.46										
1.5.1.3	0.23	0.75	0.77										
1.5.1.4	0.23	27.70	1.54										
1.5.2.1	0.30	1.00	0.01	1.5.2	0.27	1.39	0.95						
1.5.2.2	0.26	33.57	0.46										
1.5.2.3	0.22	0.59	0.17										
1.5.2.4	0.22	33.62	0.74										
1.5.3.1	0.29	0.00	0.00	1.5.3	0.18	0.52	1.04						
1.5.3.2	0.29	6.45	0.10										
1.5.3.3	0.21	0.13	0.01										
1.5.3.4	0.21	51.80	0.41										
1.6.1.1	0.26	2.80	0.79	1.6.1	1.00	11.07	3.21	1.6	0.14	11.07	3.21		
1.6.1.2	0.26	29.03	2.71										
1.6.1.3	0.24	0.76	2.44										
1.6.1.4	0.24	11.07	5.13										

Table 11 provides a recap of all input data for columns: measure local wt., x assessment, component local wt., and subsystem local wt. Output is italicized by columns measuring v(x), component v(x), component omega value, subsystem v(x) and omega value, and system V(x) and corresponding omega value. The following charts are additional output graphs from the model that provide a pictorial representation of the system's vulnerability.

Figure 20 is a bar graph of overall system value score. The graph shows the ideal score and each subsystem's contribution to the ideal score. The bar to the right is the system's actual value score. Each slice in the bar represents each subsystem's

contribution to the score achieved. The difference in the bar graph height is the omega vulnerability value for the system; $\Omega = V^*(X) - V(X) = 100 - 68.12 = 31.88$.

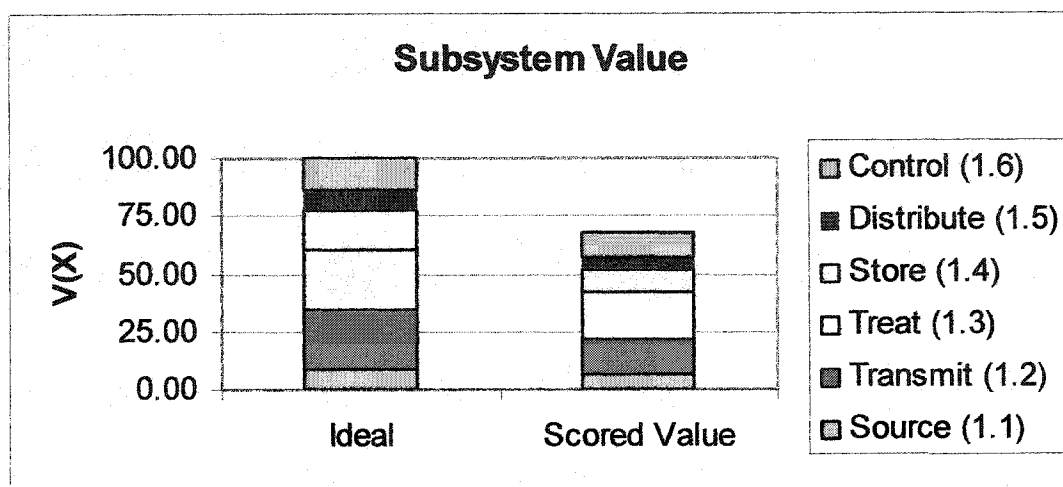


Figure 20. Ideal and Actual System Value

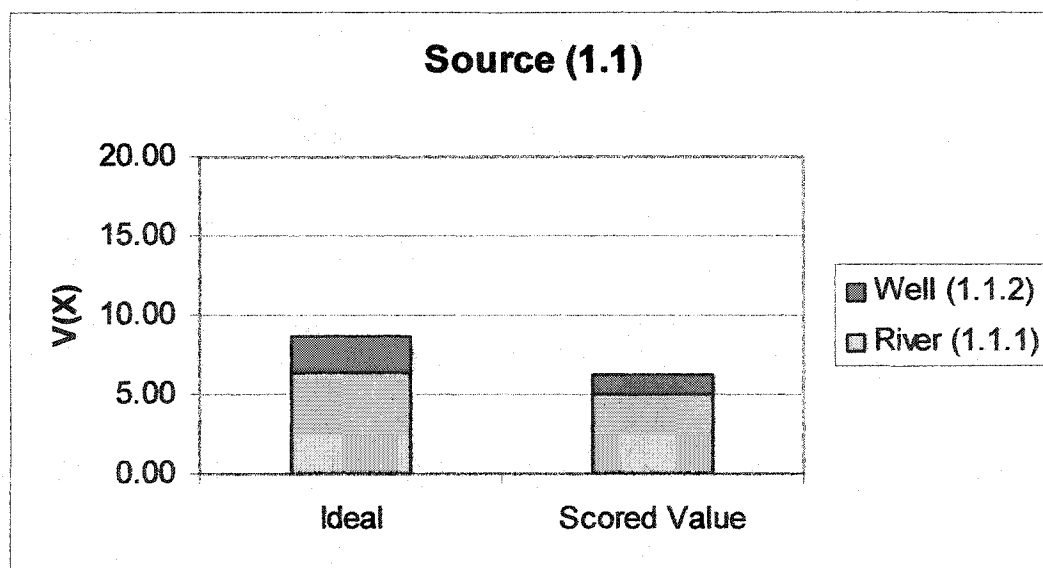


Figure 21. Source Subsystem Value

In figure 21, the well and river source components were assessed below the ideal score for the clean water system. Figures 22-26 reveal the same type of information in that one can easily see the component's assessment compared to its ideal score.

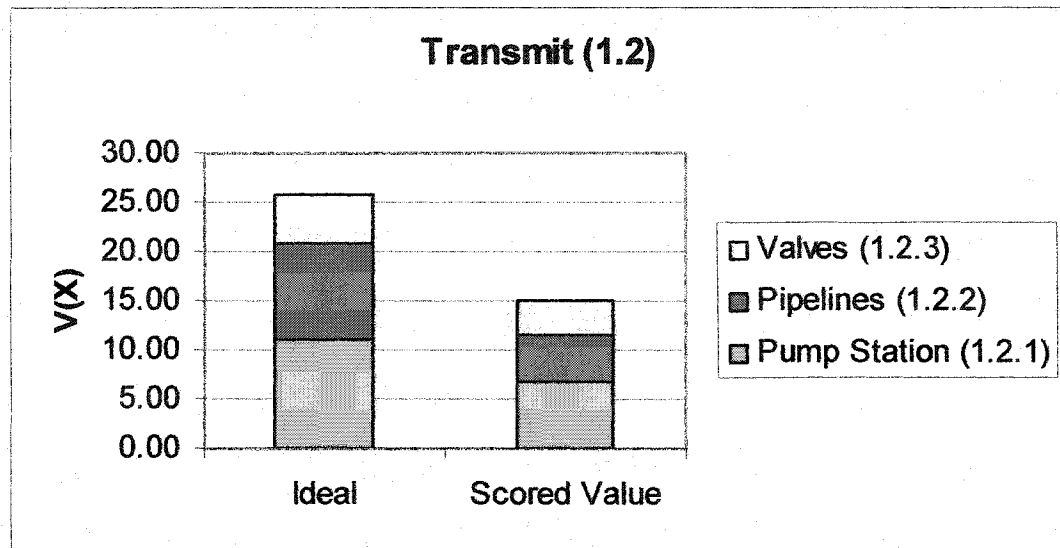


Figure 22. Transmit Subsystem Value

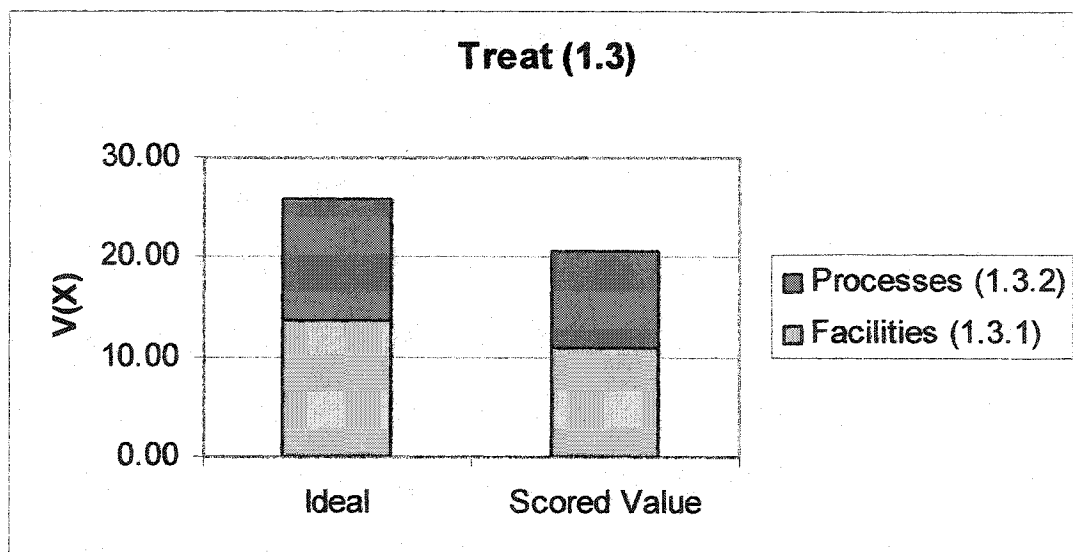


Figure 23. Treatment Subsystem Value

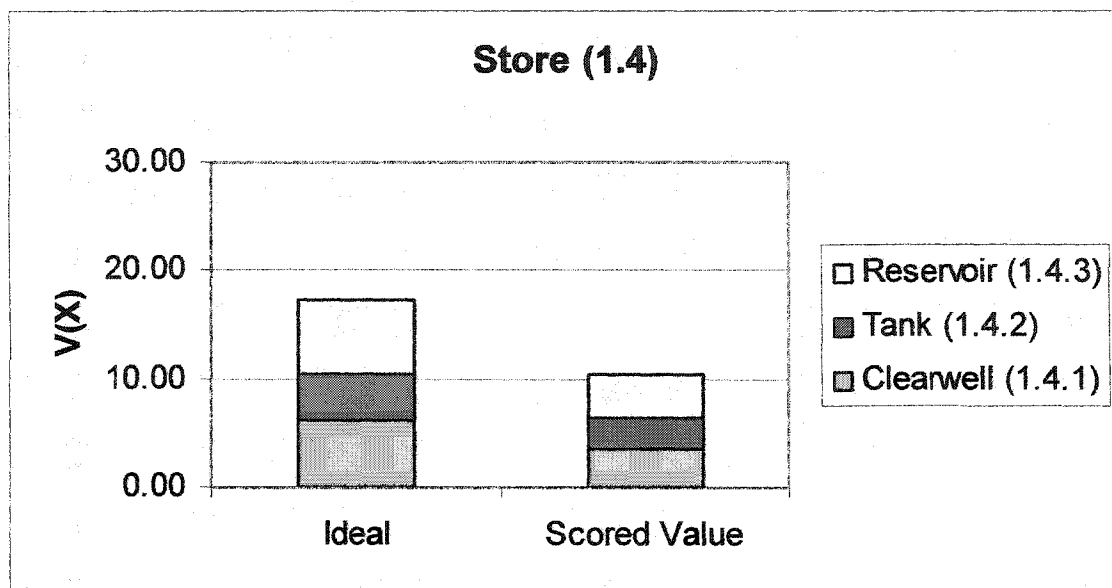


Figure 24. Storage Subsystem Value

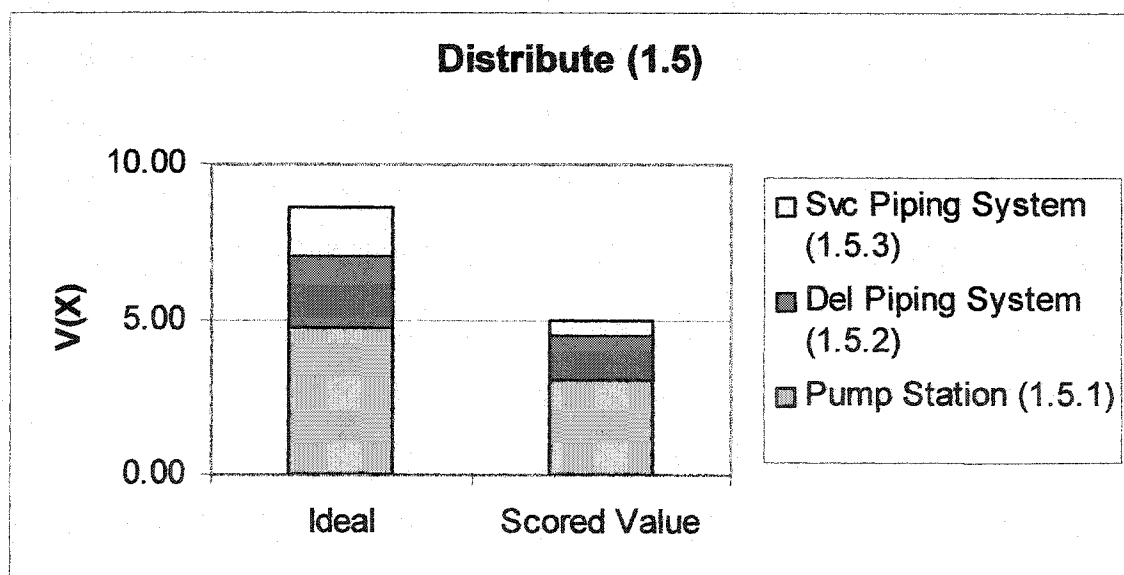


Figure 25. Distribution Subsystem Value

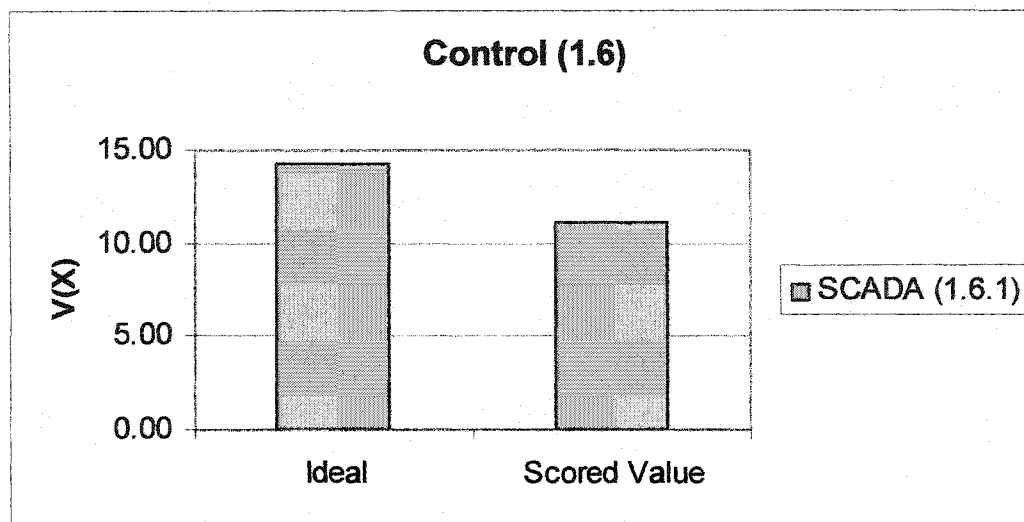


Figure 26. Control Subsystem Value

Figure 27 is different from figures 21-26 in that it shows the distribution of values of vulnerability. The distribution is the result of a simulation of 150,000 trials.

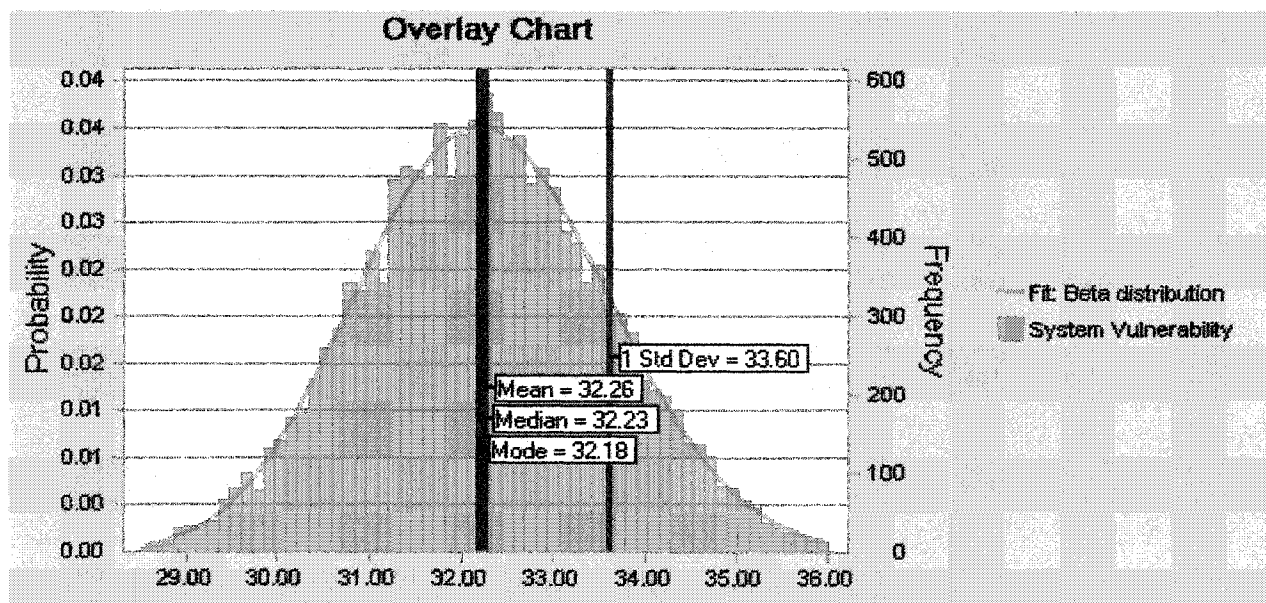


Figure 27. System Distribution of Vulnerability (Ω)

Sensitivity Analysis

Sensitivity of the model was assessed in two ways. The first was to look at the type of simulation: Monte Carlo and Latin Hyper-cube. For each simulation, the mean, median, mode and standard deviation were very close, within 1/100th of 1 percent as shown in the table 11 below. However, the Gamma distribution was slightly better fit than the Beta distribution for the Latin Hyper-cube simulation. An example of the Latin Hyper-cube is shown in figure 28 below.

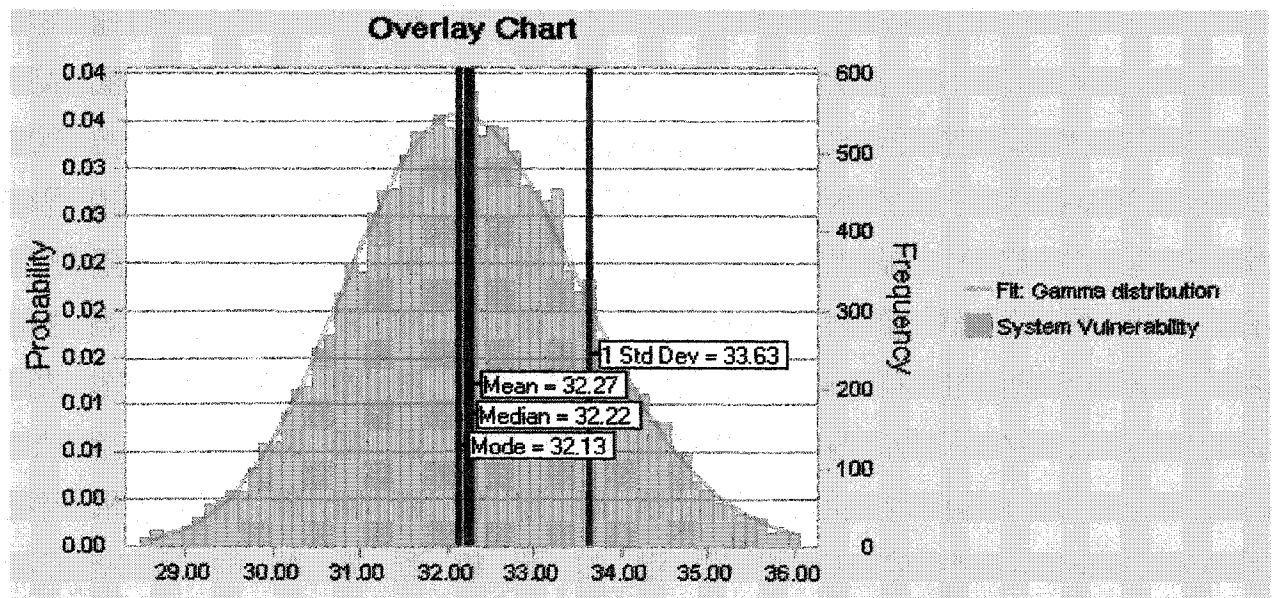


Figure 28. Latin Hyper-cube simulation of 15,000 trials

Table 11 summarizes the comparison of Monte Carlo and Latin Hyper-cube simulations.

Table 11. Sensitivity of Simulation Runs: Monte Carlo vs. Latin Hyper-cube

Trials	Monte Carlo	Latin Hyper-cube
150,000	Mean: 32.26	Mean: 32.27

Trials	Monte Carlo	Latin Hyper-cube
	Median: 32.23 Mode: 32.18 Standard Dev: 33.60 Distribution: Beta	Median: 32.22 Mode: 32.13 Standard Dev: 33.63 Distribution: Beta

The second way that sensitivity was addressed was to determine which model parameters contributed most to output. Figure 29 shows the each parameters contribution to variance within the model. This is useful because it allows the user to focus in on what assumptions are most important and which are not important.

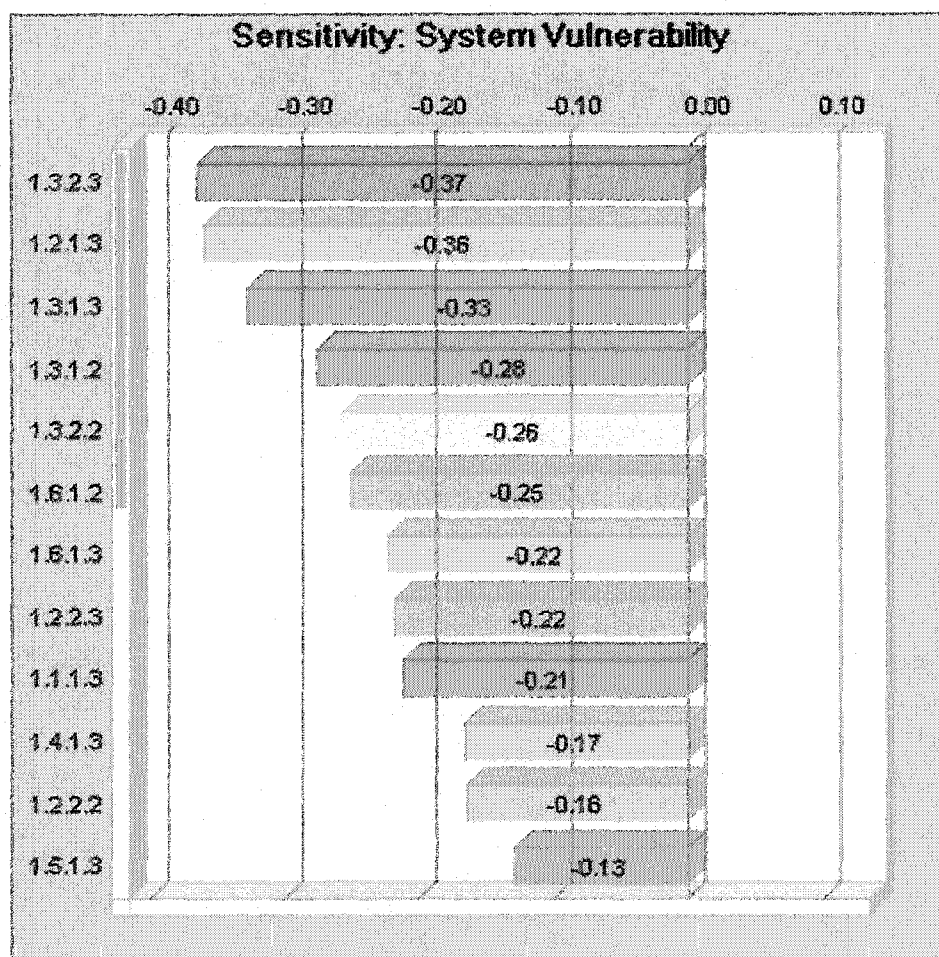


Figure 29. Output Sensitivity to Input Parameters

Eight of 14 detection probabilities are sensitive. A change in detection weights could modify the overall system score. Put another way, detection probability is very important in the model and lends insight into where one might study the system closely to determine where one might improve system performance. Delay is also sensitive. Three of 14 components were affected by the delay measure weight. As in the case of detection, delay offers insight into how one might improve system performance. The areas shaded in grey in table 12 below indicate where in the model measures are sensitive. The implication here is that significant changes to the weights from figure 29 would may change the score. But just as importantly, the parameters identified in figure 29 also inform the researcher where improvements could be made to improve vulnerability in the system.

Table 12. Location of Sensitive Measures in the Model

Measure	Component	Subsystem	System
Deter (.1)	River (1.1.1)	Source (1.1)	Clean Water System
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Well(1.1.2)	Source (1.1)	
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Pump Station (1.2.1)	Transmit (1.2)	
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Pipelines (1.2.2)	Transmit (1.2)	
Delay (.2)			

Measure	Component	Subsystem	System
Detect (.3)	Valves (1.2.3)		
Respond (.4)			
Deter (.1)			
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Facilities (1.3.1)	Treat (1.3)	
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Processes (1.3.2)		
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Clearwell (1.4.1)	Store (1.4)	
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Tank (1.4.2)		
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Reservoir (1.4.3)		
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Pump Station (1.5.1)	Distribute (1.5)	
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Del Piping System (1.5.2)		
Delay (.2)			
Detect (.3)			
Respond (.4)			
Deter (.1)	Svc Piping System (1.5.3)		
Delay (.2)			

Measure	Component	Subsystem	System
Detect (.3)			
Respond (.4)			
Deter (.1)	SCADA (1.6.1)	Control (1.6)	
Delay (.2)			
Detect (.3)			
Respond (.4)			

Face Validity

SMEs 1,2, and 3 was shown the model and engaged in a discussion of its design and use guided by the semi-structured interview form in Appendix F.. SME-3 admired the model and its usefulness in water systems. One criticism was the user interface which he considered very poor. Another criticism was that the decomposition although a very good approximation of most systems, might have to be changed to account for unique designs. For instance, the physical locations of a treatment facility may in some cases be so close to the storage component that the decomposition may need to be treated differently. SME-3 was asked to comment on the model's usefulness in other areas such as sewage, Supervisory Control and Acquisition Systems or Distributed Control Systems exclusively, as well as other infrastructure sectors. Based on the model structure and the design, he saw value in each of these areas.

SME-2 was enthused about the model. He liked the fact that the model is built upon the values of the experts who know the most about the system. He was concerned however, about whether a utility staff could use the model in its current form due to the number of spreadsheets and workbooks. One major advantage that SME-2 pointed out was the fact that if he and his staff developed an action plan to change their system in

response to vulnerability assessment score, they could reenter the change and observe how the model changed.

SME-1 was concerned that the control system was not decomposed into tremendous detail and analyzed separate from the water system. However, accepting how the model was designed to work, he agreed that the output would be useful in at a minimum understanding where the system was vulnerable. With an actual number, omega value in hand, he could approach management with justification to spend resources as the model suggested.

Summary

Chapter IV provided the results of the research design. The research design was carefully followed to ensure the validity of the results. The clean water system vulnerability value model was applied to a notional clean water system and shown to quantify vulnerability. The results of the model indicated an omega value of vulnerability of 32. Sensitivity analysis showed the model to be stable for Monte Carlo and Latin Hyper-cube random number sampling techniques with virtually no changes in output. A sufficiently large trial size of 150,000 provided assurance of the score and the distribution of vulnerability and an acceptable standard error. Sensitivity analysis also indicated that the detection probability and delay measure are important in that they impact the output more than deter and response protection measures. Subject matter experts believe that the model does what it claims to do and would be useful in quantifying vulnerability to a clean water system. On the question of face validity, all SMEs felt the model did what it claimed to do and would be useful in water systems as

well as Supervisory Control and Data Acquisition Systems, Distributed Control Systems and other critical infrastructures such as the electric sector.

CHAPTER V

CONCLUSION

This research began with four research questions that were introduced in Chapter I to guide the scholarly inquiry. Chapter II comprised the literature review to determine the extent to which vulnerability needed addressed. It became clear that vulnerability was not defined in a rigorous way, nor was it found to be quantified in any previous research. This justified the worthiness of this research effort and Chapter III was used to develop the methodology and research design that would guide the research. Chapter IV provided the results and the analysis of the research. Chapter V begins with a summary of the findings of the research. Next, it provides a discussion of future research to improve the body of knowledge on the theory of vulnerability. Finally, the chapter concludes with a discussion of the significance of this research and the contribution to theory, academia and practice.

This research was comprised of four study questions: (1) What is vulnerability as it applies to critical infrastructure systems?, (2) How does risk and systems theory apply to critical infrastructure vulnerability?, (3) How can critical infrastructure vulnerability be quantified?, and, (4) What results from the deployment of a systems-based model that quantifies vulnerability to a critical infrastructure such as a water system? This research answered these questions in a rigorous manner using the research design presented in Chapter III. This was significant because each question represented a gap in the scholarly body of research on critical infrastructure vulnerability.

As the research conveyed in Chapter II and III, vulnerability is the susceptibility of the infrastructure to threat scenarios. This research has shown that vulnerability can be quantified by the protection measures of deterrence, detection, delay and response as designed in Chapter III and demonstrated in Chapter IV. Quantification of vulnerability is meaningful because the omega value of vulnerability can be readily compared to the system's ideal score. This research has shown that the threat scenario is the link between risk and vulnerability. Risk is comprised of scenario, likelihood, and consequence and vulnerability is comprised of scenario, protection, and relative importance. Systems theory was used to inform the vulnerability value model design. Chapter III showed how vulnerability could be quantified by using the value model construct. The value model provided the logical means to quantify vulnerability because the model is based on the values of the experts who know their system. The deployment of the model in Chapter IV showed that a clean water system's vulnerability could be quantified and represented mathematically. The result of deploying the model was the quantification of vulnerability in a meaningful way. This research provides engineering managers, risk professionals and water managers with a means to quantify vulnerability to medium sized clean water systems.

Significance

Quantifying vulnerability to clean water systems is a significant contribution because the US alone has 54,000 systems providing water to 263 million customers American Water Works Association (AWWA) 2002. The number of utilities and customers who could benefit from this research in the US alone represents a large number of people.

This research contributed to the body of knowledge by reviewing and then synthesizing the limited literature on vulnerability in Chapter II, culminating with a definition of vulnerability and the beginning of a theory of vulnerability for the research community. The theory of vulnerability is unique and novel contribution with potential to expand in research in many directions of work. But this research did not test the theory of vulnerability, as task was beyond the scope. It is however encouraged of the future researcher. This research established the link between risk and vulnerability as the threat scenario. A discussion of future research on threat scenarios is presented later in this chapter. In addition, contributions also included academia and practical (DOD, governments, and private industries). The academic contribution to the field of engineering management is the systems-based vulnerability model that quantifies vulnerability for a critical infrastructure, which until this point has never been accomplished. The practical implications of the research include providing decision-makers with a model to help them understand system vulnerability so that resources can be allocated in a meaningful way. Practitioners are provided with the model and the references that allow them to conduct their own analysis. The model was significant in that the manner in which vulnerability is quantified can be useful in other critical infrastructures. The following section discusses ideas and concepts that will hopefully motivate future researchers to continue to expand the body of knowledge with respect to quantification of vulnerability..

Discussion of Future Research

This research has shown how one can quantify vulnerability to clean water systems. The research does not demonstrate how one may use the logic of value models to quantify vulnerability to other systems or critical infrastructures. For example, electric power can be decomposed into subsystems and components and appropriate measures identified to measure. In a similar fashion, all critical infrastructures may be decomposed and their vulnerability assessed. The idea here is that this research approach should be expanded into other critical infrastructures.

One limitation of the value model design is the necessity of independence between each component and subsystem. It may be shown that for some systems, independence is not possible so there exists a need to account for the dependencies. One way to accomplish this is to use interaction matrices and causal diagrams to identify the dependencies. Coefficients of dependence might be used to account for dependence before applying the value model. For example, causal loop diagrams could indicate the influence either the same or opposite. The strengths of those influences could be assessed as future research, then accounted for through a coefficient of interaction before the data is entered into the Vulnerability Value Model.

Another limitation is that the theory of vulnerability, although novel, is still in the beginning stages. Future researchers should design research to test the theory. Future researchers might look at the evaluation measures of protection and from additional research refine the relationship beyond the triplet presented in this research. In addition, a future researcher should develop a complete vulnerability assessment methodology as

this body of research pointed out in Chapter II that no systems-based methodology can be found in the literature.

Vulnerability Index Score

Another potentially useful area of research is designing a vulnerability index score that is benchmarked to known standards such as the Homeland Security standard for threat level. An index score is useful because national or state policy requirements could be associated with each index. For example, figures 30 and 31 show an index of 1-4 corresponding to Homeland Security standards.

In practice, any critical infrastructure that achieves a score beyond an acceptable level would require action on the part of the stakeholders. Figure 30 is a sample from a model that changes color based on vulnerability level. The scores are indexed to Homeland Security. The future researcher would want to determine the benchmark to create the index. It is believed by the author that a vulnerability index would be a significant contribution to Homeland Security. In the final section, threat scenarios were identified in this research as the link between risk and vulnerability. Yet this body of research did not explore how threat scenarios might be used in quantifying vulnerability. The final section provides a background that might be useful for future researchers.

Subsystem-->	Source								Transmit											
local wt-->	0.08								0.13											
Component-->	River				Well				Pump Station				Pipelines				Valves			
local wt-->	0.23				0.77				0.45				0.18				0.36			
Eval Measure-->	d1	d2	d3	r	d1	d2	d3	r	d1	d2	d3	r	d1	d2	d3	r	d1	d2	d3	r
local wt-->	0.11	0.26	0.26	0.37	0.11	0.26	0.26	0.37	0.11	0.26	0.26	0.37	0.11	0.26	0.26	0.37	0.11	0.26	0.26	0.37
global wt-->	0.0020	0.0046	0.0046	0.0066	0.0066	0.0153	0.0153	0.0219	0.0065	0.0151	0.0151	0.0216	0.0026	0.0060	0.0060	0.0086	0.0052	0.0121	0.0121	0.0173

RAW DATA MATRIX

Ideal-->	5	1.00	120	0	5	1.00	120	0	5	1.00	120	0	5	1.00	120	0	5	1.00	120	0
Baseline-->	2	0.20	0	30	3	0.40	5	5	3	0.60	10	5	2	0.50	10	15	1	0.30	15	20

VALUE MATRIX

PROTECTION VALUE

Ideal-->	0.20	0.46	0.46	0.66	0.66	1.53	1.53	2.19	0.65	1.51	1.51	2.16	0.26	0.60	0.60	0.86	0.52	1.21	1.21	1.73
Baseline-->	0.06	0.05	0.00	0.05	0.39	0.92	0.92	1.10	0.39	1.06	1.10	1.08	0.08	0.39	0.44	0.09	0.05	0.42	1.03	0.16

COMPONENT VALUE AND VULNERABILITY

	River	Well	Pump Station	Pipelines	Valves
Ideal-->	1.78	5.92	5.83	2.33	4.66
Baseline-->	0.15	3.33	3.62	0.99	1.66
Vulnerability-->	1.62	2.59	2.21	1.34	3.00

SUBSYSTEM VALUE AND VULNERABILITY

	Source	Transmit
Ideal-->	7.69	12.82
Baseline-->	3.49	6.28
Vulnerability-->	4.21	6.54

VULNERABILITY INDEX SCORE

component-->	4	2	2	3	3
subsystem-->	3		3		
Overall System-->	2				

Figure 30. Vulnerability Index Score Model

Vulnerability Index Legend				
Bins		Index	Color	Level
0	0.24	1	White	Low
0.25	0.49	2	Yellow	Guarded
0.5	0.74	3	Orange	Elevated
0.75	1	4		Sever

Figure 31. Vulnerability Index Score

Threat Scenarios

A scenario is defined as an outline, script, or sequence of events (dictionary.com, 2003). In the discipline of risk analysis, scenarios were made explicit by Kaplan and Garrick (1981); Kaplan, Zlotin, and Vishnipolski (1999); and refined by Kaplan, Haines and Garrick (2001). Fundamental to the theory of scenario structuring is the requirement that scenarios be (1) complete, (2) finite, and (3) disjoint. In Kaplan and Garrick (1981) the authors point out that scenario was loosely defined as “What can go wrong?” In Kaplan, Haines and Garrick (2001); the authors attempt to bridge Hierarchical Holographic Modeling (HHM) Haines (1981), a means for identify sources of risk with the theory of uncertainty. The approach focuses on using the philosophy of HHM to holistically identify sources of risk from multiple perspectives: functional, temporal, geographical, etc. The authors then introduce rate and weight methodologies to arrive at a subset of scenarios from which to proceed. The authors do not address however, how one explicitly defines a scenario, nor the limit of the universal set of all risks and scenarios. In fact, even if one satisfies the criteria above, the essential components of the scenario remain an open question in the literature.

AWWA (2002) identify water system scenarios as potentially bad situations for desktop exercises. The list is a much less rigorous approach than the academic approaches of Kaplan, Haines, and Garrick. AWWA (2002) did not attempt rigor. Instead they developed commonsense situations to guide the thought process of how to assess the security of their water system. The limitation of this approach is that identifying a simple list of situations as scenarios does not use any formal data to substantiate the list of scenarios and therefore they are susceptible to criticism. The list of situations, however, are the ones deemed important by the water community.

The Emergency Management Division(EMD) (2001) identifies six hazard categories that are useful in addressing scenarios against water systems: biological, chemical, nuclear, incendiary, explosive, and cyber. EMD (2001) also use the term “target” which is similar to Haines (1981) “sources of risk” identified with HHM. AWWA (2002) presents a similar list that is more closely focused on water contamination: blister, nerve, biological, chemical and bacterial hazards. AWWA (2002) then estimates the likelihood and severity of each hazard. Whereas some work on structuring scenarios is present in the literature, there is no agreed upon definition of scenario or unified structure to scenarios. For example, a future researcher might define a scenario as a hazard plus an action event (verb) and an object for the action (object): hazard + verb + action. There are several techniques in the literature for organizing scenarios. Affinity diagramming (Kawakita, 2002) might be used to map AWWA (2002) hazards and EMD (2001) scenarios into one hierarchy. To complete the notion of a complete scenario (hazard + verb + object), one might use an organized approach to

hierarchy design such as Armstrong and Sage (1999) and Gibson (1991). Both use the notion of verb and object to complete the idea of an objective. To ideate scenarios, many techniques exist such as strategy tables, brainstorming, brain writing, dynamic confrontation etc. The important point is that this research does not present new theory on scenario development. Instead, this research uses well known scenarios and hazards and represents them in the form: (1) hazard, (2) verb and (3) object. To be a scenario, all three attributes must be present. The theoretical number of possible scenarios then is based on the fundamental principle of counting. The set of all possible scenarios for a system is the number of hazards times the number of verbs that describes the action and the objects of the action. This might become the universal set of scenarios for a system. There is some data available and a more thorough literature review may reveal more.

For example, a survey conducted by Ezell (2003) concluded that the disgruntled employee is the most dangerous person of concern to water system managers. Using the information from EMD (2001) and AWWA (2002) five scenarios are presented for use in the application of quantifying vulnerability to a clean water system. Much reliance is placed on the scenarios identified by AWWA (2002) and supplemented by EMD (2001) in the form of hazard, verb, and object. Although it is convenient to include additional contextual information such as who, when and why, this research uses what (hazard and verb) and where (object) for quantifying vulnerability. In summary, constructing a scenario is an event comprised of a (1) hazard, (2) verb (action), and (3) object (of the action). Scenarios are taken from the general form and tailored to the system in focus.

Scenario 1: Disgruntled employee damages pumping stations beyond reasonable repair that provides water flow for the entire distribution system.

Scenario 2: Terrorist dump a substance** into a water tank that provides clean drinking water for a large neighborhood

Scenario 3: Hackers conduct a Denial-of-service attack against the Utility's SCADA System

Using the vulnerability value model, virtually all scenarios could be assessed.

Dominate scenarios would score the highest and become the basis for allocating resources. Determining what scenario to model is potentially an art and a science based on the experience of experts, political environment and other factors. Future researchers will find this domain an open area to explore. The implication here is that a future researcher could infer from the literature and develop a new theory and methodologies of scenarios that could be useful to the vulnerability and risk research disciplines.

Summary

This chapter provided a recap of the findings of this research and a discussion of future research. This research showed that multiple definitions of vulnerability and quantification has not been adequately addressed. Therefore this research endeavored to develop and deploy a systems-based model that quantifies vulnerability to critical infrastructure, focusing on clean water systems. This research defined critical infrastructure vulnerability as a measure of the susceptibility of critical infrastructure to threat scenarios. The research established that vulnerability is a function of 1) threat scenario, 2) protection and 3) importance. Also, critical infrastructure vulnerability was

measured by a system's 1) deterrence, 2) detection, 3) delay and 4) response capabilities. The importance of components and subsystems in the overall clean water system, implied that some subsystems are more critical to overall system performance than other subsystems. A value model was used as the logic construct for quantifying vulnerability. Subject-matter experts were queried to establish the shapes of value functions and importance (weights) in the model. Another set of subject-matter experts were queried to assess a notional clean water system with respect to each protection measure within the vulnerability value model. To accomplish this, two simulations were executed in the model. The first simulation aggregated expert assessments into one assessment. The results were then used as inputs into the vulnerability value portion of the model for use in the second simulation where vulnerability was quantified. Results of this research demonstrate that vulnerability can be quantified and that quantifying vulnerability is useful to decision-makers who prefer quantification to qualitative treatment of vulnerability. Subject matter experts agreed that the model passed the face validity test. This research is a novel contribution to the body of scholarly work by 1) providing a rigorous method to quantify vulnerability to critical infrastructure, 2) introducing the beginning of a theory of vulnerability, and 3) specifying the relationship between vulnerability and risk. Subject matter experts conclude that there is value in the approach put forward in this body of research as it is applied to clean water systems, so it may be useful in other critical infrastructures. The research closes with directions for further research. Chapter V indicated that research in a vulnerability index score tied to Homeland Security, as well as research in scenario design are potentially beneficial areas

to research.

REFERENCES

- Alkin, M. (1979). *Using Evaluations: Does Making Evaluations Make a Difference?* Sage, Beverly Hills, CA.
- Armstrong J.E., and Sage, A.P. (1999). *An Introduction to Systems Engineering*, John Wiley and Sons, New York, NY.
- American Public Power Association (APPA) (2003). *Annual Directory and Statistical Report*. Retrieved February 21, 2003 from www.appanet.org.
- Ang, A. and Tang, W. H. (1984). *Probability Concepts in Engineering Planning and Design: Volume II Decision, Risk, and Reliability*, John Wiley and Sons, New York, NY, Chapter 4.
- American Water Works Association (AWWA) (2002a). *Emergency Planning for Water Utilities*. Retrieved September 15, 2002 from <http://www.awwa.org/communications/offer/september.cfm>.
- American Water Works Association (AWWA) (2002b). *Water System Security: A Field Guide*, American Water Works Association.
- Association of State Drinking Water Administrators (2002). *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems*, National Rural Water Association (NWRA). Retrieved August 2002 from <http://www.mrwa.com/downloads/SecurityAssessment-Final20Small20System20VA20tool.pdf>.
- Babbie, E. (2001). *The Practice of Social Research: 9th Edition*, Wadsworth Thomas Learning, Belmont, CA., pp.124-125.
- Barnett, V. (1991). *Sample Survey Principles and Methods*, Edward Arnold Publisher, London, England.
- Blaikie, P., Cannon, T., Davis, I., and Wisner, B. (1994). *At Risk: Natural Hazards, People's Vulnerability, and Disasters*, Routledge, London, UK.
- Buckle, P. (2000). *Assessing Resilience and Vulnerability in the Context of Emergencies: Guidelines*, Victorian Government Publishing Service. Retrieved October 20, 2002 from www.anglia.ac.uk/geography/radix/resources/buckle-guidelines.pdf.
- Buckle, P., and Mars, G. (2000). "New Approaches to Assessing Vulnerability and Resilience", *Australian Journal of Emergency Management*, Winter. Retrieved

October 20, 2002 from <http://www.anglia.ac.uk/geography/radix/resources/buckle-marsh.pdf>

Center for Defense Information (CDI) (2002). *Securing U.S. Water Supplies*. Retrieved January 20, 2003 from <http://www.cdi.org/terrorism/water-pr.cfm>.

Chytka, T.M. (2003). Development of an Aggregation Methodology for Risk Analysis in Aerospace Conceptual Vehicle Design, Ph.D. Dissertation. Department of Engineering Management, Old Dominion University, Norfolk, VA.

Creswell, J.W. (1994). *Research Design: Qualitative and Quantitative Approaches*, Sage publications, London, England.

Decisioneering (1996). Crystal Ball User's Manual, Decisioneering, Inc., United States of America.

Emergency Management Division, Washington Military Department, Hazard Specific Assessment (EMD) (2001). *Emergency Management Council of State-Wide Emergency Preparedness*. Retrieved July 2004 from www.emd.wa.gov.

Erlandson, D., Harris, E., Skipper, B., and Allen, S. (1993), *Doing Naturalistic Inquiry*, London: Sage Publications.

Ezell, B.C. (1998). "Quantifying The Risk Of Cyber Intrusion Through Total Risk Management", *SCADA at the Crossroads Proceedings*, Institute of Engineers of Australia, November 6, 1998, Perth, AU.

Ezell, B.C., Haimes, Y.Y., and Lambert, J.H. (2001). "Risks of Cyber Attack to Water Utility Supervisory Control and Data Acquisition Systems", *Military Operations Research Journal*, Vol. 6, No. 2, pp. 30-46.

Ezell, B., Farr, J., and Wiese, I. (2000a). "Infrastructure Risk Analysis Model", *Journal of Infrastructure Systems*, Vol. 6, No. 3, pp. 114-117.

Ezell, B.C., Farr, J.V., Wiese, I. (2000b) "An Infrastructure Risk Analysis of a Municipal Water Distribution System", *Journal of Infrastructure Systems*, Vol. 6, No. 3, pp. 118-122.

Ezell, B.C. (2003a). "Security and Risk Management in SCADA systems", Keynote presentation, sponsored by IBC Conferences on Information and Communication, February 12, 2003, London, UK.

- Ezell, B.C. (2003b). "Vulnerability, SCADA and Critical Infrastructure", Keynote presentation, sponsored by IBC Conferences on Information and Communication, June 16, 2003, Sydney, AU.
- Ezell, B.C. (2003c), "The Amorphous Security Model: Contextual Security in SCADA and Critical Infrastructure", Keynote presentation, sponsored by IBC Conferences on Information and Communication, October 6, 2003, Auckland, NZ.
- Gheorghe, A.V., Vamanu, D. V. (2001). *Fundamentals of Risk and Vulnerability Management QVA-Quantitative Vulnerability Assessment*. Retrieved January 20, 2002 from http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Gheorghe/tsld001.htm
- Gibson, J. (1991). *How to Do Systems Analysis and a Systems Decalogue*, University of Virginia Printing and Copying Services, Charlottesville, VA.
- Haimes, Y.Y. (1981). "Hierarchical Holographic Modeling." *IEEE Transactions on Systems on Systems, Man and Cybernetics*, Vol. SMC-11, No. 9.
- Haimes, Y.Y. (1998). *Risk Modeling, Assessment, and Management*, John Wiley and Sons, New York, NY.
- Haimes, Y. Y., Lambert, J. H., and Kaplan, S. (2002). "Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling", *Risk Analysis*, Vol. 22, No. 2.
- Hightower, M. (2001). *Water Infrastructure Protection and Security-Emerging National Issues*, Sandia National Laboratories.
- International Strategy for Disaster Reduction (ISDR) (2001). *Targeting Vulnerability*, Retrieved February 3, 2002 from <http://www.unisdr.org/unisdr/camp2001guide.htm>
- Jackson, M. C. (1991). *Systems Methodology for the Management Sciences*, Perseus Publishing.
- Kaplan, S. (1997). "The Words of Risk Analysis." *Risk Analysis*, Vol. 17, No. 4.
- Kaplan, S., Zlotin, B., Zussman, A, and Vishnipolski, S. (1999). "New Tools for Failure and Risk Analysis—Anticipatory Failure Determination and the Theory of Scenario Structuring", Ideation International, Inc.
- Kaplan, S. and Garrick, B.J. (1981). "On the Quantitative Definition of Risk", *Risk Analysis*, Vol. 1, No. 1.

- Kaplan, S., Haimes, Y.Y. and Garrick, B.J. (2001), "Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk", *Risk Analysis*, Vol. 21. No. 5.
- Kawakita J. (2002). *Affinity Diagramming*. Retrieved July 1, 2004 from www.skymark.com.
- Keating, C. (2003a), ENMA 715/815 Systems Analysis, *Chapter 8: Gibson's Systems Methodology I*, Department of Engineering Management, Old Dominion University, Norfolk, VA.
- Keating, C. (2003b). ENMA 715/815 Systems Analysis, *Chapter 9: Gibson's Systems Methodology II*, Department of Engineering Management, Old Dominion University, Norfolk, VA.
- Keeney, R.L. (1992). *Value Focused Thinking; A Path to Creative Decision Making*, Harvard University Press (1992).
- Keeney, R.L. and Raiffa, H. (1993). *Decisions with Multiple Objectives; Preferences and Value Tradeoffs*, Cambridge University Press (1993).
- Kidder, L. and Judd, C.M. (1986). *Research Methods in Social Relations 5th Edition*, Holt, Rinehart and Winston, New York, NY.
- Leedy, D. and Ormrod, J. E. (2001). *Practical Research: Planning and Design 7th Edition*, Merrill Prentice Hall, New Jersey, pp. 148-149.
- Lowrance, W. (1976). *Of Acceptable Risk: Science and the Determination of Safety*, William Kaufmann, Inc., Los Altos, CA.
- McFadden II, W. (2002). A Systems-Based Methodology for the Construction And Representation of the Organizational Knowledge System, Ph.D. Dissertation. Department of Engineering Management, Old Dominion University, Norfolk, VA.
- National Oceanic and Atmospheric Administration. (NOAA) (2002). *Vulnerability Assessment*. Retrieved January 20, 2002 from <http://www.csc.noaa.gov/products/nchaz/htm/tut.htm>.
- Nilsson, J., Magnusson, S., Hallin, P and Lenntorp, B. (2002). *Vulnerability Analysis and Auditing of Municipalities*, Lund University. Retrieved October 20 from <http://www.isn.ethz.ch/crn/basics/process/documents/vulnerability.pdf>.

- National Security Telecommunications Advisory Committee (NSTAC) (1997). *Information Assurance Task Force Risk Assessment*. Retrieved December 3, 1997 from http://www.ncs.gov/n5_hp/reports/EPRA.html.
- Parnell, G.S., Jackson, J.A., Jones, B.L., Lehmkuhl, L.J., Conley, H.W., and Andrew, J.M., (1998). "Foundations 2025: A Value Model for Evaluating Future Air and Space Forces", *Management Sciences*, 44:10, pp.1336-1350.
- Palmquist, M. (2003). *Research Writing Guide*, Colorado State University. Retrieved November 10, 2003 from <http://writing.colostate.edu/references/research/gentrans/com2c1.cfm>
- Patton, M.Q. (2002). *Qualitative Research and Evaluation Methods 3rd Edition*, Sage Publications, London, England.
- Presidential Decision Directive 63 (PDD 63) (1998). *The Clinton Administration's Policy on Critical Infrastructure Protection*. Retrieved January 12, 2000 from <http://www.info-sec.com/ciao/paper598.pdf>.
- Rogers, R. (2002). ENMA 821, Research Design, Department of Engineering Management and Systems Engineering, Old Dominion University, Spring, 2002.
- Sousa-Poza, A. (2003). ENMA 828, Socio-Technical Systems Design, Department of Engineering Management and Systems Engineering, Old Dominion University, Spring, 2003.
- Stake, R.E. (1995). *The Art of Case Study Research*, Sage Publications, London, England.
- Wenger, A, Metzger, J., and Dunn, M. (2002). *International CIIP Handbook: An Inventory of Protection Policies in Eight Countries*, Center for Security Studies and Conflict Research.
- Yin, R.K. (1994). *Case Study Research: Design and Methods Volume 5*, Sage Publications, London, England.

APPENDIX A (Glossary of Terms)

This glossary of terms does not represent a rigorous set of definitions. It explains how these terms are used in this research.

1. A **system** is a group of elements or components that work together for a useful purpose (Armstrong and Sage 1999).
2. **Critical infrastructure** refers to those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private (PDD 63 1998).
3. **Generalizability** is as the extension of research findings and conclusions from a study conducted on a sample population to the population at large (Palmquist 2003).
4. **Risk** is a triplet of scenario, likelihood, and consequences (Kaplan 1997).
5. **System context** refers to a rich description of a system in a way that determines and frames its meaning. In systems analysis, contextual appreciation is necessary in understanding the problem. System context requires an appreciation of the set of circumstances, factors, conditions, values and patterns that are influential in constraining and enabling the systems engineering process, the system solution, and system solution deployment (Keating 2003a).
6. **Systems-Based methodology** is viewed from three perspectives along a continuum of philosophy, method, and technique. Philosophically, a systems-based methodology indicates a view that complex problems should be addressed holistically from a systemic perspective using system principles, concepts, and thinking. At the “method” level several frameworks can be used and are usually designed within the context of the study. And in the case of technique, many tools apply (simulation, math programming, etc.)(Keating 2003b)

7. **Triangulation** is the process of using multiple data collection methods, data sources, or theories to validate the findings of a research study (Erlandson, Harris, Skipper, & Allen, 1993).
8. **Transferability** is a process performed by readers of research. Readers note the specifics of the research situation and compare them to the specifics of an environment or situation with which they are familiar. If there are enough similarities between the two situations, readers may be able to infer that the results of the research would be the same or similar in their own situation. In other words, they "transfer" the results of a study to another context (Palmquist 2003).
9. **Traceability** refers to tracking and confirming the steps and procedures used by the researcher in developing the research concepts and administering the research design strategy. Traceability strives to ensure credibility and fidelity in the research explanation, data collection, analysis, and findings (Erlandson, Harris, Skipper, & Allen, 1993).

APPENDIX B SME-1 Interview Template and Notes

This interview is part of my research to fulfill requirements for a PhD in Engineering Management from the Department of Engineering Management and Systems Engineering, Old Dominion University.

Do you agree to participate? Sign and date: _____

1. Describe your experience?
2. How many years of experience do you have in water systems?
3. What duties do you perform?
4. How many years have you been employed at Fort Monroe, VA Public Works?
5. Based on research from the American Water Works Association, a clean water system can be functionally decomposed into the following areas (Show him the decomposition). Based on your experience do you agree or disagree with this representation?
6. If you disagree, how would you modify the representation?

APPENDIX C SME-2 Establishing the Importance Weights

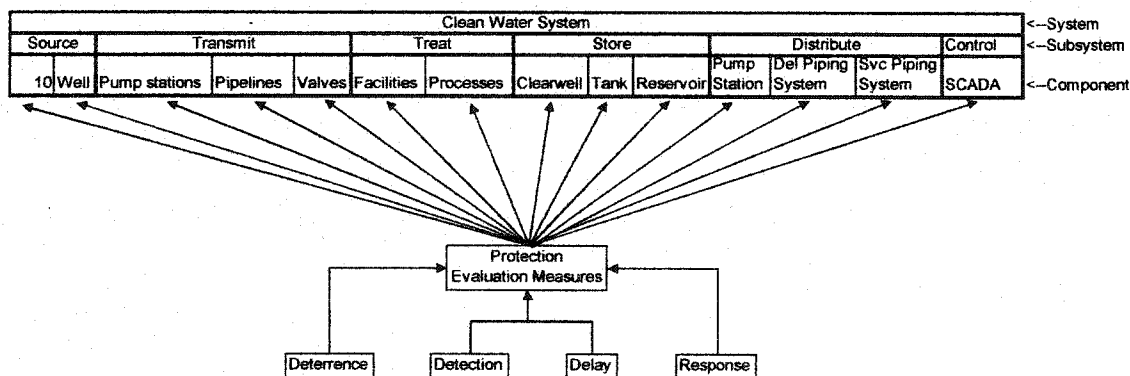
Instructions:

Rate your expertise on Water Systems on a scale of 1 to 10 where 1 is poor and 10 is the very best in the business.	7
How many years of experience do you have in water systems?	19
Please describe (below) what you believe makes an expert in water systems	

Note that self rating "expertise" is highly subjective. This is a very general question that can be a thesis question in itself. I'll try to take a stab at it. Expertise can be from the engineering/design standpoint- work with utilities to improve or upgrade operations and processes or equipment, after on-site study of issues such as existing infrastructure, required future demands and capital improvements, etc. Other experts come from the operations/management end, usually employed by the utility or Operations and Management Company, with hands on capabilities in the day to day operations of the system. Note that these are rough generalizations and there is mobility between the two broad groupings.

<-Enter rating here

****Upon completion, email this spreadsheet and your vitae or resume to barry.ezell@us.army.mil**



This picture represents a clean water system that is functionally decomposed into the subsystems and components shown above. The research asserts that protection can be measured by assessing deterrence, detection, delay and response. This consultation requests that you rate the "relative importance" of the subsystems, components and evaluation measures in this model. Please click the next tab... Thank you for your help.

Subsystem:

When you consider the overall importance of each subsystem of a clean water system decomposed below, rate the relative importance of each subsystem to the accomplishment of the purpose of the clean water system where 1 is not important and 10 is absolutely important. Importance is an important measure of vulnerability. The more important a sub-system function to overall system performance, increases the vulnerability.

Example level of importance

Rate the relative importance of each

Clean Water System	On a scale of 1 to 10...		Comment on why you changed
	Ex.	Expert	
1.0 Source	3	9	For wells, sources are usually multiple wells in a field. Contamination or loss of one well would be an inconvenience but not a disaster, hence a rating of 3. Contamination of a surface water source or run of river is usually much more difficult than an individual well but the effects can be more profound, hence a rating of 9
2.0 Transmit	4	9	Transmission mains can be a weak link in a water distribution system, and because of their long run, typically including isolated areas, sabotage can lead to disruption of service for prolonged periods.
3.0 Treat	10	9	For a water treatment plant, being out of commission can lead to extended loss of service from several days to weeks or months depending upon the extent of damage or contamination.
4.0 Store	5	6	Storage is important as contamination or destruction of storage can leave an area isolated for extended periods of time
5.0 Distribute	7	3	Usually, the distribution system is divided into zones that can be isolated (by manual valves) when either a commonplace disruption occurs (e.g. main burst) or sabotage
6.0 Control (SCADA)	8	5	In an emergency, a properly designed system can be operated, albeit with more difficulty and degraded efficiency, off line (i.e. in manual mode)

When you consider the overall importance of each subsystem of a clean water system decomposed below, rate the relative importance of each subsystem to the accomplishment of the purpose of the clean water system where 1 is not important and 10 is absolutely important.

1.0 Source	On a scale of 1 to 10		Comment on why you changed
	Ex.	Expert	
River	4	9	Loss of run of river source would usually put the system out of commission until contamination can be remedied.
Wells	9	3	Usually multiple wells in field. Loss of single well is more a nuisance than critical

When you consider the overall importance of each subsystem of a clean water system decomposed below, rate the relative importance of each subsystem to the accomplishment of the purpose of the clean water system where 1 is not important and 10 is absolutely important.

3.0 Treat	On a scale of 1 to 10		Comment on why you changed
	Ex.	Expert	
Facilities	10	10	Agree with rating. Not sure how you can divide facilities and processes. Destruction of facilities, if the intention is physical infrastructure is of course more difficult and time consuming to correct than disruption of processes, which may include sabotage of the SCADA system if distributed automated control used.
Processes	10	9	Disruption of process, usually can be contained by manual override

When you consider the overall importance of each subsystem of a clean water system decomposed below, rate the relative importance of each subsystem to the accomplishment of the purpose of the clean water system where 1 is not important and 10 is absolutely important.

4.0 Store	On a scale of 1 to 10		Comment on why you changed
	Ex.	Expert	
Clearwell	7		Tanks are more localized. Contamination of clearwell can put the WTP out of service until it can be drained and cleaned. Physical damage to clearwell of 9 course is more time consuming to rectify and hence more serious.
Tank	9		Tanks usually serve a local area. Elevated tanks are more for pressure regulation than long term storage.
Reservoir	10	10	Reservoirs generally serve a larger area than tanks and are more difficult to drain and clean in the event of contamination.

When you consider the overall importance of each subsystem of a clean water system decomposed below, rate the relative importance of each subsystem to the accomplishment of the purpose of the clean water system where 1 is not important and 10 is absolutely important.

5.0 Distribute	On a scale of 1 to 10		Comment on why you changed
	Ex.	Expert	
Pump Station	10		Pump systems are more difficult to repair or replace than pipe. As a rule, service 6 an extended area and cannot be isolated by valves
Delivery Piping System	7		3<--Relatively lower ratings due to localized nature. (to neighborhood)
Service Piping System	3		2<--Relatively lower ratings due to localized nature. (to single customer)

Rate the relative importance of deterrence, detection, delay, and response for each component.

1.0 Source	
> deterrence	10
> detection	10
> delay	9
> response	9
> deterrence	7
> detection	8
> delay	6
> response	6

3.0 Treat	
> deterrence	10
> detection	10
> delay	9
> response	10
> deterrence	10
> detection	10
> delay	8
> response	8

5.0 Distribute	
> deterrence	8
> detection	8
> delay	7
> response	7
> deterrence	7
> detection	6
> delay	5
> response	5

2.0 Transmit	
> deterrence	9
> detection	9
> delay	8
> response	8
> deterrence	9
> detection	10
> delay	9
> response	10
> deterrence	9
> detection	9
> delay	8
> response	7

4.0 Transmit	
> deterrence	10
> detection	10
> delay	9
> response	9
> deterrence	9
> detection	8
> delay	8
> response	7
> deterrence	10
> detection	10
> delay	10
> response	10

6.0 Control	
> deterrence	9
> detection	9
> delay	8
> response	8

Legend
 Subsystem

APPENDIX D SME-2 Establishing the Value Function

Instructions:

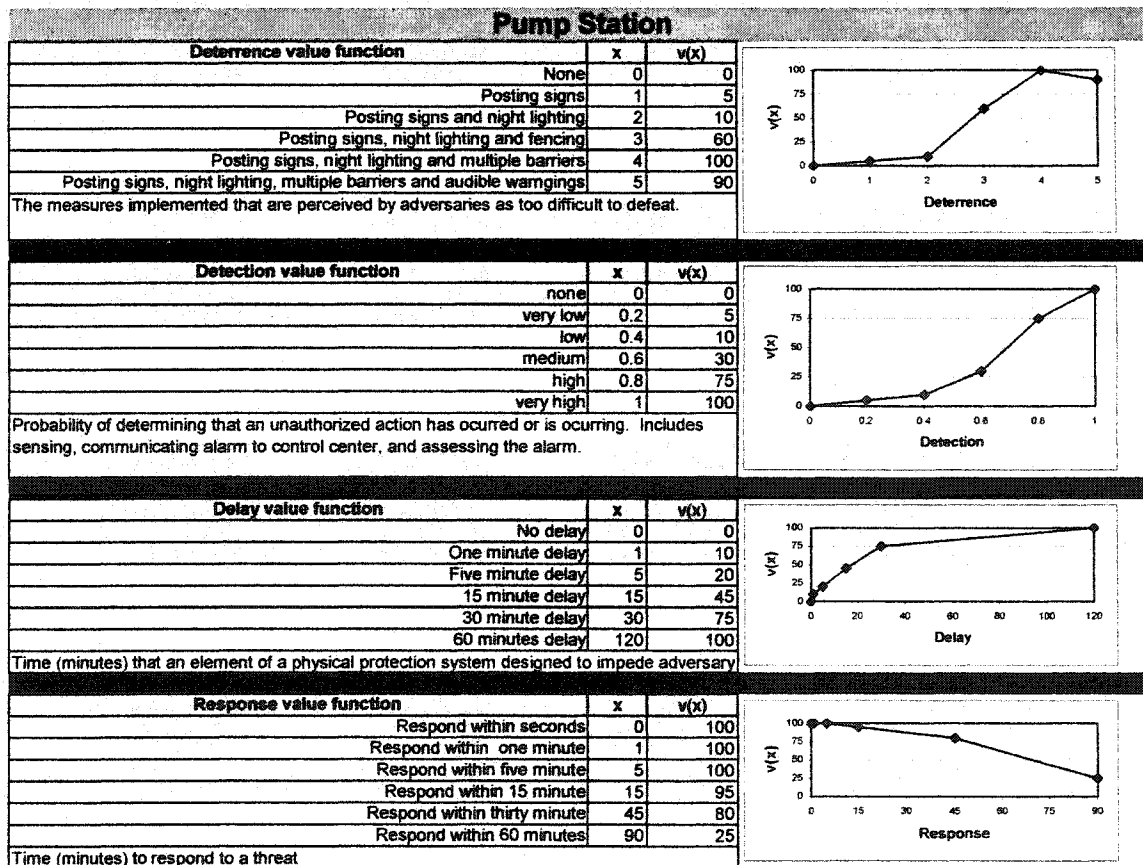
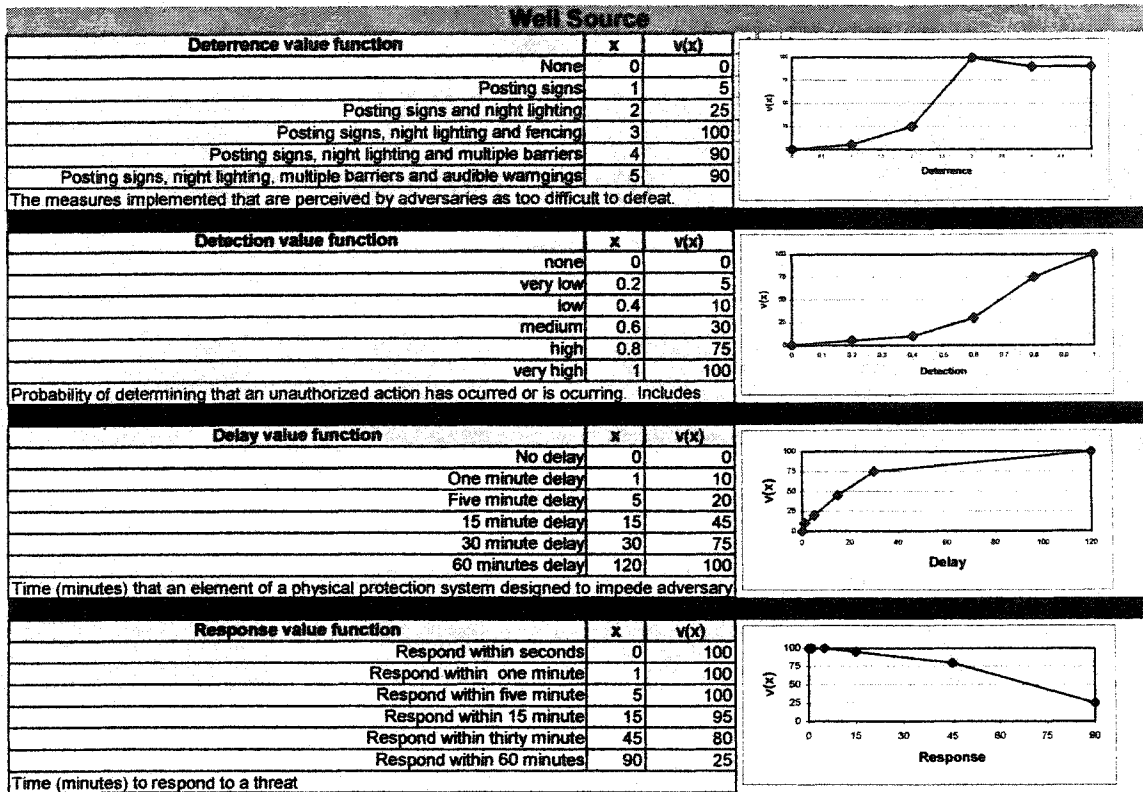
Adjust the cell under the V(x) column and determine the shape of the value function.

River Source		
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	20
Posting signs and night lighting	2	50
Posting signs, night lighting and fencing	3	100
Posting signs, night lighting and multiple barriers	4	90
Posting signs, night lighting, multiple barriers and audible warnings	5	90
The measures implemented that are perceived by adversaries as too difficult to defeat.		

Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100
Probability of determining that an unauthorized action has occurred or is occurring. Includes sensing, communicating alarm to control center, and assessing the alarm.		

Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100
Time (minutes) that an element of a physical protection system designed to impede adversary penetration into or exit from the protected area.		

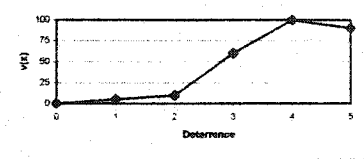
Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	75
Time (minutes) to respond to a threat		



Pipeline

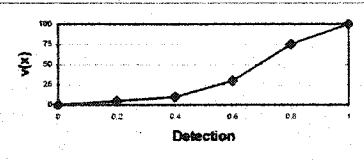
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	60
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



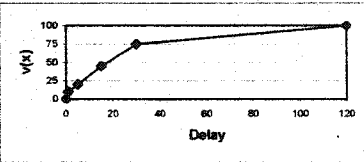
Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes



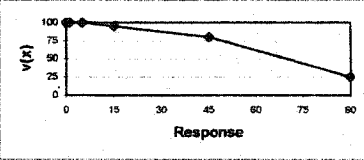
Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary



Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	25

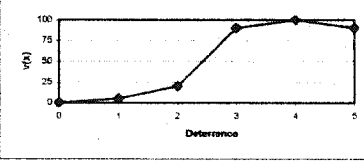
Time (minutes) to respond to a threat



Valves

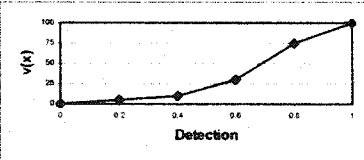
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	20
Posting signs, night lighting and fencing	3	90
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



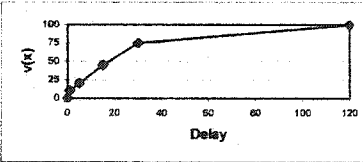
Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes



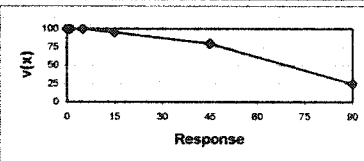
Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary



Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	25

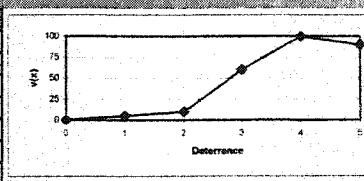
Time (minutes) to respond to a threat



Facilities

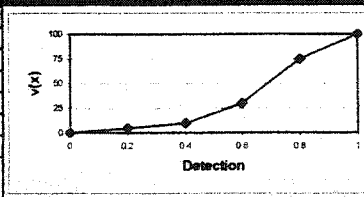
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	60
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



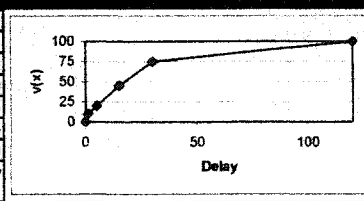
Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes sensing, communicating alarm to control center, and assessing the alarm.



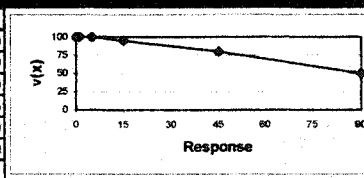
Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary penetration into or exit from the protected area.



Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	50

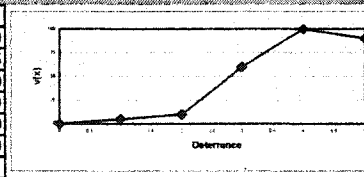
Time (minutes) to respond to a threat



Processes

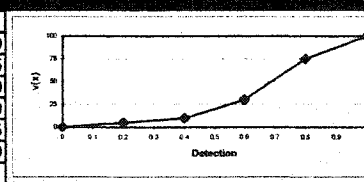
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	60
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



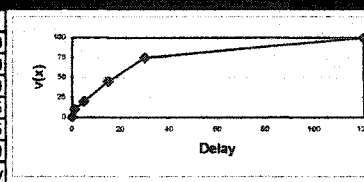
Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes



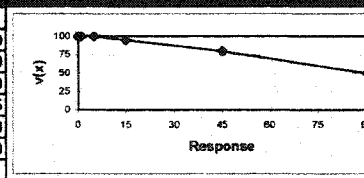
Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary



Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	50

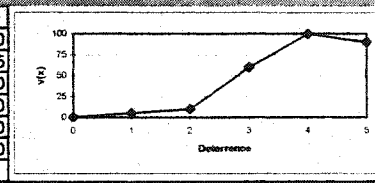
Time (minutes) to respond to a threat



Clearwell

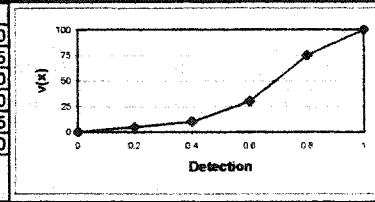
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	60
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



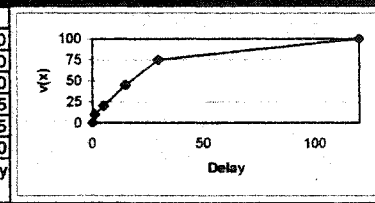
Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes sensing, communicating alarm to control center, and assessing the alarm.



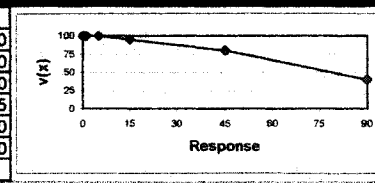
Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary penetration into or exit from the protected area.



Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	40

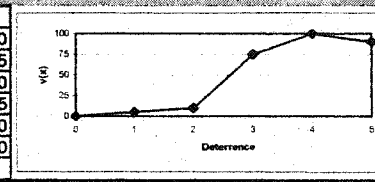
Time (minutes) to respond to a threat



Tank

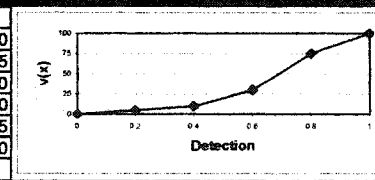
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	75
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



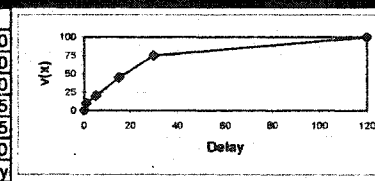
Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes

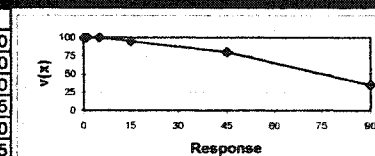


Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary



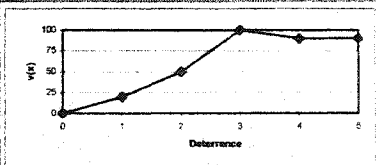
Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	35



Reservoir

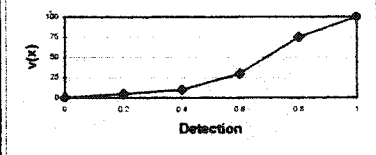
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	20
Posting signs and night lighting	2	50
Posting signs, night lighting and fencing	3	100
Posting signs, night lighting and multiple barriers	4	90
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



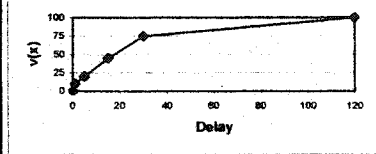
Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes



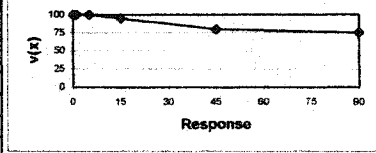
Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary



Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	75

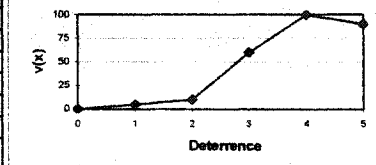
Time (minutes) to respond to a threat



Pump Station

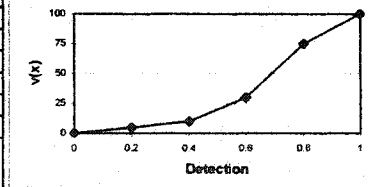
Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	60
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



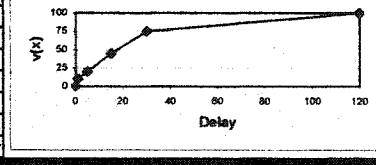
Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes sensing, communicating alarm to control center, and assessing the alarm.

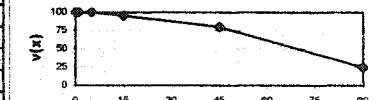


Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary

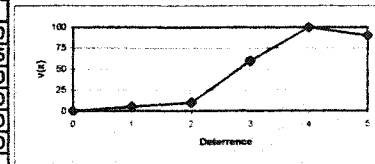


Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80



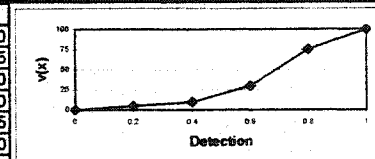
Def Piping System

Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	60
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90



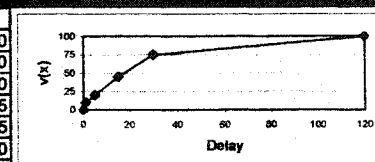
The measures implemented that are perceived by adversaries as too difficult to defeat.

Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100



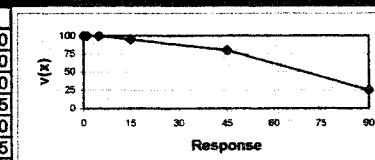
Probability of determining that an unauthorized action has occurred or is occurring. Includes

Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100



Time (minutes) that an element of a physical protection system designed to impede adversary

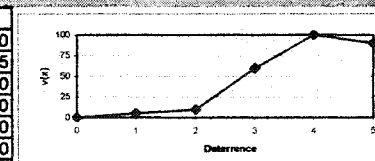
Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	25



Time (minutes) to respond to a threat

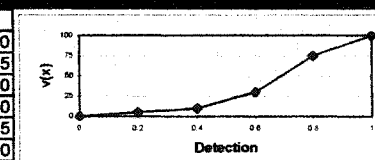
Src Piping System

Deterrence value function	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	60
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90



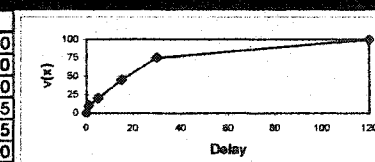
The measures implemented that are perceived by adversaries as too difficult to defeat.

Detection value function	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100



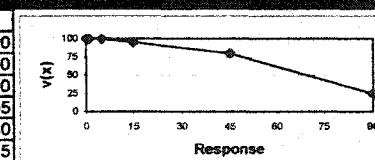
Probability of determining that an unauthorized action has occurred or is occurring. Includes

Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100



Time (minutes) that an element of a physical protection system designed to impede adversary

Response value function	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	25

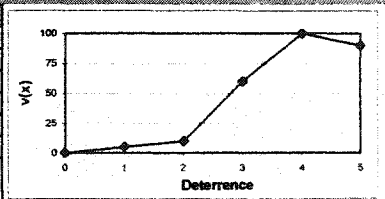


Time (minutes) to respond to a threat

SCADA

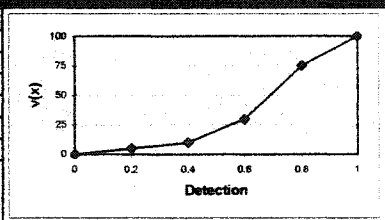
Deterrence value function		
	x	v(x)
None	0	0
Posting signs	1	5
Posting signs and night lighting	2	10
Posting signs, night lighting and fencing	3	60
Posting signs, night lighting and multiple barriers	4	100
Posting signs, night lighting, multiple barriers and audible warnings	5	90

The measures implemented that are perceived by adversaries as too difficult to defeat.



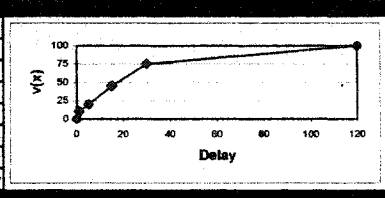
Detection value function		
	x	v(x)
none	0	0
very low	0.2	5
low	0.4	10
medium	0.6	30
high	0.8	75
very high	1	100

Probability of determining that an unauthorized action has occurred or is occurring. Includes sensing, communicating alarm to control center, and assessing the alarm.



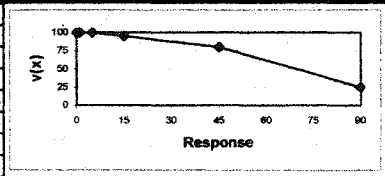
Delay value function		
	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	45
30 minute delay	30	75
60 minutes delay	120	100

Time (minutes) that an element of a physical protection system designed to impede adversary



Response value function		
	x	v(x)
Respond within seconds	0	100
Respond within one minute	1	100
Respond within five minute	5	100
Respond within 15 minute	15	95
Respond within thirty minute	45	80
Respond within 60 minutes	90	25

Time (minutes) to respond to a threat



APPENDIX E SME-1 and -2 CWS Assessment

Shown below is a sample of the spreadsheet that the SMEs used to score the clean water system. Below the example is the raw data from both SMEs organized into a table.

River Source		
Deterrence value function	x	v(x)
None	0	1
Posting signs	1	10
Posting signs and night lighting	2	30
Posting signs, night lighting and fencing	3	80
Posting signs, night lighting and multiple barriers	4	80
Posting signs, night lighting, multiple barriers and	5	100
The measures implemented that are perceived by adversaries as too		
Evaluation measure source	Garcia, 2001	
Value function source	SME-1	
Type of evaluation measure	Direct,	
Detection value function	x	v(x)
none	0	0
very low	0.2	10
low	0.4	10
medium	0.6	80
high	0.8	90
very high	1	100
Probability of determining that an unauthorized action has occurred or is		
Evaluation measure source	Garcia, 2001	
Value function source	SME-2	
Type of evaluation measure	Direct, Natural	
Delay value function	x	v(x)
No delay	0	0
One minute delay	1	10
Five minute delay	5	20
15 minute delay	15	60
30 minute delay	30	90
60 minutes delay	120	100
Time (minutes) that an element of a physical protection system		
Evaluation measure source	Garcia, 2001	
Value function source	SME-1	
Type of evaluation measure	Direct, Natural	

	Min	Most Likely	Max
x axis	1	3	5

Comment:

	Min	Most Likely	Max
x axis	0.2	0.8	1

Comment:

	Min	Most Likely	Max
x axis	1	10	60

Comment:

				SME1		
1.1.1.1	Source	River Source	Delay	5	30	60
1.1.2.1	Source	Well Source	Delay	1	5	15
1.2.1.1	Transmit	Trans Pump Station	Delay	1	10	15
1.2.2.1	Transmit	Pipeline	Delay	10	30	60
1.2.3.1	Transmit	Valves	Delay	5	15	40
1.3.1.1	Treat	Facilities	Delay	5	30	60
1.3.2.1	Treat	Processes	Delay	5	20	60
1.4.1.1	Store	Clearwell	Delay	5	20	60
1.4.2.1	Store	Tank	Delay	5	20	60
1.4.3.1	Store	Reservoir	Delay	5	10	15
1.5.1.1	Distribute	Distr Pump Station	Delay	1	10	20
1.5.2.1	Distribute	Del Piping System	Delay	5	50	60
1.5.3.1	Distribute	Svc Piping System	Delay	0	5	10
1.6.1.1	Control	SCADA	Delay	5	30	60
1.1.1.2	Source	River Source	Detection	0.4	0.75	1
1.1.2.2	Source	Well Source	Detection	0.2	0.6	1
1.2.1.2	Transmit	Trans Pump Station	Detection	0.4	0.8	1
1.2.2.2	Transmit	Pipeline	Detection	0.4	0.8	0.9
1.2.3.2	Transmit	Valves	Detection	0.5	0.75	0.8
1.3.1.2	Treat	Facilities	Detection	0.5	0.8	0.9
1.3.2.2	Treat	Processes	Detection	0.5	0.8	1
1.4.1.2	Store	Clearwell	Detection	0.5	0.8	1
1.4.2.2	Store	Tank	Detection	0.4	0.7	1
1.4.3.2	Store	Reservoir	Detection	0.1	0.4	0.75
1.5.1.2	Distribute	Distr Pump Station	Detection	0.4	0.8	1
1.5.2.2	Distribute	Del Piping System	Detection	0.4	0.8	1
1.5.3.2	Distribute	Svc Piping System	Detection	0	0.1	0.3
1.6.1.2	Control	SCADA	Detection	0.6	0.8	0.9
1.1.1.3	Source	River Source	Deterrence		3	
1.1.2.3	Source	Well Source	Deterrence		3	
1.2.1.3	Transmit	Trans Pump Station	Deterrence		3	
1.2.2.3	Transmit	Pipeline	Deterrence		0	
1.2.3.3	Transmit	Valves	Deterrence		3	
1.3.1.3	Treat	Facilities	Deterrence		4	
1.3.2.3	Treat	Processes	Deterrence		4	
1.4.1.3	Store	Clearwell	Deterrence		2	
1.4.2.3	Store	Tank	Deterrence		3	
1.4.3.3	Store	Reservoir	Deterrence		3	
1.5.1.3	Distribute	Distr Pump Station	Deterrence		3	
1.5.2.3	Distribute	Del Piping System	Deterrence		1	
1.5.3.3	Distribute	Svc Piping System	Deterrence		0	
1.6.1.3	Control	SCADA	Deterrence		4	
1.1.1.4	Source	River Source	Response	15	30	60
1.1.2.4	Source	Well Source	Response	15	30	60
1.2.1.4	Transmit	Trans Pump Station	Response	5	20	60
1.2.2.4	Transmit	Pipeline	Response	5	30	60
1.2.3.4	Transmit	Valves	Response	10	30	60
1.3.1.4	Treat	Facilities	Response	2	10	20
1.3.2.4	Treat	Processes	Response	2	10	20
1.4.1.4	Store	Clearwell	Response	2	10	20
1.4.2.4	Store	Tank	Response	10	20	45
1.4.3.4	Store	Reservoir	Response	10	20	60
1.5.1.4	Distribute	Distr Pump Station	Response	5	20	60
1.5.2.4	Distribute	Del Piping System	Response	5	30	60
1.5.3.4	Distribute	Svc Piping System	Response	20	45	90
1.6.1.4	Control	SCADA	Response	2	10	20

				wt	0.4	
				SME2		
1.1.1.1	Source	River Source	Delay	1	10	60
1.1.2.1	Source	Well Source	Delay	1	5	10
1.2.1.1	Transmit	Trans Pump Station	Delay	5	10	20
1.2.2.1	Transmit	Pipeline	Delay	5	15	30
1.2.3.1	Transmit	Valves	Delay	10	20	45
1.3.1.1	Treat	Facilities	Delay	5	10	15
1.3.2.1	Treat	Processes	Delay	5	10	15
1.4.1.1	Store	Clearwell	Delay	5	10	15
1.4.2.1	Store	Tank	Delay	5	25	45
1.4.3.1	Store	Reservoir	Delay	5	10	15
1.5.1.1	Distribute	Distr Pump Station	Delay	5	15	25
1.5.2.1	Distribute	Del Piping System	Delay	10	25	45
1.5.3.1	Distribute	Svc Piping System	Delay	1	10	15
1.6.1.1	Control	SCADA	Delay	10	20	45
1.1.1.2	Source	River Source	Detection	0.2	0.8	1
1.1.2.2	Source	Well Source	Detection	0.2	0.7	0.9
1.2.1.2	Transmit	Trans Pump Station	Detection	0.5	0.8	1
1.2.2.2	Transmit	Pipeline	Detection	0.1	0.4	0.7
1.2.3.2	Transmit	Valves	Detection	0.6	0.75	0.9
1.3.1.2	Treat	Facilities	Detection	0.5	0.8	1
1.3.2.2	Treat	Processes	Detection	0.5	0.7	1
1.4.1.2	Store	Clearwell	Detection	0.4	0.6	0.7
1.4.2.2	Store	Tank	Detection	0.4	0.8	0.9
1.4.3.2	Store	Reservoir	Detection	0.2	0.25	0.5
1.5.1.2	Distribute	Distr Pump Station	Detection	0.5	0.8	1
1.5.2.2	Distribute	Del Piping System	Detection	0.1	0.3	0.7
1.5.3.2	Distribute	Svc Piping System	Detection	0	0.1	0.3
1.6.1.2	Control	SCADA	Detection	0.7	0.75	0.8
1.1.1.3	Source	River Source	Deterrence		3	
1.1.2.3	Source	Well Source	Deterrence		3	
1.2.1.3	Transmit	Trans Pump Station	Deterrence		3	
1.2.2.3	Transmit	Pipeline	Deterrence		1	
1.2.3.3	Transmit	Valves	Deterrence		3	
1.3.1.3	Treat	Facilities	Deterrence		4	
1.3.2.3	Treat	Processes	Deterrence		4	
1.4.1.3	Store	Clearwell	Deterrence		3	
1.4.2.3	Store	Tank	Deterrence		3	
1.4.3.3	Store	Reservoir	Deterrence		3	
1.5.1.3	Distribute	Distr Pump Station	Deterrence		3	
1.5.2.3	Distribute	Del Piping System	Deterrence		1	
1.5.3.3	Distribute	Svc Piping System	Deterrence		0	
1.6.1.3	Control	SCADA	Deterrence		1	
1.1.1.4	Source	River Source	Response	15	30	60
1.1.2.4	Source	Well Source	Response	10	20	60
1.2.1.4	Transmit	Trans Pump Station	Response	10	30	45
1.2.2.4	Transmit	Pipeline	Response	15	40	60
1.2.3.4	Transmit	Valves	Response	10	30	60
1.3.1.4	Treat	Facilities	Response	5	15	25
1.3.2.4	Treat	Processes	Response	5	15	25
1.4.1.4	Store	Clearwell	Response	5	15	25
1.4.2.4	Store	Tank	Response	10	30	45
1.4.3.4	Store	Reservoir	Response	10	20	45
1.5.1.4	Distribute	Distr Pump Station	Response	15	25	40
1.5.2.4	Distribute	Del Piping System	Response	15	35	60
1.5.3.4	Distribute	Svc Piping System	Response	20	45	90
1.6.1.4	Control	SCADA	Response	5	10	20

Listed below is a summary of the assessments, assumptions, and forecast means for the aggregation of SME one and two.

Comp	SME1(.6)				SME2 (.4)				Combined
	Min	ML	Max	Distr	Min	ML	Max	Distr	
1.1.1.2	5.00	30.00	60.00	31.67	15.00	25.00	60.00	33.33	32.33
1.1.1.3	0.10	0.40	0.75	0.42	0.20	0.25	0.50	0.32	0.38
1.1.1.4	10.00	30.00	60.00	33.33	1.00	10.00	60.00	23.67	29.47
1.1.2.2	10.00	20.00	60.00	30.00	10.00	20.00	45.00	25.00	28.00
1.1.2.3	0.40	0.75	1.00	0.72	0.20	0.80	1.00	0.67	0.70
1.1.2.4	5.00	30.00	60.00	31.67	5.00	10.00	15.00	10.00	23.00
1.2.1.2	15.00	30.00	60.00	35.00	20.00	35.00	60.00	38.33	36.33
1.2.1.3	0.50	0.80	0.90	0.73	0.50	0.80	1.00	0.77	0.75
1.2.1.4	1.00	10.00	20.00	10.33	5.00	15.00	25.00	15.00	12.20
1.2.2.2	1.00	5.00	15.00	7.00	1.00	5.00	8.00	4.67	6.07
1.2.2.3	0.40	0.80	1.00	0.73	0.50	0.80	1.00	0.77	0.75
1.2.2.4	2.00	10.00	20.00	10.67	5.00	15.00	25.00	15.00	12.40
1.2.3.2	5.00	20.00	60.00	28.33	15.00	25.00	40.00	26.67	27.67
1.2.3.3	0.20	0.60	1.00	0.60	0.20	0.70	0.90	0.60	0.60
1.2.3.4	5.00	20.00	60.00	28.33	5.00	10.00	15.00	10.00	21.00
1.3.1.2	15.00	30.00	60.00	35.00	10.00	20.00	60.00	30.00	33.00
1.3.1.3	0.50	0.80	1.00	0.77	0.50	0.70	1.00	0.73	0.75
1.3.1.4	5.00	50.00	60.00	38.33	10.00	25.00	45.00	26.67	33.67
1.3.2.2	1.00	10.00	15.00	8.67	5.00	15.00	20.00	13.33	10.53
1.3.2.3	0.40	0.80	1.00	0.73	0.10	0.30	0.70	0.37	0.59
1.3.2.4	2.00	10.00	20.00	10.67	5.00	10.00	25.00	13.33	11.73
1.4.1.2	5.00	30.00	60.00	31.67	15.00	35.00	60.00	36.67	33.67
1.4.1.3	0.40	0.70	0.90	0.67	0.50	0.80	1.00	0.77	0.71
1.4.1.4	5.00	20.00	60.00	28.33	5.00	10.00	30.00	15.00	23.00
1.4.2.2	5.00	20.00	60.00	28.33	10.00	30.00	45.00	28.33	28.33
1.4.2.3	0.50	0.80	1.00	0.77	0.40	0.60	0.70	0.57	0.69
1.4.2.4	0.00	5.00	10.00	5.00	1.00	10.00	15.00	8.67	6.47
1.4.3.2	10.00	30.00	60.00	33.33	5.00	20.00	30.00	18.33	27.33
1.4.3.3	0.00	0.10	0.30	0.13	0.00	0.10	0.30	0.13	0.13
1.4.3.4	2.00	10.00	20.00	10.67	5.00	15.00	25.00	15.00	12.40
1.5.1.2	20.00	45.00	90.00	51.67	20.00	55.00	90.00	55.00	53.00
1.5.1.3	0.40	0.80	0.90	0.70	0.10	0.40	0.70	0.40	0.58
1.5.1.4	5.00	20.00	60.00	28.33	5.00	25.00	45.00	25.00	27.00
1.5.2.2	5.00	30.00	60.00	31.67	15.00	40.00	60.00	38.33	34.33
1.5.2.3	0.50	0.70	0.95	0.72	0.40	0.80	0.90	0.70	0.71
1.5.2.4	5.00	30.00	60.00	31.67	10.00	20.00	45.00	25.00	29.00
1.5.3.2	5.00	15.00	40.00	20.00	10.00	20.00	45.00	25.00	22.00
1.5.3.3	0.60	0.80	0.90	0.77	0.70	0.75	0.80	0.75	0.76
1.5.3.4	10.00	20.00	45.00	25.00	10.00	30.00	45.00	28.33	26.33
1.6.1.2	2.00	10.00	20.00	10.67	5.00	20.00	25.00	16.67	13.07
1.6.1.3	0.50	0.75	0.80	0.68	0.60	0.75	0.90	0.75	0.71
1.6.1.4	5.00	10.00	15.00	10.00	10.00	15.00	20.00	15.00	12.00

APPENDIX F SME-3 Weighting Factors (SME-1 and -2)

This interview is part of my research to fulfill requirements for a PhD in Engineering Management from the Department of Engineering Management and Systems Engineering, Old Dominion University.

Do you agree to participate? Sign and date: _____

1. Describe your experience?
2. How many years of experience do you have in water systems?
3. What duties do you perform?
4. Based on the expert criteria presented in each SME's resume, rate their expertise on a scale of one to ten as it applies to clean water systems.

Expert Criteria:

<u>Criteria</u>	<u>SME-1 (wt: 1-10)</u>	<u>SME-2 (1-10)</u>
Years of Experience		
Educational Background		
Ability to discern usefulness of data		
Appropriate expertise for discipline specific tasks		
<u>Overall</u>		

APPENDIX G Face Validity of The Model

Based on the model as you understand it, does it seem useful?

From your understanding of what the model is doing, would the results be believable by your peers in the water system business?

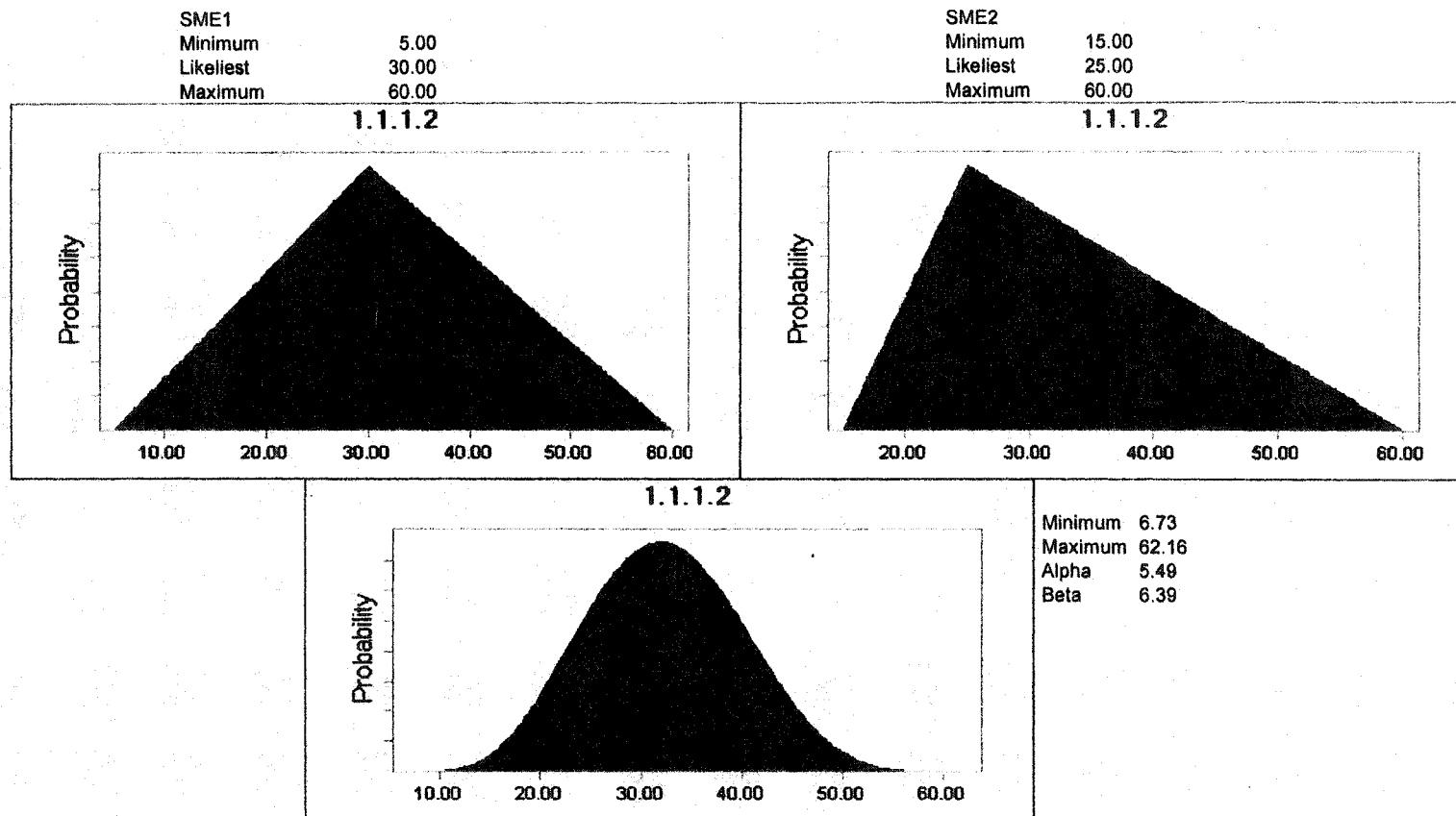
What are your criticisms of the model?

Where could this modeling approach be used in other places, such as Sewage Systems?

Do you think this model would be useful in other sectors such as electric systems, SCADA, DCS?

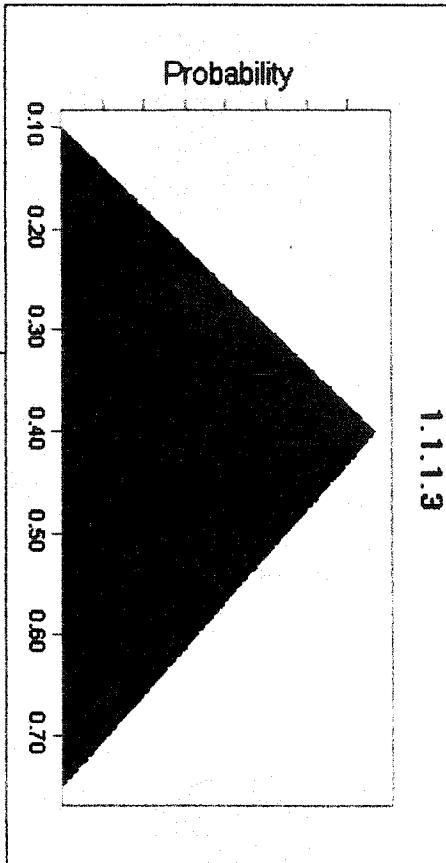
APPENDIX H Aggregation Assessments SME-1 and -2

The appendix shows the distributions for each measure scored by the experts and the resulting distribution from the inner loop aggregation simulation.



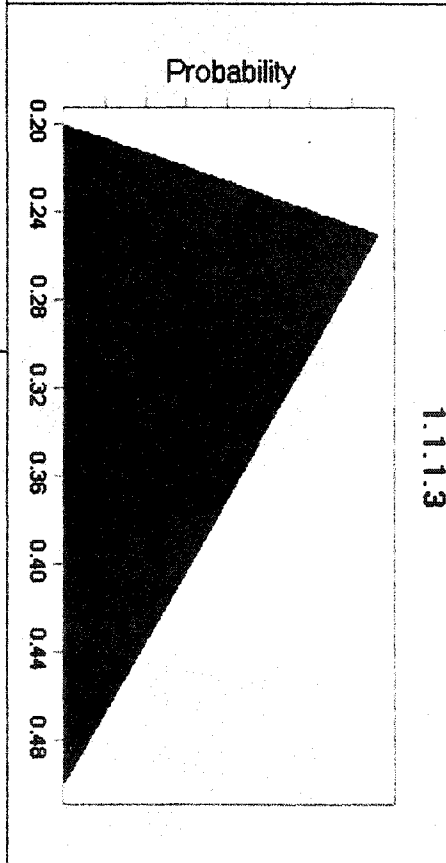
SME1
Minimum 0.10
Likeliest 0.40
Maximum 0.75

1.1.1.3

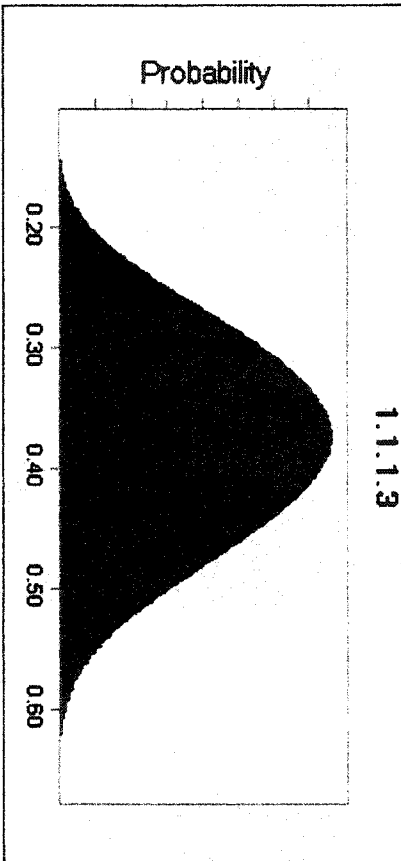


SME2
Minimum 0.20
Likeliest 0.25
Maximum 0.50

1.1.1.3

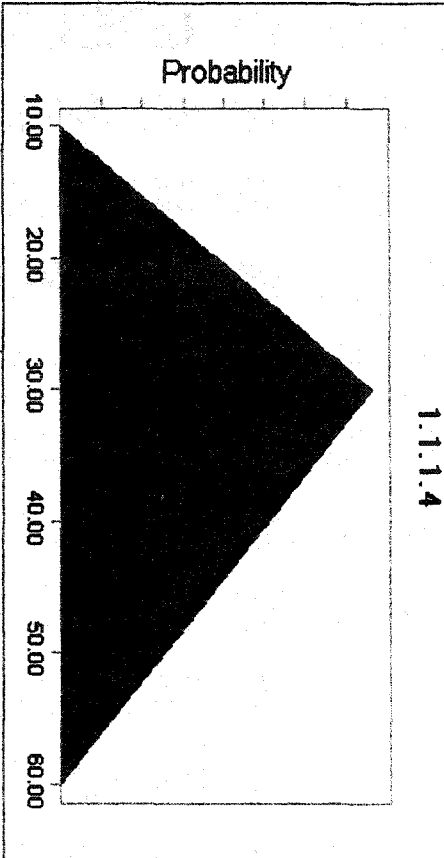


Minimum 0.12
Maximum 0.66
Alpha 4.66
Beta 5.12

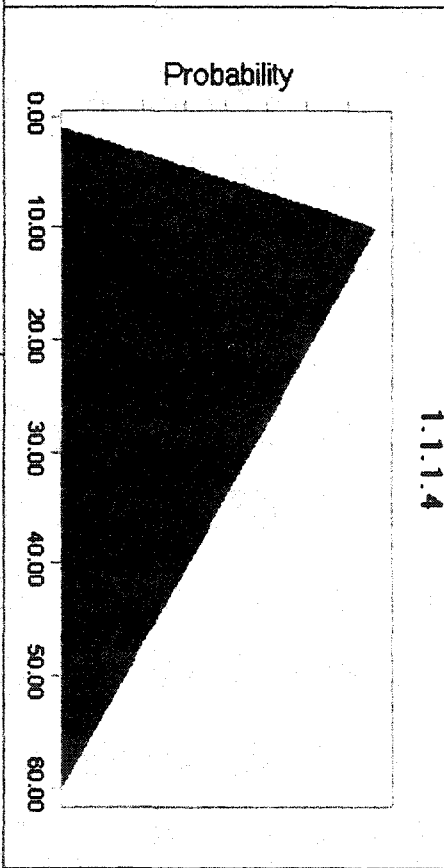


1.1.1.3

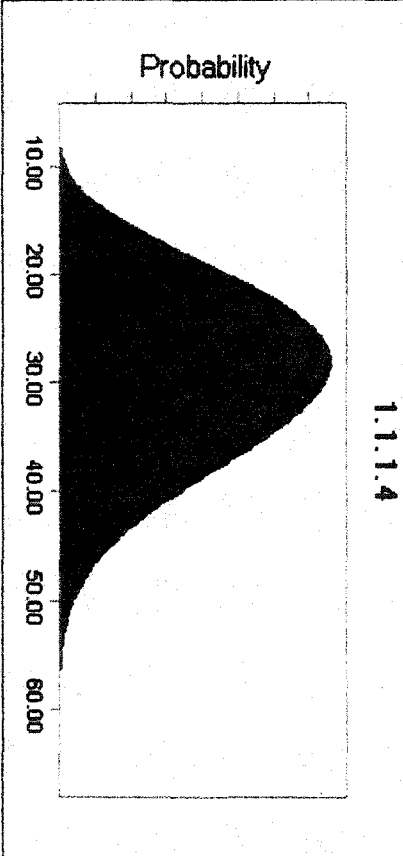
SME1
Minimum 10.00
Likeliest 30.00
Maximum 60.00



SME2
Minimum 1.00
Likeliest 10.00
Maximum 60.00

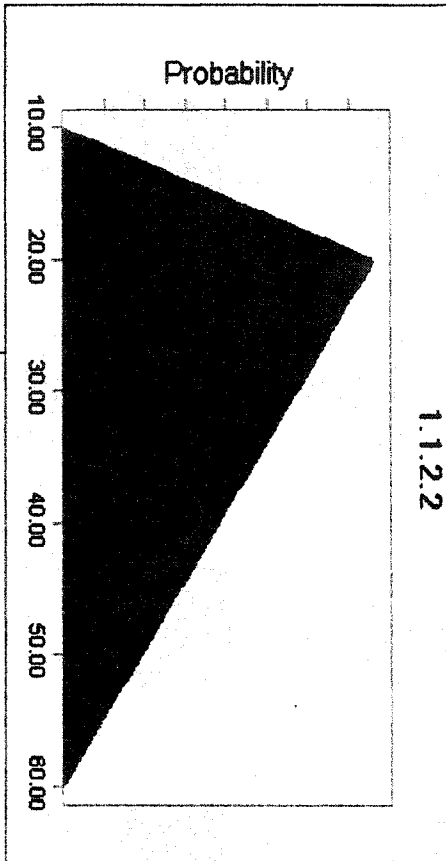


Minimum 5.72
Maximum 66.40
Alpha 4.84
Beta 7.56



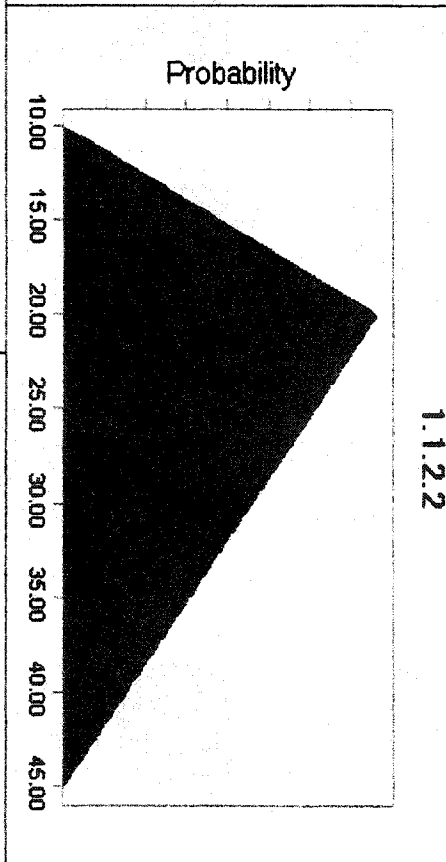
SME1
Minimum 10.00
Likeliest 20.00
Maximum 60.00

1.1.2.2



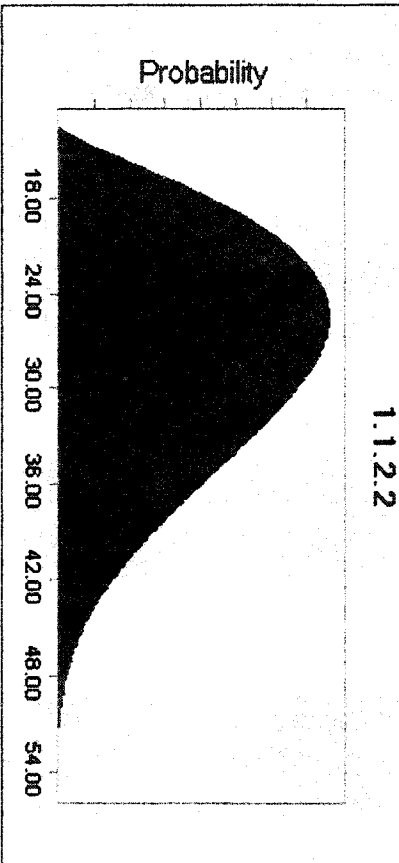
SME2
Minimum 10.00
Likeliest 20.00
Maximum 45.00

1.1.2.2



Minimum 13.42
Maximum 54.79
Alpha 2.39
Beta 4.39

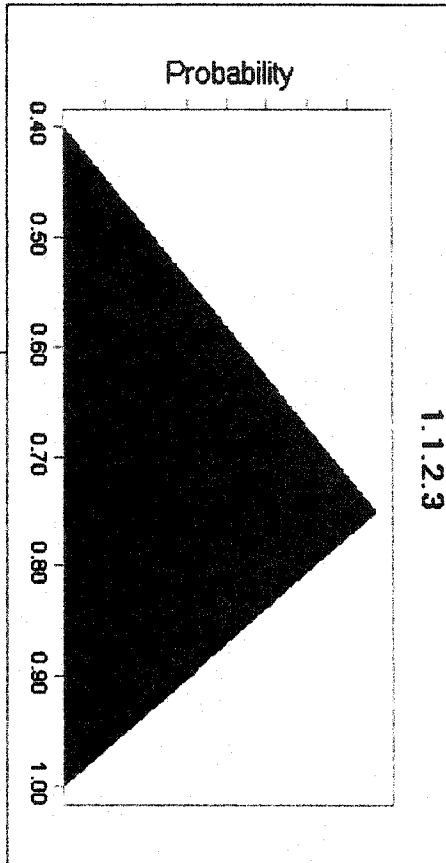
1.1.2.2



SME1
Minimum
Likeliest
Maximum

0.40
0.75
1.00

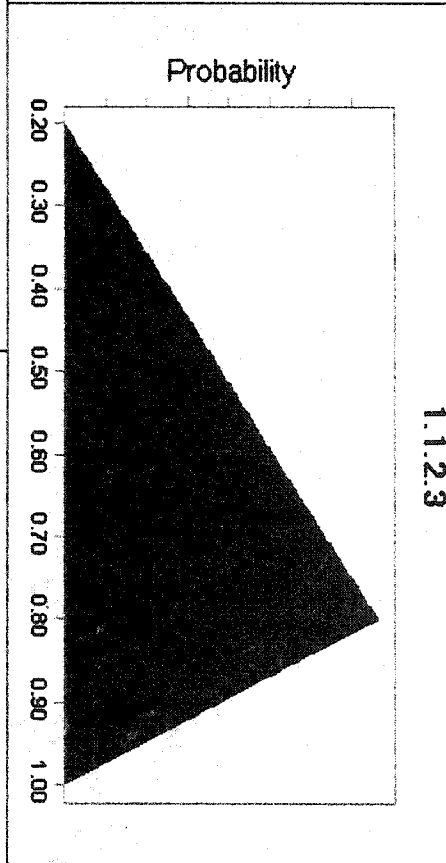
1.1.2.3



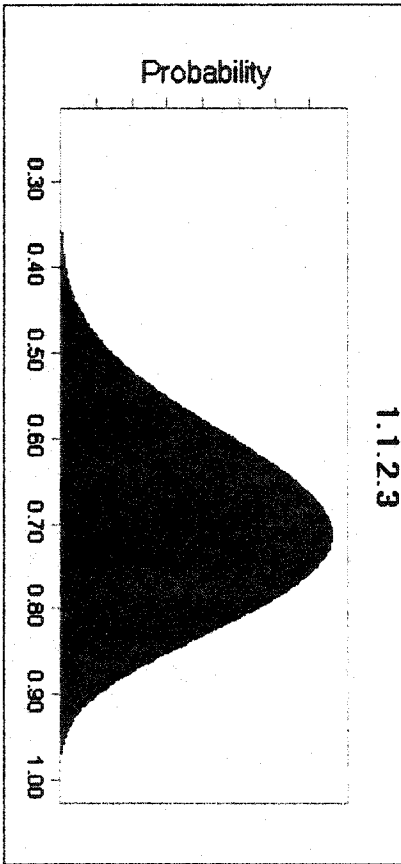
SME2
Minimum
Likeliest
Maximum

0.20
0.80
1.00

1.1.2.3

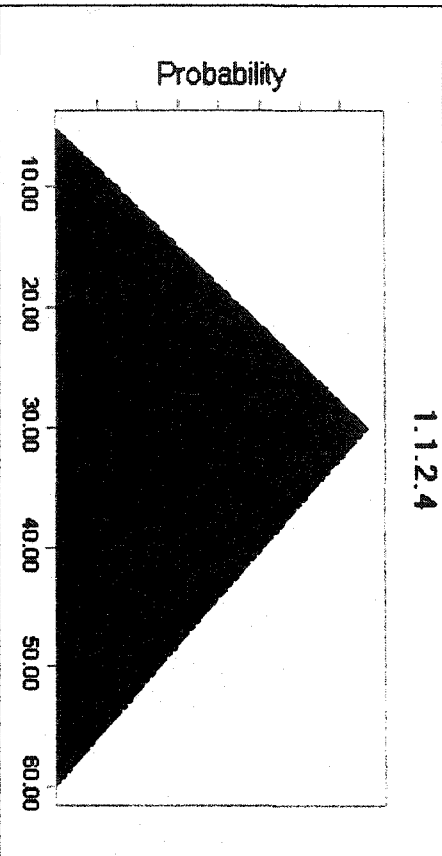


1.1.2.3

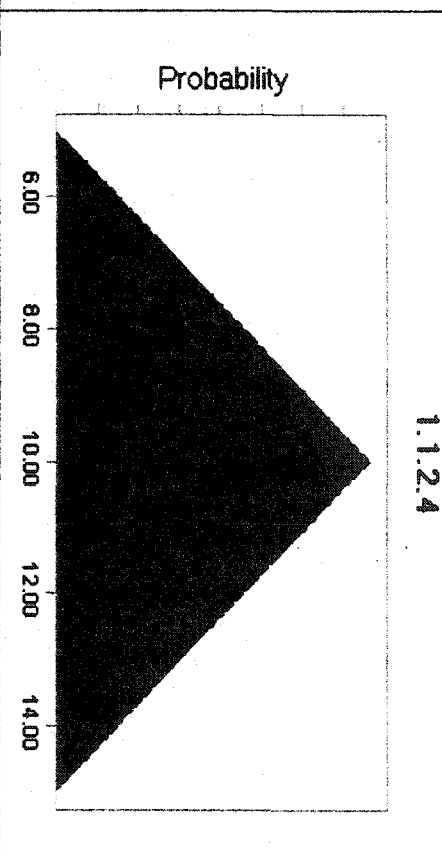


Minimum 0.23
Maximum 1.00
Alpha 7.60
Beta 5.03

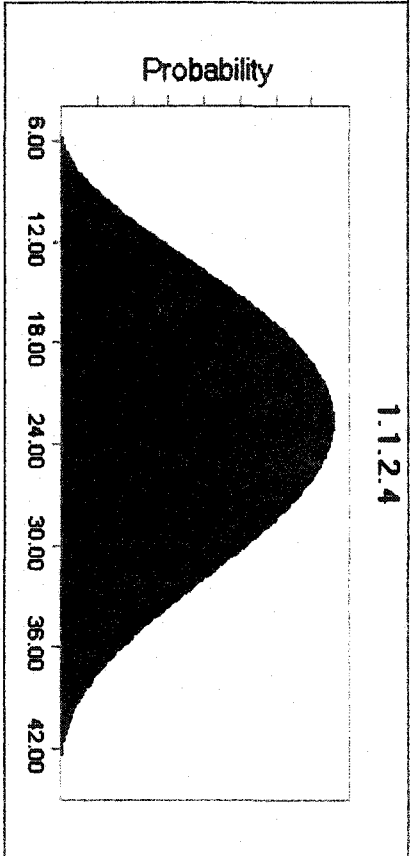
SME1
Minimum 5.00
Likeliest 30.00
Maximum 60.00



SME2
Minimum 5.00
Likeliest 10.00
Maximum 15.00

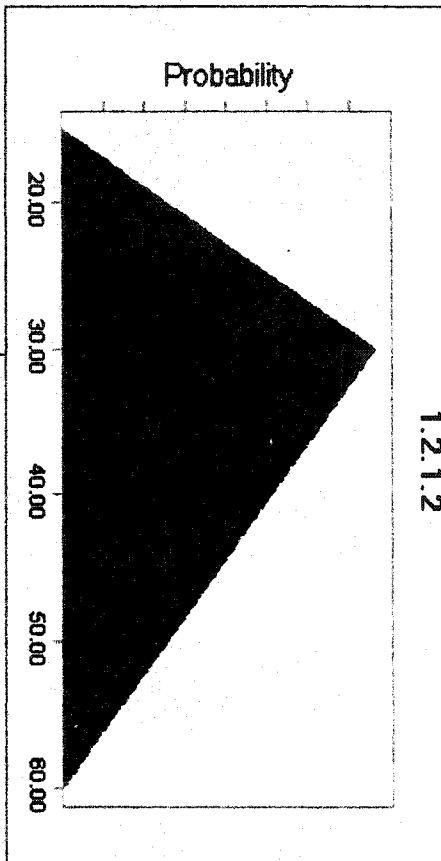


Minimum 4.90
Maximum 43.96
Alpha 3.30
Beta 3.80



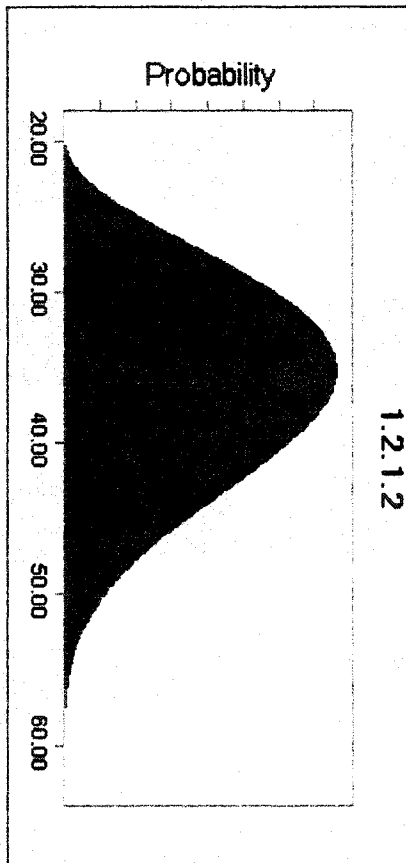
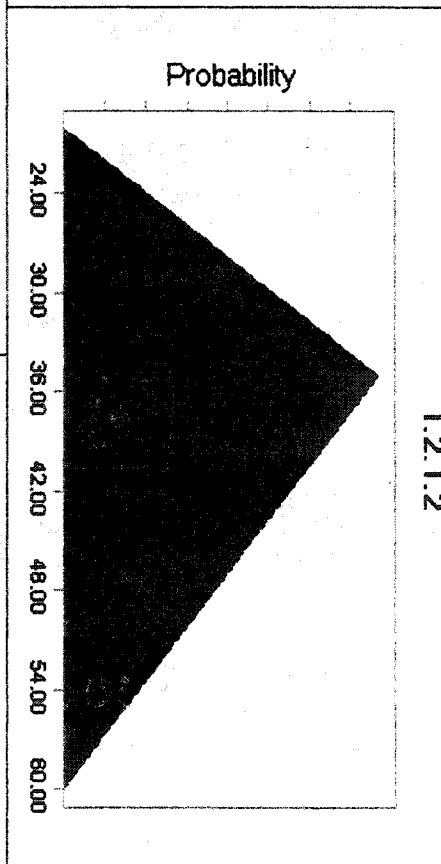
SME1
Minimum 15.00
Likeliest 30.00
Maximum 60.00

1.2.1.2



SME2
Minimum 20.00
Likeliest 35.00
Maximum 60.00

1.2.1.2

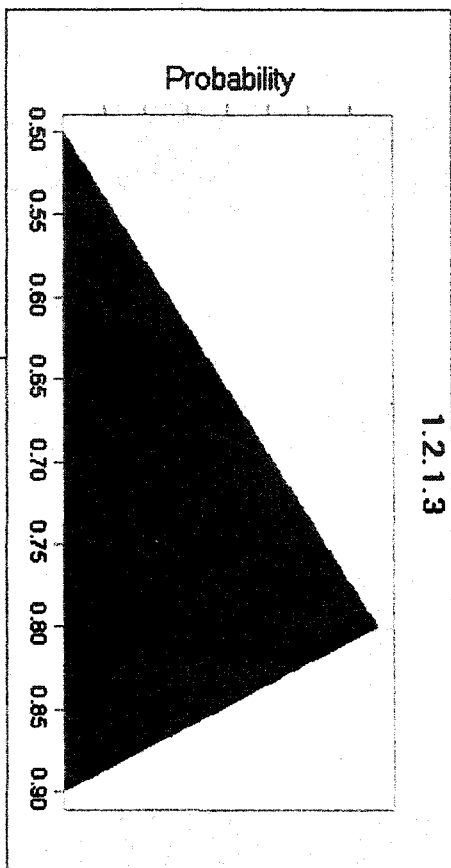


Minimum 19.00
Maximum 62.71
Alpha 3.81
Beta 5.84

1.2.1.2

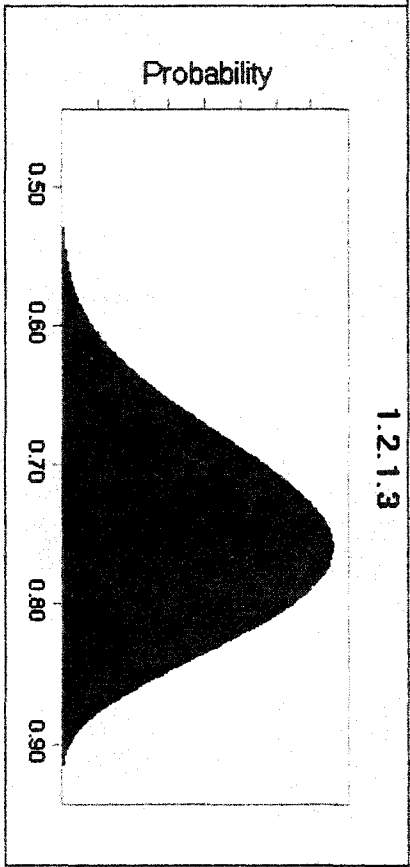
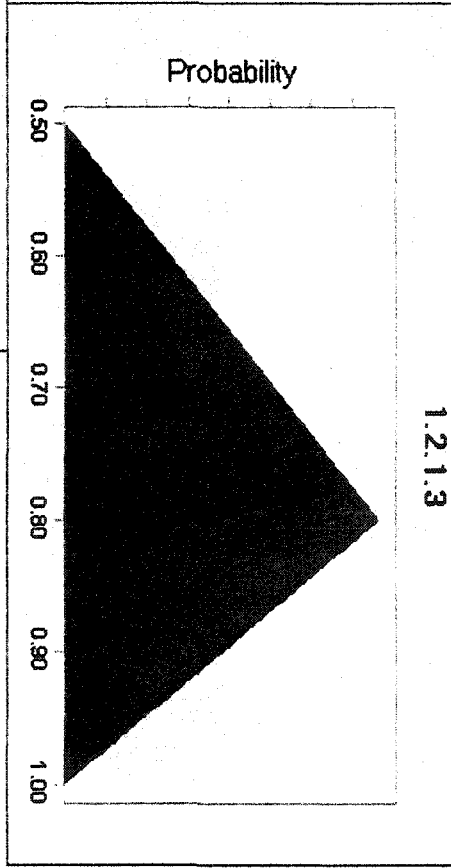
SME1
Minimum 0.50
Likeliest 0.80
Maximum 0.90

1.2.1.3



SME2
Minimum 0.50
Likeliest 0.80
Maximum 1.00

1.2.1.3

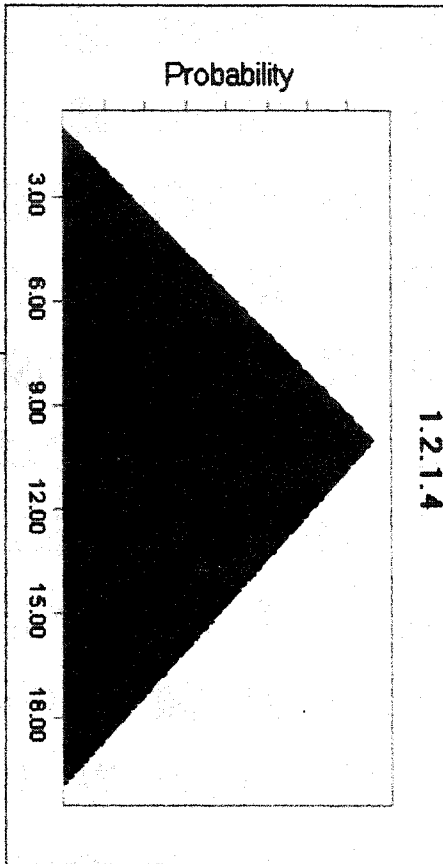


1.2.1.3

Minimum 0.46
Maximum 0.93
Alpha 6.88
Beta 4.33

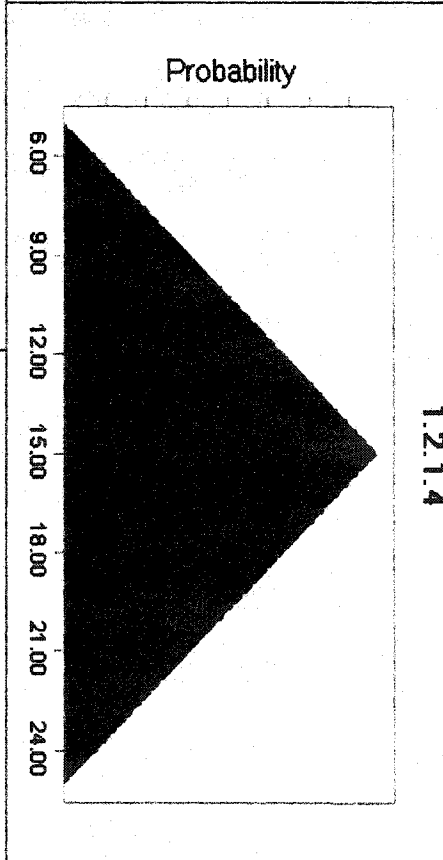
SME1
Minimum 1.00
Likeliest 10.00
Maximum 20.00

1.2.1.4

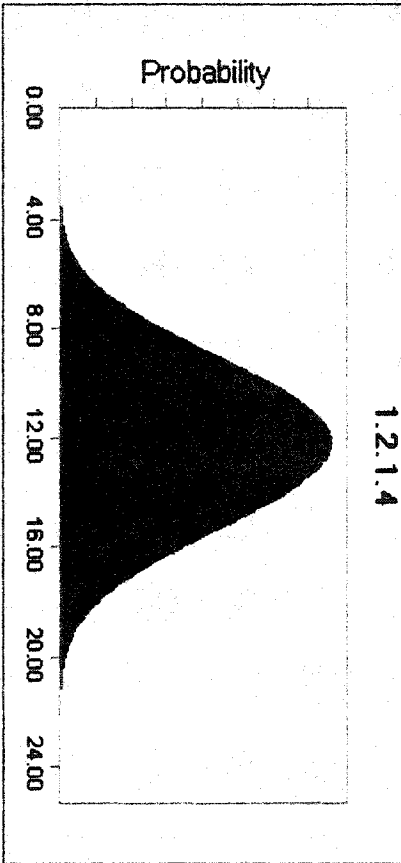


SME2
Minimum 5.00
Likeliest 15.00
Maximum 25.00

1.2.1.4

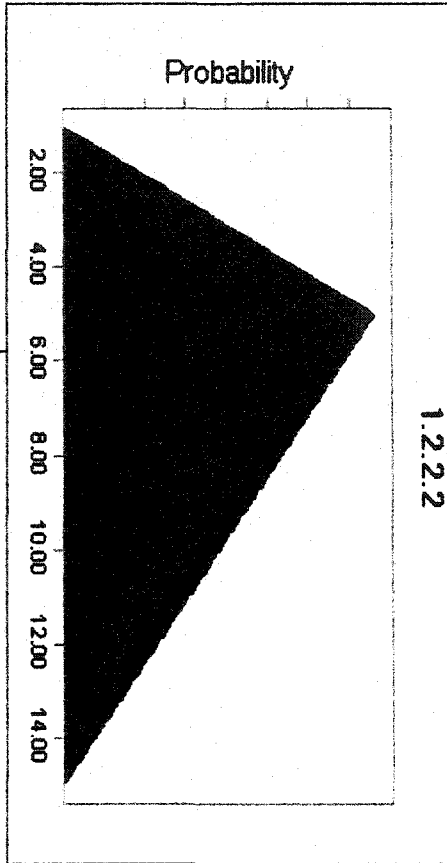


Minimum 0.50
Maximum 24.65
Alpha 8.27
Beta 8.80



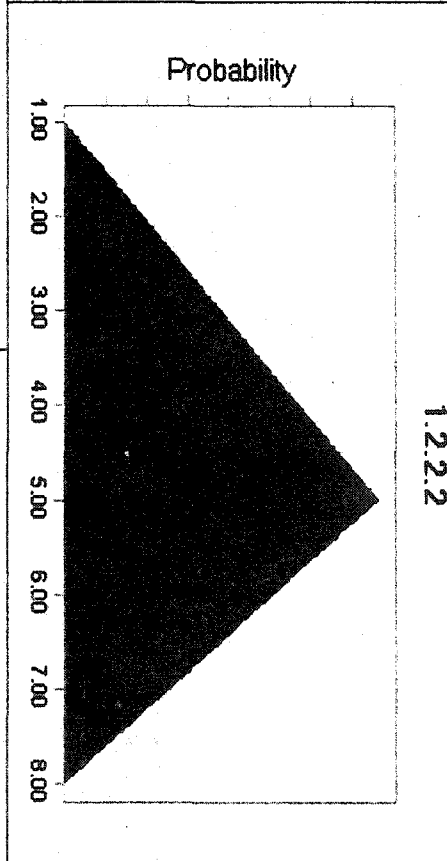
SME1
Minimum 1.00
Likeliest 5.00
Maximum 15.00

1.2.2.2

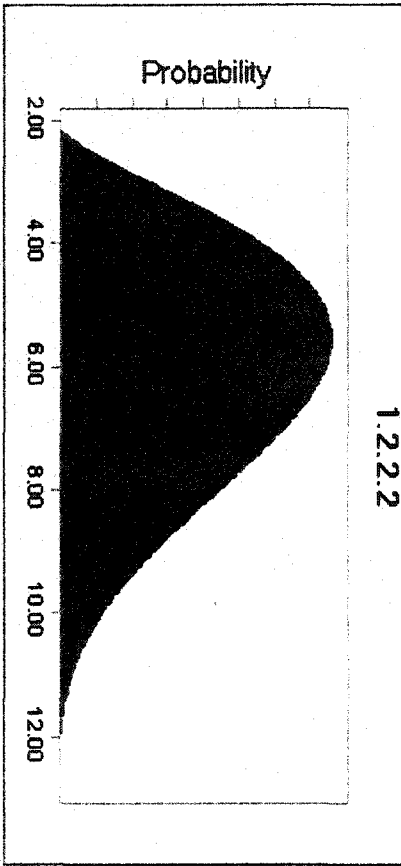


SME2
Minimum 1.00
Likeliest 5.00
Maximum 8.00

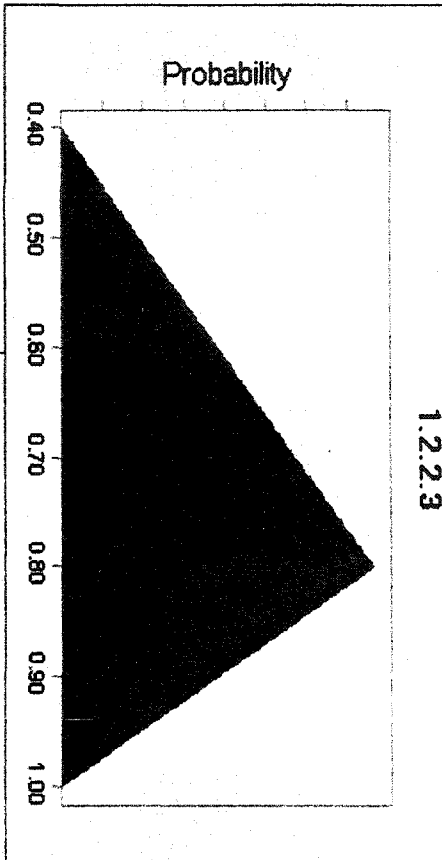
1.2.2.2



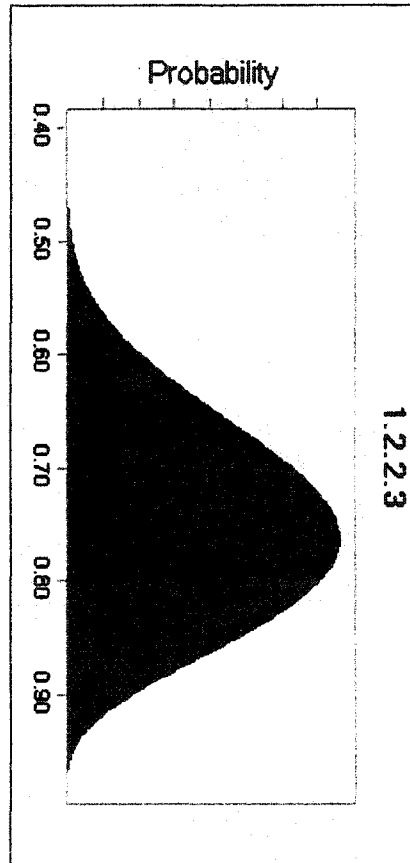
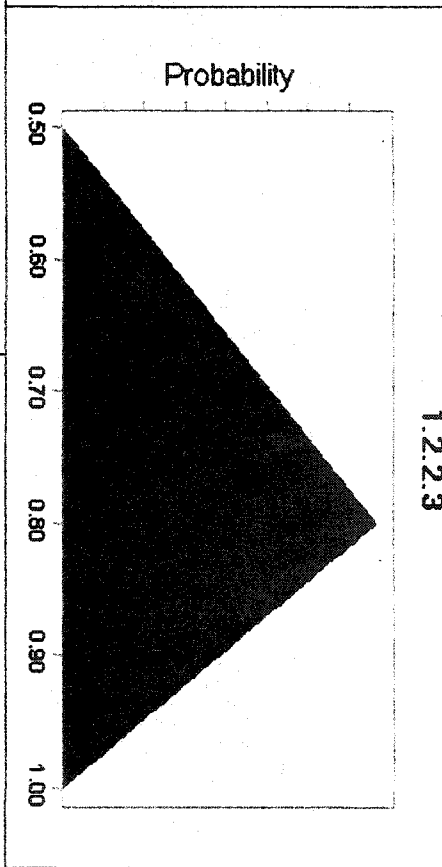
Minimum 2.06
Maximum 12.77
Alpha 2.58
Beta 4.31



SME1
Minimum 0.40
Likeliest 0.80
Maximum 1.00



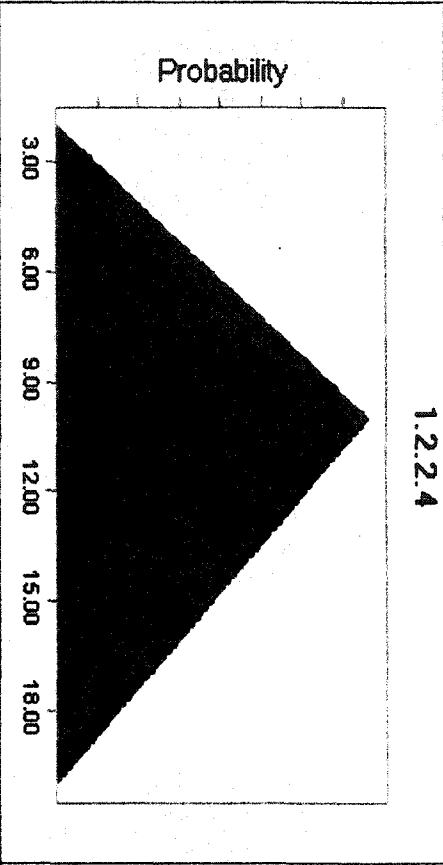
SME2
Minimum 0.50
Likeliest 0.80
Maximum 1.00



Minimum 0.40
Maximum 0.98
Alpha 6.07
Beta 4.03

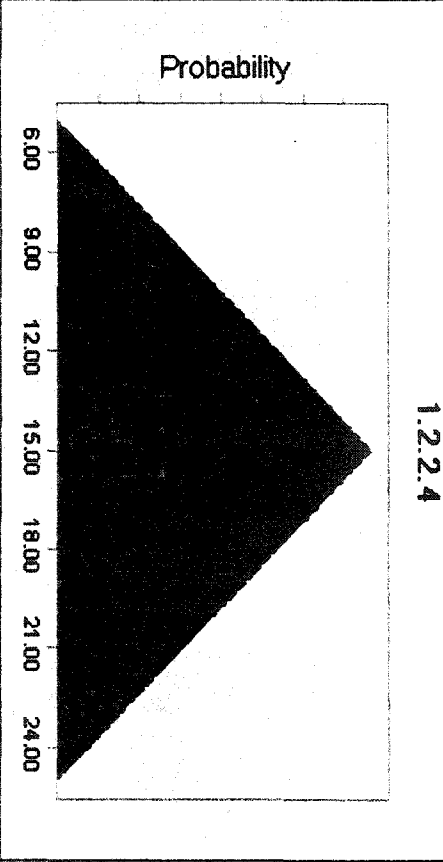
SME1
Minimum 2.00
Likeliest 10.00
Maximum 20.00

1.2.2.4



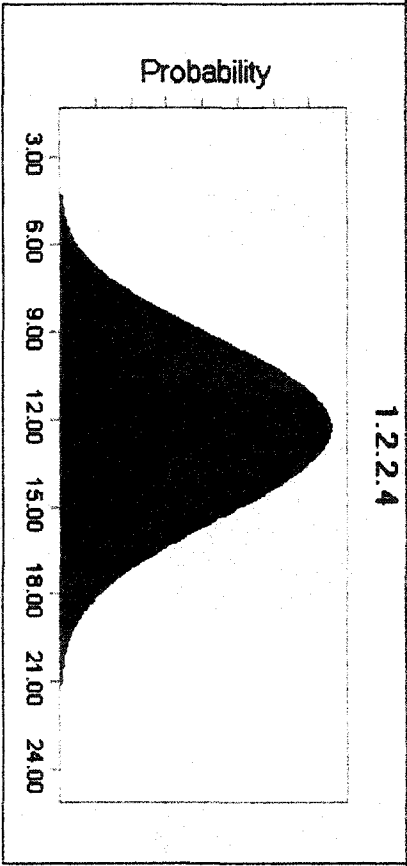
SME2
Minimum 5.00
Likeliest 15.00
Maximum 25.00

1.2.2.4

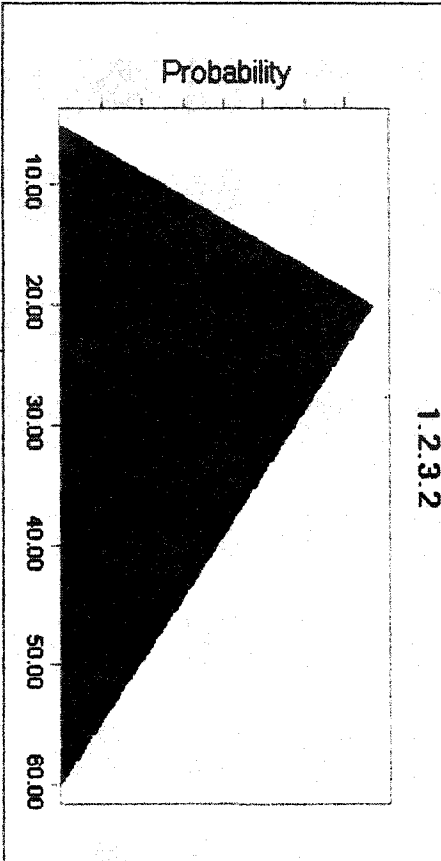


Minimum 1.88
Maximum 24.47
Alpha 7.32
Beta 8.42

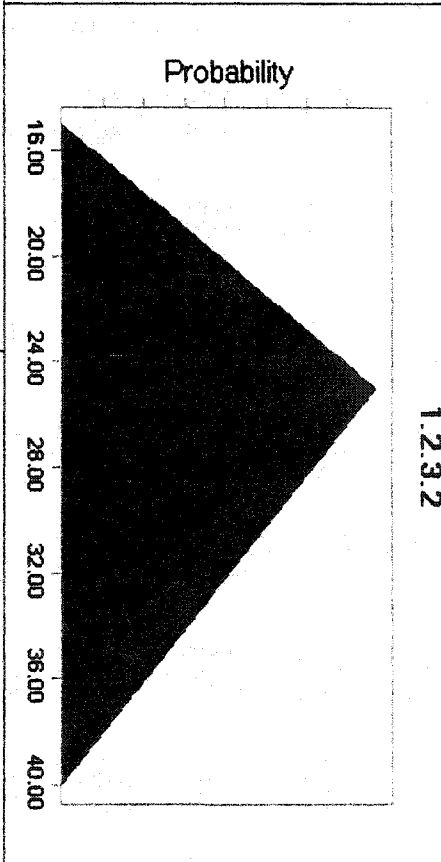
1.2.2.4



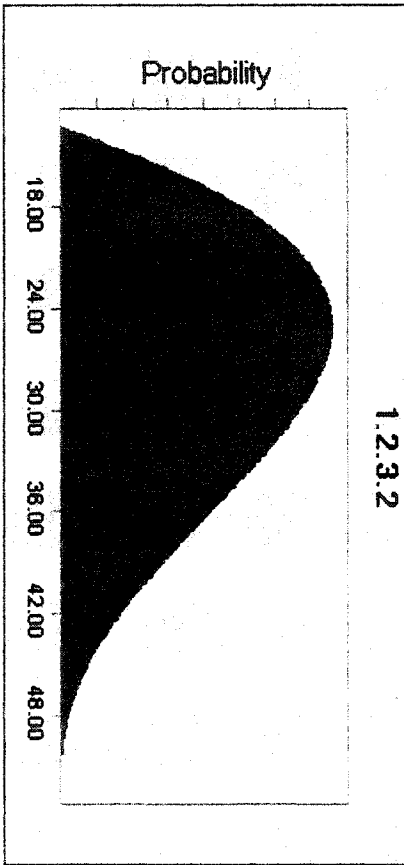
SME1
Minimum 5.00
Likeliest 20.00
Maximum 60.00



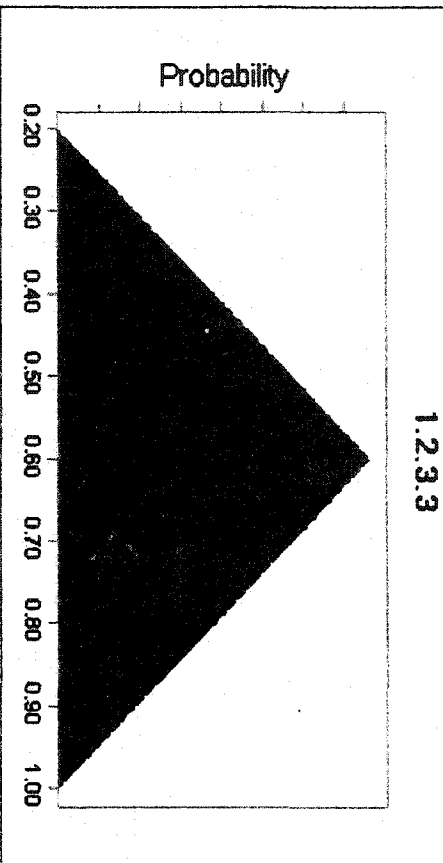
SME2
Minimum 15.00
Likeliest 25.00
Maximum 40.00



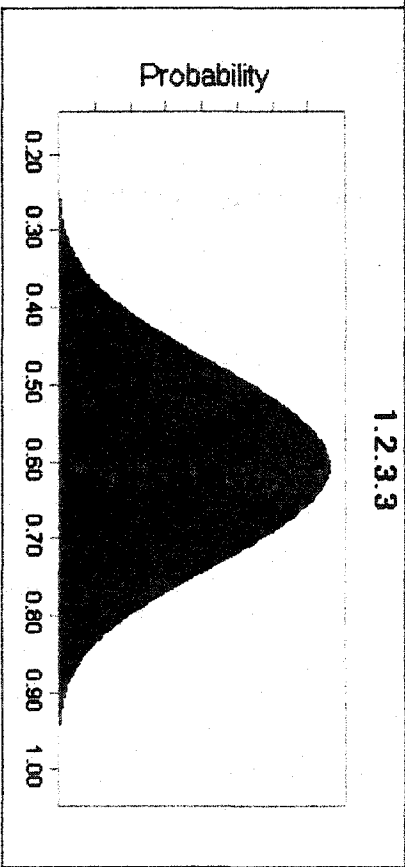
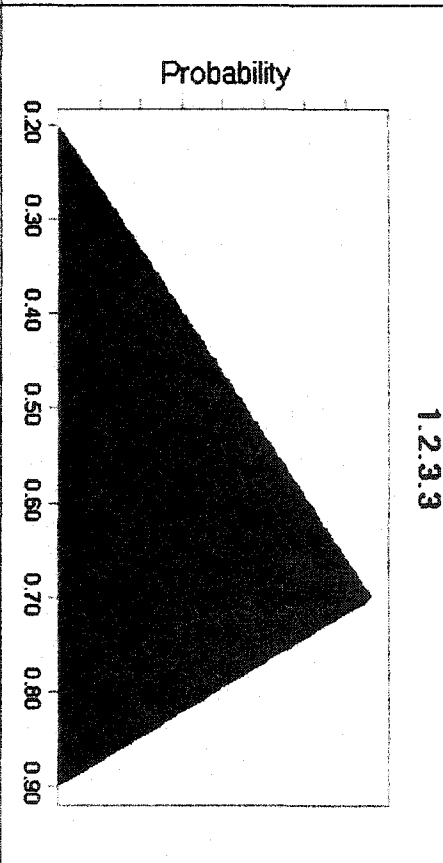
Minimum 13.12
Maximum 52.13
Alpha 2.10
Beta 3.53



SME1
Minimum 0.20
Likeliest 0.60
Maximum 1.00



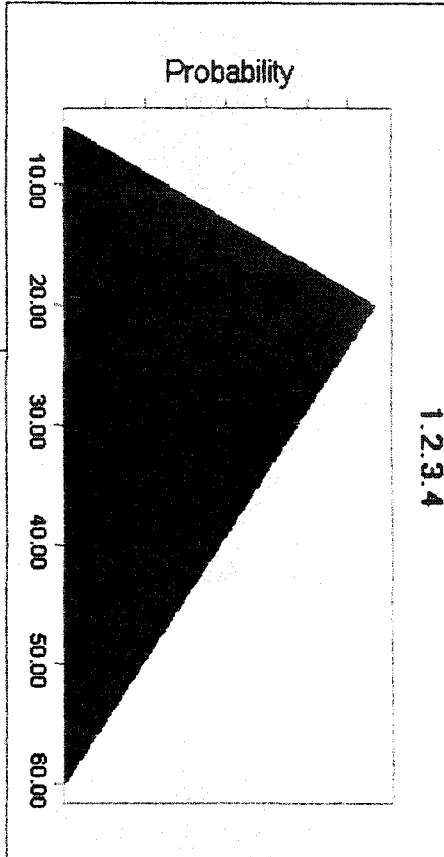
SME2
Minimum 0.20
Likeliest 0.70
Maximum 0.90



Minimum 0.17
Maximum 1.02
Alpha 6.73
Beta 6.48

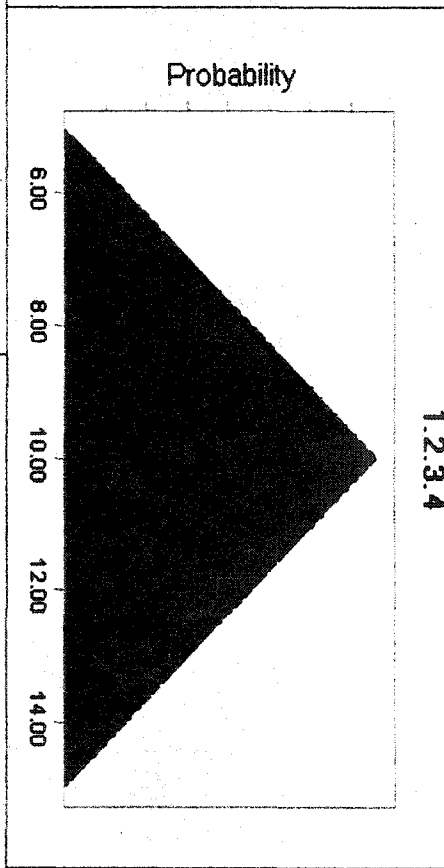
SME1
Minimum 5.00
Likeliest 20.00
Maximum 60.00

1.2.3.4



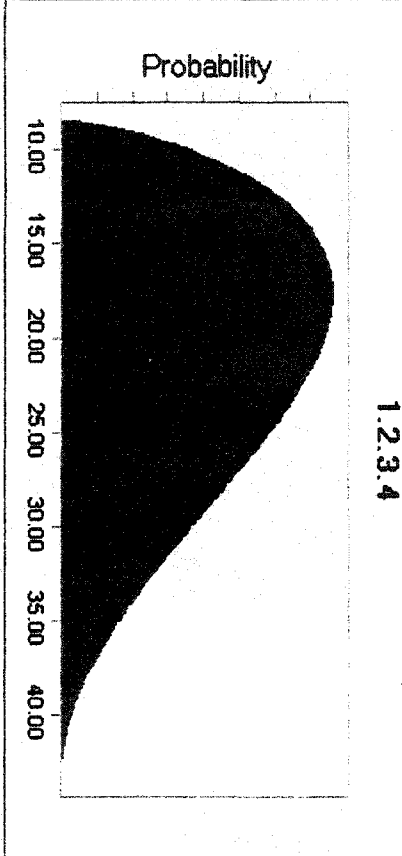
SME2
Minimum 5.00
Likeliest 10.00
Maximum 15.00

1.2.3.4



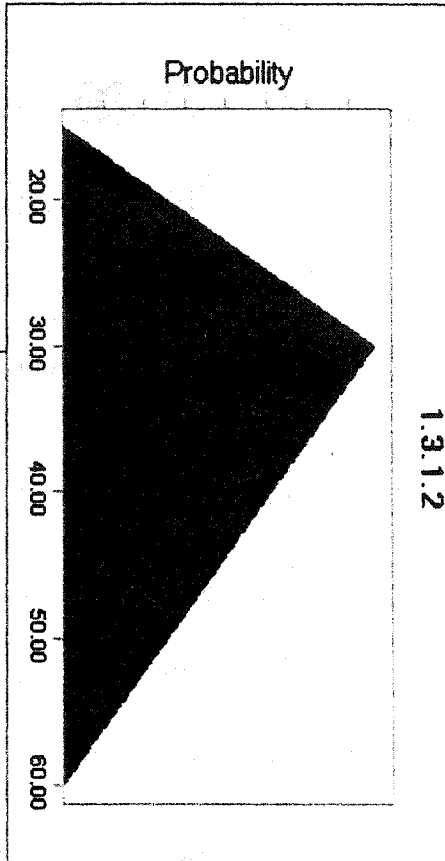
Minimum 8.35
Maximum 43.33
Alpha 1.74
Beta 3.06

1.2.3.4



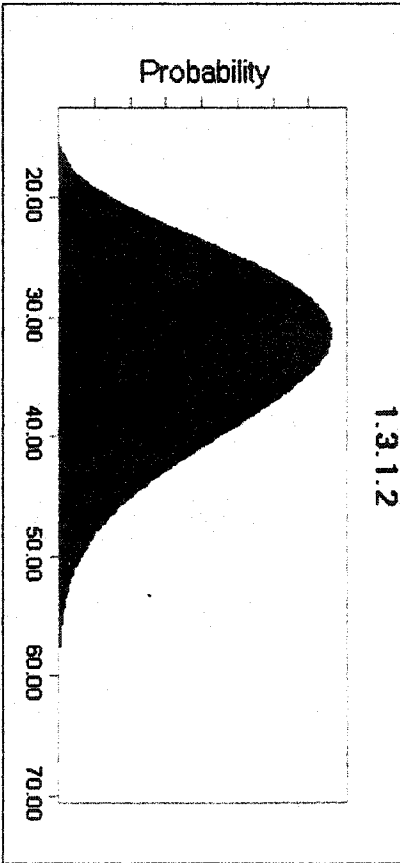
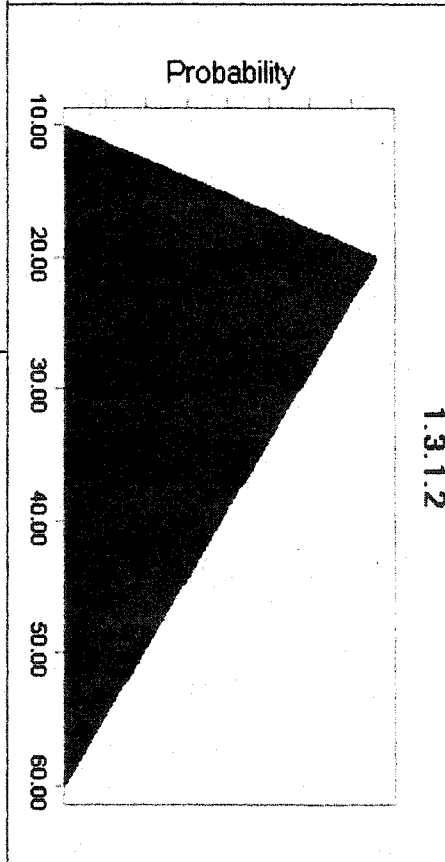
SME1
Minimum 15.00
Likeliest 30.00
Maximum 60.00

1.3.1.2



SME2
Minimum 10.00
Likeliest 20.00
Maximum 60.00

1.3.1.2

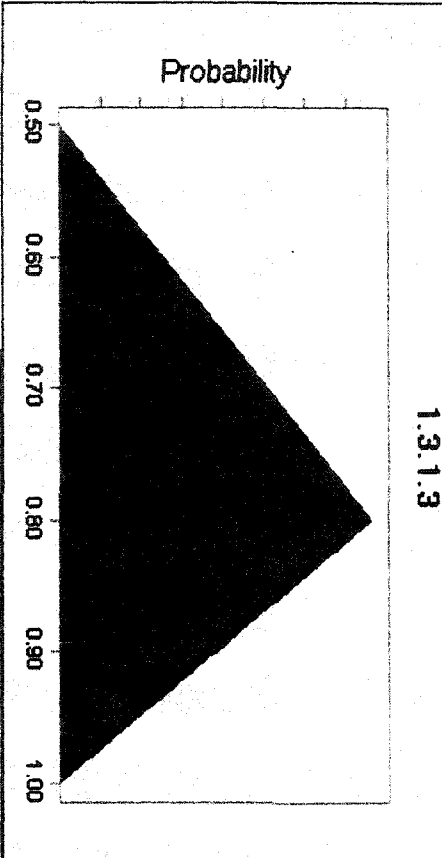


Minimum 13.78
Maximum 69.02
Alpha 4.40
Beta 8.27

1.3.1.2

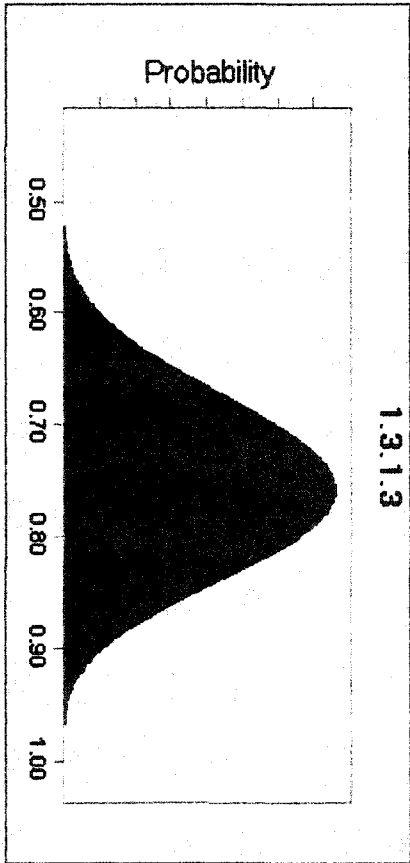
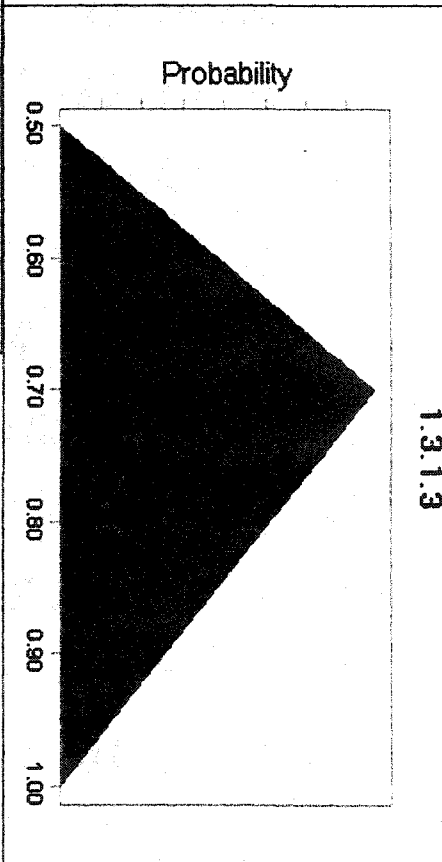
SME1
Minimum 0.50
Likeliest 0.80
Maximum 1.00

1.3.1.3



SME2
Minimum 0.50
Likeliest 0.70
Maximum 1.00

1.3.1.3

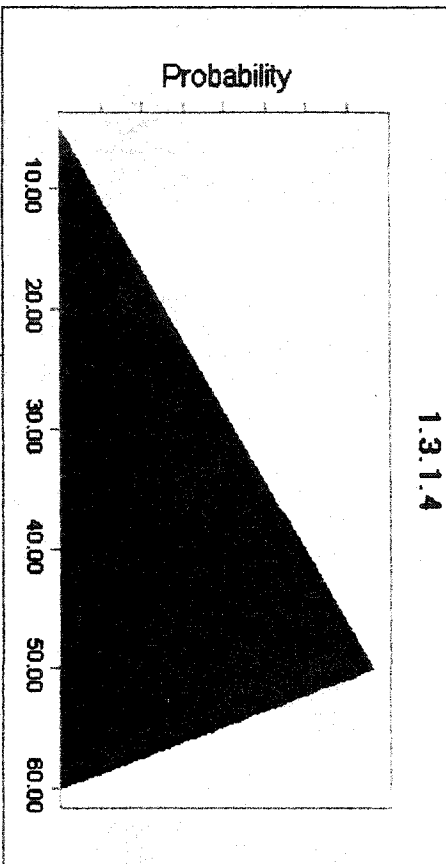


Minimum 0.43
Maximum 1.02
Alpha 8.11
Beta 6.74

1.3.1.3

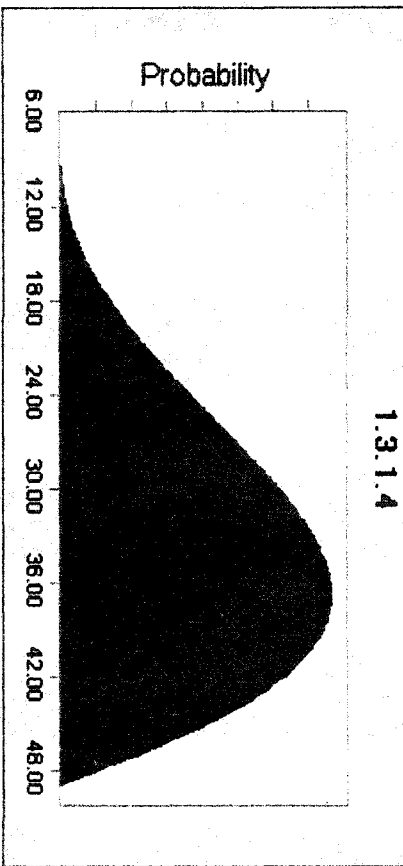
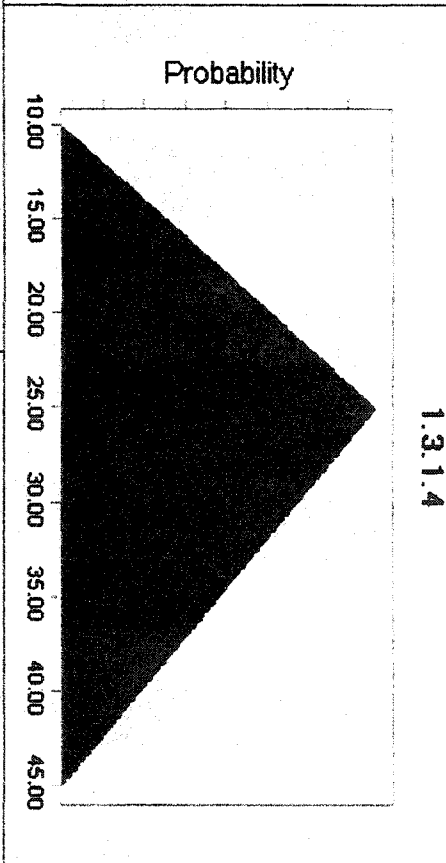
SME1
 Minimum 5.00
 Likeliest 50.00
 Maximum 60.00

1.3.1.4



SME2
 Minimum 10.00
 Likeliest 25.00
 Maximum 45.00

1.3.1.4

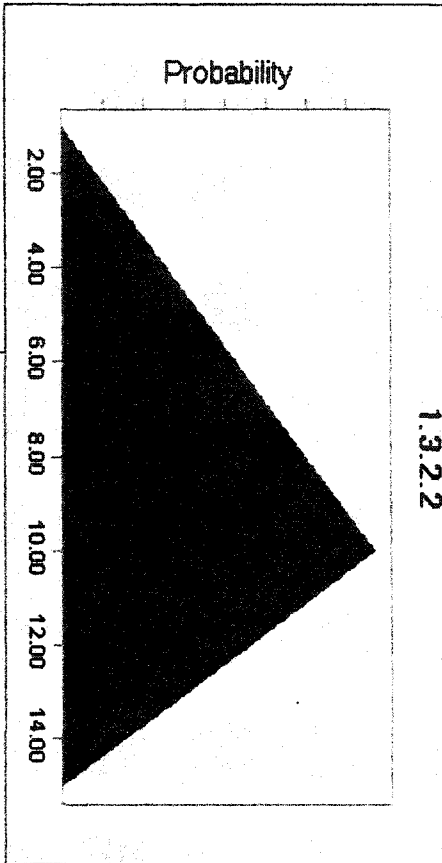


Minimum 6.90
 Maximum 48.99
 Alpha 3.77
 Beta 2.15

1.3.1.4

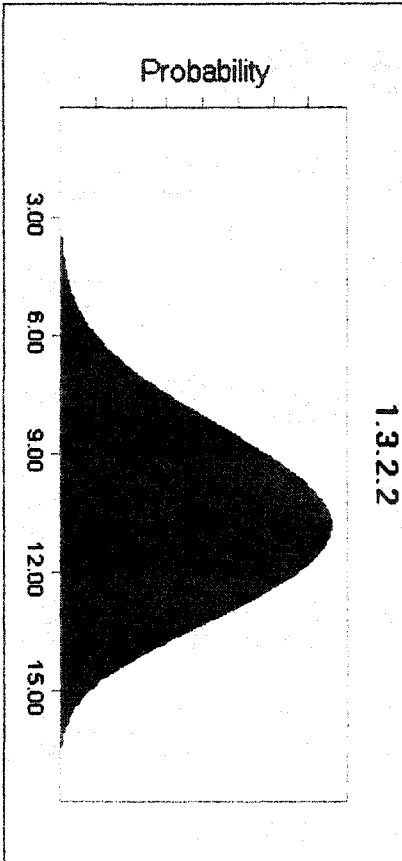
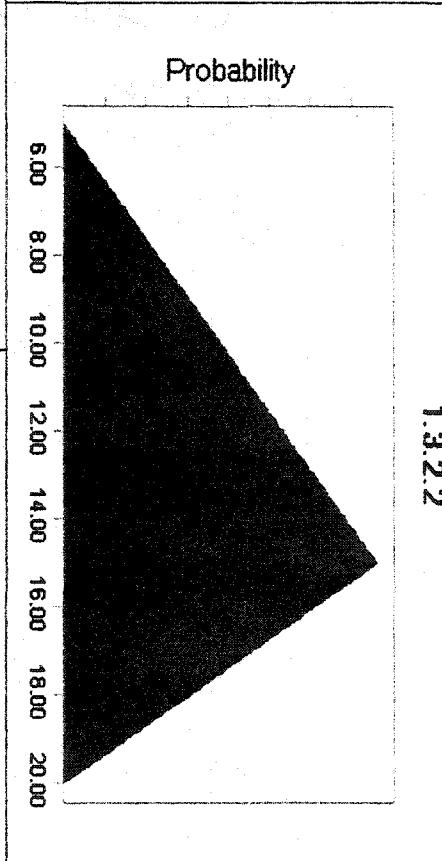
SME1
Minimum 1.00
Likeliest 10.00
Maximum 15.00

1.3.2.2



SME2
Minimum 5.00
Likeliest 15.00
Maximum 20.00

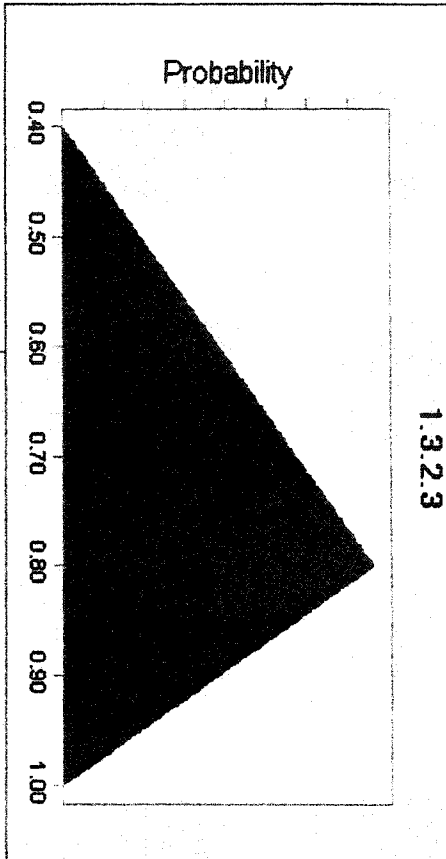
1.3.2.2



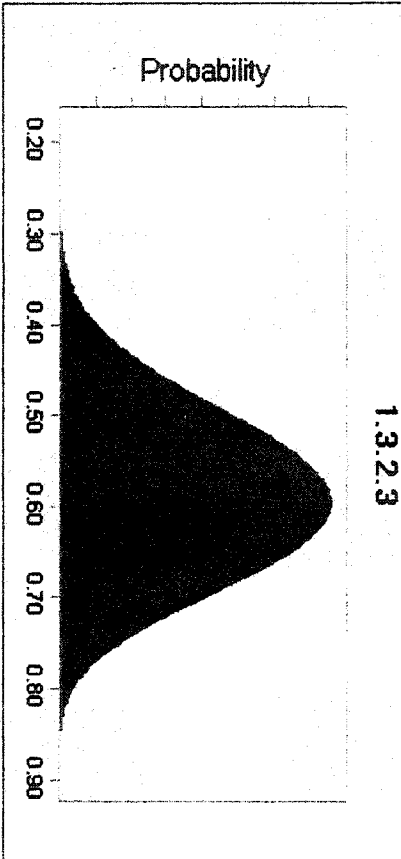
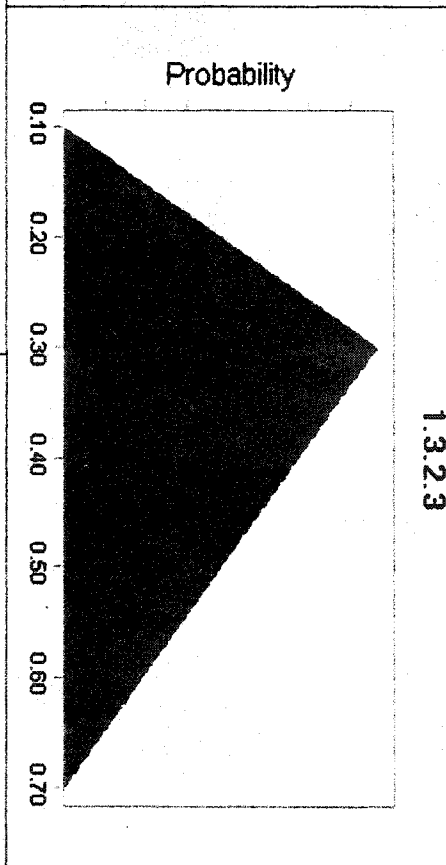
Minimum 0.61
Maximum 17.30
Alpha 8.10
Beta 5.55

1.3.2.2

SME1
Minimum 0.40
Likeliest 0.80
Maximum 1.00



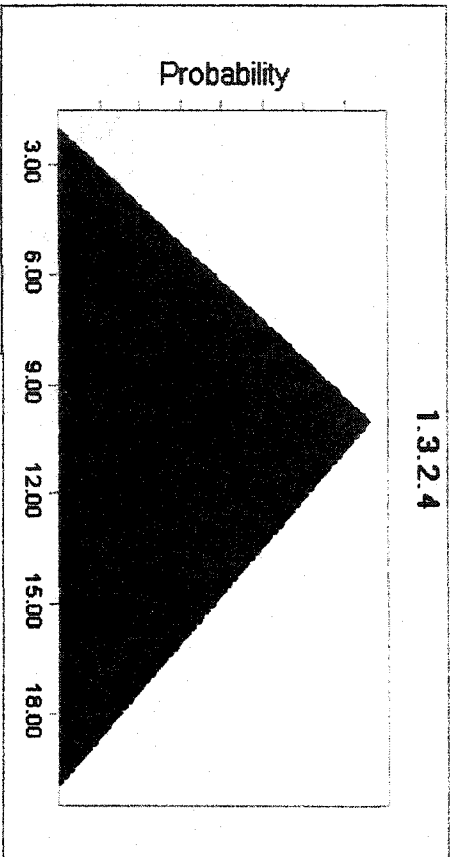
SME2
Minimum 0.10
Likeliest 0.30
Maximum 0.70



Minimum 0.18
Maximum 0.90
Alpha 8.41
Beta 6.49

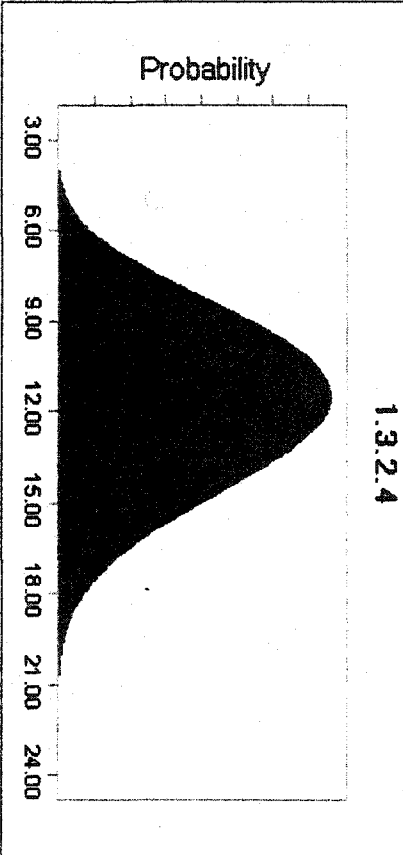
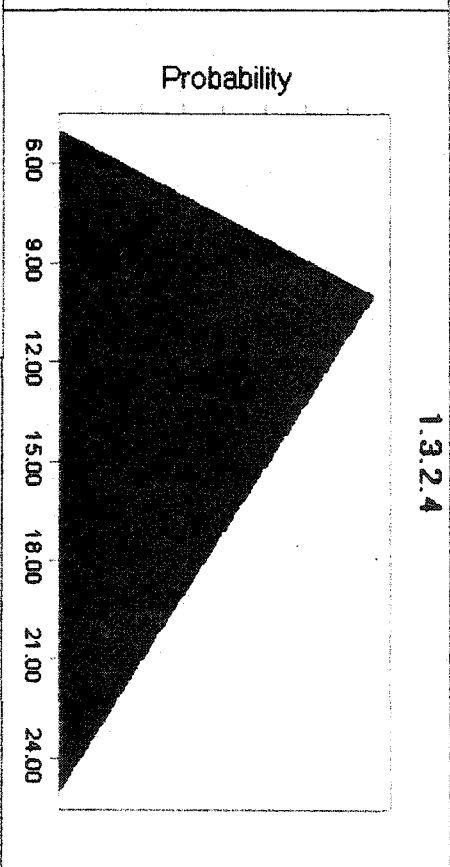
SME1
Minimum 2.00
Likeliest 10.00
Maximum 20.00

1.3.2.4



SME2
Minimum 5.00
Likeliest 10.00
Maximum 25.00

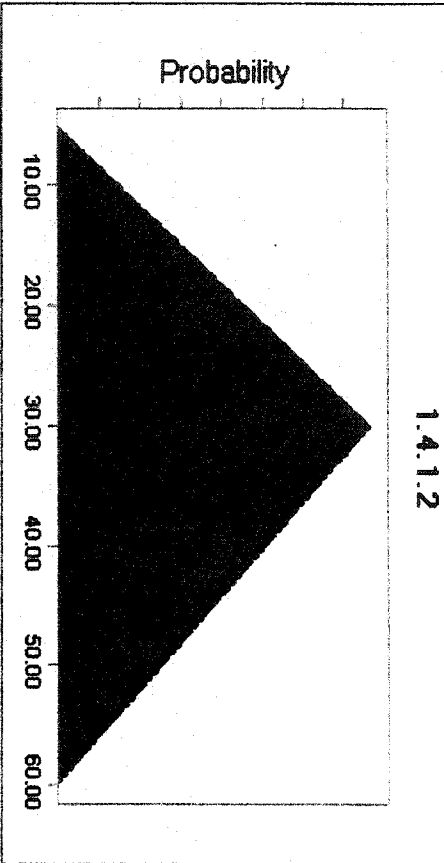
1.3.2.4



Minimum 2.40
Maximum 24.17
Alpha 6.04
Beta 8.08

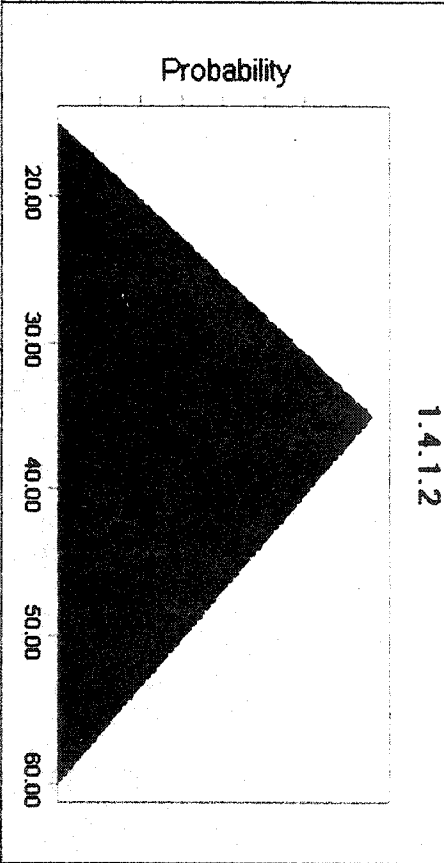
SME1
Minimum 5.00
Likeliest 30.00
Maximum 60.00

1.4.1.2

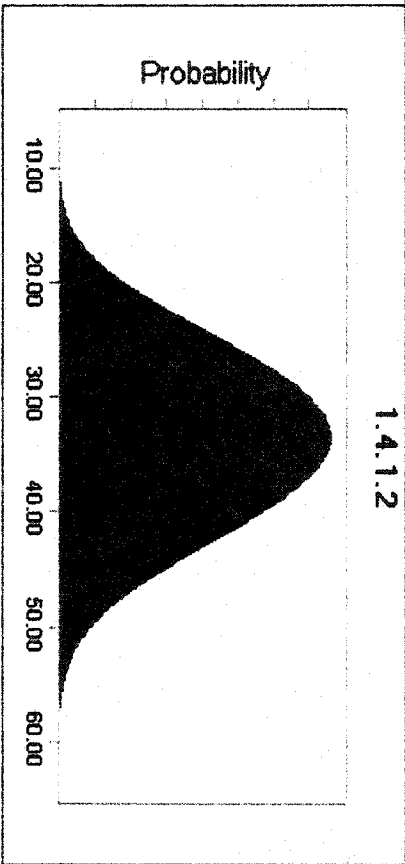


SME2
Minimum 15.00
Likeliest 35.00
Maximum 60.00

1.4.1.2



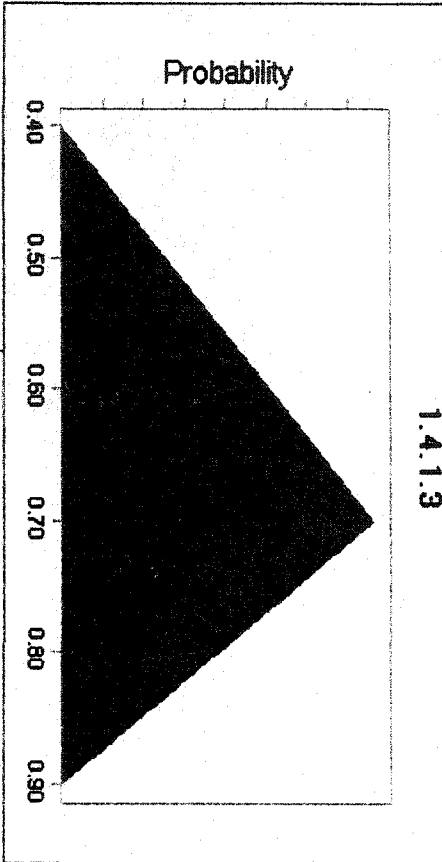
Minimum 6.28
Maximum 63.76
Alpha 6.23
Beta 6.85



1.4.1.2

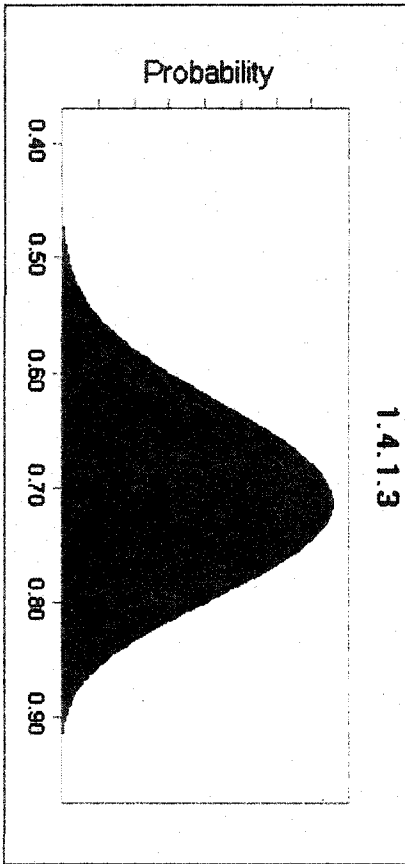
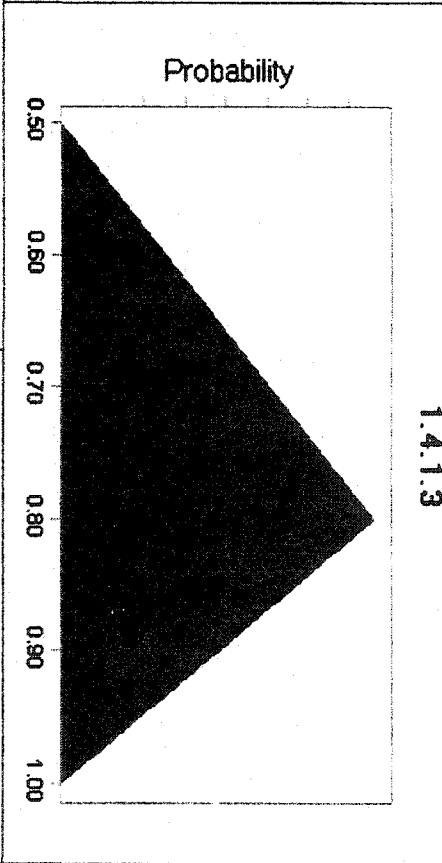
SME1
Minimum 0.40
Likeliest 0.70
Maximum 0.90

1.4.1.3



SME2
Minimum 0.50
Likeliest 0.80
Maximum 1.00

1.4.1.3

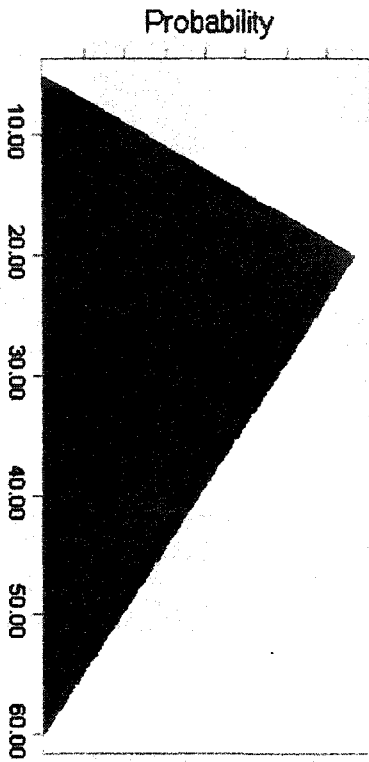


Minimum 0.38
Maximum 0.96
Alpha 7.80
Beta 6.09

1.4.1.3

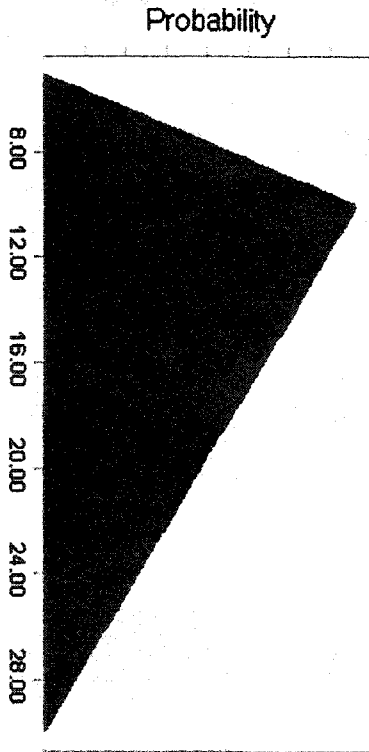
SME1
Minimum 5.00
Likeliest 20.00
Maximum 60.00

1.4.1.4



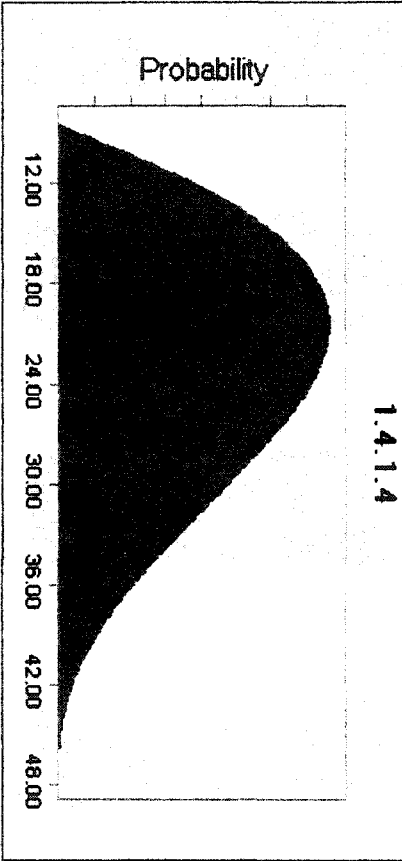
SME2
Minimum 5.00
Likeliest 10.00
Maximum 30.00

1.4.1.4

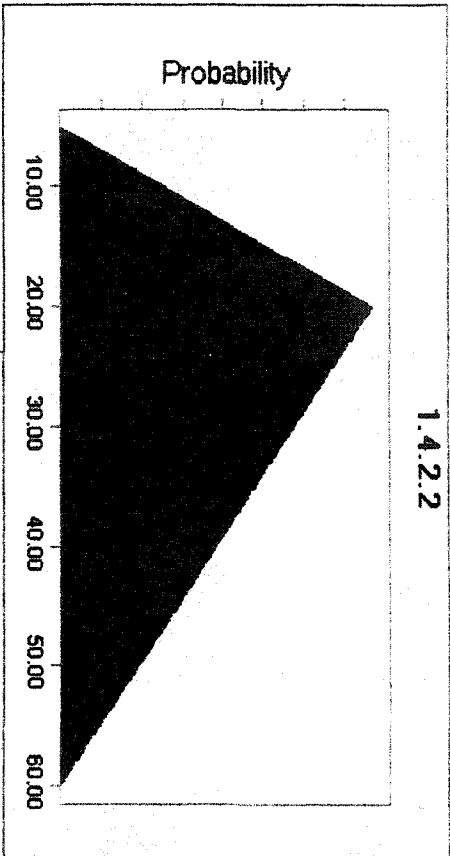


1.4.1.4

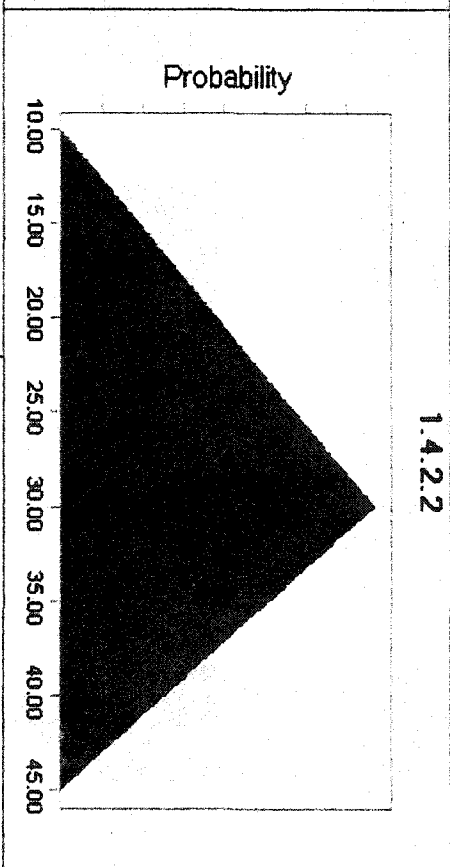
Minimum 8.32
Maximum 47.70
Alpha 2.18
Beta 3.67



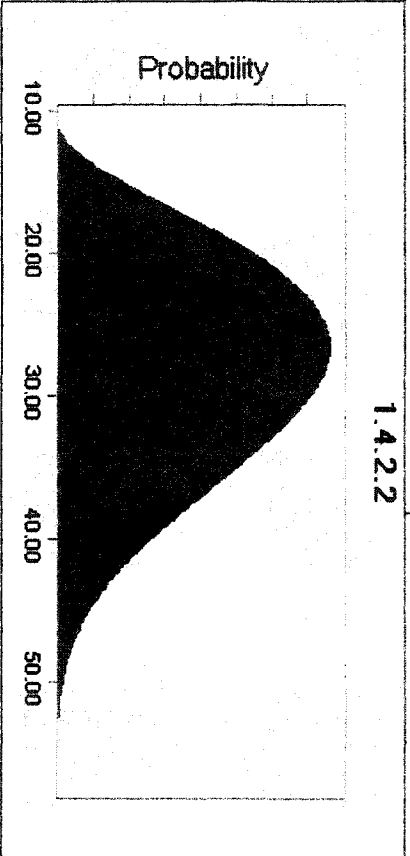
SME1
Minimum 5.00
Likeliest 20.00
Maximum 60.00



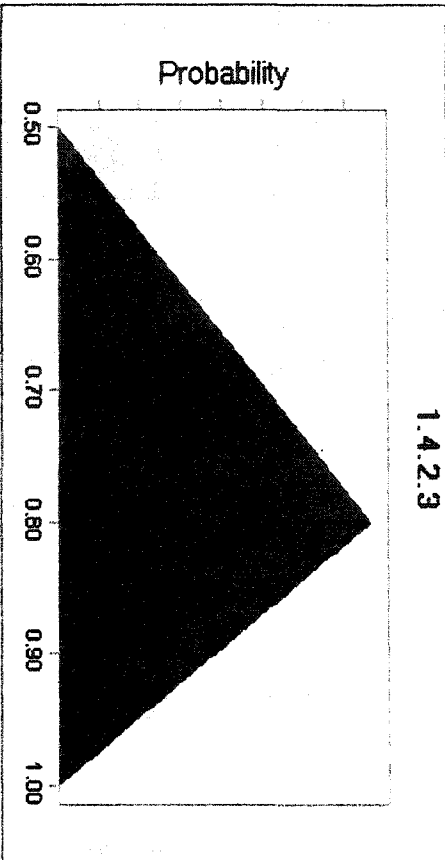
SME2
Minimum 10.00
Likeliest 30.00
Maximum 45.00



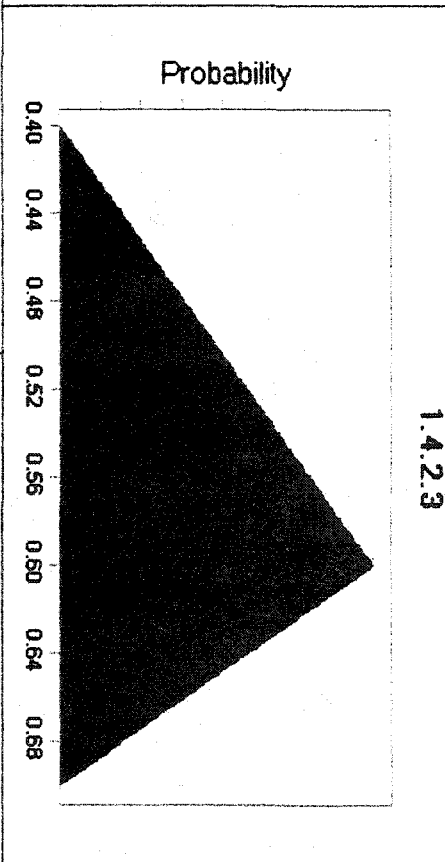
Minimum 10.67
Maximum 56.87
Alpha 3.07
Beta 4.97



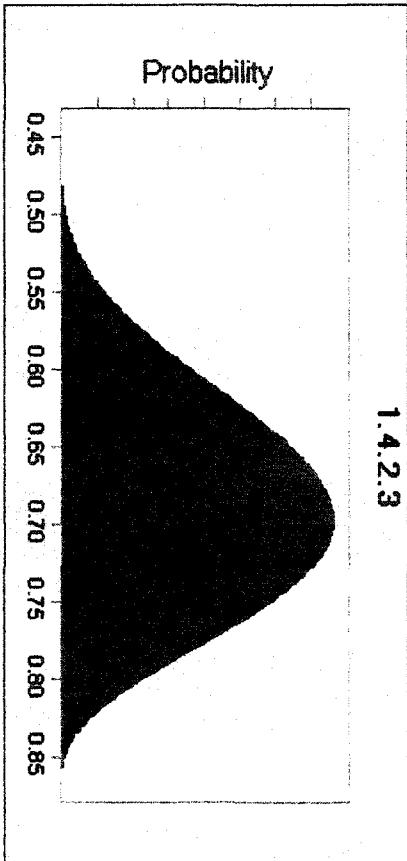
SME1
Minimum 0.50
Likeliest 0.80
Maximum 1.00



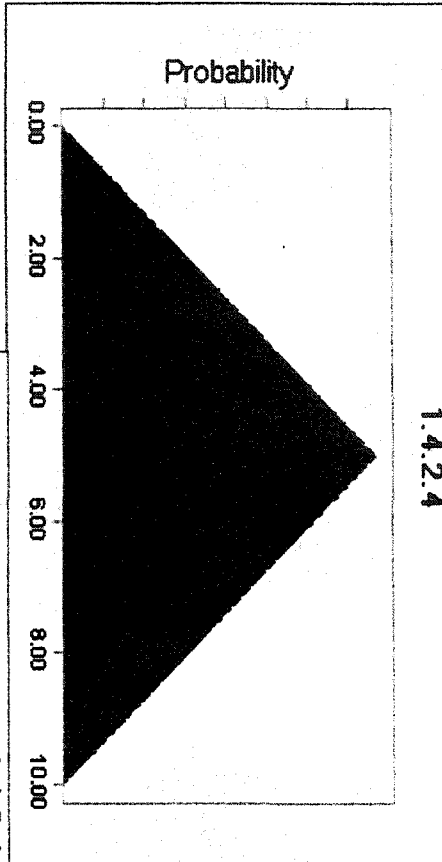
SME2
Minimum 0.40
Likeliest 0.60
Maximum 0.70



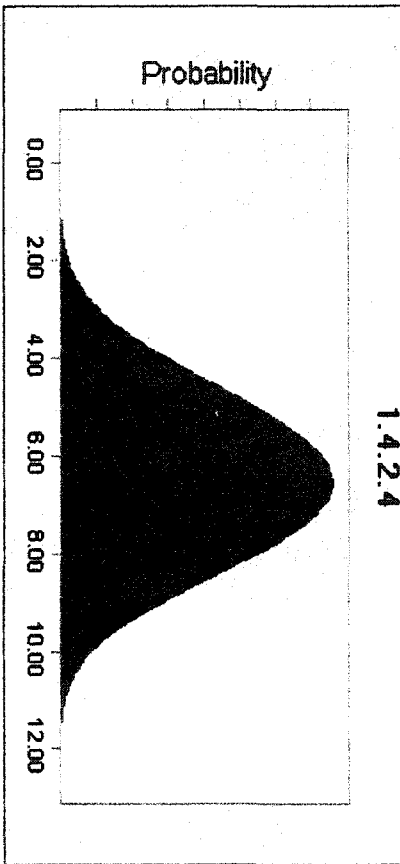
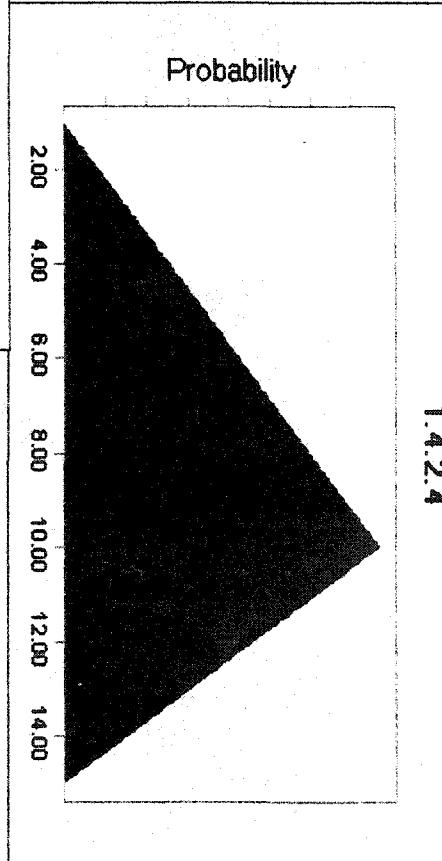
Minimum 0.44
Maximum 0.87
Alpha 5.18
Beta 3.81



SME1
Minimum 0.00
Likeliest 5.00
Maximum 10.00



SME2
Minimum 1.00
Likeliest 10.00
Maximum 15.00

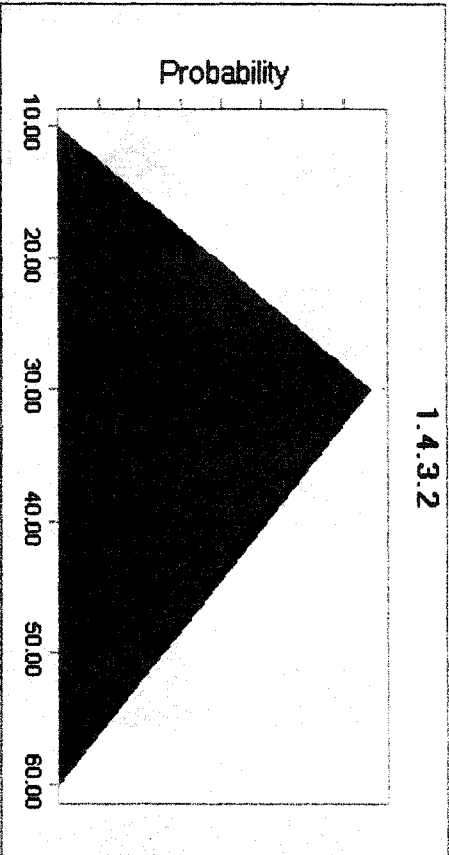


Minimum -0.76
Maximum 12.73
Alpha 7.96
Beta 6.92

SME1
Minimum
Likeliest
Maximum

10.00
30.00
60.00

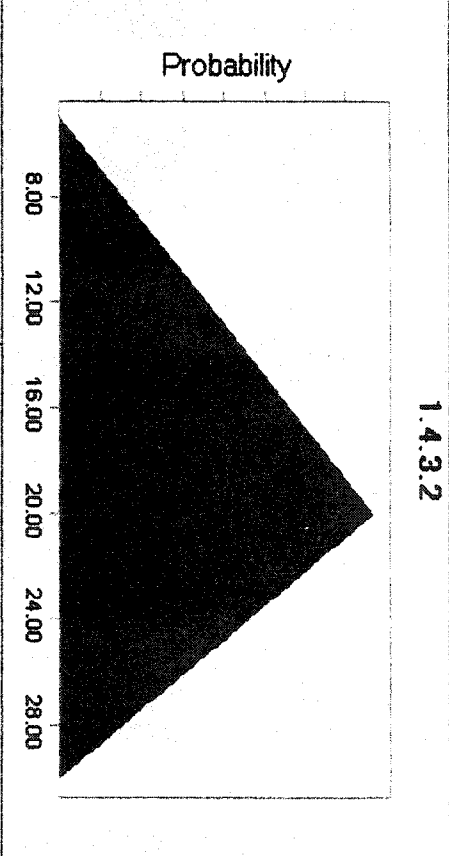
1.4.3.2



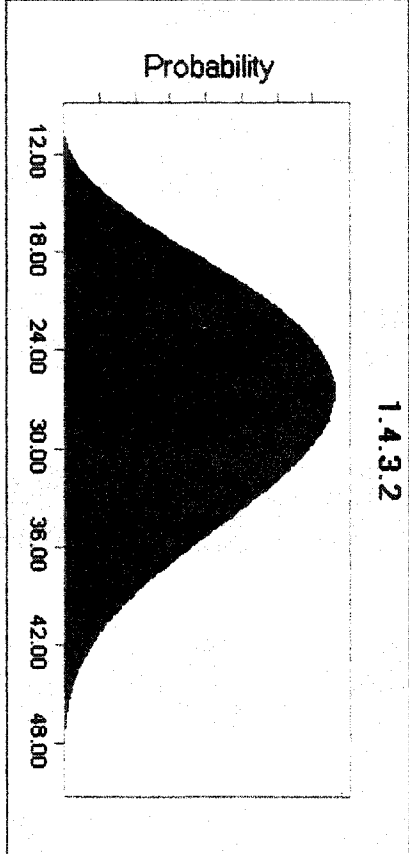
SME2
Minimum
Likeliest
Maximum

5.00
20.00
30.00

1.4.3.2



Probability

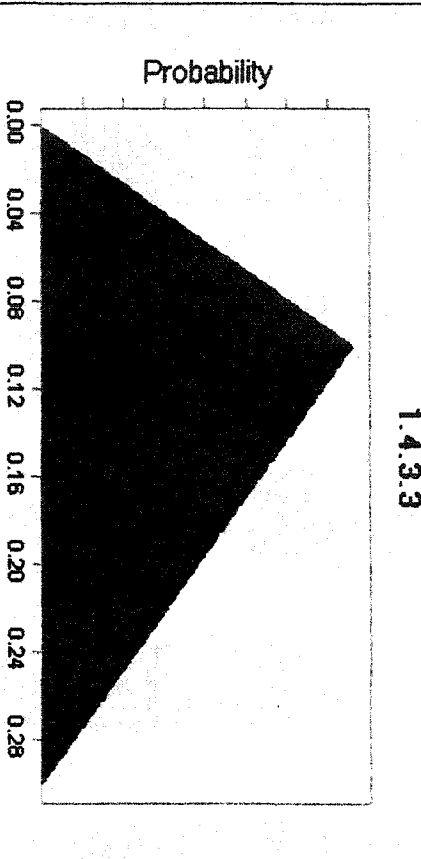


Minimum 9.87
Maximum 50.12
Alpha 3.67
Beta 4.80

1.4.3.2

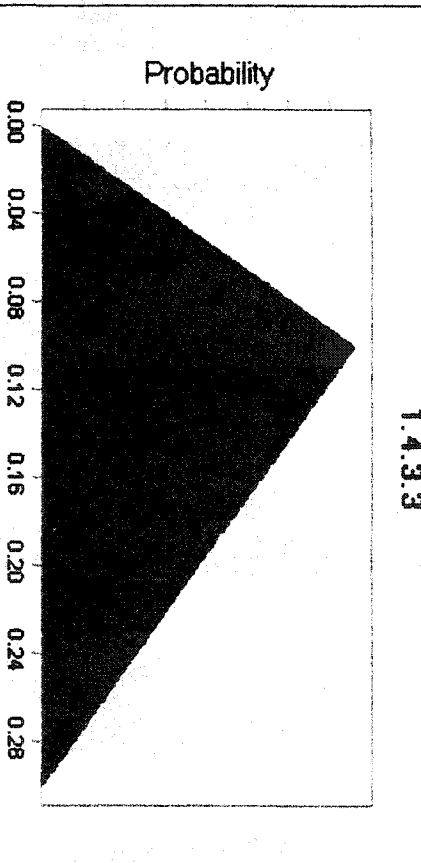
SME1
Minimum 0.00
Likelitest 0.10
Maximum 0.30

1.4.3.3

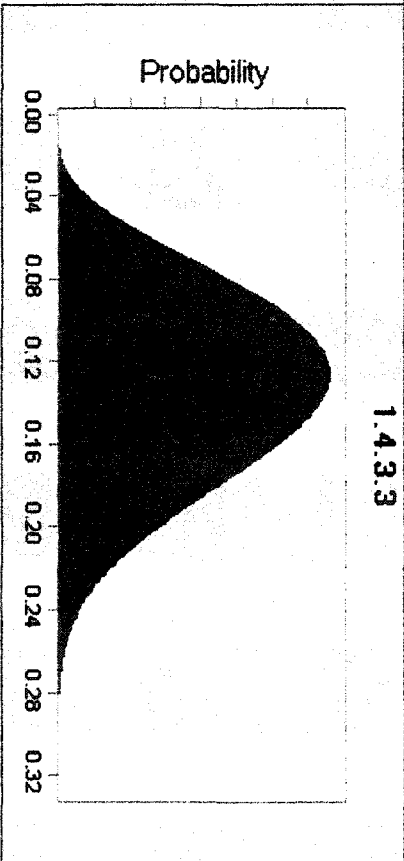


SME2
Minimum 0.00
Likelitest 0.10
Maximum 0.30

1.4.3.3

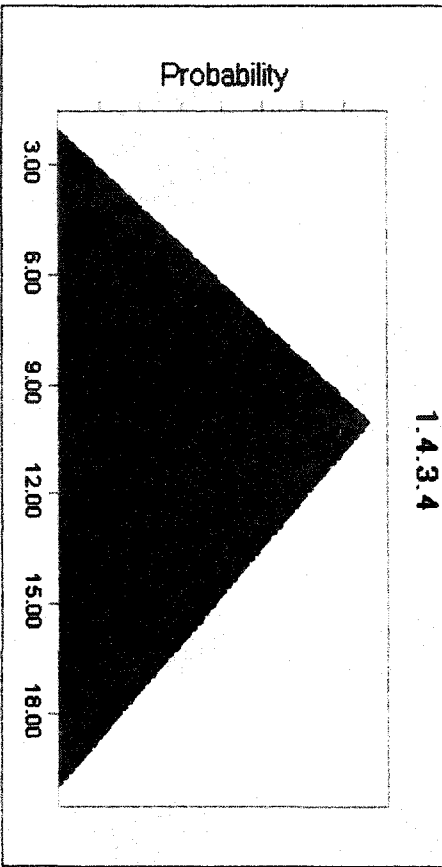


1.4.3.3

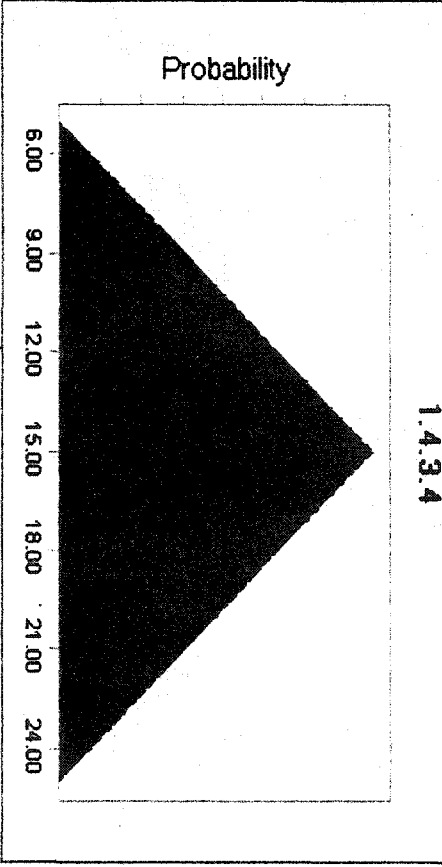


Minimum 0.01
Maximum 0.32
Alpha 4.43
Beta 6.62

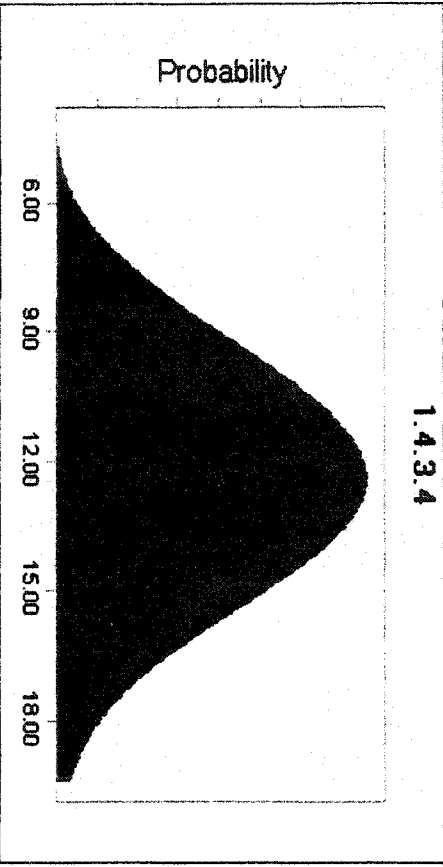
SME1
Minimum 2.00
Likeliest 10.00
Maximum 20.00



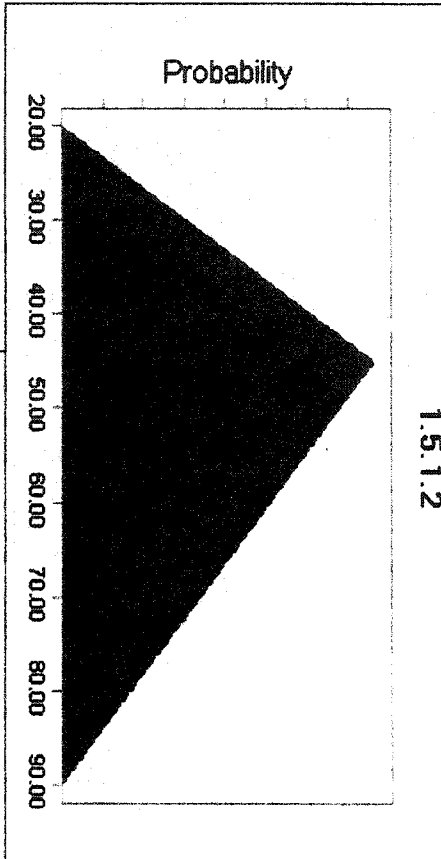
SME2
Minimum 5.00
Likeliest 15.00
Maximum 25.00



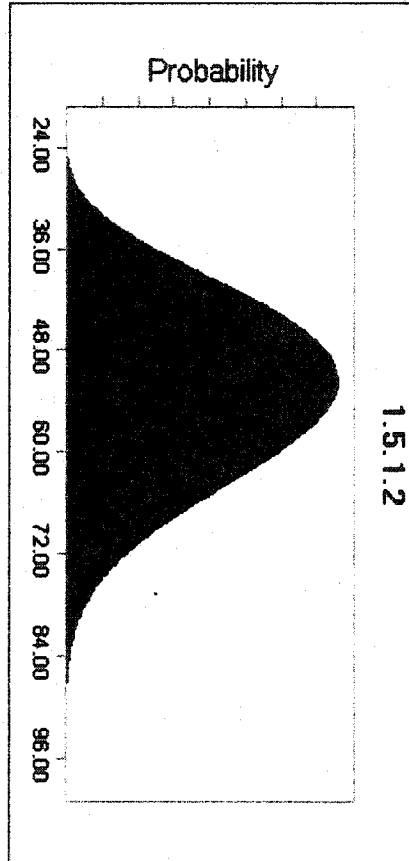
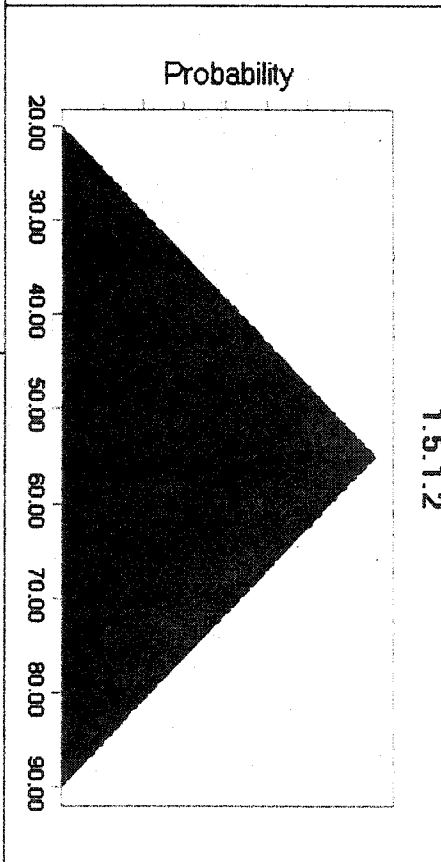
Location 4.17
Scale 9.18
Shape 3.28



SME1
Minimum 20.00
Likeliest 45.00
Maximum 90.00



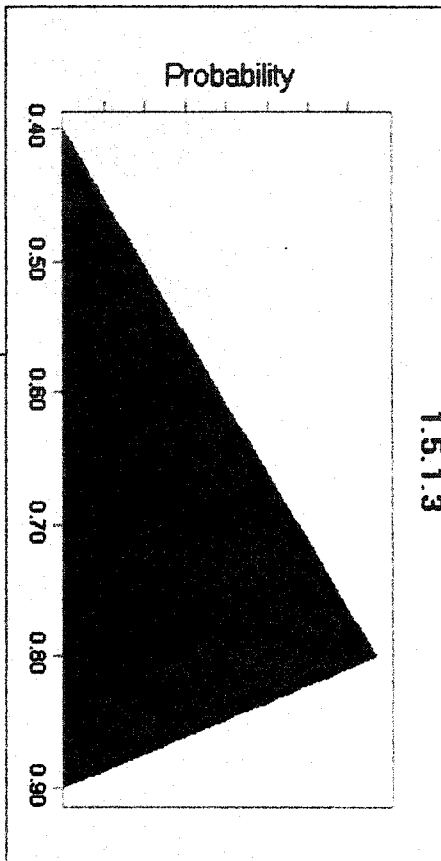
SME2
Minimum 20.00
Likeliest 55.00
Maximum 90.00



Minimum 21.21
Maximum 98.92
Alpha 5.08
Beta 7.37

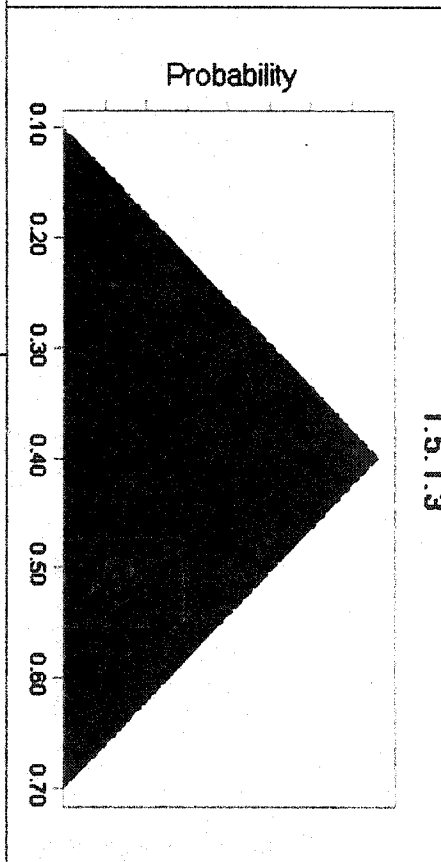
SME1
 Minimum 0.40
 Likeliest 0.80
 Maximum 0.90

1.5.1.3

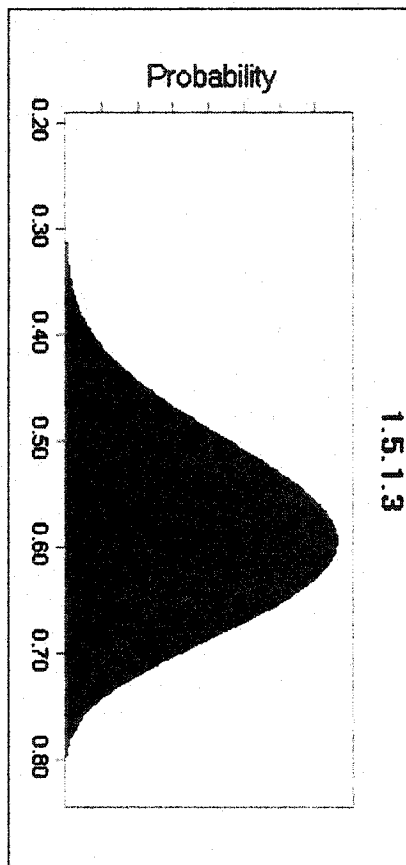


SME2
 Minimum 0.10
 Likeliest 0.40
 Maximum 0.70

1.5.1.3



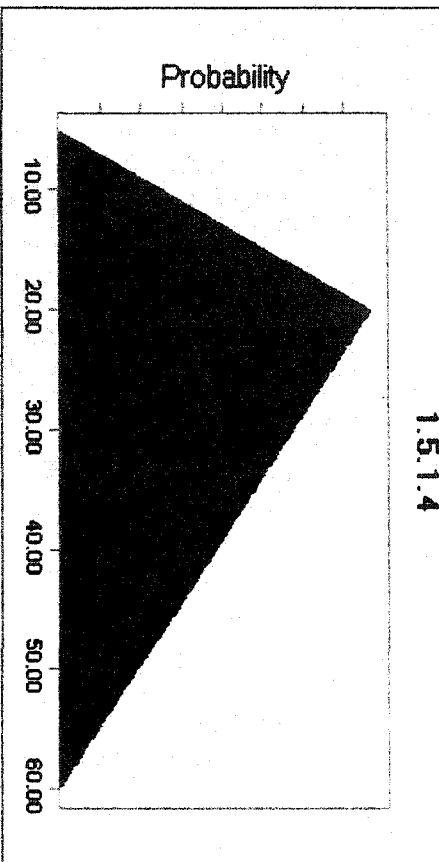
Minimum 0.21
 Maximum 0.83
 Alpha 7.95
 Beta 5.18



1.5.1.3

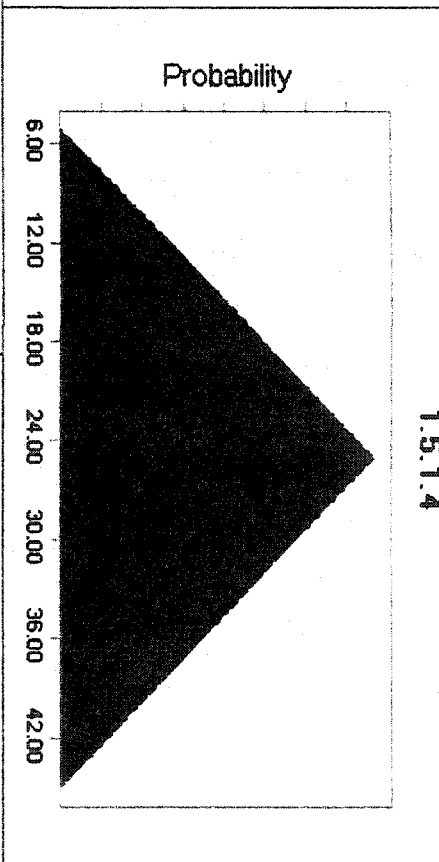
SME1
 Minimum 5.00
 Likeliest 20.00
 Maximum 60.00

1.5.1.4

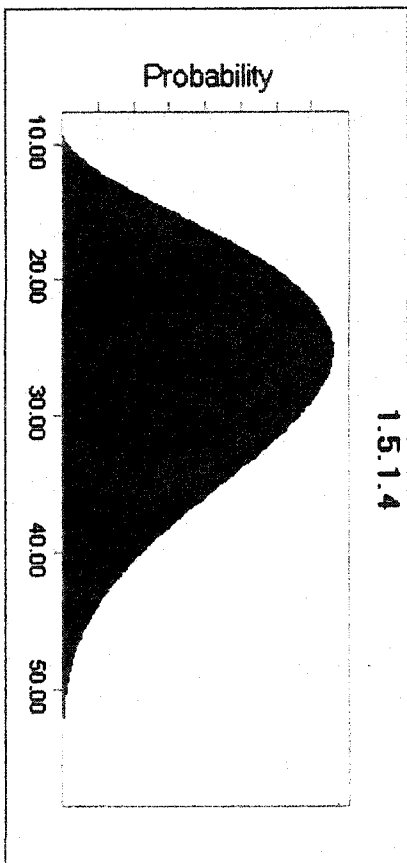


SME2
 Minimum 5.00
 Likeliest 25.00
 Maximum 45.00

1.5.1.4



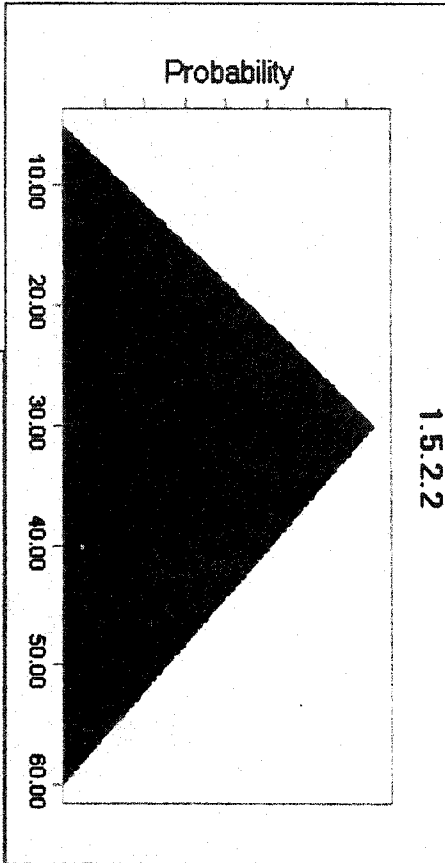
Minimum 8.88
 Maximum 57.23
 Alpha 3.10
 Beta 5.18



1.5.1.4

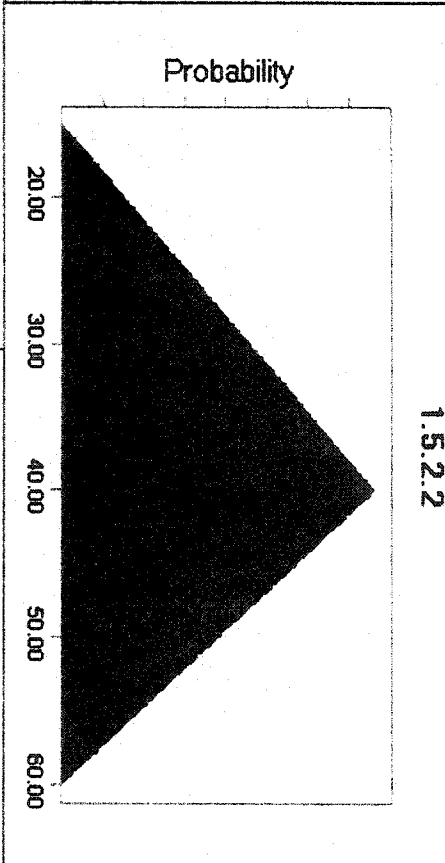
SME1
Minimum 5.00
Likeliest 30.00
Maximum 60.00

1.5.2.2



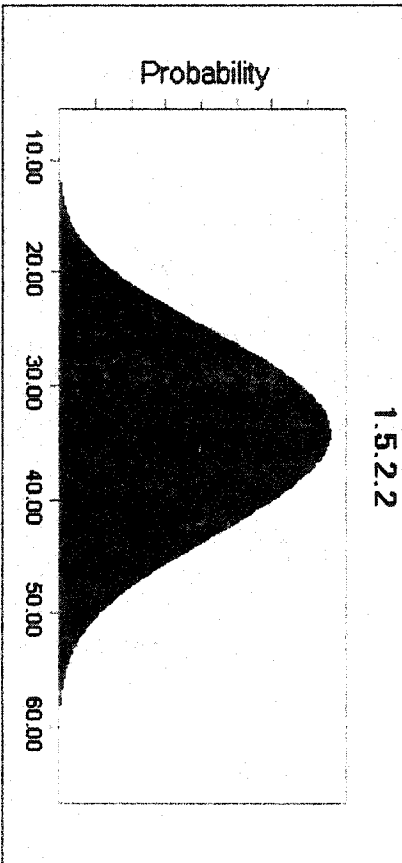
SME2
Minimum 15.00
Likeliest 40.00
Maximum 60.00

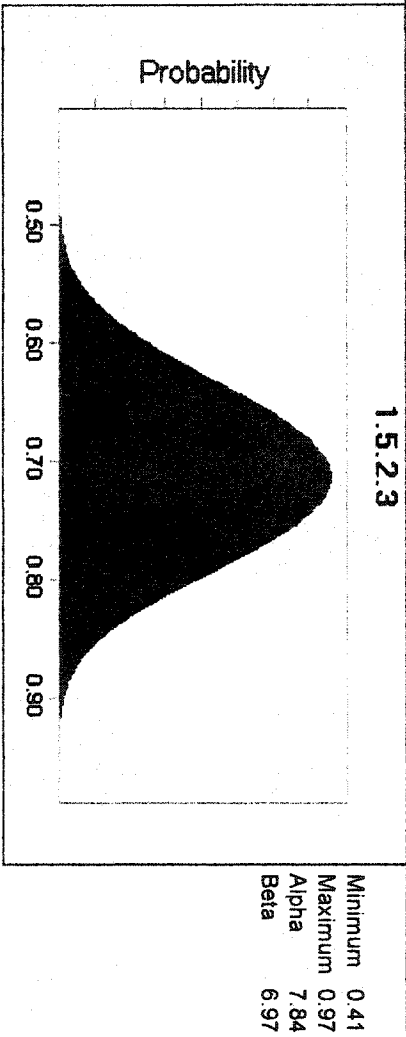
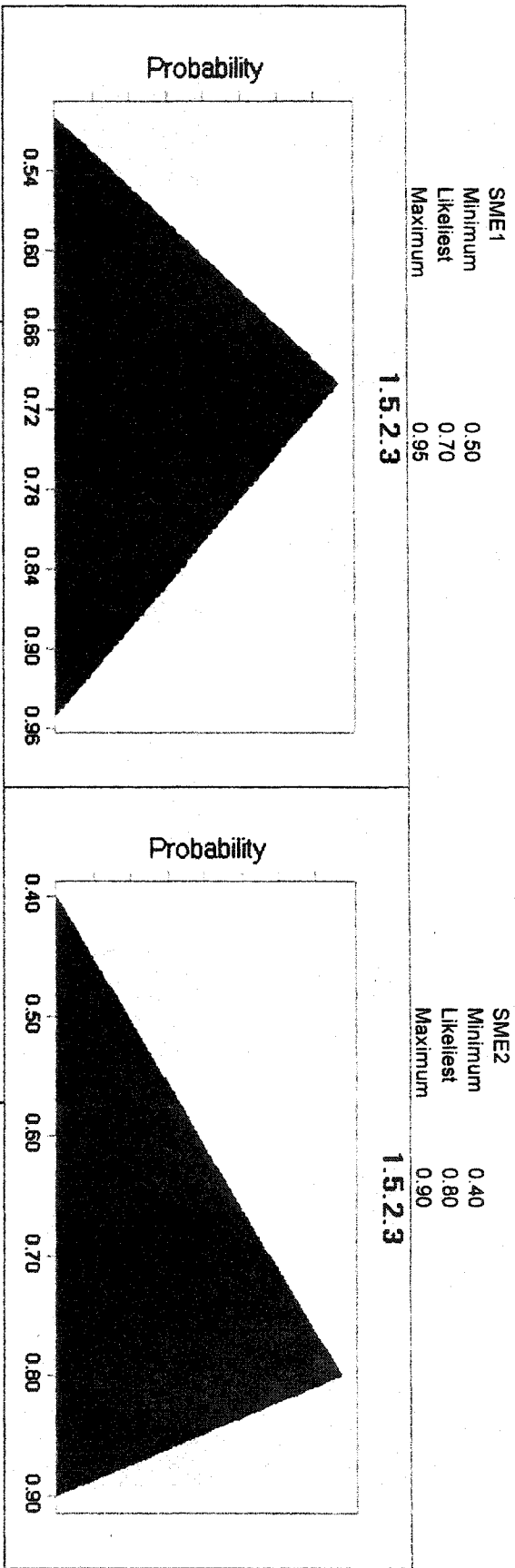
1.5.2.2



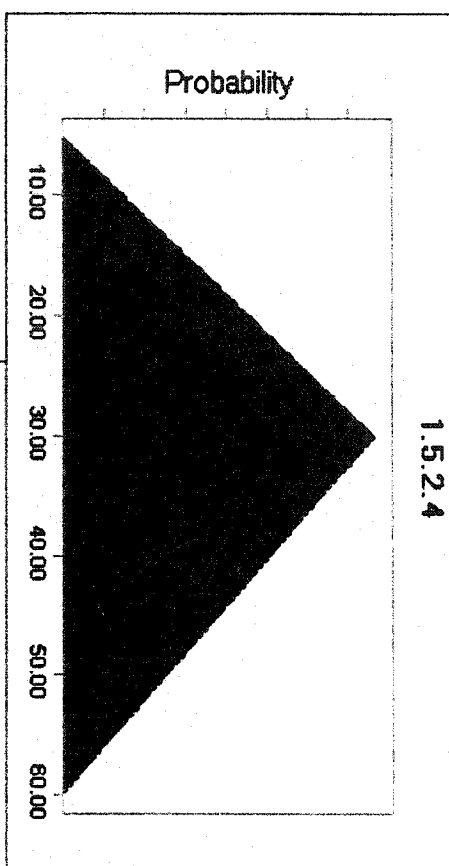
Minimum 7.03
Maximum 64.98
Alpha 6.17
Beta 6.94

1.5.2.2

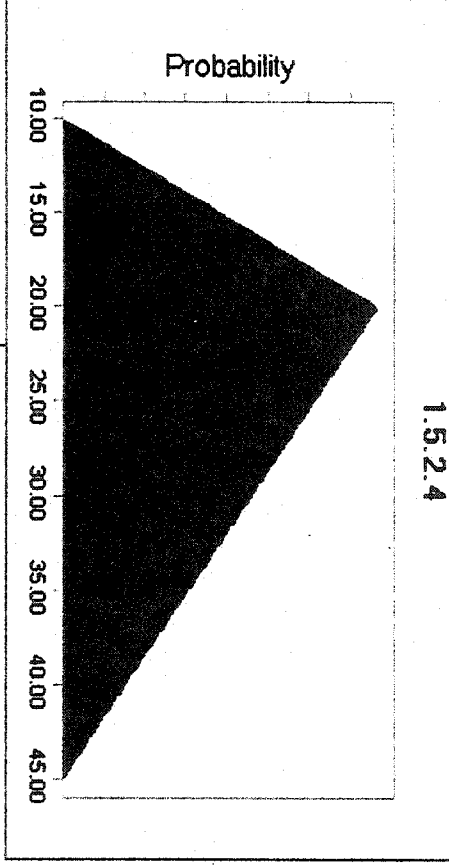




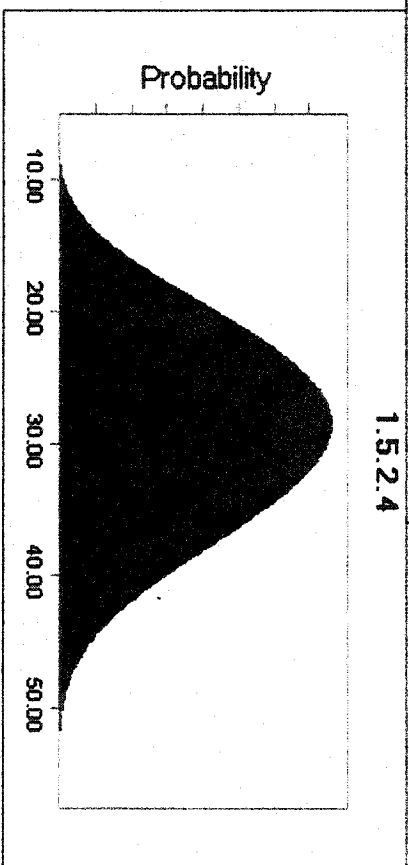
SME1
Minimum 5.00
Likeliest 30.00
Maximum 60.00



SME2
Minimum 10.00
Likeliest 20.00
Maximum 45.00

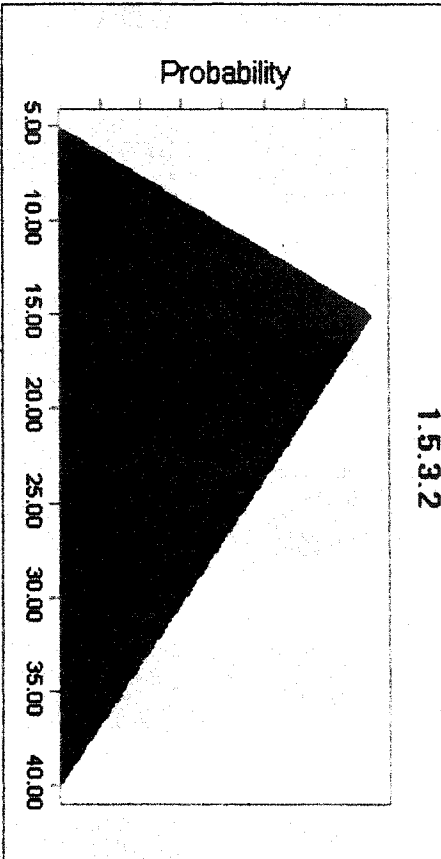


Minimum 6.26
Maximum 56.19
Alpha 4.73
Beta 5.65



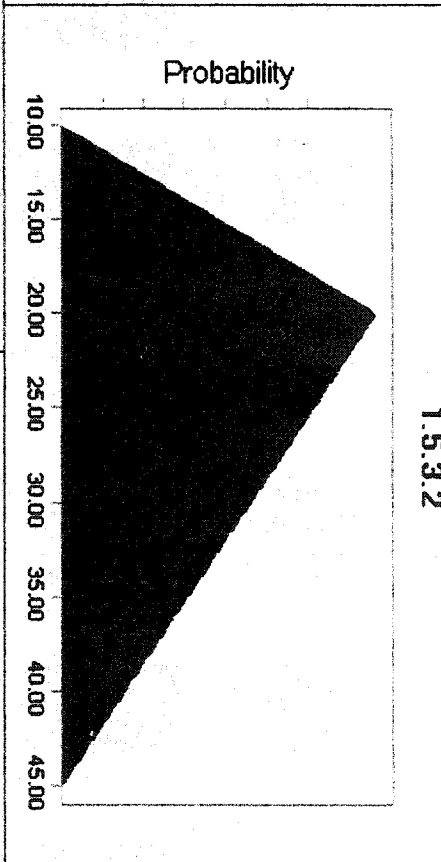
SME1
Minimum 5.00
Likeliest 15.00
Maximum 40.00

1.5.3.2

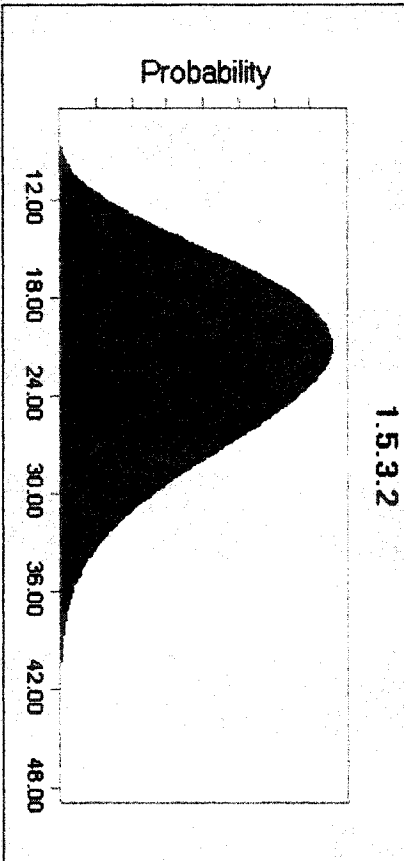


SME2
Minimum 10.00
Likeliest 20.00
Maximum 45.00

1.5.3.2

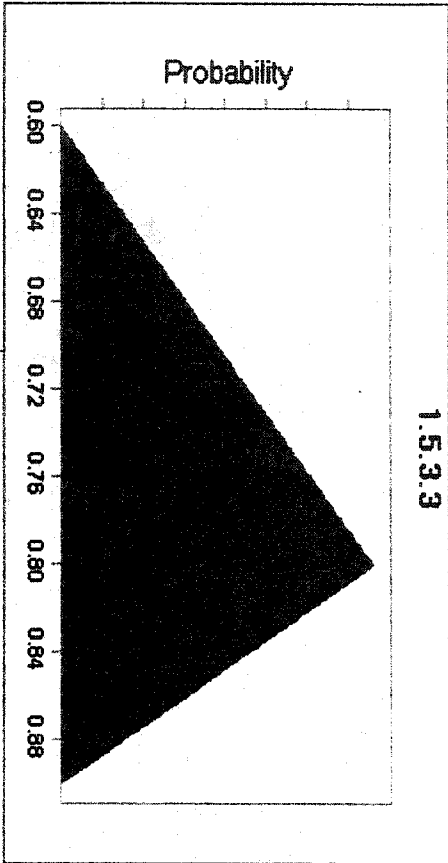


Minimum 7.44
Maximum 47.79
Alpha 4.46
Beta 7.89



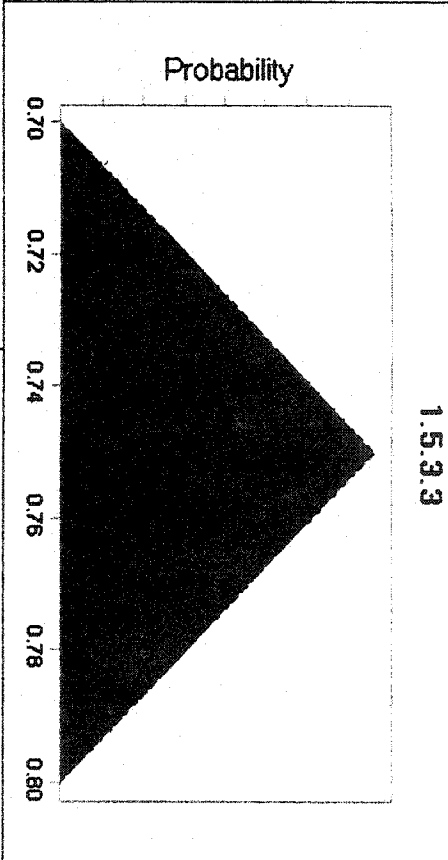
SME1
Minimum 0.60
Likeliest 0.80
Maximum 0.90

1.5.3.3

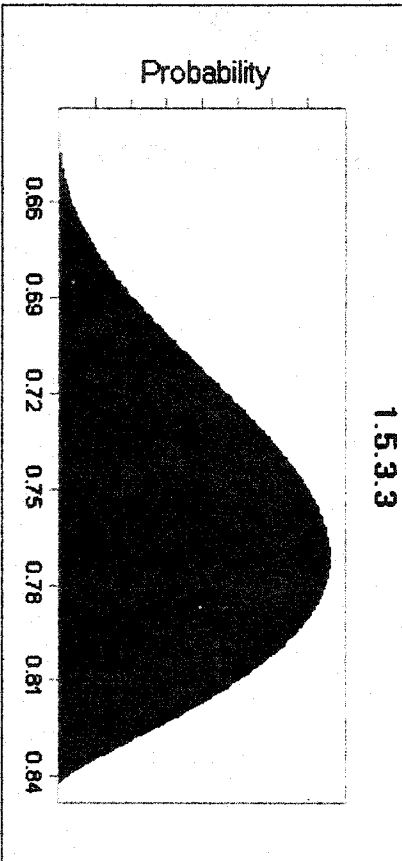


SME2
Minimum 0.70
Likeliest 0.75
Maximum 0.80

1.5.3.3

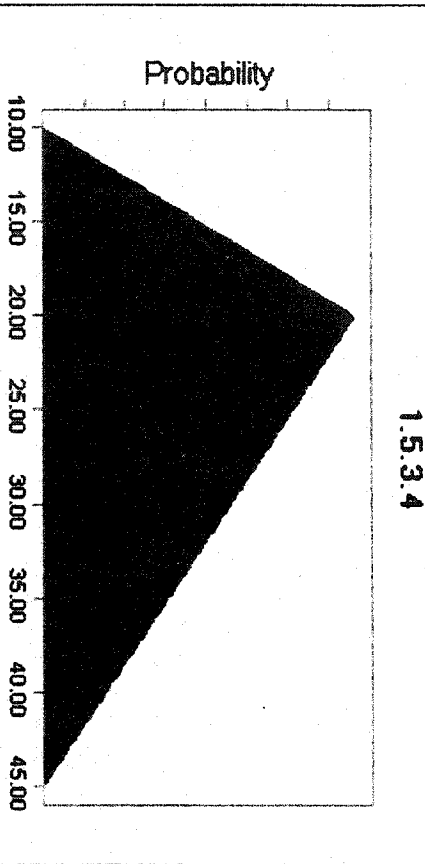


Minimum 0.64
Maximum 0.84
Alpha 3.55
Beta 2.35



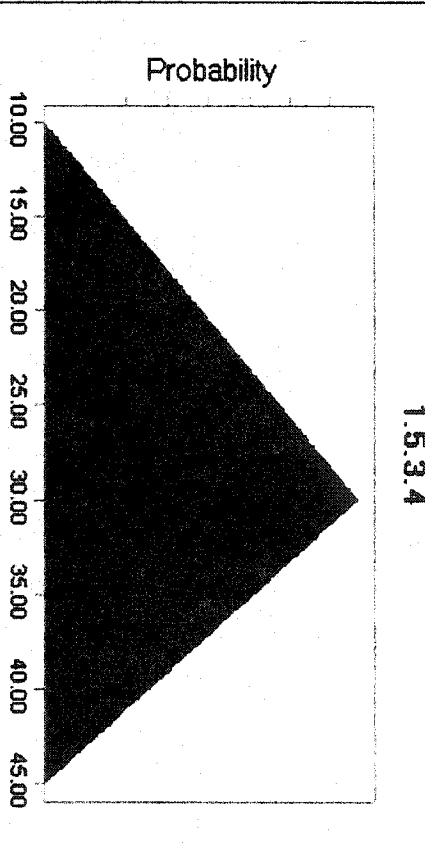
SME1
Minimum 10.00
Likeliest 20.00
Maximum 45.00

1.5.3.4

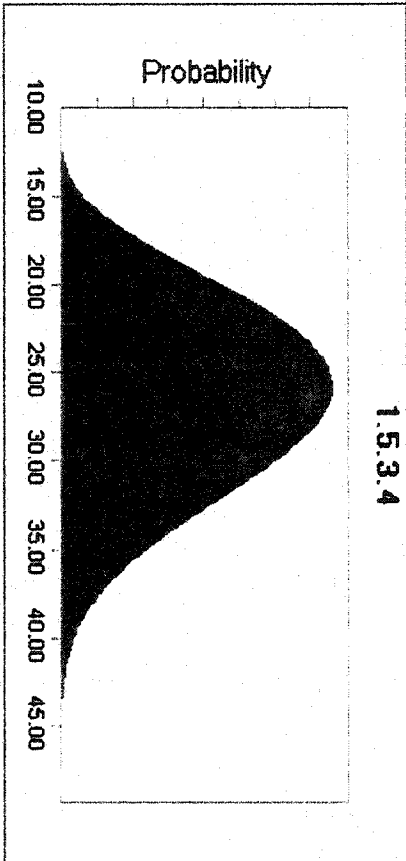


SME2
Minimum 10.00
Likeliest 30.00
Maximum 45.00

1.5.3.4



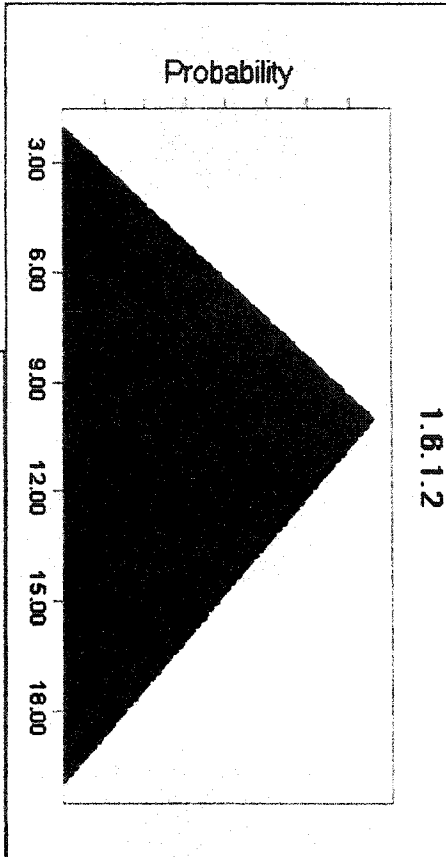
1.5.3.4



Minimum 10.82
Maximum 48.26
Alpha 4.64
Beta 6.50

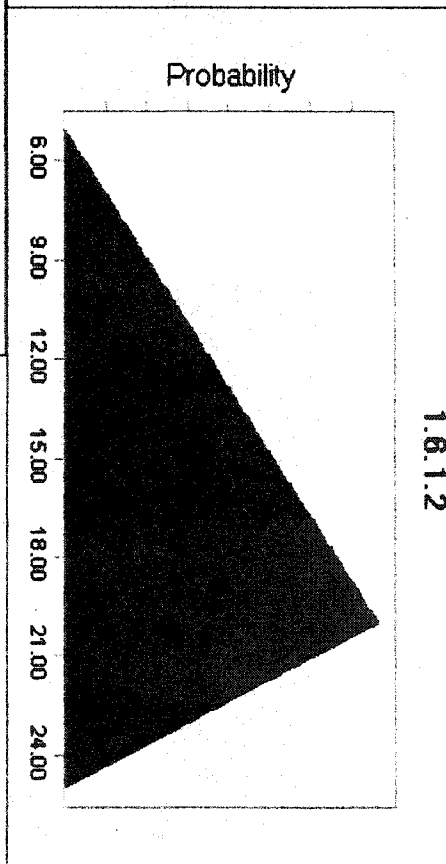
SME1
Minimum 2.00
Likeliest 10.00
Maximum 20.00

1.6.1.2

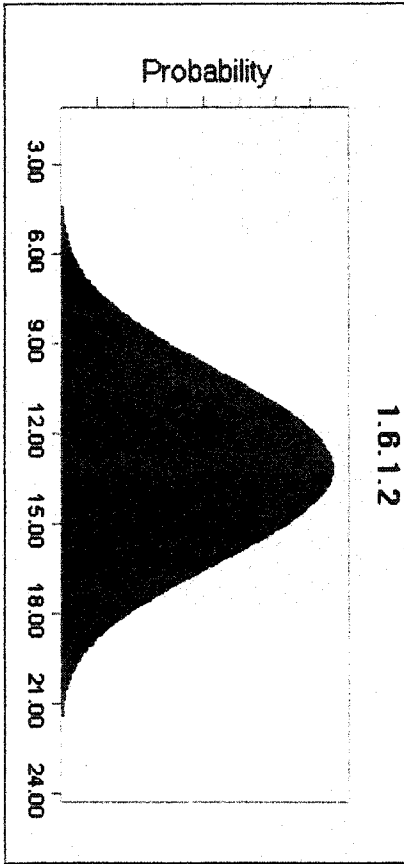


SME2
Minimum 5.00
Likeliest 20.00
Maximum 25.00

1.6.1.2

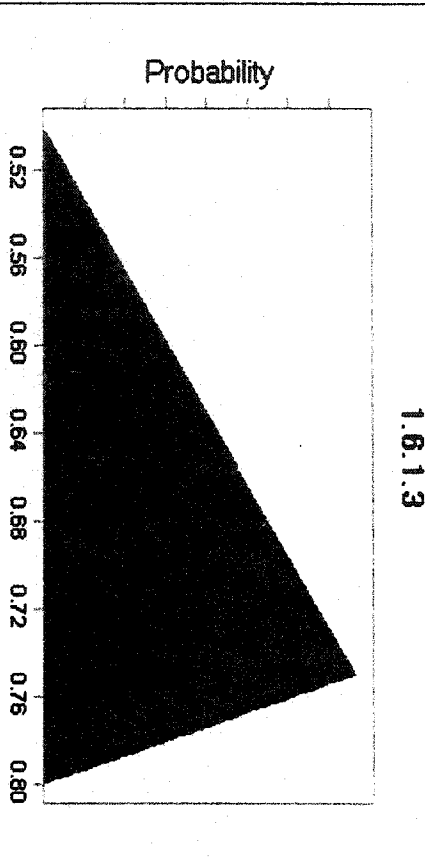


Minimum 1.64
Maximum 23.67
Alpha 7.41
Beta 6.87



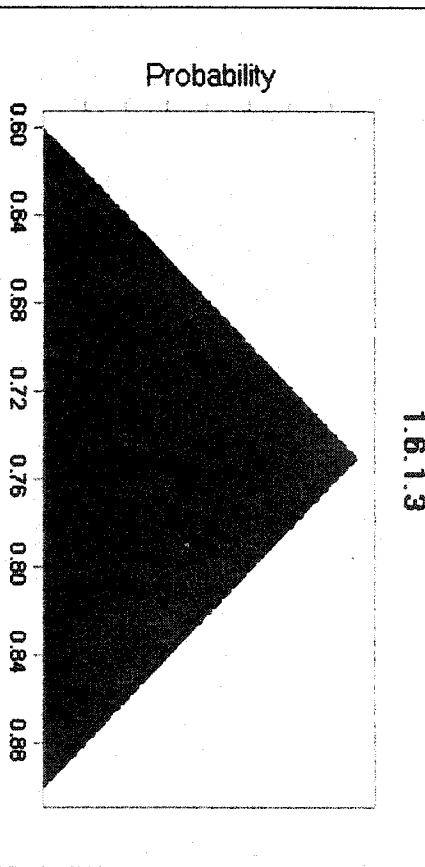
SME1
Minimum 0.50
Likeliest 0.75
Maximum 0.80

1.6.1.3

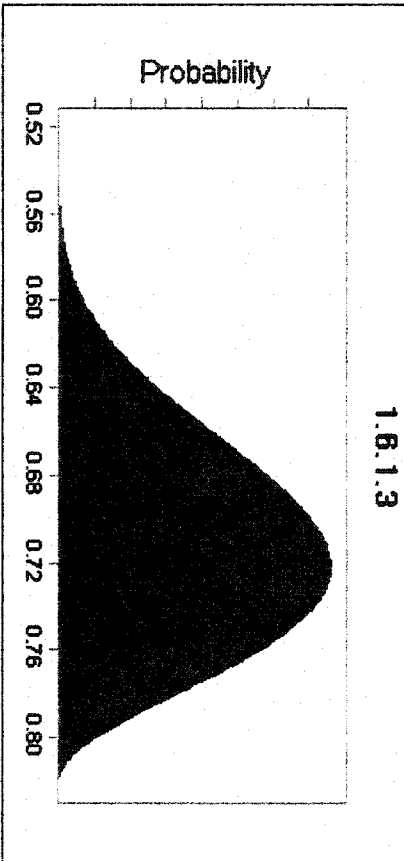


SME2
Minimum 0.60
Likeliest 0.75
Maximum 0.90

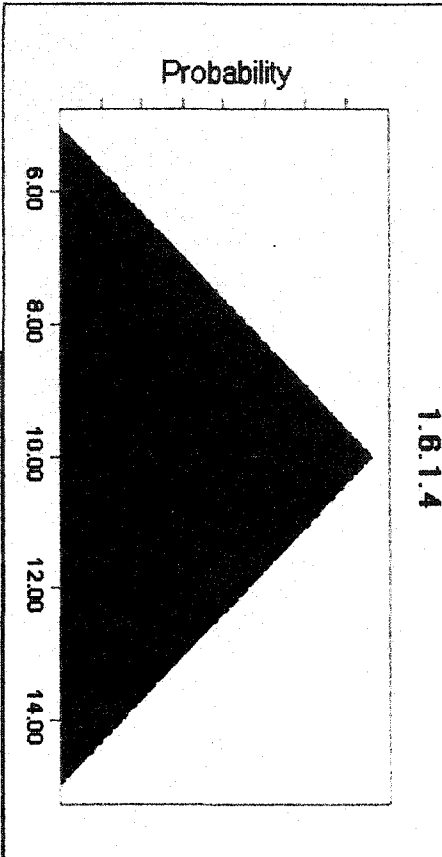
1.6.1.3



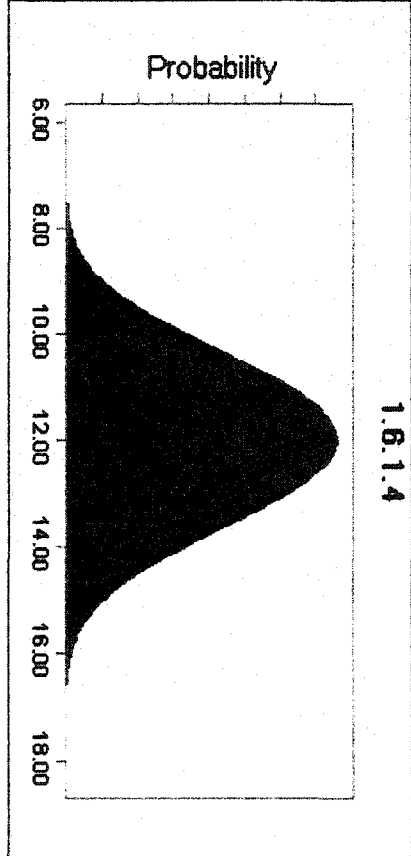
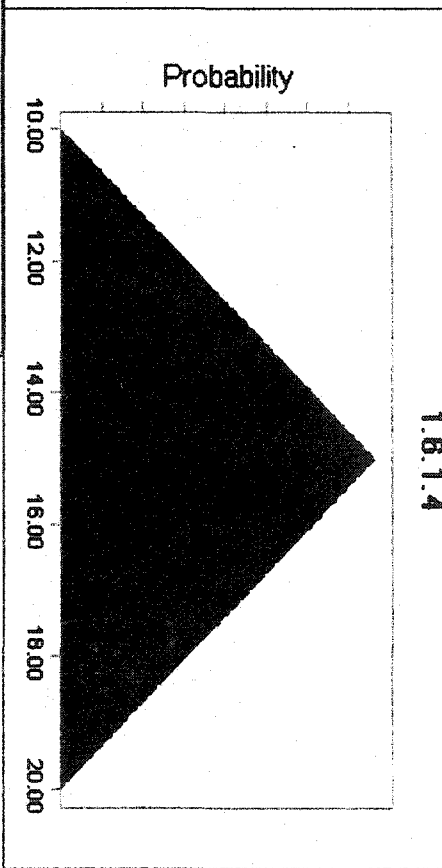
Minimum 0.52
Maximum 0.82
Alpha 5.54
Beta 3.25



SME1
Minimum 5.00
Likeliest 10.00
Maximum 15.00



SME2
Minimum 10.00
Likeliest 15.00
Maximum 20.00



Minimum 5.98
Maximum 18.36
Alpha 8.14
Beta 8.60

APPENDIX I Vita

Education

1. Ph.D., Engineering Management, Department of Engineering Management and Systems Engineering, Old Dominion University, Norfolk, VA.
2. MS, Systems Engineering, Department of Systems and Information Engineering Information, University of Virginia, Charlottesville, VA.
3. BS, Mechanical Engineering Technology, University of Southern Mississippi, Hattiesburg, MS.

Experience Summary

1. Current research is centered on doctoral dissertation: Quantifying Vulnerability to Critical Infrastructure.
2. Six years of experience conducting basic research on military transformational issues, future space and air operations, designing complex organizational system value models and measures of effectiveness.
3. 19 years of military service in various command, staff and academic positions in the US Army
4. Conducted system studies and published numerous papers developing methodologies to address infrastructure security, joint military headquarters, and base camp design.
5. Research - focused on the field of cyber risk to supervisory control and data acquisition (SCADA) systems (i.e. the computer systems that control critical infrastructures); future base camp design (where to locate, what to bring, and optimal layout), and joint strike force (future joint C2 headquarters design).
6. Numerous facilitation sessions and workshops, applying the principles of risk analysis, decision-making, problem-solving, operations research and systems theory to a myriad of military governmental issues.
7. Invited speaker at conferences and workshops chairman in England, Australia, and New Zealand regarding novel approaches to amorphous security models for critical infrastructures.

Academic and Military Positions

1. Academy Professor Selectee, Department of Systems Engineering, United States Military Academy, West Point, New York, December 2002 - June 2003.
2. Analyst, Operations Research Center of Excellence and Assistant Professor, Department of Systems Engineering, United States Military Academy, West Point, New York, 1998-2002.
3. Battery Commander, C/4-3 Air Defense Artillery, Fort Riley, Kansas, 1995-1996
4. Stinger Platoon Leader, 197th Infantry Brigade (M)(S), Fort Benning, Georgia and Desert Shield/Storm, 1990-1993
5. Vulcan Platoon Leader, A/5-5 Air Defense Artillery, Korea 1989-1990

Presentations and Awards

1. Invited Speaker: Quantifying Vulnerability to Critical Infrastructure, Homeland Security Symposium, University of Southern California, 15-16 January 2005.
2. Invited Speaker: Keynote Address, The Amorphous Security Model: Contextual security in SCADA and critical infrastructure, Inaugural National SCADA Conference of New Zealand, upcoming, 28-29 October 2003.
3. Chairman: SCADA Security Technical Workshop, upcoming, 30 October 2003.
4. Invited Speaker: Keynote Address, A Systems-based Vulnerability Assessment Methodology for Critical Infrastructure Systems, Australian SCADA Conference, Sydney, Australia, 16-17 June 2003.
5. Chairman, Workshop A: Security and Risk Management in SCADA Systems, and Conference Chair, Day 2, Sydney, Australia, 18 June 2003.
6. Chairman, Working Group 24 (Measures of Effectiveness) for the Military Operations Research Society, June 2003.
7. Chairman, Workshop for Technical Focus on Vulnerability to Critical Infrastructures, European SCADA Conference, London, England, 14-16 February 2003.
8. Invited Speaker, Engineering Foundation Conference on Risk-Based Decision-making in Water Resources IX, October 2002.
9. Panel member and Invited Speaker, Society of American Military Engineers Conference June 2001
10. Co-Chairman, Working Group 24 (Measures of Effectiveness) for the Military Operations Research Society, 16-18 June 2001.
11. Chairman, Working Group 24 (Measures of Effectiveness) for the Military Operations Research Society, 10-12 June 2002.
12. Panel member and Invited Speaker, Engineering Foundation Conference on Risk-Based Decision-making in Water Resources IX, October 2000.
13. Recipient of the 1998 Distinguished Graduate Student Award for Outstanding Scholarship and Public Service from the Center for Risk Management of Engineering Systems, University of Virginia.
14. Invited Keynote Speaker, Institution of Engineers, Australia, Western Australian Division: *SCADA at the Crossroads 1998*, (an international conference at the Sheraton Perth Hotel, Western Australia), November 16-19, 1998.
15. Commandant's List graduate, Infantry Officer Advance Course, 1993.
16. Graduated with Honors, University of Southern Mississippi, 1988.
17. Distinguished Military Graduate, University of Southern Mississippi (1988).

Teaching Experience

1. SE401 Introduction to Systems Design (United States Military Academy), Fall 1998.
2. SE402 Systems Design (United States Military Academy), Spring 1998, Fall 1999 and 2000.
3. SE403 Systems Design II (United States Military Academy), Spring 1999, 2000, and 2001.

4. SE489 Advanced Individual Studies (United States Military Academy), Spring 1999, 2000, 2001.
5. MTH 206 Elementary Statistics (Adjunct Professor Mount Saint Mary's College), Summer 2000 and Spring 2001.
6. PSY 210 Statistical Methods in Psychology (Adjunct Professor Saint Thomas Aquinas College), Spring 2001.

Membership In Professional Societies

1. American Waterworks Association
2. Association of the United States Army
3. Society of the First Division
4. 24th Infantry Division Association (Life)
5. Air Defense Artillery Association (Life)
6. Military Operations Research Society
7. Society of American Military Engineers
8. The Institute of Electrical and Electronics Engineers: Systems, Man, And Cybernetics
9. Society for Risk Analysis

Scholarly Publications

1. Barry C. Ezell, "Toward a Systems-Based Vulnerability Assessment Methodology for Water Supply Systems", Engineering Foundation Conference on Risk-Based Decision-Making in Water Resources X Proceedings, February 2003.
2. Barry C. Ezell, "Base Camp Technical Report", Operations Research Center, United States Military Academy, West Point, NY, June 2001.
3. Mark W. Brantley and Barry C. Ezell, "Analysis Paradigms: Are you thinking on-, in, or outside-the-box?" *Military Engineer*, Vol. 93, No. 612, 2001.
4. Barry C. Ezell, Mark W. Brantley, and Mark J. Davis, "Base Camp Design: Developing a Decision Support Tool for Site Selection and Facility Layout", *Military Engineer*, Vol. 93, No. 610, 2001.
5. Matthew U. Robertson, Barry C. Ezell, and Michael L. McGinnis, "Base Camp Facility Layout", *IEEE 2001 International Conference on Systems, Man and Cybernetics*, October 2001 Proceedings.
6. Randall Klingaman, Ricardo O. Morales, Barry C. Ezell, and Michael L. McGinnis, "Using Cluster Analysis to Develop a Uniformed Joint Task List For Rapid Decisive Operations", *IEEE 2001 International Conference on Systems, Man and Cybernetics*, October 2001 Proceedings.

7. Barry C. Ezell, Yacov Y. Haimes, and James H. Lambert, "Risks of Cyber Attack to Water Utility Supervisory Control and Data Acquisition Systems", *Military Operations Research Journal*, Vol. 6, No. 2, 2001.
8. Greg Parnell, Barry C. Ezell, Yacov Y. Haimes, Kent Schlüssel and Mark Sulcoski, "Designing a OOTW Knowledge Hierarchy for a OOTW Decision Support System for Military Planners", *Phalanx: A Bulletin for the Military Operations Research Society*, December, 2000.
9. Barry C. Ezell, Daniel J. McCarthy, William L. Ratliff, Jr., and Michael L. McGinnis, "Joint Military Headquarters Redesign", *IEEE 2000 International Conference on Systems, Man and Cybernetics*, October 2000 Proceedings.
10. Barry C. Ezell, Gregory Parnell, Yacov Y. Haimes, and James H. Lambert, "Designing an OOTW Decision Support System Military Planners", *IEEE 2000 International Conference on Systems, Man and Cybernetics*, October 2000 Proceedings.
11. Barry C. Ezell, Mark J. Davis, and Michael L. McGinnis, "Designing A Decision Support System For Military Base Camp Site Selection And Facility Layout", Engineering Foundation Conference on Risk-Based Decision Making in Water Resources IX Proceedings, October 2000.
12. Barry C. Ezell, John V. Farr, and Ian Wiese, "The Infrastructure Risk Analysis Model", The American Society of Civil Engineers (ASCE): *Journal of Infrastructure Systems*, Vol. 6, No. 3, 2000.
13. Barry C. Ezell, John V. Farr, and Ian Wiese, "An Infrastructure Risk Analysis of a Municipal Water Distribution System", The American Society of Civil Engineers (ASCE): *Journal of Infrastructure Systems*, Vol. 6, No. 3, 2000.
14. Barry C. Ezell, "Quantifying the Risk of Cyber Intrusion through Total Risk Management", the Proceedings of the Institution of Engineers, Australia, Western Australian Division: SCADA at the Crossroads 1998, (an international conference at the Sheraton Perth Hotel, Western Australia), November 16-19, 1998.
15. Barry C. Ezell, "Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply". A Thesis Presented to the Faculty of the School of Engineering and Applied Science, University of Virginia, May 1998.
16. Barry C. Ezell, "Air Defense for the 197th Infantry Brigade (Separate) during Operation Desert Shield and Storm", *Arabian Knights: A Special Publication for and about our Air Defense Artillery Veterans of Operation Desert Storm*, August 1991.