Awwa
Research
Foundation
Advancing the Science of Water®

Sandia
National
Laboratories

Risk Assessment Methodology for Water Utilities

Second Edition

PROPRIETARY and CONFIDENTIAL REPORT

NUMBER: 1074

LOANED TO

NAME: James Pierce Jr.

AFFILIATION: Town of Addison

Awwa Research Foundation
6666 West Quincy Avenue
Denver, Colorado 80235
Telephone: (303) 347-6100 • Fax: (303) 730-0851 • E-mail: info@awwarf.com

The mission of the Awwa Research Foundation is to advance the science of water to improve the quality of life. Funded primarily through annual subscription payments from over 1,000 utilities, consulting firms, and manufacturers in North America and abroad, AwwaRF sponsors research on all aspects of drinking water, including supply and resources, treatment, monitoring and analysis, distribution, management, and health effects.

From its headquarters in Denver, Colorado, the AwwaRF staff directs and supports the efforts of over 500 volunteers, who are the heart of the research program. These volunteers, serving on various boards and committees, use their expertise to select and monitor research studies to benefit the entire drinking water community.

Research findings are disseminated through a number of technology transfer activities, includingresearch reports, conferences, videotape summaries, and periodicals.

RISK ASSESSMENT METHODOLOGY FOR WATER UTILITIES (RAM-W^{SM}) Second Edition

Prepared by

Security Systems and Technology Center

Sandia National Laboratories
Albuquerque, NM 87185-0789

Jointly sponsored by

Awwa Research Foundation

6666 West Quincy Avenue
Denver, CO 80235-3098

and

U.S. Environmental Protection Agency

Ariel Rios Building
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

This document contains information that is not appropriate for public dissemination. Do not copy or further distribute this information. This information may be subject to International Trade in Arms regulations (ITAR) 22CFR 120-130. Export of ITAR information may require a license from the U.S. Department of State.

Published by the
Awwa Research Foundation

DISCLAIMER

This study was jointly funded by the Awwa Research Foundation (AwwaRF) and the U.S. Environmental Protection Agency under Cooperative Agreement No. X-82956501. AwwaRF and USEPA assume no responsibility for the content of the research study reported in this publication or for the opinions or statements of fact expressed in the report. The mention of trade names for commercial products does not represent or imply the approval or endorsement of AwwaRF or USEPA. This report is presented solely for informational purposes.

Proprietary - Copyrighted

NOT APPROVED FOR PUBLIC RELEASE – This document contains information exempt from mandatory disclosure under the FOIA. Exemption 2 applies.

WARNING – This document contains data whose disclosure is restricted by 5 U.S.C. § 552(b)(2) (2000), the Freedom of Information Act, and the U.S. Attorney General FOIA Memorandum of October 12, 2001. Dissemination of this document is controlled. Violation of governing laws is subject to severe criminal penalties.

DISTRIBUTION – Department of Energy approval required prior to public release. This document may not be transmitted over the open Internet unless it is encrypted.

DESTRUCTION – Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Disclaimer of Liability

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Prepared by Sandia National Laboratories. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

CONTENTS

TABLES

FIGURES

FOREWORD

The Awwa Research Foundation is a nonprofit corporation dedicated to the implementation of a research effort to help water utilities respond to regulatory requirements and traditional high-priority concerns of the industry. The research agenda is developed through consultation with subscribers and drinking water professionals. Under the umbrella of a Strategic Research Plan, the Research Advisory Council prioritizes the suggested projects based upon current and future needs, applicability, and past work; the Council's recommendations are then forwarded to the Board of Trustees for final selection. The foundation also sponsors research projects through unsolicited proposals; the Collaborative Research, Research Applications, and Tailored Collaboration programs; and various joint research efforts with organizations such as the U.S. Environmental Protection Agency, the U.S. Bureau of Reclamation, and the Association of California Water Agencies.

This publication is a result of one of these sponsored studies; it is hoped that its findings will be applied in communities throughout the world. The following report serves not only as a means of communicating the results of the water industry's centralized research program, but also as a tool to enlist the further support of nonmember water utilities and individuals.

Projects are managed closely from their inception to the final report by the foundation's staff and a large cadre of volunteers who willingly contribute their time and expertise. The foundation serves a planning and management function and awards contracts to such other institutions as water utilities, universities, and engineering firms. The funding for this research effort comes primarily from the Subscription Program, through which water utilities subscribe to the research program and make an annual payment proportionate to the volume of water they deliver. Consultants and manufacturers subscribe based on their annual billings. The program is designed to offer a cost-effective and fair method for funding research in the public interest.

A broad spectrum of water supply issues is addressed by the foundation's research agenda: resources, treatment and operations, distribution and storage, water quality and analysis, toxicology, economics, and management. The ultimate purpose of the coordinated effort is to assist water suppliers to provide the highest possible quality of water economically and reliably. The true benefits are realized when the results are implemented at the utility level. The foundation's trustees are pleased to offer this publication as a contribution toward that end.

The security of water utilities has become a more prominent concern in recent years. In 1998, President Clinton signed Presidential Decision Directive (PDD) 63, Protecting America's Critical Infrastructures. PDD 63 identifies eight critical infrastructures across the country, including the water supply sector. PDD 63 envisioned a public-private partnership between the owners and operators of these critical infrastructures and the federal government to help improve security. This report for the water supply community is one product of that partnership; it represents a joint effort between the water supply community, the U.S. Environmental Protection Agency, and the U.S. Department of Energy. This report identifies a methodology that a medium or large water utility can use to review their facilities and make informed decisions to reduce the risks from malevolent attack. This methodology will help water utilities first identify what facilities and operations are most critical to accomplishing their missions and then consider how best these critical operations might be protected. The methodology presented in this report will help drinking water utilities decide where security measures can be most effectively applied and thus put to better use the limited time and money resources available for security issues.

Edmund G. Archuleta, P.E	James F. Manwaring, P.E.
Chair, Board of Trustees	Executive Director
Awwa Research Foundation	Awwa Research Foundation

ACKNOWLEDGMENTS

Several drinking water utilities have contributed significant amounts of their time and resources to create both Version 1 and Version 2 of RAM-W^{SM}. AwwaRF, Sandia National Laboratories, and the U.S. Environmental Protection Agency would like to thank the management and staff of the following water utilities:

City of Alamogordo
Milwaukee Water Works
Seattle Public Utilities
Tucson Water
Massachusetts Water Resources Authority
Washington Aqueduct
District of Columbia Water and Sewer Authority

Additionally, the authors would like to acknowledge the many hours of review and input from the Project Advisory Committee assembled by AwwaRF whose careful review and thoughtful comments improved the quality of the final product:

- Russel Balbirona, Bureau of Reclamation
- Kevin Brown, DEQ Division of Drinking Water
- Steve Dennis, Alameda County Water District
- Kevin Gertig, Fort Collins Water Utilities
- Robin J. Hamblet, CISSP, City of Portland
- Steve Jackson, Bureau of Reclamation
- Jack Jacobs, EMA, Inc.
- Bruce Johnson, City of Tucson Water Department
- Thomas Kahler, Newport News Waterworks
- Jerry Obrist, Lincoln Water System
- John W. Porco, PE, Michael Baker, Jr., Inc.
- Raymond Riordan, East Bay Municipal Utility District
- Alan Roberson, AWWA
- Marty Swickard, USEPA Region 8
- Frank Blaha, PE, Awwa Research Foundation
- Jeff Oxenford, Awwa Research Foundation

EXECUTIVE SUMMARY

In partnership with the Awwa Research Foundation (AwwaRF) and Sandia National Laboratories (Sandia), the EPA has undertaken a program to improve security at water utilities across the United States. At the national level, the EPA has the responsibility to create a Public – Private partnership for improving the security of the water infrastructure. To meet the security needs of the AwwaRF, water utilities, and the EPA, Sandia developed the Risk Assessment Methodology for Water Utilities (RAM-W^{SM}). Version 1 of RAM-W^{SM} was issued in November of 2001. This report contains Version 2, developed and validated over the course of six detailed case studies. Version 2 also contains a cyber assessment methodology, which was not sufficiently developed for inclusion in Version 1. Included as a separate document, to go hand-in-hand with Version 2, is a worked example to demonstrate application of the methodology. Training has been, and continues to be, available on the methodology from consultants trained and licensed by Sandia. Contact information for the trainers can be found at <www.epa.gov/safewater/security/>.

Version 2 is much more than a methodology. It represents the wisdom and experience gained through multiple water utility assessments intertwined with years of security experience. Examples of how to apply the methodology are included in the body of the text as well as in the separate example water utility.

Although this version of RAM-W^{SM} completely updates and better explains the methodology, it is still strongly recommended that assessment teams receive training before undertaking an assessment. The training has been specifically designed for this methodology and will provide additional information, examples, and hands-on experience.

1 INTRODUCTION AND BACKGROUND

1.1 INTRODUCTION

This document presents, explains, and demonstrates the Risk Assessment Methodology for Water Utilities (RAM-W^{SM}), designed to assist water and security professionals in assessing the risks from malevolent threats. Through a systematic, thorough evaluation of the water utility operations, a prioritized plan for consequence mitigation, security upgrades, modifications to operational procedures, and/or policy changes can be developed to mitigate identified risks. This consequence-driven risk-management program is a performance-based approach designed to facilitate a comparative analysis that relies on relative risk rankings and uses a simple-to-understand risk equation. Physical security and cyber security assessment methodologies are both included. Users of RAM-W^{SM} should strive to apply it in a performance-based manner, which ultimately requires some form of performance testing to verify that protection and/or mitigation objectives are met.

The quality of the assessment results is directly related to the training, expertise, and commitment of the team(s) performing the assessment, and the commitment and support of senior management. Following the methodology will aid in describing critical facilities and assets to protect, identifying system vulnerabilities, and determining the level of protection to which the security system should be designed. The goal of RAM-W^{SM} is to provide a plan for balanced risk reduction measures by appropriately applying valuable water utility resources.

1.2 BACKGROUND

During the Clinton administration the National Security Council issued directives that designated several U.S. infrastructures as critical, including the water infrastructure. The Environmental Protection Agency (EPA) was assigned the responsibility to develop plans for improving water infrastructure security, in cooperation with water industry associations, such as the Association of Metropolitan Water Agencies (AMWA) and the American Water Works Association (AWWA), as well as metropolitan water agencies. During this same period, the American Water Works Association Research Foundation (AwwaRF) noted an increased concern about security among its membership of water utilities. In response, AwwaRF embarked on a program to develop a methodology and the associated tools for completing security risk assessments of water utilities.

Version 1 of RAM-W^{SM} was issued in November of 2001, and a training program on how to apply the methodology followed in December of the same year. On June 12, 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 into law (PL 107-188). This Bioterrorism Act requires community water systems serving populations of greater than 3,300 persons to conduct vulnerability assessments. Over 8,000 communities are required to assess and report on their vulnerabilities determined through a security risk assessment. The EPA requires the following elements in the risk assessment:

"A satisfactory vulnerability assessment (V/A) is comprised of the following eight major elements and processes. A V/A is a systematic analysis used to determine the malevolent risks posed to the operations of water supply, treatment, and distribution systems. A satisfactory V/A is a thorough and systematic evaluation of the … water utility system, characterized by the following elements:

1. Determination of water system objectives by:
   - Identifying the important missions/functions of the system to be assessed,
   - Identifying the undesirable consequences that could affect the missions/functions.
   - Determining the assets that need to be protected to minimize the impacts of the undesirable events/consequences,
   - Determining the malevolent acts that could reasonably cause these events/consequences.
2. Prioritization of adverse events/consequences affecting the water system and the surrounding community including:
   - Loss of critical function and/or major service disruption,
   - Intentional attack on public safety via water utility assets, contamination of the water supply, and chemical releases or chemical theft.
3. Definition of how the malevolent acts might be conducted, such as:
   - Physical damage,
   - Chemical, biological, and radiological contamination,

- Cyber attacks on the Supervisory Control and Data Acquisition (SCADA) or other process control systems,
- Interdependency disruptions (e.g., electrical, transportation, etc.)

4. Assessment of the likelihood (qualitative probability) of such malevolent acts from defined threat sources (e.g. terrorist, insider, determined vandal, casual vandal, etc.)
5. Systematic site characterization of the water system to include the collection of performance data on:
   - Important facilities, processes, and assets,
   - Physical protection system features of deterrence, detection, delay, and response.
   - Cyber protection system features,
- Security policies and procedures and compliance with same.

6. The approach to the V/A is "performance-based," meaning that is evaluates the risk to the water system based on the effectiveness of the security system against the specific malevolent acts determined in the initial step.
7. The V/A determines the most critical assets (targets) in a water system, details their interrelationships within other assets in the system, identifies the consequences of malevolent acts that could be directed against them, and evaluates the effectiveness of both existing and proposed protection systems.
8. The V/A identifies a system's vulnerabilities and provides a prioritized plan for security upgrades, modifications of operational procedures, and/or policy changes to mitigate identified risks to critical assets. The V/A also provides a basis for comparing the cost of protection against the risks posed."

Version 2 of RAM-W^{SM} incorporates significant improvements learned through multiple assessments of some of the largest metropolitan water utilities in the United States as well as input received from scores of water utility personnel during RAM-W^{SM} training sessions. Appendices including worked examples have been added to assist the practitioner. The Generic Undesired Event Fault Tree has been completely reworked to make it easier to follow and apply. More explanation has been added to all chapters, and additional sections included where necessary.

The efforts of EPA, AWWA, AwwaRF, and AMWA have been coordinated through this project with the goal of developing a generic security risk assessment methodology to assist water utilities in understanding and mitigating their security risks. Several water utilities have graciously opened their doors and offered countless hours of their staff's time to develop and refine this version of RAM-W^{SM}.

1.3 Design Philosophy: Design and Evaluation of Physical Protection Systems

For more than 25 years, Sandia National Laboratories (Sandia) has employed performance-based methods for designing and evaluating physical protection systems (PPS). This approach has been applied for many years to high-consequence government facilities, and more recently to several critical infrastructures (e.g., federal dams, power utilities, etc.). This document describes the adaptation of this process to the requirements of the water infrastructure. An overview of the Sandia process provides the underlying assumptions used in the adaptation:

> *A PPS integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks. The design of an effective PPS requires a methodical approach in which the designer weighs the objectives of the PPS against available resources and then evaluates the proposed design to determine how well it meets the objectives. Without this kind of careful assessment, the PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points of the facility. For example, it would probably be unwise to protect a facility's employee cafeteria with the same level of protection as the central computing area. Similarly, maximum security at a facility's main entrance would be wasted if entry were also possible through an unprotected loading dock. Each facility is unique, even if performing generally the same activities, so this systematic approach allows flexibility in the application of security tools to address local conditions.*
>
> *The foundation of this approach is the design of an integrated performance-based system. Performance measures (i.e., validated numeric characteristics) for various system components, such as sensors, video, or response time, allow the use of models to predict system performance against the*

> *identified threat. This effectiveness measure can then be used to provide the business rationale for investing in the system or upgrade, based on a measurable increase in system performance and an associated decrease in risk to the facility. Looking at system improvement compared to costs can then support a cost-benefit analysis. By following this process, the system designer will include elements of business, technology, and the criminal justice system into the most effective design within the constraints and budget of the facility. (Garcia, 2001)*

This PPS design philosophy has been applied to the development of RAM-W^{SM}, the security risk assessment methodology for water utilities described in this document. The philosophy has been extended to also consider contributions of non-physical security elements in determining protection system effectiveness. These non-physical security elements, referred to as operational elements, are elements that are intrinsic to the water utility operation. This will be discussed more in later chapters.

The cyber security assessment portion of RAM-W^{SM} is based on a relative ranking assessment approach to water utility SCADA systems. A guided top-down approach provides the basic structure and integrates elements from a variety of IT assessment and evaluation approaches. The process provides an effective means to evaluate the overall system security of water utility SCADA systems and to guide the development and integration of sustainable security improvements. A final, prioritized list of SCADA system assets, ranked by relative security deficiency, indicates an order for applying resources to improve SCADA security.

1.4 RISK ASSESSMENT METHODOLOGY

Chapter 1 of this document provides background information and introduces the methodology. Figure 1.1 is a "waterfall flow diagram" showing the generic risk assessment methodology. This document follows the waterfall flow diagram starting with Chapter 3, explaining each of the major steps along the path. Chapter 2 discusses management decisions and acceptable risks. After discussing project planning and team selection, Chapter 3 introduces the concept of pairwise comparison and provides an example application. Pairwise comparison is a screening tool used to prioritize the water utility's mission objectives and helps identify and prioritize critical facilities for risk evaluation. Chapter 4 discusses threat assessment and provides tools to uncover and understand threats posed by insiders, outsiders, and outsiders working in collusion with insiders. The Cyber Threat is also introduced in Chapter 4. The concept of a Design Basis Threat (DBT) (i.e., the threat level the water utility owner decides the water utility must be protected against with high confidence) is also discussed in this chapter. Chapter 5 presents the site characterization phase and discusses several customized tools. The Undesired Event Generic Fault Tree is a tool introduced in this chapter that should be carefully controlled because it organizes sensitive material that is collected by the water utility as the security risk assessment is applied. The generic fault tree will be customized for the site to identify the most vulnerable parts of the water utility operation being evaluated. Critical assets are identified from the site-specific fault tree, which are assigned consequence levels based on the water utility's site-specific consequence table. How to define consequence measures and develop a site-specific consequence table is presented in Chapter 5.

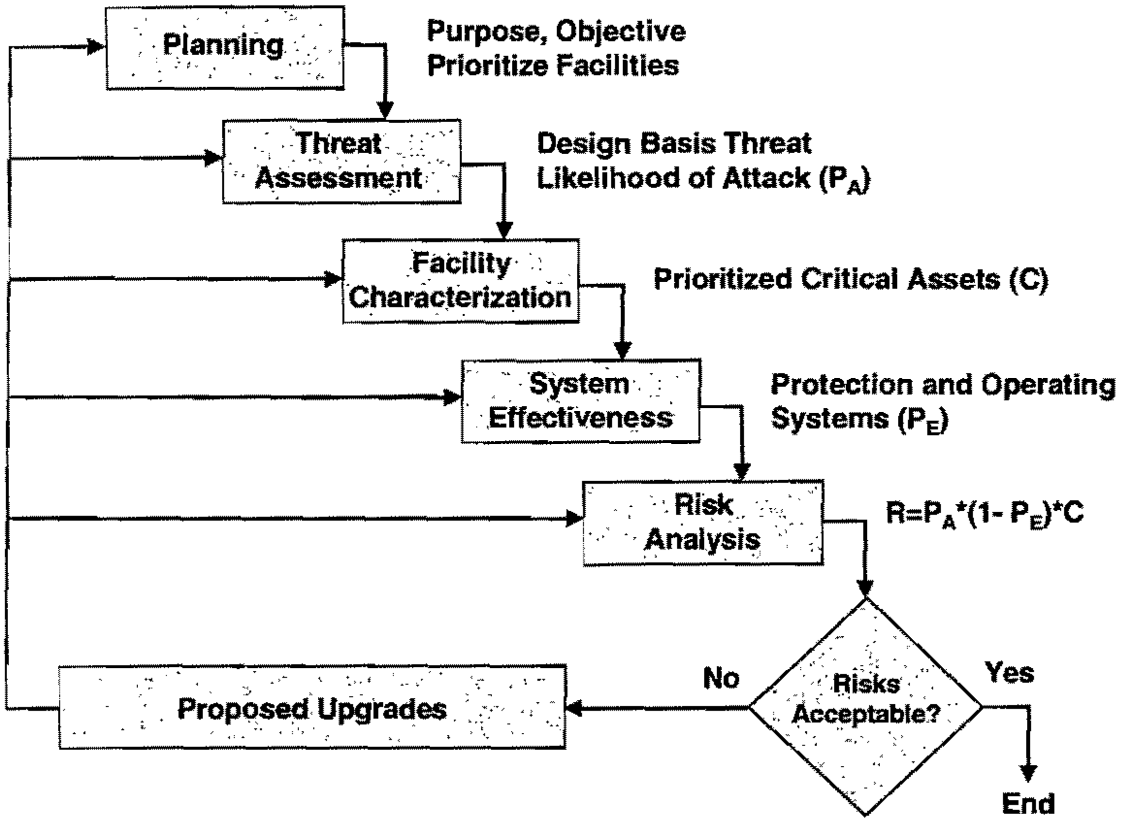


Figure 1.1. RAM-W^{SM} "Waterfall Flow Diagram"

How to collect information about the existing protection system is presented in Chapter 5. This chapter includes a description of the SCADA assessment methodology (the RAM-W^{SM} is an integration of both physical security and SCADA security) and a description of how to evaluate the risk of contamination from onsite chemicals. Chapter 6 describes physical protection systems in general and introduces the concepts of detection, delay, and response. Chapter 7 describes the System Effectiveness analysis process. The concepts of adversary strategy, adversary sequence diagrams, and scenarios and timelines (path analysis) are introduced. The path analysis tool is applied to understand how an adversary might attack the water utility and how effective the existing protection system (i.e., physical protection and operational design systems) is against that attack. In Chapter 7, after estimating the current system effectiveness, system vulnerabilities are identified. Chapter 8 uses the information collected and developed in all the previous chapters to perform a risk analysis that allows decision-makers to consider whether the identified risks are acceptable. Finally, if the risks are deemed unacceptable, Chapter 9 discusses steps that might be taken to reduce the risk and describes generic recommendations including "good business practices." Chapter 10 describes the organization and content of the final report. The appendices contain detailed information on examples, processes, worksheets, tools, etc., supporting the applicable chapter.

1.4.1 Risk Equation

Reducing risk can be accomplished by either increasing the effectiveness of the security system and/or operational system or by decreasing the consequences of an adversarial attack. A relative estimate of risk is calculated for each identified critical asset using the following risk equation:

$$R = P_A * (1 - P_E) * C$$

where: R = risk associated with the adversary attack

P_A = likelihood of the attack

P_E = probability the security system and/or the operational system (robustness) is effective against the attack

$(1 - P_E)$ = probability that the adversary attack is successful (also, the probability that the security system is not effective against the attack)

C = consequence of the loss from the attack.

It is important to recognize that in the RAM-W^{SM} application of this risk equation to water utilities, the variables are not true probabilities, but qualitative values expressed in terms of low, medium, and high. This is due to the lack of performance-based probability data currently available. As water utilities implement improvements to lower the risks from malevolent attack, testing data may become available to better quantify the variables. Initially in the analysis the assessment team will determine these qualitative values, and later define and substitute numerical values between 0 and 1 for the variables. This conversion to a numerical scale, however, is done only for aggregation purposes and ultimately does not have any more absolute quantitative meaning other than the three levels of high, medium, or low (there is no more granularity than the three levels of high, medium, or low). Note that the risk values that result from RAM-W^{SM} are relative versus absolute, because the parameters used to calculate risk (P_A, P_E, and C) are estimated and are based on engineering judgment and expert opinion. The comparison of risk on an asset-by-asset basis allows the water utility to clearly and systematically define and defend those its facilities or assets that present the greatest relative risk(s) to the overall mission. The ultimate goal should be to develop a balanced approach to understanding and managing risk.

1.5 Tools

This methodology makes extensive use of pairwise comparisons (screening tool), fault trees, consequence analysis, questionnaires, path analysis, and risk analysis. All tools and the associated examples have been specifically tailored for water utilities. However, the presentations in this report are generic and must be adapted to each specific water utility. All of the tools employed are discussed in either the body of the document or in the appendices. Many of the sections contain generic modules that may not apply to a specific water utility and thus can be eliminated at the outset. It is important to remember that this assessment provides a snapshot in time; the process must be revisited as threats change, facilities are upgraded, or operations are modified.

It is highly recommended that the assessment team and senior management be trained in the risk assessment methodology, and a security professional, trained and experienced in performance-based security system design and risk assessment, guide the team through the initial application of the process. As the assessment team is trained and becomes proficient at applying the process, they will be able to complete updates and analyze proposed system changes in the conceptual stage without significant guidance.

2 DECISIONS AND RISK

RAM-W^{SM} is a very systematic, thorough security risk assessment methodology designed to assist water utilities in making a determination about the risks from malevolent threats to the operations of a water utility. Along the way, many decisions will have to be made that will directly impact the final results. Decisions on the Design Basis Threat, the measures of consequence, and the priority mission objectives are difficult at best, but they are necessary to complete the assessment. There will always be adversaries beyond the capabilities of any water utility to defeat, so it's important to make improvements that bring the greatest returns.

Essentially, RAM-W^{SM} begins with a clear statement of the performance requirements desired by the water utility for the security program. The rest of the process then determines the ability of the system to meet those performance requirements. Through a systematic analysis, the DBT is defined, the undesired events are determined, and the critical assets are identified whose compromise can bring about those undesired events. The existing security system effectiveness is evaluated. Worst-case paths for the adversary to cause undesired events are postulated and analyzed. The vulnerabilities identified are then used as input to create balanced protection against malevolent attacks.

Once the information is collected, the risk analysis is performed to determine whether the performance requirements have been met. If the performance requirements have not been met, the choice has to be made to select more realistic requirements, mitigate consequences, or increase the effectiveness of the security system. It is important to remember that realistic system effectiveness can only be determined if the water utility has decided what level of threat it desires to defeat. The overarching decision that must be made by the water utility management is how much risk is acceptable and how much risk reduction is enough (Figure 2.1). The decision process to reduce risk starts with the water utility's mission objectives. Using the pairwise ranking of mission objectives, the water utility can address the operations showing the greatest risks that affect the most important mission objectives. For example, if public safety is the most important mission objective, then lowering the potential consequences from catastrophic release of chemicals may be the area of greatest risk and the first candidate to investigate. Using a priority ranking system allows the water utility to invest in risk reduction in a systematic manner in line with the mission objectives and provides clear documentation of the decision-making process.

Water utilities will always face a multitude of risks. Security is one more business risk that must be considered and addressed. The lack of historical data on high-consequence, low-probability events makes the analysis challenging and requires that hard decisions be made. How much is enough? That question will have to be answered by each individual water utility.

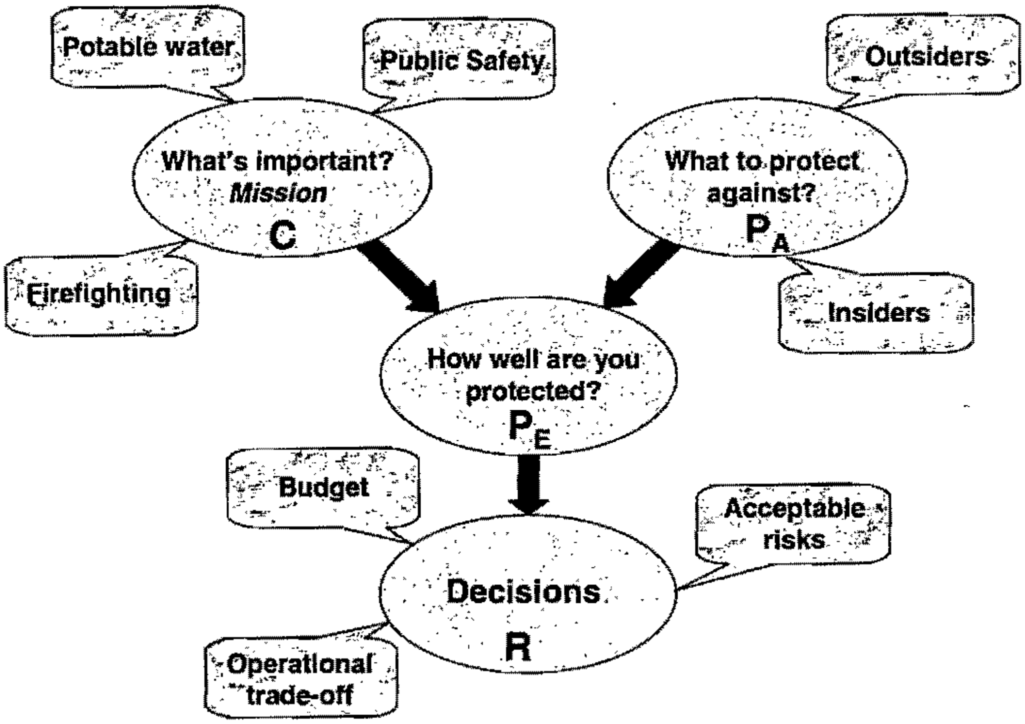
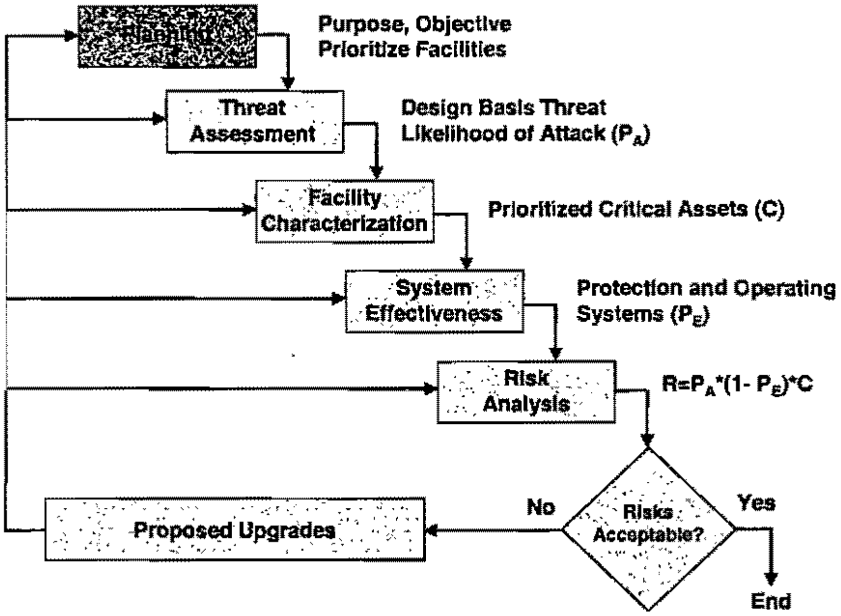


Figure 2.1. Decisions and Risk: How Much Is Enough?

3 PLANNING FOR SECURITY RISK ASSESSMENTS



Waterfall Flow Diagram – Process Locator

3.1 Management Roles and Responsibilities

Due to the interactive and iterative nature of the RAM-W^{SM}, certain responsibilities will be placed on the water utility management team. The methodology involves both an initial assessment phase and a long-term iteration phase. The initial assessment characterizes the current state of security risk for the water utility, and the long-term phase accommodates the dynamic nature of the threat as well as physical/operational changes to the water utility. The initial assessment is guided and analyzed by either an internal assessment team or an agency/contractor, but in the long term, the water utility's management must ensure that the process is effectively utilized, implemented, and maintained.

If the management of a water utility is to be effective in the pursuit of a secure operating environment, it must be willing to commit to and lead the necessary changes. As a part of this commitment, someone in the organization (i.e., senior management) must have the overall responsibility, authority, accountability, and ownership of security for the entire water utility. The individual(s) assigned the responsibility should be willing and able to take on the long-term iterative responsibility of the RAM-W^{SM}.

Management's input will be required to successfully complete the initial assessment phase of the RAM-W^{SM}. A team of water utility employees must be identified and assigned to participate in the process from start to finish. This assessment team should consist of at least one management-level representative, one or two highly experienced and knowledgeable senior staff members, a SCADA expert, and several operator-level employees. If existing water utility personnel do not have experience with risk management and security assessment, the assessment team should consider hiring or acquiring this expertise for the initial assessment phase. The entire assessment team should be provided with the opportunity to receive the RAM-W^{SM} training. It would be helpful for management to receive a high-level training session on the methodology as well.

The assessment team must complete several steps crucial to the process in the early stages of the assessment, including prioritization of mission objectives, mission-weighted prioritization of facilities, determination and characterization of the DBT, and the formulation of the consequence matrix. Water utility personnel also need to research and provide extensive system documentation and to facilitate coordination with other related local agencies (law enforcement, city government, etc.). It is highly recommended that the security assessment team secure the buy-in of the entire water utility management team on prioritization of the mission objectives, the mission-weighted prioritization of facilities, the consequence matrix, and the DBT before proceeding. This information is critical to the process and will drive the outcome of all the remaining steps.

In the final stages of the assessment, the water utility management will be presented with a comprehensive draft report that characterizes the risk spectrum. The draft report includes many tables, details, and recommendations that rank the relative risks currently faced by the water utility. This report should be reviewed by the appropriate management and staff and then critiqued for accuracy. This feedback is then incorporated into the final report.

The management team should oversee the development and implementation of an action plan based on the risks described in the final report. The implementation plan should also include a provision for the long-term iterative application of the RAM-W^{SM} process. Management must make several major decisions about the approach and risk mitigation philosophy prior to the development of the final implementation plan. These decisions center on a trade-off analysis between various constraints including:

- The implementation schedule and priorities,
- Operational constraints,

- Aesthetic constraints,
- The risk exposure comfort level,
- The resources available to achieve the desired results, and
- Costs of any upgrades to the system.

A critical part of the methodology will require the assessment team to look for ways that an adversary could exploit the assets of the water utility to cause a Weapons of Mass Destruction (WMD)–type event. Examples of these WMD-type events include flooding or hazardous release of water treatment chemicals. The ability of the adversary to cause high numbers of deaths and injuries to the public and how this might be accomplished should be fully understood by the water utility. Management of the water utility should be made fully aware of the consequences of these types of events and consider actions to reduce the risks associated with them before considering other risk reduction measures.

Because the consequences are so high, WMD-type events should be considered at threat levels even beyond the DBT (i.e., the threat level management decides the system should protect against). While it may not be possible to protect against or mitigate such an event, the water utility management must still recognize the risk. Such situations may generate concerns beyond the sole responsibility of the water utility. For example, if reliable intelligence were obtained on a potential adversary planning to cause a WMD-type event at a water utility, extreme emergency measures such as posting of the National Guard may be necessary until the threat-level changes or until the water utility can effect a change in operations to eliminate or minimize the event.

3.2 PROJECT MANAGEMENT

A security risk analysis undertaken for a water utility is a limited-time project. Using project planning concepts to plan the analysis will provide a great deal of assistance to the project leader and the assessment team by ensuring that essential work is conducted and management's requirements and expectations are met. Planning is an important part of a successful analysis, but the amount of time and resources the assessment team spends will depend on the size and complexity of the analysis and the complexity of the water utility itself. Sufficient time spent up-front determining management's expectations is a requirement for a successful analysis. Appendix B describes some basic project management concepts for planning and conducting a security risk assessment. Appendix B also provides estimated times for completion of each step of the process.

3.2.1 Assessment Team Selection

As noted in Section 3.1, several individuals with differing skills and knowledge of the water utility form the optimal assessment team to successfully complete the security risk assessment (see Appendix B for greater detail). Because it is important to understand how requirements are actually implemented, versus how some might perceive the requirements to be implemented, the assessment team must cut across all levels within the organization. Understanding the nuances and numbers of employees on site during different shifts, on weekends and holidays, as well as how the water utility controls the access of visitors, contractors, and vendors, are all very important. The team may want to consider including personnel from interdependencies (e.g., wholesalers, power utilities, etc.).

It is suggested that the assessment team oversee the entire process through the completion of the recommended upgrades. Individuals selected for the assessment team will identify and understand vulnerabilities within the system; therefore, management must be comfortable with the assessment team members possessing this sensitive information.

The assessment team must ensure that information gathered from employees and contractors during interviews is protected and that no retribution occurs against anyone participating in the process. In order to gather credible data and information, employees and contractors should feel comfortable in describing actual vulnerabilities that exist. It is crucial that information on actual operations be gathered because security is dependent on policies and procedures as well as technology. Through experience with multiple water utility assessments, it has been found that employees often have knowledge of critical vulnerabilities that may not be obvious to others.

The assessment team will gather sensitive information throughout the process. A document control plan should be developed and approved for how to control all documentation gathered and generated. The following issues should be addressed:

- Distribution of plans, operational data, and other descriptive material.
- Distribution of all documents created in association with the assessment.
- Marking of all documentation including numbering, stamping, and assigning responsibility.

- Review of State Freedom of Information Act (Sunshine Laws) to avoid having to publicly disclose sensitive information.
- Approval by appropriate legal authorities of the document control plan.
- Level of access to the information granted to contractors and the types of information they may access.
- Control of all information including transmission, copying, locking up (controlling), and ultimately disposing.
- Control of all SCADA documentation including network diagrams, configuration procedures, access control lists, etc.

The final report will explicitly detail major vulnerabilities and the associated consequences if compromised and should be carefully controlled. Another item for the assessment team to discuss is whether or not to make sensitive information available to third parties that may work closely with the water utility. This would include contract guard services, maintenance contractors, vendors, etc. Levels of information protection and access should be determined for all third party services.

The RAM-W^{SM} process requires certain steps to be completed in order. Assumptions and decisions made at every major step of the process need to be communicated, agreed to, and documented. This documentation is required input in later stages of the assessment. When the final results are determined, a complete, logical document trail leading to the final results and recommendations should exist.

3.2.2 Document Facility Operations

Understanding and documenting the operations of the water utility is one of the first activities the assessment team will undertake. The following is a partial list of facility operations that should be described and documented; this list will change depending on the assets of the water utility:

- Population served including a list of critical and noncritical customers,
- Inventory of hazardous chemicals,
- Process diagrams of the entire operation,
- High and low demand water delivery rates for all major systems and subsystems,

- Description of all water sources, treatment facilities, pumping stations, storage facilities, and the distribution system,
- SCADA system description,
- Security system diagrams,
- Interdependencies (e.g., electrical, SCADA, wholesalers, etc.),
- Other as necessary.

The goal is to create an inventory of the major facilities and assets of the water utility. This information will be used in Section 3.4 to prioritize the facilities for security risk assessment.

3.3 Define and Prioritize Mission Objectives

Before proceeding with the next step of the process, it is important for the assessment team to identify the water utility's mission objectives. The mission objectives will be used in several parts of the assessment and later in risk analysis and risk reduction. First, the mission objectives will be prioritized to understand the most critical function(s) of the water utility. This will help focus on which assets to assess and will be an important consideration when the risk reduction goals are being developed. The initial risk reduction efforts should begin with those necessary to support the most important mission objective. This will help the water utility receive the greatest return for its security investment. The mission objectives might include all or some subset of:

- Supply potable water
- Distribute water
- Ensure public safety
- Treat water for consumption
- Provide adequate water supply for fire protection

Next, the prioritized mission objectives will be used as weighting factors to determine the critical facilities and/or assets within the water utility. Budgetary constraints will prevent the water utility from lowering risk everywhere in the operation at once, so prioritizing the facilities helps determine where to begin. Section 3.4 describes the pairwise comparison process and provides a completed example.

3.4 Screening (Facility Prioritization)

An important step in RAM-W^{SM} is the screening/prioritization process. A pairwise comparison tool allows water utilities to prioritize the myriad facilities that may be spread over a large geographical area. The assessment team starts by reviewing a process diagram of the entire water utility. The goal is to determine the critical facilities (assets) from a high-level perspective. Facilities to include would be major treatment plants, major pump stations (both before and after treatment), major storage facilities, critical wells, critical pipelines, and critical reservoirs. The goal is *not* to create a 1 through *n*th priority ranking, but rather to understand which facilities are essential to water system operation. It is an attempt to determine the absolute minimum number of facilities that must remain operational to ensure the water utility's mission objectives are achieved.

For large, complex water utilities, the assessment team may want to consider using "tiers" of assets during the facility prioritization. Placing all the assets into one pairwise comparison matrix can become difficult due to the large number of assets. Lower-level of importance assets will generally be rated low and may be overlooked. A pairwise comparison for each "tier" of water utility assets could be done to identify which facilities within each tier group are most critical to the mission. For example, a large water treatment facility that supplies a large percent of the treated water for the entire water utility will generally rank much higher than a small finished water storage tank out in the distribution system.

Using tiers of assets allows for easier accounting and also facilitates grouping of like assets. Separating facilities through a tiered approach will keep the smaller facilities from being completely overshadowed during the pairwise comparison and thus allow the assessment team to clearly identify which facilities in each tier are most critical. Continuing the example from the previous paragraph, grouping all the storage tanks in the distribution system is a natural pairing and allows comparison of like assets. The assessment team can then easily determine which storage tanks are more critical than others. All this analysis can be accomplished via one matrix, but accounting for all the pairwise comparisons can be tedious and may not add much value.

The facility prioritization step is important for another reason. This step allows the water utility to assess the operations from a "systems" perspective. The remaining sections of the methodology will look at successively lower levels of detail, but this step helps the assessment team understand the big picture. Important questions should be asked at this point such as:

1. What is the minimum flow required in an emergency situation?
2. If more than one source exists, what is the minimum number that must remain operational to meet the water utility mission objectives?
3. Are there redundant paths to treat or deliver water, and if so, how many are absolutely necessary?
4. Are some paths through the operation more exposed than others?
5. Are some paths more important than others?
6. Are there critical customers?
7. What is the minimum flow required for critical customers?
8. Are there single points of failure?

The assessment team should understand the big picture before proceeding to lower levels of detail. Through the pairwise comparison, the assessment team might decide **not** to include some less than critical facilities/assets for further analysis. For example, a systems analysis might point to the fact that the water utility primarily relies on surface water, but has a few wells for peak demands during the summer months. The wells have very limited capability and investing security dollars to protect them would result in very little risk reduction. The assessment team might only review the wells to ensure that reasonable steps have been taken to protect those assets and also to ensure that they were screened for WMD-type events. At that point, the assessment team might decide not to consider the wells any further in the analysis.

This is the type of information that can be gleaned from the facility prioritization. The prioritization will help the assessment team focus on those parts of the operation that must be functional for the water utility to meet the mission objectives. The facility prioritization information will be used to help prioritize risk reduction measures and will be used as a starting point in the fault tree analysis. The fault trees, described in Section 5.4, are developed to describe the entire system, at least at a high level. The fault trees will help identify any potential WMD-type events and critical assets at the water utility that did not come out of the facility prioritization. If any potential WMD-type events are found, they should be included in the analysis. Also, the fault tree can be developed in more detail wherever necessary, allowing for more in-depth analysis than the facility prioritization.

To prioritize the major facilities, a simplified pairwise comparison is used. Two or more facilities are compared using stated criteria (based on the mission objectives) in a structured way, resulting in a relative ranking of the facilities. The facilities are ranked in the context of each criterion using a comparison scale described in detail in Appendix C. In the following section, an example water utility is introduced, which will be used throughout this document, and a pairwise comparison completed.

3.4.1 Example Water Utility

The following example water utility will be used throughout this document to illustrate key concepts and points. A detailed description of the water utility is given in Appendix A. The water utility serves a population of 250,000 people. This is a surface and ground water utility. There are three water treatment facilities (Figure 3.1), two with integral pump stations and storage. One treatment facility is fed by wells. There are two major pump stations in addition to the two integral pump stations at the treatment plants.

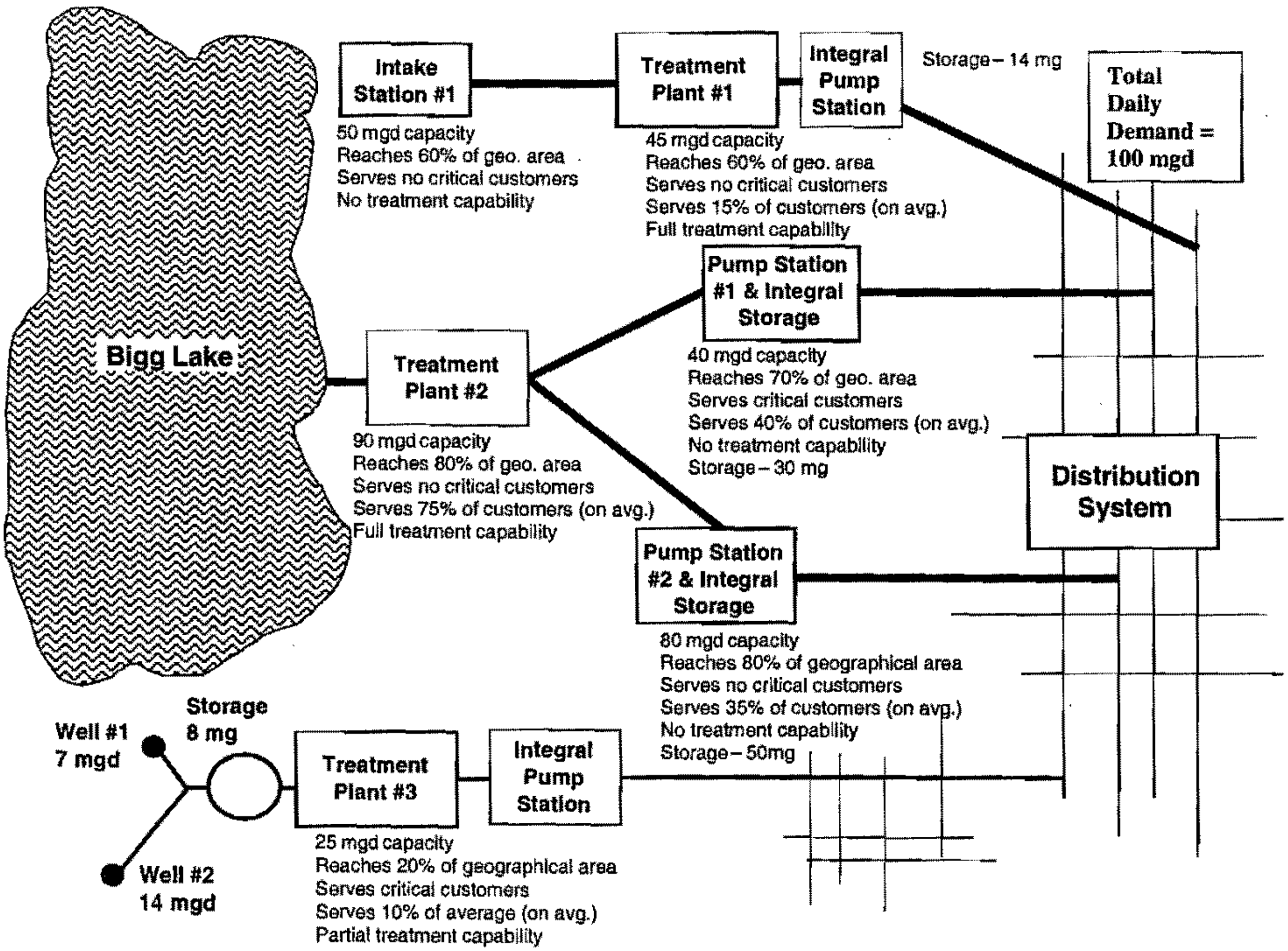

Bigg Lake
Intake Station #1
50 mgd capacity
Reaches 60% of geo. area
Serves no critical customers
No treatment capability
Treatment Plant #1
45 mgd capacity
Reaches 60% of geo. area
Serves no critical customers
Serves 15% of customers (on avg.)
Full treatment capability
Integral Pump Station
Storage – 14 mg
Total Daily Demand = 100 mgd
Treatment Plant #2
90 mgd capacity
Reaches 80% of geo. area
Serves no critical customers
Serves 75% of customers (on avg.)
Full treatment capability
Pump Station #1 & Integral Storage
40 mgd capacity
Reaches 70% of geo. area
Serves critical customers
Serves 40% of customers (on avg.)
No treatment capability
Storage – 30 mg
Distribution System
Pump Station #2 & Integral Storage
80 mgd capacity
Reaches 80% of geographical area
Serves no critical customers
Serves 35% of customers (on avg.)
No treatment capability
Storage – 50mg
Well #1
7 mgd
Well #2
14 mgd
Storage
8 mg
Treatment Plant #3
25 mgd capacity
Reaches 20% of geographical area
Serves critical customers
Serves 10% of average (on avg.)
Partial treatment capability
Integral Pump Station

Figure 3.1. Example Water Utility

3.4.2 Screening (Facility Prioritization) for Example Water Utility

For the example water utility four main mission objectives were identified (see Appendix C for more details):

1. Provide sufficient fire-fighting flows (**capacity**)
2. Serve (**critical customers**)
3. Greatest geographical service possible (**geographical extent**)
4. Provide potable water (**water quality**)

These mission objectives are placed into a pairwise matrix and compared against one another. The pairwise criteria for comparison are shown in Table 3.1.

Table 3.1. Values for Ranking Criteria in Pairwise Comparison

Importance of Item One Relative to Item Two	Importance of Item Two Relative to Item One
much greater than (5)	much lower than (1)
greater than (4)	lower than (2)
the same as (3)	the same as (3)
lower than (2)	greater than (4)
much lower than (1)	much greater than (5)

The outcome of the analysis for the example water utility is shown in Table 3.2. Further details of the pairwise process and the final outcomes are contained in Appendix C.

Table 3.2. Mission Objective Comparison for the Example Water Utility System

Mission Objective Comparison	Capacity	Geographical Extent	Critical Customers	Water Quality	Sum
Capacity	■	4	5	4	13
Geographical Extent	2	■	3	4	9
Critical Customers	1	3	■	4	8
Water Quality	2	2	2	■	6

As can be noted in Table 3.2, the most important mission objective for the example water utility is to provide sufficient fire protection (capacity), followed by the ability to reach the greatest geographical extent. Service to critical customers is ranked third. Finally, water quality ranks lowest. The rankings in Table 3.2 are then used to complete a pairwise comparison of the major components (i.e., facilities) of the water system.

For the example, water utility the assessment team decided to include the following major facilities in the pairwise comparison:

- Treatment Plant 1
- Treatment Plant 2
- Treatment Plant 3
- Pump Station 1
- Pump Station 2

To begin the process of prioritizing the facilities, the facilities are compared for each of the criteria (mission objectives). A separate matrix is used for each criterion (see Appendix C for the complete pairwise comparison). For the example water utility, the criterion of "capacity" was used to compare the facilities (Table 3.3).

3.4.2 Screening (Facility Prioritization) for Example Water Utility

For the example water utility four main mission objectives were identified (see Appendix C for more details):

1. Provide sufficient fire-fighting flows (**capacity**)
2. Serve (**critical customers**)
3. Greatest geographical service possible (**geographical extent**)
4. Provide potable water (**water quality**)

These mission objectives are placed into a pairwise matrix and compared against one another. The pairwise criteria for comparison are shown in Table 3.1.

Table 3.1. Values for Ranking Criteria in Pairwise Comparison

Importance of Item One Relative to Item Two	Importance of Item Two Relative to Item One
much greater than (5)	much lower than (1)
greater than (4)	lower than (2)
the same as (3)	the same as (3)
lower than (2)	greater than (4)
much lower than (1)	much greater than (5)

The outcome of the analysis for the example water utility is shown in Table 3.2. Further details of the pairwise process and the final outcomes are contained in Appendix C.

Table 3.2. Mission Objective Comparison for the Example Water Utility System

Mission Objective Comparison	Capacity	Geographical Extent	Critical Customers	Water Quality	Sum
Capacity		4	5	4	13
Geographical Extent	2		3	4	9
Critical Customers	1	3		4	8
Water Quality	2	2	2		6

As can be noted in Table 3.2, the most important mission objective for the example water utility is to provide sufficient fire protection (capacity), followed by the ability to reach the greatest geographical extent. Service to critical customers is ranked third. Finally, water quality ranks lowest. The rankings in Table 3.2 are then used to complete a pairwise comparison of the major components (i.e., facilities) of the water system.

For the example, water utility the assessment team decided to include the following major facilities in the pairwise comparison:

- Treatment Plant 1
- Treatment Plant 2
- Treatment Plant 3
- Pump Station 1
- Pump Station 2

To begin the process of prioritizing the facilities, the facilities are compared for each of the criteria (mission objectives). A separate matrix is used for each criterion (see Appendix C for the complete pairwise comparison). For the example water utility, the criterion of "capacity" was used to compare the facilities (Table 3.3).

Table 3.3. Facility Comparison – Example Water Utility (Criterion "Capacity")

Facility Comparison (Criterion = Capacity)	Treatment Plant #1	Treatment Plant #2	Treatment Plant #3	Pump Station #1	Pump Station #2	Sum	Weighted Number (Criteria Sum X Sum)
Treatment Plant #1		1	5	3	2	11	143
Treatment Plant #2	5		5	4	3	17	221
Treatment Plant #3	1	1		1	1	4	52
Pump Station #1	3	2	5		2	12	156
Pump Station #2	4	3	5	4		16	208

Based on the criterion of capacity, Treatment Plant 2 is ranked the highest. The Weighted Number for a facility is arrived at by multiplying the sum for that facility by the sum for that criterion (see Table 3.3). In this example, Treatment Plant No. 1 has a sum of 11, which is multiplied by 13, the sum for the criterion Capacity, which results in a Weighted Number of 143. The final ranking based on all the criteria is shown in Table 3.4.

Table 3.4. Facility Comparison for the Example Water Utility (All Criteria)

Facility Comparison Based on all Criteria	Capacity	Geographical Extent	Critical Customers	Water Quality	Sum	Rank
Treatment Plant #1	143	99	80	108	430	3
Treatment Plant #2	221	144	80	108	553	1
Treatment Plant #3	52	27	160	84	323	5
Pump Station #1	156	117	80	30	383	4
Pump Station #2	208	153	80	30	471	2

Once the prioritized list of facilities is completed, the assessment team should determine how far down the list to go with the initial security risk assessment based on available resources and management input. As assessments and upgrades are completed at the most important facilities, the assessment process will continue down the prioritized list. A trade-off analysis should be completed as the assessment team moves down the list to determine whether to continue making upgrades at a particular facility or to consider the next facility on the list. Each new project should be the highest priority determined by the security risk assessment. Some minimum level of security will most likely be undertaken at all facilities, so following a prioritized process does not mean that lower consequence facilities are simply ignored.

3.5 DEFINING RISK REDUCTION GOALS

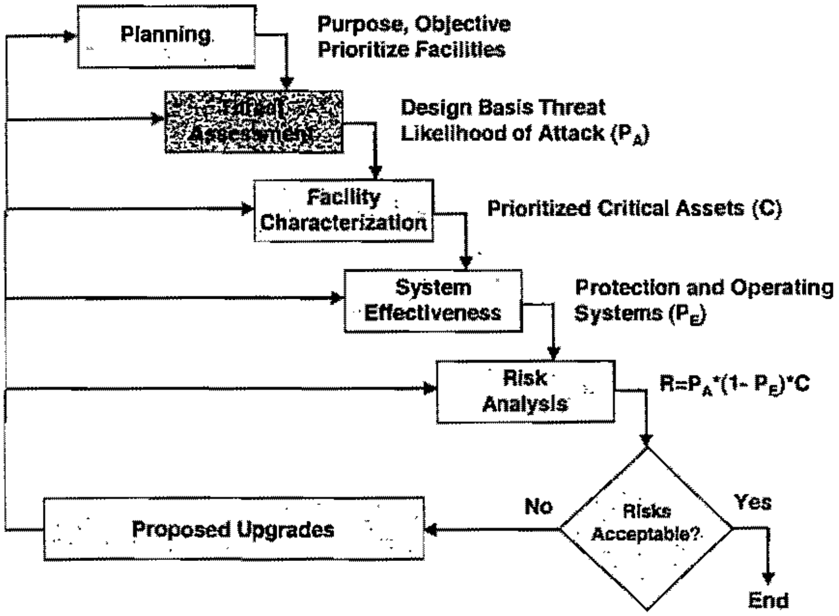
RAM-W^{SM} provides a systematic structure to estimate relative levels of risk due to malevolent threats. This information will be used for decision-making in implementing system upgrades to reduce risks deemed unacceptable to the water utility. Early on, the assessment team should discuss and document the goals for the upgraded security system. The protection goal(s) may be to:

1. Deter the adversary.
2. Prevent the adversary from causing undesired event(s) (i.e., disrupting the mission objectives).
3. Detect the adversary and mitigate the consequences of the attack.
4. Protect employees.
5. Collect information for later prosecution.
6. Increase redundancy in the operations.
7. Eliminate single-points-of-failure in the system.

Note that only Goals 2, 3, 4, 6, and 7 actually reduce the risk value by either increasing protection system effectiveness or reducing consequences in the risk equation. Goal 5 may reduce risk in the future by reducing the incidence, but this likelihood is difficult to predict and measure. Deterrents may work, but the ability to lower the risk is unknown and hard to quantify without the event actually happening.

Each increased level of protection has an associated cost; therefore, protection goals may be resource-constrained. It is important to be specific and refer to the defined goals throughout the security risk assessment process, particularly when discussing upgrades. The assessment team must constantly review the protection goals of the assessment. To reduce the risk, it is strongly recommended to improve the system effectiveness and/or design consequence mitigation measures that will stop an adversary from achieving his/her objective (i.e., prevent the undesired event) with a high likelihood of success. Each water utility will need to decide where to set the bar for preventing undesired events.

4 UNDERSTANDING THE THREAT



Waterfall Flow Diagram – Process Locator

4.1 Threat Assessment

A threat assessment helps identify and describe the types of adversaries (malevolent persons or groups) that may try to prevent a water utility from performing one or more of its mission objectives. This chapter provides guidance that can be used to develop a definition of threat, known as the Design Basis Threat or DBT, for a water utility. The choice of DBT is an important part of the assessment as it drives the determination of critical assets during the risk analysis. The DBT, which is comprised of the numbers of adversaries, their capabilities, and their tools, should be carefully researched and discussed before undertaking the assessment. Choosing an unrealistically high DBT will result in high risks throughout the system and will not show any discrimination in the importance of various assets. Conversely, choosing an unrealistically low DBT will simply show little or no risk to the water utility. During the risk analysis, the existing security and/or operation systems are evaluated to determine their effectiveness at defeating the DBT.

Collecting threat information, organizing it, evaluating it, and using it to determine which threat a particular water utility may encounter forms the basis of the threat assessment. This threat information will also be used to develop adversary strategies and scenarios.

4.2 DESIGN BASIS THREAT

To begin, the assessment team will want to consider all potential threat levels (e.g., mischievous vandals up to sophisticated terrorists)—even those considered "outside the box." The assessment team must acknowledge that extremely high threat levels exist and there is little the water utility can do to defeat these threats. However, it is strongly recommended that the water utility complete the assessment with a terrorist-level threat to understand system vulnerabilities due to high-level threats. Only considering lower-level threats may result in exclusion of high-consequence targets that could have devastating impacts to the water utility if compromised. After gathering information on all potential threats the assessment team begins to develop the conceptual threat (Figure 4.1). This is the threat level that the water utility would ideally like its system to defeat if there were no constraints. The next step in the Threat assessment involves reviewing operational (safety, legal, etc.) constraints during the site characterization phase, and their impact on the ability of the water utility to lower risk. The conceptual threat is then modified based on these constraints. This will likely be an iterative process, as the assessment team will be working with incomplete information until the risk analysis is finished. Some of the constraints will not be fully understood until critical assets are identified and attempts are made to lower risk. When the analysis is complete (See Figure 4.1), the water utility may discover that they only have resources to design against a very low threat level. Ultimately, the DBT is a management decision and may or may not reflect threat information collected. This in no way diminishes the importance of gathering threat information, but recognizes that real constraints may prevent the water utility from achieving the level of security desired.

The DBT is the maximum **credible** threat to which a water utility will design its security and operational systems. Once established, the DBT should be protected as sensitive information, approved by management, reviewed periodically, and updated as necessary. Figure 4.1 demonstrates the iterative nature of the DBT development that occurs throughout the assessment.

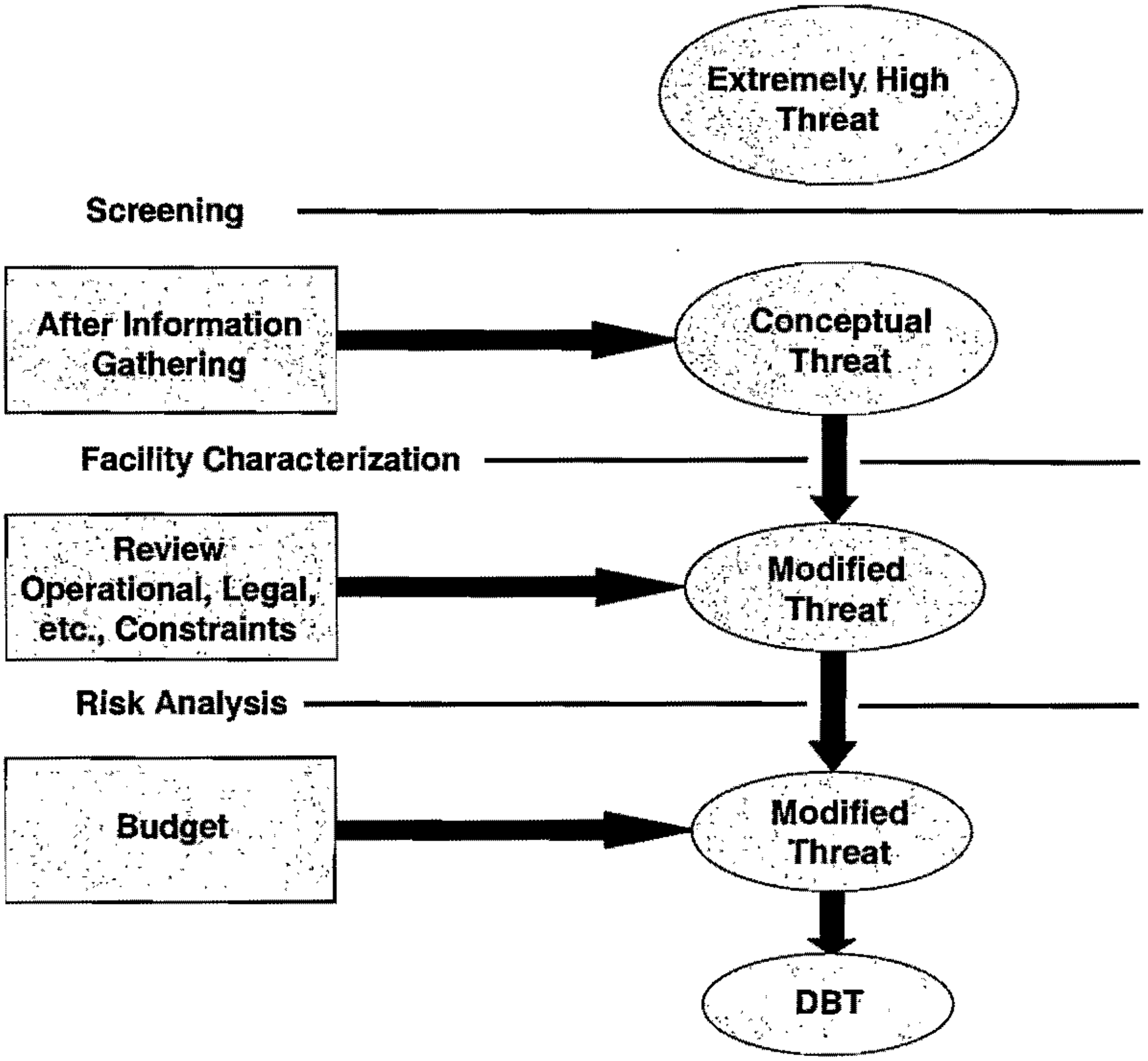


Figure 4.1. Screening Process for Developing the DBT

4.3 CATEGORIES OF ADVERSARIES

Before time is spent collecting information, it is important to decide what kind of data is needed to complete a definition of threat for a water utility. Generic descriptions of potential insider and outsider adversaries are listed below. In the next few sections, additional information is provided about the types of adversaries that the water utility may want to consider as the DBT is developed.

4.3.1 Categories of Outsiders

Listed below are broad categories of outsider adversaries:

- Vandals
- Protesters
  - Demonstrators
  - Activists
  - Extremists
- Terrorists
- Criminals
- Computer hackers

Vandals generally intend to damage or steal property, but are not motivated to risk their lives or gather intelligence data about the water utility operations. The protestor group has different kinds of people with different motivations, most of whom are no threat to the water utility. The largest percentage of protesters is the demonstrators—these are well-meaning people who are generally led into the protest by leaders with specific agendas. The activists will generally use force and do some active thing to cause physical damage. The innermost group may be a hard-core group of extremists whose intention is to stop critical operations to which they object. They tend to be well trained and well supported, and may be armed with weapons and explosives. Terrorists are often well funded and well trained, and they may be willing to die for their cause. They may spend a significant amount of time studying the operations of a potential target before executing an attack. Criminals tend to work in small groups (usually one). The cyber hacker and other levels of cyber threats will be addressed in Section 4.6. When developing the threat, collusion must also be considered—the outside adversary working with an insider (who can assume either a passive or active role).

4.3.2 Categories of Insiders

Listed below are broad categories of insider adversaries:

- Betrayal (criminal)
- Revenge
- Abnormal behavior (psychotics)
- Terrorist insider
- Coercion

The criminal betrays the trust shown by the water utility by hiring him/her and allowing unescorted access. Revenge is a situation in which an employee or contractor causes damage because he/she is angry about something. Psychotics are people who simply do not know right from wrong. The terrorist insider intentionally gets hired by the water utility in order to build trust and get access to inside operations. Coercion occurs when an employee or contractor is forced into causing damage (e.g., family members are held hostage, blackmail, etc.).

4.3.3 Contamination Threat

The contamination threat is a difficult issue to assess due to the large number of scenarios that could be postulated. The EPA, in its guidance document available to water utilities (not publicly available) through the water Information Sharing and Analysis Center (ISAC), describes this threat in some detail (see <www.amwa.net> for information on the ISAC). Additionally, the EPA, in cooperation with the Centers for Disease Control, Sandia, industry associations, and others, created a State of the Knowledge document (controlled) to understand the range of contaminants and their possible uses. Literally thousands of chemicals, biological agents, and radiological agents are available to the adversary. Many of them would not be a threat to the water supply for a variety of reasons. However, depending on the capabilities of the DBT, the potential exists to contaminate even the largest water utility system. Each water utility will have to decide how far to pursue the contaminant analysis. Unfortunately, for many of the agents that could be used, testing data are not available to characterize the threat.

In their guidance document, the EPA recommends using existing measurement techniques (Total Organic Carbon, Chlorine Residual, etc.) to monitor the quality of the water throughout the system. This will help detect some of the potential contaminants, but information is available that suggests they will miss several that are of concern. Real-time monitoring equipment that will provide timely warning does not exist and will not likely exist for many years. Without timely detection, the water utility will probably be unaware of an intentional contamination event.

During the security risk assessment, the assessment team should evaluate the potential for intentional contamination throughout the system. If the water source is very large, it is unlikely that chemicals could be used as a contaminant due to the large amounts required. However, some of the biological agents might still be of concern. Effective filtering, disinfection, and advanced treatment techniques such as ultraviolet light and ozonation will greatly lower the risk from biological agents. Different types of treatment processes provide varying levels of protection against certain classes of contaminants. See the guidance document referenced above for further detail. The assessment team may decide that upstream from the treatment facilities would be a low risk, depending on the size of the water demand and the types of treatment employed. Post treatment is obviously a more vulnerable location. Most water utilities of any size have thousands of access points into the distribution system that an adversary could potentially exploit. This is a high-risk part of the operation and will likely stay at that level for the foreseeable future. Water utilities should take appropriate action to secure the parts of the distribution system that provide easy access for an adversary, especially storage reservoirs, as they provide an atmospheric pressure water surface.

Modeling and simulation efforts under way to understand contaminant fate and transport in the distribution system indicate the risk of human effects due to a contamination event could be lowered with early warning systems, but will never reach levels the public will accept. The number of instruments required and the ability to immediately react are both barriers to effectively deal with contamination. See the Congressional Testimony from Jeffrey J. Danneels, Sandia National Laboratories, for additional thoughts on how to lower the risk from intentional contamination. The November 14, 2001, testimony is available at <www.sandia.gov/news-center/resources/congress-testimony/index.html>.

4.4 INFORMATION GATHERING

To determine the levels of threat that might exist, information can be sought for regional, national, and international threats. The extent of the effort is dependent on the mission and location of the water utility. Ideally, an assessment team member with a law-enforcement background will have the primary responsibility for gathering and organizing information about individuals or groups that might pose a threat to the water utility. Threat information is acquired by interviewing employees, managers, and law enforcement agencies, and by performing literature searches. Trends or indications that the level of threat may increase in the future (e.g., increasing dissatisfaction with the union/management relationship) should be noted.

Sources to be searched include:

- Incident reports, unusual occurrence reports, criminal reports, intelligence reports, and other historical data associated with water utilities or similar operations.
- Employee data on union disputes, employee conflicts/violence, expressed threats, etc.
- Internet, industry associations, professional journals, or other sources of data.
- Government directives and legislation.

Groups to be contacted include:

- Local law enforcement
- State/regional law enforcement
- Local/state offices of emergency management
- Local/state offices of counter-terrorism
- Federal law enforcement (Federal Bureau of Investigation)
- Local Infraguard
- EPA Water Security Task Force (developed and made available guidance on various types of threat)
- Industry associations such as AwwaRF (compiled information on past security incidents at water utilities)
- Water Information Sharing and Analysis Center, operated by AMWA (to start operations at the end of 2002), database on threats and security incidents
- Department of Homeland Security

4.5 Threat Attributes

Tables 4.1 through 4.3 in this chapter, describe what information to collect about outsider and insider threat attributes and provide an integrated example for the example water utility. As the various parts of the water utility are being reviewed, the ability of the adversary to damage and/or destroy assets is dependent on the attributes captured during the threat assessment.

4.5.1 Outsider Threat Attributes

When considering the outsider the following list of attributes will help to define the threat:

- Incidents (historical)
- Targeting
- Motivation
- Expected number
- Tactics (force, stealth, or deceit)
- Equipment
- Weapons
- Explosives
- Transportation
- Intelligence gathering means
- Technical skills and knowledge
- Financial resources and sources
- Potential for collusion with insider

Historically speaking, the hardest attribute to agree upon is the "expected number." As the assessment team deliberates they will have to define each threat category based on these attributes. Table 4.1 is a water system threat analysis worksheet completed for the example water utility (Appendix A) and is based on a terrorist-type threat. The worksheet lists the type of information required to describe the outsider threat. This information will later be used to develop adversary strategies and scenarios and evaluate system effectiveness for these scenarios.

In Appendix D several outsider examples are included for consideration. In addition, definitions for the low, medium, high, and very high outsider threats are presented. These examples are the starting point for a threat assessment and will require further development by the assessment team.

Table 4.1. Completed Water System Outsider Threat Analysis Worksheet for the Example Water Utility

WATER SYSTEM OUTSIDER THREAT ANALYSIS WORKSHEET	
Utility: Example Water Utility	
Date: May 15, 2002	Recorded by: I. Drinkwater
Adversary: Terrorist	Is this a continuation sheet: □ Yes ☒ No
Information Category	**Description**
1. Incidents (historical)	International, none in the US
2. Has the adversary targeted the water utility or a similar (nearby) facility?	No (but FBI information exists for a potential occurrence)
3. Motivation (Ideological, economic, or personal)	Ideological
4. Expected number of adversaries	3
5. Tactics	Destruction of assets to disrupt water
6. Equipment	Power tools, hand tools, bolt cutter
7. Weapons	Handguns, small automatics
8. Explosives	Explosives (5 lb or less)
9. Transportation	Car/truck, 4 x 4, ATVs
10. Intelligence gathering means	Websites, publications, public literature, might have taken tour of facility
11. Technical skills and knowledge	Limited knowledge of security system and water processing facility, some cyber capabilities
12. Financial resources	Well funded
13. Potential for collusion with insider	Potential exists (no background checks conducted on employees)

The assessment team will complete this worksheet for **each** potential category of outsider adversary (see Appendix D for a blank form of the worksheet). This is the kind of information that the assessment team will collect, organize, and analyze so that it can make an informed decision about the outsider threat.

4.5.2 Insider Threat Attributes

When considering the insider the following list of attributes will help to define the threat:

- Identify insider positions (i.e., positions, not people)
- Potential for active or passive role
- Access to critical assets (including the SCADA system)
- Access to security system

Identifying the potential insider threats of concern is accomplished by systematically evaluating the access to critical assets of each position (e.g., the guards, the maintenance people, the plant manager, the mechanical operator, SCADA administrator, etc.) within the water utility. These positions may be grouped together as many of the employees have the same level of access authority. This process requires the assessment team to list the types of positions (not individual people) that have access to critical facilities and assets. Each of the positions that have unique access authority will have to be evaluated based on all the attributes. A passive insider will only give information (e.g., operational, security, utility maps, etc.), whereas an active insider will actively participate somehow in the attack (they could be violent or non-violent). For example, an active insider will open a valve, door, or gate, cut a wire, place explosives, plant weapons, etc. Table 4.2 lists the types of insider positions at the facility and summarizes part of the information needed to address the capabilities of the insider threat. Table 4.3 lists the type of information required to describe the insider. Both these tables are completed for the example water utility (Appendix A). The worksheet in Table 4.3 is specifically completed for the Control Room Operator as a potential insider threat.

Table 4.2. Example of a Completed Water System Insider Threat Analysis Worksheet—Part 1 for the Example Water Utility

WATER SYSTEM INSIDER THREAT ANALYSIS WORKSHEET–PART 1	
Utility: Example Water Utility	
Date: May 15, 2002	Recorded by: I. Drinkwater
Adversary: Insider	Is this a continuation sheet: □ Yes ☒ No
List insider positions of concern: • Plant Manager • Control Room Operators • Maintenance Technician • SCADA Administrator • Etc.	
To complete the section below, indicate the potential of frequency for each insider position with the following qualitative indicators: Never, Occasionally, Often	

Insider Position	***Access to Critical Facilities***	***Access to Security System***	***Access to SCADA System***
Plant Manager	Oft	Occ	Occ
Control Room Operator	Oft	Oft	Oft
Maintenance Technician	Oft	Occ	Nev
SCADA Administrator	Occ	Oft	Oft

Based on the information for the example water utility, the next form collects more detailed information and in this case is filled out for a Control Room Operator (refer to Appendix A).

Table 4.3. Example of a Completed Water System Insider Threat Analysis Worksheet—Part 2 for the Example Water Utility

WATER SYSTEM INSIDER THREAT ANALYSIS WORKSHEET–PART 2	
Utility: Example Water Utility	
Date: May 15, 2002	Recorded by: I. Drinkwater
Adversary: Control Room Operator	Is this a continuation sheet: □ Yes ☒ No
Information Category	**Description**
1. Incidents (historical)	Information not available
2. Expected number of adversaries	One
3. Tactics	Contaminate water system with onsite chemicals
4. Equipment	Access to water utility-owned power tools and hand tools
5. Technical skills and knowledge	Knowledgeable about water processing, emergency response, security system, SCADA system, security procedures

The assessment team needs to determine whether it is required to consider an insider as a potential threat. If it does consider an insider, it will complete this worksheet for any potential category of insider adversary (see Appendix D for a blank form of the worksheet). This is the kind of information that the assessment team will collect, organize, and analyze so that it can make an informed decision about the insider threat. In Appendix D, several insider examples are included for consideration. Definitions for the low-, medium-, and high-level insider threats are also presented. These are only starting points in the development of the insider portion of the DBT and must be further developed.

4.6 CYBER THREAT

The threats to the SCADA system considered fall into four major categories: (1) human intentional, (2) human unintentional, (3) natural, and (4) environmental. The level or sophistication of the threat directly impacts resources required in any mitigation efforts, so a clear and accurate description of the threat under consideration in the risk assessment process is critical to the overall security improvements. This particular assessment focuses primarily on category 1, with some consideration for 2. Categories 3 and 4 receive only secondary consideration in the process.

Within the human intentional or malicious category there are two basic types of adversaries to be considered: "outsiders" and "insiders." It is generally the goal of an outsider adversary to either become an insider, or to acquire the access and other attributes of an insider. Thus, some of the differentiating attributes of the various outsider adversaries will be the ability to acquire a high-level of insider access. The next several sections provide details on characterizing the insider and outsider cyber threats.

4.6.1 Outsider Adversary Levels

The difference in sophistication between cyber adversaries is not necessarily with respect to the tools employed, but more in their ability to use and customize these tools. Figure 4.2 depicts the increasing sophistication level of cyber adversaries. Similar tools are available for each adversary type. A clearer distinction is the adversary's ability to discover the actual security architecture that has been implemented, as well as the level of access needed to perform their mission. In the water SCADA assessment, the focus is at the hacker level due to the immaturity of security prevalent in the current information technology (i.e., cyber systems at water utilities). For the short term, most water utilities will need to focus on the hacker level threat but should recognize that the long-term goal is to protect against the cyber terrorist.

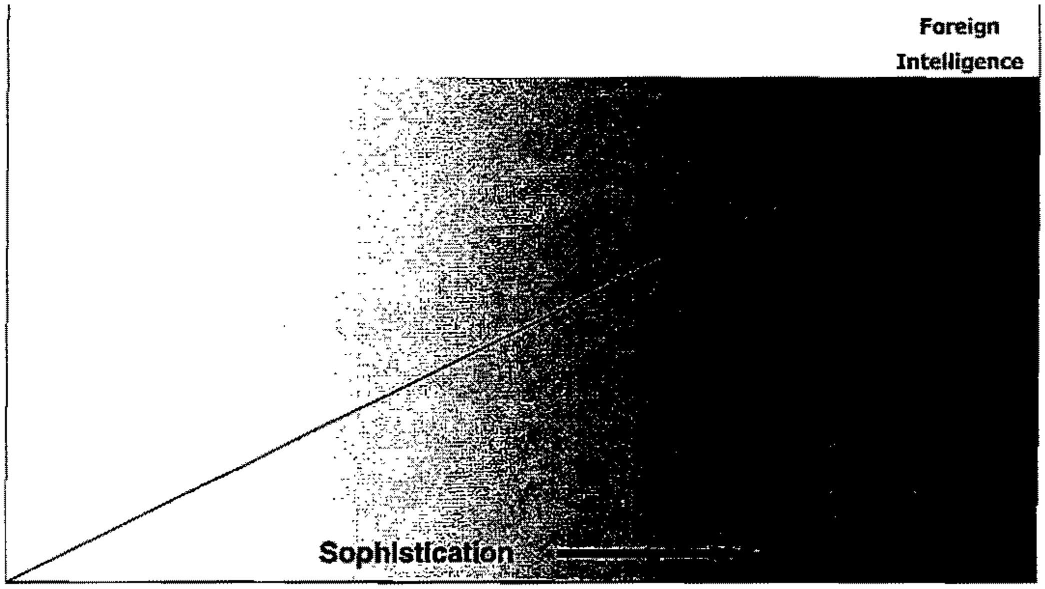


Figure 4.2. Outsider Adversary Levels

4.6.2 Insider Levels

The insider threat includes many people with various degrees of knowledge and various degrees of access within a water utility (Figure 4.3). The person who can do the most damage to a water utility with the least amount of effort is an insider who already has access to the computer system. Insiders have erased complete files of companies, inserted "bugs" into software that are very difficult to find, and may do their damage and remain as an employee. Again, the sophistication level is key in distinguishing between different insider adversaries. Due to the immaturity of security in the cyber systems, the SCADA assessment typically focuses on the operator with knowledge and privileges (i.e., operator who uses the software but may not know how the software works).

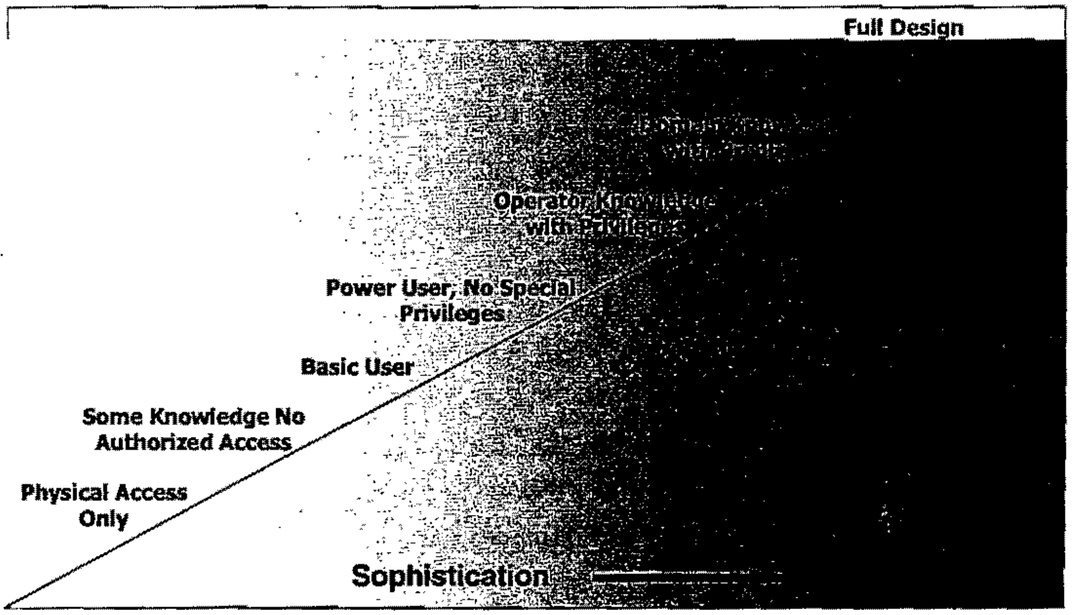

Full Design
Operator Knowledge with Privileges
Power User, No Special Privileges
Basic User
Some Knowledge No Authorized Access
Physical Access Only
Sophistication

Figure 4.3. Insider Adversary Levels

The threat of cyber attack is becoming a very important subject and a vulnerability that water utilities need to address. As water utilities become more dependent on SCADA systems to control their operations, they are becoming more vulnerable to someone hacking into the system and damaging assets. A denial of service attack on the SCADA operation affects more than the automated control of the water process. It affects the entire water utility. The cyber threat is dependent on the water utility's cyber features and is the domain of some very specific people within the organization.

4.6.3 Cyber Threat Attributes

It is recommended that the water utilities initially use the hacker as the DBT and secure to that level before attempting to secure to the higher level of a cyber terrorist. The outsider and insider adversaries, with associated attributes, are listed in Tables 4.4 and 4.5, respectively. Appendix D contains definitions for the low-, medium-, and high-level hacker threats, which are starting points in the development of the outsider hacker portion of the DBT.

Table 4.4. Outsider Adversaries and Attributes

Adversary	Level of Sophistication	Resources	Mission	Risk Tolerance	Motivation
Naïve Novice	Low	Low – No skills	Tactical – fun	High – No concept of penalties or risk	Exploration, recreation
Experienced Novice	Low	Low – Few skills only	Tactical – fun	High – Little concept of penalties or risk	Exploration, recreation
Hacker/Cracker	Moderate	Low – Skills only	Tactical – knowledge, visible effects	Moderate – Knowledge of penalties, accepts risk of being caught after deed	Exploration, recreation, searching for knowledge and experience
Hacker Coalition/ Hactivitists	High	Moderate – Aggregated skills only	Tactical – statement, visible effects, social or political change	Moderate – Knowledge of penalties, accepts risk of being caught after deed	Common goal, political or social motives
Organized Crime	High	High – Approximately $10M	Strategic – gain control, financial gains	Low – Does not want to be caught during any phase	Financial
Cyber Terrorist	High	High – Approximately $10M	Strategic – goal oriented, other targets of opportunity	Low – Does not want to be caught in intel gathering or implantation	Political or social motives
Foreign Intelligence Service	High	High – National level	Strategic – goal oriented	Low – Does not want to get caught during any phase, especially by "allies"	Political motives

Table 4.5. Insider Adversaries and Attributes

Adversary	Level of Sophistication	Resources	Mission	Risk Tolerance	Motivation
Physical Access Only	Low	Low - Moderate	Disruption	Low - Moderate	Anger, collaboration, operative
Some Knowledge, No Authorized Access	Low	Low	Disruption	Low - Moderate	Anger, collaboration, operative
Basic User, No Special Privileges	Low	Low	Disruption, Financial gain	Low	Anger, collaboration, operative
Power User, No Special Privileges	Moderate	Low	Disruption, Financial gain	Low	Anger, collaboration, operative
Operator Knowledge, Some Privileges	Moderate - High	Low	Disruption, Financial gain	Low	Anger, collaboration, operative
Domain Knowledge, Some Privileges	High	Moderate	Disruption, Financial gain	Low	Anger, collaboration, operative
Full Design Knowledge, Full Privileges	High	Moderate	Disruption, Financial gain	Low	Anger, collaboration, operative

4.6.4 Emerging System Weaknesses

It is important to understand the trends in modern SCADA systems to understand the nature of the cyber threat. Some of the key trends include:

- SCADA systems are transitioning from proprietary hardware and software platforms towards commercial off-the-shelf products (i.e., Windows, Unix, Cisco network devices etc.).
- The configurations and operations closely resemble other IT systems.
- For business purposes, SCADA systems are being connected to other IT networks such as the corporate Local Area Network (LAN) and the Internet.
- Many water utilities have "piggy-backed" their security systems on the SCADA system, resulting in the loss of both systems during a successful attack.

As a result of these trends, SCADA systems inherit the same vulnerabilities as other IT systems today, but the consequences may be greater. In addition, there may be unique vulnerabilities inherent to the SCADA applications because they were not designed with security as a primary requirement. For example, a denial-of-service (DoS) attack against a SCADA system that supports transport of physical alarms puts the entire water utility at risk.

4.7 Threat Analysis Summary

The outsider and insider worksheets for all potential threats need to be completed and analyzed so that entire threat spectrum can be examined. The examination of the threat spectrum leads to the definition of a DBT. For the example water utility, the DBT is summarized in Table 4.6.

Table 4.6. Water System Threat Analysis Summary for Example Water Utility

Adversary	Number	Equipment/ Vehicles	Knowledge	Weapons	Tactics
Outsider	3	Hand tools, power tools, pick up, 4 x 4, car	Limited knowledge of security system and water processing facility; limited cyber capability	Handguns, automatics, Explosives (5 lb or less)	Damage water system, disrupt water flow
Insider	1	Onsite tools, SCADA access, company vehicles	Knowledgeable about water processing emergency response, security system, SCADA system, security procedures	N/A	Contaminate with onsite chemicals
Outside Hacker	1	Computer and hacker software tools	Access to Internet, knowledge of hacker tools	N/A	Damage assets through SCADA system

The proposed DBT should be drafted, reviewed, and agreed to by management before proceeding on with the detailed assessment. The final definition of threat for the water utility is required information for the security design and system effectiveness analysis.

4.8 LIKELIHOOD OF ATTACK (P_A)

In the risk equation

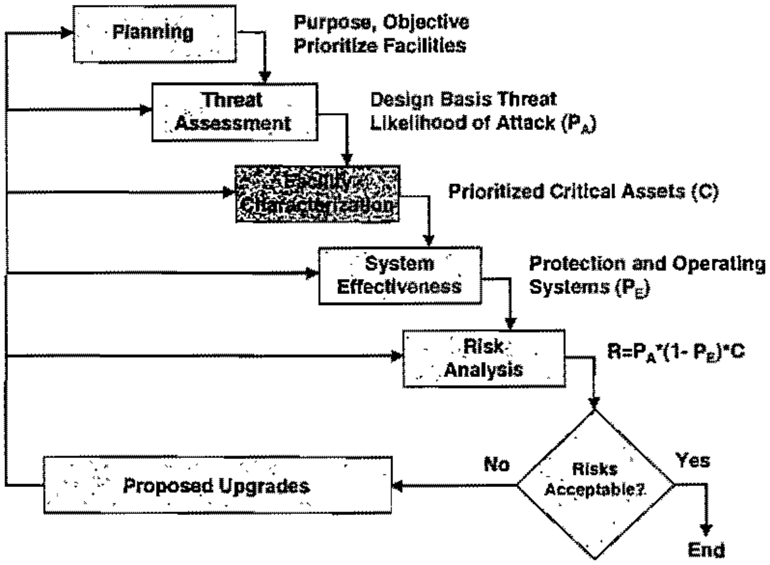
$$R = P_A * (1 - P_E) * C,$$

the term, P_A, refers to likelihood of attack by the adversary. P_A is an extremely difficult term to estimate due the lack of sufficient intelligence data available. Its estimation involves a little bit of predicting the future. The risk equation calculation can be entirely thrown off without sufficient data to be able to come up with a good estimate of P_A.

In the RAM-W^{SM} application of this risk equation to water utilities, it is therefore recommended to set the term P_A to 1.0. The calculation of risk (setting P_A to 1.0), ranks the assets only by consequence, C, and by system effectiveness, P_E. Both of these terms can be estimated far better than the ability to estimate P_A. Not using P_A as a discriminator among assets makes sense for risk assessments that are localized to a single water utility.

Note the subtle distinction between setting P_A to 1.0 in order to calculate probability and setting P_A to 1.0 because it is believed that the probability the water utility will be attacked by an adversary is 1.0. Calculating probability in this manner does not imply a belief that the water utility will definitely be attacked by an adversary.

5 SITE CHARACTERIZATION



Waterfall Flow Diagram – Process Locator

5.1 Preparation for Site Characterization

It is absolutely essential that a site be fully understood in terms of constraints, performance parameters, operations, and the circumstances in which it exists. Information and data about all the various aspects must be obtained and reviewed. When collecting information a variety of sources should be used including drawings, policies and procedures, tours, briefings, reference material, and personal interviews.

A system process diagram will greatly assist the assessment team in the early phases of the assessment. The assessment team should be especially concerned with single points of failure (SPOFs) that are easily accessed and damaged and/or destroyed. It is also important to understand how the parts of the process interrelate and how an undesired event can be overcome operationally. It is generally much more cost effective if an operational or a design change can be made to reduce a consequence rather than installing expensive security features.

5.2 Risk Assessment Scope

The assessment team must define the scope of the analysis for the water utility. The assessment team should review the system process diagrams, interview the facility operators and others that understand in detail how the system operates, review emergency operations plans, and consider the interdependencies with other critical infrastructures to help define the boundaries of the assessment (i.e., the assessment team needs to define what will and will not be included in the analysis). For example, electrical power, communication lines, natural gas, and piping systems enter and leave each of the facilities in multiple locations and a decision has to be made as to how far each of these systems will be assessed. It is important for the assessment team to focus on assets that are under the control of the water utility.

5.2.1 Interdependencies

The assessment team will need to understand the interdependencies and how easy or difficult they are to disrupt. Examples of interdependencies are:

- Electrical power
- Natural gas
- Diesel fuel
- SCADA
- Communications
- Transportation of Chemicals

The assessment team will want to evaluate the ability of an adversary to cause disruptions using an interdependent infrastructure. Electrical substations may be in very vulnerable locations, but unless the water utility owns the substation, it may be that very little can be done to improve the security. Developing relationships with critical suppliers (e.g., wholesalers, electrical power companies, etc.) and having a written plan in place to recover quickly in the event that critical components of the system are disabled or destroyed can reduce the consequences of a malevolent attack.

5.3 DOCUMENTS REQUIRED FOR SITE CHARACTERIZATION

After the critical facilities are prioritized and the assessment team understands the proposed DBT, the next phase is to begin a more detailed analysis of the operations to be studied. The following information should be gathered and reviewed:

- Unusual occurrence reports.
- Facility drawings and site plans.
- Utility maps (electrical, gas, water, and wastewater).
- Emergency operations plans.
- Emergency response plans.
- Chemical impact analyses (chemical releases into air or water).

- Back-up system diagrams.
- SCADA system design and operation documents.
- Operational reports.
- Communication system design and operation documents.
- Employee security policies and procedures.
- Visitor policies and procedures.
- Contractor policies and procedures.
- Security alarm logs.
- Existing security system design and operational data.

Before going to the field, simple block diagrams should be developed that outline the buildings, building openings; critical assets (if known), site perimeters, etc. In Figure 5.1, a block diagram has been created to represent one of the treatment paths for the water withdrawn from Bigg Lake for the example water utility (Treatment Plant 1). Single points of failure (SPOFs) exist all along the path. These SPOFs will need to be evaluated to see if significant risks from the DBT exist.

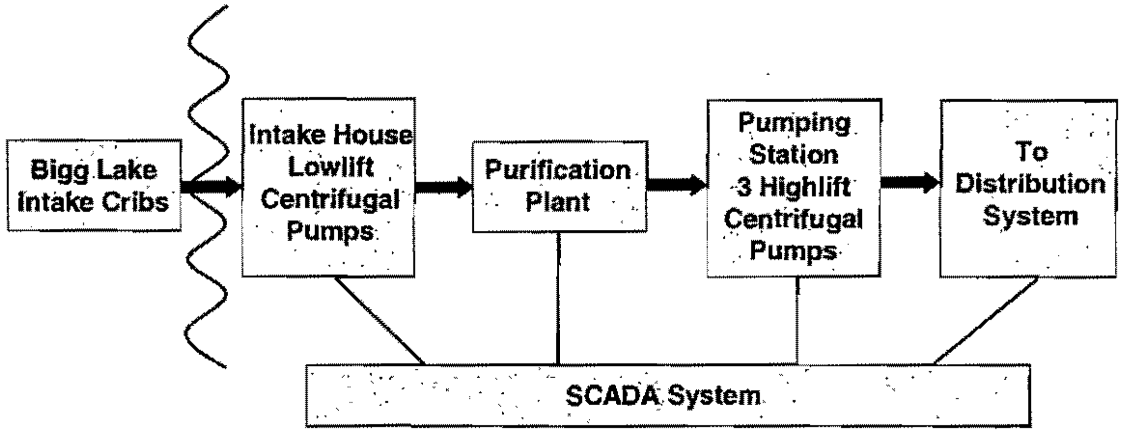

Bigg Lake Intake Cribs
Intake House Lowlift Centrifugal Pumps
Purification Plant
Pumping Station 3 Highlift Centrifugal Pumps
To Distribution System
SCADA System

Figure 5.1. Water System Block Diagram for Treatment Plant 1 (Example Water Utility)

5.3.1 Site Survey

After all the background documentation and block diagrams have been reviewed and a site-specific fault tree (Section 5.4) constructed, a site survey is conducted to verify the information. As the survey progresses, the assessment team will uncover vulnerabilities and sensitive information. It is critical that this information be briefed to management before discussion in meetings or feedback sessions. Avoid discussion on security system enhancement recommendations until the risk analysis is complete. One-on-one interviews with employees and contractors at all levels are very helpful; however, direct managers should not be present to ensure candor and all conversations must be treated as confidential. Visits during the off-shifts and non-operational hours are necessary to review the operations, security system functionality, lighting levels, and other pertinent details.

Photographs are imperative during the site survey. The assessment team should take many photos for easy reference and reminders when analyzing the data at a later date. Log and label the photos as they are taken. Both panoramic shots of the entire facility (outdoor) as well as detailed photos of existing security and operational features are required. A color-coding scheme keyed to a particular facility or set of facilities for the questionnaires (Appendix F) and sketches is recommended.

5.3.1.1 Distribution System

One of the more difficult decisions for the assessment team involves the determination of how far to carry the assessment into the distribution system. Large mains and distribution areas with few supply paths available should be included. All storage reservoirs should be included as well. Large, complex systems with several storage reservoirs may need to tier their assets (Section 3.4) in order to keep the analyses to a manageable size. The assessment team should look for and review any exposed mains (e.g., over ravines, rivers, etc.). Having alternate supply paths available for all easily damaged/destroyed exposed mains should be a goal of the risk reduction efforts. If this is not possible, then contingency plans are warranted.

The assessment team should base its decision on how far to carry the analysis in a large part on the consequences of loss. Water mains break often, so most water utilities have experience isolating and repairing water lines. Look for areas that could be compromised that would result in consequences beyond normal. Think like the adversary. Where would someone attack the system and cause high consequences? What parts/equipment have long lead times to replace? If the water utility has been modeled in some type of software (EPANET), then conducting "what if" analyses can be conducted to assist the assessment team.

5.3.2 Existing Chemicals

The assessment team should collect information on all onsite chemicals and then analyze the ability of the adversary to use the chemicals to damage and/or destroy critical assets as well as to contaminate the water. Data to be gathered include:

- Location, concentration, and quantities of all chemicals,
- Containment strategies (barriers, dams, scrubbers) and capacity for unintentional release,
- Maximum amount of chemicals stored on site,
- Delivery frequency, amounts, methods of delivery (containers, slurry, bulk, etc.),
- MSDS sheets for all chemicals to be included in analysis,
- Access controls in place for chemical treatment areas,
- System capacity for injecting chemicals,
  - Number of pumps available,
  - Pump flow rates,
  - Sizes and pressure ratings on piping,
  - Water flow rates at point of injection,
  - Ease of bypassing metering system,
  - Potential for breach of container for complete release of material,
- Existing sensors,
- Process control features on delivered chemicals to the plant,
- Residence time of the treated water from the effluent of the treatment process to the first customer.

Treatment chemicals in high enough doses can constitute a threat to the water utility staff as well as consumers. Additionally, many of the chemicals stored at a water utility could be used as accelerants (LOX) or fuels (diesel, gasoline), and could be mixed with air to form explosive mixtures (propane), or in some other manner by an adversary. The assessment team should understand why and how the chemicals are stored, controls on their use, and whether or not safer alternatives are available. The effects of catastrophic breach of multiple containers should be considered, not only within the bounds of the treatment plant, but also on the surrounding community. A worksheet for collecting information on existing chemicals is included in Appendix F.

5.4 The Generic Undesired Event Fault Tree

As mentioned earlier, the facility prioritization will help the assessment team focus on those parts of the operation that must be functional for the water utility to meet the mission objectives and will be used as a starting point in the fault tree analysis described in this section. The fault trees are developed to describe the entire system, at least at a high level. The main purpose of doing this is to look for any potential WMD-type events at the water utility that did not come out of the facility prioritization. If any potential WMD-type events are found, they should be included in the analysis. Also, the fault tree can be developed in more detail wherever necessary, allowing for more in-depth analysis than the facility prioritization.

The Generic Undesired Event Fault Tree (fault tree), provided in Appendix E, is applied to the specific facility/asset that is being assessed. Appendix E provides a full-sized fault tree, a fault-tree broken into individual pieces, and a brief introduction to fault tree symbols. It is suggested that the assessment team open the full-sized fault tree as this section is reviewed.

5.4.1 Introduction to the Fault Tree

The entire fault tree is constructed from the adversary's point of view. It describes how the mission objectives of a water system can be defeated. The most generalized events are found in the upper layers of the tree. As the causes of these events are developed deeper in the tree, adversary strategies and the targets of attacks are revealed. The events are numbered in outline format beginning at the second layer and proceeding downward. The upper levels of the Generic Undesired Event Fault Tree are described in this section.

5.4.1.1 Upper Levels of the Generic Undesired Event Fault Tree

The upper levels of the Generic Undesired Event Fault Tree are shown in Figure 5.2.

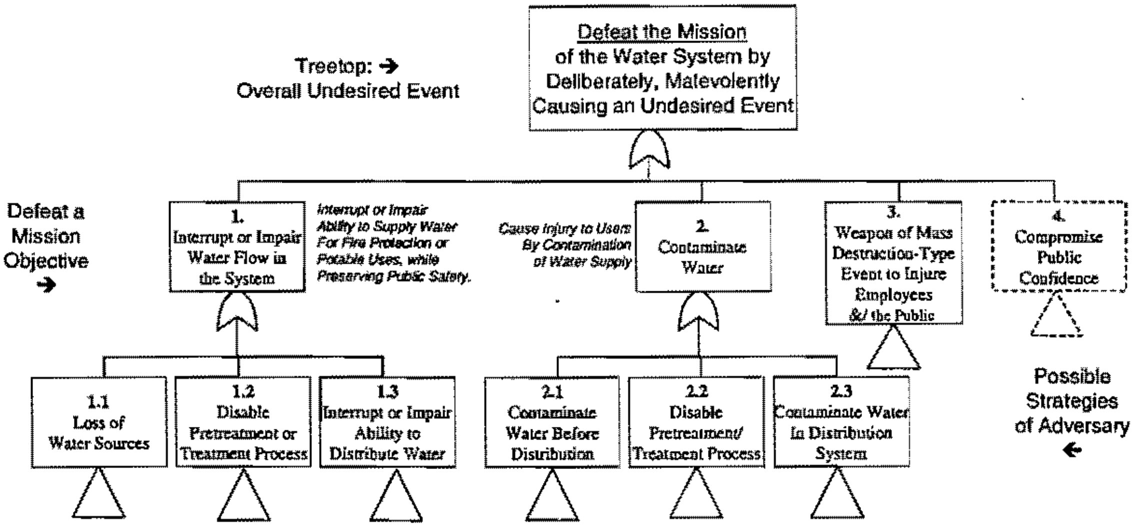


Figure 5.2. Upper levels of Generic Undesired Event Fault Tree

5.4.1.2 Treetop – Defeat Overall Mission

The overall goal of the adversary is stated in the topmost event (treetop): the adversary seeks to *defeat the mission of the water system by deliberately, malevolently causing an undesired event.* The treetop is the first layer of the tree. Every event on the tree is undesired from the viewpoint of the water utility (but desirable from the point of view of the adversary).

5.4.1.3 Layer 2 – Defeat Mission Objectives

The second layer of the tree consists of events that cause the defeat of mission objectives of the water system. They are numbered 1 through 4.

A mission objective of the water utility is to continuously maintain a flow of water to the customers. Event 1 is *Interrupt or impair water flow in the system.*

A second mission objective is to assure that the water supplied to customers is not harmfully contaminated. Event 2 is *Contaminate water.*

A third mission objective is to prevent mass injuries to employees or the public. Event 3 is *Weapon of mass destruction-type event to injure employees or the public.* An adversary might seek to accomplish Event 3 alone, or in combination with Event 1 or 2.

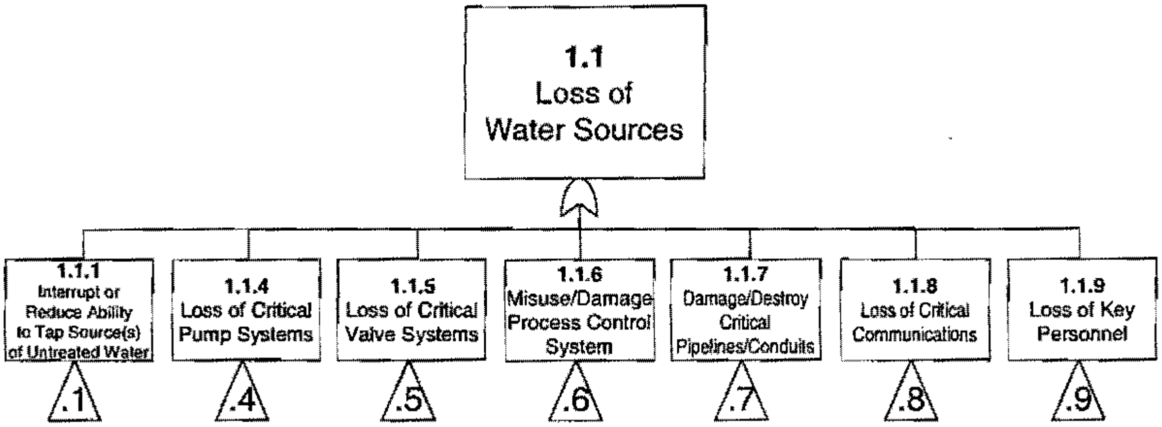
A fourth mission objective is to maintain public confidence in the water system. Event 4 is *Compromise public confidence.* This event is usually of secondary importance, so it is shown as dashed, and it is not extensively developed.

5.4.1.4 Layer 3 – Attack a Major Stage of the Water Utility

The third layer of the tree partitions Events 1 and 2 into attacks on a major stage of the water utility. The development of Event 1 follows the progress of water through the facility from source (1.1), through pretreatment and treatment (1.2), to distribution to the customer (1.3). The undesired events address attacks made at these stages to interrupt or impair water flow. The development of Event 2 addresses a contamination act before distribution (2.1), where pretreatment or treatment occurs (2.2), or in the distribution system (2.3).

5.4.1.5 Layer 4 – Adversary Strategies

The fourth layer of the tree shows diverse adversary strategies to cause each third layer event. To see the complete fourth layer, refer to the full-sized fault tree. Figure 5.3 shows how Event 1.1 is developed in layer 4. Events that develop 1.1 are 1.1.1, 1.1.4, 1.1.5, etc. At this level of development and deeper, assets are identified that are critical to the functioning of the water utility. For example, Event 1.1.4 addresses critical pump systems, Event 1.1.5 addresses critical valve systems, Event 1.1.6 addresses the process control system, 1.1.7 addresses critical pipelines or conduits, etc.


1.1
Loss of Water Sources
1.1.1
Interrupt or Reduce Ability to Tap Source(s) of Untreated Water
1.1.4
Loss of Critical Pump Systems
1.1.5
Loss of Critical Valve Systems
1.1.6
Misuse/Damage Process Control System
1.1.7
Damage/Destroy Critical Pipelines/Conduits
1.1.8
Loss of Critical Communications
1.1.9
Loss of Key Personnel
.1
.4
.5
.6
.7
.8
.9

Subtrees .1, .4, .5, .6, .7, .8, and .9 develop these events.

Figure 5.3. Development of *Loss of Water Sources*

5.4.2 Process for Customizing the Fault Tree

This section covers customizing the generic tree to apply to the example water utility described in Appendix A. The water utility description focuses on one of three water supply channels. Each channel has a treatment plant, but only Treatment Plant 2 is described. The customized fault tree is confined to the water supply channel that involves Treatment Plant 2.

The concentration on Treatment Plant 2 might result from pairwise comparison of the importance of the facilities of the water utility, and finding that Treatment Plant 2 is significantly more important than the others.

Not all water utilities have all the mission objectives and features shown on the generic fault tree. To apply the fault tree to a specific facility, delete (prune) irrelevant objectives and modify descriptions to match the facility. Similarly, for those features not shown on the tree, graft them at the correct location and develop them far enough to understand what an adversary might do to compromise that specific feature.

5.4.2.1 Pruning

Prune the fault tree by removing events that do not apply to the specific water utility being analyzed and remove any lower level development. Prune further, working level by level downward through the tree. Review the development of undesired events that have been kept in the tree, and remove events that cannot occur at the facility/asset being evaluated.

These pruning steps are illustrated for the example water utility described in Appendix A. The upper levels of the pruned tree are shown in Figure 5.4. The mission requires that water flow be maintained for fire protection and other public safety uses. Thus, Event 1 cannot be pruned. Treatment Plant 2 is designed to eliminate naturally occurring contamination; and a study indicates that Bigg Lake is too large to contaminate. Thus, Event 2.1 can be pruned, but Events 2.2 and 2.3 must be kept on the tree. Because of the potential for very high consequences, it is recommended that Event 3, *Weapon of mass destruction-type event to injure employees or the public*, never be pruned and be kept as part of the tree (at least at the treetop) to serve as a reminder to always look for those WMD-type events in the analysis.

The threat assessment for the facility shows no history of attacks that inflicted massive damage (large fires, floods, explosions, toxic releases, etc.), but gaseous chlorine is employed at the treatment plants. On this basis, Event 3 cannot be pruned.

The mission statement does not refer to issues of maintaining public confidence, so Event 4 is pruned.

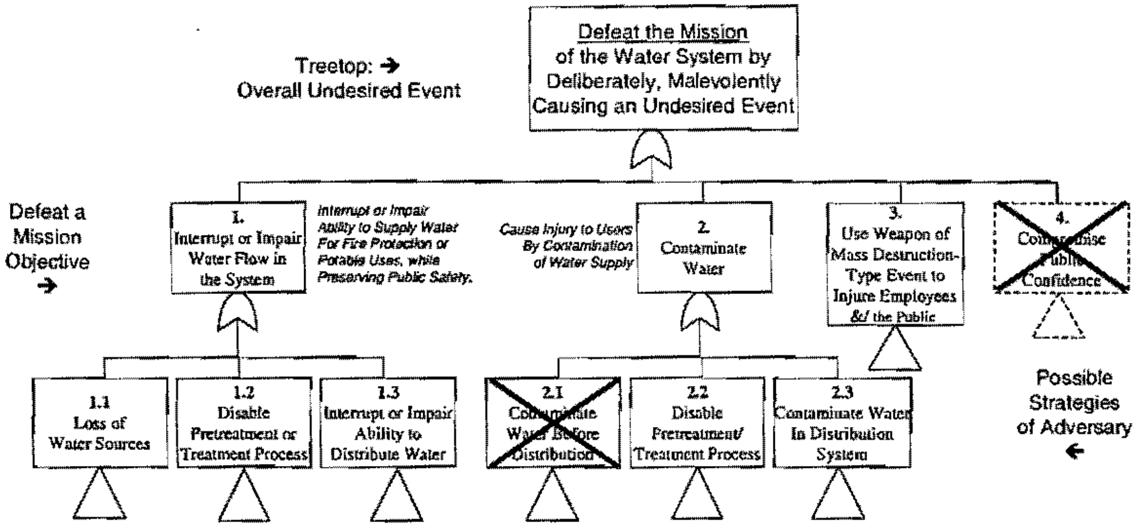


Figure 5.4. Upper levels of Site Specific Fault Tree for the Example Water Utility

To continue the example, only the development of Event 1.1, *Loss of Water Sources,* is discussed. The other events still contained on the site-specific fault tree should be treated similarly.

Figure 5.5 shows that an adversary has seven diverse ways, identified as 1.1.1, 1.1.4, etc., to cause the loss of water sources by attacking various targets (critical assets). The example water utility description shows, explicitly or implicitly, that all seven targets are present. Thus, no pruning of the fault tree is needed to customize it for the example water utility. Critical pumps, critical pipelines or conduits, key personnel, and process control (both manual and SCADA) are explicitly cited. Implicitly, process control acts through valves and requires communication lines to carry control information. Also implicit is the necessity of intake structures to bring water into the system. All of the events that develop 1.1, *Loss of Water Sources*, are retained in the tree.

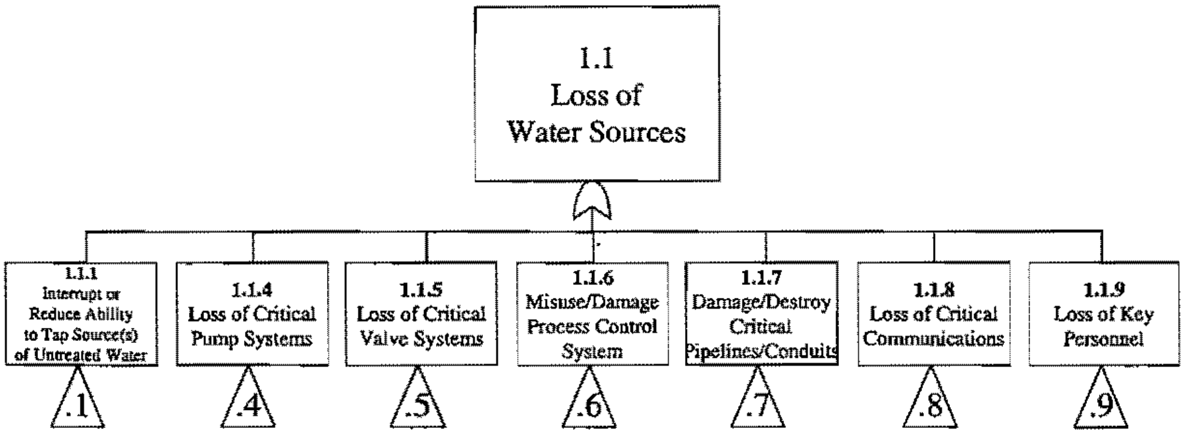


Figure 5.5. *Loss of Water Sources* for the Example Water Utility

For the example water utility, the completely customized development of Event 1.1.1 looks like Figure 5.6, assuming that :

1. No wholesaler's water is purchased,
2. The SCADA system plays no role from Bigg Lake to the plant; and
3. No ground water is delivered to Treatment Plant 2.

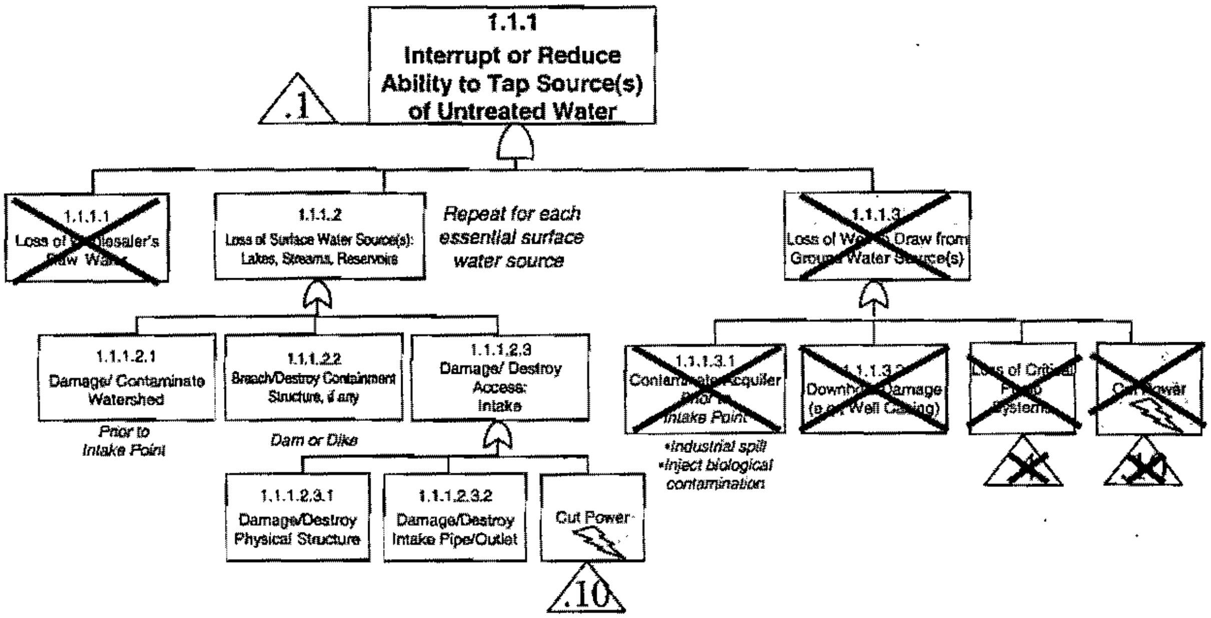

1.1.1
Interrupt or Reduce Ability to Tap Source(s) of Untreated Water
.1
1.1.1.1
Loss of Wholesaler's Raw Water
1.1.1.2
Loss of Surface Water Source(s): Lakes, Streams, Reservoirs
Repeat for each essential surface water source
1.1.1.3
Loss of Water Draw from Ground Water Source(s)
1.1.1.2.1
Damage/ Contaminate Watershed
Prior to Intake Point
1.1.1.2.2
Breach/Destroy Containment Structure, if any
Dam or Dike
1.1.1.2.3
Damage/ Destroy Access: Intake
1.1.1.2.3.1
Damage/Destroy Physical Structure
1.1.1.2.3.2
Damage/Destroy Intake Pipe/Outlet
Cut Power
.10
1.1.1.3.1
Contaminate Acquifer Prior to Intake Point
•Industrial spill
•Inject biological contamination
1.1.1.3.2
Downhole Damage (e.g. Well Casing)
Loss of Critical Pump Systems
.4
Cut Power
.10

Figure 5.6. Customized Generic Undesired Event Subtree for Example Water Utility

5.4.2.2 Grafting

Customizing the fault tree involves not only pruning but also grafting. Grafting may be necessary for two reasons. First, an undesired event that is not on the generic fault tree may occur at the site being analyzed. The event might be the defeat of a site-specific mission objective. However, the event may belong deeper in a development. The missing event should be grafted or added on and developed in a similar manner to the other fault tree events. Second, an undesired event that is on the tree may apply to several versions of the same critical asset. Graft the development of the critical asset for each different type of the asset to ensure that the differing security implications of all cases are examined.

For example, the example water utility description says that three electrical motors and pump assemblies are co-located at Treatment Plant 2. They move treated water to Pump Stations #1 and #2. On the generic tree, Event 1.3, *Interrupt or Impair Ability to Distribute Water,* includes one instance of Event 1.3.4, *Loss of Critical Pump Systems.* If the three pump systems are not identical, each different pump system should be represented on the tree by its own subtree .4, *Loss of Critical Pump Systems.*

Suppose that one pump system is a high-capacity unit, and the remaining two pumps are identical low-capacity units. On the tree, these pumps belong in the development of Event 1.2, *Disable Pretreatment or Treatment Process* as Event 1.2.4 developed by subtree .4, *Loss of Critical Pump Systems.* Since there are two different kinds of pump to represent, a second use of subtree .4 must be grafted to customize the tree. One copy of subtree .4 should be labeled "High Capacity Pump System" and the other should be labeled "Low Capacity Pump System." See Figure 5.7 for an example of grafting.

The assessment team will continue working through the fault tree until a customized version is created for the specific facility/asset being studied.

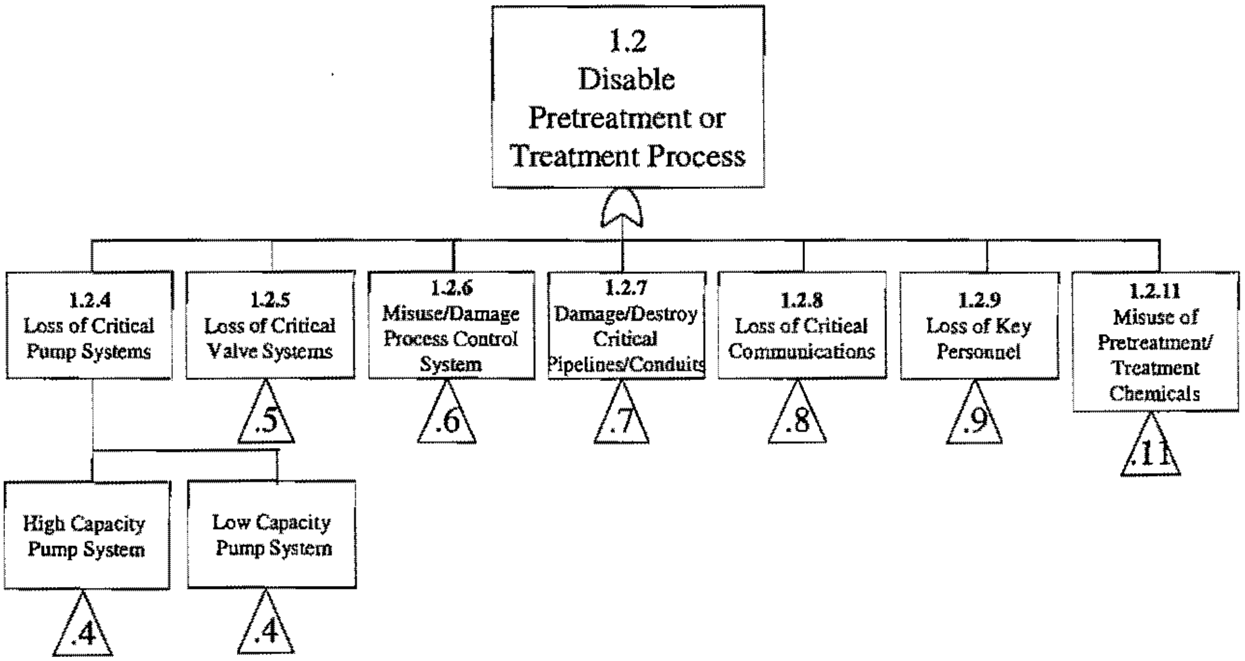


Figure 5.7. Grafted *Loss of Critical Pump Systems* for Example Water Utility

5.4.3 Identifying Critical Assets

Once completed, the fault tree should identify undesired events and thus include the critical assets that must be protected to prevent the undesired events from occurring. The highest-priority critical assets will become the targets that an adversary might attack and will be used in the risk analysis. In the next step, specific information about the mission objectives remaining on the fault tree will be collected. Critical assets might include:

- Pump systems
- Valve systems
- Pipelines or conduits
- Process control system
- Communications
- Key Personnel
- Pretreatment or treatment chemicals
- A watershed
- An aquifer
- Containment structure
- Water intake
- Well casing
- Electrical substation
- Backup power system
- Power distribution bus or switches

5.5 QUESTIONNAIRES

A series of questionnaires (Appendix F) have been developed to assist the assessment team during the site characterization activities. These questionnaires help the assessment team understand the features of the water utility and also begin to collect existing performance data about the security and operational systems. The first set of questionnaires, F.1, included in Appendix F cover the security policies and procedures, security training, emergency response readiness, and other important aspects of the overall security program at the water utility. It is recommended these questionnaires first be completed through an interview with management and then verified through interviews with staff members that are responsible for implementation. For example, if a policy exists that all employees are to call and verify their identities before entering an alarmed area, the question then becomes whether or not this policy is followed. This can be verified through interviews with operators, maintenance staff, and others requiring access to the site. If the policy is not followed, then a performance test is not required and the system effectiveness for that portion of the operation would be rated low. If the policy appears to be followed, then a performance test could be devised to determine the system effectiveness against the DBT. The questionnaires are not exhaustive, nor are they the end point of the analysis. They are simply included to facilitate the assessment team in their understanding of system performance and should be used as the beginning of discussion for thought experiments or actual performance tests to ensure the system meets the security objectives.

The second set of questionnaires, F.2, has been developed to assist the assessment team during the fault tree analysis. These questionnaires are designed to complement the fault tree and provide additional detail on how an adversary might defeat the asset being analyzed. As noted in the previous section, these questionnaires are not intended to be exhaustive or the end point of the analysis, but to help the assessment team really understand the water utility operation in detail. By going through the existing questions and creating additional ones as necessary, a detailed understanding can be gained about potential vulnerabilities. It is not possible to design a questionnaire for every situation that an assessment team might encounter, so it is more important to learn the art of asking probing questions rather than to focus on mechanically answering the questions included. Every water utility has some number of unique vulnerabilities and it is the assessment teams' responsibility to uncover as many of them as possible.

The third set of questionnaires, F.3, provides a mechanism to collect data on current security system operations. This data will be used to determine if any or all the elements of the security system can help defeat the DBT. If the risk analysis determines thatthe system has a high probability of defeating the DBT, then performance tests can be developed to validate or invalidate the analysis. The security questionnaires are completed for each of the facilities/assets included in the assessment. The assessment team may find that existing PPS features are very similar or identical at many locations and may be able to shorten the information gathering process by copying partially completed forms and filling in only the site specific items. For example, if all sites have an eight-foot-high fence of the same construction, this item can be completed once for all facilities/assets.

The fourth set of questionnaires, F.4, helps determine the importance of the SCADA system to the operations of the water utility. The fifth set of questionnaires, F.5, characterizes the SCADA if it is to be analyzed. And the final questionnaire, F.6, is a guide for gathering information about onsite chemicals. The questionnaire lists three chemicals (a solid, a liquid, and a gas) that are filled out as an example.

5.6 Consequence Assessment

It is not possible or practical to protect all the assets owned by a water utility. The criteria for selecting assets to protect will depend on the desire to avoid undesirable consequences and the capabilities of the adversary. The consequence assessment process uses

The second set of questionnaires, F.2, has been developed to assist the assessment team during the fault tree analysis. These questionnaires are designed to complement the fault tree and provide additional detail on how an adversary might defeat the asset being analyzed. As noted in the previous section, these questionnaires are not intended to be exhaustive or the end point of the analysis, but to help the assessment team really understand the water utility operation in detail. By going through the existing questions and creating additional ones as necessary, a detailed understanding can be gained about potential vulnerabilities. It is not possible to design a questionnaire for every situation that an assessment team might encounter, so it is more important to learn the art of asking probing questions rather than to focus on mechanically answering the questions included. Every water utility has some number of unique vulnerabilities and it is the assessment teams' responsibility to uncover as many of them as possible.

The third set of questionnaires, F.3, provides a mechanism to collect data on current security system operations. This data will be used to determine if any or all the elements of the security system can help defeat the DBT. If the risk analysis determines thatthe system has a high probability of defeating the DBT, then performance tests can be developed to validate or invalidate the analysis. The security questionnaires are completed for each of the facilities/assets included in the assessment. The assessment team may find that existing PPS features are very similar or identical at many locations and may be able to shorten the information gathering process by copying partially completed forms and filling in only the site specific items. For example, if all sites have an eight-foot-high fence of the same construction, this item can be completed once for all facilities/assets.

The fourth set of questionnaires, F.4, helps determine the importance of the SCADA system to the operations of the water utility. The fifth set of questionnaires, F.5, characterizes the SCADA if it is to be analyzed. And the final questionnaire, F.6, is a guide for gathering information about onsite chemicals. The questionnaire lists three chemicals (a solid, a liquid, and a gas) that are filled out as an example.

5.6 CONSEQUENCE ASSESSMENT

It is not possible or practical to protect all the assets owned by a water utility. The criteria for selecting assets to protect will depend on the desire to avoid undesirable consequences and the capabilities of the adversary. The consequence assessment process uses the consequence of the loss to help determine which assets are at greatest risk relative to all the assets owned by the water utility.

5.6.1 Define Measures of Consequence

This section presents the concept of consequence measure and defines a consequence matrix by which the water utility's facilities and assets will be evaluated. A consequence assessment determines a consequence value (i.e., high, medium, or low) for all undesired events identified during the assessment. If values for some of the undesired events are not readily available, expert opinion of the assessment team or other subject matter experts can be used. Each undesired event can have several types of consequences and all must be captured. The final consequences used in the risk analyses are the highest of the estimated consequences for each undesired event. Once the consequence matrix has been established, an appropriate consequence value is assigned to each undesired event or asset loss. The measures of consequence could possibly include the following:

- Economic loss to water utility (equipment, facilities, loss of revenue, etc.)
- Economic loss to society
- Cost to repair/replace
- Deaths
- Illnesses
- Duration of loss
- Number of customers affected (critical and non-critical)
- Loss of fire protection

The assessment team must define its own site-specific measures of consequence and document the rationale for the measures and values selected.

5.6.1.1 Documentation to Review

To help define measures of consequence and completely understand the consequences related to defeating one or more of the mission objectives of the water utility, the following information should be considered:

- Facility drawings and site plans with supporting documentation
- Utility maps (electrical, gas, water, and wastewater)
- . Maintenance and Service records

- Chemical impact statements
- Water utility budgetary authority (financial records)
- Water quality standards reports and documentation
- Historical public confidence indicators

5.6.2 Develop Site Specific Consequence Matrix

To help assessment teams understand how to construct a matrix, an example generic consequence matrix (Table 5.1) has been included as a starting point. The matrix is useful in helping to identify possible measures that could be applied. When constructing the matrix, it is important not to set the measures too low, which could lead to all assets being ranked high priority (value of "C" would not be a discriminatory factor). Defining realistic and pragmatic values for high, medium, and low will be a challenge for the assessment team and therefore will need to be developed methodically. The assessment team will likely need input from the financial officer and upper management to construct and gain approval of the consequence matrix.

As noted in Chapter 4, some undesirable events have consequences far exceeding the high category and may be candidates for being labeled as WMD-type events. The consequences of the WMD-type events are likely catastrophic to the operation of the water utility and to public safety.

Table 5.1. Example Generic Consequence Matrix

Undesired Event	Measure of Consequence	Very High	High	Medium	Low
Loss of water sources	Economic loss	N/A	>$5M	$500K–$5M	<$500K
	Duration of loss	N/A	>4 weeks	1–4 weeks	<1 week
	Number of users impacted	N/A	>100K	5K–100K	<5K
	Loss of fire protection	N/A	>4 hr	0–4 hr	<0 hr
Disable Pretreatment or Treatment Process	Economic loss	N/A	>$5M	$500K–$5M	<$500K
	Duration of loss	N/A	>5 days	1–5 days	<1 day
	Number of users impacted	N/A	>100K	5K–100K	<5K
Interrupt or Impair Ability to Distribute Water	Economic loss	N/A	>$5M	$500K–$5M	<$500K
	Number of users impacted	N/A	>100K	5K–100K	<5K
	Loss of fire protection	N/A	>4 hr	0–4 hr	<0 hr
	Deaths	N/A	>5	0–5	<0
	Illnesses	N/A	>5K	500–5K	<500
WMD-type Event	Economic loss	TBD	N/A	N/A	N/A
	Number of users impacted	TBD	N/A	N/A	N/A
	Loss of fire protection	TBD	N/A	N/A	N/A
	Deaths	TBD	N/A	N/A	N/A
	Illnesses	TBD	N/A	N/A	N/A

The assessment team will construct a site-specific consequence matrix based on the measures of consequence identified and the information and data collected from the documentation review as well as the responses to the questionnaires. As an example, a site-specific consequence matrix for the example water utility was developed based on the information provided in the description (Appendix A) and is shown in Table 5.2. The consequence matrix includes five columns. The first column lists the measures of consequence (economic loss, duration of loss, number of user impacted) and the remaining columns indicate the threshold levels at which the consequence is to be evaluated for a corresponding measure.

Table 5.2. Site-Specific Consequence Matrix for the Example Water Utility

Measure of Consequence	Very High	High	Medium	Low
Economic Loss	TBD	>$2M	$2M–$500K	<$500K
Duration of Loss	TBD	>24 hr	24–8 hr	<8 hr
Number of Users Impacted	TBD	>2,000	200–2,000	< 200

It is suggested that the assessment team perform a pairwise comparison on its consequence matrix for validation. Each measure would be placed into a pairwise matrix and compared against one another for each consequence value (high, medium, low) to determine if all the measures included under each specific column are indeed at a similar level. The measures included in the consequence matrix will drive the assets that are labeled critical when the risk analysis is complete. It may be beneficial to use multiple consequence matrices for different parts of the water utility operation. The measures of consequence should be reevaluated periodically. The matrix should also be revisited when significant changes are either planned or completed for the water utility. Once the consequence matrix has been established, an appropriate consequence value will be assigned to each asset in subsequent risk analyses.

5.6.3 Determine Critical Assets Consequence Levels

After the assessment team develops and agrees to the site-specific consequence matrix, they then review the critical assets identified from the fault tree and rank the consequence of the undesirable Events as low, medium, high, or very high (WMD-type events). To help determine the consequence value for each critical asset, a table is used that lists the undesired events and the critical assets on the left and the measures of consequence across the top. A Consequence Value Table (Table 5.3) for Treatment Plant 2 of the example water utility was developed based on Table 5.2 and information provided in the example water utility description (Appendix A). A detailed description of how the high, medium, and low consequence values were derived for the example water utility is given in Appendix G. For each critical asset and measure of consequence a value of high (H), medium (M), or low (L) is assigned. When all the values are filled in then an overall consequence value can be determined. Clearly if all "H" values are assigned across a row, then the overall consequence value would be High. If there was one "H" and the rest "M" across a row, it might be evaluated as a "H-M" asset. The assessment team will have to develop rules for determining the overall consequence value (note: averaging values is not a recommended approach).

Table 5.3. Consequence Values for Undesired Events for the Example Water Utility

		Measures of Consequence			
		Economic Loss	Duration of Loss	No. of Users Impacted	***Overall Consequence Value***
Undesired Events	Damage or destroy pipelines/conduits	L	H	H	**H**
	Damage or destroy disinfection capability	M	M	M	**M**
	Loss of pumps	L	H	H	**H**
	Loss of key personnel	L	L	L	**L**

Some undesired events have a higher consequence than others, so the loss of the critical assets associated with them will have a higher "C" value, making them higher priority critical assets.

5.7 EXISTING PROTECTION SYSTEMS

The RAM-W^{SM} term, protection system, refers not only to the physical protection system, but has been extended to also include non-physical security elements that contribute to protection system effectiveness. These non-physical security elements, referred to as operational elements, are elements that are intrinsic to the water utility operation. Typically, these elements were put in place to serve other purposes but contribute to security by preventing an adversary from achieving their goal.

To evaluate system effectiveness, it is important to understand how the Physical Protection System (PPS) and the Operational System (OS) work together. First, detection must occur. Detection can come from either the PPS or the OS. Once detection occurs, if either the PPS's or the OS's delay and response prevent the adversary from achieving his/her objective, then the protection system is effective. This is a very high-level description of how the PPS and the OS work together. Timelines are used in Chapter 7 to explain system effectiveness in much more detail.

5.7.1 Collect Information on the Existing Security System

As part of the site characterization, the assessment team will collect information about the existing PPS. As noted in Section 5.5, the assessment team should review policies and procedures on all elements of security including:

- Security policies and procedures,
- Visitor policies and procedures,
- Contractor policies and procedures,
- Existing security system design and operational data.

After reviewing available documentation, the assessment team will collect information about potential adversary paths. The assessment team should follow a systematic process to capture information on all existing PPS elements. One suggested method is to start at the boundaries (e.g., fences, gates, openings, etc.) and work in to the critical asset(s), recording pertinent information (e.g., building perimeters, doors, sensors, interior barriers, etc.) along the way. The following are examples of data to collect:

- Detection capabilities with respect to the DBT.
- Alarm assessment capabilities.
- Estimated delay times for the DBT considering tools, technologies, and skills.
- Expected response times from onsite resources, local police, or sheriff, and any other emergency responders.

This information will be used to characterize the existing security system and establish a baseline of performance. Data may be available, but if not, tests will need to be performed to derive it. The assessment team needs to integrate all data collected so that one is not looking at "silos" of information.

5.7.1.1 Physical Protection System Features Worksheet

Table 5.4 is a completed worksheet for Treatment Plant 2 that lists the standard features of the PPS. The assessment team will want to customize this worksheet for their site by adding or deleting appropriate features. Examine and verify that each feature exists. Do not assume that they exist and are functional because they show up on a drawing or were mentioned by personnel during an interview. It is not unusual to find presumably locked doors open, sensors installed improperly (pointing the wrong way), response forces assumed to show up in a certain time when they do not know where to go once they arrive at the facility, etc. This worksheet can be a helpful guide in verifying features from an adversary standpoint. A blank copy of the worksheet is contained in Appendix F.

Table 5.4. Example Physical Protection System Features Worksheet

WATER SYSTEM DATA COLLECTION WORKSHEET – PHYSICAL PROTECTION SYSTEM FEATURES		
Facility: Example Water Utility		
Date: May 15, 2002		**Recorded by:**
Functional Area: Treatment Plant 2		**I. Drinkwater**
Physical Protection Features	**Reviewed**	**Photo**
	Yes/No/NA	**Disc/Aperture**
1. Boundary	Yes	
1a. Fence (height and construction)	Chain Link 8'-0"	
1b. Vehicle barriers	None	
2. Entrances (Site)	Yes	
2a. Personnel/Vehicle	Both	
2b. Entrance Construction	Chain Link (both)	
2c. Entrance Locks	Padlock	
2d. Entrance Barriers	None	
3. Distance between boundary and building	60'	
4. Building construction	Brick and Stone	
5. Entrance (doors, windows, vents, skylights) construction	Hollow metal doors, regular glass.	
5a. Entrance Locks	Commercial	
5b. Entrance Barriers	None	
6. Distance between entrance and critical asset	Avg. 20'	
7. Critical asset enclosure construction	None	
8. Critical asset enclosure entrance construction	None	
8a. Enclosure locks	N/A	
8b. Enclosure barriers	N/A	
9. Sensors (fence, intrusion, door/gate position, penetration, motion)	Personnel doors only	

WATER SYSTEM DATA COLLECTION WORKSHEET – PHYSICAL PROTECTION SYSTEM FEATURES		
Facility: Example Water Utility		
10. Detection by personnel	Low	
11. ID checks	No	
12. Contraband detection (persons, packages, vehicles)	No	
13. Assessment by camera or personnel	No	

5.7.2 Review the Performance of the Existing Security System

Once the assessment team has collected and organized the information for the existing security system, the next step is to evaluate the performance of each PPS feature. This information is categorized as estimates of the following:

- Detection probabilities (detection of the DBT intrusion)
- Assessment probabilities (after detection, communicate and verify the alarm)
- Delay (time required of the DBT at the barriers)
- Response time and capability (response by a force soon enough and capable enough to stop the adversary from completing their objective)

This all needs to be in the context of the adversary attack scenario timeline and will be described in more detail in Chapter 7.

Performance of the security system also needs to be reviewed during shift changes, weekends, holidays, under inclement weather, and during operational and non-operational hours. There can be distinctly different performance metrics in comparison to the daytime operational hours.

5.7.3 Review the Performance of the Existing Operational System

The operational system often plays an important role in reducing risk from malevolent attack. The assessment team must thoroughly understand the existing operations and how undesired events may be overcome. Some operational components may be too difficult for the adversary to defeat when considering the DBT capabilities. Examples would be deep rock tunnels and impoundment structures that would require large amounts of explosives and large storage reservoirs that would be difficult to contaminate. The consequences may be high if the events were to occur, but the capability to accomplish the feat may be beyond the DBT.

Having redundancy available is another way the operational system can overcome undesired events. Credit can be taken for redundancy if both are not easily damaged and/or destroyed. For example, if one large main were exposed on a bridge and easily damaged, having two large mains exposed will not lower risk. However, if the second main is buried and not easily accessible, then the DBT may have a difficult time disrupting both (or not even be aware that redundancy exists).

Many water utilities are dependent on the electrical grid to pump water through their treatment facilities and to deliver potable water to their customers. Electrical gear is easy to damage, can be easily accessed, and may take years to replace. The adversary would not even need to access the water utility site to accomplish a major disruption. Having mobile gear available to provide back-up power could significantly lower the risk, especially if the mobile equipment is stored in a secure location.

All these examples are included to demonstrate the type of information the assessment team will need to collect. Where SPOFs and interdependencies are noted, the assessment team will need to evaluate the operational options available to the water utility to determine the degree of vulnerability.

5.8 SCADA ASSESSMENT METHODOLOGY

Note: The methodology discussed in this section focuses on the SCADA system(s) of the water utility, but all IT systems critical to the water utility should be assessed.

The SCADA security assessment portion of RAM-W^{SM} is based on a relative ranking assessment approach to water utility SCADA systems. A guided top-down approach provides the basic structure and integrates elements from a variety of IT assessment and evaluation approaches. The process provides an effective means to evaluate the overall system security of water utility SCADA systems and to guide the development and integration of sustainable security improvements. The SCADA Security Policy Framework^{TM} and the CobiT$^{®}$ (Control Objectives for Information and related Technologies) framework provide guidance during the assessment and mitigation formulation stages. A final, prioritized list of SCADA system assets, ranked by relative security deficiency, indicates an order for applying resources to improve SCADA security.

Shown in Figure 5.8 is an overview of the methodology used to assess the SCADA system. This methodology can be used whether or not the SCADA system has been identified as a critical asset to the mission of the water utility and provides a systematic assessment approach to evaluate the logical and physical security aspects of the SCADA system. In this approach, modern SCADA systems are viewed as IT based systems due to their constituent components and operational requirements. A life-cycle approach to mitigation strategies is required because effective security in IT based systems is an ongoing process, not a one-time technology fix. To help meet this objective, CobiT® is an integral part of the SCADA system assessment approach and the resulting mitigation strategies. This process resides primarily in the IT Security category of assessment processes utilized at Sandia National Laboratories, but also draws from the Red Team and System Risk approaches in several important areas. In addition, the mitigation strategies integrate with the general IT Management approach via the inclusion of CobiT®. The ultimate goal of this effort is to provide the water utilities with an assessment approach that supports sustainable security for their SCADA systems.

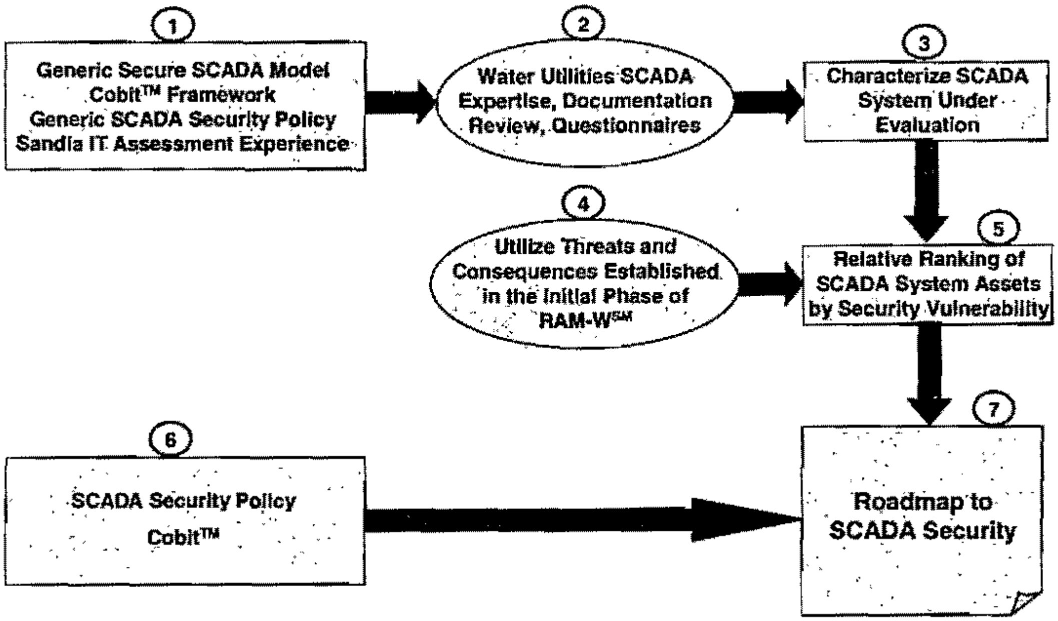

1
Generic Secure SCADA Model
CobitTM Framework
Generic SCADA Security Policy
Sandia IT Assessment Experience
2
Water Utilities SCADA Expertise, Documentation Review, Questionnaires
3
Characterize SCADA System Under Evaluation
4
Utilize Threats and Consequences Established in the Initial Phase of RAM-WSM
5
Relative Ranking of SCADA System Assets by Security Vulnerability
6
SCADA Security Policy
CobitTM
7
Roadmap to SCADA Security

Figure 5.8. SCADA Assessment Methodology

For Figure 5.8:

1. These elements guide the data gathering and review process in the next step.
2. Information gathering and formulation stage specific to water utility SCADA needs, which leads to the next step.
3. SCADA system characterized from a security perspective.
4. Threats and consequences ranked against results from previous step to provide a relative ranking of SCADA assets by security vulnerability.
5. Input for the final step.
6. Input for the final step.
7. Roadmap or path to SCADA security.

5.8.1 Documentation Review

Documentation requested in the planning stage of the methodology aids the assessors in understanding the SCADA system. Standard policy and plans documentation required for the assessment include:

- SCADA Security Policy,
- SCADA Security Plan,
- Configuration control/management procedural documentation, and
- SCADA security training documentation.

The SCADA security policy is specific to the SCADA system as opposed to the overall IT system. The SCADA security policy is reviewed to determine to what degree the water utility is securing its SCADA system. In addition to policy and plan documentation review, standard hardware documentation is also required for the assessment and includes the following:

- Network diagram (Visio-style document) and/or the control center LAN diagram,
- Logical topology drawing of the SCADA network,
- Interface points defined as where the SCADA and business networks are connected,
- List of network equipment (i.e., routers, Ethernet switches, CSUs/DSUs, etc.), used in the SCADA network,
- List of SCADA computer platforms (i.e., servers, workstations, etc.), and
- Locate Access Control Lists (ACLs) on the network diagram (match them up with devices).

Network diagrams can be used to see an overall picture of the network and can identify vulnerabilities quickly. The gathered information should be controlled according to the Document Control Plan.

5.8.2 SCADA System Characterization

Detailed questionnaires (see Appendix F) help both the training of personnel in the process as well as completing the various pairwise decision matrices. The questionnaires are not restrictive in scope, but do ensure a minimum threshold of knowledge about the security of a particular SCADA system before completing the relative ranking process. CobiT®, the generic depiction of a secure water SCADA system, and previous assessment experience all influence the type and level of questions developed for the assessment process.

5.8.3 Relative Ranking Process

The first step in the relative ranking process requires identification of the system assets, which are delineated into two general classes, technology and operations/procedures. Each class of assets is ranked independently; hence, the final ranking consists of two lists. The generic depiction of a secure water SCADA system (Sandia is developing this model) helps in the asset determination process. Table 5.5 depicts examples of typical assets.

Table 5.5. Examples of Water SCADA System Assets

Physical/Hardware Assets	**Operational/Procedural Assets**
Cables (fiber optic, copper)	Security Policy*
Ethernet Switches	Configuration Management*
ATM Switches, Frame Relay, etc.	Security Training*
Routers	
SCADA Servers	Security Plan*
Remote Network Connections	SCADA Network Management
Connections to other Organizations	Backup Configurations*
Internet Connections	Remote SCADA operations
Intrusion Detection Systems (IDS)	Skilled Personnel*
Data Protection Methods (encryption) #	SCADA Account Restrictions*
Data Separation (PVCs, VPNs, VLANs)	Control Data*
Firewalls #	Support Data*
Access Control Lists (ACLs) #	
RTUs, PLCs, IEDs	
Physical Protections of SCADA equipment*	
SCADA Network Architecture	
SCADA Terminals	
Wireless links (microwave, satellite, etc.)	
FEPs, IOCs	
Mux/Demux	
Modems	
SCADA Software	
Note “#' indicates a critical secure asset if SCADA network is not completely isolated.	Note: “*” indicates a critical security asset

Two classes of assets create two relative ranking lists, which support a more intuitive final result than simply including all assets in one list, and help in training new users of the approach. For example, understanding the relationship between security training and programmable logic controllers (PLCs) requires a level of abstraction, while the relationship between security training and security policy appears more direct.

Upon determination of the SCADA system assets, the relative ranking process proceeds as depicted in Figure 5.9. SCADA system assets provide the continuity within the ranking process and are viewed within the context of the SCADA system rather than as individual entities. For example, the vulnerability of a SCADA server depends on its function and location within the SCADA architecture, as opposed to viewing the server as a stand-alone device.

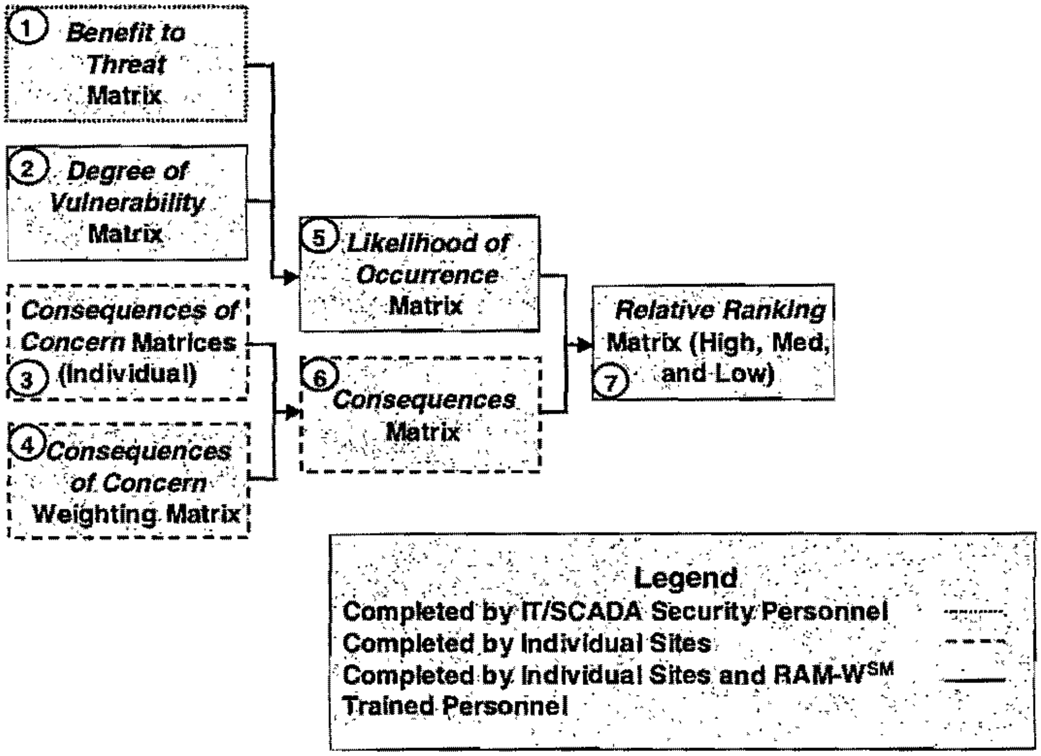

1 Benefit to Threat Matrix
2 Degree of Vulnerability Matrix
Consequences of Concern Matrices 3 (Individual)
4 Consequences of Concern Weighting Matrix
5 Likelihood of Occurrence Matrix
6 Consequences Matrix
Relative Ranking Matrix (High, Med, 7 and Low)
Legend
Completed by IT/SCADA Security Personnel
Completed by Individual Sites
Completed by Individual Sites and RAM-W^{SM} Trained Personnel

Figure 5.9. SCADA System Asset Relative Ranking Process

In the relative ranking process, pairwise decision matrices capture different viewpoints on the various assets of the system, with all matrices utilizing identical assets (with the exception of the *consequences of concern* weighting matrix). Descriptions of the matrices in Figure 5.9 reside in Table 5.6.

Table 5.6. Description of Relative Ranking Matrices

	Matrix	Brief Description
1	*Benefit to Threat*	• Assets pairwise compared on their ability to support adversary objectives • Considers sophistication level of the adversary
2	*Degree of Vulnerability*	• Completed for individual sites by RAM-W trained personnel and SCADA system administrators • Assets evaluated against secure SCADA baseline • Assets pairwise compared on their relative degree of security vulnerability
3	*Consequences of Concern* - individual	• A single, undesired consequence represented by a single matrix, e.g., loss of ability to provide potable water • Assets are pairwise compared on ability to bring about the consequence
4	*Consequences of Concern* - weighting	• Pairwise ranking of individual undesired consequences • Establishes relative importance between undesired consequences • Typically considers 4–7 undesired consequences
5	*Likelihood of Occurrence*	• Combination of *Benefit to Threat* and *Degree of Vulnerability* matrices • Output provides relative ranking on the potential compromise of assets
6	*Consequences* – combined	• Weighted average of individual *Consequences of Concern* matrices • Output provides relative ranking of assets by consequences
7	*Relative Ranking*	• Indicates which assets warrant the greatest security improvement

Initial pairwise ranking of the assets occurs with respect to two categories: *degree of vulnerability* and *benefit to threat.* The pairwise ranking between assets utilizes the numerical values shown in Table 5.7.

Table 5.7. Numerical Ranking Values

Row Asset versus Column Asset	Numerical Value
greater than	5
equal (or non-distinguishable)	3
less than (or non-existent)	1

The *benefit to threat* category is developed by an understanding of water utility SCADA systems, combined with an understanding of which elements of the SCADA system are most beneficial to a threat or adversary's objectives. The following questions are considered when filling out the *benefit to threat* matrix:

1. What are the malicious activities that can compromise the SCADA system?
2. Which assets are used to support these malicious activities?

Then the pairwise decisions are made as to which assets are generally most beneficial to the threat. Note: this can done for each individual attack scenario and then averaged for the final result, or estimated by the expert without the formal decomposition of each individual attack scenario.

The *degree of vulnerability* matrix is developed from data gathered about a particular SCADA system, with analysis of the data guided by the general notion of a secure SCADA approach (Sandia National Laboratories is in the process of creating a generic secure SCADA Model), relative CobiT® control objectives, and general information security best practices. Results from the detailed questionnaires guide pairwise decisions in regards to differentiating vulnerability levels between assets. The sophistication level of the threat should be considered in the decision process, but detailed knowledge of specific attacks is not necessary. Detailed attack information is captured in the *benefit to threat* matrix.

Examples of these two rankings follow below (Tables 5.8 and 5.9). To interpret the table, select an asset from the left most column, follow the row until it intersects the column of the asset for comparison, and determine the relation between the two assets. For example (see shaded area), in Table 5.8:

1. Select the "Physical Cabling" row;
2. Follow the row across until intersecting the "Internet Connections" column
3. Read the value of 1; *Interpret the relationship*, as "Internet Connections are more beneficial to a threat (adversary) than Physical Cabling."

The SCADA assets in these matrices represent a subset of the physical assets depicted in the example water utility described in Appendix A. Results from the onsite SCADA interview (Section A.7) and the SCADA network diagrams provide the information used in completing the pairwise decisions. For example, operating system (OS) security patches are not maintained on the SCADA platforms, and the modems are enabled on those servers. The RTUs are only reachable by a console port or through the SCADA network and do not utilize a standard OS such as Windows NT, Unix, etc. This information dictates the decision that the SCADA servers are more vulnerable than the RTUs. (See Table. 5.9, row 1, column 3.) Note: the matrices used in this explanation do not include all the physical assets of the example water utility system. In addition, a parallel analysis would be necessary for the operational assets.

Table 5.8. Example of Benefit to Threat (Adversary) Matrix

Benefit to Threat	SCADA Server(s)	RTUs	Firewalls	Physical Cabling	Physical Protections	Internet Connections	**Raw Totals**	**Normalized**
SCADA Server(s)		5	5	3	5	3	21	0.23
RTUs	1		5	3	1	1	11	0.12
Firewalls	1	1		3	5	1	11	0.12
Physical Cabling	3	3	3		3	1	13	0.14
Physical Protections	1	5	1	3		1	11	0.12
Internet Connections	3	5	5	5	5		23	0.26
						Total	90	1.00

Table 5.9. Example of Degree of Vulnerability Matrix

Degree of Vulnerability	SCADA Server(s)	RTUs	Firewalls	Physical Cabling	Physical Protections	Internet Connections	**Raw Totals**	**Normalized**
SCADA Server(s)		5	5	3	3	3	19	0.21
RTUs	1		3	3	3	1	11	0.12
Firewalls	1	3		3	3	1	11	0.12
Physical Cabling	3	3	3		5	5	19	0.21
Physical Protections	3	3	3	1		1	11	0.12
Internet Connections	3	5	5	1	5		19	0.21
						Total	90	1.00

The results of the two matrices above (i.e., the last column) are multiplied to form the relative likelihood of occurrence, which provides one of the inputs to the relative risk analysis. For this example, Table 5.10 below depicts the results of this calculation, with the inputs normalized for the calculation process, and the final result normalized for subsequent calculations in the process.

Table 5.10. Example Calculation of Relative Likelihood of Occurrence

Criteria Assets	Benefit to Threat	Degree of Vulnerability	Relative Likelihood of Occurrence
SCADA Server(s)	0.23	0.21	0.05
RTUs	0.12	0.12	0.01
Firewalls	0.12	0.12	0.01
Physical Cabling	0.14	0.21	0.03
Physical Protections	0.12	0.12	0.01
Internet Connections	0.26	0.21	0.05

5.8.4 Pairwise Ranking of Assets in Relation to Consequences

The Consequences category of the analysis is initially decomposed for the ranking process into specific consequences of concern. As in the previous rankings, pairwise decisions are made on the assets of the SCADA system with regard to a particular element or criteria of the decomposition. The decomposition follows directly from the initial Consequence Assessment from Section 5.6. A typical decomposition is as follows.

Consequences:

1. Interrupt or impair water flow in the system
2. Contaminate water
3. WMD-type event

After an initial ranking, the individual results are recombined subject to the relative weights of the consequences. An example of pairwise weighting values is shown in the Table 5.11, with all consequences receiving equal weighting. The example water utility considers the three typical consequences listed above and utilizes equal weighting between these three consequences.

Table 5.11. Consequence Weighting Matrix

Criteria Criteria	Interrupt or impair water flow in the system	Contaminate water	Weapon of mass destruction-type (WMD) event	Raw Score	Relative Decision Value
Interrupt or impair water flow in the system	■	3	3	6	0.33
Contaminate water	3	■	3	6	0.33
Weapon of mass destruction-type (WMD) event	3	3	■	6	0.33
			Total	18	1.00

Assets are ranked in terms of their ability to affect each of these consequences of concern. The pairwise decisions are made on the significance of the role a particular asset plays in bringing about the consequence. For example, in order for the SCADA system to cause the "Interrupt or impair water flow in the system" consequence, the SCADA server must be compromised. Table 5.12 follows from the example water utility in Appendix A and depicts the pairwise decisions for the "Interrupt or impair water flow in the system" consequence.

Table 5.12. Example of Interrupt or Impair Water Flow in the System

Interrupt or impair water flow in the system (1)	SCADA Server(s)	RTUs	Firewalls	Physical Cabling	Physical Protections	Internet Connections	Raw Totals	Normalized
SCADA Server(s)		5	5	5	5	5	25	0.28
RTUs	1		5	5	5	5	21	0.23
Firewalls	1	1		1	3	1	7	0.08
Physical Cabling	1	1	5		5	3	15	0.17
Physical Protections	1	1	3	1		1	7	0.08
Internet Connections	1	1	5	3	5		15	0.17
						Total	90	1.00

To reach the final relative ranking, the consequences of concern are recombined to form the Consequences relative ranking. Table 5.13 below illustrates the combination of the four consequences used in this example. The values are normalized for the calculation process.

Table 5.13. Example of Combined Consequences Matrix

Consequences	Interrupt or impair water flow in the system (1)	Contaminate water (2)	Weapon of mass destruction-type (WMD) event (3)	Consequences Weighted Total
SCADA Server(s)	0.28	0.26	0.26	0.26
RTUs	0.23	0.26	0.19	0.23
Firewalls	0.08	0.10	0.10	0.09
Physical Cabling	0.17	0.10	0.14	0.14
Physical Protections	0.08	0.17	0.14	0.13
Internet Connections	0.17	0.12	0.17	0.15
			Total	1.00

5.8.5 Generate Relative Risk Rankings

The individual consequences are combined into one matrix called Consequences by a weighted average calculation indicated in the previous step. The output of that calculation represents the aggregate rankings of assets within each consequence criteria. (See Consequences Weighted Total column in Table 5.13 above.) The final step requires multiplication of the

Relative Likelihood of Occurrence and the Consequences results. Table 5.14 below shows the results from the example used in this document. Again, the values are normalized for the calculation.

Table 5.14. Example of Relative Risk Calculation

Criteria Assets	Consequences	Relative Likelihood of Occurrence	Relative Risk	Normalized Relative Risk
SCADA Server(s)	0.263	0.049	0.013	0.405
RTUs	0.226	0.015	0.003	0.105
Firewalls	0.093	0.015	0.001	0.043
Physical Cabling	0.137	0.030	0.004	0.131
Physical Protections	0.130	0.015	0.002	0.060
Internet Connections	0.152	0.054	0.008	0.256
		Total	0.032	1.00

An example of relative risks for critical physical assets is shown in Table 5.15. The final ranking of assets occurs by listing the assets in descending order according to their computed relative risk value. A final ranking based on the computed risk values identifies where resources should be applied to improve the security of the system with assets in the High category warranting the most attention. In Table 5.15 below, the SCADA servers belong to the High category, followed by the Internet Connections in the Medium category. The remaining assets fall into the Low category. This final relative ranking list indicates where the example water utility should focus SCADA security improvement efforts.

Table 5.15. Example of Relative Ranking for Physcial Assets

Final Relative Ranking	Relative Security Vulnerability
SCADA Server(s)	High
Internet Connections	Medium
Physical Cabling	Low
RTUs	Low
Physical Protections	Low
Firewalls	Low

This process requires identification of SCADA system assets, and the ranking of those assets over a variety of criteria, and within the context of the system. Accurate and meaningful questions to assist or guide the ranking of the assets are a key aspect necessary to make this process effective in a self-assessment effort, particularity in the areas not involving security experts.

A final, prioritized list of SCADA system assets indicates an order for applying resources to improve SCADA security. As in the initial assessment activities, the depiction of a generic secure water SCADA system helps identify possible mitigation approaches and ensures that the proposed mitigation approaches function within the system as a whole. The inclusion of CobiT® supports the integration of any mitigation strategies with the overall business objectives of the particular water utility.

5.9 Onsite Chemical Characterization

5.9.1 Contamination of Water with Onsite Chemicals

An example analysis of the onsite chemicals is included here to determine the potential consequences of malevolent events using already available chemicals. Various scenarios are presented and discussed on how an adversary might impact the water utility through:

- Affecting chemical feed rates
- Intentional misuse of the chemicals
- Combining chemicals

Treatment chemicals, in high enough doses, can constitute a threat for employees and the neighboring community. This analysis is an attempt to categorize and identify the level of risk from onsite chemicals. This is not an analysis involving the introduction of an outside agent into the water system; it only addresses using the chemicals available on site. This section will not discuss access and will assume that either an insider or an outsider with sufficient knowledge can access the raw/finished water and contaminate the stream. An average flow through the various parts of the system will be needed to perform the calculations. For Treatment Plant 2, the rates are 90 mgd. The chemicals used are contained in storage tanks, or individual containers, which are then fed via metering systems (or injected directly) into the water flow. Dispersing the entire contents of all storage tanks into the system rapidly (beyond the speeds of the metering pumps) would require plumbing of bypass lines into the water flow. In most cases, this would not be practical due to the distance of the storage tanks from the water injection system, the requirement to do a hot tap on a line full of pressurized hazardous chemicals, the need to provide long pieces of large O.D. pipe, and the time required to complete this task when there are simpler ways to disrupt the system.

The following analysis will assume that an adversary could dispense onsite chemicals at the maximum possible flow rate into the water system for an entire day, undetected. The focus of this investigation is with short-term threats—not with long-term 10–20 year threats (cancer). Table 5.16 defines several terms used in the analysis.

Table 5.16. Toxicology

LD_{50}	Lowest dose to cause 50% mortality in test subjects.
LD_{Lo}	Lowest known dose to cause mortality (human).
TD_{Lo}	Lowest known dose to cause exhibited symptoms (human)
(pulm)	Inhalation dosing.
(i.p.)	Intraperitoneal injection dosing
(i.m.)	Intramuscular injection dosing
(i.v.)	Intravenous injection dosing
(oral)	Oral dosing

LD_{50} is the concentration of a chemical dose (expressed on a weight basis of contaminant to body mass, mg/kg of body weight) that killed 50% of the test subjects. All LD_{50} values are oral unless otherwise noted. Some, but not all, are actual human values. In cases where multiple species exhibited different susceptibilities to the chemical, the lowest LD_{50} is reported to be conservative. LD_{Lo} is the lowest known lethal dose for humans and TD_{Lo} is the lowest dose of a substance introduced by any route other than inhalation over any given period of time and reported to produce any toxic effect in human. Looking at the graph in Figure 5.10 and the straight line drawn onto the graph, it is obvious that the LD_{50} does not offer a linear method to determine the point at which there will be zero fatalities. Nor can an adversary be assured of killing all individuals by simply doubling the dose. Minor amounts of most substances, no matter how toxic, can be tolerated without fatality.

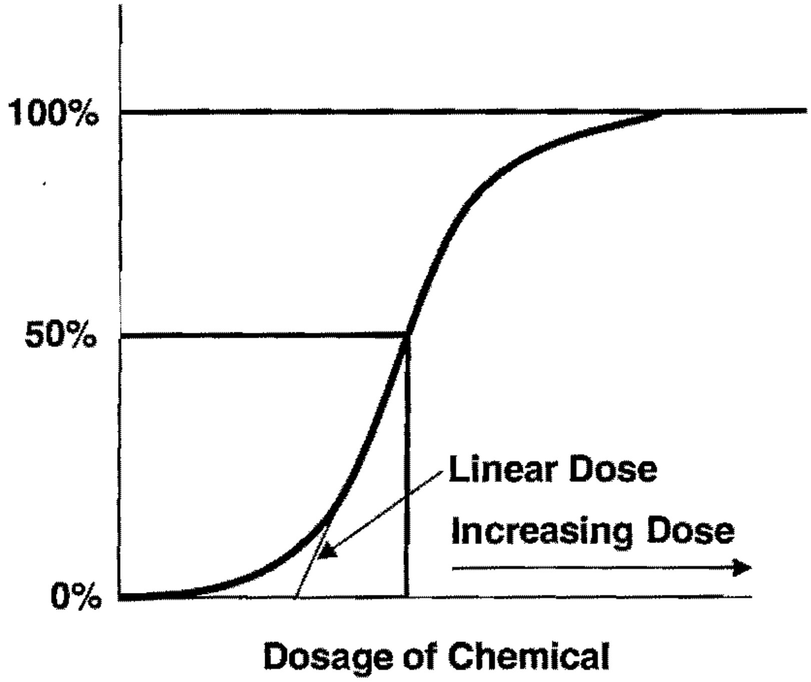


Figure 5.10. Dose vs. Toxic Chemical. % of Subjects Exhibiting Response vs. Dosage

Some assumptions need to be made to create an anticipated dosage that an adversary would like to achieve to harm the users of the system. An average "person" will be 100 kg and an average child will be 10 kg to make the numbers easier to calculate. Typical adults would actually be closer to 70 kg (as defined by the EPA), but the accuracy of the dosage will not be precise enough to matter significantly, particularly when the stated amounts are LD_{50} and the intention is to deny the potential for more than a few deaths. The amounts of material in the water will be expressed as parts per million (ppm), which is 1 mg/kg of contaminate/kg of solution. If the level of contamination is 10 ppm, then 1 liter (approximately 1 kg) consumed would represent 10 mg of material ingested. Toxicity is mg ingested per kg of body weight. A 100-kg man would suffer adverse health effects at 10 mg/100 kg or 0.1 mg/kg. A child, however, would be 10 mg/10 kg or 1mg/kg. If the caculated lethal dose is 0.5 mg/kg, the adult would be below the lethal dose, but the child would be above the lethal dose (i.e., lethal to the child but not the adult)

Table 5.17 lists chemicals stored on site for Treatment Plant 2, assuming that the maximum storage limits have been reached. The chemical is listed as well as the stated weight percent (wt %) as delivered to the water utility. The active amount is defined as the amount of chemical of interest in the solutions and is obtained by multiplying the wt% with the amounts of chemical being stored or using the density if the reported amounts are not in mass units. The daily max feed is based on pumping rates for that chemical (see Table 5.18). Pumping limited is an indication whether the pumps can empty the complete inventory over a 24 hr period. This is determined by pumping rates as well as delivery methods for the chemical. If the installed pumps can deplete the inventory, then the entire active chemical inventory is considered in the dosage calculation. The day-long levels are then determined from the amount of active chemical that can be released over 24 hours assuming a constant water flow and chemical injection rate for the facility.

Table 5.17. Chemicals Stored Onsite at Treatment Plant 2

Chemical	Maximum Storage	(wt %)	Solution Density	Active amount (kg)	Daily max feed (kg/day)	Pumping Limited	Day long levels (ppm)
Ammonia (water solution)	16,000 gal	20 wt%	0.9 kg/l	10,944 kg	2736	Yes	8
Chlorine	20,000 lb	100	NA	9091 kg	4090	Yes	12
Potassium permanganate	5 bins (9,900 lb)	100	NA	7500 kg	3300	Yes	9.6

Note: these numbers are for distribution from the bulk and do not represent the active amounts of chemicals.

Table 5.18. Maximum Feed Rates for Chemicals into Water

Chemical	Number of pump/feeders	Total max feed all pumps	Limitations
Chlorine	2	10,000 lb/day	Vacuum limited to 9,000 lb/day
Ammonia	2	4000 gal/day	May not be able to run both pumps at full max
Potassium Permanaganate	1	3300 lb/day	Container would need to be changed to empty more than one bin

5.9.2 Specific Chemicals (liquids/solids)

All the toxic limits and values listed below (and in the following sections) were obtained from The Merck Index, 12th edition, or Section 11 (toxicological information) from the Material Safety Data Sheet for the chemical.

Typically, ammonium hydroxide solution is used to react with chlorine to form chloramines, a residual disinfectant to protect the water in the distribution system. It is injected directly into the water at the very end of the process treatment stream.

16,000 gal ammonia solution (3.8 l/gal)(0.9 kg/l)(0.2 wt ratio)=10,944 kg of NH_3 *available*

The pumps can only dispense 4,000 gallons in a 24 hr period so only ¼ of the above active amount needs to be considered (2,736 kg NH_3). This amount is distributed in 90 mg of water.

$$\frac{2.736 \times 10^3 \text{ kg } NH_3 \,(10^6 \text{ mg/kg})}{9 \times 10^7 \text{ gallons } (3.8 \text{ l/gallon})} = 8 \text{ (mg/l) ppm}$$

Therefore, a total level of 8 ppm would be present if the pumps are operated at the maximum injection rate for an entire day. The LD_{Lo} for ammonia (as ammonium hydroxide solution) is 43 mg/kg. The TD_{Lo} is 0.09 mg/kg. Assuming a 1-liter dosage, a 10-kg child would ingest only 0.8 mg/kg, which is about ten times above the lower limits of toxic response (most likely exhibited as nausea) and well below the lowest known lethal limit. It is unknown whether 8 ppm in water would be detectable by smell. Human detection limits are around 53 ppm_v in air (for ammonia gas, NH_3). Since the dosage is more than 50 times less than the LD_{Lo}, it is not considered a significant threat for ingestion that would produce fatalities.

Potassium permanganate is used as an algaecide in the fall/summer to decompose some of the humic load from organic material in the incoming water (strong oxidizer) at the intake for Treatment Plant #2. It also is employed to address taste/smell concerns and to oxidize Fe^{+2} to Fe^{+3} so that it is easier to remove with standard flocculation aids. A screw auger system is used to dispense the material and is limited to one container at a time. Using the Treatment Plant 2 water flow rates, a 9.6 ppm level can be achieved during a 24-hour period and possibly higher if the dispenser can be emptied faster. The TD_{Lo} for $KMnO_4$ is 1.4 mg/kg , 100 ppm for the LD_{Lo}. A child drinking 1 liter of water would be dosed at 0.96 mg/kg. This is below the threshold level and substantially below the lowest known lethal level. This chemical has to be reduced as a perceived vulnerability because it is being used in the direct treatment of incoming water rather than as a post treatment step. Therefore, the general treatment steps may mitigate this as a threat. A more likely potential threat is the use of this as the oxidizer in either a fire attack or as a component of an explosive mixture if mixed with an appropriate fuel. Initial dispersion of MnO_2

into the water creates a deep purple color; at higher concentration levels, the water turns black. This should also deter customers from drinking the water.

5.9.3 Specific Chemicals (gases)

Method of introduction makes dispersion of gaseous materials, outside the normal injection system, very difficult to achieve. The assumption will be that it can be performed efficiently at maximum feed with the system injectors. The analysis will then estimate the consequences.

Chlorine gas is the primary disinfectant and maintains residual disinfection within the water distribution system. It is injected via a vacuum supply system controlled by water flow. The chlorine gas in this system is delivered as a gas over a liquid in 2000 lb of (primarily liquid) elemental chlorine. These tanks are pressurized to about 80 psi at room temperature and are not cooled. Each tank contains two valves, one for dispensing liquid and another for dispensing gas. There is also a fusible lead plug designed to melt/blow out if pressure/temperature of the tank becomes too high for the container to handle. This limits the amount of shrapnel produced during a pressure event but does not prevent the gas from escaping. Calculations (and information from the manufacturer of the container) have indicated that Joule-Thompson cooling would work to seal small leaks in the tanks in the event of an accident. The company that manufactures the containers includes repair kits to seal small leaks in the tanks by trained personnel using appropriate safety equipment. If the gas injector system is used at the maximum feed rate , the concentration throughout the day can be maintained at 8 ppm (ignoring incoming/system biological and organic oxidation load). The solubility limits for Cl_2 in water at 25 ^{o}C are 4.39 gm/l or 4390 ppm, the limits for the secondary product (HOCl) is 1.58 gm/l or 1,580 ppm. Therefore, solubility is not limiting for this scenario. Chlorine is detectable at 0.08 ppm_v in air and causes mucous membrane irritation at 0.2 ppm. The OSHA inhalation limit is 1 ppm_v (pulm) and 25–50 ppm_v (pulm) is considered a dangerous level. Chlorine appears to be much less toxic when ingested than when inhaled. The oral rat TD_{Lo} is 42 gm/kg continuous over 2 weeks. Since most people can detect around 0.5 ppm of chlorine in water (by smell), it is not likely that this feed rate would be maintained for more than a few hours. Once water has a "bleach" smell to it, it is also less likely to be ingested. Over-chlorination of the water is not a likely threat in terms of injuring the customers.

5.9.4 Potential Reactions

Since many of the chemicals are hazardous in sufficient concentration on site, they will not be discussed individually. However, there may be some potential for reacting two or more components to form an unrealized toxic hazard or a strong exothermic event. Since many of the chemicals are contained and delivered in water slurries, the exothermic potential for the reaction is not as likely. Most mixing scenarios would require a contained common area that would need to be plumbed from each tank. This is not a significant threat unless one tank could be directly fed into another tank, but then the concern is more about a tank rupture and subsequent chemical release event than a chemical contamination of the water event.

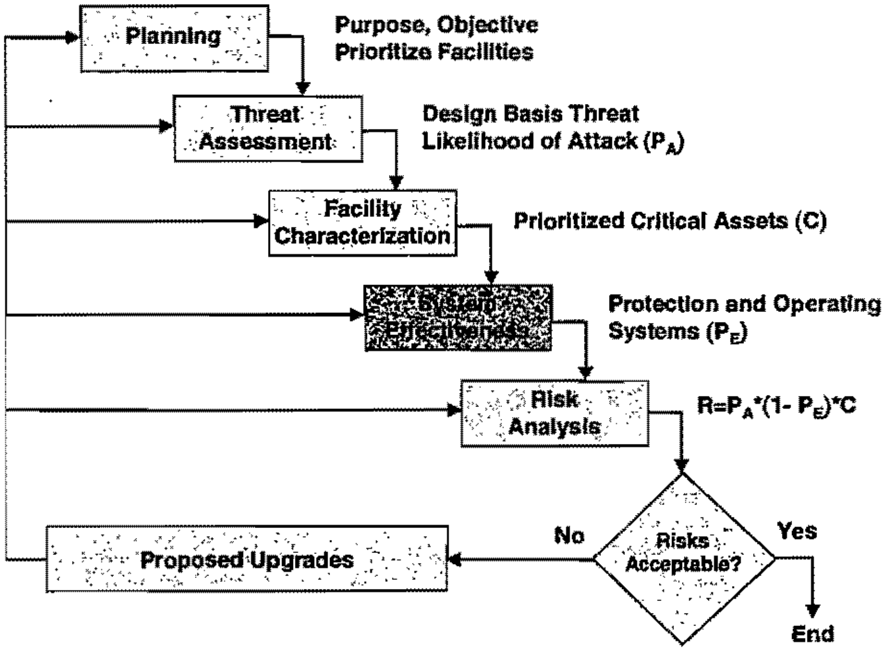
5.9.5 Incorrect Tank Fill

This threat is related to the situation where an outsider is looking to destroy one of the onsite tanks through deliberate introduction of a chemical agent that would have a catastrophic interaction with the tank contents. This would be disruptive, but not likely to interrupt the ability of the plant to treat water. Another possible threat is the introduction of a (pressurized) reducing agent or fuel to the chlorine manifold system. This could cause a rupture that would endanger plant personnel and cause a chlorine release, and it may be powerful enough to deny access to the plant and inhibit purification of the water. Destruction of a single tank by itself would not likely stop the plant from operating unless it also damaged some of the non-redundant systems or an entire manifold of tanks.

5.9.6 Conclusions for Treatment Plant Chemicals

Unless temporary piping/pumping arrangements were installed by an adversary, the onsite chemicals at Treatment Plant 2 would not pose an immediate contamination health risk to consumers. Rupture of multiple chlorine gas cylinders that would overwhelm the chlorine storage area scrubber system is a concern for the surrounding community. Any catastrophic rupture of chemical storage tanks without sufficient safeguards (containment berm or dams) is a potential method for quick introduction of a "slug" of contaminates (to the air or the water). Whereas this is undesirable for many reasons, it is not likely to occur unnoticed. Quick detection through either employees witnessing the event or spikes in detection equipment should give the water utility sufficient time to warn their customers.

6 PHYSICAL PROTECTION SYSTEM DESCRIPTION



Waterfall Flow Diagram – Process Locator

In the next chapter (Chapter 7, System Effectiveness), the assessment team will need to estimate how effective the physical security elements will perform with respect to the DBT. To assist in the analysis, this chapter provides information on how an effective Physical Protection System (PPS) is designed, installed, and operated. An effective PPS will:

- Provide protection in depth,
- Provide balanced protection, and
- Minimize the consequence of component failure.

Expert opinion is a good starting point for evaluating security systems, but only performance testing can ensure that the system will work as designed.

The PPS objective should be to prevent the accomplishment of a malevolent action. However, because of the significant delays inherent in some water utility operations, the objective may be to detect malevolent action with a high degree of probability and then follow an emergency response plan. Preventing malevolent actions can be accomplished by either deterrence or a combination of detection, delay, and response. For a system to be effective, there must be notification and assessment of an attack (detection), the adversary progress must be slowed (delay), and the response force time short enough to interrupt or stop the adversary (response). The primary functions of a PPS (detection, delay, and response) and some of their components are shown in Figure 6.1. The key to a successful PPS is the integration of people, procedures, and equipment into a system that protects assets from malevolent adversaries.

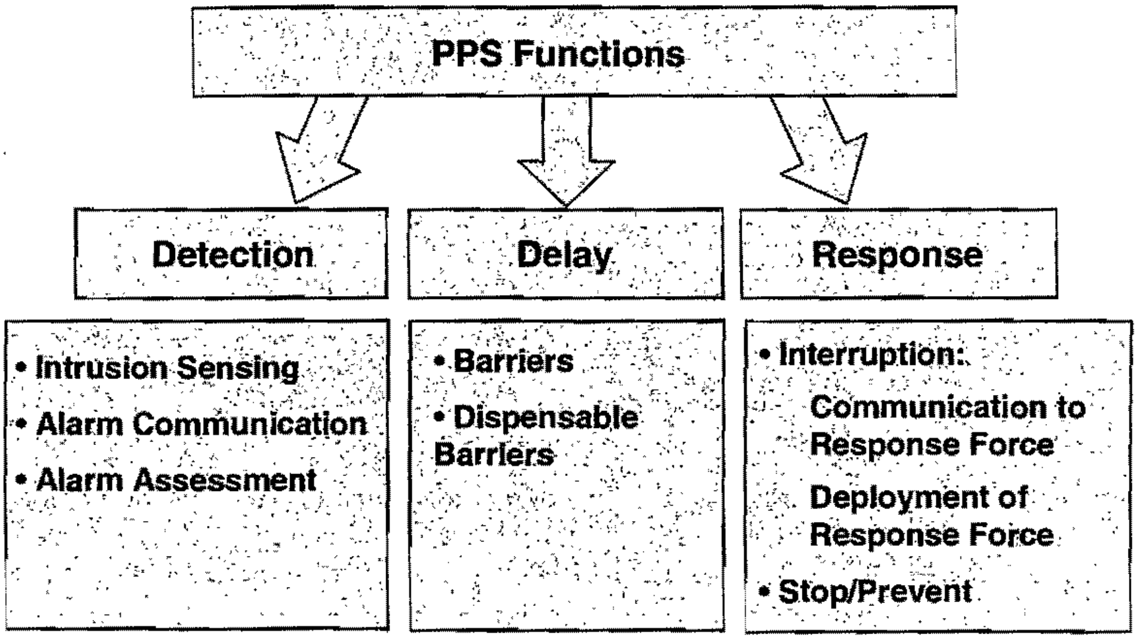


Figure 6.1. Functions of a Physical Protection System

6.1 Design and Evaluation Process Outline

A graphical representation of the Design and Evaluation Process Outline (DEPO) for a PPS is shown in Figure 6.2. The process starts by determining the PPS objectives. The next step is to design a PPS system to meet those objectives. Finally, an evaluation is undertaken to determine how well the system performs.

The remainder of this chapter will focus on discussing the primary PPS functions of detection, delay, and response. The system functions will be considered in detail, since a thorough understanding of these functions and the measure of effectiveness of each is required to evaluate the system.

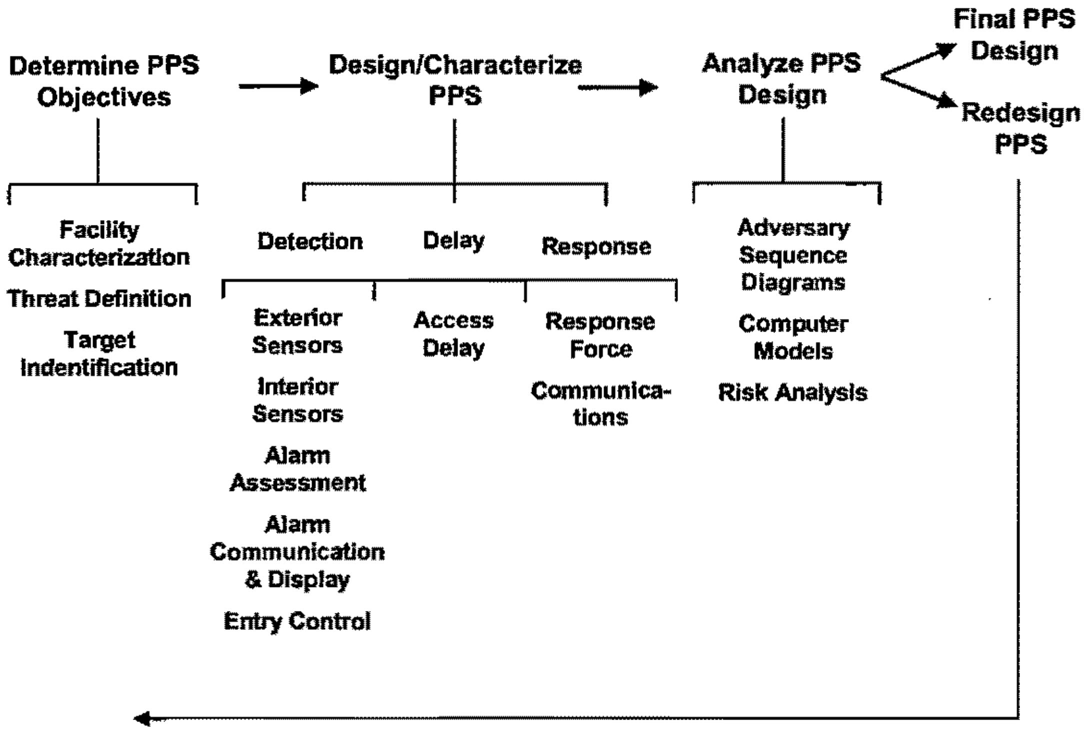


Figure 6.2. Design and Evaluation Process Outline (DEPO)

6.1.1 Detection

It is important to understand that detection includes assessment (i.e., detection without assessment is not detection). The first required function of a security system is the discovery of adversarial action, which may be either covert or overt. To detect an adversarial action, the following events must occur:

- Sensor (equipment or personnel) reacts to an abnormal occurrence and initiates an alarm.
- Information from the sensor and assessment subsystems is reported and displayed.
- Someone assesses this information and determines the alarm to be valid or invalid.

These events are depicted in Figure 6.3. Methods of detection include a wide range of technologies and personnel. Entry control (a means of allowing entry of authorized personnel and detecting the attempted entry of unauthorized personnel and contraband) is included in the detection function of PPS. Because entry control includes locks in some cases, it may also be considered a delay factor. Entry control to various areas of the water utility should be designed to filter and reduce the population that has access to critical assets. Security guards or other personnel also can accomplish detection.

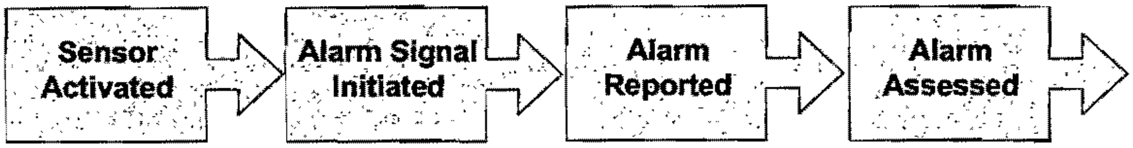


Figure 6.3. Detection Functions in a PPS

An effective detection assessment subsystem provides two types of information associated with detection:

- Information about whether the alarm is a valid alarm or a nuisance alarm.
- Details about the cause of the alarm (i.e., what, who, where, and how many).

It is important to recognize that detection must be accomplished for delay to be effective. The performance measures for detection are:

- Probability of detection
- Time for communication and assessment
- Frequency of nuisance alarms

The probability of detection refers to the likelihood that a given detection subsystem will be effective against the DBT. Fence sensors and other outdoor sensors that are clearly visible may work against an unsophisticated adversary, but may provide little or no protection against a more sophisticated adversary. This is why having an understanding of the DBT capabilities and performance testing the PPS are so important. Good perimeter design systems that will detect more sophisticated adversaries may require covert systems to work in concert with the overt systems to be successful.

The time for communication and assessment includes the time for the alarm to be processed by the system, the time for someone to be alerted, and the time for someone to assess the alarm. For example, if a door alarm were received at a remote facility, it would take time for the alarm to be received and processed. The security force then has to monitor the assessment subsystem, most likely a camera, to see if the alarm is valid.

All alarms have to be treated as valid until they can be assessed and shown to be a nuisance alarm. Nuisance alarm rates are critical statistics to be logged by the water utility. High nuisance alarm rates will eventually render the performance of the entire security system ineffective. Malfunctioning alarms must be corrected as quickly as possible.

6.1.2 Delay

Delay is the second required function of a security system and is designed to impede adversary progress. Delay can be accomplished by fixed or active barriers (e.g., doors, vaults, and locks) or by sensor-activated barriers (e.g., dispensed liquids, smoke, or hardware). The security guard force can be considered an element of delay if personnel are in fixed, well-protected positions. Figure 6.4 summarizes the function of delay in a PPS. The performance measure for delay is time to defeat obstacles.

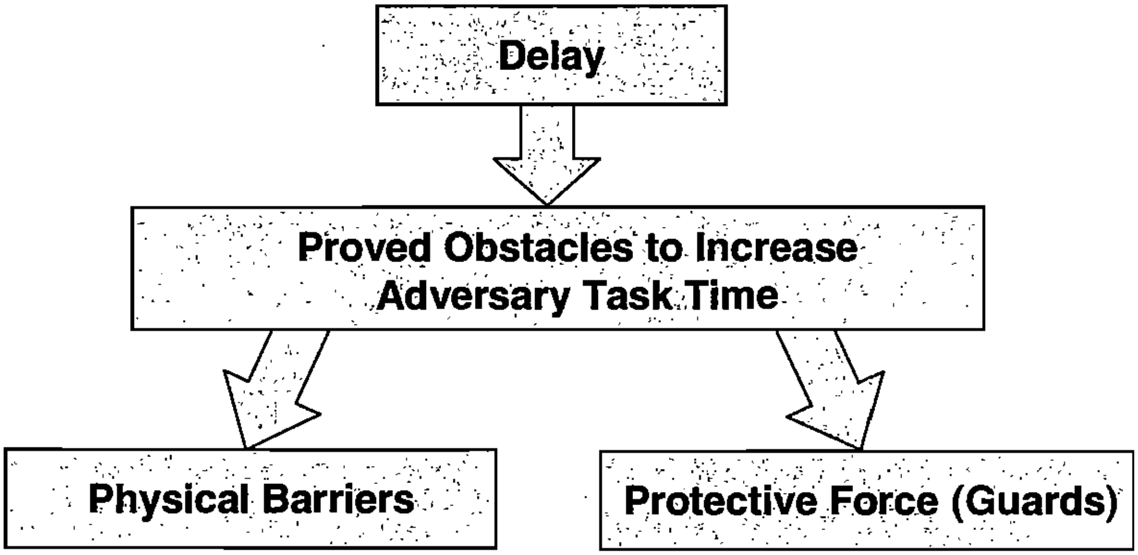

Delay
Proved Obstacles to Increase Adversary Task Time
Physical Barriers
Protective Force (Guards)

Figure 6.4. Delay Function

The time to defeat an obstacle will be dependent on the adversary capabilities. If a highly effective detection system is in place, delay elements can be designed to slow down or stop the adversary. For example, if the adversary only has small amounts of explosives available and the delay element requires large amounts to damage/destroy the barrier, the system will be very effective. Note the importance of the detection function. If the adversary can make repeated attempts without intervention, it will eventually defeat the delay element.

6.1.3 Response

Response involves actions taken by the security force (facility guards, police, or law enforcement) to prevent adversarial success. Response consists of *interrupting* and *stopping* the adversary. The measure of response effectiveness is the time between receiving a communication of an adversarial action and interrupting and stopping it. An effective security system must be able to detect the adversary early and delay the adversary long enough for the response to arrive and stop the adversary. The PPS response function is shown in Figure 6.5. Performance measures for response are:

- Probability of accurate communication to response force
- Time to communicate
- Probability of deployment to adversary location
- Time to deploy
- Response force effectiveness

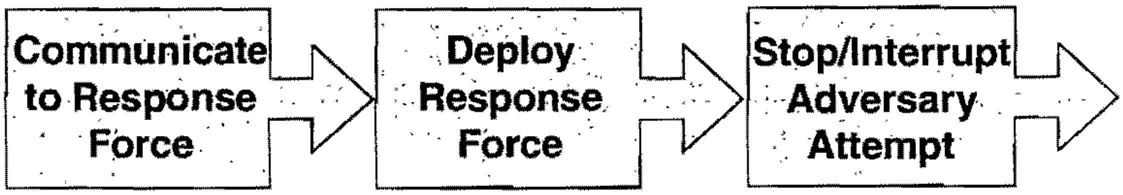

Communicate to Response Force
Deploy Response Force
Stop/Interrupt Adversary Attempt

Figure 6.5. Response Function

The first effectiveness measure for the response function is the probability of accurate communication to response force. If the alarm is considered just another nuisance alarm, then the communication will not take place. The person monitoring and assessing the alarms must be trained to react quickly and treat every alarm as valid. The procedure for communicating the alarm has to be written down and practiced. The security guard should have ready access to the response force on an open communication system. Dialing numbers or running down a list of parties to contact will cost valuable time in the event of an actual emergency, especially considering the stress of the situation.

The PPS must give accurate information to the security guard monitoring the system and allow deployment of the response force to the correct location. The time to deploy is likely the variable requiring the greatest amount of time in the response function. Water utilities must develop good working relationships with local law enforcement to reduce this time as much as possible. Conducting exercises with local law enforcement to make sure it understands the location of critical assets and how to quickly protect them is crucial. The effectiveness of the response force will be linked to the effectiveness of the assessment subsystem during the detection function. The response force will require resources and procedures dependent on the type and number of adversaries that attack. If the response force does not have accurate information or authority, their ability to defeat the adversary will likely be low at best.

6.2 Mitigation

System effectiveness against the DBT is comprised of a physical security component (guards, fences, sensors, locks, and security policy and procedures) and an operational design component (engineered robustness, spare parts and equipment, operational alternatives, and engineering and operational policy and procedures). These two components are considered together in the analyses to estimate the overall system effectiveness term, P_E. In the case where the undesired event cannot be prevented by the security system (i.e., system effectiveness is judged to be low), risk can be reduced by mitigation features that reduce consequences (C). Mitigation features could include:

- Redundancy – have other ways of accomplishing a task if a critical asset is destroyed.
- Backup systems – have alternate systems to bring on line if an asset is destroyed.
- Spares – be able to repair a destroyed asset rapidly.
- Emergency Response Plans – have a pre-thought out and pre-planned set of actions to put into place immediately if an attack occurs.
- Administrative or Operational Changes – there may be administrative or operational procedures/policies that can help to reduce the importance of critical assets.
- Personnel and training – if personnel are trained in the emergency response plans and trained in recovering from an attack, then the consequence may be lower than originally assumed.
- Computer security policy – have emergency response plans in place for the SCADA operators to follow if the SCADA system becomes unavailable.

How well the security system prevents the adversary from achieving his/her goal is reflected in the term P_E. In cases where the security system cannot prevent the adversary from achieving the goal, but mitigation can occur after the fact, risk reduction should be reflected in the consequence term, C.

6.3 DETERRENTS

The role of deterrence in security has proven to be difficult to measure. The most effective deterrence is provided by an effective PPS.

> *Theft, sabotage, and other malevolent acts at a facility may be prevented in two ways—by deterring the adversary or by defeating the adversary. Deterrence occurs by implementing measures that are perceived by potential adversaries as too difficult to defeat; it makes the facility an unattractive target, so the adversary abandons or never attempts an attack. Examples of deterrents are the presence of security guards in the parking lots, adequate lighting at night, posting of signs, and the use of barriers, such as bars on windows. These are features that are often implemented with no additional layers of protection in the event of an attack. Deterrence can be very helpful in discouraging attacks by adversaries; however, it is less useful against an adversary who chooses to attack anyway. It would be a mistake to assume that because an adversary has not challenged a system, the effectiveness of the system has been proven. The deterrence function of a PPS is difficult to measure, and reliance on successful deterrence can be risky; thus it is considered a secondary function.* (Garcia, 2001)

As more research is done on the measurable and long-term value of deterrents, this data may be incorporated into protection system design. To date, however, there is no statistically valid information to support the effectiveness of deterrents. There are, however, studies that indicate that deterrence is not as effective after implementation as is hoped (Garcia, 2001).

6.4 Relationship of PPS Functions

Figure 6.6 shows the relationships between adversary task time and the time required for the PPS to do its job. The total time required for the adversary to accomplish his/her goal has been labeled Adversary Task Time; it is dependent upon the delay provided by the PPS. The adversary may begin the task at some time before the first alarm occurs (T_0). The adversary task time is shown before T_0 because delay is not effective before detection. After the alarm, the information must be reported and assessed to determine if the alarm is valid. The time at which the alarm is assessed to be valid is T_A, and at this time, the location of the alarm must be communicated to the members of the response force. Further time is then required for the response force to respond in adequate numbers and with adequate equipment to interrupt the adversarial actions. The time at which the response force interrupts the adversary is T_I, and adversary task time completion is T_C. For the PPS to accomplish its objective, T_I must occur before T_C. From this diagram, it is obvious that a PPS performs better if detection is as far from the critical asset as possible and delay elements are near the critical asset.

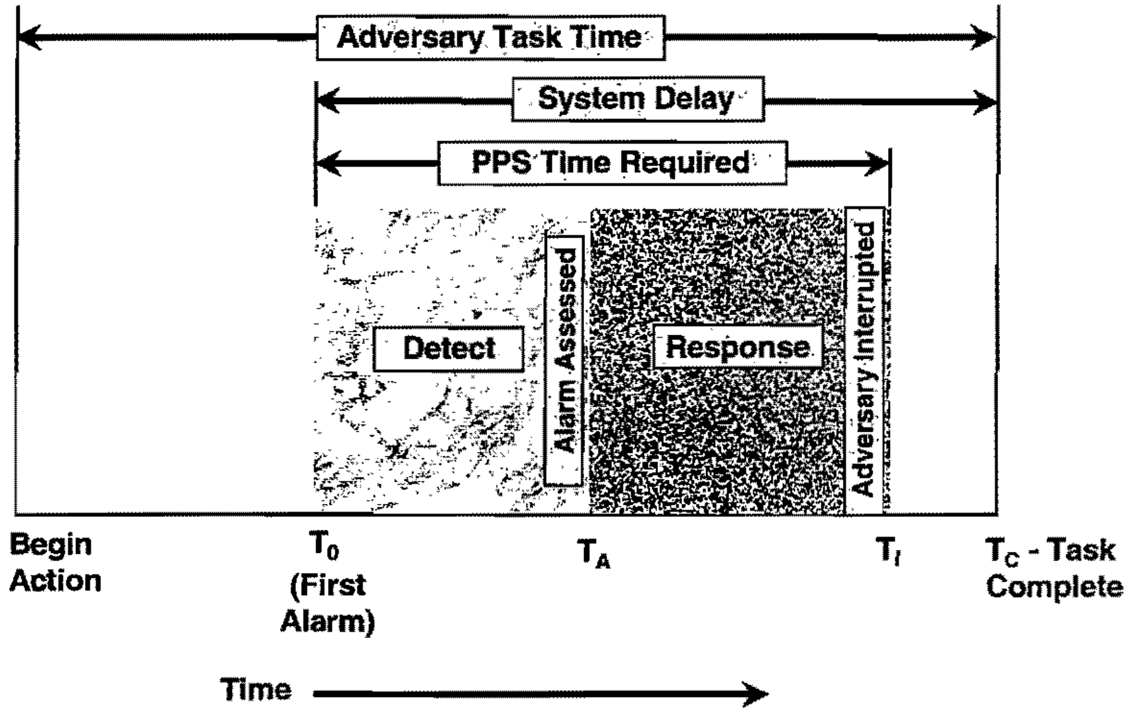


Figure 6.6. Interrelationship of PPS Functions

6.4.1 Interrelationship of PPS Functions - Example Water Utility

For the example water utility, a scenario likely to achieve the adversary's goal of reducing the ability to treat the water supply might be as follows: during non-operational hours (nighttime), after staging their equipment/weapons outside the property fence and observing no personnel in the area, the adversary cuts through the perimeter fence, runs across the property area to the building, and breaks into Treatment Plant 2 through a locked sensored door (using hand tools). Once inside the building, the adversary locates the pumps, preps the area, and plants 5 lb of high explosives on all the exposed pumps. The adversary sets the detonators, exits the building and property, and retreats to a safe haven before the explosives detonate. For this example, T_0 occurs at the first alarm (when the adversary entered through the sensored door). Assume that there are cameras in the building for assessment purposes. T_A occurs when the door alarm was activated, and a SCADA operator was able to assess the alarm and determine that unauthorized personnel with weapons had accessed the building. At this point, the SCADA operator would communicate the alarm and assessment to local law enforcement. Assume that the local law enforcement was trained (and tested) to respond to this type of malevolent act and could respond to the scene with adequate numbers and adequate equipment/weapons. If the response force could arrive on the scene and interrupt the adversary's activities before the explosives detonate, this would be T_I. T_C would occur before T_I if the response force could not arrive in time and the pumps had been destroyed.

6.5 CHARACTERISTICS OF AN EFFECTIVE PPS

Not only must all the hardware elements of the system be installed and operated properly, but they also must be maintained and tested. The procedures of the PPS must be compatible with the water utility's procedures and integrated into the PPS design. Effective training of personnel in policies, procedures, and operation of equipment is also important to system effectiveness. Security, safety, and operational objectives must be accomplished at all times. A well-engineered PPS will exhibit the following characteristics:

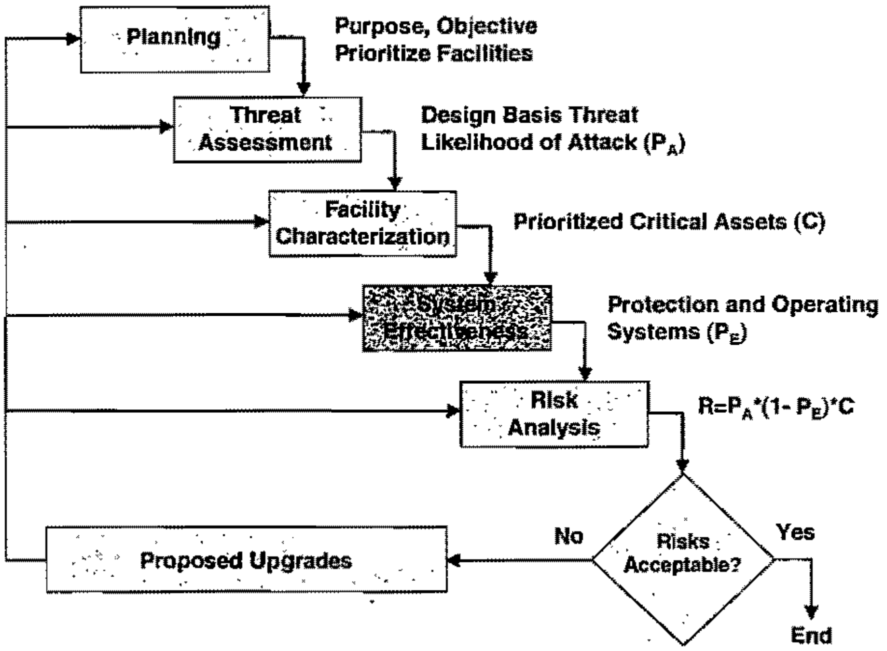
- Protection-in-depth (i.e., an adversary should be required to avoid or defeat a number of protective devices in sequence)
- Minimum consequence of component failure (contingency plans need to be in place

so the overall system continues to operate without interruption)

- Balanced protection (i.e., the minimum time required to penetrate each barrier is equal, and the minimum probability of detecting penetration of each barrier would be equal)

Detection, delay, and response are all required functions of an effective PPS. These functions must be performed in this order and within a length of time that is less than the time required for the adversary to complete their task. In addition, a design process based on performance criteria, rather than feature criteria, will select elements and procedures according to the contribution they make to the overall system performance. In feature-based systems, the effectiveness measure is often the absence or presence of security features. In general, performance-based design criteria are better than feature-based when measuring overall system effectiveness. Finally, performance testing is the only way to ensure that the system will work as designed.

7 SYSTEM EFFECTIVENESS



Waterfall Flow Diagram – Process Location

Analyzing how well the protection system (PPS and operating system) can defeat specific threats is part of the system effectiveness analysis. If the protection system effectiveness is judged to be low, specific vulnerabilities can be identified. The elements of system effectiveness analysis include:

- Describing the protection system.
- Determining the attack scenario most likely to achieve adversary goal(s).
- Estimating system effectiveness against the adversary for these attack scenarios.
- Identifying any protection system vulnerabilities.

7.1 Concept of System Effectiveness

In RAM-W^{SM} the term P$_E$ has been extended beyond the PPS to also consider contributions of non-physical security elements in determining system effectiveness (Figure 7.1). These non-physical security elements, referred to as operational elements, are elements that are intrinsic to the water utility itself or its operation. Even though they are not security elements, they are able to provide some level of detection, delay, or response towards preventing the adversary from achieving its goal.

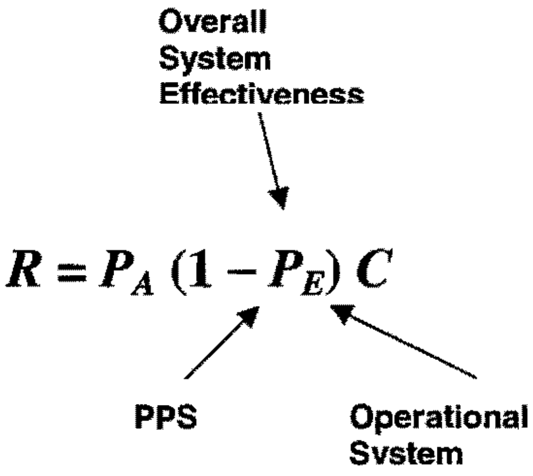


Figure 7.1. System Effectiveness, P_E

How well the protection system prevents the adversary from achieving its goal is reflected in the term P_E. There are cases where the protection system cannot prevent the adversary from achieving its goal (i.e., ill effects are felt beyond the system), but mitigation can occur after the fact. The effects of such mitigation should be reflected in the consequence term, C, of the risk equation. Adjustments to consequence will be discussed in Chapter 8. The assessment team must be careful not to take credit for proposed upgrades to the protection system in both P_E and C. The upgrades can be either for prevention or for mitigation, but not both.

7.1.1 Operating System Effectiveness for the Example Water Utility

In the example water utility, there are three pumps in operation at Treatment Plant 2 and a minimum of two is needed to meet the plant daily demand. For the example, assume that an adversary destroys two of the pumps. To avoid being detected by the security alarms on the door, the adversary breaks through the window to get inside the building. The adversary destroys two pumps, and the interruption of water flow from Treatment Plant 2 is picked up by the SCADA system. This detection by the SCADA system and assessment of the situation takes 1 hour (Figure 7.2). Since there are no backups stored on site, it will take 24 hours to replace one of the pumps (the third one was not destroyed). The 24 hours can be thought of as the System Response time. Pump Station 1 has 30 mg of storage with a pumping capacity of 40 mgd, and Pump Station 2 has 50 mg of storage with a pumping capacity of 80 mgd.

The System Delay time can therefore be thought of as the minimum of (50mg/80mgd*24hr/day, 30mg/40mgd*24hr/day), which is 15 hr. Even in the best case of a detection and assessment time of zero, one can see that the System Response time will have exceeded the System Delay time. The protection system could not prevent the adversary from achieving his/her goal of disrupting service from Treatment Plant 2 (i.e., the effects of the adversary action could not be isolated within Treatment Plant 2 and will be felt outside the system).

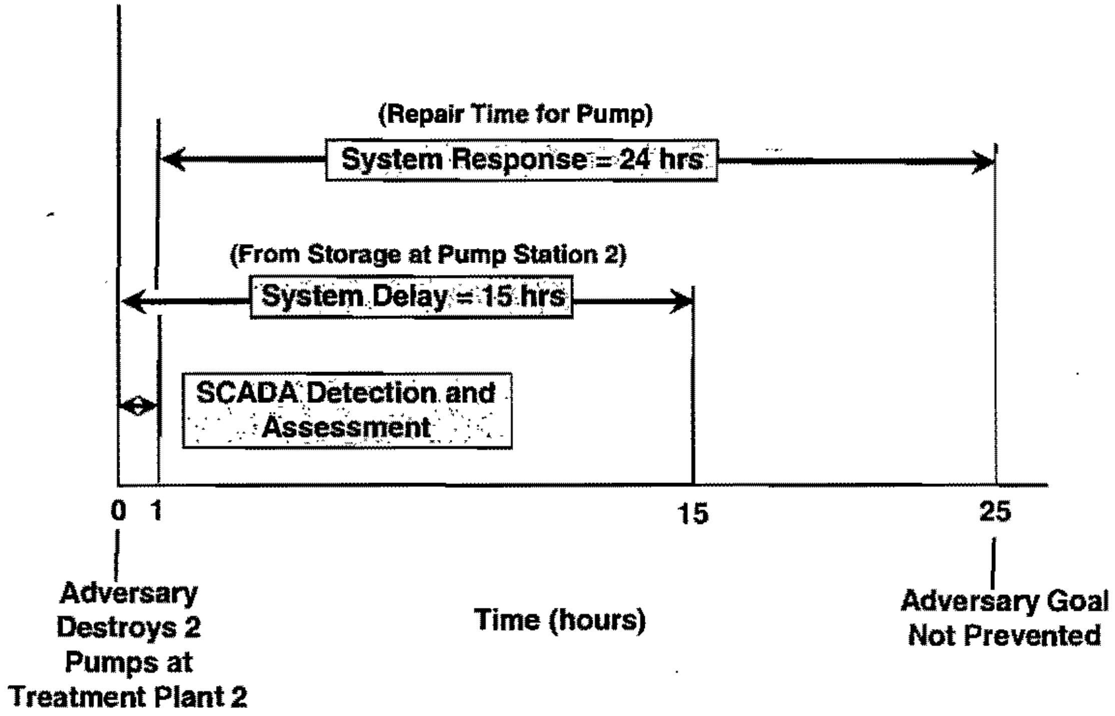

(Repair Time for Pump)
System Response = 24 hrs
(From Storage at Pump Station 2)
System Delay = 15 hrs
SCADA Detection and Assessment
0
1
15
25
Adversary Destroys 2 Pumps at Treatment Plant 2
Time (hours)
Adversary Goal Not Prevented

Figure 7.2. Operating System Effectiveness for the Example Water Utility

If, however, a backup pump were stored on site, cutting the replacement time in half (12 hr), there would be no disruption of service from Treatment Plant 2 (Figure 7.3). The pump could be replaced before the rest of the system was affected. The adversary is not considered to have achieved its goal since the protection system was able to isolate the effects of the action within Treatment Plant 2 and they were not felt outside the system. Because of this, consideration of these protection elements should be included as part of System Effectiveness, P_E, in the risk equation.

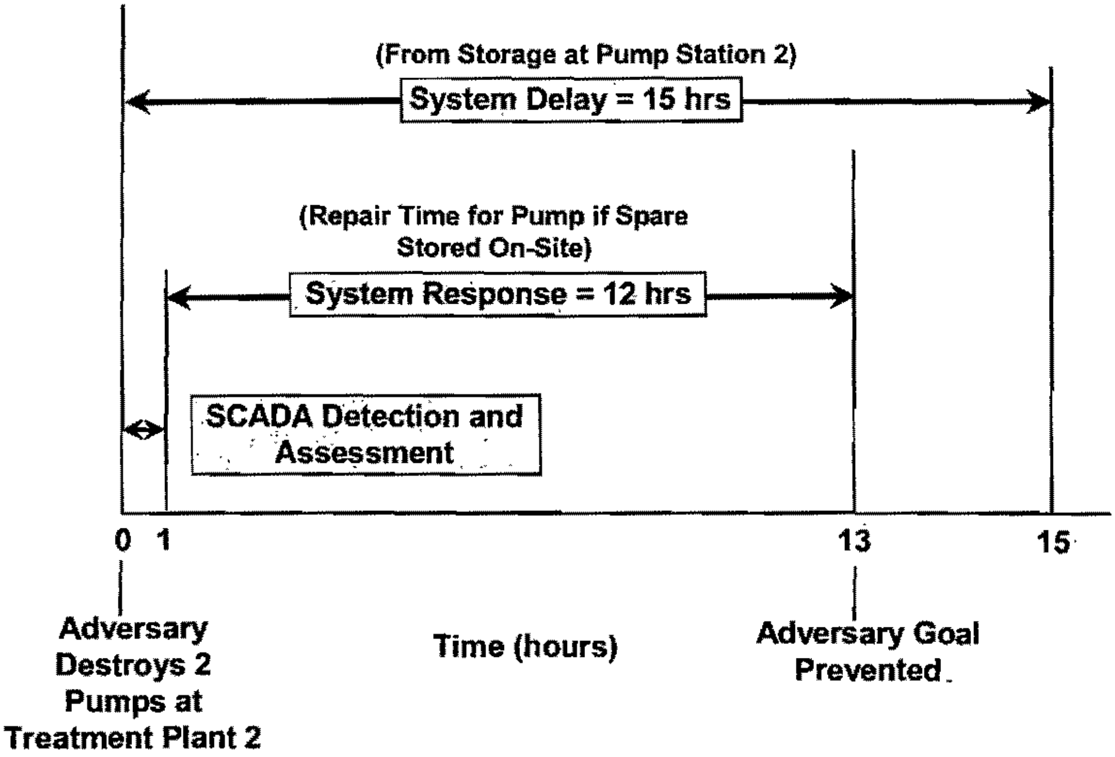

(From Storage at Pump Station 2)
System Delay = 15 hrs
(Repair Time for Pump if Spare Stored On-Site)
System Response = 12 hrs
SCADA Detection and Assessment
0
1
13
15
Adversary Destroys 2 Pumps at Treatment Plant 2
Time (hours)
Adversary Goal Prevented.

Figure 7.3. Operating System Effectiveness for the Example Water Utility

Note that the timeline could be extended beyond prevention into mitigation. In the first example presented where the adversary was not prevented from achieving the goal of disrupting service from Treatment Plant 2, if mitigation measures were then employed, such as delivering water via trucks to affected areas, credit for the mitigation measure would be considered in the consequence term, C, of the risk equation.

7.2 System Effectiveness Analysis Process

The following are the steps involved for determining P_E:

- Identify the most potentially successful Adversary Strategy.
- Create an Adversary Sequence Diagram (ASD) on which all possible paths into the critical asset(s) are identified. Using the ASD, postulate the most vulnerable path.
- With the adversary strategy and path known, then an adversary attack scenario timeline can be determined. This is a worst-case scenario from the water utility's perspective.

In the context of the adversary attack scenario timeline, the assessment team then estimates the system effectiveness (for detection, delay, and response) and determines the effectiveness of each function (high, medium, or low) against the DBT attacking along the worst-case path. Factors such as how reliable and timely the detection, delay, and response are with respect to the DBT capabilities should be considered (This should be done in the context of the Adversary Attack Scenario Timeline which is described later). Ideally, performance testing, which adds credibility to these evaluations, is also part of this determination.

7.2.1 Adversary Strategy

Adversary strategies are identified for use in considering paths that the adversary could follow to access critical assets. Considering PPS weaknesses and facility states (e.g., shut down, middle of the night, holidays) and then considering the worst consequences that the adversary might cause by having access to the critical asset(s), the assessment team derives the most potentially successful strategy. The strategy is a simple statement of what the DBT is going to do to the asset(s) and roughly how it will be done (intention). It should not be path-specific since the next step is to determine the worst path. A strategy statement for the example water utility would be as follows: The DBT (3 outsiders) will plant 5 lb of high explosives on two pumps and destroy them.

For example, assume that the undesired event is to interrupt or reduce the ability to treat the water supply. Using the generic fault tree, some of the options for adversary strategy are:

- Adversely affect pretreatment
- Cause loss of pipelines/conduits
- Adversely affect treatment
- Cause loss of key personnel
- Cause loss of SCADA system
- Cause loss of pumps
- Cause loss of valves

Assume that the expert opinion of the assessment team is that the easiest way for the adversary to defeat treatment of the water supply is to cause the loss of pumps. Further analysis of this undesired event will be based on this identified adversary strategy of choice (i.e., defeating the treatment of the water supply by causing the loss of the pumps). If it is too difficult to decide which adversary strategy is the most potentially successful, then more strategies should be addressed for the undesired event. As many strategies as needed should be developed to provide confidence in the judgment. The item or area that is the target of the strategy becomes the critical asset to be protected to prevent the undesired event. The next element to be considered is the best way for the adversary to get to the critical asset; specifically, the analysis identifies the physical path to the area or critical asset to be protected.

7.2.2 Adversary Sequence Diagram (Path Analysis)

The physical paths that adversaries can follow to accomplish their objective and the PPS and operational design features along the paths are important in determining the adversary attack scenario most likely to succeed. All possible adversary paths should be considered. For the example used earlier, the pumps would be the critical assets, and the task would be to consider all adversary paths to the pumps (Figure 7.4)

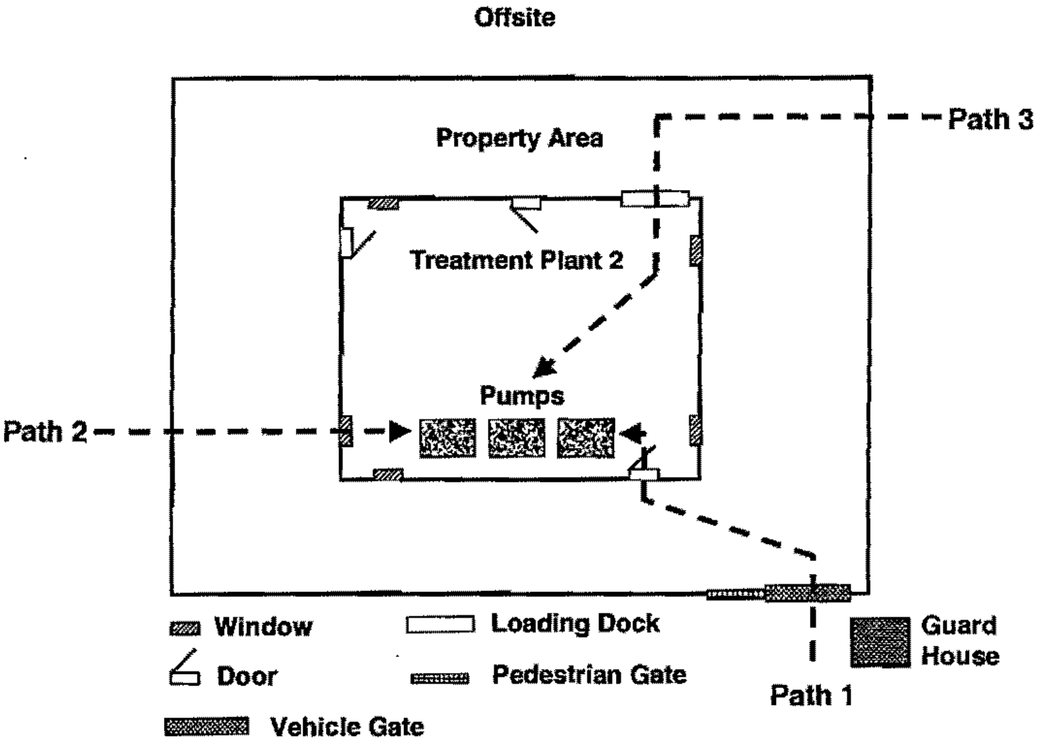


Figure 7.4. Adversary Path Development for Treatment Plant 2

There are many paths that an adversary could take to get to the asset. In this simple example for Treatment Plant 2, three paths are shown, but there are numerous possible paths:

- They could use many ways to get into the property area
  - Through, over, under the gate
  - Through, over, under the fence
- They could then use many ways to get into the building to sabotage the pumps.
  - Through the door (pedestrian or loading dock)
  - Through the window
  - Through the wall (assuming that the walls and the roof are of the same construction).

There are many possible combinations of ways to get to the asset and damage it. An Adversary Sequence Diagram (ASD) is needed to visualize all the possible paths. The ASD will aid us in postulating worst-case paths. Note that ASDs are used to determine physical paths (and not used for cyber paths, for example).

The first step in drawing an ASD is to identify the concentric areas (adjacent physical areas) through which the adversaries will have to pass as they go from off site to the critical asset (Figure 7.5). In between these areas are layers that bound each area and through which the adversary has to pass. In these layers are physical protection elements (detection elements or delay elements). An ASD includes protection layers indicating every way that the adversary may pass from one area to the next, and these must include all of the possible areas. An ASD for Treatment Plant 2 is shown in Figure 7.6.

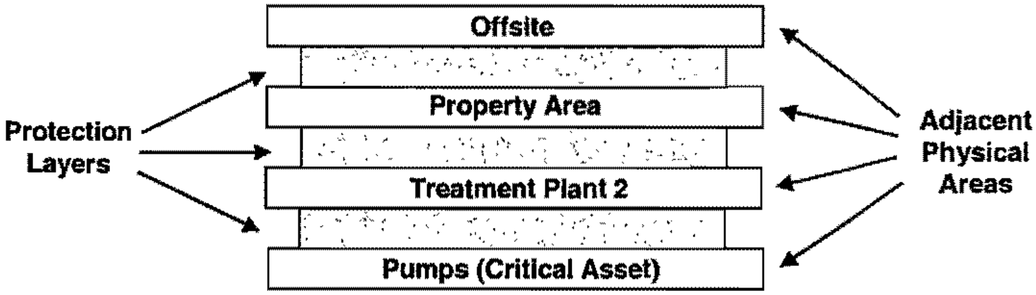


Figure 7.5. Adversary Sequence Diagram (ASD) for Treatment Plant 2

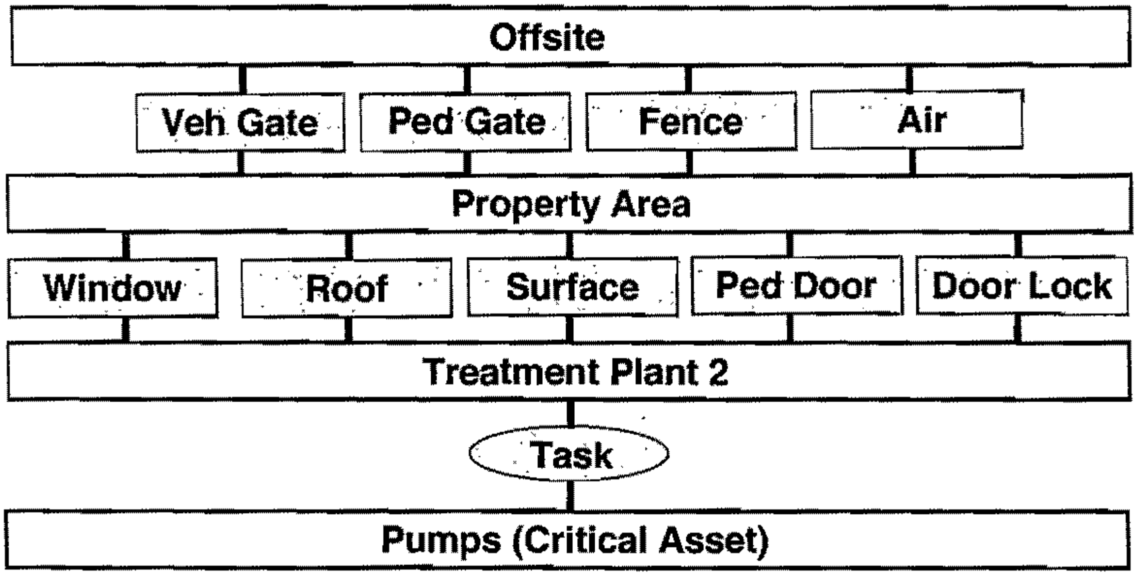


Figure 7.6. ASD for Treatment Plant 2 with Path Elements

For Treatment Plant 2, there are four path elements allowing one to get from Offsite to the Property Area, and five path elements to get into the Building from the Property Area. The final single step occurs when the adversary is in the presence of the critical asset and takes the necessary time to complete the task. There may be detection and delay elements associated with the final task. From this diagram the assessment team decides on the worst-case path. In this case, it could be that the adversary will come over the fence (no detection) and through the window (no detection) into the room and destroy the pumps. That may be the fastest path with the least probability of detection for the DBT (a sophisticated well-trained adversary will identify the most advantageous path).

This is a very simple diagram because the facility is relatively simple. An ASD is a way to represent all possible paths in one picture and it helps the assessment team in postulating worst-case path(s). Also, for further insight, a computer code, EASI (Estimate of Adversary Sequence Interruption), can be used in evaluating PPS performance along a single path if sufficient data can be provided. EASI is a simple calculation tool that quantitatively illustrates the effect of changing physical protection parameters (delay, response, and communication values) along a specific path and is described in the reference Garcia, 2001.

It is easier to carry a single worst-case path through the analysis. However, if it is not clear which worst-case path to choose, then it would be prudent to examine more than one path in the analysis and estimate the effectiveness for each one. This extra effort could yield important insights that might otherwise be overlooked.

7.2.3 Derive Most Vulnerable Adversary Attack Scenarios

Adversary attack scenarios are developed from the strategies together with specific paths, defeat methods, and tactics. Tools that are used to estimate PPS effectiveness are based on specific adversary scenarios. An assumption of the analysis process is that the protection system effectiveness is measured by its performance against what is considered the adversary scenario most likely to succeed for each undesired event.

This optimal adversary scenario is identified using expert opinion based on assessment team members' knowledge of the water utility, operations, and the existing protection system features. Several factors must be considered in judging which adversary scenario might be the most successful:

- Protection system weaknesses noted on data collection worksheets and site survey.
  - Least-protected paths (detection, delay, response).
  - Easiest system features to defeat.
  - Worst consequences.
- Facility operating states that the adversary could use to an advantage.
  - Emergency conditions.
  - No personnel on site.
  - Inclement weather.

Further development of the path (including methods and tactics that the adversary could use to defeat protection system features) leads to the development of the specific scenario that the adversary could follow that would be most likely to cause the undesired event. The best path to carry out the strategy (from the adversary perspective) would be the one that:

- Is physically the easiest for the adversary to complete.
- Avoids any security features, such as sensors or barriers.
- Could be predicted to achieve the adversary's goal.

This judgment is based on the assessment team's expert opinion formed by reviewing the information collected and analyzed. The scenario description includes the development of the most likely strategy and path to achieve adversary goals. The scenario includes specific system features, specific defeat methods, and tactics. The protection provided by the system against these particular scenarios will be used to estimate system effectiveness for the undesired event.

For the example water utility, a description of the scenario most likely to achieve the adversary's goal of reducing the ability to treat the water supply might be as follows: During nighttime hours after observing no personnel in the area, the adversary cuts through the perimeter fence (15 sec), runs across the protected areas to the building (10 sec) and enters the pump building through a window (5 sec). Once inside they locate the pumps (10 sec), plant 5-lbs of high explosives on the exposed pumps to destroy two pumps (25 sec) and thus disrupt the flow of water to the treatment facility. The adversaries exit the building before the explosives detonate. The time required for this scenario is 65 seconds.

7.2.3.1 Adversary Attack Scenario Timeline Analysis

A timeline can be used to further describe and analyze an adversary attack scenario. This timeline (Figure 7.7) shows only PPS elements, but as shown earlier it could also include operating system elements as well. *The capabilities of the adversary must be considered in the development of the attack scenario timeline.* Figure 7.7 illustrates the concept of timely detection in the PPS context. The critical detection point (CDP) is where the minimum time along the remaining portion of the adversary path (TR) just exceeds the response force time (RFT). Timely detection is when the adversary is reliably detected at the CDP or earlier. In that case, the adversary is interrupted (prevented from continuing along his task). A protection system that achieves timely detection is effective. The performance of a protection system's detection, delay, and response should be judged in this context. Determining where the CDP lies is very important in the timeline analysis. Its location provides insights for determining effective upgrades to the protection system since system effectiveness is increased by improving detection along the timeline before the CDP and adding delay along the timeline after the CDP. The CDP can be mentally assigned based on where the analyst predicts the time remaining just exceeds the response time. Another way to help achieve timely detection is by reducing response time.

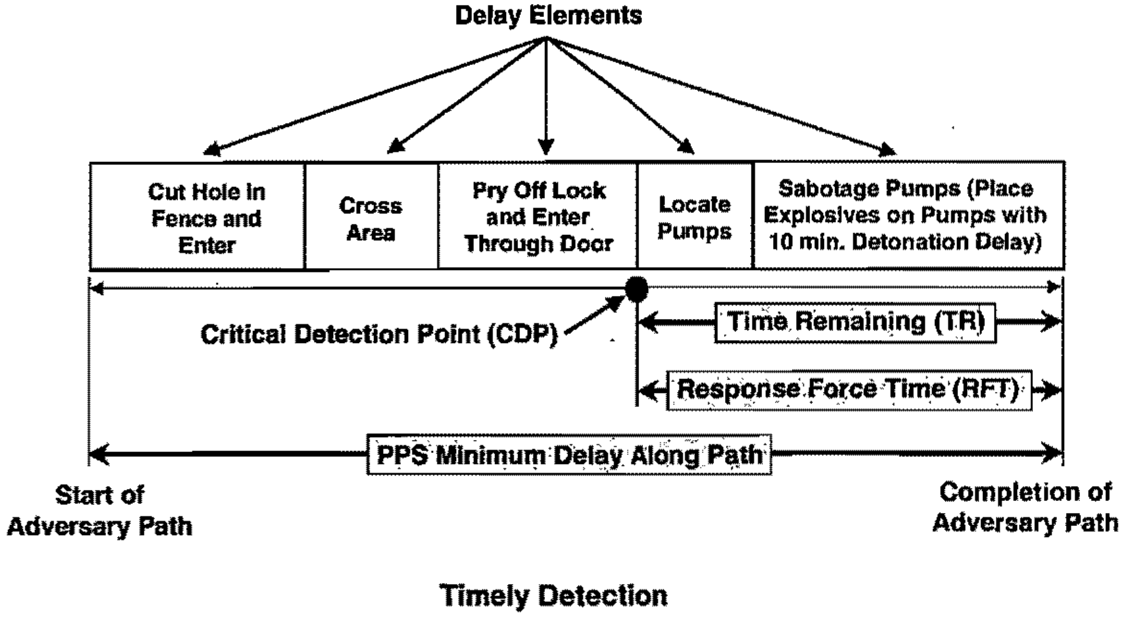

Delay Elements
Cut Hole in Fence and Enter
Cross Area
Pry Off Lock and Enter Through Door
Locate Pumps
Sabotage Pumps (Place Explosives on Pumps with 10 min. Detonation Delay)
Critical Detection Point (CDP)
Time Remaining (TR)
Response Force Time (RFT)
PPS Minimum Delay Along Path
Start of Adversary Path
Completion of Adversary Path
Timely Detection

Figure 7.7. Adversary Attack Scenario Timeline (PPS Example)

In Figure 7.8, the PPS system response is not timely, but the operational detection and response is sufficient—so it would seem that no improvements are needed in the PPS or operational system.

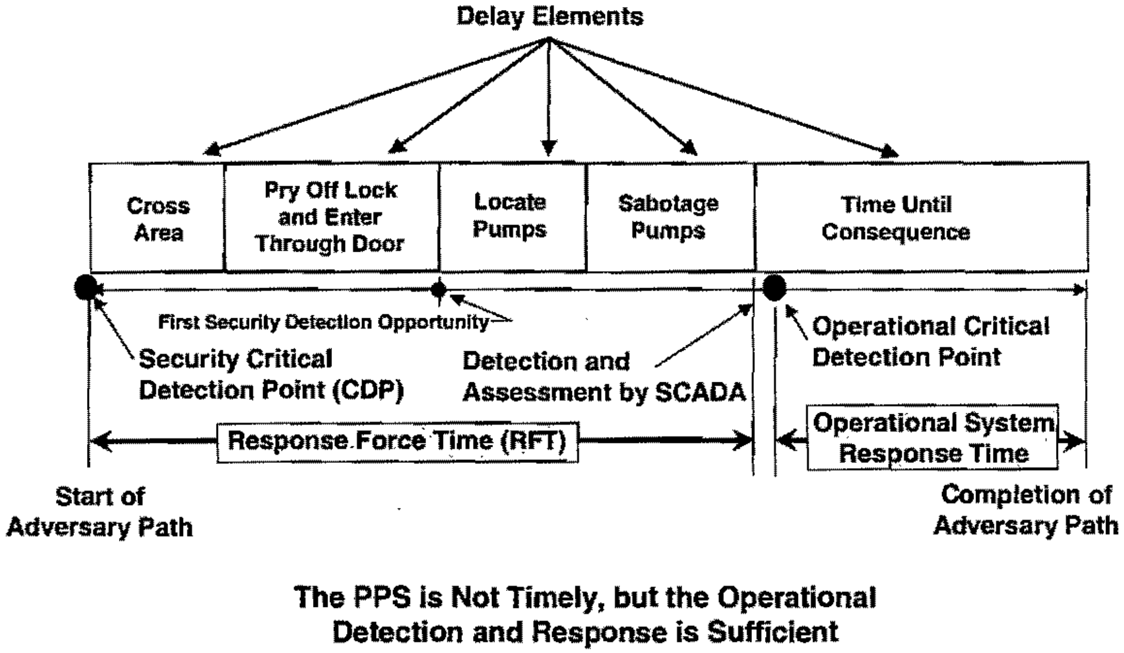

Delay Elements
Cross Area
Pry Off Lock and Enter Through Door
Locate Pumps
Sabotage Pumps
Time Until Consequence
First Security Detection Opportunity
Security Critical Detection Point (CDP)
Detection and Assessment by SCADA
Operational Critical Detection Point
Response Force Time (RFT)
Operational System Response Time
Start of Adversary Path
Completion of Adversary Path
The PPS is Not Timely, but the Operational Detection and Response is Sufficient

Figure 7.8. Combined Timeline First Case for Treatment Plant 2

In Figure 7.9 neither the PPS nor operational detection and response is sufficient since the first detection opportunities for both occur after the CDPs.

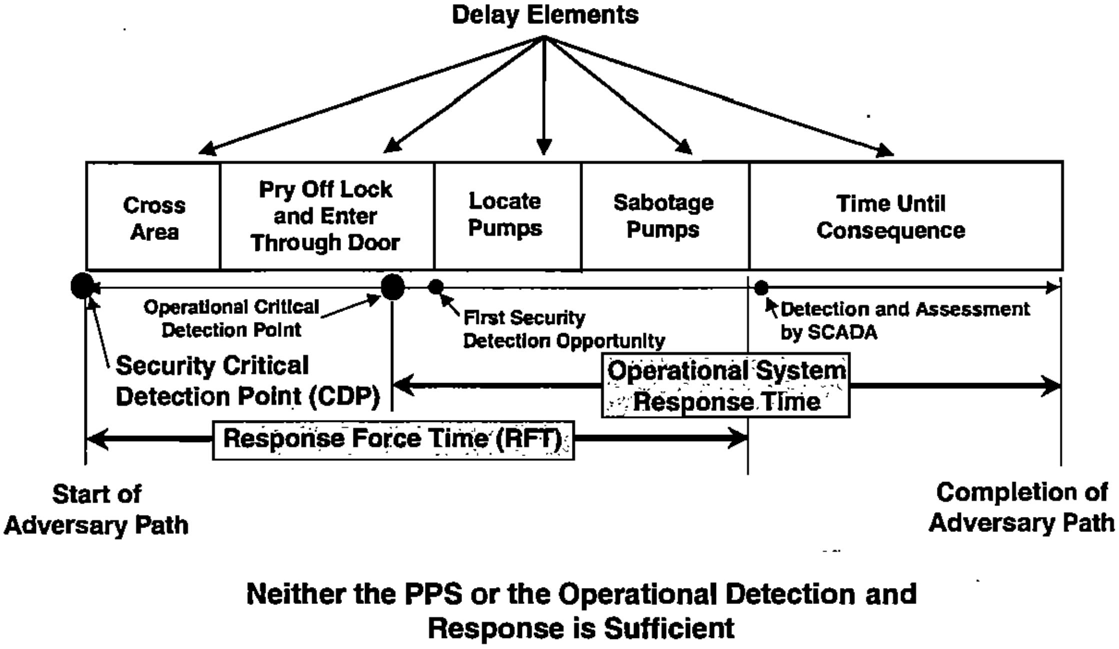

Delay Elements
Cross Area
Pry Off Lock and Enter Through Door
Locate Pumps
Sabotage Pumps
Time Until Consequence
Operational Critical Detection Point
First Security Detection Opportunity
Detection and Assessment by SCADA
Security Critical Detection Point (CDP)
Operational System Response Time
Response Force Time (RFT)
Start of Adversary Path
Completion of Adversary Path
Neither the PPS or the Operational Detection and Response is Sufficient

Figure 7.9. Combined Timeline Second Case for Treatment Plant 2

In Figure 7.10, the PPS is not timely, but the detection at the first security detection opportunity is timely in terms of the operational system response. A possible example of such a situation is that the adversary is detected by the PPS system, the water utility knows the adversary is going to destroy the pumps before the security response force (local law enforcement) can arrive, and so the water utility decides to start working on an operational response right away.

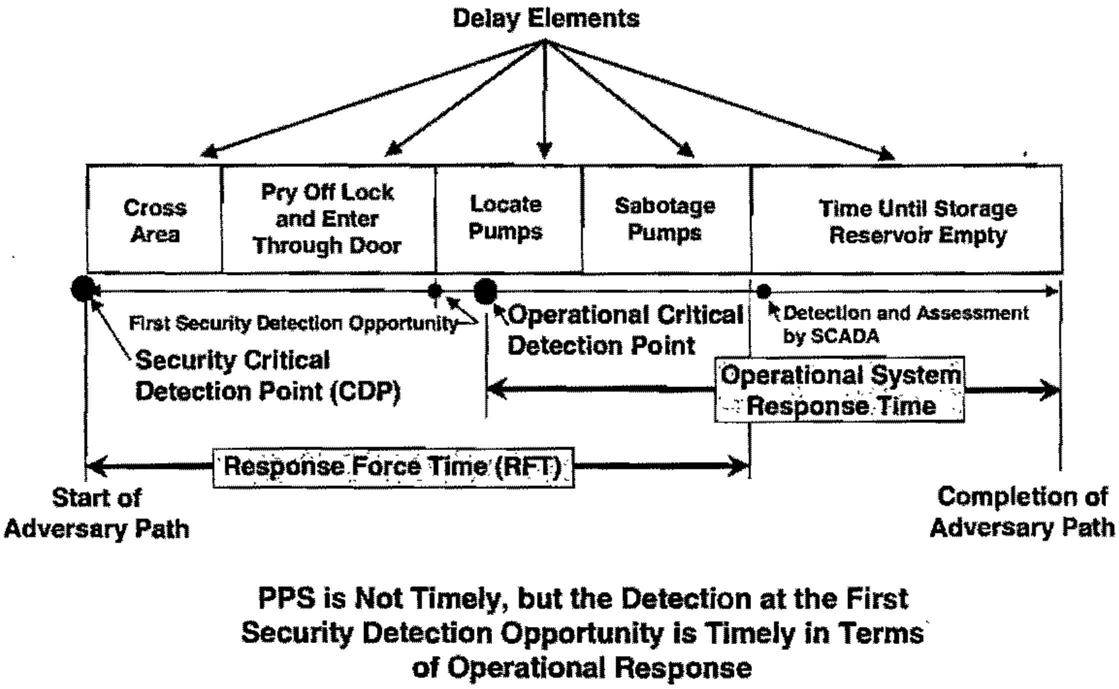

Delay Elements
Cross Area
Pry Off Lock and Enter Through Door
Locate Pumps
Sabotage Pumps
Time Until Storage Reservoir Empty
First Security Detection Opportunity
Security Critical Detection Point (CDP)
Operational Critical Detection Point
Detection and Assessment by SCADA
Operational System Response Time
Response Force Time (RFT)
Start of Adversary Path
Completion of Adversary Path
PPS is Not Timely, but the Detection at the First Security Detection Opportunity is Timely in Terms of Operational Response

Figure 7.10. Combined Timeline Third Case for Treatment Plant 2

7.3 Estimated System Effectiveness

The attack scenarios most likely to result in adversary success are used to estimate protection system effectiveness for each undesired event. An assumption of the analysis process is that the effectiveness of the protection system is only as good as the protection that it provides against the worst-case adversary scenario. Here is the basic process used to estimate protection system effectiveness:

- For each selected adversary scenario, list features of the protection system that provide detection (sensing, assessment, alarm communication, alarm display), delay, and response. Use this to help develop an adversary attack timeline.
- Assess level of effectiveness of the detection, delay, and response features of the PPS and Operational System listed.
    - o Bear in mind the adversary attack scenario timeline and the concept of timely detection. Determine how timely and reliable the elements of detection, delay, and response are with respect to the adversary attack scenario timeline.

- It is very important to try and conduct performance tests of the elements being evaluated. Do so in the context of the adversary attack scenario timeline. The tests can be very simple (e.g., can this valve be shut off in 1 hour?), but they should be designed to support the estimates of performance with data.

- Estimate overall protection system effectiveness for each scenario.

The first step includes listing the features of the protection system that either provide detection, delay, and response for the selected adversary scenario. For the example water utility, the listing might look like the first two columns of Table 7.1. Note that at this point, if any elements of detection, delay, or response are not present (i.e., they are not covered by either the PPS or the Operational System), the overall system effectiveness can already be judged as Low.

Table 7.1. Protection System (PPS and Operational) Features for Treatment Plant 2

Feature	Type	Level of Effectiveness (Timeliness and Reliability)
Detection	All doors alarmed during non-operational hours; windows are not alarmed (PPS)	Low (Minimum of Med Timeliness and Low Reliability)
	SCADA detects drop in pressure after pumps sabotaged (OS)	Low (Minimum of Low Timeliness and Med Reliability)
Delay	Delays are fences, doors, and task times (PPS)	Med
	15 hours worth of storage capacity (OS)	High
Response	Law enforcement is located over an hour away (PPS)	Low
	Replace pump (with spare pump located on site.) (OS)	Med

The second step includes judging the level of effectiveness of the features listed in the table to accomplish detection, delay, and response for the scenario. Determine how reliable and timely the elements of detection, delay, and response are with respect to the adversary attack scenario timeline. As an example, assume thatthe adversary attack scenario timeline is described in Figure 7.10. Considering thatthe reliability of detection is an especially crucial factor in the estimation of effectiveness. The adversary attack scenario timelines provide insight and can also be enhanced by including information on the reliability of detection at certain points as shown in Figure 7.11.

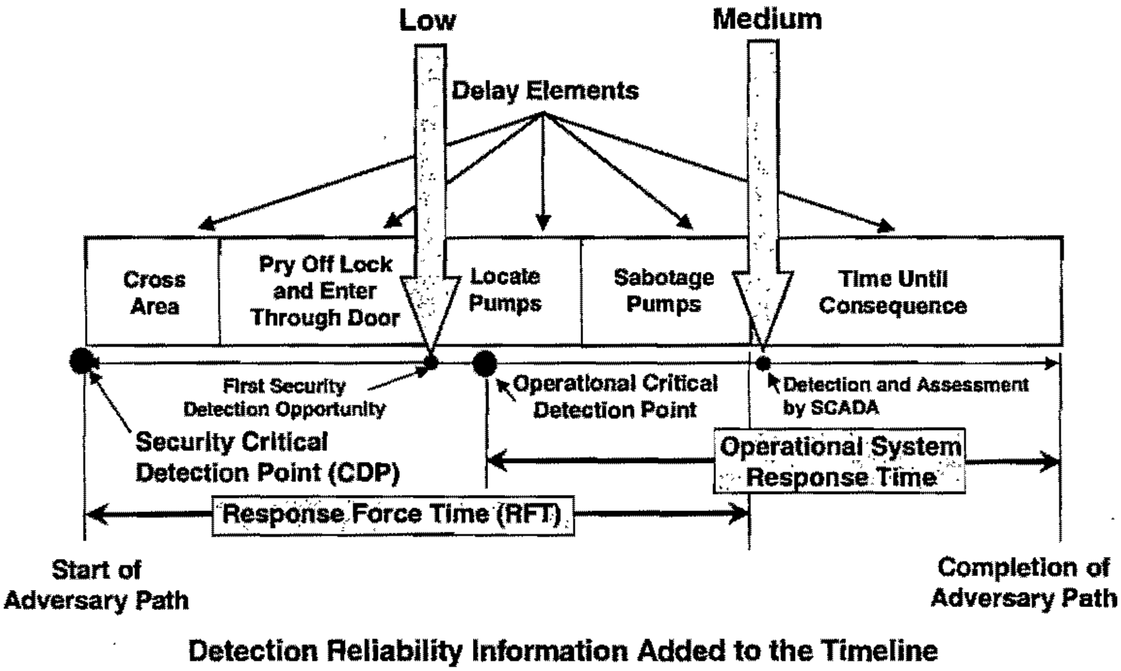

Low
Medium
Delay Elements
Cross Area
Pry Off Lock and Enter Through Door
Locate Pumps
Sabotage Pumps
Time Until Consequence
First Security Detection Opportunity
Operational Critical Detection Point
Detection and Assessment by SCADA
Security Critical Detection Point (CDP)
Operational System Response Time
Response Force Time (RFT)
Start of Adversary Path
Completion of Adversary Path
Detection Reliability Information Added to the Timeline

Figure 7.11. Combined Timeline Third Case for Treatment Plant 2 with Detection Reliability Added

Consider the level of effectiveness for detection shown in Table 7.1. In Figure 7.11, it can be noted that the PPS detection is timely with respect to the operational CDP (at least med), but its reliability is judged to be low (perhaps performance testing showed that the door sensors do not always work). Therefore, low is put down for level of effectiveness of PPS detection. The operational system detection is judged to have a medium reliability but is not timely with respect to any of the CDPs and so its level of effectiveness is entered as low.

Detection, delay, and response are all interrelated with respect to timeliness. As just mentioned, in filling out the effectiveness value for detection in Table 7.1, both timeliness and reliability are considered. In evaluating timeliness of detection, the timeliness of all three variables (detection, delay, and response) is in fact being considered. In evaluating the reliability and timeliness of detection for Table 7.1, the other two variables (delay and response) are held constant (i.e., both of their reliabilities are assumed to be 100%). The delay and response reliabilities, however, must also be accounted for in determining level of effectiveness. This is addressed by entering in the reliability values for PPS and OS delays and responses under the Level of Effectiveness column in Table 7.1.

When referring to reliability of delay, one of the things considered is the variability of the delay value used in the timeline. For example, with a variability less than 33% use low, with a variability between 33% and 66% use medium, and with a variability greater than 67% use high. For a PPS delay with a medium variability, medium is entered in the Level of Effectiveness column for PPS delay. And if, for the OS delay, there usually exists 15 hours of storage capacity (low variability), a high is entered in the Level of Effectiveness column for OS delay.

When referring to reliability of response, the variability of the response time should be considered. The effectiveness of the response force should also be considered in the PPS response evaluation, which includes things like "Do they know where to go?", "Do they know what to do?" "Is there an MOU in place?" Considering all of this, the PPS response is judged to have low reliability and the OS response to have medium reliability, which are then entered into Table 7.1.

The next step is to estimate overall system effectiveness. This is shown in Table 7.2 and involves assigning values for detection, delay, and response against the DBT for each of the undesired events. Since protection system effectiveness considers the contributions of PPS and Operational elements, enter the highest value of PPS or Operational protection system effectiveness from Table 7.1 that makes logical sense in the context of the scenario being considered for each system function of detection, delay, and response. An example of the results for Treatment Plant 2 is given in Table 7.2.

Table 7.2. Example Results for Estimating System Effectiveness for Treatment Plant 2

PPS or Operational	Outsider DBT Critical Asset: Pumps
Detection	Low
Delay	High
Response	Med
Estimate Overall System Effectiveness, P_E	**Low**
Note: P_E is the lowest of detection, delay, and response	

Estimates of protection system effectiveness values against the DBT must be made for all undesired events. An example is shown in Table 7.3. These values of protection system effectiveness are used in the next chapter to estimate the value of risk associated with each undesired event.

Table 7.3. More Example Results for Estimating System Effectiveness for Treatment Plant 2

PPS or Operational	Outsider DBT Critical Asset: Pumps	Insider DBT Critical Asset: Onsite Chemicals
Detection	Low	Low
Delay	High	Low
Response	Med	Low
Estimate Overall System Effectiveness, P_E	**Low**	**Low**
Note: P_E is the lowest of detection, delay, and response		

7.4 Protection System Vulnerabilities

Whenever a protection system is judged to have lower than medium or high performance for a system function of detection, delay, or response for a given scenario, a significant system vulnerability is implied. The explanation for why a performance level is judged to be lower than high should identify a specific weakness or vulnerability in the system. Identification of specific vulnerabilities is valuable in suggesting upgrades to the system, both in the protection system and the mitigation system. A list of vulnerabilities for Treatment Plant 2 is shown in Table 7.4.

Table 7.4. Example System Vulnerabilities at Treatment Plant 2

Threat	Function	Vulnerabilities
Outsider DBT	Detection	• No fence or windows sensors or assessment capabilities • No sensors during operational hours • Few personnel during off hours
	Delay	• No barriers or impedance
	Response	• Lack of timely response from local law enforcement • Local law enforcement does not have access to locked facility
	Mitigation	• No spare pumps
Insider DBT	Detection	• No policy on key control • Few personnel during off hours
	Delay	• No delay features for employee
	Response	• Time to respond not reliable • Lack timely response
	Mitigation	• No spare pumps

More discussion and guidance on upgrades is included in Chapter 9.

7.5 MITIGATION

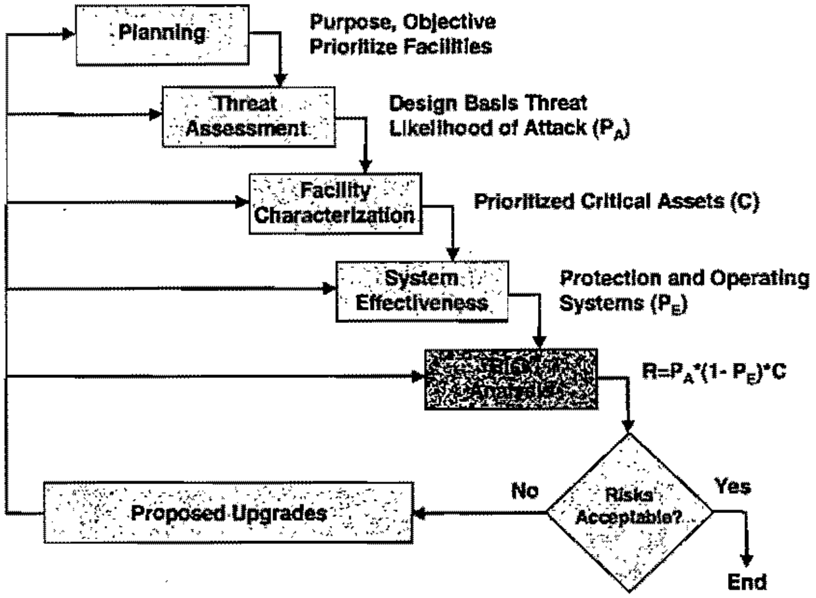
After system effectiveness, mitigation is the next thing to consider in the analysis. To analyze mitigation, review the consequence values associated with the adversary scenario most likely to cause each undesired event. If mitigation features would reduce the effects or consequences of a successful adversary scenario, the consequence level assigned to the undesired event should be reduced. The consequence definition table in Chapter 5 should be used to change the consequence level.

Mitigation was mentioned in Section 6.2, and it will be addressed again in the Risk Analysis and Risk Reduction and Recommendations sections. Mitigation is being mentioned in this section because the adversary attack scenario timelines can be extended to cover mitigation.

In extending the timeline to cover mitigation, the concept of timely detection for mitigation emerges. To illustrate this concept using a hypothetical example, say water was maliciously contaminated at a storage tank. The residence time (from the effluent of the storage tank to the first customer) can be viewed as an operational delay and notifying the public and trucking in water can be viewed as a mitigation measure. This would not be part of system effectiveness since the adversary was not prevented from achieving his goal—ill effects are felt beyond the system since water had to be trucked in.

Timely detection for mitigation in this case refers to being able to detect the contamination early enough that the public can be warned and water trucked in before any customers become sick from drinking contaminated water. By notifying the public and trucking in water, the consequence value can be lowered to low (per Table 5.1) if the number of illnesses drops below 500 and there are no deaths.

8 RISK ANALYSIS



Waterfall Flow Diagram – Process Location

The risk analysis uses the values calculated for likelihood of adversary attack estimates (P_A discussed in Chapter 4); existing system effectiveness estimates (P_E discussed in Chapter 7); and the associated consequence value (C discussed in Chapter 5); to calculate the risk value for each undesired event for each specific threat level at each critical asset. A matrix is created by undesired event, containing each critical asset with the results of the multiplication of the Consequences times the System Effectiveness.

8.1 RISK EQUATION

The general risk equation for each undesired event is as follows:

$$R = P_A * (1 - P_E) * C$$

where:

R = risk associated with adversary attack

P_A = likelihood of the attack

P_E = probability the physical security system and the operational system (design robustness) is effective against the attack

$(1 - P_E)$ = probability that the adversary attack is successful (also the probability that the system is not effective against the attack)

C = consequence of the loss from the attack.

It is only through P_E and C that risk can be affected. This represents an important consideration because P_E includes those activities, equipment, technologies, procedures, etc., that the water utility can employ to reduce the risk of loss of a successful undesired event. Likewise, C represents mitigation efforts related to operations that can be undertaken (e.g., facilities, equipment, procedures) to create redundancy or a contingency. These two terms in the risk equation represent quantifiable ways to reduce risk. It is important to remember that system effectiveness (P_E) is comprised of both the PPS and the operational system. If operational detection, delay, and response can be affected before the adversary can cause a high-level consequence, then P_E would be affected. If the water utility cannot prevent the adversary from causing the high-level consequence but can mitigate after the fact, then C would be affected.

8.2 Estimate Risk Values

When the assessment team estimates P_E and C, they assign qualitative values (low, medium, and high). For the purpose of risk analyses, numerical values are associated with the qualitative values. This conversion to a numerical scale is done only for aggregation purposes and ultimately does not have any more quantitative meaning other than the three levels of high, medium, or low. Note that these values are used for calculations to estimate *a relative risk number and not an absolute risk number or probability.* The numerical values associated with the qualitative values are:

Low (L) = 0.1
Medium (M) = 0.5
High (H) = 0.9

Using these numbers, numerical estimates can be calculated for the risk values for each undesired event and threat group by critical asset. Table 8.1 provides an example summary of the risk calculation for the critical assets identified for Treatment Plant 2.

Table 8.1. Outcome of Risk Analysis – Example Water Utility

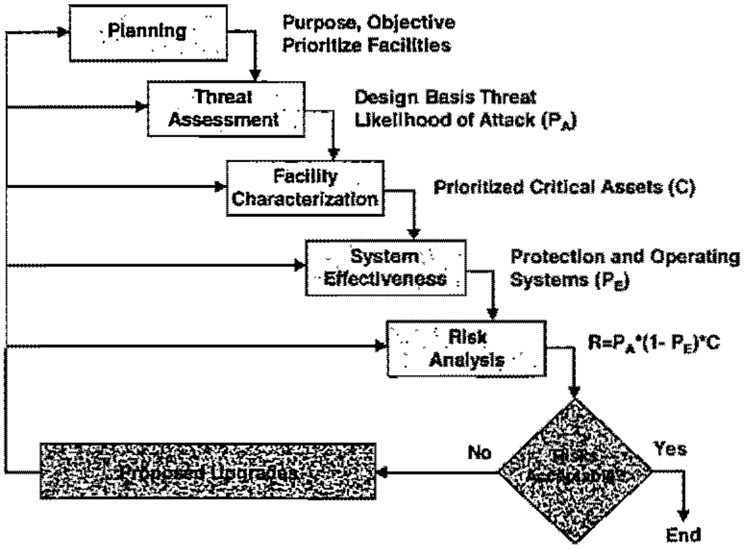
Loss of Ability to Treat Water Supply					
Facility: Treatment Plant 2	**Consequence Factor (from Chap 5)**	**System Ineffectiveness (1 - P_E, from Chap's 6&7)**		**Relative Risk $R=P_A*(1-P_E)*C$**	
Asset (effect):		**Outsider**	**Insider**	**Outsider**	**Insider**
Pumps	0.9	0.9	0.9	0.81	0.81
Chlorine Cylinders	0.9	0.9	0.9	0.81	0.81
Building	0.5	0.5	0.1	0.25	0.05
Key Personnel	0.1	0.5	0.1	0.05	0.01
Incoming Pipeline	0.9	0.5	0.1	0.45	0.09

The consequence value is identical to the consequence defined in Chapter 5 for each of the assets (high = 0.9, medium = 0.5, and low = 0.1). The current system "ineffectiveness" (i.e., 1 minus the system effectiveness) was defined and identified in Chapter 7 (high = 0.9, medium = 0.5, and low = 0.1). The range of threat described by the DBT is included in the table. The *relative risk* of the loss of each asset is calculated for the range of threat listed. It is recommended that the water utility highlight the last column (risk) to somewhat further illustrate the gradations. A suggested color-coding scheme:

- Risk values at a level of 0.81 code with red,
- Risk values at a level of 0.45 code with yellow.

This is done to highlight those risk values that are high compared to the remainder of the critical assets. At this point in the analysis, the calculated values of risk are presented to the project's management for a determination whether they are acceptable or unacceptable. If risk values are too high, then protection system improvements (PPS and operational) and consequence mitigation efforts to reduce risk can be suggested and evaluated.

9 RISK REDUCTION AND RECOMMENDATIONS



Waterfall Flow Diagram – Process Location

Risk can be reduced by increasing the system effectiveness, P_E, or by decreasing consequences, C, or by doing both. Upgrades that reduce risk should be considered for each critical asset with an unacceptably high risk level. The assessment team should review any potential WMD-type events first and apply resources to lower the risk of those events before considering other high-consequence events. The assessment team should then review the high-risk critical assets and prioritize them by mission objectives. In other words, if the highest ranked mission objective is to provide sufficient pressure for fighting fires, high-risk critical assets that support this mission objective should be addressed first. The basic elements of risk reduction include:

- Improvements in the security policies and procedures.
- Consideration of upgrades to prevent the undesired event (protection system upgrades).
- Consideration of upgrades to reduce the consequences of the undesired event (mitigation features).
- Consideration of upgrades to deter the adversary.

9.1 Mission Objectives

The risk calculations performed for the baseline security system will determine if the protection objectives have been achieved. If not, then the assessment team will start making upgrade suggestions to lower risk. Upgrades will differ depending on the protection objectives and the design and operation of the water utility. The categories of protection objectives include:

- Preventing the undesired event.
- Reducing the consequences of the undesired event occurring.
- Deterring the adversary.

As noted in the previous section, it is important for the assessment team to focus resources on the highest priority critical assets. The assessment team might consider resorting the risk analysis outcome to sort the high and medium risk critical assets by mission objective. Some critical assets will support several or all of the mission objectives. Building on the Treatment Plant 2 example, since Capacity ranked #1 and Water Quality ranked #4 (see Appendix C), any critical asset identified that supports only the water treatment operation would be ranked much lower than those that support Capacity. What becomes obvious is the fact that flowing water through Treatment Plant 2 is more important than the treatment function (in an emergency). If Treatment Plant 2 is vulnerable and an easy adversary target, the assessment team might consider installing a bypass around the plant to continue supporting the Number 1 mission objective to mitigate risk.

9.2 SECURITY POLICY AND PROCEDURES (GENERAL GUIDELINES)

The entire risk-reduction program for any water utility hinges on performance. Performance of the system is heavily dependent on policies, procedures, and training. Critical areas for the assessment team to examine during the assessment include how well security, operational, and emergency response plans are documented, how well employees are trained on the plans, and how exercises are conducted to reinforce the training. The presence or absence of well documented, consistently applied, and trained policies and procedures can be an indication of the corporate culture—a culture that will likely need to change to implement higher levels of security.

Here is a partial list of security policies and procedures that may need to be in place to improve security. Again, each water utility is different, and the list will change depending on the specific requirements.

- **Training**
  - Develop a training program to provide security training for employees, onsite contractors and vendors, including refresher courses and testing (assure understanding).
  - Develop cross-training between operators and guards where applicable.
  - Train security guards and periodically test performance.
  - Develop training on operational responses.
- **Access Control**
  - Develop and enforce badge policies.
  - Compartmentalize facilities – provide access on "as-needed" basis.
  - Create and enforce a key control policy.
  - Control the access of all visitors, contractors, and vendors.
  - Create and enforce a vehicle control policy.
- **Performance Testing**
  - Conduct "Table-Top" exercises regularly (such as conducted during Y2K and following 9/11) and evaluate performance on malevolent events and emergency response.
  - Maintain a supply of critical replacement parts, conduct tests to evaluate timeliness of replacement.
- **Teaming with other Agencies**
  - Develop/Educate/Exercise Memoranda of Understanding (MOUs) with other governmental agencies.
  - Team with interdependent local utility providers.
  - Create MOUs with the electrical and gas utility companies.
    - Improve contacts with power utility personnel.
    - Inquire on the contingency plans the electrical utility has if they were to lose a feeder or transformer and how long it may take to restore the system.
    - Identify priority power and gas requirements in the event of electrical and gas restrictions.

    - Establish MOUs with and between other municipal departments and law enforcement agencies both local and state wide.
    - Development of a regional spare parts inventory with other agencies.
- **Procedures and Plans**
    - Develop acceptance procedures and verify (assay) chemical deliveries.
    - Perform background checks on key employees and key contractor employees.
    - Create and enforce employee separation policies.
    - Create an unusual occurrence log, train employees to document unusual occurrences.
    - Review and trend the data from the unusual occurrence log at specific intervals.
    - Develop and document contingency plans for an electrical outage in the event of:
        - Losing one facility/system,
        - Losing two facilities/systems,
        - Outage of the entire regional power system lasting more than 48 hours.
    - Policies and procedures should be reviewed annually, updated, and/or eliminated if necessary.
- **Security Alarms**
    - Develop, train personnel, and test procedures for how to respond to all security alarms.
    - Log all security alarms.
    - Follow-up on all security alarms, evaluate response to alarms.
    - Write a disposition of all security alarms.

9.3 SYSTEM UPGRADES TO PREVENT UNDESIRED EVENTS

The assessment team may decide to install PPS upgrades as part of the risk reduction plan. For some critical assets, especially those in vulnerable urban areas, PPS upgrades may be the most cost-effective solution. The final PPS upgrade package will likely consist of detection, delay, and response features that are intended to prevent the undesired event from occurring. Guidance for selecting upgrade features include:

- Protection for common vulnerabilities and common system features.
- Protection-in-depth.

- Balanced protection.

Vulnerabilities that are common to several or all undesired events should be addressed first. In general, the first detection point must be as early as possible and as far away from the critical asset as practical, whereas placing the delay features closer to the critical asset could provide the most benefit if all adversary paths are affected.

Protection-in-depth means that an adversary should be required to avoid or defeat a number of protective devices in sequence to accomplish his/her objective. Layers of features cause adversity for the adversary, including increased uncertainty about the system, more extensive preparations prior to the attack, and additional steps where failure could occur.

Balanced protection ensures that an adversary will encounter effective elements of the PPS no matter how the critical asset is approached. For a completely balanced layer of system features, the delay times and detection performance would be equal. Complete balance is probably not possible or desirable. Some features may have inherent protection. Walls, for example, may be resistant to penetration, not because of physical protection requirements, but because of structural or safety requirements. Door, hatch, and grille delays may be less than wall delays and still be adequate. There is no advantage to over designing single elements, for example, installing a costly vault door on a flimsy wall. Table 9.1 provides examples of features that might increase PPS effectiveness for Treatment Plant 2. An analysis that includes performance testing would be required to determine if the upgrades would increase system effectiveness.

Table 9.1. Examples of Features that Might Increase Physical Protection System Effectiveness at Treatment Plant 2 (Example Water Utility)

DBT	PPS Function	Upgrades
Outsider: 3 Critical Asset: Pumps Capabilities: tools, weapons, explosives, knowledgeable about water and security system	***Detection***	• Add sensors on fences, doors, and windows • Add CCTV & lighting, establish policies • Add tamper indication and line supervision on all lines carrying PPS signals • Enhance portal access control with badge and PIN
	Delay	• Lock doors 24/7 • Harden doors, including hardened locks • Add mesh or bars to windows (inside) • Add pump/motor protection cage to 2 pumps and controls
	Response	• Develop closer coordination with local law enforcement and performance test response time • Provide security-related training for employees and contractors • Add alternative communications (i.e., cellular phones) for employees • Develop an alarm response policy
Insider: 1 Critical Asset: Onsite Chemicals Capabilities: onsite tools, weapon, extensive knowledgeable about water and security system, SCADA system and authorized access	***Detection***	• Separately keyed doors with strict key control and limited authorization for employees to enter areas • Criminal and financial background checks on employees • Add scheduled and random patrols
	Delay	• Additional barriers (doors, walls, fences, and surfaces) near the chemicals • Better and stronger locks • Two-person control over chemical access
	Response	• Better training of response force • Less nuisance alarms • Security personnel located at site 24/7

9.4 System Upgrades to Reduce Consequences

Mitigation is defined as reducing the severity or harshness of an undesired event. Generally mitigation is a more cost-effective approach for reducing risk than purchasing and implementing physical protection technologies, especially when considering life-cycle costs. Mitigation or consequence reduction features should be considered and evaluated for each undesired event. Mitigation features might include redundancy, contingency plans, early warning systems, or stockpiling of critical equipment in a secure location. Listed are some general practical steps for reducing consequences (this list is not all inclusive):

- Develop and implement policies, procedures, and plans for responding to the loss of critical assets identified during the assessment and test them on a periodic basis.
- Have spare equipment and parts ready and available in a secure location (performance test ability to replace spares based on established time requirements). Develop a regional spare parts inventory, if applicable.
- Have backup systems for critical assets where practical.
- Ensure that redundancy exists and operates sufficiently for high consequence undesirable events.
- Develop tie-ins to neighboring water utilities.

Listed are example mitigation features for the pumps located within Treatment Plant 2:

- Install natural gas pumps to mitigate interdependency risk with electrical power.
- Purchase a spare pump and store at another location.
- Increase water storage within the system to allow for longer outages.
- Performance test ability to replace pumps.
- Increase the capacity of other treatment facilities.
- Provide ties between the treatment facilities.
- Work with local electrical power utility to allow their portable electrical generation equipment to quickly connect to the water utility power system.

9.5 SCADA Recommendations

Increasing the security level of the complete SCADA system will require much more than simple "technology fixes." The adoption of an Information Technology (IT) framework such as CobiT[1] will allow the water utility to effectively design and maintain a robust, secure SCADA system. The development and maintenance of a security policy is the first recommendation to be addressed. Sandia developed a SCADA Security Policy Framework™ located in Appendix H in two forms: one is the framework with the areas that need to be addressed in a security policy and the other shows the mapping of those areas to CobiT. Basic security policies would include access and password controls, network perimeter definition, and data sensitivity definition requirements. Addressing the security policy issue in a timely manner is critical for the secure implementation and management SCADA systems.

The following lists of recommendations are mitigations for commonly seen vulnerabilities. It is important to note that these recommendations, particularly the security policy development, should take place before technology solutions are incorporated into the system to avoid redoing the technology solutions that conflict with the decided security policy. The recommendations have been grouped into four categories:

1. Policy/Procedure/Configuration Management,
2. System,
3. Network, and
4. Platform.

9.5.1 Policy/Procedure/Configuration Management

- Develop a SCADA specific security policy.
- SCADA security training and administration programs, based on formal security policies and procedures, must be developed and implemented. Security awareness must improve. Recognition that security is an ongoing process is essential to maintaining a secure SCADA system on a continual basis.

[1] IT Governance Institute, *CobiT, Governance, Control, and Audit for Information and Related Technology*, Information Systems Audit and Control Foundation, Rolling Hills, IL, 2000.

- Formal configuration management requirements and responsibilities should be developed and implemented.

9.5.2 SCADA System

- Identify a security perimeter for the SCADA system.
- Protect SCADA assets including networking equipment with a minimum of two layers of physical protection.
- Evaluate potential consequences of data manipulation or snooping and assign sensitivity levels to data. Develop policies for protecting different data sensitivity levels. Train staff in these policies.
- Encrypt SCADA data traversing untrusted networks.
- Provide strong separation between administrative and SCADA data.

9.5.3 SCADA Network

- Identify which communication links are critical and review options for providing true link redundancy. Implement redundancy when possible. If it is not practical to provide true redundancy, contingency plans should take this limitation into account.
- Provide a separate communication system for all critical physical security alarms. If this is not possible, ensure that the security procedures in both areas (i.e. physical and cyber, recognize that a compromise in the SCADA system requires a response in the physical security as well).
- Password generation and time limit policies should be developed and implemented.
- Create individual accounts for all personnel that login into the SCADA network remotely, including system administrators. Utilize a stronger authentication process (i.e., dial-back, Smart Cards, etc). Audit activities on the remote connection via logging, and review the audit logs as part on a regular basis.
- Implement security monitoring of SCADA workstations.

9.5.4 SCADA Platform

- Assign formal ownership of SCADA hardware and software.
- Develop policy and procedures for installing operating system patches.
- Use virus-checking software on the SCADA network, and maintain regular updates.

9.6 SYSTEM-WIDE RISK REDUCTION

The assessment team should create a list of system effectiveness and consequence mitigation features to lower risk for every critical asset that has unacceptably high levels of risk. Think creatively. There is no one right way to reduce risk, and every water utility has unique operational features and constraints. When the list of upgrades is complete, the assessment team should then take a "systems-level" view of the entire water utility operation to determine what might be done system-wide to lower risk. Are there multiple sources of water? If there are, can redundancy be increased? Are there multiple pump stations? If there are, can redundancy be increased? Is there one pump station that can be hardened easier than the others, and how much of the system demand can it meet? Are there multiple distribution paths, and how might redundancy be increased? How well protected are the distribution paths? Before blindly going down the list of high-risk assets and embarking on improvements, the assessment team should spend time working "what if" scenarios to determine the best system-level improvements. The assessment team might end up recommending to "do nothing" with a few high-risk assets because improvements elsewhere in the system will lower the risk when completed.

9.7 SYSTEM UPGRADES TO DETER ADVERSARY

Deterrence is an attempt to increase the perception level of the security system (i.e., it discourages an adversary from attempting an attack by making a successful attack appear very difficult or impossible). The deterrence function of a PPS is difficult to measure, and reliance on successful deterrence can be risky; therefore, it is considered a secondary function. Deterrence may be accomplished by adding visible security features (e.g., increased lighting, warning signage, fences, cameras, or security officers) or by adding surveillance equipment or features that provide identification for prosecution evidence. It would be a mistake to assume that because an adversary has not challenged a system, the effectiveness of the system has deterred such challenges. Further, note that not all threats are going to be deterred, and some level of prevention or mitigation is still required. Listed are examples of features that might increase the perception of the protection system (this is not an all inclusive list):

- Add visible features
    - Warning signage

    - Locked doors
    - Cameras for surveillance
    - Patrols
    - Barriers for critical assets (insider)
- Add identification means
    - Surveillance and recording devices for prosecution data
    - Witness program

9.8 Calculate Risk for Upgrade Package

Most of the upgrades that have been discussed in this chapter are general recommendations along the lines of Best Practices. Ultimately, however, they may or may not reduce risk. The only way of knowing if they reduce risk, and if so, by how much, is to examine the upgrades in the context of the adversary attack scenario. As mentioned in Chapter 7, location of the CDP provides guidance on how best to improve protection system effectiveness. If the proposed upgrades contribute to moving the protection system towards timely detection, then the protection system effectiveness will increase. It is very important to performance test the recommended upgrades in order to verify and measure the improvement to the protection system. The assessment team must reanalyze the ASDs, scenarios, and other materials created for the risk analysis to ensure that the upgrades will effectively lower risk. Similarly, consequence values associated with each undesired event should be reviewed to determine the effects of the proposed consequence reduction features. Finally, the risk values for the baseline system can be compared to that of the upgraded system to determine the amount of risk reduction. If risk values are still unacceptable, the upgrade process may have to be repeated.

If risk values are now in the acceptable range, consideration may be given to the other impacts imposed on the facility or system as a result of the upgrades. Some of the factors include cost, operations, or public opinion.

9.8.1 Example of Using Adversary Attack Scenarios and Timelines

A further illustration is the upgrading of one of the highest relative risk cases from Table 8.1, Outsider attack to the pumps. Since risk reduction via increasing system effectiveness is less straight-forward than with consequence reduction, the focus is on increasing system effectiveness in this example. Continuing from calculating system effectiveness in Section 7.3, an adversary attack scenario timeline was described in Figure 7.11 and levels of effectiveness for detection, delay, and response were described in Tables 7.1 and 7.2. From Table 7.2, it appears that improving detection might be a way to increase overall system effectiveness. Table 7.1 and Figure 7.11 provide insight on how to do that.

As determined from Figure 7.11, even though PPS detection was timely (at least medium), its reliability is judged to be low, so its overall level of effectiveness is listed as low. So if the reliability of the PPS detection was increased to a medium or a high, detection would go up to a medium or a high, increasing overall system effectiveness from low.

There is another possible way to increase system effectiveness from Figure 7.11. OS detection by the SCADA was judged to be of medium reliability but was not timely, so OS detection was listed as low. If OS response could be reduced enough that the SCADA detection became timely, OS detection would go up and increase overall system effectiveness.

To implement any of these upgrades, as mentioned before, the next step would be to performance test the upgrades to verify and measure increased system effectiveness.

10 FINAL RAM-W^{SM} REPORT

In this chapter, suggestions are presented on how to organize the final report. The final report represents the efforts of the entire assessment team and becomes the basis for future risk reduction efforts. Providing a well thought out, systematically organized, final report accomplishes several goals including:

- Documents entire process including definitions and decisions
- Makes it easy for others to follow the methodology
- Contains an Executive Summary for management review
- Creates a defensible end product
- Streamlines the ability to update the assessment when conditions change
- Provides a professional product.

The final report format presented here is based on numerous RAM-W^{SM} assessment feedback reports prepared by Sandia National Laboratories. The final report is organized to correspond to the RAM-W^{SM} assessment process and describes how the information necessary for the risk equation was gathered and/or analyzed.

10.1 CONTENTS BY CHAPTER

Executive Summary, probably the most important part of the document and the most widely read. It should contain a very short overview of the entire process and summarize major findings, outcomes, and recommendations.

Chapter 1, Introduction, contains introductory and background information on the RAM-W^{SM} assessment process. This chapter explains why the risk assessment was undertaken and should capture high-level planning elements. It also describes the scope of the assessment, customer requirements, and the organization of the final report.

Chapter 2, Planning, details the assessment planning process. The assessment team participants are noted along with the team's purpose and objectives. The mission objectives of the water utility are identified, and the facilities screened for inclusion in the vulnerability assessment are listed. By means of pairwise comparisons, the mission objectives are ranked against one another and the results presented in a table. A pairwise comparison is completed for the facilities included in the assessment for each of the mission objectives. A table is constructed that contains a summary of all the pairwise comparisons, weighted by the mission objectives, and lists the relative importance of each facility. The risk reduction goals are documented.

Chapter 3, Threat Assessment, discusses how threats were determined, defines the DBT, and discusses the likelihood of occurrence, $P_{A,}$ used in the risk equation. Based on multiple interviews and other available information, the threat assessment identifies and describes the types of adversaries, or malevolent persons or groups, that might try to prevent the water utility from performing one or more of its mission objectives. The DBT presented in the final report represents the adversary model against which the water utility's system effectiveness can be evaluated. The DBT used results from examination of general DBT spectrum definitions and consultation with various information sources and the consolidation of that information. The DBT is a management decision and must be clearly established for the water utility. Discussion is included on the likelihood of occurrence, $P_{A,}$ which is either arbitrarily set at a conservative value because of the lack of industry-wide threat information, or used in some consistent manner to discriminate threats.

Chapter 4, Site Characterization and Consequence Assessment, provides an overview of the water utility system, the site-specific fault tree, and assessment activities. In the site characterization overview, the assets in the water system are described along with their function, interconnections, and potential vulnerabilities. The potential vulnerabilities posed to public health by onsite chemicals are analyzed. The SCADA system and its vulnerabilities are described. Operational and security policies and procedures (including record keeping and training processes) are described and evaluated in terms of their completeness and the extent to which they are implemented. Existing security measures are captured and evaluation of their effectiveness included.

By customizing the generic fault tree, the water utility indicates which of the undesired events are achievable at their site. From the customized fault tree, critical assets are identified and a consequence value is assigned to each asset from the site-specific consequence matrix. The level of consequence that loss of a particular asset would represent to the water utility is determined by engineering judgment and/or expert opinion. Different levels of severity (high, medium, low), or consequence, are determined for each of the undesired events (critical assets).

Chapter 5, System Effectiveness (P_E), provides an analysis of the existing physical security and operating systems' effectiveness against the DBT. Worst-case adversary strategies or tactics are identified that could accomplish one or more of the undesired events for high-consequence critical assets. An adversary sequence diagram (ASD) is developed to identify the worst-case scenario of events that describes in detail how the adversary could accomplish their objective. The final report describes the process of expert judgment by which system effectiveness is tested against adversary scenarios on an asset-by-asset basis. The integrated functions of detection, delay, and response are evaluated for each physical security component and operational component to arrive at an overall estimate of effectiveness (high, medium, low). The System Effectiveness table lists the overall estimates of effectiveness (P_E) for each asset against the DBT.

Chapter 6, Risk Analysis, presents the risk analysis, which uses the potential for adversary attack (P_A), system effectiveness (P_E), and consequence values (C) from earlier chapters to calculate the current relevant risk value for each undesired event for specific adversary types at each critical asset. Note that only system effectiveness, $P_{E,}$ and consequence, C, can be mitigated to reduce risk. A table lists the relative risk, based on the risk equation, for each of the assets identified. It should be emphasized that the results are relative values and **not** probabilities.

Chapter 7, General Recommendations, offers insights into risk reduction and general recommendations or upgrades and best practices for operations, including SCADA, security, and consequence mitigation. Suggestions are made to reduce risk at specific sites. The importance of security permeating all operations is emphasized. The need to establish upgrade goals and to balance risk reduction against budgetary constraints is discussed. A table shows the potential effect on all levels of risk if specific upgrades were undertaken in accordance with the established risk-reduction goals. Also include in this section are recommendations for any WMD-type scenarios which may have been identified during the assessment even if the analysis shows them to be of low relative risk. This is done simply as a prudent measure.

Appendices, supporting background information is included in the appendices. The types of information that might be included in the appendices are:

- Worksheets,
- Chemical/biological threat discussions,
- The entire generic fault tree,

- Site specific fault tree elements,
- Questionnaire responses and notes, etc.

10.2 PROTECTION OF INFORMATION

Each page of the final report is marked in the appropriate manner to reflect the sensitivity of the data, and it should be secured on the computer and/or in a locked filing cabinet when it is not under the immediate control of the individual using the document (working documents should also be marked and controlled in a similar manner). The access, reproduction, and disposal limitations should be described on the back of the report's title page. Obviously, a report of this nature would be most helpful to potential adversaries, as would any materials produced to support the analysis and mitigation activities called for in the final report. It is the responsibility of the water utility to define the process necessary to prevent this information from being improperly disseminated.

10.3 ORGANIZATION OF FINAL REPORT

The organization of the final report is shown in Figure 10.1. It shows the primary subject areas in each chapter of the report as well as specific topic details within each chapter. The report flowchart also shows that after completion of the risk analysis, the water utility management team is faced with a decision step: Is the calculated risk acceptable? If the calculated risk is acceptable, then the application of RAM-W^{SM} is complete. If the calculated risk is not acceptable, then the application of RAM-W^{SM} must be iterated. Note that the process is repeated until upgrades have reduced the risk and the reduction goals are met.

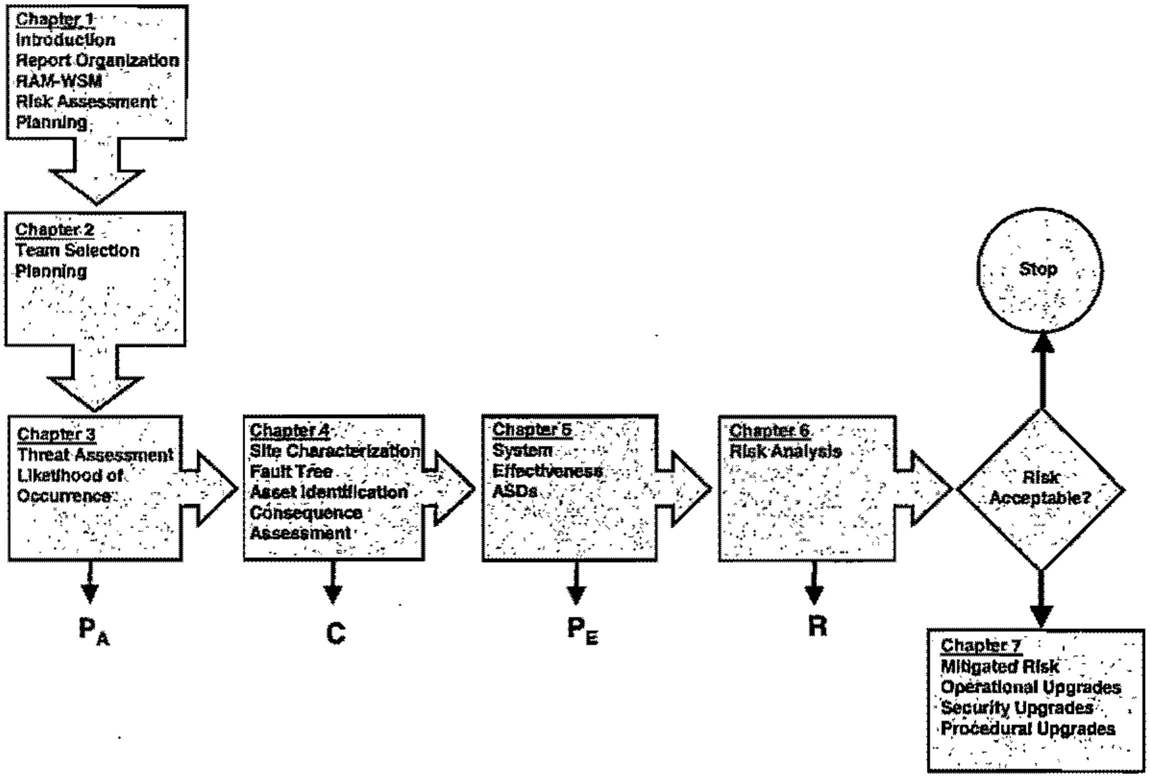


Figure 10.1. Organization of Final Report

APPENDIX A. EXAMPLE WATER UTILITY

A.1 OVERVIEW

This appendix contains the description of a fictitious municipal water system (referred to as the "example water utility"). The major process elements of the methodology are presented in the body of the report to help illustrate concepts. The reader should be aware that much detail is omitted, and the example is intended only for its instructive value. Any similarity to an existing water utility is purely coincidental.

A.2 EXAMPLE WATER UTILITY BACKGROUND INFORMATION

The example water utility to be used throughout this document to help illustrate concepts is described below (Figure A.1). The water utility serves a population of 250,000 people. The water utility is comprised of:

- Surface (Bigg Lake) and groundwater sources
- Three water treatment facilities
  - Two with integral pump stations and storage
  - Treatment Plant 2 has three water intake pumps
- One of the treatment facilities is supplied by wells
- Two major pump stations separate from the treatment facilities

A.2.1 Water Utility Description

Table A.1 provides some basic information (e.g., capacity, geographic extent, customer base, etc.) about each major facility within the example water utility.

Table A.1 Example Water Utility Information

Total system daily demand (minimum)	**100 mgd**
Intake Station 1	50 mgd capacity
	Reaches 60% of geographical area
	Serves no critical customers
	No treatment capabilities
Treatment Plant 1 and Integral Pump Station	45 mgd capacity
	Reaches 60% of geographical area
	Serves no critical customers
	Serves 15% of customers (on average)
	Full treatment capabilities
	Storage – 14 mg
Treatment Plant 2 and integral intake	90 mgd capacity
	Reaches 80% of geographical area
	Serves no critical customers
	Serves 75% of customers (on average)
	Full treatment capabilities
Treatment Plant 3	25 mgd capacity
	Reaches 20% of geographical area
	Serves critical customers
	Serves 10% of customers (on average)
	Partial treatment capabilities
Pump Station 1	40 mgd capacity
	Reaches 70% of geographical area
	Serves critical customers
	Serves 40% of customers (on average)
	No treatment capabilities
	Storage - 30 mg

(continued)

Pump Station 2	80 mgd capacity
	Reaches 80% of geographical area
	Serves no critical customers
	Serves 35% of customers (on average)
	Storage - 50 mg
Well 1	7 mgd capacity
Well 2	14 mgd capacity
Storage Tank	8 mg

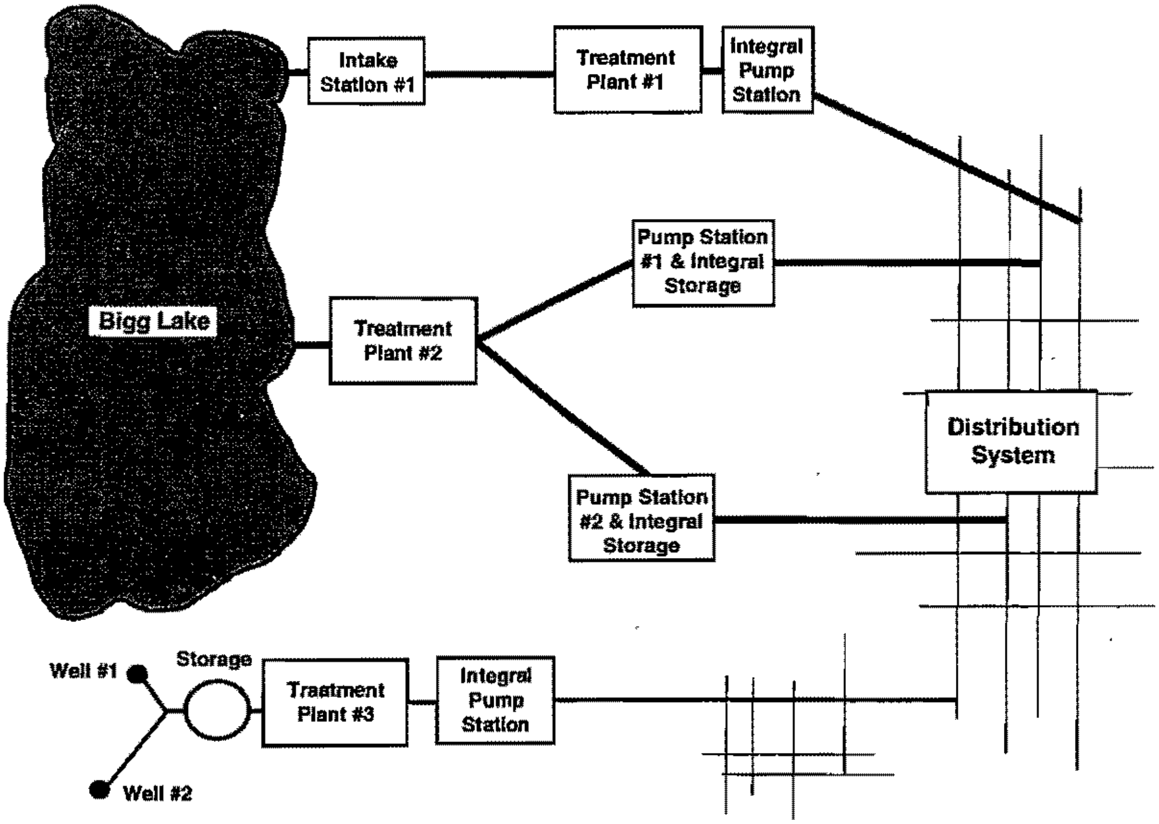


Figure A.1. Example Water Utility

A.3 Water Utility Mission Statement

At the initial assessment team meeting, the assembled group from the water utility overwhelmingly agreed upon the mission of the water system, as set forth in the water utility official Mission Statement. During the discussion, the following mission objectives were drafted from the mission statement and were then prioritized as follows:

- Maintain adequate pressure for fire protection and other public safety uses.
- Maintain adequate volumetric water supply.
- Maintain reasonable costs for public water supplies.
- Serve critical customers.
- Maintain water quality, with emphasis on producing potable water.

The pairwise criteria were developed from the water utility mission objectives and are listed below. Some of the mission objectives were combined and one was eliminated. It was decided that in an emergency, the water utility would not worry about the cost of the water.

Capacity – facility's ability to meet customers' demand (e.g., emergency demand).

Geographic Extent – delivering water to the maximum number of customers.

Critical Customers – delivering (24/7) to city hospitals, power plants, and critical manufacturers.

Quality – meet and exceed EPA requirements for potable water.

This information (mission objectives, criteria, facilities) is used to develop the pairwise comparison. Refer to Section 3.4.2 and Appendix C for full details.

A.3.1 Water Utility Threat Information

The water utility gathered the following extensive information to help them in defining their threat assessment. Not all this information was found to be relevant in developing and determining the DBT. However, it is a typical list of information that assessment teams gather when they first start identifying the threat.

- The water utility unusual incidents report for the last 12 months includes: eight pieces of water utility equipment found missing and 16 reports of vandalism/property damage

- Water utility treatment plant operators have full access to all plant controls, SCADA, and chemicals.
- The water utility web site (H2O) has been attacked by hackers since 9/11. Prior to 9/11, all water utility information (water system, operational information, facility description, facility functions, drawings, and security capabilities) was available on the web site. This disclosure was for good public relations and for contractors bidding on water utility work.
- Thirteen incidents of expressed threats or violence involving several water utility employees/contractors over union disputes were noted over the past five years.
- No background checks (criminal or financial) are conducted on employees or contractors.
- Local law enforcement and the FBI have published through the regional InfraGard that 5–10 lb of construction-type explosives were stolen in the last six months. In addition, law enforcement reports that an organized and armed militant group was recruiting and operating in the region.
- Below is a message received from FBI headquarters regarding today's notice of a terrorist threat against U.S. water systems. The FBI called XYZ Water Association's office this morning indicating that the threat came "from a knowledge source capable of carrying out such a threat."

FBI Message: Today, the XYZ Water Agency disseminated an urgent communication indicating that a terrorist group was threatening water operations in 68 medium-to-large U.S. cities. The communication advised that since the threat was coming from a "credible, well known source with an organization structure capable of carrying out such a threat," the FBI had asked water utilities to step up surveillance and take precautions. The FBI did become aware of a threat that mentioned water systems in a number of U.S. cities (and contacted XYZ regarding the threat); the FBI has assessed the threat (1-3 participants) as being of Medium to High credibility . The FBI in New York is continuing to investigate this matter in order to obtain further information regarding the nature of the threat.

This information was used to develop the DBT. Refer to Section 4.5 for full details.

A.4 TREATMENT PLANT 2: ASSETS REQUIRED FOR THE ABILITY TO TREAT WATER SUPPLY

The water utility focused on Treatment Plant 2 as its most important facility and determined which assets were needed for the ability to treat the water supply. The top of the Fault Tree customized to represent Treatment Plant 2 is shown in Figure A.2. The mission objectives shown to be under threat from the adversary are "Maintaining Water Flow" and "Avoiding Contamination". Water in the system flows through many components serially. The adversary can interrupt or impair water flow to customers by destroying, damaging, or misusing any one of the components. For Treatment Plant 2, five assets are identified from the fault tree segment shown in figure A.2:

- Pipelines/Conduits
- Treatment Process
- Critical Pump Systems
- Key Personnel
- Control System

These assets and their criticality to the operation of the Treatment Plant 2 system are discussed below.

Damage/Destroy Pipelines or Conduits: Single source water pipeline exposed above ground - a single pipe transmits water from Bigg Lake to the plant, there is no redundancy. This pipe is a single point of failure in the water system. This asset was determined to be a critical asset from the fault tree analysis.

Treatment Process: Other contaminants could be introduced into the system (vs. EPA standard contaminants normally identified in the system).

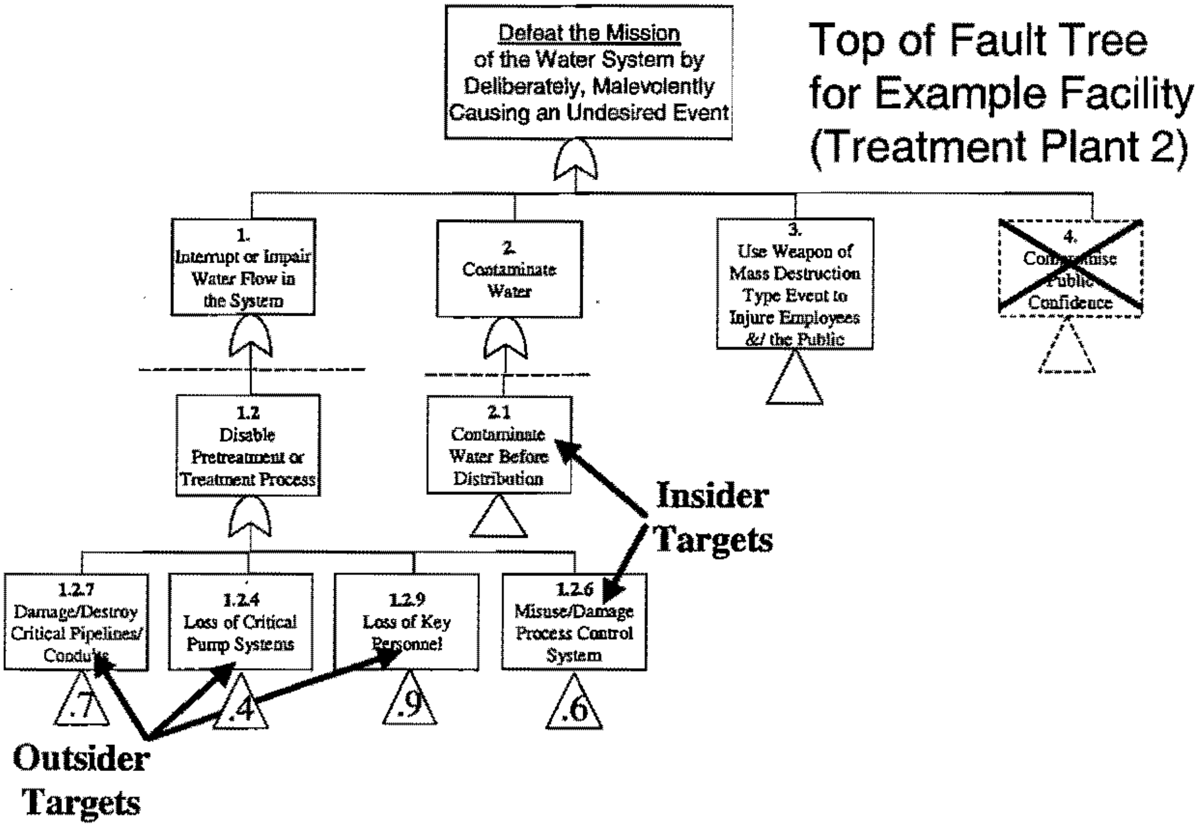

Defeat the Mission of the Water System by Deliberately, Malevolently Causing an Undesired Event
Top of Fault Tree for Example Facility (Treatment Plant 2)
1. Interrupt or Impair Water Flow in the System
2. Contaminate Water
3. Use Weapon of Mass Destruction Type Event to Injure Employees &/ the Public
~~4. Compromise Public Confidence~~
1.2 Disable Pretreatment or Treatment Process
2.1 Contaminate Water Before Distribution
Insider Targets
1.2.7 Damage/Destroy Critical Pipelines/ Conduits
1.2.4 Loss of Critical Pump Systems
1.2.9 Loss of Key Personnel
1.2.6 Misuse/Damage Process Control System
.7
.4
.9
.6
Outsider Targets

Figure A.2. Top of the Fault Tree for Treatment Plant 2

Misuse/Damage Control System: The control system is exposed and standalone. The control system equipment is unprotected and allows direct access to the water flowing through the process. There are seven inputs and/or access points through the plant to the treated water.

Loss of Pumps: Three electrical motor and pump assemblies are located in the plant. The pumps are required to move the water through the plant and on to the city pumping stations (Pump Stations 1 and 2). The pump assemblies have exposed workings and are vulnerable to malevolent acts. There are no spare pumps on site.

Loss of Key Personnel: At each of the treatment plants, there is only one treatment plant operator on duty at any time. They have other duties (some processes on the first floor are manual and require their physical presence) and therefore they are not always in the control room. There are 15 certified treatment plant operators on-roll for the entire water utility. Treatment plant operators belong to the union.

This information was used to customize the site-specific fault tree and to identify critical assets. Refer to Section 5.4 for full details.

A.5 Consequence Assessment

After much detailed discussion, the assessment team brainstormed the following list of potential consequence measures:

- Loss of life
- Illnesses
- Impact on water utility ratepayers
- Impact on regional economic base
- Duration of widespread loss of fire protection
- Duration of widespread loss of water potability
- Economic loss
- Number of users impacted
- Cost to repair
- Number of critical customers impacted

Since the water utility focused on the topmost undesired event (interrupt or reduce ability to treat water supply), the following data were collected:

The water utility reviewed its financial records and estimated that they could withstand an economic loss less than $500,000. Anything greater than $2,000,000 would be a great hardship. Reviewing their routine maintenance logs, the water utility determined that it could shut down the treatment plant for 8 hours and not impact their overall mission. They estimated that a shutdown over 24 hours would cause them severe problems. After reviewing their routine maintenance logs and public confidence records, they estimated that impacting less than 200 customers was an acceptable level. They estimated that impacting over 2500 customers would result in a severe consequence.

This information was used to develop the site-specific consequence matrix and to determine the consequence level for each critical asset. Refer to Section 5.6 for full details (consequence measures and matrix for the example water utility).

A.6 Facility Characterization and Physical Protection System for Treatment Plant 2

The facility is located on five acres owned and operated by the water utility. The facility is located 5 miles east of the Bigg Lake and 10 miles from the suburbs. The facility was built in the 1930s as the single treatment facility. Other facilities were added to the processing as the town grew. The Plant 2 complex (1400 ft × 2500 ft) is enclosed by an 8-foot unsensored chainlink fence. The building (100 ft × 100 ft) is two stories tall and constructed of brick and stone. The building has many windows, allowing it to blend in with the local architecture. The plant control room is located on the second floor. The control room is operated 24/7, but the operator has other duties. Therefore, the console is not staffed continuously. All plant chemicals and treatment process areas are located on the first floor. The facility uses one-ton chlorine cylinders for disinfection. They have 4 to 5 on line and 4 to 5 spares at any one time. Three 300-hp motors and pumps are in the first floor high bay area (see Figure A.3). All first floor doors into the building are alarmed during non-operational hours. A loading dock is located on the north side for chemical deliveries. All doors and windows are of typical commercial construction.

All vehicles (private and government), employees, contractors, and deliveries enter through the single vehicle gate. A pedestrian gate is co-located. One contract employee (an unarmed guard) controls access only during operational hours. Access is by recognition of employees or via a daily access list for deliveries and contractors. All security, water, and chemical alarms actuate locally in the plant control room and at the SCADA control center located downtown at the water utility's headquarters. Local law enforcement does not have access to any of the locked facilities, but they are the only armed response.

The water is transported by a 48-inch-diameter steel pipe from Bigg Lake to Treatment Plant 2. This main delivery pipe was constructed in the 1930s. Performance-testing on equivalent pipes determined that the pipe could withstand 110 psi. The pipe enters the facility above ground through the perimeter fence into a holding pond. The pipe is supported by reinforced concrete stands leaving the pipe exposed. The water is then pumped through the treatment process. A minimum of two pumps is required to meet the plant daily demand/capacity. The required chemicals are added to the water through intakes located on the first floor of the treatment facility and regulated by SCADA through onsite operators.

This information was used to evaluate the existing physical protection and operating systems, and to identify vulnerabilities. Refer to Section 5.7.2 for full details.

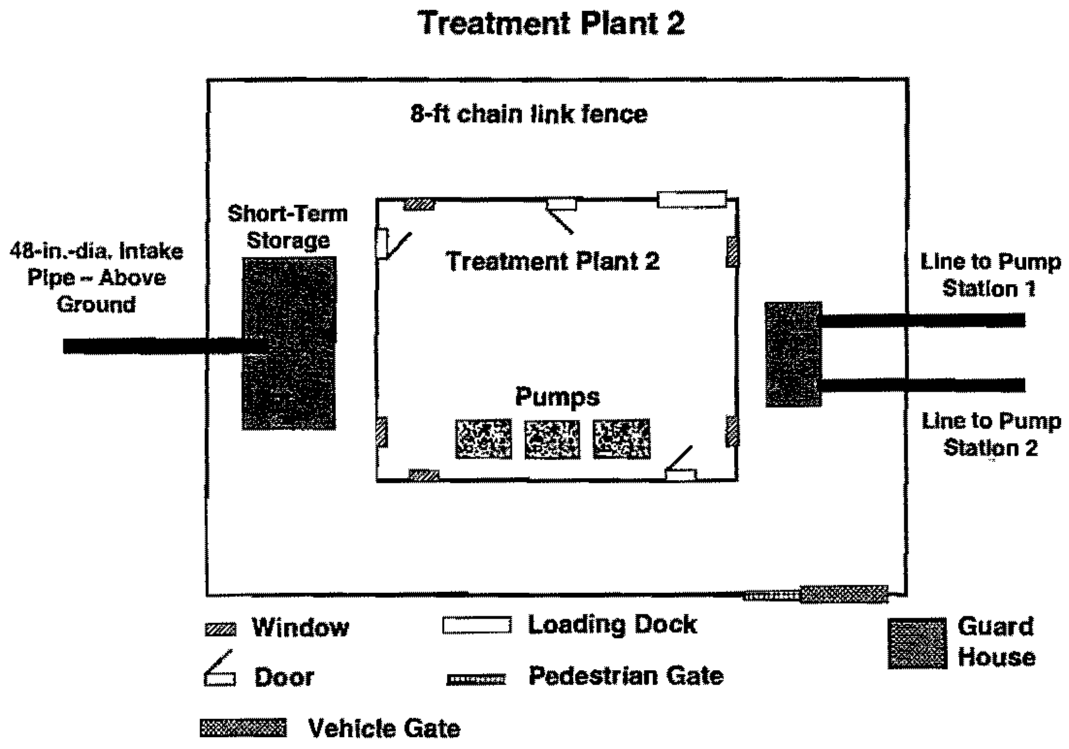


Figure A.3. Schematic of Treatment Plant 2

A.7 Onsite SCADA Interview

The assessment team interviewed the SCADA personnel (system administrators and operators) following a detailed structured interviewing tool to characterize the SCADA system. Responses from the onsite interview were as follows:

- The SCADA server equipment is within a locked room in a controlled access building
- Manual operation is an option if the SCADA system fails
- The SCADA system includes leased lines from the local phone company
- The city department of public works ATM network is used for SCADA operations

    - Data separation and protection strategies have not been considered or implemented
- SCADA and IOC software are not designed with any inherent security
- Data transmissions are not encrypted or authenticated
- Operating systems security patches are not maintained
- Subcontracted janitors and security guards have access to control room instrumentation
    - Contracting agency must provide names and social security numbers of workers
    - A water utility employee is in the main control room (downtown) at all times
- The original SCADA system configuration management documents from the vendor are available
- Remote access connectivity to the SCADA network is used for troubleshooting
    - Remote access is not a critical capability, it is a convenience
- Passwords are used for access control of remote access
    - Passwords are shared
    - Passwords are periodically changed (no set period of time between password changes)
    - Management can provide remote access privileges to non-water utility personnel
- Modems are located on servers that can reach all parts of the network through login
- The SCADA network is connected to the business network
- System administrators are aware of critical system components but this information is not formally documented
- The SCADA system has no security policy or plan
- Unnecessary services (such as Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) have not been disabled on the SCADA platforms
- Security alarms for SCADA equipment use the same communication lines as the SCADA control network
- Information sensitivity levels have not been identified
- RTUs are only reachable though the SCADA network or a local console port

    - No direct dial-up accessibility
- RTUs do not use a standard OS such as Windows, Unix, Linux, etc.
- Remote SCADA equipment is contained within locked buildings
    - A number of employees have keys to these buildings
    - Laptops can be connected to the remote equipment if necessary

The two diagrams below provide additional descriptions of the SCADA system. Diagrams are extremely valuable in the SCADA analysis process. Figure A.4 depicts an overlay of the SCADA system on the water utility's other operations, and Figure A.5 illustrates the SCADA network at Treatment Plant #3.

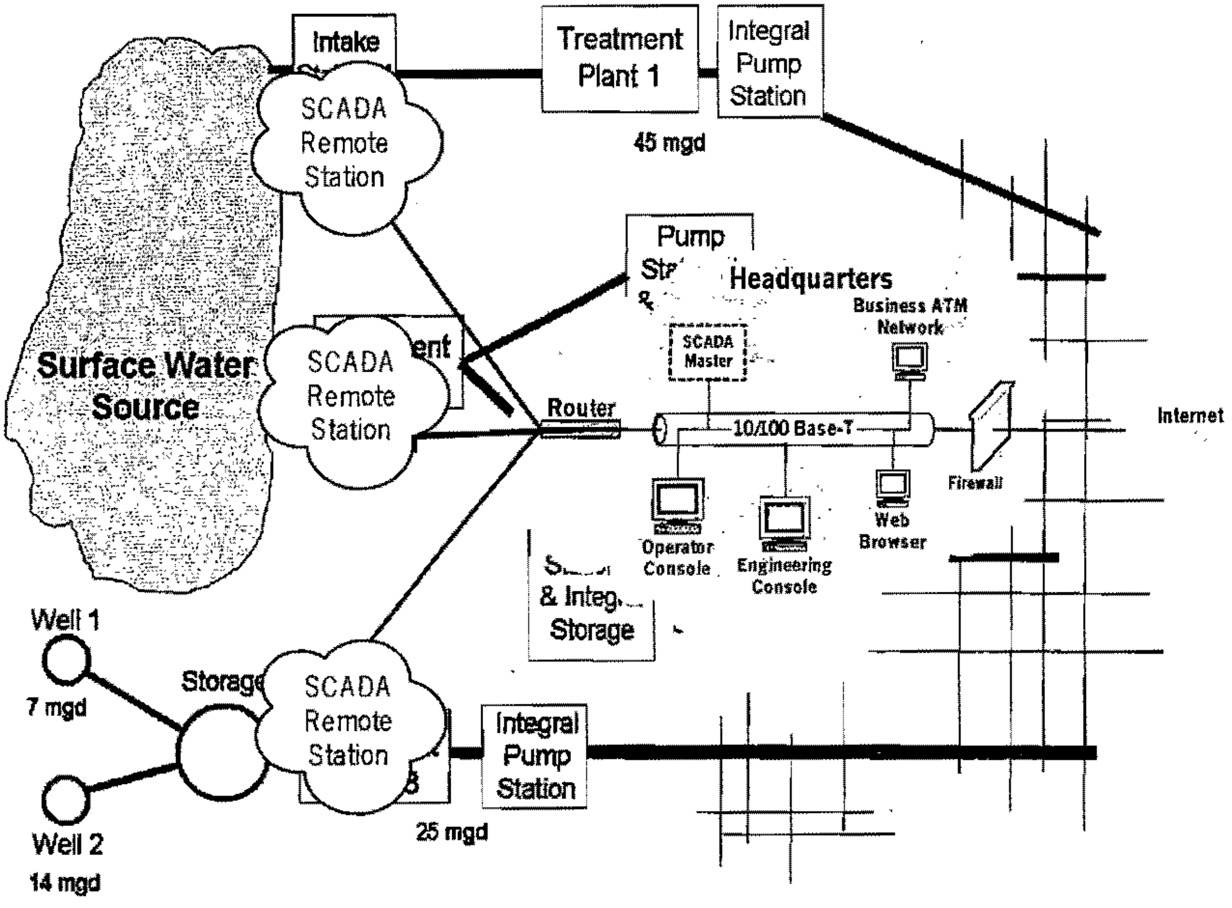


Figure A.4. SCADA Overlay on Example Water Utility

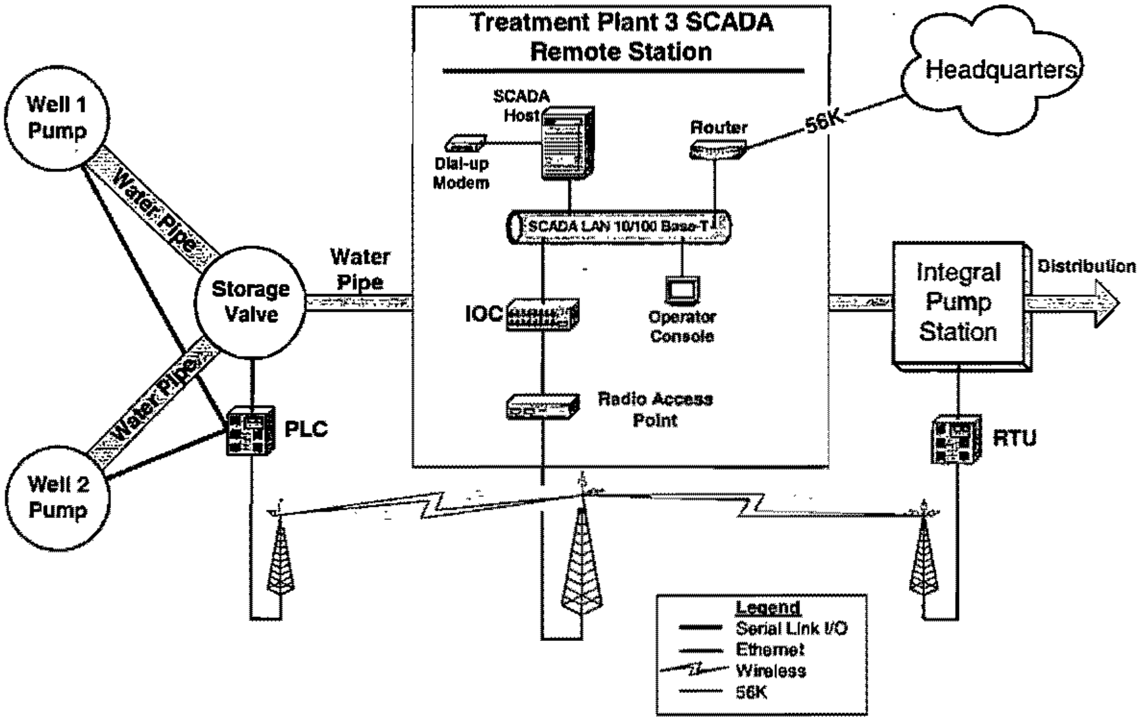


Figure A.5. SCADA Network at Treatment Plant #3 for Example Water Utility

APPENDIX B: PROJECT PLANNING AND TEAM SELECTION

B.1 PROJECT PLANNING

A security risk analysis of a water utility is a limited time project. Using project planning concepts to plan an analysis will provide a great deal of assistance to senior management, the project leader, the assessment team, and supporting staff by ensuring that work essential to the analysis is conducted and senior management's requirements and expectations are met. Planning is an important part of a successful assessment and the amount of time and resources the assessment team devotes to the effort will depend on the size and complexity of the analysis.

Senior management's expectations and requirements must be defined at the very beginning of the project. A project mission statement is then developed based on senior management's input to document the purpose and scope of the project. Objectives are generated from the purpose statement. A work breakdown structure (WBS) (i.e., activities and tasks) is generated to meet the objectives. The WBS is translated into a timeline schedule and a responsibility chart to assign tasks and deadlines to specific assessment team members. For more details on project management refer to the following references:

- Barkley, Bruce, and Saylor, James, 1994. *Customer-Driven Project Management*, McGraw-Hill Inc.
- Ruskin, Arnold. *What Every Engineer Should Know About Project Management*.
- Archibald, Russell. *Managing High-Technology Programs and Projects.*

B.1.1 Work Breakdown Structure

A sample WBS to assist the assessment teams in getting started on a security risk assessment for a water utility is shown in Table B.1.

Table B.1. Work Breakdown Structure for a Risk Assessment

Activity	Tasks	Time Required
Getting Started	• Establish management's commitment to risk assessment and implementation • Identify and organize team members (identify supporting staff and resources) • Collection of water utility information and review of documentation • Preparation for Pre-Planning meeting • Documentation	5 to 7 days
Training	• Coordination and logistics for training • Training for assessment team • Overview training for senior management	4 to 5 days
Pre-Planning Meeting	• Meet with the following: o Management o Local Law Enforcement o State Law Enforcement o FBI o Local Emergency Responders o State Emergency Responders • Develop/document management's requirements • Establish water utility's overall mission, develop mission objectives • Develop Threat Level o Ranges: High, medium, low • Develop Consequence Matrix o Consider WMD-type events • Pairwise Comparison o Mission Objectives, criteria o Facilities	1 to 3 days
Project Planning	• Develop Schedule with milestones and deliverables • Refine team selection and identify supporting staff and resources • Establish team's purpose and objectives and define each member's roles and responsibilities	1 to 2 days

Activity	Tasks	Time Required
Refine Deliverables	• Prioritization of Facilities • Design Basis Threat • Consequence Matrix • Review with management and get agreement • Document	1 to 2 days
Pre-Site Characterization	• Review appropriate documentation and diagrams • Systems-level understanding • Create a preliminary fault tree from site characterization documentation and discussion • Plan and prepare logistics for site characterization	2 to 3 days
Site Characterization	• For a large water utility, a team of 5 to 10 specialists/experts may be required for the onsite survey o SCADA designer/operator o Operations expert o Electrician o Mechanical systems designer o Chemist (contamination, chemical analyst) o Risk assessment analyst o Security professional • The water utility may need to supply counterparts to escort and answer questions	2 to 4 days
	• Interview management on policies, procedures, and documentation • Review the Emergency Response Plan • At the end of the site characterization a 1 to 2 hour feedback session is conducted o Findings o Concerns	1 to 2 days
Refine Deliverables	• Finalize the fault tree • Identify and develop list of critical assets and their consequence level • Summarize and analyze responses and observations from interviewing sessions • Review with management and get agreement • Document	3 to 5 days

Activity	Tasks	Time Required
Analysis	• System effectiveness analysis • Risk Analysis of the current state • List of prioritized targets • Recommendations to reduce risk • Document	2 to 5 weeks
Draft Report	• Make team assignments for documentation • Write draft Report • Team members review draft report	2 to 6 weeks
Feedback Workshop	• Give final draft report to management for review • Review with management o PPS o Operational Security o Consequence Mitigation o Recommendations • Record feedback	2 to 5 days
Final Report	• Incorporate revisions • Determine life cycle costs • Finalize and distribute final report	1 to 2 weeks

B.2 TEAM SELECTION

The assessment team must have a broad and deep understanding of the water utility operations. For the make-up of the assessment team, senior management and the project leader together identify and select members that are appropriate for the scope of work and available resources. Different skill sets are required for different tasks of RAM-W^{SM}. Table B.2 provides a list of the individual participants and team or teams that may be required to accomplish the security risk assessment, the particular tasks for which these teams or individuals bear primary responsibility, and the skill sets that are required to successfully accomplish the tasks. An assessment team with 4 to 8 members with specialized expertise (including the project leader) is a manageable size to conduct a risk assessment effectively and efficiently. There may be several subject matter experts that are interviewed or who support and contribute to the assessment during appropriate phases in the process.

Table B.2. RAM-W^{SM} Team Makeup and Special Skills Requirements

PARTICIPANTS	TASKS	SKILLS
Senior Management Team and Project Leader	• Project Definition and Scope • Identify Team Members • Risk Acceptability • Risk Reduction • Review Report	• Communication • Broad and deep understanding of water utility operations • Working knowledge and experience with the analytic process • Authority and ability to determine acceptable risk level
Project Leader	• Survey Schedule and Information Assembly • Evaluate Impacts • Documentation • Final Report	• Project Management • Delegation • Consequence evaluation • Technical writing
Assessment Team and Subject Matter Experts • Project leader • Operator • Operations mgr./engineer • Maintenance mgr. • Analyst • SCADA System Administrator • Security mgr. • Technical Writer	• Facility Prioritization • Customize Fault Tree • Consequence Assessment • Threat Assessment • Design Basis Threat Definition • Preparation for Site Survey • Site Survey • System Effectiveness Analysis • Risk Analysis • Risk Reduction & Recommendations • Report • Implementation	• Information/data collection and analysis • Ability to interpret and modify fault tree • Broad and deep understanding of water utility operations • Ability to collect data from law enforcement • Expert threat judgment • Working knowledge of the critical functions and assets of the water utility • Knowledge of SCADA and security systems • Working knowledge and experience with the analytic process • Knowledge of security system technologies • Extensive knowledge of the facility operations and structure

APPENDIX C: PROCESS FOR PAIRWISE COMPARISON

To prioritize the major facilities within a water utility system, a simplified pairwise comparison is used. Two or more facilities are compared using stated criteria (developed from mission objectives) in a structured way, resulting in a relative ranking of the facilities. The facilities are ranked in the context of each criterion using the following comparison scale:

With respect to the criterion, the importance of Item One is

much greater than	(5)
greater than	(4)
the same as	(3)
lower than	(2)
much lower than	(1)

the importance of Item Two.

The comparisons of Item One vs. Item Two and Item Two vs. Item One are complementary. For instance, if the importance of Item One is *much greater than* that of Item Two, then the importance of Item Two is *much lower than* that of Item One. Also, if the importance of Item One is *the same as* that of Item Two, then necessarily the importance of Item Two is *the same as* that of Item One.

Ranking Criteria. Mission objectives are developed based on the water utility's overall mission. Criteria are based on the mission objectives. For example a mission objective could be "Provide sufficient fire-fighting flows," the criteria developed based on the mission objective could be "capacity." Because all criteria are not of equal importance, the criteria must be developed and ranked before the facilities are selected and ranked. The criteria are ranked according to relative importance to the mission objectives of the water utility. This provides a weighted criteria ranking that can then be used to create a weighted ranking of the facilities' importance. This is ***the most critical part of the prioritization process*** because it will determine which facility(ies) to consider first for increased security measures or consequence mitigation. Appropriate criteria that are both necessary and sufficient must be carefully developed to allow an accurate system analysis. Failure to allocate adequate time and informed effort to this phase can lead to confusing and ambiguous results.

It is recommended that no more than five criteria be used, with three or four being optimal. For the example water utility four main mission objectives were identified (see Appendix A for more details):

Criterion 1	Provide sufficient fire-fighting flows (**capacity**)
Criterion 2	Greatest geographical service possible (**geographical extent**)
Criterion 3	Serve **critical customers**
Criterion 4	Provide potable water (**water quality**)

Capacity is a measure of the volume of water that can be produced by a particular facility to meet the overall system demand. This has to be reviewed for high and low demand periods, but the focus should be on emergency conditions. **Geographical Extent** is the ability to serve the maximum percentage of the distribution system. Due to factors such as topography and pipe limitations, a facility may be able to meet a large part of the demand, but is not able to serve a large distribution area. **Critical Customers** are water system users unable to be without water for an extended period of time, such as emergency services, water-dependent industry, farming, etc. Finally, **Water Quality** relates to the quality of the water being delivered as defined by established standards. Pumping raw water into the system for fire fighting is of value, but being able to fight fires *and* consume the water is of higher value. Before comparing the criteria, it is critically important that all assessment team members understand the mission and mission objectives of the water utility and agree on the priority order of those missions.

Table C.1 is an example of the criteria placed into a matrix for pairwise comparison. The process starts by selecting the first criterion, **Capacity**, and comparing it to each of the other criteria (compare each row to each column above the diagonal). In this example, the importance to the mission of **Capacity** is deemed to be *greater than* the importance of **Geographical Extent** and is thus given a 4. **Capacity** is judged to have importance *much greater than* **Critical Customers** and is given a 5. This process is followed to complete all the rows **above** the diagonal. Because of the mirror nature of the matrix (i.e., values across the diagonal are complementary), values entered above and below the diagonal will sum to 6. In this example, on the second line, **Geographical Extent** should be rated *lower than* the importance of **Capacity** and a 2 placed into the matrix. This process is followed to complete all the rows below the diagonal and then each rows is summed to determine the "sum" value for the criterion (Table C.2). Before continuing on, a reality check should occur to make sure the assessment team is in agreement over the prioritization of the mission objectives. These priorities will be used during the risk reduction analysis to determine where to begin investing the water utility's resources.

Table C.1. Mission Objectives/Criteria Comparison – Example Water Utility

Mission Comparison	Capacity	Geographical Extent	Critical Customers	Water Quality
Capacity	■	4	5	4
Geographical Extent	2	■	3	4
Critical Customers	1	3	■	4
Water Quality	2	2	2	■

Table C.2. Matrix for Ranking Criteria and Sum Values for Each Criterion

Criteria Comparison	Capacity	Geographical Extent	Critical Customers	Water Quality	Sum
Capacity	■	4	5	4	13
Geographical Extent	2	■	3	4	9
Critical Customers	1	3	■	4	8
Water Quality	2	2	2	■	6

To continue with the example water utility, it is assumed that the utility (surface water) has the facilities and constraints as shown in Figure C.1.

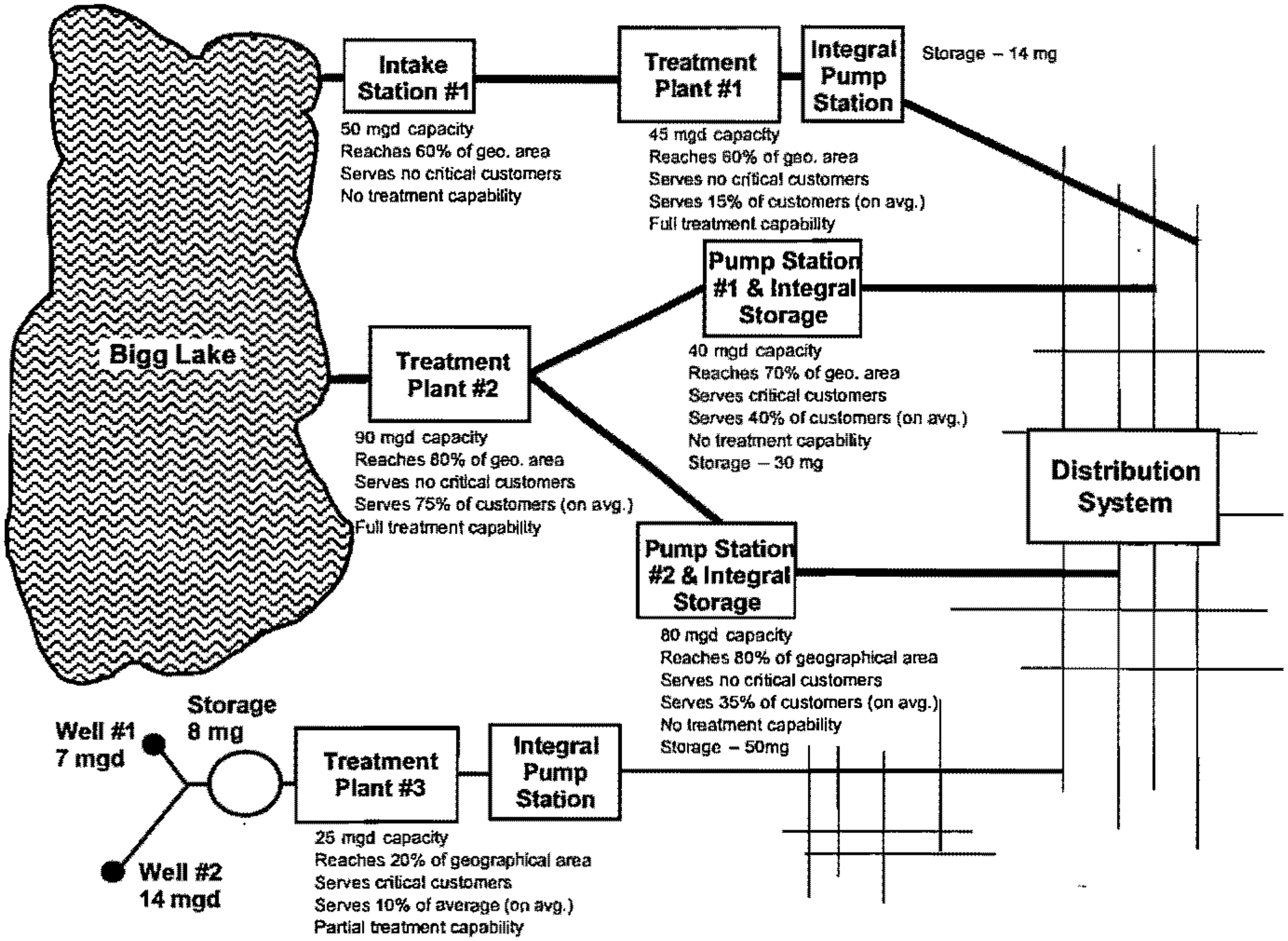

Bigg Lake
Intake Station #1
50 mgd capacity
Reaches 60% of geo. area
Serves no critical customers
No treatment capability
Treatment Plant #1
45 mgd capacity
Reaches 60% of geo. area
Serves no critical customers
Serves 15% of customers (on avg.)
Full treatment capability
Integral Pump Station
Storage – 14 mg
Pump Station #1 & Integral Storage
40 mgd capacity
Reaches 70% of geo. area
Serves critical customers
Serves 40% of customers (on avg.)
No treatment capability
Storage – 30 mg
Treatment Plant #2
90 mgd capacity
Reaches 80% of geo. area
Serves no critical customers
Serves 75% of customers (on avg.)
Full treatment capability
Pump Station #2 & Integral Storage
80 mgd capacity
Reaches 80% of geographical area
Serves no critical customers
Serves 35% of customers (on avg.)
No treatment capability
Storage – 50mg
Distribution System
Well #1
7 mgd
Storage
8 mg
Well #2
14 mgd
Treatment Plant #3
25 mgd capacity
Reaches 20% of geographical area
Serves critical customers
Serves 10% of average (on avg.)
Partial treatment capability
Integral Pump Station

Figure C.1. Example Water Utility System

To begin the process of prioritizing the facilities, the facilities are compared for each of the criteria. A separate sheet is used for each criterion. In Table C.3, the criterion **Capacity** is used to compare the facilities. As drawn above, Intake Station 1, Treatment Plant 1, and the Integral Pump Station located at Treatment Plant 1 can only be operated in a series; therefore, these facilities should be considered as one item. If any one of these facilities were utilized by other facilities, then they would be considered separately. If, for example, water from Intake Station 1 could be routed to Treatment Plant 2, then Intake Station 1 has value beyond just the series combination with Treatment Plant 1.

The same procedure used to prioritize the criteria is used to prioritize the facilities. In the example, when **Treatment Plant 1** is compared to **Treatment Plant 2** in terms of **Capacity**, it is determined that the importance of **Treatment Plant 1** (capacity = 50 mgd) is *much lower than* the importance of **Treatment Plant 2** (capacity = 90 mgd). A "1" is inserted into the matrix. Likewise, **Treatment Plant 1** is determined to be *much greater than* **Treatment Plant 3** (capacity = 10 mgd) in importance for this criterion, and a 5 is inserted in the matrix. Continue in this manner to complete all squares **above** the diagonal. The mirror images **below** the diagonal can then be completed and the rows summed. The **Weighted Number** for a facility is arrived at by multiplying the sum for that facility by the sum for that criterion. In this example, **Treatment Plant 1** has a sum of 11, which is multiplied by 13, the sum for the criterion **Capacity** (from Table C.3), yielding a **Weighted Number** of 143. The remaining sums for the facilities are also multiplied by 13, the sum used to rank the criterion **Capacity** and placed in the last column ("weighted number") to complete the matrix (Table C.3).

Table C.3. Facility Comparison – Example Water Utility (Criterion "Capacity")

Facility Comparison (Criteria = Capacity, Sum = 13)	Treatment Plant #1	Treatment Plant #2	Treatment Plant #3	Pump Station #1	Pump Station #2	Sum	Weighted Number (Criteria Sum X Sum)
Treatment Plant #1	■	1	5	3	2	11	143
Treatment Plant #2	5	■	5	4	3	17	221
Treatment Plant #3	1	1	■	1	1	4	52
Pump Station #1	3	2	5	■	2	12	156
Pump Station #2	4	3	5	4	■	16	208

This pairwise comparison is applied to each criterion developed and defined by the assessment team and a facility comparison matrix similar to Table C.3 completed for each criterion (i.e., continue the same process for "geographical extent," "critical customers," and "water quality"). Once all the comparisons are completed and the **Weighted Numbers** determined, a final facility matrix is completed to compare and rank the facilities (Table C.4) based on all the criteria. The weight of the criterion **Capacity** plays a major role in the analysis; thus the assessment team should agree on the importance of this criterion. If this is indeed correct, the highest prioritized facilities would be considered first for a comprehensive security risk assessment.

Table C.4. Facility Comparison and Ranking - Example Water Utility (All Criteria)

Facility Comparison Based on all criteria	Capacity	Geographical Extent	Critical Customers	Water Quality	Sum	Rank
Treatment Plant #1	143	99	80	108	430	3
Treatment Plant #2	221	144	80	108	553	1
Treatment Plant #3	52	27	160	84	323	5
Pump Station #1	156	117	80	30	383	4
Pump Station #2	208	153	80	30	471	2

APPENDIX D: THREAT ASSESSMENT

Appendix D contains:

- Definitions for the low, medium, high, and very high-level outsider threat
  - Examples of outsider threats
- Definitions for the low, medium, and high insider threat
  - Examples of insider threats
- Definitions for the low, medium, and high cyber hacker threat
  - Examples of insider and outsider hacker threats
- Definition for collusion
- Blank Threat Analysis Worksheets for
  - Outsider Threat
  - Insider Threat – Part 1
  - Insider Threat – Part 2
  - Summary Description

D.1 OUTSIDER THREAT DEFINITIONS

Low-Level Threat. One or two outsiders, vandals with no authorized access or inside information, using portable hand tools with the intent to inflict physical damage to the water utility facility or theft of water utility property or equipment. These outsiders do not intend to cause physical harm to water utility employees or to end-users.

Medium-Level Threat. A group of one to three outsiders equipped with sophisticated tools and weapons. All equipment is person portable and easily obtainable. The outsiders have limited knowledge of the security system and of the water operations. The outsiders' goal is to inhibit delivery of water by causing damage to critical assets of the water utility facility.

High-Level Threat. An organized, highly motivated group of up to five outsiders, equipped with sophisticated tools, explosives, weapons, and possibly chemical or biological agents. All equipment is person portable and easily obtainable. The outsiders have extensive knowledge of the security system and of the water operations. They also have sophisticated cyber capabilities with moderate resources, including a combination of physical and cyber attacks on the water system assets to inhibit the delivery of water. The outsiders can work as a single unit or in teams to achieve their goals. The outsiders' goal is to inhibit delivery of water by causing damage to water utility critical assets or to introduce chemical/biological agents into the water supply to harm end users.

Very High Level Threat. This group of adversaries possess all the attributes that the outsider-high level threat has plus larger than backpack quantities of explosives (truck bombs) and chemical, biological, and radiological materials with the intent to use them to cause massive deaths and inhibit the distribution of water.

D.1.2 Outsider Threat Examples

Example 1. A single outsider, with no authorized access or inside information, using hand tools and small power tools, who intends to inflict sufficient physical damage to the assets of the water utility to impede delivery of water for X hours for Y users. The outsider does not intend to cause physical harm to water utility employees or to end-users.

Example 2. A single former employee, with no authorized access, but having knowledge of the system, using hand tools and small power tools. The former employee's goal is to damage assets of the water utility to impede delivery of water for X hours and Y users and/or to introduce substances (chemicals available at the water utility only) into the water supply to harm (make ill, kill) end-users.

Example 3. A group of one to three terrorists with sophisticated tools, explosives, and weapons. The terrorists' goal is to damage assets of the water utility to impede delivery of water for X hours and Y users and/or to introduce substances (chemicals available at the water utility only) into the water supply to harm (make ill, kill) end-users.

D.2 INSIDER THREAT DEFINITIONS

Low-Level Threat. One insider (employee or authorized contractor) with access to onsite hand and power tools whose intent is to inflict physical damage to the water utility or theft of water utility property or equipment.

Medium-Level Threat. A single, motivated employee or contractor working unaccompanied with authorized access, possessing extensive knowledge of the water operations, the emergency response, the security systems, and the cyber (including SCADA) systems. The insider has access to hand and power tools and authorization to access the chemicals available at the water utility. The insider has knowledge of the security procedures and uses this knowledge to achieve their goals. The insider's goal is to inhibit delivery of water by damaging or manipulating assets of the water utility or to introduce substances (onsite chemicals) into the water supply to harm end users. This insider has power-user types of skills. The cyber adversary has console or network access to all of the control equipment in one facility, and may, through knowledge of the Supervisory Control and Data Acquisition (SCADA) system, be capable of manipulating the entire system.

High-Level Threat. A single motivated or disgruntled employee or authorized contractor working unaccompanied with authorized access, possessing extensive knowledge of the water system, the security system, and detailed knowledge of the SCADA hardware and software. This insider has access to the same equipment as the medium-level threat but possesses greater knowledge and access to SCADA hardware and software. The insider-high adversary also may use handguns to intimidate or harm water utility personnel.

D.2.1 Insider Threat Examples

Example 1. A former disgruntled employee or contractor with limited access to some facilities (water utility has no key control procedure/process), has some limited knowledge of the water system and security system, and would use available hand and power tools. The former employee/contractor's goal is to damage or steal property.

Example 2. A single employee with authorized access, possessing knowledge of the water system, using hand and power tools readily available (will not bring their own tools), with access to the chemicals available at the water utility. The employee has knowledge of the security system. The employee's goal is to damage assets of the water utility facility to impede delivery of water for X hours and Y users and/or to introduce substances into the water supply to harm (make ill, kill) end-users.

D.3 Hacker Threat Definitions

Low-Level Threat. An individual with no insider knowledge of the water utility. Access is via Internet only. Minor cyber vandalism to non-critical business areas.

Medium-Level Threat. An individual with limited knowledge of Information Technology (IT) structure for the water utility. This individual may have direct access via modem or PC connected to IT structure and may have and use sophisticated hacker tools to compromise the systems. Actions may include: denial of service, and disruption of some business functions.

High-Level Threat. An individual or small group. They may possess full knowledge of IT infrastructure and the SCADA system, have access to the administrator function, and may coordinate a cyber attack with a physical attack. May use sophisticated network sniffing gear and/or other hacker tools. Actions may include a coordinated cyber attack, with the destruction of data and systems. Business continuity is threatened.

D.3.1 Hacker Threat Examples

Outsider Threat Example. A single hacker, with no authorized access or inside information, attempting to remotely break into the SCADA system, who intends to take control of various assets and/or deny access to the control system. The outsider does not intend to cause physical harm to water utility employees or to end-users.

Insider Threat Example. A single employee with authorized access, possessing knowledge of the SCADA system. The employee's goal is to damage the assets of the water utility through manipulation of the SCADA system to impede delivery of water for X hours and Y users and/or to introduce substances into the water, or reduce the water quality through altered treatment processes, to harm (make ill, kill) end-users.

D.4 COLLUSION

Collusion is defined as an insider working together with Medium-, High-,or Very High-Level Threat Outsiders. A passive insider would brief the outsiders giving full details of the water operations, providing maps and diagrams, and describing the emergency and the security systems. An active insider (can be violent or non-violent) would prepare the site systems for the outsiders and actively engage to some degree with the attack. This threat would have attributes from a combination of the insider and outsider threats. Collusion was not evaluated for the example water utility.

D.5 Water System Threat Analysis Worksheets

D.5.1 Worksheet for the Outsider Threat Analysis

Table D.1 is a water system threat analysis worksheet (a completed worksheet for the example water utility is shown in Section 4.5.1). The worksheet lists the type of information required to describe the outsider threat. Table D.4 provides a format to summarize the type and capabilities of the potential threat spectrum for the water utility. This information will later be used to develop adversary strategies and scenarios and evaluate system effectiveness for these scenarios. The assessment team will complete this worksheet for **each** potential category of outsider adversary. All of information that the assessment team will collect, organize, and analyze will help them make an informed decision about the outsider threat.

The following guidance will help in completing the form:

Line 1: Description of historical incidents associated with the threat type.

Line 2: Review of potential threats to similar facilities.

Line 3: Motivations that might prompt potential adversaries to undertake criminal actions can be grouped into three broad categories. Ideological motivations are those linked to a political or philosophical system. Economic motivations involve a desire for financial gain. Personal motivations pertain to the special situations of specific individuals.

Line 4: Estimate the number of adversaries.

Line 5: Adversaries will be expected to use any tactics that increase their chances of achieving their objective. These tactics include force, stealth, and deceit. A force tactic is one in which the adversary overpowers the system or personnel with no attempt to hide their intention. Stealth refers to the adversary tying to enter a facility covertly; the goal is to remain undiscovered for as long as possible. Deceit implies the use of real or forged credentials to gain access to information or assets. Adversaries could use a combination of tactics (e.g., a criminal might use stealth and deceit).

Line 6: Available tools include weapons, hand and power tools, and cutting torches, as well as any equipment located at the site of the attack. This might include such things as chemicals, forklifts, or company vehicles.

Line 7: Will the adversary be armed and if so, with what type of weapons?

Line 8: Will the adversary have explosives and if so, what kind?

Line 9: Describe their means of transportation (truck, helicopter, etc.)

Line 10: Where and how can the adversary get diagrams and information about the water utility's operations and security system (public information, tours, insider knowledge, websites, etc)?

Line 11: How sophisticated is the adversary?

Line 12: How well supported is the adversary?

Line 13: Will the adversary have insider assistance?

Table D.1. Water System Outsider Threat Analysis Worksheet

WATER SYSTEM OUTSIDER THREAT ANALYSIS WORKSHEET	
Utility:	
Date:	**Recorded by:**
Adversary:	**Is this a continuation sheet? Y N** (circle)
Information Category	**Description**
1. Incidents (Historical)	
2. Has the adversary targeted the water utility or a similar (nearby) facility?	
3. Motivation (ideological, economic, or personal)	
4. Expected number of adversaries	
5. Tactics	
6. Equipment	
7. Weapons	
8. Explosives	
9. Transportation	
10. Intelligence gathering means	
11. Technical skills and knowledge	
12. Financial resources	
13. Potential for collusion with insider	

Table D.2 is the Insider Threat Analysis Worksheet. The different types of insiders at a water utility should be listed and the information in the table completed. Types of insiders might include the security designer, SCADA operator, maintenance person, engineer, clerical workers, plant manager, security guard, and so on. The assessment team evaluates (based on interviews) about how often each type of insider has access to critical facilities (assets), the security system, and the SCADA system. Qualitative indicators "never," "occasionally," and "often" are used to indicate the frequency of access for each type of insider. Table D.3 (Part 2 Worksheet) lists the type of information required to describe the insider and is similar to the outsider threat worksheet. Both these tables are completed for the example water utility (Section 4.5.2).

Table D.2. Water System Insider Threat Analysis Worksheet – Part 1

WATER SYSTEM INSIDER THREAT ANALYSIS WORKSHEET–PART 1	
Utility:	
Date:	Recorded by:
Adversary:	Is this a continuation sheet: □ Yes □ No
List insider positions of concern: • • • • • • •	

To complete the section below, indicate the potential of frequency for each insider position with the following qualitative indicators: Never, Occasionally, Often

Insider Position	***Access to Critical Facilities***	***Access to Security System***	***Access to SCADA System***

The following form collects more detailed information and in this case is filled out for the insider threat. The assessment team needs to determine whether they are required to consider an insider as a potential threat. If they do consider an insider they will complete this worksheet for any potential category of insider adversary. This is the kind of information that the assessment team will collect, organize, and analyze so they can make an informed decision about the insider threat.

Table D.3. Water System Insider Threat Analysis Worksheet – Part 2

WATER SYSTEM INSIDER THREAT ANALYSIS WORKSHEET–PART 2	
Utility:	
Date:	Recorded by:
Adversary:	Is this a continuation sheet: □ Yes □ No
Information Category	**Description**
1. Incidents (historical)	
2. Expected number of adversaries	
3. Tactics	
4. Equipment	
5. Technical skills and knowledge	

The outsider and insider worksheets for all potential threats need to be completed and analyzed so that entire threat spectrum can be examined. The examination of the threat spectrum leads to the definition of a DBT. This part of the process is accomplished by consultation between the water utility management, the assessment team, and outside sources such as consultants and local law enforcement agencies, which may have intelligence that relates to the threat. Consideration is given to several factors such as the nature of likely attacks provoked by the local environment, reasonable measures that might be taken to thwart an adversary, physical characteristics of the water utility, etc. The threat spectrum is summarized in Table D.4 and the DBT is selected from this Worksheet.

Table D.4. Water System Threat Analysis Summary for Example Water Utility

Threat Analysis Summary Worksheet					
Adversary	Number	Equipment /Vehicles	Knowledge	Weapons	Tactics
Outsider (Low)					
Outsider (Medium)					
Outsider (High)					
Outsider (Very High)					
Insider (Low)					
Insider (Medium)					
Insider (High)					
Cyber Threat (Low)					
Cyber Threat (Medium)					
Cyber Threat (High)					

An examination of the threat spectrum defined in Table D.4 leads to the definition of a DBT. The proposed DBT should be drafted and reviewed and agreed to by management before proceeding on with the detailed assessment. The final definition of threat for the water utility is required information for the remainder of the risk analysis.

APPENDIX E: FAULT TREE ANALYSIS

The fault tree is a tool used in security risk assessments that logically describes the operations and shows the interconnections between subsystems. They are constructed from the adversary's point of view. Fault trees are, therefore, essentially logic diagrams that, if carefully created and maintained, indicate what an adversary might do to defeat one or more of the mission objectives of the water utility. Sandia developed a Generic Undesired Event fault tree for water utilities that attempts to capture the essential water utility mission(s) and includes a host of likely undesired events.

The symbols are important elements of the fault tree that make up the tree elements. Each of these symbols has specific meaning. The general symbols used in fault tree analyses are shown below. Version 2 of the methodology also includes a large-sheet copy of the generic fault tree.

E.1 FAULT TREE SYMBOLS

E.1.1 UNDESIRED EVENTS

Every boxed item on the tree is an event. The Generic Fault Tree is composed of undesired events. They defeat or impair the ability of the water infrastructure to meet its design objectives. Undesired events describe the misuse, damage, or destruction of critical assets. The tree shows how a malevolent human adversary can defeat the mission objectives by accomplishing one or more undesired events.

E.1.2 "OR GATE" SYMBOL

The top of the "Or Gate" is an arch; the bottom is a chevron. The Undesired Event above the Or Gate occurs if any of the Undesired Events below the Or Gate occur.

E.1.3 "AND GATE" SYMBOL

The top of the "And Gate" is an arch; the bottom is a straight line. The Undesired Event above the And Gate occurs if all of the Undesired Events below the And Gate occur.

E.1.4 "TRANSFER TO" SYMBOL

The symbol is a triangle beneath an event box. When it is inconvenient to develop the tree directly under Undesired Event A, the development is "transferred to" a more convenient location on the page. The Transfer triangle beneath Undesired Event A contains a number by which the development is identified.

E.1.5 "TRANSFER FROM" SYMBOL

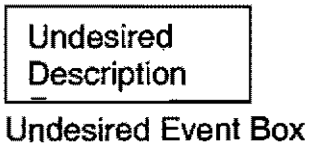
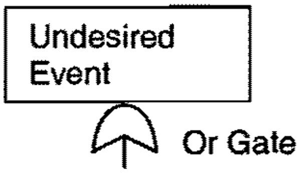
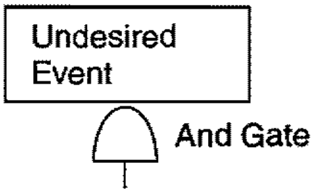
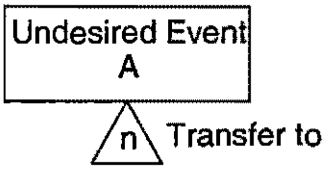
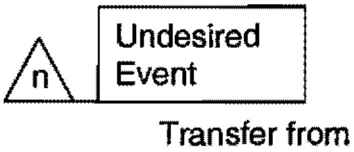
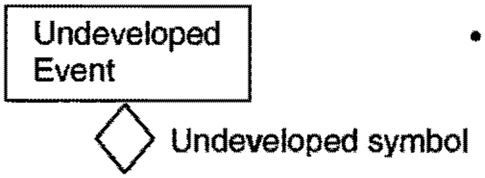
The symbol is a triangle to the left of the event box to which the transfer is made. The triangle contains the same number that appeared in the related "transfer to" triangle.

E.1.6 "UNDEVELOPED EVENTS" SYMBOL

The symbol is a diamond beneath the undeveloped event box. Undeveloped events may be relevant to the mission but are not within the scope of the assessment.

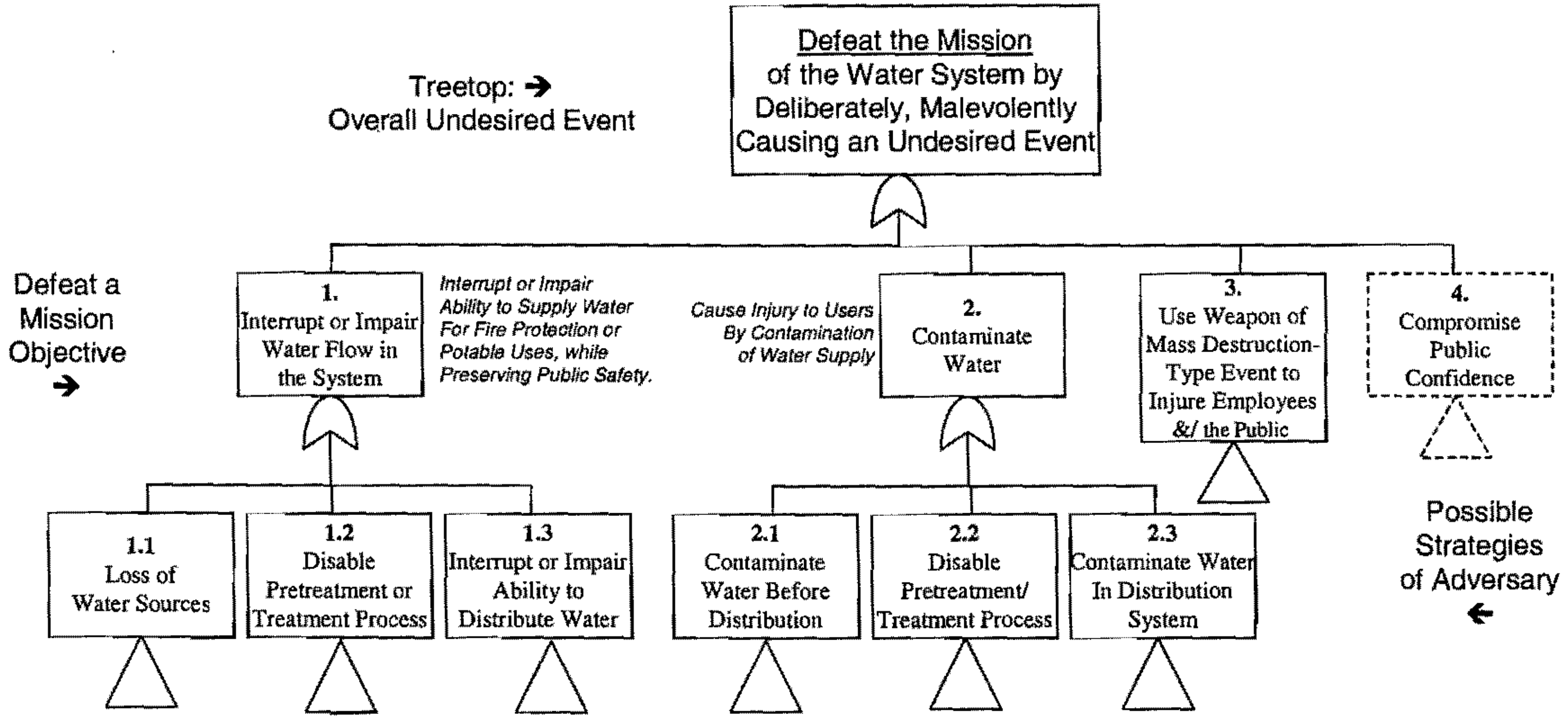
Table E.1 is a key to fault tree symbols.

Table E.1 Fault Tree Symbols

	**Undesired Event** • **Every event in a fault tree is undesired.** • **The highest event on the tree is the Treetop.** • **The lowest event on any path is a Basic Event.** • **Events between the Treetop and the Basic Events are Intermediate Events.**
	**Or Gate** • **The Undesired Event above the Or Gate occurs if any of the Undesired Events below the Or Gate occur.**
	**And Gate** • **The Undesired Event above the And Gate occurs if any of the Undesired Events below the Or Gate occur.**
	**Undesired Event** • **Every event in a fault tree is undesired.** • **The highest event on the tree is the Treetop.** • **The lowest event on any path is a Basic Event.** • **Events between the Treetop and the Basic Events are Intermediate Events.**
	**"Transfer to" Symbol** • **When it is inconvenient to develop the tree directly Undesired Event A, the development is "transferred to" a more convenient location on the page. The Transfer triangle beneath Undesired Event A contains a number by which the development is identified.**
	**"Transfer from" Symbol** • **When it is inconvenient to develop the tree directly Undesired Event A, the development is "transferred from" a more convenient location on the page. The Transfer triangle beneath Undesired Event A contains a number by which the development is identified.**

Water System Fault Tree

Top Levels (Generic)



Treetop: ➔
Overall Undesired Event

Defeat the Mission
of the Water System by
Deliberately, Malevolently
Causing an Undesired Event

Defeat a
Mission
Objective
➔

1.
Interrupt or Impair
Water Flow in
the System

*Interrupt or Impair
Ability to Supply Water
For Fire Protection or
Potable Uses, while
Preserving Public Safety.*

*Cause Injury to Users
By Contamination
of Water Supply*

2.
Contaminate
Water

3.
Use Weapon of
Mass Destruction-
Type Event to
Injure Employees
&/ the Public

4.
Compromise
Public
Confidence

1.1
Loss of
Water Sources

1.2
Disable
Pretreatment or
Treatment Process

1.3
Interrupt or Impair
Ability to
Distribute Water

2.1
Contaminate
Water Before
Distribution

2.2
Disable
Pretreatment/
Treatment Process

2.3
Contaminate Water
In Distribution
System

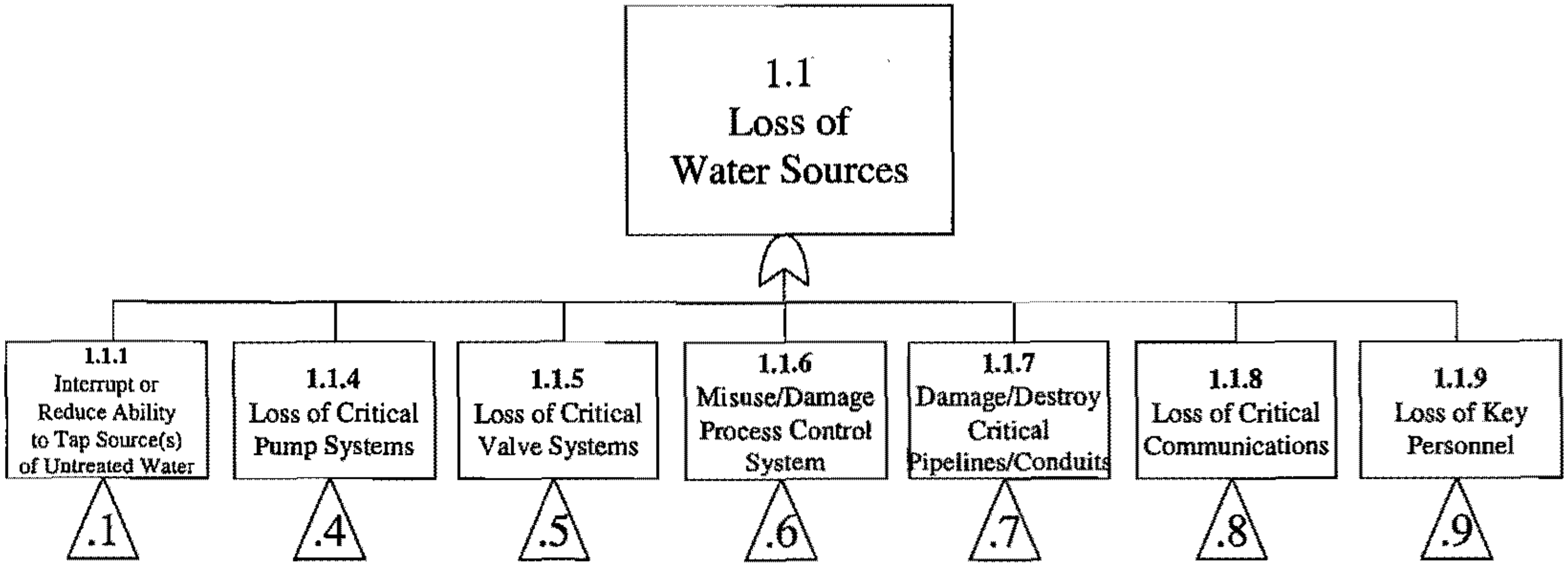
Possible
Strategies
of Adversary
🡐

These events are developed on succeeding slides. Subtrees 2.1, 2.2, and 2.3 develop these events.

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

1.1 Loss of Water Sources

Identify Source(s): ____

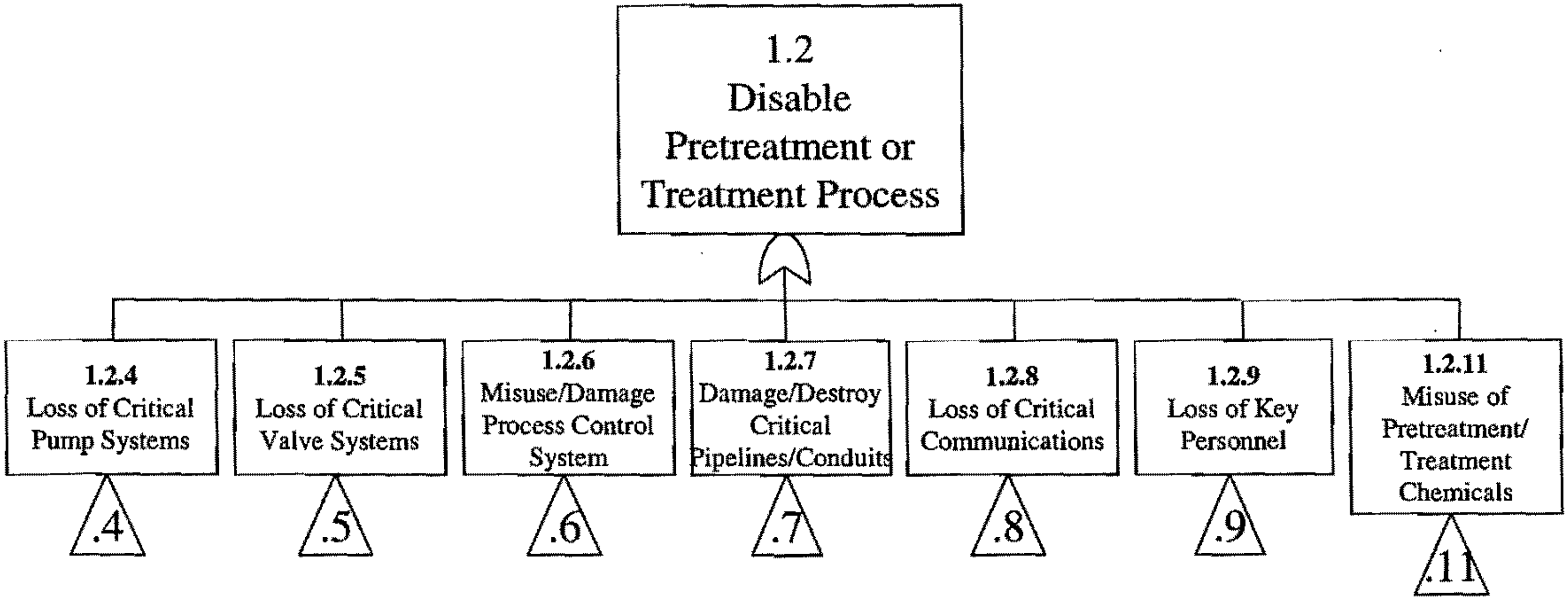


Subtrees .1, .4, .5, .6, .7, .8, and .9 develop these events.

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

1.2 Disable Pretreatment or Treatment Process

Identify Site of Pretreatment or Treatment: ____

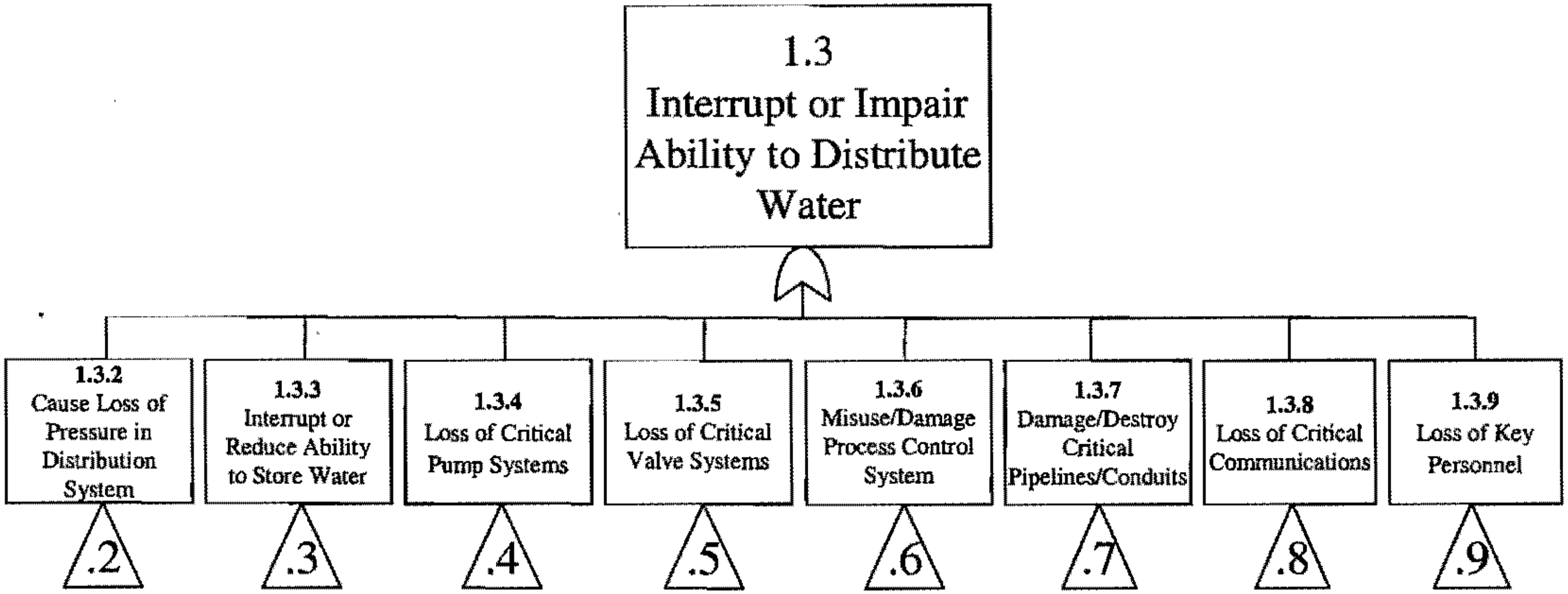


Subtrees .4, .5, .6, .7, .8, .9, and .11 develop these events.

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

1.3 Interrupt or Impair Ability to Distribute Water

Identify Location of Event: ______________________________


1.3
Interrupt or Impair Ability to Distribute Water
1.3.2
Cause Loss of Pressure in Distribution System
1.3.3
Interrupt or Reduce Ability to Store Water
1.3.4
Loss of Critical Pump Systems
1.3.5
Loss of Critical Valve Systems
1.3.6
Misuse/Damage Process Control System
1.3.7
Damage/Destroy Critical Pipelines/Conduits
1.3.8
Loss of Critical Communications
1.3.9
Loss of Key Personnel
.2
.3
.4
.5
.6
.7
.8
.9

Subtrees .2, .3, .4, .5, .6, .7, .8, and .9 develop these events.

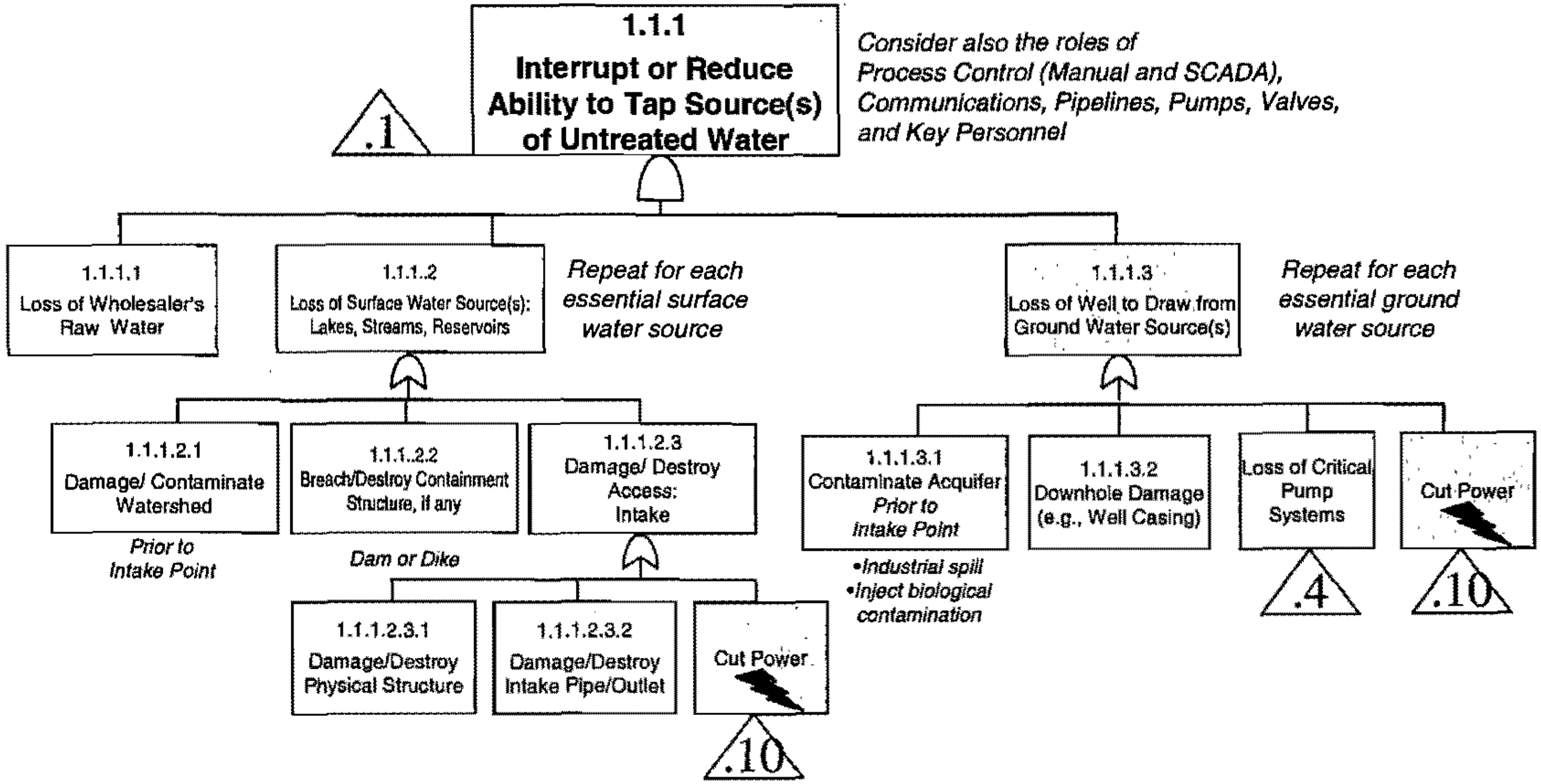
SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

Generic Subtrees

Interrupt or Impair Water Flow in the System

1.1.1 Interrupt or Reduce Ability to Tap Source(s) of Untreated Water

Identify Source(s): ______________________________


1.1.1
Interrupt or Reduce Ability to Tap Source(s) of Untreated Water
.1
1.1.1.1
Loss of Wholesaler's Raw Water
1.1.1.2
Loss of Surface Water Source(s): Lakes, Streams, Reservoirs
1.1.1.3
Loss of Well to Draw from Ground Water Source(s)
1.1.1.2.1
Damage/ Contaminate Watershed
Prior to Intake Point
1.1.1.2.2
Breach/Destroy Containment Structure, if any
Dam or Dike
1.1.1.2.3
Damage/ Destroy Access: Intake
1.1.1.2.3.1
Damage/Destroy Physical Structure
1.1.1.2.3.2
Damage/Destroy Intake Pipe/Outlet
Cut Power
.10
1.1.1.3.1
Contaminate Acquifer Prior to Intake Point
•Industrial spill
•Inject biological contamination
1.1.1.3.2
Downhole Damage (e.g., Well Casing)
Loss of Critical Pump Systems
.4
Cut Power
.10

Consider also the roles of Process Control (Manual and SCADA), Communications, Pipelines, Pumps, Valves, and Key Personnel

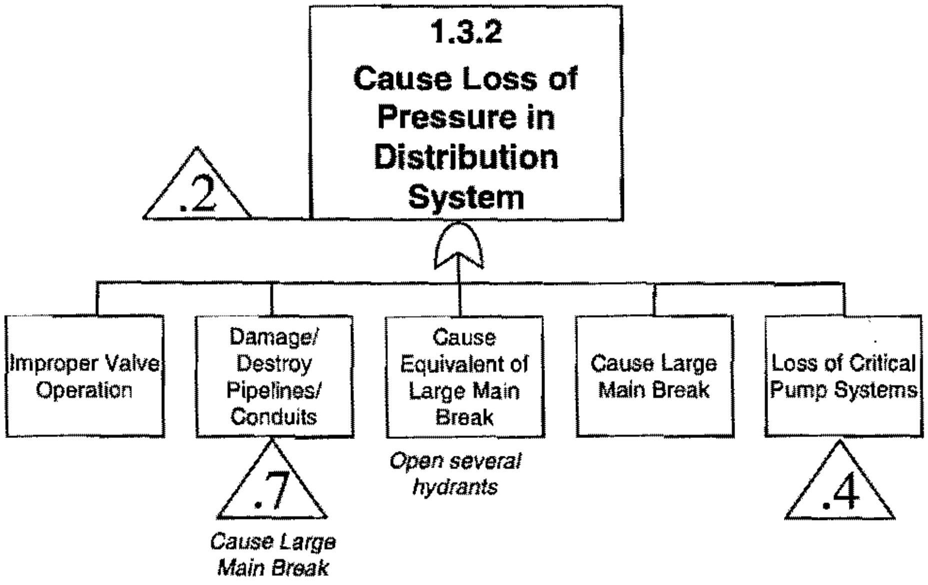
Repeat for each essential surface water source

Repeat for each essential ground water source

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

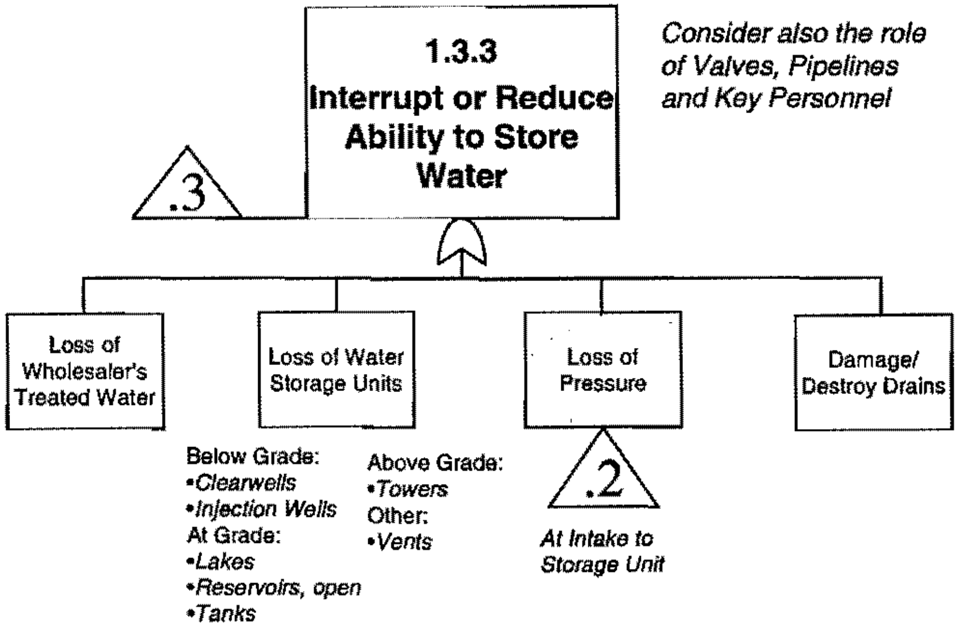
1.3.2 Cause Loss of Pressure in Distribution System

Identify Location of Pressure Loss: ______________________________


1.3.2
Cause Loss of Pressure in Distribution System
.2
Improper Valve Operation
Damage/ Destroy Pipelines/ Conduits
Cause Equivalent of Large Main Break
Cause Large Main Break
Loss of Critical Pump Systems
.7
Open several hydrants
.4
Cause Large Main Break

1.3.3 Interrupt or Reduce Ability to Store Water

Identify Storage Unit: ____


1.3.3
Interrupt or Reduce Ability to Store Water
.3
Loss of Wholesaler's Treated Water
Loss of Water Storage Units
Loss of Pressure
Damage/ Destroy Drains
.2

Consider also the role of Valves, Pipelines and Key Personnel

Below Grade:
- *Clearwells*
- *Injection Wells*

At Grade:
- *Lakes*
- *Reservoirs, open*
- *Tanks*

Above Grade:
- *Towers*

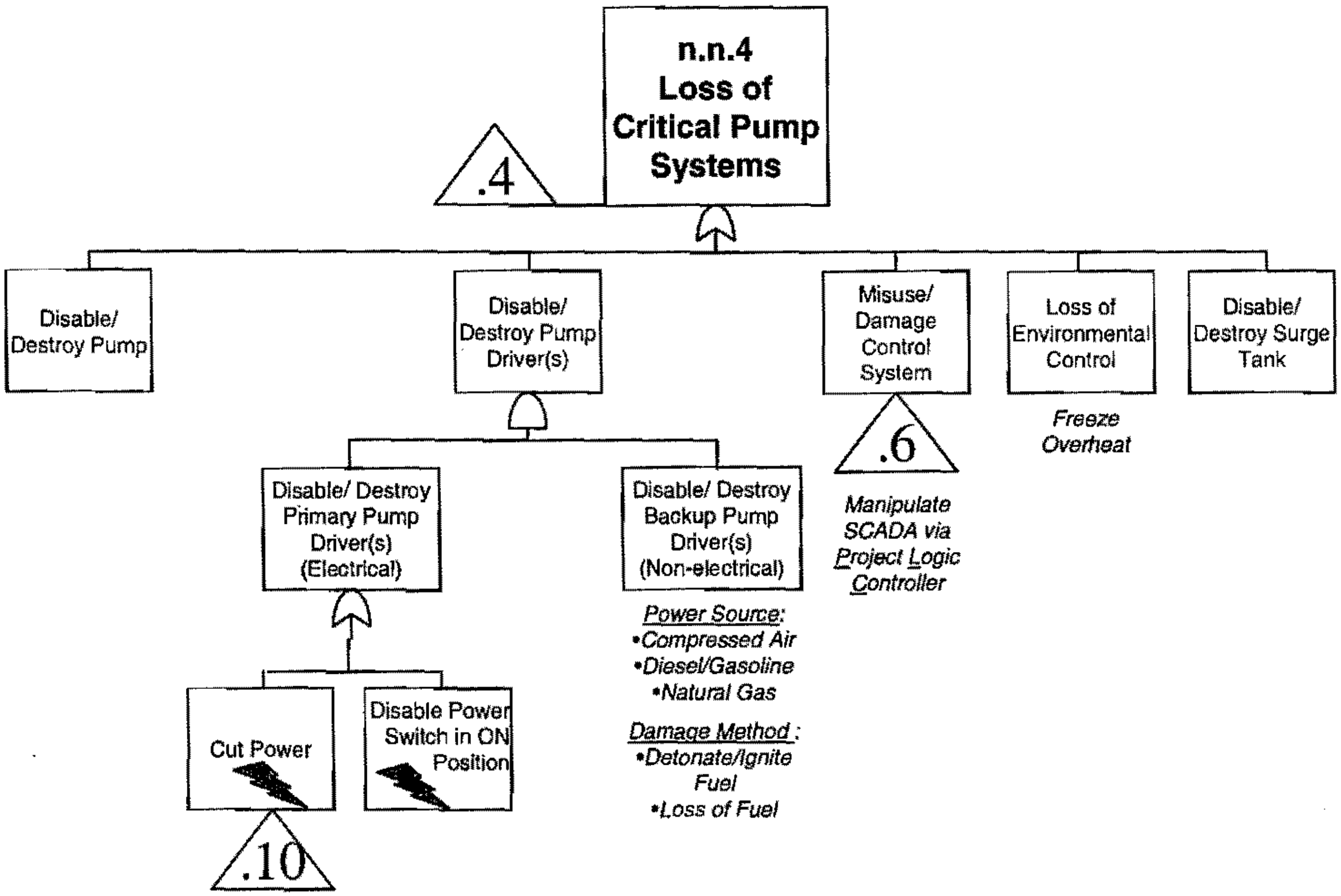
Other:
- *Vents*

At Intake to Storage Unit

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

n.n.4 Loss of Critical Pump Systems

Identify Pump(s): ______________________________



n.n.4 Loss of Critical Pump Systems

.4

Disable/ Destroy Pump

Disable/ Destroy Pump Driver(s)

Misuse/ Damage Control System

.6

Manipulate SCADA via Project Logic Controller

Loss of Environmental Control

Freeze
Overheat

Disable/ Destroy Surge Tank

Disable/ Destroy Primary Pump Driver(s) (Electrical)

Cut Power

.10

Disable Power Switch in ON Position

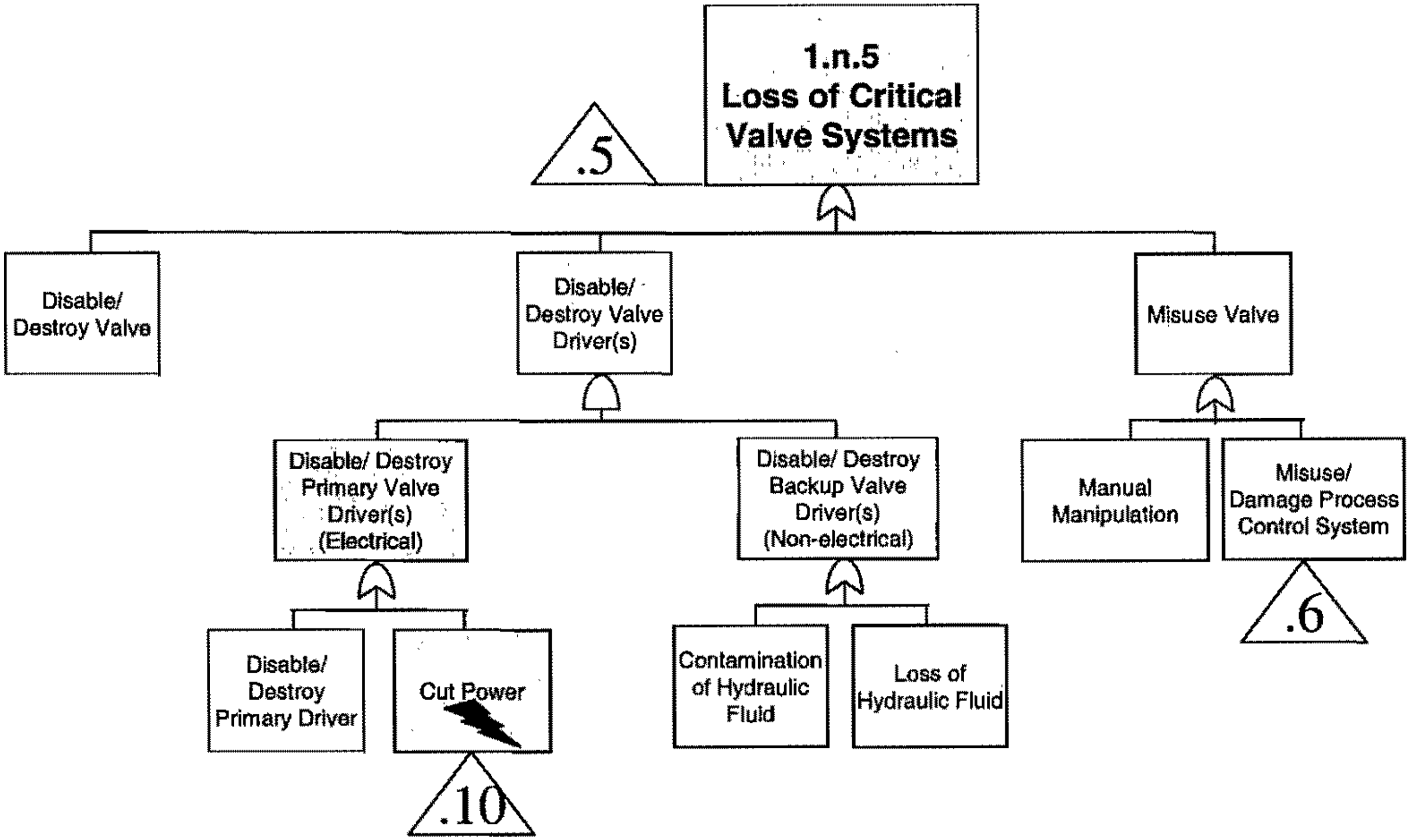
Disable/ Destroy Backup Pump Driver(s) (Non-electrical)

Power Source:
•Compressed Air
•Diesel/Gasoline
•Natural Gas

Damage Method :
•Detonate/Ignite Fuel
•Loss of Fuel

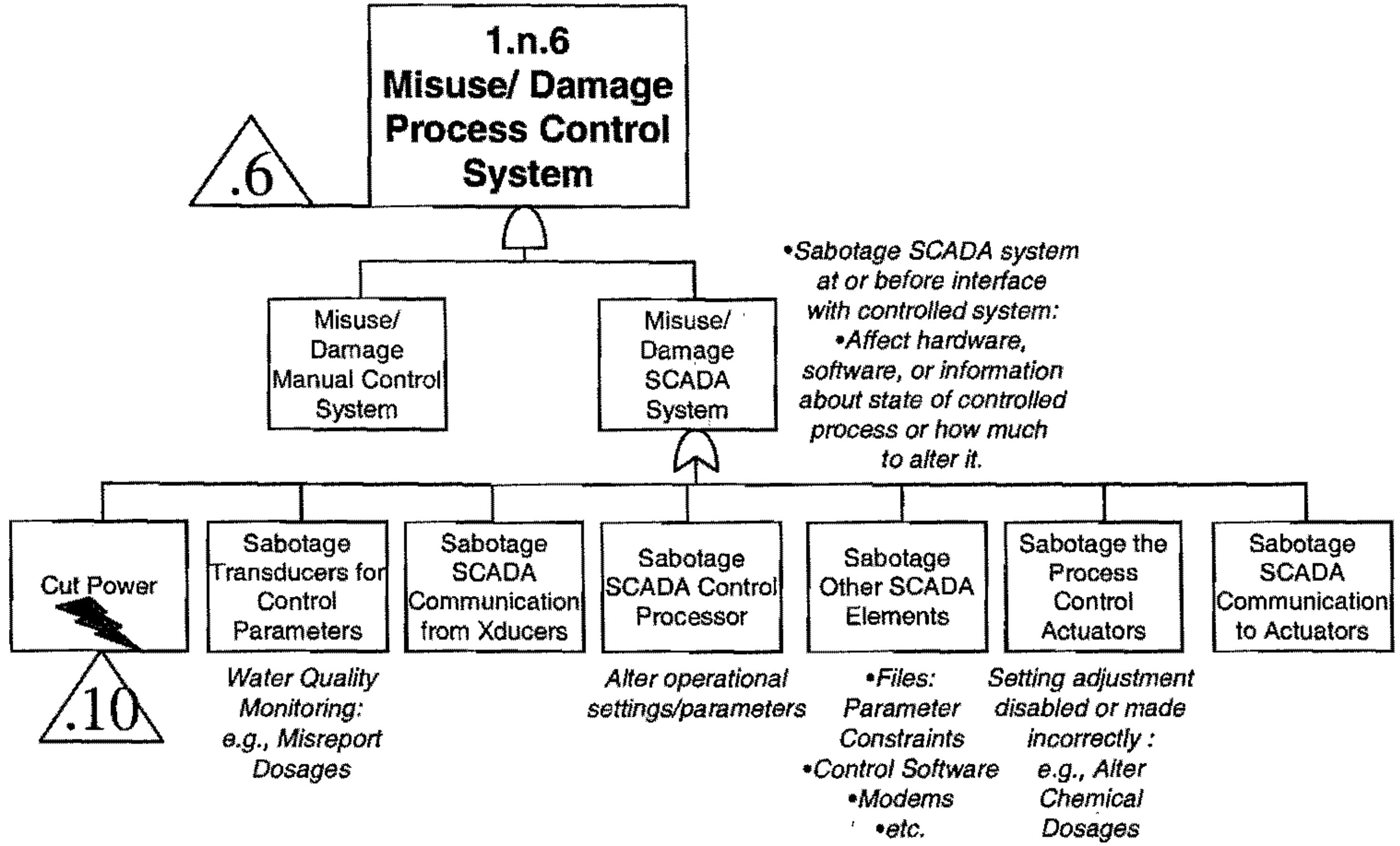
1.n.5 Loss of Critical Valve Systems

Identify Valve(s): ______________________________


1.n.5
Loss of Critical Valve Systems
.5
Disable/ Destroy Valve
Disable/ Destroy Valve Driver(s)
Misuse Valve
Disable/ Destroy Primary Valve Driver(s) (Electrical)
Disable/ Destroy Backup Valve Driver(s) (Non-electrical)
Manual Manipulation
Misuse/ Damage Process Control System
.6
Disable/ Destroy Primary Driver
Cut Power
.10
Contamination of Hydraulic Fluid
Loss of Hydraulic Fluid

1.n.6 Misuse/Damage Process Control System

Identify Control System: ________________________________



1.n.6 Misuse/ Damage Process Control System

.6

Misuse/ Damage Manual Control System

Misuse/ Damage SCADA System

- *Sabotage SCADA system at or before interface with controlled system:*
  - *Affect hardware, software, or information about state of controlled process or how much to alter it.*

Cut Power

.10

Sabotage Transducers for Control Parameters

Water Quality Monitoring: e.g., Misreport Dosages

Sabotage SCADA Communication from Xducers

Sabotage SCADA Control Processor

Alter operational settings/parameters

Sabotage Other SCADA Elements

- *Files: Parameter Constraints*
- *Control Software*
- *Modems*
- *etc.*

Sabotage the Process Control Actuators

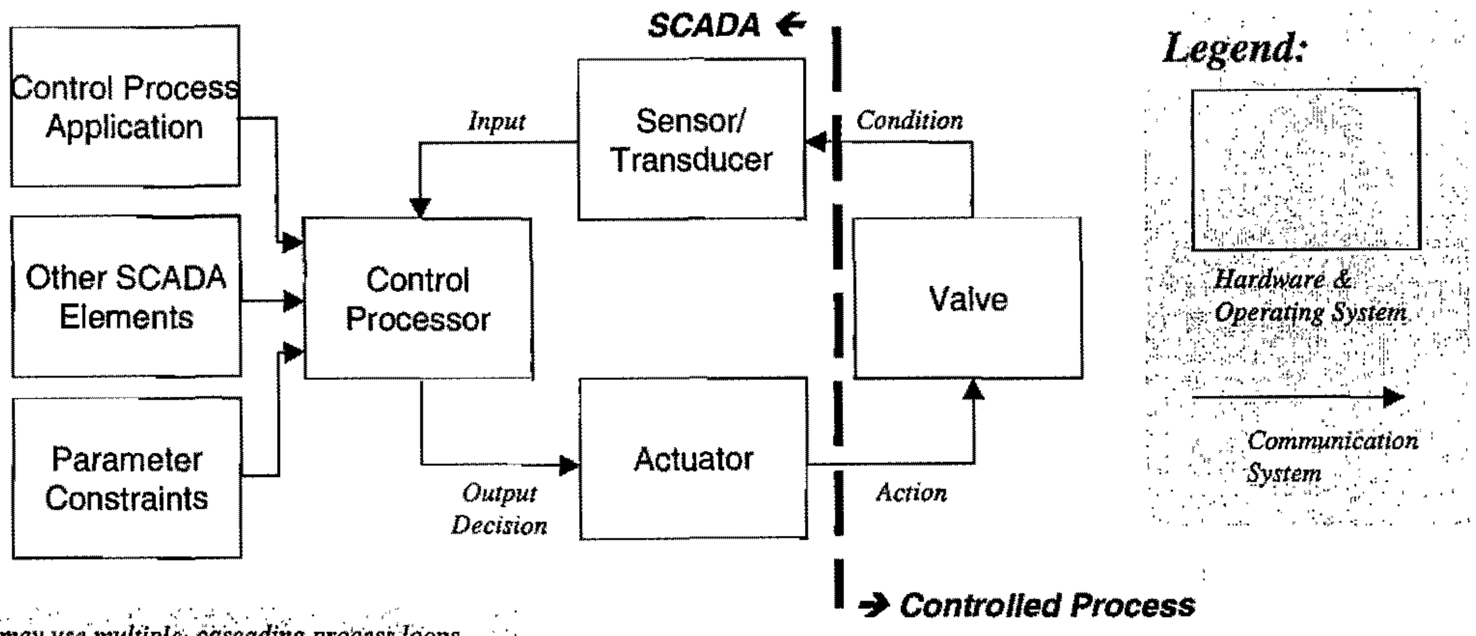
Setting adjustment disabled or made incorrectly : e.g., Alter Chemical Dosages

Sabotage SCADA Communication to Actuators

SCADA - Supervisory Control and Data Acquisition

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

Generic Control Process



SCADA ←

Control Process Application

Other SCADA Elements

Parameter Constraints

Control Processor

Input

Sensor/ Transducer

Output Decision

Actuator

Condition

Valve

Action

→ Controlled Process

Legend:

Hardware & Operating System

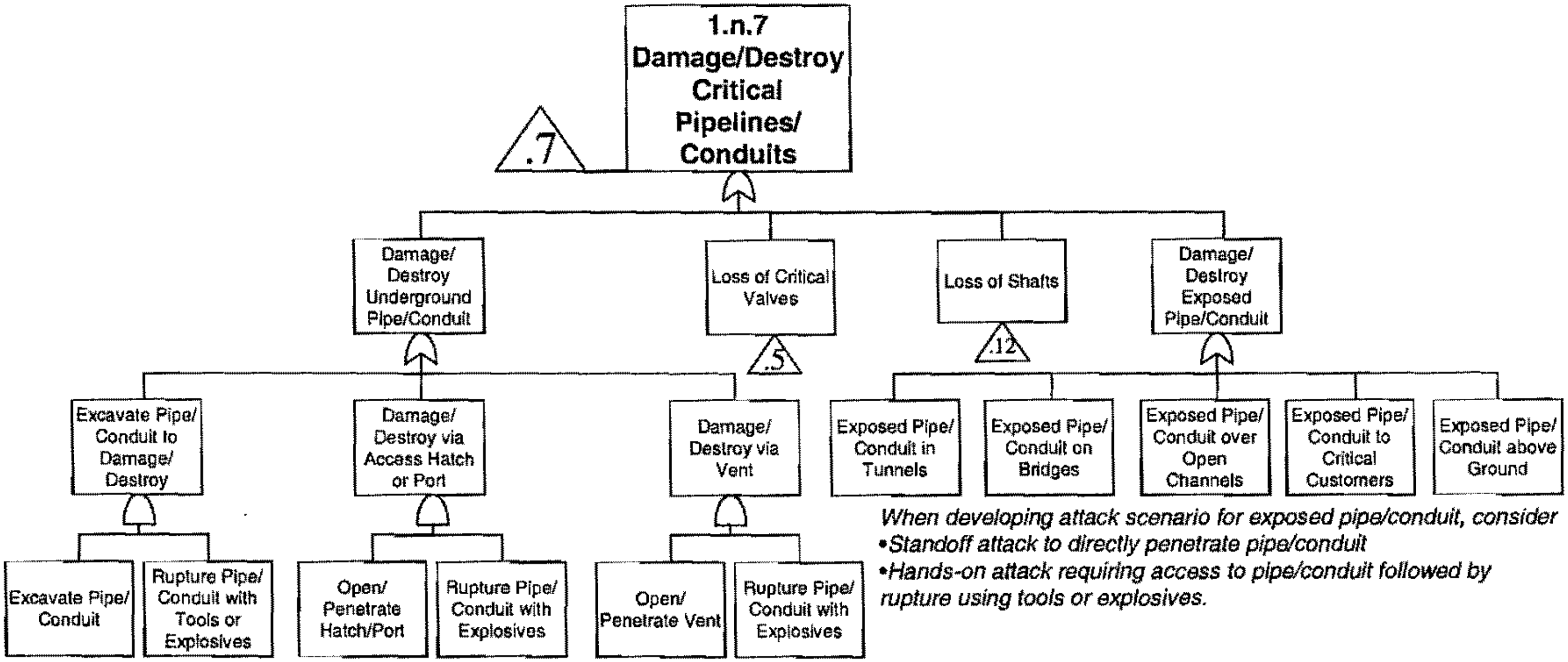
Communication System

•A plant may use multiple, cascading process loops

•Process may be distributed, imbedded, remote, or local

1.n.7 Damage/Destroy Critical Pipelines/Conduits

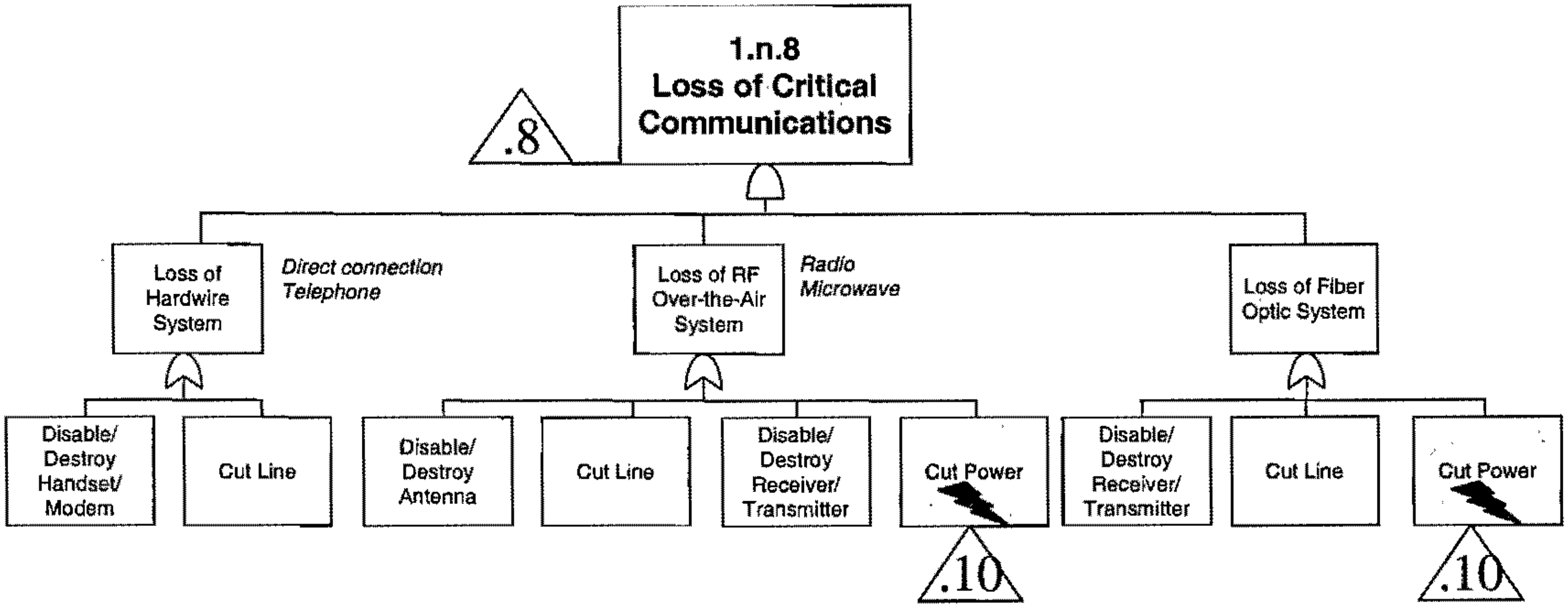
Identify Pipeline/Conduit: ______________________________


1.n.7 Damage/Destroy Critical Pipelines/ Conduits
.7
Damage/ Destroy Underground Pipe/Conduit
Loss of Critical Valves
.5
Loss of Shafts
.12
Damage/ Destroy Exposed Pipe/Conduit
Excavate Pipe/ Conduit to Damage/ Destroy
Damage/ Destroy via Access Hatch or Port
Damage/ Destroy via Vent
Exposed Pipe/ Conduit in Tunnels
Exposed Pipe/ Conduit on Bridges
Exposed Pipe/ Conduit over Open Channels
Exposed Pipe/ Conduit to Critical Customers
Exposed Pipe/ Conduit above Ground
Excavate Pipe/ Conduit
Rupture Pipe/ Conduit with Tools or Explosives
Open/ Penetrate Hatch/Port
Rupture Pipe/ Conduit with Explosives
Open/ Penetrate Vent
Rupture Pipe/ Conduit with Explosives

When developing attack scenario for exposed pipe/conduit, consider
- *Standoff attack to directly penetrate pipe/conduit*
- *Hands-on attack requiring access to pipe/conduit followed by rupture using tools or explosives.*

1.n.8 Loss of Critical Communications

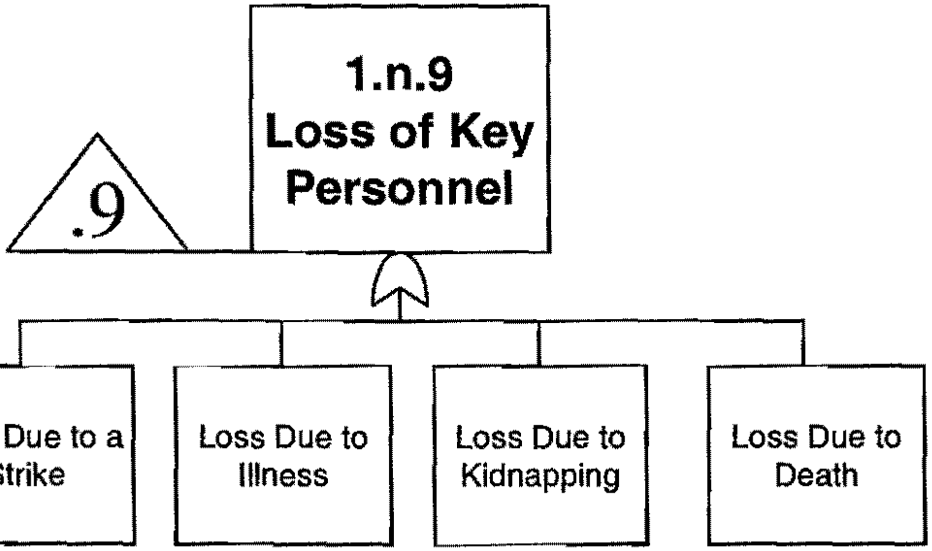
Identify Communications System: ______________________________


.8
1.n.8
Loss of Critical Communications
Loss of Hardwire System
Direct connection
Telephone
Loss of RF Over-the-Air System
Radio
Microwave
Loss of Fiber Optic System
Disable/ Destroy Handset/ Modem
Cut Line
Disable/ Destroy Antenna
Cut Line
Disable/ Destroy Receiver/ Transmitter
Cut Power
.10
Disable/ Destroy Receiver/ Transmitter
Cut Line
Cut Power
.10

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

1.n.9 Loss of Key Personnel

Identify Position & Location: ______________________________

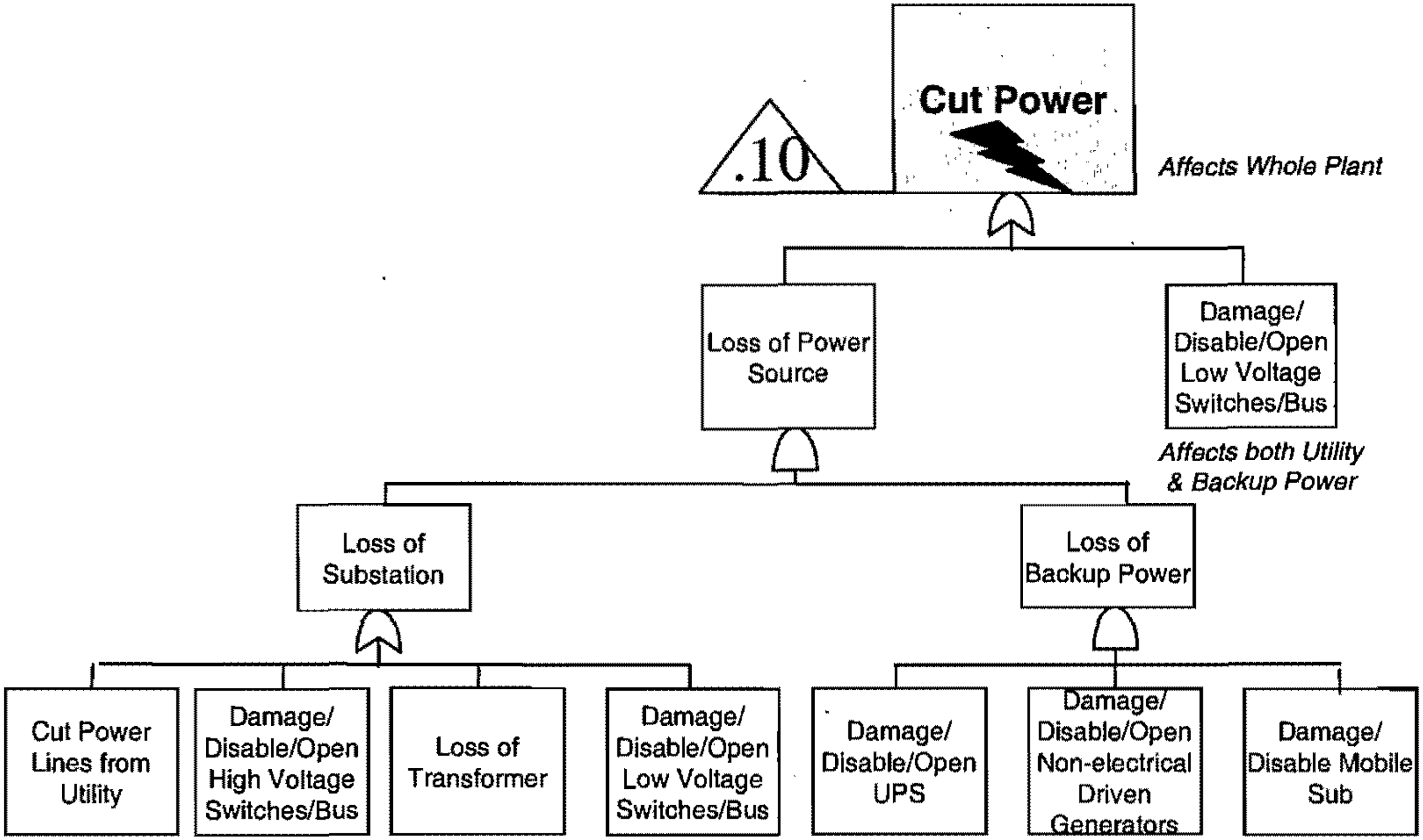


These events, malevolently caused, do not by themselves defeat mission objectives; they would impair ability to cope with a crisis or recover from it in the most timely manner. Minimizing the number of key personnel, for example by cross training is desirable.

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

. . .10 Cut Power

Identify Power System: ______________________________



.10

Cut Power

Affects Whole Plant

Loss of Power Source

Damage/ Disable/Open Low Voltage Switches/Bus

Affects both Utility & Backup Power

Loss of Substation

Loss of Backup Power

Cut Power Lines from Utility

Damage/ Disable/Open High Voltage Switches/Bus

Loss of Transformer

Damage/ Disable/Open Low Voltage Switches/Bus

Damage/ Disable/Open UPS

Damage/ Disable/Open Non-electrical Driven Generators

Damage/ Disable Mobile Sub

SCADA, Short Circuit

Destroy, Rupture Tank, Short Circuit

SCADA, Short Circuit

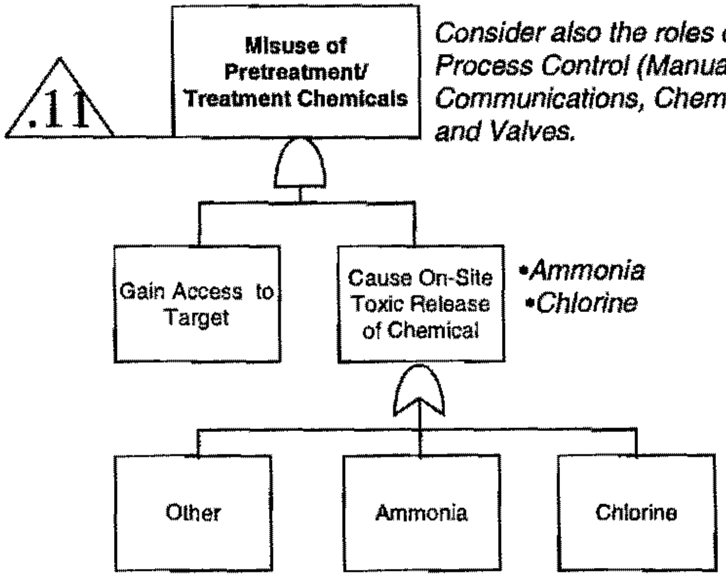
SCADA, Short Circuit

SCADA

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

n.n.11 Misuse of Pretreatment/Treatment Chemical(s)

Identify Chemical, Quantity and Location: ______________________________


.11
Misuse of Pretreatment/ Treatment Chemicals
Gain Access to Target
Cause On-Site Toxic Release of Chemical
Other
Ammonia
Chlorine

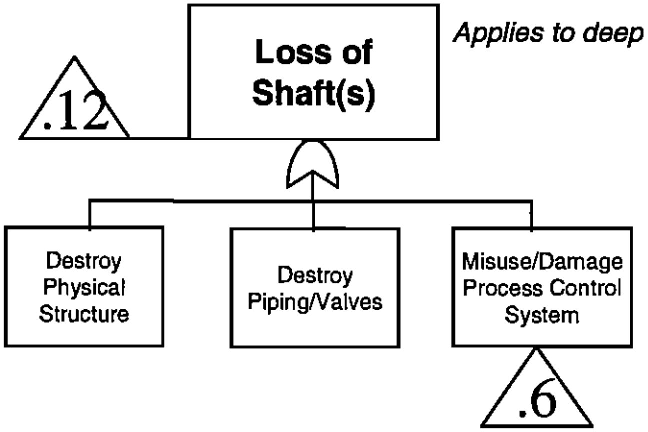
Consider also the roles of Process Control (Manual and SCADA), Communications, Chemical Feed Pumps, and Valves.

- *Ammonia*
- *Chlorine*

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

n.n.12 Loss of Shaft(s)

Identify Shaft: ______________________________



Loss of Shaft(s)
.12
Destroy Physical Structure
Destroy Piping/Valves
Misuse/Damage Process Control System
.6

Applies to deep rock tunnels.

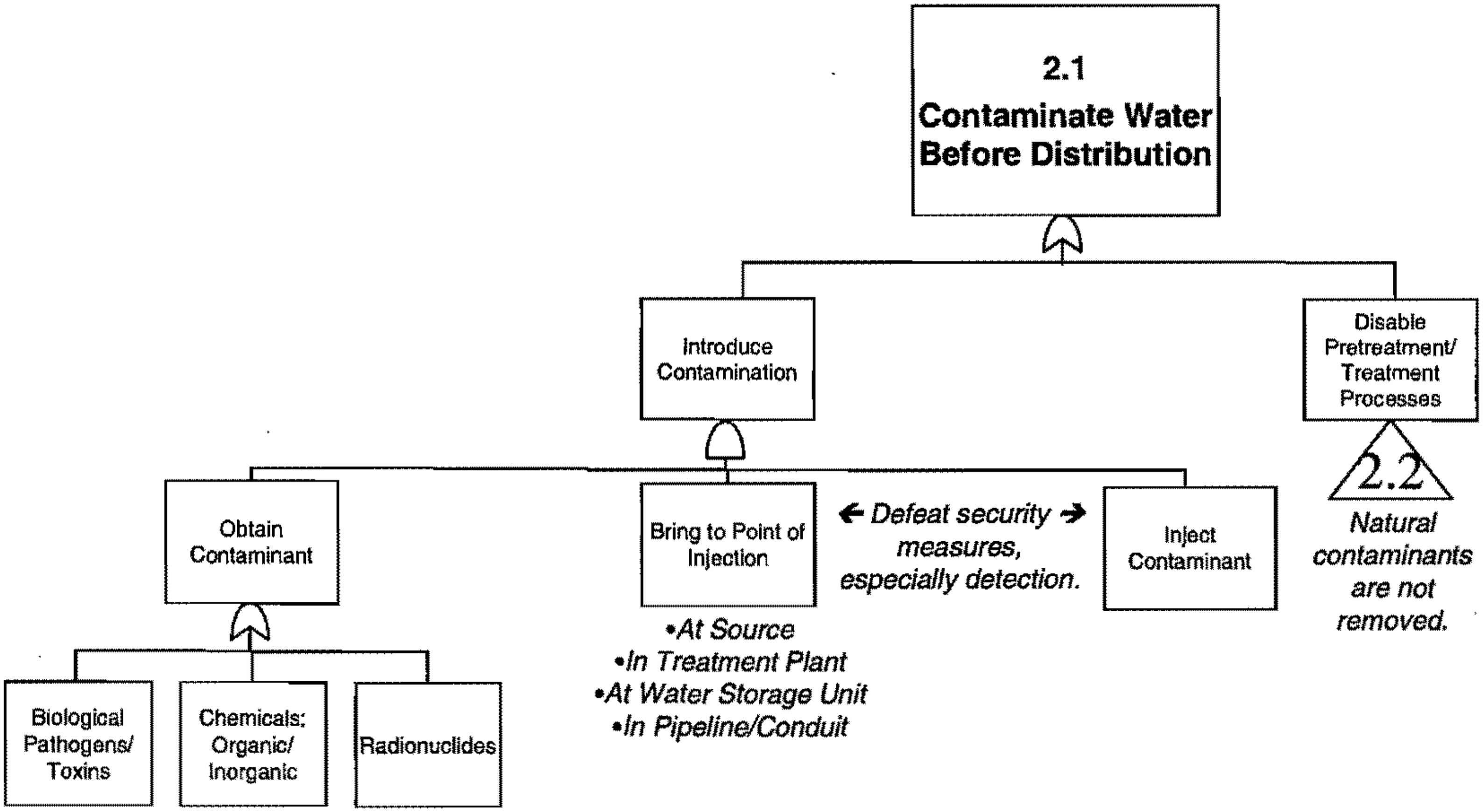
SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

Generic Subtrees

Contaminate Water in the System

2.1 Contaminate Water Before Distribution

Site of Contamination: ____________________



2.1
Contaminate Water Before Distribution

Introduce Contamination

Disable Pretreatment/ Treatment Processes

2.2

Natural contaminants are not removed.

Obtain Contaminant

Bring to Point of Injection

← Defeat security → measures, especially detection.

Inject Contaminant

Biological Pathogens/ Toxins

Chemicals: Organic/ Inorganic

Radionuclides

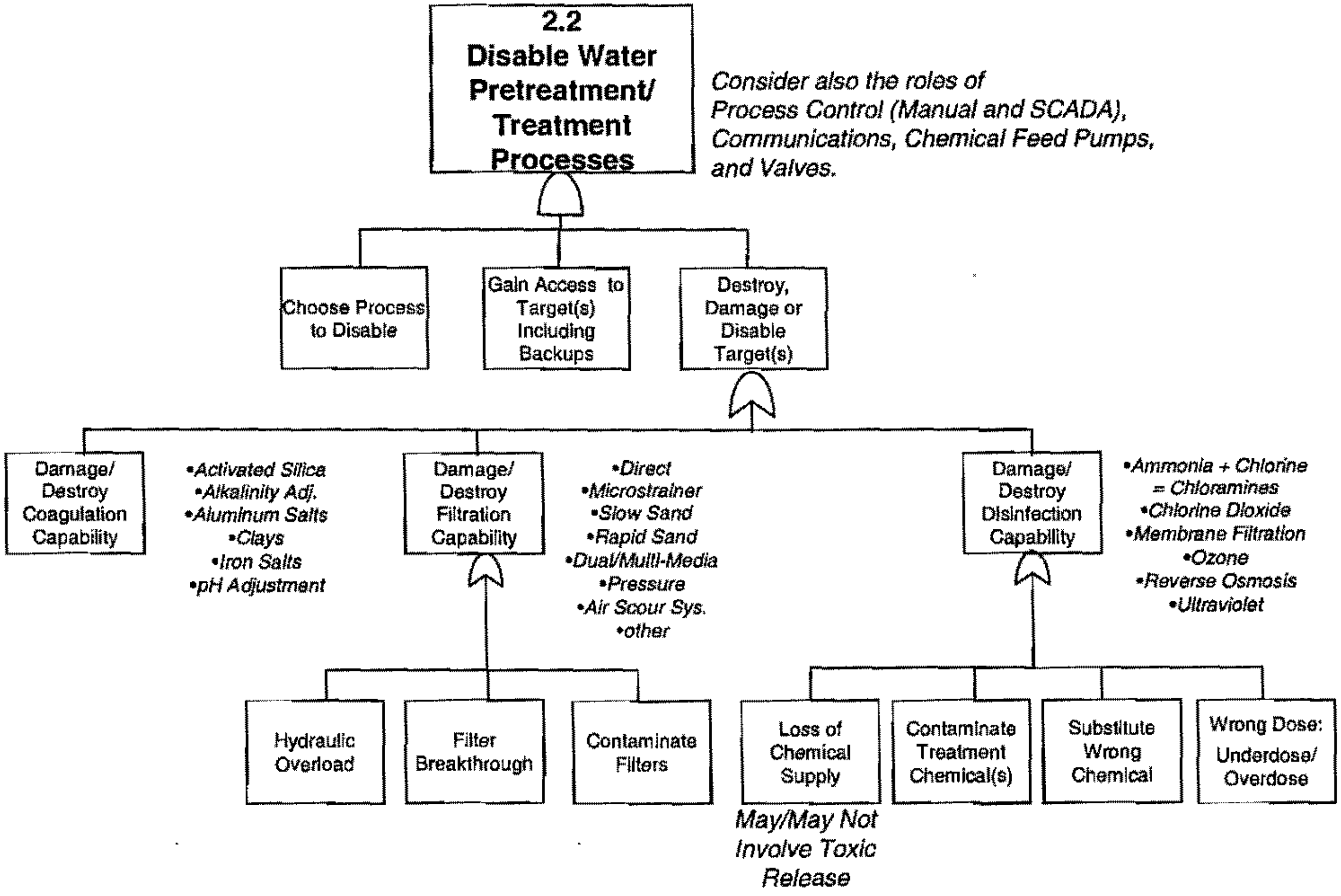
- *At Source*
- *In Treatment Plant*
- *At Water Storage Unit*
- *In Pipeline/Conduit*

Consider Hazardous Material Spills, accidental or deliberate, and beyond capability of water treatment to remove

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

2.2 Disable Pretreatment / Treatment Processes

Identify Site of Treatment/Pretreatment: ______________________________



2.2 Disable Water Pretreatment/ Treatment Processes

Consider also the roles of Process Control (Manual and SCADA), Communications, Chemical Feed Pumps, and Valves.

Choose Process to Disable

Gain Access to Target(s) Including Backups

Destroy, Damage or Disable Target(s)

Damage/ Destroy Coagulation Capability

- *Activated Silica*
- *Alkalinity Adj.*
- *Aluminum Salts*
- *Clays*
- *Iron Salts*
- *pH Adjustment*

Damage/ Destroy Filtration Capability

- *Direct*
- *Microstrainer*
- *Slow Sand*
- *Rapid Sand*
- *Dual/Multi-Media*
- *Pressure*
- *Air Scour Sys.*
- *other*

Hydraulic Overload

Filter Breakthrough

Contaminate Filters

Damage/ Destroy Disinfection Capability

- *Ammonia + Chlorine = Chloramines*
- *Chlorine Dioxide*
- *Membrane Filtration*
- *Ozone*
- *Reverse Osmosis*
- *Ultraviolet*

Loss of Chemical Supply

May/May Not Involve Toxic Release

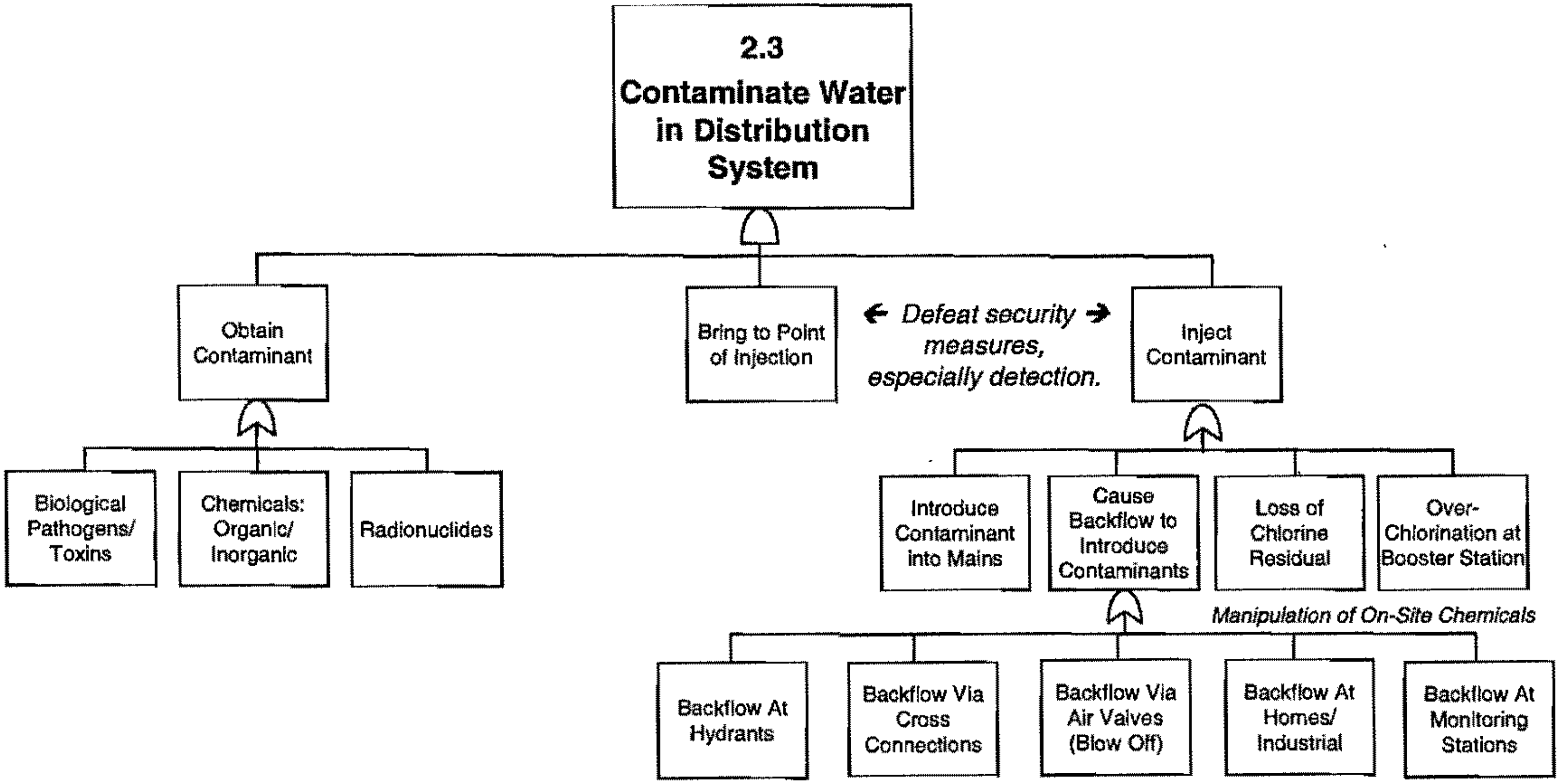
Contaminate Treatment Chemical(s)

Substitute Wrong Chemical

Wrong Dose: Underdose/ Overdose

2.3 Contaminate Water in Distribution System

Site of Contamination: ____

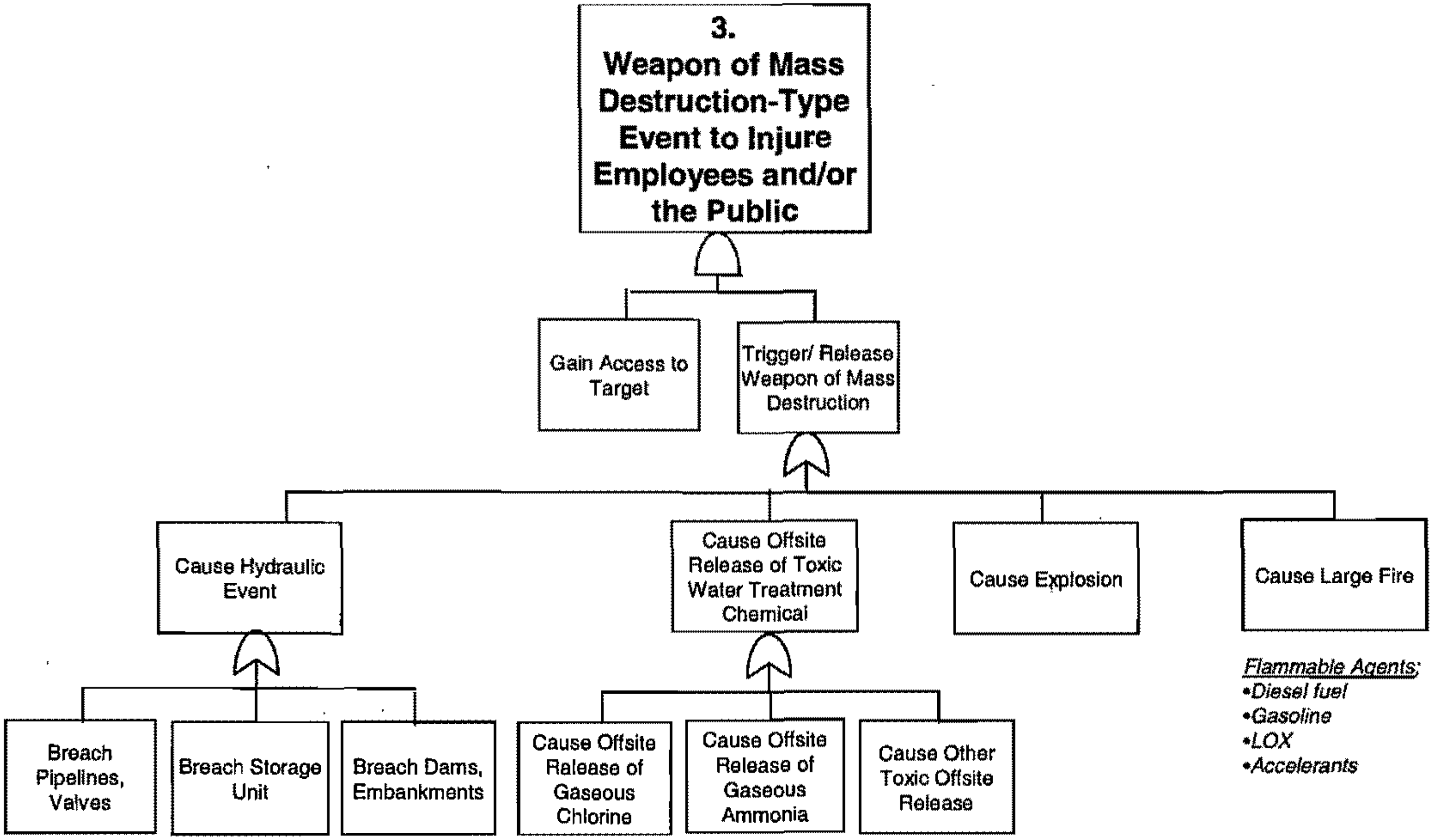

2.3 Contaminate Water in Distribution System
Obtain Contaminant
Bring to Point of Injection
← Defeat security → measures, especially detection.
Inject Contaminant
Biological Pathogens/ Toxins
Chemicals: Organic/ Inorganic
Radionuclides
Introduce Contaminant into Mains
Cause Backflow to Introduce Contaminants
Loss of Chlorine Residual
Over-Chlorination at Booster Station
Manipulation of On-Site Chemicals
Backflow At Hydrants
Backflow Via Cross Connections
Backflow Via Air Valves (Blow Off)
Backflow At Homes/ Industrial
Backflow At Monitoring Stations

Generic Subtrees

Use Weapon of Mass Destruction-Type Event to Injure Employees and/or the Public

3. Weapon of Mass Destruction-Type Event to Injure Employees and/or the Public

Site of Event: ______________________________



3. Weapon of Mass Destruction-Type Event to Injure Employees and/or the Public

Gain Access to Target

Trigger/ Release Weapon of Mass Destruction

Cause Hydraulic Event

Cause Offsite Release of Toxic Water Treatment Chemical

Cause Explosion

Cause Large Fire

Breach Pipelines, Valves

Breach Storage Unit

Breach Dams, Embankments

Cause Offsite Release of Gaseous Chlorine

Cause Offsite Release of Gaseous Ammonia

Cause Other Toxic Offsite Release

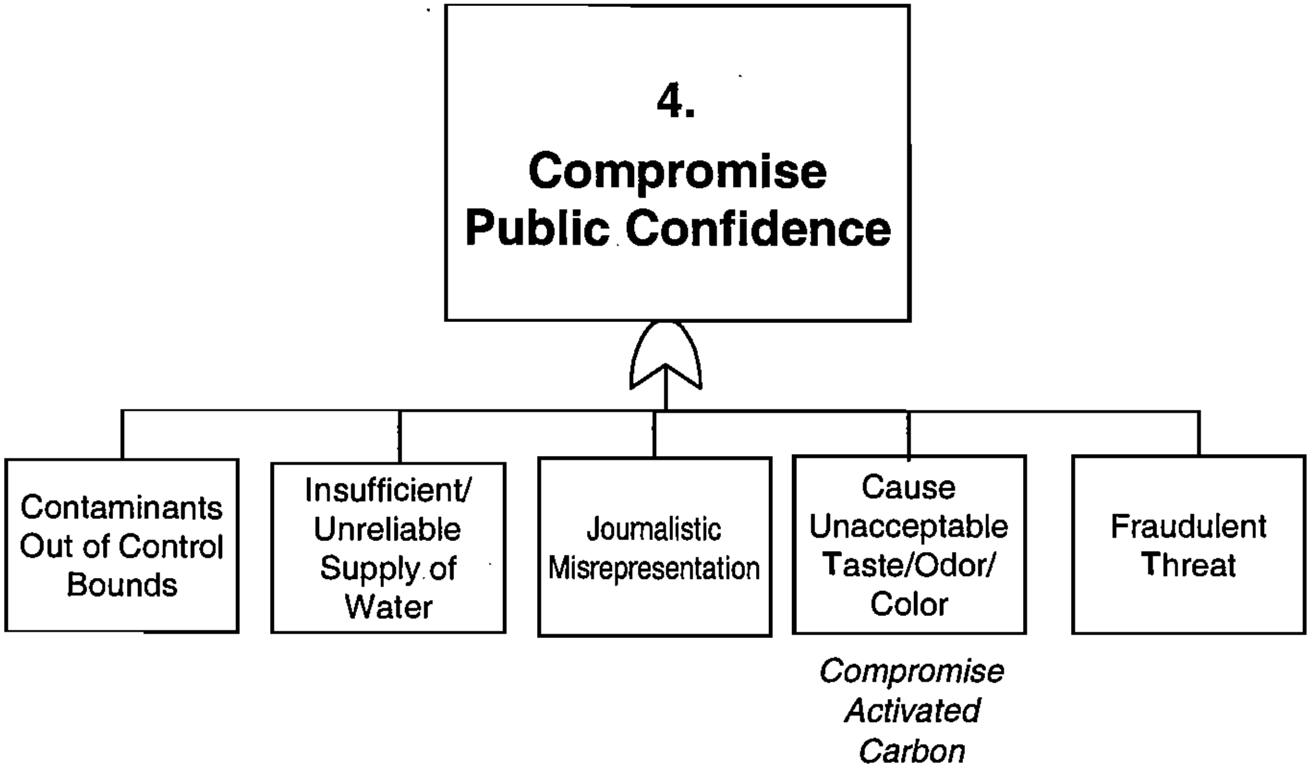
Flammable Agents;
- *Diesel fuel*
- *Gasoline*
- *LOX*
- *Accelerants*

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

Generic Subtrees

Compromise Public Confidence

4. Compromise Public Confidence



4.
Compromise Public Confidence

Contaminants Out of Control Bounds

Insufficient/ Unreliable Supply of Water

Journalistic Misrepresentation

Cause Unacceptable Taste/Odor/ Color

Compromise Activated Carbon

Fraudulent Threat

APPENDIX F: DATA COLLECTION QUESTIONNAIRES

The questionnaires and worksheets in Appendix F are used to collect data about the water utility. They are certainly not exhaustive and can be thought of as "ticklers" to help the analyst in eliciting information about the water system.

F.1. Policies and Procedures Questionnaire: This questionnaire tries to explore what security –related policies and procedures are in place.

F.2. Consequence Worksheet: The Consequence Worksheet uses a matrix with checkmarks to map relevant questions to elements of the Generic Undesired Event Fault Tree.

F.3. Water System Data Collection Worksheets: The Water System Data Collection Worksheets/Tables are used to collect various types of information about the water system.

F.4. SCADA Fault Tree Questions: The SCADA Fault Tree questions map various questions to the generic subtrees to determine whether SCADA can bring about any of the undesirable events.

F.5. SCADA Characterization Questions: If it is determined that SCADA can cause undesirable events, the SCADA Characterization Questionnaire is used to characterize the SCADA system.

5.6. Onsite Chemical Assessment Worksheet: The Onsite Chemical Assessment Worksheet is used to gather information about the chemicals on the site. There are three chemical listings on the worksheet (shown in gray) provided as an example.

F.1. Policies and Procedures Questionnaire For Water Utilities

1. Policies/Procedures/Incident Occurrence Reporting

A. Do they have written security policies and procedures?

What do they contain?

If so, review a copy.

Where are they normally kept?

Does everyone have access?

How?

Who do they apply to?

How are employees trained?

How often are they trained?

Are training records kept and accessible?

How are they enforced?

B. Do they have a badge policy?

How are folks trained?

How often are they trained?

How are they enforced?

Policy if someone loses or forgets their badge?

What type(s) of access control (site and/or building) systems do they employ?

Where are they operational?

Are PIN's used?

Do all employees have access to all facilities?

Do they have a key control policy?

How enforced?

C. Do they perform background checks on employees?

How detailed?

How often updated?

Drug and alcohol screening?

D. Do they have other organizations sharing their facilities?

How are they controlled?

F.1. Policies and Procedures Questionnaire – Continued

E. Do they have exit procedures for employees leaving?

- How detailed?
- If so, review a copy?
  - Keys required to be turned in?
  - Badges required to be turned in?
  - Passwords automatically disabled?

F. Do they have a response force?

- Contract or direct?
- How trained?
- Are they armed?
  - Do they have a policy on lethal force?
- Do they do rounds or random patrols?
- How do operators and guards interact?
  - Is there any joint training?
- Who sees the security alarms?
  - What are the procedures to handle alarms?
    - Are they logged?
    - Does the log contain a disposition of each alarm?
  - What is the nuisance alarm rate?
    - Is it within acceptable limits?
- Are alarms turned off during business hours?
- Do any of their alarms alert outside parties?
  - Does the alarm system run through the SCADA system?
  - How are operators trained on security?
- Are their duress alarms?
  - Where and what happens?

G. What is the policy for confronting unknown visitors accessing the site?

- Guards response?
- Employee response?
- Do they notify anyone before they confront someone?

F.1. Policies and Procedures Questionnaire – Continued

H. How do they deal with contractors?

Do they captive contractors?

Janitorial, maintenance, etc.?

Background checks on captive contractors?

How are they trained on security policies and procedures?

What are their requirements for site access?

Construction and other contractors?

How is their access controlled?

What are their requirements for site access?

I. How do they deal with vendors?

How is their access controlled?

J. How do they control chemical deliveries?

Check chemicals before unloading?

Restrict hours of delivery?

K. How do they deal with other visitors?

Do they give tours?

How do they control vehicular traffic to the site?

Do they do random searches?

Do they use car decals?

L. Do they have an Incident Command System?

If so, review a copy.

What does it include?

Does it include information on responding to terrorism events?

Have they done any training with other emergency services providers?

What emergency response plans do they currently have?

Do they train on them?

Is the training documented and available?

How communicated?

F.1. Policies and Procedures Questionnaire – Continued

M. Do they have any agreements in place with local law enforcement?

How long is the typical response time?

Who is most likely to respond?

How are they trained?

N. Incident Reporting

Do they have an unusual occurrence reporting system?

How long has it been operational?

Who sees the reports?

What action is taken in response if any?

Is the data trended in any way?

Do the guards keep a log?

Do the operators keep a log?

What types of incidents have happened in the past?

Vandalism?

Threats/

Intrusion?

Hacking?

Do they have a theft problem?

What types of employee incidents have occurred?

How do they characterize the management/union relationship?

F.2. Consequence Worksheet

1. Interrupt/Impair Water Flow in the System
1.1 Loss of Water Sources
1.1.1 Interrupt or Reduce Ability to Tap Source(s) of Untreated Water

Questions	1.1.1.1 Loss of Wholesaler's Raw Water	1.1.1.2.1 Damage/ Contaminate Watershed	1.1.1.2.2 Surface - Containment	1.1.1.2.3 Surface – Damage/Destroy Intake	1.1.1.3.1 Ground: Contaminate Aquifer	1.1.1.3.2 Ground: Downhole Damage
Contingency plans	✓			✓	✓	
Interdependencies	✓		✓	✓		
Historical problems	✓		✓		✓	
Location concerns			✓		✓	
Single points of failure						
Alternate sources	✓					
Concerns with the watershed		✓				
Critical containment structures			✓			
Ease/difficulty to damage the containment structure			✓			
Size of the source			✓		✓	
What happens with a power loss				✓		
Ease or difficulty to disrupt				✓		
Intake systems: include other control structures				✓		
Concerns with the aquifer					✓	
Destroy/damage casings						✓
Contaminate casings						✓

F.2. Consequence Worksheet – Continued

1. Interrupt/Impair Water Flow in the System
1.3 Interrupt or Impair Ability to Distribute Water

Questions	1.3.2 Cause Loss of Pressure	1.3.3 Reduce Ability to Store Water	1.3.3 Reduce Ability to Store Wholesaler's Water
Contingency plans			✓
Interdependencies		✓	✓
Historical problems	✓	✓	✓
Location concerns			
Single points of failure	✓		
Ability to simulate main breaks	✓		
Size of storage		✓	
Ability of storage to supply system		✓	
Flooding/collateral damage concerns		✓	
Loss of wholesaler's treated water			✓
Concerns with dependence on a source			✓

F.2. Consequence Worksheet – Continued

Subroutines, .4 through .9

Questions	.4 Critical Pump Systems	.5 Critical Valve Systems	.6 Misuse/Damage Process Control	.7 Pipelines/ Conduits	.8 Loss of Critical Communications	.9 Key Personnel
Contingency plans				✓		
Interdependencies	✓	✓				
Historical problems	✓	✓		✓		
Location concerns	✓	✓				
Single points of failure	✓	✓		✓		
Back-up systems	✓	✓				
Spares	✓	✓				
Redundancy	✓	✓		✓		
Ability to replace	✓	✓				
Criticality to operation	✓	✓				
Type of drivers	✓	✓				
Ability to cause a valve malfunction		✓				
What happens with a loss of power	✓	✓		✓		
Ability to operate facility			✓			✓
Ability to manipulate processes			✓			
Alter/misreport data			✓			
Loss of energy source			✓			
Exposed lines				✓		
Size and flow rates				✓		
Access points				✓		
Locations marked				✓		
Contamination issues				✓		
Critical valves				✓		
Connections to other systems or customers				✓		
Ability to operate					✓	
Control or feedback					✓	
Alternate paths/methods					✓	
Concerns with key personnel						✓
Concerns with attacks on key personnel						✓

F.2. Consequence Worksheet – Continued

Subroutines, .10 through .11

Questions	.10 Cut Power	.11 Misuse Pretreatment Chemicals	.11 Misuse Treatment Chemicals
Contingency plans	✓		
Interdependencies			✓
Historical problems	✓	✓	✓
Location concerns		✓	✓
Single points of failure	✓		
Concerns with chemicals		✓	
Impacts if pretreatment disabled		✓	
Chemicals validated before delivery		✓	
Ability to cause toxic release		✓	✓
Ability to use chemicals as accelerants or in explosives		✓	✓
Types of treatment processes			✓
Chemicals			✓
Risk management plans required			✓
Ability to respond to chemical spills/leaks			✓
Types of filtration processes			✓
Backwash processes			✓
Loss of feed pumps			✓
Ability to substitute wrong chemical			✓
Natural contamination issues			✓
What happens with a loss of power	✓		
Ability to operate facility	✓		
Back-up systems	✓		
Ease or difficulty to cut power	✓		
Ability to replace	✓		

F.2. Consequence Worksheet – Continued

2. Contaminate Water

Questions	2.1 Contaminate Water Before Distribution	2.2 Disable Pretreatment/ Treatment Process	2.3 Contaminate Water in Distribution System
Biological contaminants of concern	✓		✓
Chemical contaminants of concern	✓		✓
Radiological concerns	✓		✓
Contingency plans	✓	✓	✓
Ability to detect unexpected contaminants	✓		✓
Natural contamination issues		✓	✓
Ability to disable pretreatment/treatment process		✓	
Impacts if coagulation disabled		✓	
Impacts if filtration disabled		✓	
Impacts if disinfection disabled		✓	

F.2. Consequence Worksheet – Continued

3. Use Weapon of Mass Destruction Type Event to Injure Employees and/or the Public

Questions	3 Use Weapon of Mass Destruction Type Event to Injure Employees . . .					
Destroy facilities	✓					
Fire	✓					
Explosives	✓					
Chemical releases	✓					
Affecting public areas	✓					
Large pipeline failures	✓					
Collateral damage	✓					
Flooding	✓					
Pump failures	✓					
Fire	✓					
Containment structure failures	✓					
Flooding	✓					
Collateral damage	✓					

F.3. DATA COLLECTION QUESTIONNAIRES

Table F.3.1. Water System Data Collection Worksheet

WATER SYSTEM DATA COLLECTION WORKSHEET

DEFINITIONS FOR ASSET CRITICALITY RATING

Very High: associated with WMD-type event

High:

High criticality implies that loss of the function of the asset would produce an undesired consequence having a seriously adverse impact on the mission of the site.

- Loss of capability of the site to provide water to all customers for a period in excess of t_1 days &/ causing losses in excess of $\$L_1$
- Loss of capability of the site to provide water to a critical customer (e.g., a hospital) for a period in excess of t_2 days
- Contamination of water by monitored substances greatly in excess of federal standards and causing immediate serious health problems for the most susceptible people (e.g., infants, people with compromised immune systems, etc.)
- Contamination of water delivered to all customers by unmonitored substances that would cause serious illness or death

Medium:

Medium criticality implies that loss of the function of the asset would produce an undesired consequence having a moderately adverse impact on the mission of the site.

- Loss of capability of the site to provide water to customers in m zone(s) for a period in excess of t_3 days &/ causing losses between $\$L_1$ and $\$L_2$
- Contamination of water by monitored substances in excess of federal standards and causing delayed serious health problems
- Contamination of water delivered to any customer by unmonitored substances that would cause serious illness or death

Low:

Low criticality implies that loss of the function of the asset would produce an undesired consequence and have a slightly adverse impact on the mission of the site.

- Loss of capability of the site to provide water to a few specific customers for a period in excess of t_4 days &/ causing losses of less than $\$L_2$
- Contamination of water by monitored substances slightly in excess of federal standards
- Contamination of water by substances that would affect taste, color, or odor of water, but would not cause serious illness or death
- Property damage (vandalism)

Note: This form is provided to help the water utility define consequence measures. The values on this form (t_1, t_2, & $\$L_1$, etc.), all come from the consequence table. This is simply an aid and is not included in the body of the methodology.

Notes:

Table F.3.2. Water System Data Collection Worksheet

WATER SYSTEM DATA COLLECTION WORKSHEET
PHYSICAL PROTECTION SYSTEM DESCRIPTION

Facility:

Date:	**Recorded by:**

Instructions:

Obtain answers to the following questions.

- Questions should be answered on this page and continuation pages if required.
  - Answer Yes (Y) or No (N) to the right of each question.
  - Supply additional comment in "Notes" keyed to the related question.

Questions:	**Answer**
Threat tactics:	
(1) Describe how adversary can disable/destroy asset	
(2) What mitigating measures can be employed to limit adversary attack?	
Physical Security:	
(3) Describe route(s) adversary can access asset	
(4) Describe existing protection measures	
(5) Describe natural terrain or geographical features that might be barriers to the adversary	
(6) Describe potential vulnerabilities	
Police Response Force	
(7) Describe response in terms of numbers and time to respond	
(8) Describe means of communication to response force.	
(9) Describe equipment and training of response force	
Control Access & Authority	
(10) How is "access and authority" by non-employee personnel, (Contractors, Vendors, Casuals, Delivery Personnel) to this facility controlled?	
(11) Does abandoned or secondary access exist for this facility (Tunnels, Water Mains, Utility Chases, etc).	
(12) If Yes, how are they controlled and documented?	
Security System Integration	
(13) Describe where and how alarms are annunciated.	
(14) Describe protection for communication lines	
(15) Describe procedures for what happens when an alarm sounds.	

Notes:

Table F.3.3. Water System Data Collection Worksheet

WATER SYSTEM DATA COLLECTION WORKSHEET
PHYSICAL PROTECTION FEATURES

Facility:

Date: **Recorded by:**

Functional Area:

Physical Protection Features	**Reviewed**	**Photo**
	Y/N/NA	**Disc /Aperture**
(1) Boundary		
(1a) Fence (height and construction)		
(1b) Vehicle barriers		
(2) Entrances		
(2a) Personnel/Vehicle		
(2b) Entrance construction		
(2c) Entrance locks		
(2d) Entrance barriers		
(3) Distance between boundary and building		
(4) Building construction		
(5) Entrance (doors, windows, vents, skylights) construction		
(5a) Entrance locks		
(5b) Entrance barriers		
(6 Distance between entrance and critical asset		
(7) Critical Asset enclosure construction		
(8) Critical asset enclosure entrance construction		
(8a) Enclosure locks		
(8b) Enclosure barriers		
(9) Sensors (fence, intrusion, door/gate position, penetration, motion)		
(10) Detection by personnel		
(11) ID checks		
(12) Contraband detection (persons, packages, vehicles)		
(13) Assessment by cameras or personnel		

Table F.3.4. Water System Data Collection Worksheet

WATER SYSTEM DATA COLLECTION WORKSHEET	
Facility:	
Date:	**Recorded by:**
Functional Area:	

Physical Protection Features	**Reviewed**	**Photo**
	Y/N/NA	**Disc/Aperture**
(14) Tamper indicating measures		
(14a) Alarms		
(14a1) Where displayed		
(14a2) Where controlled		
(14a3) Alarm destination (CMS, PD, etc).		
(15) Communication Lines		

Notes:

F.4 SCADA FAULT TREE QUESTIONS

The following questions help the water utility decide how critical their SCADA system is to their mission and how the SCADA system could be used to bring about undesired events. The questions map to the fault tree.

Generic Subtree	Questions
Loss of Water Sources	
1.1.1 Interrupt or Reduce Ability to Tap Source(s) of Untreated Water	01 Can the SCADA system be used to interrupt or Reduce the ability to tap sources of untreated water
1.1.4 Loss of Critical Pump System	02 Does the SCADA system control your critical pumps?
1.1.4 Loss of Critical Pump System	02a. Is there local control available?
1.1.4 Loss of Critical Pump System	02b. Through the PLC or RTU?
1.1.4 Loss of Critical Pump System	02 c. Can the pumps be operated manually?
1.1.5 Loss of Critical Valve Systems	03. Does the SCADA system control your critical valves?
1.1.5 Loss of Critical Valve Systems	03a. Is there local control available?
1.1.5 Loss of Critical Valve Systems	03b. Through the PLC or RTU?
1.1.5 Loss of Critical Valve Systems	03 c. Can the valves be operated manually?
1.1.6 Misuse/Damage Process Control System	04 Can the SCADA system be used to interrupt or Reduce the ability to tap sources of untreated water
1.1.7 Damage/Destroy Critical Pipelines/Conduits	05 Can the you damage/destroy critical Pipelines/Conduits with the SCADA system?
1.1.8 Loss of critical communications	06. What happens if you lose communications?
Disable Pretreatment or Treatment Process	

Generic Subtree	Questions
1.2.4 Loss of Critical Pump System	01 Does the SCADA system control your critical pumps?
1.2.4 Loss of Critical Pump System	01a. Is there local control available?
1.2.4 Loss of Critical Pump System	01b. Through the PLC or RTU?
1.2.4 Loss of Critical Pump System	01 c. Can the pumps be operated manually?
1.2.5 Loss of Critical Valve Systems	02. Does the SCADA system control your critical valves?
1.2.5 Loss of Critical Valve Systems	02a. Is there local control available?
1.2.5 Loss of Critical Valve Systems	02b. Through the PLC or RTU?
1.2.5 Loss of Critical Valve Systems	02 c. Can the valves be operated manually?
1.2.6 Misuse/Damage Process Control System	03 How can you disable the pretreatment or treatment process using the SCADA system?
1.2.7 Damage/Destroy Critical Pipelines/Conduits	04 Can the you damage/destroy critical Pipelines/Conduits with the SCADA system?
1.2.8 Loss of critical communications	05. What happens if you lose communications?
Interrupt or Impair Ability to Distribute Water	
1.3.2 Cause Loss of Pressure in Distribution System	01 Can the SCADA system cause a loss of pressure in the distribution system?
1.3.3 Interrupt or Reduce Ability to Store Water	02 Can the SCADA system be used to interrupt or reduce the ability to store water?

Generic Subtree	Questions
1.3.4 Loss of Critical Pump System	03 Does the SCADA system control your critical pumps?
1.3.4 Loss of Critical Pump System	03a. Is there local control available?
1.3.4 Loss of Critical Pump System	03b. Through the PLC or RTU?
1.3.4 Loss of Critical Pump System	03c. Can the pumps be operated manually?
1.3.5 Loss of Critical Valve Systems	04. Does the SCADA system control your critical valves?
1.3.5 Loss of Critical Valve Systems	04a. Is there local control available?
1.3.5 Loss of Critical Valve Systems	04b. Through the PLC or RTU?
1.3.5 Loss of Critical Valve Systems	04c. Can the valves be operated manually?
1.3.6 Misuse/Damage Process Control System	05 How can you interrupt or impair the ability to distribute water using the SCADA system?
1.3.7 Damage/Destroy Critical Pipelines/Conduits	06 Can the you damage/destroy critical Pipelines/Conduits with the SCADA system?
1.3.8 Loss of critical communications	07. What happens if you lose communications?
Contaminate Water Before Distribution	

F.5. SCADA CHARACTERIZATION QUESTIONS

The questionnaires that follow characterize the SCADA system as well as determining the security mechanisms in place within the system. Detailed questionnaires help both the training of security personnel in the process as well as completing the various pairwise decision matrices. These questionnaires also help the applicability to multiple sites by maintaining consistency in the depth and areas of coverage. The questionnaires are not restrictive in scope, but do ensure a minimum threshold of knowledge about the security of a particular SCADA system before completing the relative ranking process. CobiT®, the generic depiction of a secure water SCADA system, and previous assessment experience all influence the type and level of questions developed for the assessment process.

Asset	Questions
01. Security Policy	01. Is there an official SCADA security policy?
01. Security Policy	01a. Is the official SCADA security policy documented?
01. Security Policy	01b. Where is the official SCADA security policy located (interviewer should obtain a copy of this policy)?
01. Security Policy	01c. How often if the policy reviewed?
01. Security Policy	02. What procedures are used in lieu of an official SCADA security policy?
01. Security Policy	03. Can you describe any security threats created by security insensitive SCADA policies?
01. Security Policy	04. Do you have a privacy policy for your site, and is it displayed prominently?
01. Security Policy	05. Are there standards, policies, or procedures in your organization for configuring hardware configuration items (HWCIs) or computer system configuration items (CSCIs)?
02. Security Plan (Implementation Guidance)	01. Is there a security plan to protect IT elements/components?
02. Security Plan (Implementation Guidance)	02. Can you describe any security threats created by security insensitive on nonexistent SCADA operating procedures?
02. Security Plan (Implementation Guidance)	03. Who has permission to make OS changes?
02. Security Plan (Implementation Guidance)	04. Are passwords used?
02. Security Plan (Implementation Guidance)	05. Are passwords required?

Asset	Questions
02. Security Plan (Implementation Guidance)	05a. What is the password minimum length?
02. Security Plan (Implementation Guidance)	05b. Are the passwords machine generated?
02. Security Plan (Implementation Guidance)	05c. Do the passwords require a combination of letters and numbers?
02. Security Plan (Implementation Guidance)	05d. Do the passwords expire?
02. Security Plan (Implementation Guidance)	05e. Are the passwords audited?
02. Security Plan (Implementation Guidance)	06. Does your organization have an electronic record security plan (pursuant to the Computer Security Act of 1987)? If yes, is it documented?
02. Security Plan (Implementation Guidance)	07. Have you installed all security-related patches and updates?
03. Security Training	01. What type of security training have you received in support of your job responsibilities?
03. Security Training	02. What type of IT security training is provided or required on a regular basis?
04. Skilled Personnel	01. Are there any non-utility people that have access to the control room instrumentation?
04. Skilled Personnel	02. Do you use contract personnel to provide any services related to your SCADA operation?
04. Skilled Personnel	02a. What are the security validation processes associated with their employment?
04. Skilled Personnel	02b. Are there check-in/check-out procedures associated with their employment term?
04. Skilled Personnel	02c. Please describe the procedures.

Asset	Questions
04. Skilled Personnel	03. Are you relying on only 1 or 2 people to know about, run, or modify SCADA application?
04. Skilled Personnel	04. Who operates the network management packages(s)?
04. Skilled Personnel	05. Who is responsible for your WAN interface configuration?
04. Skilled Personnel	06. Who is responsible for configuring the ACL(s)?
04. Skilled Personnel	07. Who is responsible for reviewing the audit logs?
04. Skilled Personnel	08. How many total people have access to the control room instrumentation?
04. Skilled Personnel	09. Is there a grade or classification for employees granting access to the control room instrumentation?
04. Skilled Personnel	09a. What is this classification, and how many employees qualify?
04. Skilled Personnel	10. Who installs the Operating System on your computers?
04. Skilled Personnel	11. Who is responsible for configuring your servers?
04. Skilled Personnel	12. Who is responsible for official records in your organization?
04. Skilled Personnel	13. Who maintains the software on your computers?
05. Remote SCADA operations	01. Can you identify critical functions in your mission that depend on remote access connectivity for success?
05. Remote SCADA operations	01a. Please list function(s) and description(s).
05. Remote SCADA operations	02. What are the consequences associated with not completing remote access functions? Please list function(s) and consequence(s)
05. Remote SCADA operations	03. What methods of remote access are supported by the RTUs/PLCs (i.e., dialup, telnet, etc.)?
05. Remote SCADA operations	04. What access control is there for remote access (e.g., passwords)?

Asset	Questions
05. Remote SCADA operations	05. Can SCADA attributes be set remotely?
05. Remote SCADA operations	05a. If so, what settings are available through remote access?
05. Remote SCADA operations	06. What are the remote access points for the RTUs/PLCs (i.e., from where are they accessed)?
06. RTUs PLCs, IEDs	01. Are there any entities apart from the area control center and facility control room that have control over RTUs/PLCs?
06. RTUs PLCs, IEDs	01a. If so, please list them and their control access levels.
06. RTUs PLCs, IEDs	02. Do any RTUs/PLCs include local control intelligence?
06. RTUs PLCs, IEDs	02a. If so, please explain the control schemes.
06. RTUs PLCs, IEDs	03. How many RTUs/PLCs total are there?
06. RTUs PLCs, IEDs	04. How many RTUs/PLCs does a facility have?
06. RTUs PLCs, IEDs	05. What types of RTUs/PLCs are used in the system?
07. SCADA Servers	01. How many people have passwords to the equipment?
07. SCADA Servers	01a. Are the passwords shared?
07. SCADA Servers	02. What is the logging system for the SCADA operators?
07. SCADA Servers	03. What is the time period of unavailability for the complete SCADA system that can be tolerated before significant consequences result?
07. SCADA Servers	03a. Please explain the consequences of this unavailability.
07. SCADA Servers	04. How many control components or control algorithms are directly dependent upon the SCADA system? What are they?

Asset	Questions
07. SCADA Servers	05. From where does the input data come?
07. SCADA Servers	06. Is sensitive data shared with other applications?
07. SCADA Servers	07. Do you have back-up system configurations for the SCADA Servers?
07. SCADA Servers	08. Are the passwords audited on a regular basis?
07. SCADA Servers	09. Are the server log files protected against snooping by unprivileged users?
07. SCADA Servers	09a. How are they server logs protected?
07. SCADA Servers	10. Do any of your SCADA servers also serve as a web server, user workstation, etc. or perform duty as a general purpose machine?
07. SCADA Servers	11. How frequently are the passwords changed?
07. SCADA Servers	11a. Are the passwords audited on a regular basis?
07. SCADA Servers	12. Is access to the MMI or SCADA servers password-protected?
07. SCADA Servers	13. What platform (computer type and OS) typically supports the control room instrumentation?
07. SCADA Servers	14. At what site(s) is the SCADA application located?
07. SCADA Servers	14a. On what machine(s) is the SCADA application running?
08. SCADA Software	01. Does the application require you to run with any special privileges? (e.g., logging in with root or administrator privileges)
08. SCADA Software	02. What are the underlying platforms or external systems that the application assumes are secure? (e.g., Oracle, a user's NT workstation, DNS, etc.?)

Asset	Questions
08. SCADA Software	03. Does the application introduce concerns (requiring a specific port be opened on a firewall, dial-in modem being installed, plaintext passwords embedded in batch files, etc.)?
08. SCADA Software	04. Have any upgrades or security patches been applied to the MMI software?
08. SCADA Software	05. How many people use the SCADA application?
08. SCADA Software	06. What sorts of protection mechanisms exist for the control capabilities identified in the question above (Check-before-operate, Control timeouts, Select-execute, Others)?
08. SCADA Software	07. Who is the manufacturer and what is the product name of the SCADA and/or MMI software (note: this is not the name of the operating system)?
08. SCADA Software	07a. Is the product still supported?
09. Operating Systems – Unix	01. How many UNIX-based servers comprise the SCADA system?
09. Operating Systems – Unix	02. Do you have remote logins enabled?
09. Operating Systems – Unix	03. Is root allowed to login remotely?
09. Operating Systems – Unix	04. Do you have a security plan your UNIX servers (interviewer should obtain a copy)?
09. Operating Systems – Unix	04a. Do you have a configuration guide for your UNIX servers (interviewer should obtain a copy)?
09. Operating Systems – Unix	05. What UNIX utilities do you have enabled? (TFTP, FTP, SMTP, NFS, DFS, DCE, WEB Server, News Server, Telnet, BOOTP, SSH, Finger, rlogin, rsh, Xwindows, other)
09. Operating Systems – Unix	06. Please list the applications running on SCADA UNIX servers (Examples: databases, Web server, email, etc).
09. Operating Systems – Unix	07. Do you regularly install security patches on your UNIX servers and workstations?
09. Operating Systems – Unix	08. Please select all the automated procedures established for your SCADA UNIX platforms (backups, security checks, logging off users after inactivity, routine administration tasks, etc.).

Asset	Questions
09. Operating Systems – Unix	09. What type of data resides on the SCADA UNIX platforms (administrative – sensitive or non-sensitive, sensor output, SCADA control information , engineering data, SCADA alarm reporting, physical security alarms, Fire/Safety alarms, Other))?
09. Operating Systems – Unix	10. Do you use directory services for account management?
09. Operating Systems – Unix	11. Is remote system configuration of the UNIX servers allowed?
09. Operating Systems – Unix	12. Do you use C2 Security? (e.g., Enhanced Security for HP-UX, bmconvert for Solaris)
09. Operating Systems – Unix	13. How many people have admin accounts?
09. Operating Systems – Unix	14. Do any applications require a process to run with SUID; if so, does "root" own any of the processes?
09. Operating Systems – Unix	15. Do you have a /etc/hosts.equiv file?
09. Operating Systems – Unix	15a. Do you have active entries in this file?
09. Operating Systems – Unix	16. Do you utilize a shadowed password file?
10. Operating Systems – Windows NT	01. Can you identify the critical NT servers in your network?
10. Operating Systems – Windows NT	01a. If yes, please list them.
10. Operating Systems – Windows NT	02. Do you have a security plan for your SCADA NT platforms?
10. Operating Systems – Windows NT	02a. Do you have a configuration guide for your SCADA NT platforms?
10. Operating Systems – Windows NT	03. What versions of Windows are you running? (WinNT 3.5x, WinNT 4.0 SP3 or less, WinNT 4.0 SP4, WinNT 4.0 SP5 or higher, Windows 2000, XP)

Asset	Questions
10. Operating Systems – Windows NT	04. Are workstation users "administrators" on their own machines?
10. Operating Systems – Windows NT	05. Is remote configuration of NT devices allowed?
10. Operating Systems – Windows NT	05a. Who has permission to make changes?
10. Operating Systems – Windows NT	06. Is RAS allowed?
10. Operating Systems – Windows NT	06a. What other network resources are available upon establishing a remote connection?
10. Operating Systems – Windows NT	07. Do you perform automated auditing of user activity on the NT servers?
10. Operating Systems – Windows NT	07a. Please indicate the software and procedures involved.
10. Operating Systems – Windows NT	08. Please list the other applications that run on the SCADA NT platforms (e.g., Outlook, Exchange, Internet Information Server, Oracle, SMS, Netscape Enterprise Server)?
10. Operating Systems – Windows NT	09. What type of data resides on the SCADA NT platforms?
10. Operating Systems – Windows NT	10. On your NT devices, are any folders or drives shared, other than the NT Default (C$, Admin$, other drive letters)?
10. Operating Systems – Windows NT	10a. Are permissions set at the Share Level or the NTFS Level?
10. Operating Systems – Windows NT	11. Do you have any file sharing software installed (i.e. Web Server software, FTP Server software)?

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

Asset	Questions
10. Operating Systems – Windows NT	11a. If yes, type.
10. Operating Systems – Windows NT	12. Do you have a list or topological map of all the NT domains in your network (interviewer should obtain the map)?
10. Operating Systems – Windows NT	13. Do you have a recovery procedure for your SCADA NT platforms?
10. Operating Systems – Windows NT	14. Are you using: WinNT Server, WinNT Workstation, WinNT Server Enterprise Edition, WinNT BackOffice Server?
10. Operating Systems – Windows NT	15. Do you use accounts other than Administrator for system configuration of the NT client workstations?
10. Operating Systems – Windows NT	16. Is the user "Guest" disabled on your servers?
10. Operating Systems – Windows NT	17. Are rights assigned to individual users or groups, or are they given to everyone in general?
11. Web Servers	01. How many SCADA web servers are running at this site?
11. Web Servers	02. Which web applications, if any, are critical to the operations of this site, and why are they critical?
11. Web Servers	03. What services are your web servers providing? (e.g., SCADA display and control, web pages, database access, applications?)
11. Web Servers	04. Does the web server get monitored?
11. Web Servers	04a. By whom is the monitoring done?
11. Web Servers	04b. What gets monitored (suspicious activity, unauthorized users, monitoring of hits, etc.)?
11. Web Servers	04c. What software tools are used?

Asset	Questions
11. Web Servers	05. Do you use a web browser that supports the SSL protocol when viewing or submitting confidential information?
11. Web Servers	06. Where is the public web server in relation to the firewall?
11. Web Servers	07. How many people - internally - have access to place information on the web server?
11. Web Servers	08. How many people - externally - have access to place information on the web server?
11. Web Servers	09. How do you monitor the web server for compromise?
11. Web Servers	10. Do you use all of the log information you collect?
11. Web Servers	10a. When is the log information used?
11. Web Servers	10b. What log information is collected?
11. Web Servers	11. Do you manage what information is placed on your web server?
11. Web Servers	11a. Are there documented procedures for this?
11. Web Servers	11b. Are there undocumented procedures for this?
11. Web Servers	12. Do you have an approval process for public information being placed on the public web server?
11. Web Servers	12a. Are there procedures for this?
11. Web Servers	13. What forms of enhanced security do you use? (SSL, SHTTP, certificates, encryption, others)
11. Web Servers	14. What plug-ins and helper applications are installed in your browser?
11. Web Servers	15. Please describe all of the cryptographic protocols you are utilizing on the web server.
11. Web Servers	16. Do you allow http, https & ftp on your web server?

Asset	Questions
11. Web Servers	17. Is the web server running as "root" (UNIX) or system accounts (NT)?
11. Web Servers	18. Please note any of the application servers running (e.g., Cold Fusion, Galileo, Lotus Domino, Netscape , Oracle, SilverStream, Sybase Enterprise Server, WebObjects, other).
11. Web Servers	19. What other network services are available from the web server machine? (e.g., DNS, sendmail)
11A. Platform Security	01. Do you have modems on your clients or servers?
11A. Platform Security	02. Are any servers configured with multiple NICs?
11A. Platform Security	02a. Are they configured as routers?
11A. Platform Security	02b. Do they transfer data between the SCADA network and another network?
11A. Platform Security	03. Have you disabled all unnecessary services on SCADA platforms, including NetBIOS services, if running an NT machine?
11A. Platform Security	04. Do you have boot (BIOS) passwords installed on your computers?
11A. Platform Security	05. Do you use automatic screen savers on your computers?
11A. Platform Security	05a. Does the screen saver lock the computer when it activates?
11B. SCADA Control Terminals	01. Does the SCADA application display any sensitive or private data?
11B. SCADA Control Terminals	02. Is there a backup control center?
11B. SCADA Control Terminals	03. What are the locations of the facilities having generation or water control with electronically controlled operations?
11B. SCADA Control Terminals	04. What is the location of the main control center for the SCADA and engineering systems?
11C. SCADA Terminals	01. Is electronic access to the control room instrumentation password-protected?

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

Asset	Questions
12. SCADA Account Restrictions	01. Are there any limits on access to SCADA data?
12. SCADA Account Restrictions	01a. What are the access limits?
12. SCADA Account Restrictions	02. On what internal security mechanisms does SCADA rely? (e.g., table lookup of privileges based on user id)
13. SCADA Network Architecture	01. What is the physical topology of the network under evaluation (the interviewer should obtain a copy of the drawing; be sure there is a legend attached)?
13. SCADA Network Architecture	02. If there is no drawing available, can a sketch be provided of the network hardware?
13. SCADA Network Architecture	03. What technologies are used for the network (ATM, Frame relay, Ethernet, Gig-Ethernet, etc.)? How many devices each?
13. SCADA Network Architecture	04. Which network protocols are utilized? (TCP, IP, IPX, AppleTalk, DECNET, Other)
13. SCADA Network Architecture	05. Which routing protocols are used in the network? (RIP, IGRP, EIGRP, OSPF, NLSP, Other)
13. SCADA Network Architecture	06. Are priority/critical routes clearly identified in your topology?
13. SCADA Network Architecture	07. Are all firewall locations clearly indicated on the logical topology drawing?
13. SCADA Network Architecture	08. Is there a physical backup connection on priority routes?
13. SCADA Network Architecture	09. Where in the network are the ACL(s) located?
13. SCADA Network Architecture	10. What are the security threats created by subsystem compatibility issues (e.g., single password to access various subsystems)?
13. SCADA Network Architecture	11. What vulnerabilities are you aware of in your current SCADA network ?
13. SCADA Network Architecture	12. How do you protect your information from being intercepted by packet sniffers?
13. SCADA Network Architecture	13. Note the versions of the included protocols, and explain the response for "Other" (if applicable).

Asset	Questions
13. SCADA Network Architecture	14. Which WAN interface equipment is customer premise equipment (CPE)?
14. Connections to other Organizations	01. Is the control room instrumentation connected to the business network?
14. Connections to other Organizations	02. If the control room instrumentation is connected to the business network, describe the connection.
14. Connections to other Organizations	03. Does the SCADA data network interface with any other systems?
14. Connections to other Organizations	04. Describe the name and owner of the other systems, and the locations of the intersections. (Internet, Intranet, Independent system operators (ISOs), None, Other)
14. Connections to other Organizations	05. Do you have any Service Level Agreements (SLA) with your Local Exchange Carrier (LEC) or Internet Service Provider (ISP)?
14. Connections to other Organizations	06. What technique or packages(s) is used for auditing? What type of information is collected?
14. Connections to other Organizations	07. Does the SCADA data network include leased or shared lines?
14. Connections to other Organizations	08. Do you perform any auditing at the WAN interface?
14. Connections to other Organizations	09. Are the SLAs available for review?
14. Connections to other Organizations	09a. If yes, please indicate the location.
14. Connections to other Organizations	09b. Are the lines are leased or shared?

Asset	Questions
14. Connections to other Organizations	09c. If shared, with whom are they shared?
14. Connections to other Organizations	09d. Who has ownership of the lines?
14. Connections to other Organizations	09e. What communication protocols are used?
14. Connections to other Organizations	09f. What types of data traffic typically traverses the lines?
14. Connections to other Organizations	09g. Are there other pertinent observations that you can provide?
14. Connections to other Organizations	10. Which WAN interface equipment is provided and maintained by the service provider?
15. Internet Connections	01. Is Internet access available?
15. Internet Connections	01a. What types of connections are allowed (Web - Secure Server, Web - Unsecure Server, Telnet, Ftp, r services (rsh, rlogin, etc.), Other - Please Describe)?
15. Internet Connections	02. What data is generated/output?
15. Internet Connections	02a. Where does the output data go?
15. Internet Connections	02b. Who uses the output data?
15. Internet Connections	02c. Where are they?
15. Internet Connections	02d. For what do they use it?
15. Internet Connections	03. Do you ever browse the web while logged on as administrator on Windows NT system, or as root on UNIX systems?

Asset	Questions
16. Remote Access Connections	01. Is remote access to the SCADA network allowed - (dial-up, Internet)?
16. Remote Access Connections	02. What are the methods of remote access? (Dial Up Lines, Internet, Other, please describe)
16. Remote Access Connections	03. How is the remote user authenticated? (Knowledge of telephone number, Password, Secure token (i.e., secure ID card, S-Key), Dial-Back, Other, please describe.)
16. Remote Access Connections	04. Are the passwords shared?
16. Remote Access Connections	04a. Are the passwords audited on a regular basis?
16. Remote Access Connections	04b. What is the audit schedule?
16. Remote Access Connections	05. Please list the applications that are available by remote access.
16. Remote Access Connections	06. Does your remote access process use a stand-alone server?
16. Remote Access Connections	07. Are remote connections audited?
16. Remote Access Connections	07a. What type of information is collected?
16. Remote Access Connections	08. Is any wireless remote access available?
16. Remote Access Connections	08a. Please describe this remote access?
16. Remote Access Connections	09. What other software/applications run on the remote access server?
16. Remote Access Connections	10. How many people have administrative access to your remote access server(s)?
16. Remote Access Connections	11. What additional access is provided within the physical network after establishing a remote connection?
16. Remote Access Connections	12. What additional access is provided outside the physical network after establishing a remote connection?
17. SCADA Network Management	01. Are you using any network management packages?

Asset	Questions
17. SCADA Network Management	02. Are you using any network management security packages? (Please list)
17. SCADA Network Management	03. Can you make device configuration changes from the network management package? (Explain)
17. SCADA Network Management	04. Do you make device configuration changes from the network management package?
17. SCADA Network Management	05. How do you make remote configuration changes? (Telnet, FTP, TFTP, Web Browser, Other – Explain)
17. SCADA Network Management	06. Is remote configuration of the network equipment allowed?
17. SCADA Network Management	07. Please list the equipment remotely configurable.
17. SCADA Network Management	08. Are you monitoring/auditing the network using a network management package?
17. SCADA Network Management	09. Are you monitoring/auditing the network using a network management package? What type of information is collected?
17. SCADA Network Management	10. How would you rate your organization's dependency on the network management package(s)? (Low, Medium, High)
17. SCADA Network Management	11. Do you have a help desk?
18. Firewalls	01. Do any of the devices apply a firewall to the data traffic?
18. Firewalls	01a. Is a password required for configuration of the firewall(s)?
18. Firewalls	01b. How many people have passwords to the firewall(s) (number of people)?
18. Firewalls	01c. Are the passwords to the firewall shared?
18. Firewalls	01d. Are the firewall passwords audited on a regular basis?
18. Firewalls	01e. What is the schedule of audit?

Asset	Questions
18. Firewalls	02. How is the information flow decided upon (i.e. by policy, user request, etc.)?
18. Firewalls	03. What protocol services are enabled? (Telnet, Ftp, Mail, Other)
18. Firewalls	04. Are the firewall configurations available for review?
18. Firewalls	04a. Who is the point of Contact?
18. Firewalls	05. Firewall specifications (Type)
19. Intrusion Detection Systems (IDS)	01. Do you have an intrusion detection system?
19. Intrusion Detection Systems (IDS)	02. Are you doing host-based or network-based intrusion detection?
19. Intrusion Detection Systems (IDS)	03. Have you run a security scanner on your system?
20. Data Separation (PVCs, VPNs, VLANs)	01. Is the SCADA network physically separate from all other networks, i.e. enterprise, City Municipality, etc.?
20. Data Separation (PVCs, VPNs, VLANs)	02. Are VLANs configured in your network?
20. Data Separation (PVCs, VPNs, VLANs)	03. Which business area does each of the VLANs belong to?
20. Data Separation (PVCs, VPNs, VLANs)	04. Is a topology drawing of the VLANs available?
20. Data Separation (PVCs, VPNs, VLANs)	04a. If yes, please specify the location and point of contact.

Asset	Questions
20. Data Separation (PVCs, VPNs, VLANs)	05. How many VLANs exist in the network?
21. Data Protection Methods (encryption, etc.)	01. Do you utilize any form of data privacy (encryption) on the network?
21. Data Protection Methods (encryption, etc.)	02. How often do you scan for viruses?
21. Data Protection Methods (encryption, etc.)	02a. Is this documented?
21. Data Protection Methods (encryption, etc.)	02b.How often is the virus database updated?
21. Data Protection Methods (encryption, etc.)	03. Is sensitive data protected by any means anywhere in transit or storage (e.g., SSL, SHTTP, other encryption, etc.)?
21. Data Protection Methods (encryption, etc.)	04. Is the input data protected in transit by any means (SSL, other encryption, etc.)?
21. Data Protection Methods (encryption, etc.)	05. Do you employ authentication mechanisms for end to end circuit connectivity?
21. Data Protection Methods (encryption, etc.)	05a. Is so, please list the type of authentication used.
21. Data Protection Methods (encryption, etc.)	06. Do you utilize personal certificates?
21. Data Protection Methods (encryption, etc.)	06a. Do you password protect your personal certificate(s)?
21. Data Protection Methods (encryption, etc.)	06b. Have you made backups of your personal certificate(s)?

Asset	Questions
21. Data Protection Methods (encryption, etc.)	07. Does your site use keys or certificates?
21. Data Protection Methods (encryption, etc.)	07a. Describe how you perform key management.
21. Data Protection Methods (encryption, etc.)	07b. Do you back up your private keys and certificates?
21. Data Protection Methods (encryption, etc.)	07c. How do you protect your private key?
21. Data Protection Methods (encryption, etc.)	08. Please list the types of software or hardware that is utilized for data privacy.
21. Data Protection Methods (encryption, etc.)	09. Please list the types of software or hardware that is utilized for encryption.
22. Access Control Lists (ACLs)	01. Do any of the devices utilize access control lists (ACLs) on the data?
22. Access Control Lists (ACLs)	02. What data is blocked/allowed through the ACL(s)?
22. Access Control Lists (ACLs)	03. Are the ACLs available for review?
22. Access Control Lists (ACLs)	03a. Where are the located and who is the point of contact?
22A. Data	01. What type of data traverses the network (administrative – sensitive or non-sensitive, sensor output, SCADA control information , engineering data, SCADA alarm reporting, physical security alarms, fire/safety alarms, other)?
22A. Data	02. Describe the type of data that crosses the business network interface (administrative – sensitive or non-sensitive, sensor output, SCADA control information , engineering data, SCADA alarm reporting, physical security alarms, fire/safety alarms, other)?
22A. Data	03. How is data shared? (Specifically, what are the transfer mechanisms? Shared Oracle tables? Bulk file transfers? Other?)

Asset	Questions
22A. Data	04. How is the application data stored? (Flat files, relational DBMS, don't know/other)
22A. Data	05. Who develops the schemas for the shared corporate data repositories? Please provide a point of contact.
22A. Data	06. Who has write privileges to the above mentioned schemas?
22A. Data	07. Who maintains the schemas for the shared corporate data repositories?
25. Cables (fiber optic, copper)	01. Please select the physical transport mediums that apply (copper/electrical, fiber optic, wireless).
25. Cables (fiber optic, copper)	02. Are all communication links (i.e. Ethernet cables, fiber optic links, etc.) physically inaccessible?
25. Cables (fiber optic, copper)	03. Is there a physical backup connection for critical communications?
26. Wireless links (microwave, satellite, etc.)	01. Does the SCADA data network include microwave or radio links?
26. Wireless links (microwave, satellite, etc.)	02. Are you providing data protection (encryption, authentication, etc.) on the wireless links?
27. Routers	01. How many routers exist in your network?
28. Ethernet Switches/Hubs	01. How many Ethernet Hubs exist in your network?
28. Ethernet Switches/Hubs	02. How many switches exist in your network?
29. Bridges	01. How many bridges exist in your network?
30. Backup Configurations	01. Are backups performed?
30. Backup Configurations	01a. Who performs backups?
30. Backup Configurations	01b. How regularly are backups performed?

Asset	Questions
30. Backup Configurations	01c. Is the data verified for correctness or viruses (other?) before it is stored?
30. Backup Configurations	01d. Have you ever tried to restore from these backups?
30. Backup Configurations	01e. If so, when was the last time you tried to restore from these backups?
30. Backup Configurations	02. Is the RTUs/PLCs software code backed up?
30. Backup Configurations	02a. What are the conditions of these critical software backups?
30. Backup Configurations	03. What recovery processes or procedures do you have in place for this application?
30. Backup Configurations	04. Do you have a recovery procedure for the network equipment?
30. Backup Configurations	04a. Please describe the recovery procedure.
30. Backup Configurations	05. Do you have a recovery procedure for the firewall(s)?
30. Backup Configurations	05a. Please describe the recovery procedure.
30. Backup Configurations	06. Do you have alternate processes or procedures to use during recovery?
30. Backup Configurations	06a. Please describe these processes or procedures.
30. Backup Configurations	06b. How long does recovery take?
30. Backup Configurations	07. Do you have alternate processes or procedures if NO recovery is possible?
30. Backup Configurations	08. Do you have back-up configuration for the network equipment?
30. Backup Configurations	08a. Where is it located?
30. Backup Configurations	09. Do you have a back-up configuration for the firewall(s)?

Asset	Questions
30. Backup Configurations	09a. Where is it located?
30. Backup Configurations	10. Where is client data stored?
30. Backup Configurations	11a. How is the client data backed up?
30. Backup Configurations	11b. Where are the backups stored?
30. Backup Configurations	11c. For how long to you retain these backups?
31. Configuration Management	01. Do you have a configuration management process to maintain the SCADA architecture?
31. Configuration Management	01a. Is the configuration management process documented?
31. Configuration Management	01b. If yes, please indicate the location of the documentation
31. Configuration Management	02. What is the mechanism for training personnel in this process?
31. Configuration Management	03. What security elements are incorporated into this training?
31. Configuration Management	04. Is there a configuration management process for the control room hardware/software?
31. Configuration Management	05. Are there system configuration guidelines for client workstations?
31. Configuration Management	06. Are passwords audited on a regular basis?
31. Configuration Management	06a. What is the schedule of the audits?
31. Configuration Management	07. Have you identified the critical components in your LAN?
31. Configuration Management	07a. Is so, please list them.
31. Configuration Management	08. Have you identified the critical components in your remote access operations?

Asset	Questions
31. Configuration Management	09. Have you identified the critical components in your WAN?
31. Configuration Management	09a. Is so, please list them.
31. Configuration Management	10. Is there a configuration management process for maintaining equipment?
31. Configuration Management	10a. If not, please explain.
31. Configuration Management	11. Is there a configuration management process for maintaining LAN equipment?
31. Configuration Management	11a. If not, please explain.
31. Configuration Management	12. Is there a configuration management process for maintaining remote access capability?
31. Configuration Management	12a. If not, please explain.
31. Configuration Management	13. Are there master inventory lists of SCADA hardware and software?
31. Configuration Management	13a. What is the location of this data?
31. Configuration Management	13b. How often are they updated, reviewed, or checked?
31. Configuration Management	14. Where are the SCADA baselines stored (physical location and device)?
31. Configuration Management	15. Where are the SCADA documents and drawings stored (physical location and device)?
31. Configuration Management	16. Where is SCADA's operational baseline located? (List multiple sites, if applicable)
31. Configuration Management	17. Can copies of official records be distributed electronically?
31. Configuration Management	18. Please describe the process for preventing the loss, alteration, or unauthorized use of official records.
31. Configuration Management	19. Can non-mission critical activities be performed using copies of official records?

Asset	Questions
31. Configuration Management	20. Is the process for an employee to request remote access capability formally documented?
31. Configuration Management	21. What is the schedule for reviewing the audit logs?
32. Physical Protections of SCADA equipment	01. Is the server equipment at your facilities physically secured?
32. Physical Protections of SCADA equipment	01a. If so, how is the server equipment physically secured?
32. Physical Protections of SCADA equipment	02. Are the SCADA terminals at your facilities physically secured?
32. Physical Protections of SCADA equipment	02a. How are the SCADA terminals physically secured?
32. Physical Protections of SCADA equipment	03. How many personnel have access to the SCADA terminal equipment?
32. Physical Protections of SCADA equipment	03a. Who?
32. Physical Protections of SCADA equipment	04. Is the remote SCADA equipment at your facilities physically secured?
32. Physical Protections of SCADA equipment	04a. How is the remote SCADA equipment physically secured?
32. Physical Protections of SCADA equipment	05. Is the communication link equipment at your facilities physically secured?
32. Physical Protections of SCADA equipment	05a. How is the communication link equipment physically secured?

Asset	Questions
32. Physical Protections of SCADA equipment	06. Are the communication link termination points of the SCADA network physically secured?
32. Physical Protections of SCADA equipment	06a. How are the communication link termination points of the SCADA network physically secured?
32. Physical Protections of SCADA equipment	07. Is the LAN equipment at your facilities physically secured?
32. Physical Protections of SCADA equipment	07a. How is the LAN equipment physically secured?
32. Physical Protections of SCADA equipment	08. Is the WAN equipment at your facilities physically secured?
32. Physical Protections of SCADA equipment	08a. How is the WAN equipment physically secured?
32. Physical Protections of SCADA equipment	09. Is the remote access equipment at your facilities physically secured?
32. Physical Protections of SCADA equipment	09a. How is the remote access equipment physically secured?
32. Physical Protections of SCADA equipment	10. How many personnel have access to the SCADA server equipment?
32. Physical Protections of SCADA equipment	10a. Who?
32. Physical Protections of SCADA equipment	11. How many personnel have access to the remote SCADA equipment?
32. Physical Protections of SCADA equipment	11a. Who?

Asset	Questions
32. Physical Protections of SCADA equipment	12. How many personnel have access to the SCADA communication link equipment?
32. Physical Protections of SCADA equipment	12a. Who?
32. Physical Protections of SCADA equipment	13. How many personnel have access to the SCADA communication link termination points?
32. Physical Protections of SCADA equipment	13a. Who?
32. Physical Protections of SCADA equipment	14. How many personnel have access to the SCADA LAN equipment?
32. Physical Protections of SCADA equipment	14a. Who?
32. Physical Protections of SCADA equipment	15. How many personnel have access to the SCADA WAN equipment?
32. Physical Protections of SCADA equipment	15a. Who?
32. Physical Protections of SCADA equipment	16. How many personnel have access to the SCADA remote access equipment?
32. Physical Protections of SCADA equipment	16a. Who?

F.6. Onsite Chemical Assessment Worksheet

Onsite Chemical Assessment Worksheet

Trade Name	Chemical Name	Maximum Storage Amount	Units	Conc.	Delivery Method	Liquid Density	MSDS	Injection method, # of sites, total flow rates
Liquid Chlorine	Chlorine	10	ton	100%	1 ton cylinders	NA	Y	2 injectors rated at 5,000 lbs/day each. Vacuum limited to 9,000 lbs/day
Ammonia Water	Aqueous ammonium hydroxide	5,000	gallons	20 wt %	tanker truck	0.9	Y	2 metering pumps rated at 2,000 gal/day
Permanganate	Potassium permanganate	9,000	lbs	100%	1500 kg bins	NA	Y	Screw auger solids feed of one bin/day. Overhead crane used to change bins.

Location____________ Site________________ Maximum Water Flow______ Minimum Water Flow______

Date______________ Typical Water Flow_________ Time to 1st customer______

Comments:

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

APPENDIX G: CONSEQUENCE ASSESSMENT FOR THE EXAMPLE WATER UTILITY

G.1 Determining Critical Assets Consequence Levels

After the assessment team agrees to a site-specific consequence matrix and the associated definitions, they then review the critical assets identified from the fault tree and rank the. undesirable events as high, medium, or low. To help determine the consequence value for each undesired event (critical asset) a table is used which lists the undesired events on the left and the measures of consequence on the top. A Consequence Value Table (Table 5.3) for the example water utility was developed based on Table 5.2 (Section 5.6.2) and information provided in the water utility description (Appendix A). A detailed description of how the high, medium, and low consequence values were derived are discussed below.

Damage or Destroy Pipelines/Conduits

- Economic loss to water utility (defined as cost to repair and economic loss)
  - L = Less than $500K to replace (loss is only to exposed pipeline, most of pipeline is underground, assumed there is a turnoff valve nearby
- Duration of loss
  - H = if destroyed it will take more than 24 hours to fix (facility is out of operation during repair time)
- Number of users impacted
  - H = Serves 80% of geographical area and 75% of customers (90 mgd out of 100 mgd)

Damage or destroy disinfection capability at Treatment Plant 2

- Economic loss to water utility
  - M = Once it's been detected, the water utility needs to shutdown Treatment Plant 2, Pump Station 1 and Pump Station no. 2 and storage. Cannot deliver to the customer. Need to fix the disinfection process (may lose chemicals, equipment, treated water)
- Duration of loss

- M = Will take at least a day to fix/repair the disinfection process, however raw water can be pumped if necessary

- Number of users impacted
  - M = Treatment Plants 1 and 3 will have to run at maximum capacity and storage will have to be depleted to try to keep up with demand

Loss of pumps (loss of capability of pumping at Treatment Plant 2)

- Economic loss to water utility
  - L = Loss of capability of pumping station (e.g., a motor, a shaft, a component, less than $500K to replace)
- Duration of loss
  - H = Will take more than a day to repair (pumps are one-of-a-kind – don't have parts on the shelf)
- Number of users impacted
  - H = Loss of capability of pumping affect, water can't move through Treatment Plant 2 to Pumping Stations 1 and 2

Loss of key personnel at Treatment Plant 2

- Economic loss to water utility
  - L = If the operator at Treatment Plant 2 is affected, the process is not interrupted (treated water is still delivered)
- Duration of loss
  - L = If the operator at Treatment Plant 2 is affected, the process is not interrupted (treated water is still delivered)
- Number of users impacted
  - L = If the operator at Treatment Plant 2 is affected, the process is not interrupted (treated water is still delivered)

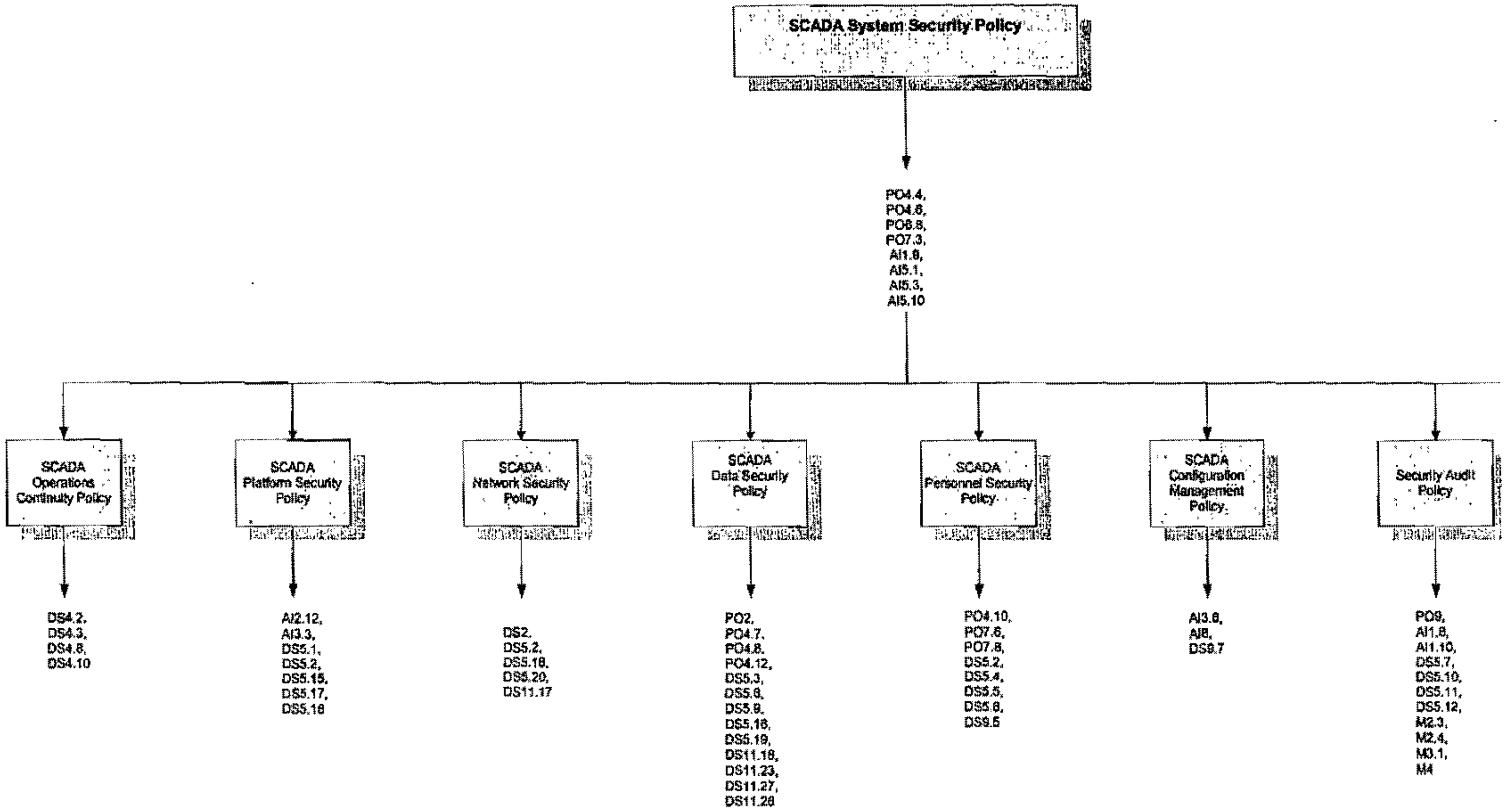
The overall consequence values in Table 5.2 were assigned based on the highest qualitative value determined for that specific undesired event. For example, for the undesired event "damage or destroy pipelines/conduits" one "L" and two "H's" were determined or the consequence measures, therefore the overall consequence value was an "H."

APPENDIX H: SCADA SECURITY POLICY FRAMEWORK

Increasing the security level of the complete SCADA system will require much more than simple "technology fixes." The adoption of an Information Technology (IT) framework such as CobiT[2] will allow the water utility to effectively design and maintain a robust, secure SCADA system. The development and maintenance of a security policy is the first recommendation to be addressed. Sandia has developed a SCADA Security Policy Framework™ that follows in two forms, one is the framework with the areas that need to be addressed in a security policy and the other shows the mapping of those areas to CobiT. Basic security policies would include access and password controls, network perimeter definition, and data sensitivity definition requirements. Addressing the security policy issue in a timely manner is critical for the secure implementation and management SCADA systems.

[2] IT Governance Institute, *CobiT, Governance, Control, and Audit for Information and Related Technology*, Information Systems Audit and Control Foundation, Rolling Hills, IL, 2000.

SCADA Security Policy Framework^{TM} to CobiT Control Objective



SCADA System Security Policy

PO4.4,
PO4.6,
PO8.8,
PO7.3,
AI1.8,
AI5.1,
AI5.3,
AI5.10

SCADA Operations Continuity Policy

DS4.2,
DS4.3,
DS4.8,
DS4.10

SCADA Platform Security Policy

AI2.12,
AI3.3,
DS5.1,
DS5.2,
DS5.15,
DS5.17,
DS5.18

SCADA Network Security Policy

DS2,
DS5.2,
DS5.18,
DS5.20,
DS11.17

SCADA Data Security Policy

PO2,
PO4.7,
PO4.8,
PO4.12,
DS5.3,
DS5.8,
DS5.9,
DS5.18,
DS5.19,
DS11.18,
DS11.23,
DS11.27,
DS11.28

SCADA Personnel Security Policy

PO4.10,
PO7.6,
PO7.8,
DS5.2,
DS5.4,
DS5.5,
DS5.8,
DS9.5

SCADA Configuration Management Policy

AI3.6,
AI8,
DS9.7

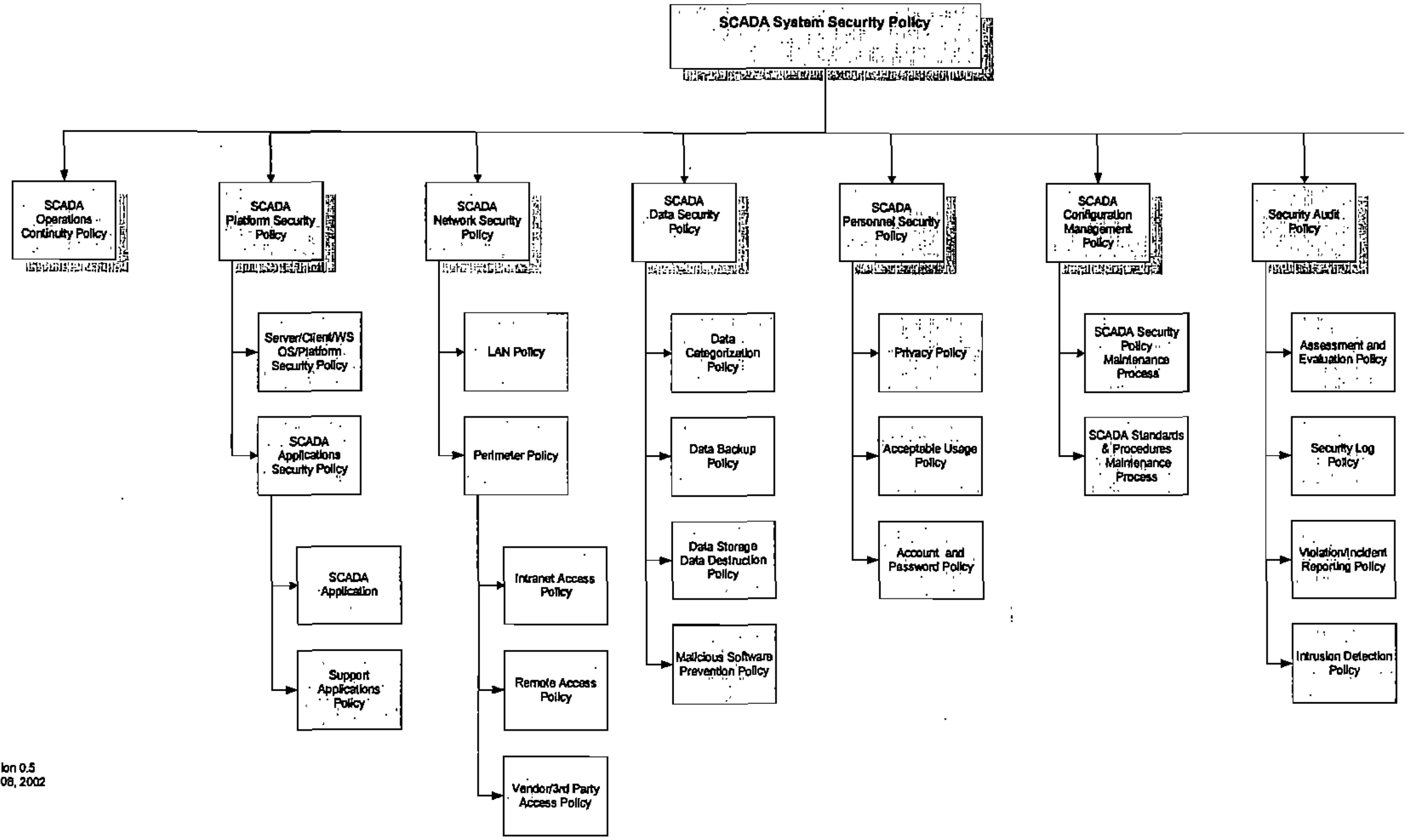
Security Audit Policy

PO9,
AI1.8,
AI1.10,
DS5.7,
DS5.10,
DS5.11,
DS5.12,
M2.3,
M2.4,
M3.1,
M4

Version 0.8
Aug 08, 2002
JDD

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

SCADA Security Policy Framework™



- SCADA System Security Policy
  - SCADA Operations Continuity Policy
  - SCADA Platform Security Policy
    - Server/Client/WS OS/Platform Security Policy
    - SCADA Applications Security Policy
      - SCADA Application
      - Support Applications Policy
  - SCADA Network Security Policy
    - LAN Policy
    - Perimeter Policy
      - Intranet Access Policy
      - Remote Access Policy
      - Vendor/3rd Party Access Policy
  - SCADA Data Security Policy
    - Data Categorization Policy
    - Data Backup Policy
    - Data Storage Data Destruction Policy
    - Malicious Software Prevention Policy
  - SCADA Personnel Security Policy
    - Privacy Policy
    - Acceptable Usage Policy
    - Account and Password Policy
  - SCADA Configuration Management Policy
    - SCADA Security Policy Maintenance Process
    - SCADA Standards & Procedures Maintenance Process
  - Security Audit Policy
    - Assessment and Evaluation Policy
    - Security Log Policy
    - Violation/Incident Reporting Policy
    - Intrusion Detection Policy

Version 0.5
Aug 08, 2002
JDD

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

REFERENCES

American Water Works Association
http://www.awwa.org/

Association of Metropolitan Water Agencies
http://www.amwa.net/

Awwa Research Foundation (AwwaRF)
http://www.awwarf.com/

Campbell, P. 2002. *A Taxonomy of Information Assurance,* SAND2002-0131, Sandia National Laboratories, Albuquerque, NM.

Environmental Protection Agency
http://www.epa.gov/safewater/security/

FBI, InfraGard
http://www.infragard.net/

Freeman, J.W., Darr, T.C., Neely, R.B. 1997. *Risk Assessment for Large Heterogeneous Systems,* IEEE Proc. 13th Annual Computer Security Applications Conference. pp. 44-52.

Garcia, Mary Lynn. 2001. *The Design and Evaluation of Physical Protection Systems*, Reed Elsevier (Butterworth-Heinemann), Boston, MA.

IT Governance Institute™ 2000. *CobiT®: Governance, Control and Audit for Information and Related Technology*, Information Systems Audit and Control Foundation, Rolling Meadows, IL.

Modarres, M. 1993. *What Every Engineer Should Know About Reliability and Risk Analysis*, Marcel Dekker, Inc., New York, NY.

National Infrastructure Protection Center (FBI)
http://www.nipc.gov/

Oddo, F., Editor. 1994. *The Memory Jogger*, GOAL/QPC, Methuen, MA.

The Merck Index, 12th edition, Susan Budavari, ed., 1996. Merck and Company Inc., Whitehouse Station, NJ.

Sandia National Laboratories (Congressional Testimony)
www.sandia.gov/news-center/resources/congress-testimony/index.html

Section 11 (Toxicological Properties) of the Material Safety Data Sheets (MSDS) for specific chemicals, MDL Information Systems, Inc., Nashville, TN

ACRONYMS AND DEFINITIONS

AMWA	Association of Metropolitan Water Agencies
ASD	Adversary Sequence Diagrams
ATM	Asynchronous Transfer Mode
AWWA	American Water Works Association
AwwaRF	Awwa Research Foundation
BMS	balanced magnetic switch
CDC	Centers for Disease Control
CDP	critical detection point
CobiT	Control Objectives for Information and Related Technology
CSU	channel service unit
DBT	Design Basis Threat
DEMUX	de-multiplexers
DEPO	Design and Evaluation Process Outline
DMZ	De-Militarized Zone (see definition)
DoS	denial of service
DSU	data service unit
EASI	Estimate of Adversary Sequence Interruption
EPA	Environmental Protection Agency
ERP	emergency response plan
FAC	free available chlorine
FBI	Federal Bureau of Investigation
FEP	front-end processor
FTP	File Transfer Protocol
GIS	Geographical Information System
GPM	gallons per minute
H	High
ID	identification
IED	intelligent electronic device
IOC	Input/Output Controller
IRP	Incident Response Plan
IT	information technology
L	Low
LAN	local area network
LOX	liquefied oxygen
M	Medium
MG	million gallons
MGD	million gallons per day
MSDS	Material Safety Data Sheet
MUX	multiplexers
N/A	not applicable
PC	personal computer
PDD	Presidential Decision Directive
PL	Public Law

PPM	parts per million
PVC	permanent virtual circuit
PPS	physical protection system (see definition)
RAM-W^{SM}	Risk Assessment Methodology for Water Utilities
RDCP	Redundant Distributed Process Controllers Routing Information Protocol
RIP	Routing Information Protocol
RFT	response force time
RTU	Remote Terminal Unit
SAVI	Systemic Analysis of Vulnerability to Intrusion
SCADA	Supervisory Control and Data Acquisition (see definition)
SMTP	Simple Mail Transfer Protocol
SOW	Scope of Work
SPOF	single point of failure
TBD	to be determined
TFTP	Trivial File Transfer Protocol
TR	time remaining
UPS	Uninterruptible Power Supply
VFD	variable frequency drives
VLAN	virtual local area network
VPN	virtual private network
WAN	wide area network
WMD	Weapon of Mass Destruction (see definition)

DEFINITIONS

Asset – A useful, valuable item dedicated to a specific purpose.

DMZ – A network located between a trusted network (SCADA) and an untrusted network (external or business).

Facility – Located on a site having a specific function, usually a building or structure.

Estimates – Results of a ranking process by which expert judgment may be used to assign relative values to subjective assessments. High (H) = .9; Medium (M) = .5; Low (L) = .1.

PPS – Provides notification that a malevolent act is being attempted (detection), makes it difficult and time consuming for an adversary to complete the malevolent act (delay), and allows a security force enough time to stop the adversary (response).

Protection System – A security system that includes both aspects of a physical protection system and operational design system.

Red Team – An independent, threat-based effort by an interdisciplinary, simulated team, which uses both active and passive capabilities to expose and exploit information assurance vulnerabilities of an IT system. (After proper safeguards are established)

SCADA – A Supervisory Control and Data Acquisition (SCADA) system is typically defined as computer-based monitoring and control system that centrally collects, displays, and stores information from remotely located data collection transducers and sensors in order to support the supervised remote control of equipment, devices, and automated functions.

Site – A geographic location providing a particular function or purpose.

Target – A specific area or component to be protected to prevent undesirable consequences. The object of an attack.

Water Utility System – The entire complex of equipment, ranging from input of water to distribution of water.

WMD – Generally, a weapon of mass destruction is any weapon capable of inflicting a large number of deaths immediately or over a period of time. Examples are chemical, biological, radiological, or explosive weapons. In this report, WMD refers to a malicious act that results in WMD-like consequences by exploiting some weakness of the water utility operation. Destruction of a dam with the resultant flood causing the death of a large number of people is an example. Another example is dispersal of toxic chemicals.

American Water Works
Association

6666 West Quincy Avenue
Denver, CO 80235-3098
T (303) 794-7711
F (303) 795-1989
www.awwa.org

The Authoritative Resource for Safe Drinking Water SM

New AWWA Security Resources

Don't miss out on these new security resources, brought to you by the American Water Works Association.

New dates now available!

Vulnerability Assessments for Water Utilities (RAM-W^{sm}) Seminar

This hands-on seminar is designed to help you develop security plans at your utility. You'll learn key components of the methodology and immediately apply them through guided exercises. By the end of the class, you'll have an action plan that may be immediately implemented at your utility. Course material is licensed from AwwaRF and Sandia National Laboratories and includes material from the first and second editions of the Risk Assessment Methodology for Water Utilities.

February 19–21, 2003	Scottsdale, Arizona
February 24–26, 2003	Dallas, Texas
March 5–7, 2003	New Orleans, Louisiana
March 12–14, 2003	Arlington, Virginia

AWWA Water Security Congress

March 23–26, 2003 • Los Angeles, California

To help you deal with the new security challenges you are facing, attend the AWWA Water Security Congress. Christie Whitman, United States Environmental Protection Agency Administrator, is scheduled to be the keynote luncheon speaker on Tuesday, March 25. The event will also feature seminars from leading water and water security experts in the nation addressing topics such as vulnerability assessments, water quality monitoring, research and legislative updates, distribution system security, crisis decision-making, security hardware and technology, crisis communications, and threat identification and response. This important opportunity will provide a forum for water industry leaders to learn, network, and share ideas. *Members who register by February 26 will save $100 on the registration fee.*

Cyber Security Seminar

In this seminar, participants will learn what types of action should be taken to secure SCADA (supervisory control and data acquisition) systems and other computer-based systems from outside intrusion.

May 13–14, 2003	Denver, Colorado
May 28–29, 2003	Syracuse, New York

Online Institute: Security Planning for Drinking Water Systems—An Operational Approach
[link is http://www.awwa.org/learnonline/]
AWWA, in conjunction with the US Environmental Protection Agency, has developed this online course to address operational procedures for securing your drinking water facility. This course is designed to introduce water professionals to appropriate security measures in the water industry including.securing planning for the total water system, physical system vulnerability assessment, operational system vulnerability assessment, and emergency response preparation.

NEW—Risk Assessment Methodology for Water Utilities, Second Edition
The second edition of Risk Assessment Methodology for Water Utilities has recently been released. This proprietary and confidential methodology is available to water utilities, government agencies, and security consultants. The procedures outlined in this report will guide drinking water utilities through a complete security review; to assist in making informed decisions about how best to reduce risks from intentional sabotage and other emergency events. Risk Assessment Methodology for Water Utilities, 2e is $85 plus shipping and handling. A confidentiality and nondisclosure agreement must be signed in order to obtain this product. To order or for more information and necessary forms, please call Eric Lovick, AWWA Customer Service, 303.734.3441.

Water System Security: A Field Guide
This book emphasizes measures any size water utility can take for better security against man-made threats. It covers emergency preparedness plans, vulnerability assessments, mitigation measures for critical components, emergency response and recovery, and crisis communications. Catalog Number 20501. Retail price: $89, AWWA Member price: $58.

Water System Security: A Video Field Guide
This companion video to Water System Security: A Field Guide covers emergency preparedness plans, vulnerability assessments, mitigation measures for critical components, emergency response and recovery, and crisis communications. Catalog number 65247. Retail price: $185, AWWA Member price: $125.

Water System Security Set
Includes *Water System Security: A Field Guide* book and video. Catalog number WSSFG. Retail price: $259.95, AWWA Member price: $169.95. Please call AWWA Customer Seri

To register or order, go to **www.awwa.org**
or call AWWA Customer Service at 800.926.7337

CASE STUDY

RISK ASSESSMENT METHODOLOGY FOR WATER UTILITIES (RAM-W^{SM})$_{\text{SECOND EDITION}}$

Prepared by
Security Systems and Technology Center
Sandia National Laboratories
Albuquerque, NM 87185-0789

Jointly sponsored by

Awwa Research Foundation
6666 West Quincy Avenue
Denver, CO 80235-3098

&

U.S. Environmental Protection Agency
Ariel Rios Building
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460

SENSITIVE SECURITY INFORMATION: CONFIDENTIAL AND PROPRIETARY

This document contains information that is not appropriate for public dissemination. Do not copy or further distribute this information. This information may be subject to International Trade in Arms regulations (ITAR) 22CFR 120-130. Export of ITAR information may require a license from the U.S. Department of State.

Published by the
Awwa Research Foundation

DISCLAIMER

This study was jointly funded by the Awwa Research Foundation (AwwaRF) and the U.S. Environmental Protection Agency under Cooperative Agreement No. X-82956501. AwwaRF and USEPA assume no responsibility for the content of the research study reported in this publication or for the opinions or statements of fact expressed in the report. The mention of trade names for commercial products does not represent or imply the approval or endorsement of AwwaRF or USEPA. This report is presented solely for informational purposes.

Proprietary - Copyrighted

NOT APPROVED FOR PUBLIC RELEASE – This document contains information exempt from mandatory disclosure under the FOIA. Exemption 2 applies.

WARNING – This document contains data whose disclosure is restricted by 5 U.S.C. § 552(b)(2) (2000), the Freedom of Information Act, and the U.S. Attorney General FOIA Memorandum of October 12, 2001. Dissemination of this document is controlled. Violation of governing laws is subject to severe criminal penalties.

DISTRIBUTION – Department of Energy approval required prior to public release. This document may not be transmitted over the open Internet unless it is encrypted.

DESTRUCTION – Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Disclaimer of Liability

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Prepared by Sandia National Laboratories. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

CONTENTS

TABLES

FIGURES

EXECUTIVE SUMMARY

INTRODUCTION

This Case Study demonstrates parts of RAM-W^{SM} and is not intended to be comprehensive, nor is it considered to be the acceptable format for a final report. From the many hours spent teaching, performing assessments, and developing the methodology, several areas have been noted that require supplemental examples to explain certain concepts. The Case Study presents another example of those areas that will help assessment teams understand and apply the concepts better.

The Case Study was not designed to be a standalone document, and the student/practitioner should review the corresponding chapters in the methodology while reviewing this material. The Case Study has been designed to be as real as possible, but certain assumptions have to be made for brevity.

Overview

This document contains an example of the application of the RAM-W^{SM} methodology to a fictitious municipal water system called MetroCity. The major elements of the process are presented for illustration purposes. The reader should be aware that much detail is omitted, and the example should be reviewed with the appropriate chapters of RAM-W^{SM}. The physical structure and facility names are fabricated, and any similarity to an existing water utility is purely coincidental. MetroCity is designed primarily to rely on gravity for water delivery to complement the example facility used in RAM-W^{SM}, which primarily relies on pumps. Also, it should be noted that water utility systems vary greatly, not only in their source and distribution infrastructure, but in the way they are managed, their mission(s), operational procedures, intrinsic vulnerabilities, etc. This example should be considered as merely a guideline and not as a strict template for all systems. The RAM-W^{SM} process is designed to be sufficiently flexible to accommodate virtually any facility architecture, but it must be applied with considerable judgment to be successful.

In general, boxed italicized text within this example is used to indicate instructive information. The remaining text indicates example material.

1 GENERAL DESCRIPTION OF THE FACILITY

1.1. Introduction

MetroCity Water District (MCWD) is primarily a gravity fed system (Figure 1), but it includes two pump stations for service to some higher elevation areas.

MCWD supplies water to 500,000 customers in the greater MetroCity area. Typical peak summer consumption is 125 million gallons per day (MGD). Annual-average usage is 90 MGD. The Santa Inez watershed is owned by MetroCity and drains 50,000 acres. Melting snow and rain are gathered and stored in the 3-billion-gallon Santa Inez Lake, which is constrained by the Santa Inez Dam and spillway. Water from the spillway flows into the Santa Inez River, and approximately 50% of this flow is diverted to the 600-million-gallon (MG) Duck Pond. At the base of the Duck Pond is the 5-MW Corona hydroelectric station fed by the penstock. A bypass line with pressure regulating valves allows all or just the excess flow to bypass Corona.

From the hydroelectric station, water flows through the McGrath tunnel. This tunnel follows the contour of the land until it reaches Shaft 1, which carries water to a deeply buried section of tunnel 300 feet below grade. At Shaft 2, water returns to grade level and continues on to the Newman Reservoir. Control valves regulate flow into the reservoir. Bypass lines can route water around the reservoir during maintenance and direct flow to the Torres Treatment Plant (TTP). Newman Reservoir has a storage capacity of 600 MG, which equates to approximately a one-week supply of water. Sluice gates regulate flow from Newman Reservoir to the inlet of TTP. The reservoir is located in forested area surrounded by a residential neighborhood.

TTP is located at the outlet of Newman Reservoir and provides primary disinfection and corrosion control. The water is screened prior to entering the treatment plant, and chlorine gas is injected for disinfection. The treatment building can store up to ten 1-ton cylinders of chlorine. Up to 50 tons of lime are stored on site for pH adjustment. In addition, up to 25,000 gallons of fluorosilicic acid are stored at the treatment plant and used for dental hygiene.

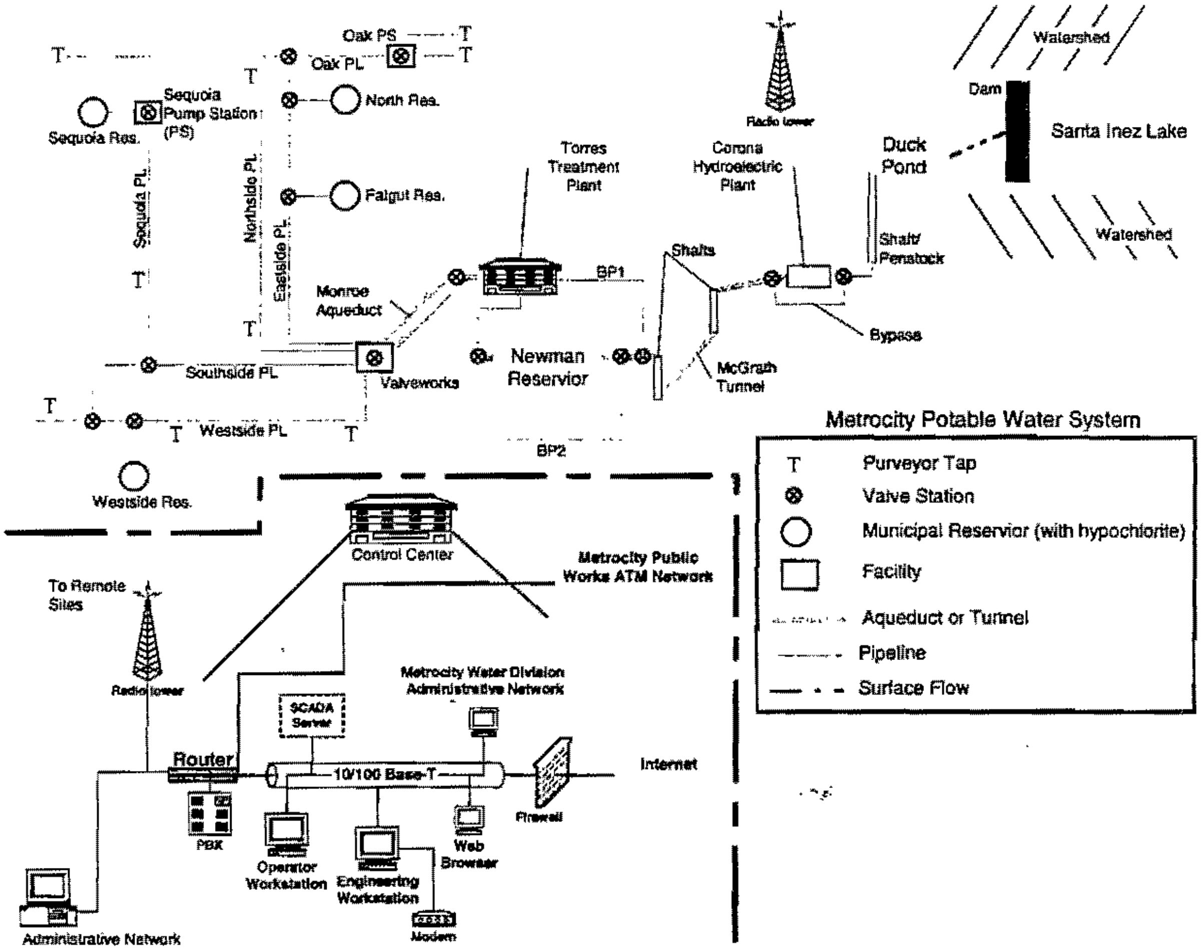


Figure 1. MCWD Schematic Diagram

From the TTP, the water is transported via the Monroe Aqueduct. The aqueduct starts as a 64-inch-diameter pipe that transports water from the TTP to a header. From there, the flow is divided into two 40-inch pipes. The 64-inch pipe follows the contour of the land and is exposed as it crosses over a major freeway. The two 40-inch pipes are buried their entire 10-mile length until they enter the Valveworks.

The Valveworks facility takes water from the Monroe Aqueduct and distributes it to four major distribution lines, each 36 inches in diameter: the Westside Pipeline, the Northside Pipeline, the Eastside Pipeline, and the Southside Pipeline. Gate valves (36-inch diameter) housed in the facility enable flow to be shut off to any of the four distribution pipelines. However, there is no ability to control the incoming supply lines from the Valveworks.

Two major pump stations boost pressure to high service areas: the Oak Pump Station and the Sequoia Pump Station. The Oak Pump Station houses two pumps, each with a capacity of 7,000 gallons per minute (gpm). This pump station feeds water to the purveyors at the end of the Eastside and Northside pipelines and to the North Reservoir. The Sequoia Pump Station has three 3,000 gpm capacity pumps that supply water to Sequoia Reservoir.

Four major reservoirs in the distribution system store treated water: Westside Reservoir (25 MG capacity), Fatgut Reservoir (60 MG), Sequoia Reservoir (5 MG), and North Reservoir (10 MG). At the outlet of each of these reservoirs, residual treatment is provided by sodium hypochlorite. The Westside, Sequoia, and North reservoirs are all covered. The Fatgut Reservoir is an open-water reservoir. Each reservoir stores approximately a 24-hour supply of water for its respective customers.

The entire system is controlled by a SCADA system located at the Control Center (CC). This system is integrated with the MetroCity Information Technology (IT) system or network by a standard firewall interconnection. The CC also monitors security alarms located throughout the system.

Roughly equal numbers of customers are serviced by each purveyor tap; however, there is a concentration of hospitals serviced by the westernmost tap of the Westside Pipeline and a military base by the two easternmost taps of the Oak Pipeline.

1.2. SCADA System Description

1.2.1. SCADA Physical/Hardware Description

The SCADA system controls and monitors 24 sites. There are approximately 100 RTUs/PLCs in this system. These control loops primarily provide (1) SCADA alarm monitoring and control, (2) water pressure and treatment monitoring, and (3) valve and pump control functions. Personnel monitor and control the system via control panels located in the CC. Valves of up to 60 inches in diameter can be controlled from the CC. Most of the pumps at the system pump stations are also controlled via the control panel in the CC. The main SCADA process control Local Area Network (LAN) consists of a redundant architecture and utilizes Ethernet technology with IP/TCP suite of network protocols. Backups are available for the critical SCADA server. Communication links include Ethernet, microwave, fiber optics, and leased phone lines. The city administers the microwave and fiber optic ATM networks, which include several critical paths. A local phone service provides T1 connectivity for part of the system.

Currently, backups do not exist for several of the MetroCity communication links. Physical protection systems for the SCADA and network equipment at the CC consist of two layers of locked doors, with administrative access only to the network equipment and the SCADA server. Some of the remote sites have no physical protection. No data protection (e.g., encryption) is utilized during data transfer or storage.

1.2.2. SCADA Operational Descriptions

There is no official SCADA security policy, although some basic security elements, such as passwords, firewalls, etc., are incorporated into the system operations. Configuration management is performed on a limited basis, mainly focusing on the SCADA-specific equipment (as opposed to the supporting network). There are three skilled SCADA system administrators, but they do not receive any regular formal security training. SCADA accounts are restricted to the levels of administrators and operators, with password verification required. Regular virus checking and formalized event logging are not explicitly defined operational requirements for the system. Intrusion detection and network management packages are not incorporated into the

SCADA system. No remote SCADA operations are allowed, but there is remote access to the engineering workstations and for some network management functions.

Public information based on SCADA data is available on the MetroCity web page, and historical data transferred from the SCADA network to the administrative network is utilized for engineering and planning decisions. As noted previously, none of the data is encrypted during either transfer or storage.

The CC PLC receives intrusion detection data for the physical intrusion detection alarms. This PLC concentrates the alarm data and sends them to both the analog display system and the SCADA system. The alarm system in the CC consists of both alarm sounds and lights. Staff indicated that most alarms are false alarms that result from weather conditions. As a result, alarm sounds are often disabled in the CC, particularly if specific weather conditions exist. A light comes on and stays on even if the alarm is turned off. Alarms are responded to at the discretion of the operator.

1.3. MCWD Mission Objective

The first step in the security assessment of a water utility is to identify and prioritize the mission objectives of the water utility. These objectives must be defined in order to accurately measure the importance of the various facilities and assets. Refer to Section 3 of the methodology document.

The (three) main mission objectives identified for MCWD are to:

(1) Provide adequate water volume for firefighting

(2) Provide water to critical customers

(3) Provide potable water

These mission objectives (Table 1) are placed into a pairwise comparison matrix and compared to one another.

Table 1. Mission Objectives Comparison for MCWD

Mission Objectives Comparison	Fire Flow	Critical Customers	Potable Water	Sum
Fire Flow	x	4	5	9
Critical Customers	2	x	4	6
Potable Water	1	2	x	3

As can be seen from the Sum column in Table 1, the pairwise process determines that the most important mission objective is to provide *fire flow*, followed by *critical customers* and then *potable water*.

1.4. Facility Prioritization

Once the mission objectives are established and prioritized, the RAM-W^{SM} process uses the rankings in Table 1 to complete a pairwise comparison of the major components of the MCWD potable water system. Each of the facilities is compared against all others for each of the mission objectives. Additionally, the mission objectives are weighted according to their relative importance shown in the Sum column in Table 1. The results of the prioritization of the facilities are shown in Tables 2, 3, and 4. The results of the mission-weighted facility prioritization are shown in Table 5.

Refer to Section 3 of the methodology document.

Table 2. Facility Comparison Results for the MCWD Fire Flow Mission Objective

Facility Prioritization for Fireflow Mission	Santa Inez Facility	Duck Pond	Corona Penstock	Corona Hydroelectric Plant	McGrath Tunnel	Torres Treatment Plant	Newman Reservoir	Monroe Aqueduct	Valveworks	Control Center	Westside PL	Southside PL	Northside	Eastside	Westside Reservoir	Sequoia Reservoir	Fatgut Reservoir	North Reservoir	Sequoia PS	Oak PS	SUM
Santa Inez Facility		3	3	5	3	5	1	1	1	1	2	2	2	2	1	1	1	1	1	1	37
Duck Pond	3		3	5	3	5	1	1	1	1	2	2	2	2	1	1	1	1	1	1	37
Corona Penstock	3	3		5	3	5	1	1	1	1	2	2	2	2	1	1	1	1	1	1	37
Corona Hydroelectric Plant	1	1	1		1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	21
McGrath Tunnel	3	3	3	5		4	2	2	2	1	2	2	2	2	2	2	2	2	2	2	45
Torres Treatment Plant	1	1	1	3	2		1	1	1	1	1	1	1	1	1	1	1	1	1	1	22
Newman Reservoir	5	5	5	5	4	5		3	2	2	3	3	3	3	4	4	4	4	4	4	72
Monroe Aqueduct	5	5	5	5	4	5	3		3	3	3	3	3	3	4	4	4	4	4	4	74
Valveworks	5	5	5	5	4	5	4	3		4	4	4	4	4	4	4	4	4	3	3	78
Control Center	5	5	5	5	5	5	4	3	2		4	4	4	4	3	3	3	3	4	4	75
Westside PL	4	4	4	5	4	5	3	3	2	2		3	3	3	4	4	4	4	3	3	67
Southside PL	4	4	4	5	4	5	3	3	2	2	3		3	3	4	4	4	4	3	3	67
Northside	4	4	4	5	4	5	3	3	2	2	3	3		3	4	4	4	4	3	3	67
Eastside	4	4	4	5	4	5	3	3	2	2	3	3	3		4	4	4	4	3	3	67
Westside Reservoir	5	5	5	5	4	5	2	2	2	3	2	2	2	2		3	3	3	4	4	63
Sequoia Reservoir	5	5	5	5	4	5	2	2	2	3	2	2	2	2	3		3	3	4	4	63
Fatgut Reservoir	5	5	5	5	4	5	2	2	2	3	2	2	2	2	3	3		3	4	4	63
North Reservoir	5	5	5	5	4	5	2	2	2	3	2	2	2	2	3	3	3		4	4	63
Sequoia PS	5	5	5	5	4	5	2	2	3	2	3	3	3	3	2	2	2	2		3	61
Oak PS	5	5	5	5	4	5	2	2	3	2	3	3	3	3	2	2	2	2	3		61

Table 3. Facility Comparison Results for the MCWD Critical Customers Mission

Facility Prioritization for Critical Customers Mission	Santa Inez Facility	Duck Pond	Corona Penstock	Corona Hydroelectric Plant	McGrath Tunnel	Torres Treatment Plant	Newman Reservoir	Monroe Aqueduct	Valveworks	Control Center	Westside PL	Southside PL	Northside	Eastside	Westside Reservoir	Sequoia Reservoir	Fatgut Reservoir	North Reservoir	Sequoia PS	Oak PS	**SUM**
Santa Inez Facility		3	3	5	3	3	2	2	2	1	1	2	2	2	2	4	2	2	4	1	46
Duck Pond	3		3	5	3	3	2	2	2	1	1	2	2	2	2	4	2	2	4	1	46
Corona Penstock	3	3		5	3	3	2	2	2	1	1	2	2	2	2	4	2	2	4	1	46
Corona Hydroelectric Plant	1	1	1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	19
McGrath Tunnel	3	3	3	5		3	2	2	2	1	1	2	2	2	2	4	2	2	4	1	46
Torres Treatment Plant	3	3	3	5	3		3	3	2	2	2	2	2	2	2	4	3	3	5	2	54
Newman Reservoir	4	4	4	5	4	3		3	3	2	2	3	3	2	2	4	2	2	5	1	58
Monroe Aqueduct	4	4	4	5	4	3	3		3	2	2	3	3	2	2	4	2	2	5	1	58
Valveworks	4	4	4	5	4	4	3	3		2	2	3	3	2	2	4	2	2	5	1	59
Control Center	5	5	5	5	5	4	4	4	4		3	3	3	3	2	5	3	2	5	2	72
Westside PL	5	5	5	5	5	4	4	4	4	3		4	3	2	3	5	4	3	5	2	75
Southside PL	4	4	4	5	4	4	3	3	3	3	2		2	2	2	5	3	2	5	2	62
Northside	4	4	4	5	4	4	3	3	3	3	3	4		2	2	4	2	2	5	1	62
Eastside	4	4	4	5	4	4	4	4	4	3	4	4	4		4	5	4	3	5	3	76
Westside Reservoir	4	4	4	5	4	4	4	4	4	4	3	4	4	2		5	4	4	5	2	74
Sequoia Reservoir	2	2	2	5	2	2	2	2	2	1	1	1	2	1	1		1	1	3	1	34
Fatgut Reservoir	4	4	4	5	4	3	4	4	4	3	2	3	4	2	2	5		2	5	2	66
North Reservoir	4	4	4	5	4	3	4	4	4	4	3	4	4	3	2	5	4		5	2	72
Sequoia PS	2	2	2	5	2	1	1	1	1	1	1	1	1	1	1	3	1	1		1	29
Oak PS	5	5	5	5	5	4	5	5	5	4	4	4	5	3	4	5	4	4	5		86

Table 4. Facility Comparison Results for the MCWD Potable Water Mission

Facility Prioritization for Potable Water Mission	Santa Inez Facility	Duck Pond	Corona Penstock	Corona Hydroelectric Plant	McGrath Tunnel	Torres Treatment Plant	Newman Reservoir	Monroe Aqueduct	Valveworks	Control Center	Westside PL	Southside PL	Northside	Eastside	Westside Reservoir	Sequoia Reservoir	Fatgut Reservoir	North Reservoir	Sequoia PS	Oak PS	**SUM**
Santa Inez Facility		3	3	5	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	70
Duck Pond	3		3	5	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	70
Corona Penstock	3	3		5	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	70
Corona Hydroelectric Plant	1	1	1		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	19
McGrath Tunnel	3	3	3	5		3	3	3	3	4	4	4	4	4	4	4	4	4	4	4	70
Torres Treatment Plant	3	3	3	5	3		3	3	3	3	4	4	4	4	4	4	4	4	5	5	71
Newman Reservoir	3	3	3	5	3	3		3	3	3	4	4	4	4	4	4	4	4	5	5	71
Monroe Aqueduct	3	3	3	5	3	3	3		3	3	4	4	4	4	4	4	4	4	5	5	71
Valveworks	3	3	3	5	3	3	3	3		4	4	4	4	4	3	3	3	3	3	3	64
Control Center	2	2	2	5	2	3	3	3	2		3	3	3	3	2	2	2	2	2	2	48
Westside PL	2	2	2	5	2	2	2	2	2	3		3	3	3	3	3	3	3	3	3	51
Southside PL	2	2	2	5	2	2	2	2	2	3	3		3	3	3	3	3	3	3	3	51
Northside	2	2	2	5	2	2	2	2	2	3	3	3		3	3	3	3	3	3	3	51
Eastside	2	2	2	5	2	2	2	2	2	3	3	3	3		3	3	3	3	3	3	51
Westside Reservoir	2	2	2	5	2	2	2	2	3	4	3	3	3	3		3	3	3	3	3	53
Sequoia Reservoir	2	2	2	5	2	2	2	2	3	4	3	3	3	3	3		3	3	3	3	53
Fatgut Reservoir	2	2	2	5	2	2	2	2	3	4	3	3	3	3	3	3		3	3	3	53
North Reservoir	2	2	2	5	2	2	2	2	3	4	3	3	3	3	3	3	3		3	3	53
Sequoia PS	2	2	2	5	2	1	1	1	3	4	3	3	3	3	3	3	3	3		3	50
Oak PS	2	2	2	5	2	1	1	1	3	4	3	3	3	3	3	3	3	3	3		50

Table 5. Facility Mission-weighted Comparison Results for MCWD

Facility	Fireflow (wt = 9)	Critical Customer (wt = 6)	Potable Water (wt = 3)	SUM	Rank
Control Center	675	432	144	1251	1
Valveworks	702	354	192	1248	2
Monroe Aqueduct	666	348	213	1227	3
Oak PS	549	516	150	1215	4
Eastside	603	456	153	1212	5
Newman Reservoir	648	348	213	1209	6
Westside PL	603	450	153	1206	7
Westside Reservoir	567	444	159	1170	8
North Reservoir	567	432	159	1158	9
Southside PL	603	372	153	1128	10
Northside	603	372	153	1128	11
Fatgut Reservoir	567	396	159	1122	12
Sequoia Reservoir	567	204	159	930	13
McGrath Tunnel	405	276	210	891	14
Sequoia PS	549	174	150	873	15
Santa Inez Facility	333	276	210	819	16
Duck Pond	333	276	210	819	17
Corona Penstock	333	276	210	819	18
Torres Treatment Plant	198	324	213	735	19
Corona Hydroelectric Plant	189	114	57	360	20

Table 5 provides an overall prioritization of the facilities within MCWD. This information is used later (in conjunction with the fault tree) to identify the critical assets. The assessment team may also wish to reference this table during its assessments.

1.5. Detailed Facility Descriptions

For the assessment process to work, individual facility detail must be considered for many security aspects. This section would normally contain information that aids in the characterization of the various facilities. For brevity, this information is not included in this example, but will rely on the general information provided earlier.

2. THREAT ANALYSIS AND CHARACTERIZATION

The threat against which the water utility is to be evaluated must also be defined. This step is necessary for several reasons, but essentially, the definition provides a standard that can be used to measure the security performance of the water utility – MCWD in this example. Refer to Section 4 of the methodology document.

Following the process outlined in Chapter 4 – Understanding the Threat, MCWD came to the Design Basis Threat (DBT) in Table 6:

Table 6. Design Basis Threat for MCWD

Adversary	Number of Adversaries	Knowledge	Equipment	Vehicles	Weapons	Objective/ Tactics
Outsider (Medium)	1–3 One Team performing a single task or two closely related tasks	Limited knowledge of facility	Hand/power tools and bulk explosives, chemicals, and/or biological contaminants, ~10 lb/person	Pickup 4 x 4	Handguns	Damage water system and chem-bio attack
Insider (Medium)	1	Some knowledge of all systems. SCADA access with Power-user operator level skills	Hand/power tools, all equipment	Pickup 4 x 4 and all vehicles	None	Disrupt water system or contam-inate with on-site chemicals
Hacker - Outsider (Medium)	1	Moderate hacker skills, little system operational knowledge	Access to internet and hacker tools	N/A	Common, available hacker tools	Denial of service, unfocused disruption

2.1. DBT Summary

The Outsider group consists of one to three outsiders working as one unit capable of attacking any single target or two targets at a single facility, equipped with sophisticated tools, explosives, and weapons. All equipment is man portable and easily obtainable. The outsiders have limited knowledge of the security system and of MCWD operations. The outsiders' goal is to inhibit delivery of water by causing damage to critical assets or to introduce chemicals into the water supply to harm end-users.

The Insider consists of a single motivated employee or contractor working unaccompanied with limited authorized access and possessing limited knowledge of the water processing, emergency, and security systems. The insider has access to MCWD hand and power tools but lacks authorization to access the available chemicals. The insider has knowledge of the security procedures and uses this knowledge to achieve his/her goals. She may also have SCADA access and skills at the operator (not administrator) level. The insider's goal is to disrupt MCWD operations. The purpose may be to show the public the vulnerability of the MCWD system and to sway opinion during employee down-sizing.

The Hacker is an individual with limited knowledge of the IT structure of MCWD. This individual may have direct access via a modem or PC connected to the IT structure and may have and use sophisticated hacker tools to compromise the systems. Actions may include denial of service and disruption of some business functions.

2.2. Likelihood of Attack

The next step in the process is to estimate the likelihood that each of the adversary groups defined in Table 6 would attempt to carry out an attack that could cause the undesired event for the facility(ies) of concern for MCWD. This provides the information for the first term in the risk equation, Likelihood of Attack, P_A. There is currently a lack of industry-wide information on possible threats to water utilities, and because there is no discernible difference in possible threat from one part of MCWD to another, P_A for the entire system is assumed in subsequent analyses to be 1. This assumption is conservative, in that the calculated relative risk is at a maximum when P_A is assumed to be 1. The actual Likelihood of Attack lies between 0 and 1.

3. UTILITY CHARACTERIZATION AND VULNERABILITY IDENTIFICATION

One of the most important tasks performed during the on-site assessment is that of characterizing the various facilities and assets and identifying the vulnerabilities. This section illustrates the vulnerabilities for MCWD.

3.1. Chemical Vulnerabilities

The issue of chemical attacks is very complicated and must be addressed carefully by an extensive analysis of all the on-site chemicals, their quantities and flow rates, uses, accessibility, and possible interactions. Also, the potential for externally introduced toxic or biological chemicals adds another dimension to the problem. For brevity, shortened examples of how to deal with these issues will be examined in this case study.

The TTP has the following chemicals on-site in the listed quantities:

- Ten 1-ton chlorine cylinders (3 injectors rated at 4000 lb/day vacuum limited to 9000 lb/day total delivery)
- Two 25-ton lime silos (four screw auger systems rated at 500 lb/day each. Lime is slaked then solution-injected.)
- One 25,000 gallon tank of fluorosilicic acid (4 metering pumps each rated at 600 gallons/day)

The average flow rate through TTP will be assumed to be 90 MG/day. Calculations were performed to see what the maximum levels are that could be maintained with the intact flow system over a 24-hour period.

Chlorine gas is the primary method for final sterilization and maintaining antimicrobial activity within the water distribution system. It is injected at the TTP via a vacuum supply system controlled by water flow. The chlorine gas in this system is delivered as gas over a liquid in 2000 lb of (primarily liquid) elemental chlorine. Each tank contains two valves, one for dispensing liquid and another for dispensing gas. There is also a fusible lead plug designed to melt/blow out if pressure/temperature of the tank becomes too high for the container to handle. If the gas injector system is used at the maximum feed rate, the concentration throughout the day can be maintained at 12 parts per million (ppm) for the TTP effluent (this concentration can be higher or lower depending on actual water flow on that day). Chlorine gas is detectable at 0.08 ppm in air. The OSHA limit is 1 ppm_v (pulm) and 25–50 ppm_v (pulm) is considered a dangerous level. Since most people can detect (by smell) 0.5 ppm of chlorine in water, it is not likely that this feed rate would be maintained for more than a few hours. Over-chlorination of the water is not a likely threat in terms of injuring the customers. LD_{Lo} for ingestion of chlorine was determined to be 42 gm/kg continuously over a two-week period for rats. A concern may be in the catastrophic release of multiple containers that can overwhelm the scrubbing capacity of the storage facility. Environmental and safety requirements should have a calculated scenario for the release of any toxic gases stored on site.

Lime is used to control the pH of the water. It is delivered as powdered quicklime (CaO), which is then hydrated (slaked) to $Ca(OH)_2$ on site. The LD_{50} is 7.3 gm/kg (oral mouse); therefore, it is practically nontoxic. Continuous injection would result in 3.51 ppm of $Ca(OH)_2$ being delivered to the customers.

Fluorosilicic acid is used to artificially fluoridate the water at the TPP. It is delivered via tanker truck as a 24-wt% aqueous solution (density =1.234 kg/l) and is stored inside the facility. If all the storage were discharged into the water lines with the pumps running at maximum capacity, a concentration of 8 ppm of fluorosilicic acid would result. The target dosage by a typical water system is ~7 ppm fluorosilicic acid for an 0.8-ppm residual fluoride target. Assuming complete inventory release, the residual fluoride level would be about 1.1 ppm. Fluoride has shown chronic effects at elevated levels (tooth staining, bone embrittlement), but acute doses are less well characterized. Information from the Centers for Disease Control (CDC) indicates that doses up to 5 mg/kg body weight of fluoride are acceptable even in children (no known toxicity at this level). Therefore, fluoride is not a useful contamination target.

As can be seen from the analysis, the largest potential consequence is not associated with contamination of the water using the chemicals on site, but rather use of the available chemicals to create a cloud of poisonous gas. There are approximately 10 tons of chlorine gas at the TTP. There is only enough scrubber capacity for one tank of chlorine, and there is only one repair kit available for repairing the chlorine tanks in case of a rupture. It is assumed in this study that the chlorine tanks would be a primary target of the adversary.

It is further assumed that the adversary will be capable (as indicated in the DBT) of introducing foreign chemicals into the system. The analysis contained in this example will allow for that kind of attack. Fortunately, in many cases, the substances will experience such high dilution rates as to make them ineffective.

3.2. SCADA Analysis and Vulnerabilities

3.2.1. Analysis

Refer to Section 5 of the methodology document for detailed information on the SCADA analysis process. For this case study, only operational assets are considered; however, for a complete analysis, both asset classes would need to be analyzed. An example of the physical assets relative ranking is detailed in Section 5 of the methodology document.

After determining the SCADA operational assets, the relative ranking process proceeds as depicted in Figure 2.

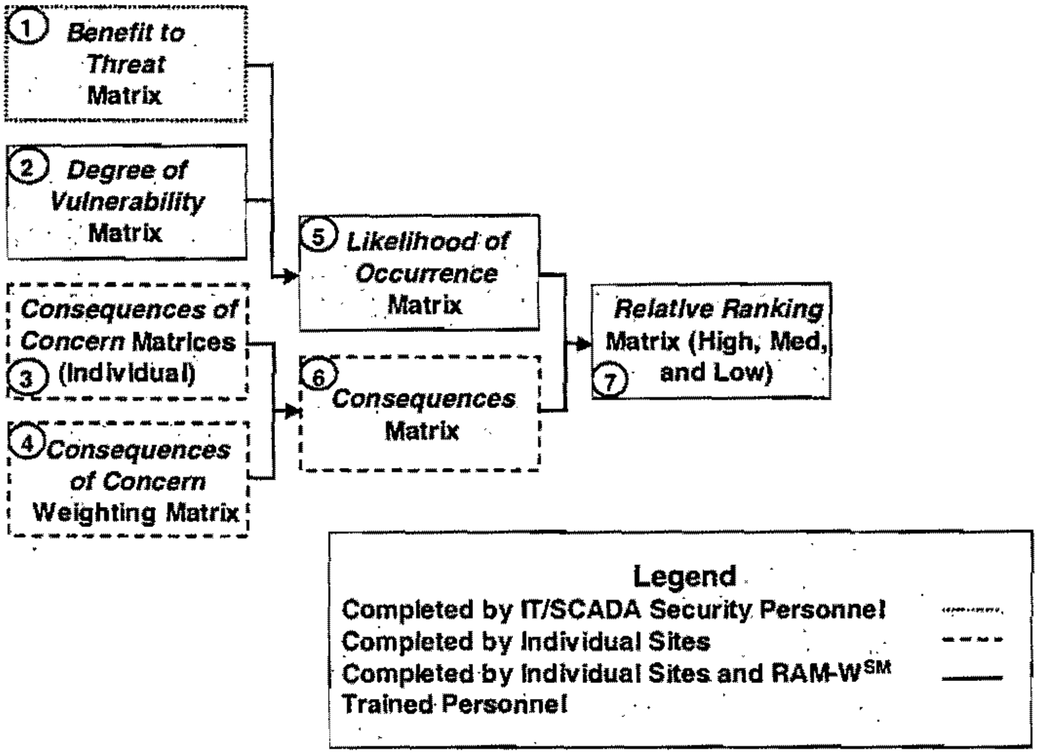

1 Benefit to Threat Matrix
2 Degree of Vulnerability Matrix
Consequences of Concern Matrices 3 (Individual)
4 Consequences of Concern Weighting Matrix
5 Likelihood of Occurrence Matrix
6 Consequences Matrix
Relative Ranking Matrix (High, Med, 7 and Low)
Legend
Completed by IT/SCADA Security Personnel
Completed by Individual Sites
Completed by Individual Sites and RAM-W^SM Trained Personnel

Figure 2. SCADA System Asset Relative Ranking Process

Tables 7a through 7i represent the SCADA analysis for the case study. For detailed explanations of each table, refer to Section 5.8 of the RAM methodology.

Table 7a. Example of Benefit to Threat (Adversary) Matrix

Benefit to Threat	Security Policy	Configuration Management	Security Training	SCADA Network Man.	Backup Configurations	Remote SCADA Operations	Skilled Personnel	SCADA Account Restrictions	SCADA Control Data	Support Data	Raw Totals	Normalized
Security Policy		5	3	5	5	3	3	3	5	5	37	0.14
Configuration Management	1		1	3	3	1	1	1	3	3	17	0.06
Security Training	3	5		5	5	3	3	3	5	5	37	0.14
SCADA Network Man.	1	3	1		5	3	3	3	5	5	29	0.11
Backup Configurations	1	3	1	1		1	1	1	3	3	15	0.06
Remote SCADA Operations	3	5	3	3	5		3	3	5	5	35	0.13
Skilled Personnel	3	5	3	3	5	3		3	5	5	35	0.13
SCADA Account Restrictions	3	5	3	3	5	3	3		5	5	35	0.13
SCADA Control Data	1	3	1	1	3	1	1	1		5	17	0.06
Support Data	1	3	1	1	3	1	1	1	1		13	0.05
										Total	270	1.00

Table 7b. Example of Degree of Vulnerability Matrix

Degree of Vulnerability	Security Policy	Configuration Management	Security Training	SCADA Network Man.	Backup Configurations	Remote SCADA Operations	Skilled Personnel	SCADA Account Restrictions	SCADA Control Data	Support Data	Raw Totals	Normalized
Security Policy	■	5	3	5	5	3	5	5	5	5	41	0.15
Configuration Management	1	■	1	5	5	5	5	5	3	3	33	0.12
Security Training	3	5	■	5	5	5	3	5	3	3	37	0.14
SCADA Network Man.	1	1	1	■	3	5	1	1	1	3	17	0.06
Backup Configurations	1	1	1	3	■	5	3	3	1	1	19	0.07
Remote SCADA Operations	3	1	1	1	1	■	1	1	1	1	11	0.04
Skilled Personnel	1	1	3	5	3	5	■	3	1	1	23	0.09
SCADA Account Restrictions	1	1	1	5	3	5	3	■	1	1	21	0.08
SCADA Control Data	1	3	3	5	5	5	5	5	■	3	35	0.13
Support Data	1	3	3	3	5	5	5	5	3	■	33	0.12
										Total	270	1.00

Table 7c. Example of a Consequence of Concern Matrix (Individual)

Interrupt or Impair Water Flow in the System	Security Policy	Configuration Management	Security Training	SCADA Network Man.	Backup Configurations	Remote SCADA Operations	Skilled Personnel	SCADA Account Restrictions	SCADA Control Data	Support Data	Raw Totals	Normalized
Security Policy	■	3	3	3	5	5	3	3	1	5	31	0.11
Configuration Management	3	■	3	3	3	5	1	1	1	3	23	0.09
Security Training	3	3	■	5	5	5	3	1	1	3	29	0.11
SCADA Network Man.	3	3	1	■	5	5	1	1	1	3	23	0.09
Backup Configurations	1	3	1	1	■	5	1	1	1	3	17	0.06
Remote SCADA Operations	1	1	1	1	1	■	1	1	1	1	9	0.03
Skilled Personnel	3	5	3	5	5	5	■	5	5	5	41	0.15
SCADA Account Restrictions	3	5	5	5	5	5	1	■	3	5	37	0.14
SCADA Control Data	5	5	5	5	5	5	1	3	■	5	39	0.14
Support Data	1	3	3	3	3	5	1	1	1	■	21	0.08
										Total	270	1.00

Table 7d. Example of a Consequence of Concern Matrix (Individual)

Contaminate Water	Security Policy	Configuration Management	Security Training	SCADA Network Man.	Backup Configurations	Remote SCADA Operations	Skilled Personnel	SCADA Account Restrictions	SCADA Control Data	Support Data	Raw Totals	Normalized
Security Policy	■	3	5	5	5	5	3	3	1	3	33	0.12
Configuration Management	3	■	3	1	5	5	1	1	1	3	23	0.09
Security Training	1	3	■	5	5	5	3	3	1	5	31	0.11
SCADA Network Man.	1	5	1	■	5	5	1	1	1	3	23	0.09
Backup Configurations	1	1	1	1	■	5	1	1	1	1	13	0.05
Remote SCADA Operations	1	1	1	1	1	■	1	1	1	1	9	0.03
Skilled Personnel	3	5	3	5	5	5	■	3	1	5	35	0.13
SCADA Account Restrictions	3	5	3	5	5	5	3	■	3	5	37	0.14
SCADA Control Data	5	5	5	5	5	5	5	3	■	5	43	0.16
Support Data	3	3	1	3	5	5	1	1	1	■	23	0.09
										Total	270	1.00

Table 7e. Example of a Consequence of Concern Matrix (Individual)

Weapon of Mass Destruction (WMD) Event	Security Policy	Configuration Management	Security Training	SCADA Network Man.	Backup Configurations	Remote SCADA Operations	Skilled Personnel	SCADA Account Restrictions	SCADA Control Data	Support Data	Raw Totals	Normalized
Security Policy		5	3	5	5	5	3	3	1	3	33	0.12
Configuration Management	1		1	1	3	5	1	1	1	1	15	0.06
Security Training	3	5		3	5	5	3	1	1	3	29	0.11
SCADA Network Man.	1	5	3		5	5	1	3	1	5	29	0.11
Backup Configurations	1	3	1	1		5	1	1	1	3	17	0.06
Remote SCADA Operations	1	1	1	1	1		1	1	1	1	9	0.03
Skilled Personnel	3	5	3	5	5	5		5	3	5	39	0.14
SCADA Account Restrictions	3	5	5	3	5	5	1		3	5	35	0.13
SCADA Control Data	5	5	5	5	5	5	3	3		5	41	0.15
Support Data	3	5	3	1	3	5	1	1	1		23	0.09
										Total	270	1.00

Table 7f. Summary Matrix for Consequences of Concern (Individual)

Consequences (Numbers refer to criteria)	Interrupt or Impair Water Flow in the System	Contaminate Water	Weapon of Mass Destruction (WMD) Event	Consequences Total	Consequences Total Normalized
Security Policy	0.11	0.12	0.12	0.12	0.12
Configuration Management	0.09	0.09	0.06	0.08	0.08
Security Training	0.11	0.11	0.11	0.11	0.11
SCADA Network Man.	0.09	0.09	0.11	0.09	0.09
Backup Configurations	0.06	0.05	0.06	0.06	0.06
Remote SCADA Operations	0.03	0.03	0.03	0.03	0.03
Skilled Personnel	0.15	0.13	0.14	0.14	0.14
SCADA Account Restrictions	0.14	0.14	0.13	0.13	0.13
SCADA Control Data	0.14	0.16	0.15	0.15	0.15
Support Data	0.08	0.09	0.09	0.08	0.08
			Total	1.00	1.00

Table 7g. Example of Consequence Weighting Matrix

Criteria Criteria	Interrupt or Impair Water Flow in the System	Contaminate Water	Weapon of Mass Destruction (WMD) Event	Raw Score	Relative Decision Value
Interrupt or Impair Water Flow in the System	■	3	3	6	0.33
Contaminate Water	3	■	3	6	0.33
Weapon of Mass Destruction (WMD) Event	3	3	■	6	0.33
			Total	18	1.00

Table 7h. Example of Relative Risk Calculation

Criteria Assets	Consequences	Benefit to Threat	Degree of Vulnerability	Relative Likelihood of Occurrence	Relative Risk	Normalized Relative Risk
Security Policy	0.1198	0.1370	0.1519	0.0208	0.0025	0.23
Configuration Management	0.0753	0.0630	0.1222	0.0077	0.0006	0.05
Security Training	0.1099	0.1370	0.1370	0.0188	0.0021	0.19
SCADA Network Man.	0.0926	0.1074	0.0630	0.0068	0.0006	0.06
Backup Configurations	0.0580	0.0556	0.0704	0.0039	0.0002	0.02
Remote SCADA Operations	0.0333	0.1296	0.0407	0.0053	0.0002	0.02
Skilled Personnel	0.1420	0.1296	0.0852	0.0110	0.0016	0.14
SCADA Account Restrictions	0.1346	0.1296	0.0778	0.0101	0.0014	0.13
SCADA Control Data	0.1519	0.0630	0.1296	0.0082	0.0012	0.11
Support Data	0.0827	0.0481	0.1222	0.0059	0.0005	0.05
				Total	0.01	1.00

Table 7i. Final relative Ranking of Operational Assets

Final Relative Ranking	Relative Security Vulnerability
Security Policy	High
Security Training	High
Skilled Personnel	Med
SCADA Account Restrictions	Med
SCADA Control Data	Med
SCADA Network Man.	Low
Configuration Management	Low
Support Data	Low
Backup Configurations	Low
Remote SCADA Operations	Low

A final, prioritized list of SCADA operational assets indicates an order for applying resources to improve SCADA security. The next section provides more details on specific vulnerabilities.

3.2.2. SCADA Vulnerabilities

The SCADA analysis provided a rank list of operational assets for focusing security improvements. In this section, we elaborate on the high and medium elements of that ranked list. (See final ranking from previous section.)

3.2.2.1. SCADA Policy/Procedure/Configuration Management Vulnerabilities

Vulnerability: The system has no security policy or security plan. There is very little security awareness, security implementation and administration are lax, and there exists a general lack of recognition that security is important.

Vulnerability: SCADA personnel do not receive regular formal security training.

Vulnerability: The dial-up access into the SCADA network for the system administrators utilizes shared passwords and shared accounts. Shared accounts and passwords are weak. In addition, activity logging on remote activities becomes impractical.

Vulnerability: Inadequate data protection exists as the SCADA data traverses the MetroCity network, both as it is transferred to other SCADA segments and as the data are sent to servers on the administrative network. The data are used for a variety of purposes, including public display and engineering efforts.

3.3. Physical Vulnerabilities

This section discusses the assessment of major facilities in the MCWD system. Included here are some general security related comments, some specific observations, and some site descriptions. During this portion of the overall assessment, ratings of the facility security robustness were also made.

These ratings are listed or reflected in later tables. These descriptions are not intended to be complete but merely to indicate what types of information is necessary for completion of the assessment.

3.3.1. General Security Comments

Generally, most facilities had intrusion detection in the form of balanced magnetic switches on the entry doors as well as all other exterior doors. Normal entry procedure requires the operator to call the Control Center to inform the operator of entry into the facility. The CC would then see a "door open" light on their computer screen. Except where noted in the site description, all exterior doors were of hollow steel construction.

3.3.2. Santa Inez Lake, Dam, Spillway, and River

The Santa Inez watershed is closed to public access. The property is adjacent to a wilderness area. Vehicles that are allowed access are limited to MCWD service and employee vehicles. Gates are secured with chains and padlocks. Although employees regularly visit the lake, no personnel are stationed there.

A concrete arch dam impounds the water for Santa Inez Lake. It is unlikely small amounts of explosives will have any effect on the integrity of the structure. The river normally flows at 2500 cfs, making it impractical to contaminate the water at this point in the system.

3.3.3. Duck Pond

Similar to Santa Inez Lake, Duck Pond is closed to public access. It borders the national forest. Gates are secured with chains and padlocks. Although employees regularly visit the lake, no personnel are stationed there.

An earthen dam contains the water in Duck Pond. It is unlikely that small amounts of explosives will have any effect on the integrity of the dam.

3.3.4. McGrath Tunnel

McGrath Tunnel follows the contour of the land until it reaches Shaft 1, where water flows into a deeply buried tunnel until it reaches Shaft 2. From Shaft 2 downstream, the tunnel again follows the contour of the land. The tops of the shafts act as vents that are covered but not sealed. Contaminants can be introduced at the tops of these shafts; however, because of the flow rate, this action would likely be ineffective.

3.3.5. Newman Reservoir

Similar to Santa Inez Lake, Newman Reservoir is closed to public access. It borders a residential area on two sides. Gates are secured with chains and padlocks. A masonry dam impounds the water in Newman Reservoir. It is unlikely that small amounts of explosives will have any effect on the integrity of the dam.

3.3.6. Torres Treatment Plant

The major target at the TTP is a maximum of ten 1-ton chlorine storage containers. Typically only six cylinders are present and being used. The site has a chlorine gas scrubber system capable of handling a 1-ton cylinder leak. The chlorine storage building is a concrete block building with a metal roof. There are eight hollow metal doors in the facility. Each door has a balanced magnetic switch sensor and a crash bar. There are three roll-up doors with roller switch sensors. Sensors are monitored locally, but are turned off during the day when doors are typically unlocked. A 7-foot chain link fence with one vehicle gate surrounds the building compound. The gate is open and unlocked. Police response is 10 to 25 minutes provided operators can make a phone call. During the off-shift, only one person is on duty.

3.3.7. Monroe Aqueduct

The 64-inch aqueduct is covered under shallow earth for most of its length. However, a section of it is exposed as it runs under an overpass, which crosses a major interstate. Flooding could cause a major disruption to traffic.

3.3.8. Valveworks

The Valveworks facility contains several valves that can be manually operated or electrically operated locally or remotely by the SCADA system. Since the valves are large, it can take more than an hour to close them. The valves are contained in a masonry block building with a metal roof. There are eight personnel doors and two roll-up doors. The doors are of hollow metal construction. All personnel doors have balanced magnetic switches. The vehicle access doors have roller switches. Before entering the building, employees must notify the CC.

The exposed piping and valves in the facility are targets. Explosives are required to breach them. The Valveworks facility is on a fenced property. The fence is 7-feet high with outriggers and borders a business area. Response would be 20 to 60 minutes for a MCWD employee during normal operation and possibly much longer, if at all, during the off-shift.

3.3.9. Control Center

The CC is located in a business area of the city. It is a modern three-story building with large glass windows on the exterior offices. The front doors are locked and alarmed and are opened by employees with a swipe of a proximity card. No one is stationed at the front to stop people coming in once an employee opens the door. Also the back doors are unlocked during the day. The control room within the CC has hollow metal doors with a small glass pane and push-button locks for entry control. It has large glass windows that look into an adjacent office area.

3.3.10. Treated Water Reservoirs and Residual Treatment Stations

The reservoirs are located in residential areas. Seven-feet tall chain link fences surround each property. Each has vehicle access gates secured with chains and padlocks. There is evidence of vandals trespassing on the properties (spray painting). Access hatches on top of the covered reservoirs (Westside, Sequoia, and North) are secured with padlocks and are alarmed with roller switches. The relatively large capacity Fatgut Reservoir is an open water reservoir. Refer to Section 3.3.12 for contaminate information with respect to these reservoirs.

3.3.11. Pump Stations

The Oak and Sequoia Pump Stations each house pumps in masonry block buildings. The doors are alarmed, and employees must notify the CC before entering. The targets for both pump stations are the pumps. Hand or power tools or explosives are required to disable the pumps.

3.3.12. Potential Contaminates

Note: this section contains fictional data–for example only.

Local and federal law enforcement agencies recently have issued alerts to local water systems to be concerned about two potential methods of contamination. One of these materials is biological and the other is chemical.

The first is Agent-SKS a terrorist-developed chemical modification of a readily available pesticide. Synthesis of this material, in a temporary facility not much larger than an illicit methlab, produces a contaminate with increased toxicity, water solubility, and chloramine resistance over the parent compound. The LD_{Lo} for this compound has been estimated at 0.579 mg/kg. This means that 50 lb would be sufficient quantity to poison one million gallons of water. Samples of this material that have been tested indicate that it has very low resistance to direct chlorination. Boiling of the water containing this material is not advised because it will force the contaminant into the gas phase where it has an increased toxicity.

The biological contaminate material is *Yersinius dinoaves*—a genetically modified version of the plague bacterium manufactured by rogue nations and supplied to terrorist organizations. A concentrated 1 liter solution contains 8 x 10^8 bacteria and weighs 1.1 kg. One thousand organisms are considered an infective dose. Therefore, approximately 10 lb of this material could contaminate one million gallons of water. This organism has been engineered to be orally infective and resist chlorine up to 20 ppm in water. It is, however, very sensitive to alkalinity of the water. Exposure to pH greater than 8.3 for a matter of a few minutes completely inactivates it. Boiling is also effective in removing this contaminant.

3.4. Fault Tree

Critical assets are identified in the RAM-W^{SM} process, first by utilizing the facility pairwise results (discussed earlier) and then by analysis of the fault tree. The pairwise process produces a rank-ordered set of facilities, and the fault tree identifies the assets within those facilities and also ensures that no critical assets/targets (system-wide) were overlooked in the process.

3.4.1. MetroCity Fault Tree

The customized fault tree, which is essentially a logic diagram that describes the operation of the water system, is presented in this section. Refer to Section 5 of the methodology document.

3.4.2. Fault Tree Analyses

The upper level of the Generic Undesired Event fault tree is shown in Figure 3a..

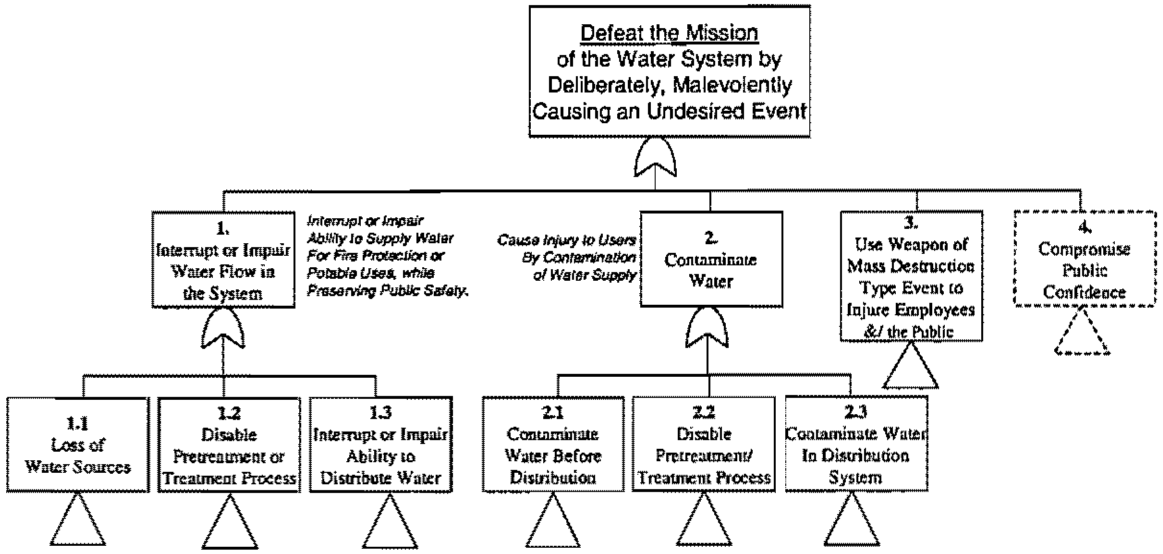

Defeat the Mission of the Water System by Deliberately, Malevolently Causing an Undesired Event
1. Interrupt or Impair Water Flow in the System
Interrupt or Impair Ability to Supply Water For Fire Protection or Potable Uses, while Preserving Public Safety.
Cause Injury to Users By Contamination of Water Supply
2. Contaminate Water
3. Use Weapon of Mass Destruction Type Event to Injure Employees &/ the Public
4. Compromise Public Confidence
1.1 Loss of Water Sources
1.2 Disable Pretreatment or Treatment Process
1.3 Interrupt or Impair Ability to Distribute Water
2.1 Contaminate Water Before Distribution
2.2 Disable Pretreatment/ Treatment Process
2.3 Contaminate Water In Distribution System

Figure 3a. Upper Level Elements of the Generic Fault Tree

The MCWD Generic Undesired Event Fault Tree will be evaluated on an element-by-element basis and customized to reflect the specificity in the system.

The fault tree analysis of MCWD will be demonstrated for the TTP. The process starts by following branch 1, *Interrupt or Impair Water Flow in the System* (see Figure 3a). Also on Figure 3a, included beneath *Interrupt or Impair Water Flow in the System*, is branch 1.2, *Disable Pretreatment or Treatment Process*. The development for *Disable Pretreatment or Treatment Process* is shown in Figure 3b.

TTP can take water from Newman Reservoir or from the bypass lines to provide disinfection. There are no filtration facilities at TTP. Disinfection is accomplished via chlorine injection from 1-ton cylinders, fluoride is added for promoting healthy teeth, and pH is adjusted by the addition of lime. For the fault tree branch shown in Figure 3b, the top-level undesired events of "Loss of Pumps," and "Loss of Valves" are crossed with a solid line because these items do not exist at TTP. There are pumps for the chemical feeds, but the water flows into the plant via gravity. Therefore, the higher level undesired event was removed. All the subsequent development under these three top-level events is removed as well. The top-level undesired event, "Loss of Key Personnel," is crossed off with an X indicating that multiple personnel are trained to operate the facility, and it is, therefore, not considered a probable adversary target.

See Appendix E (methodology document) for additional discussion on fault tree symbols and to see all elements of the generic fault tree.

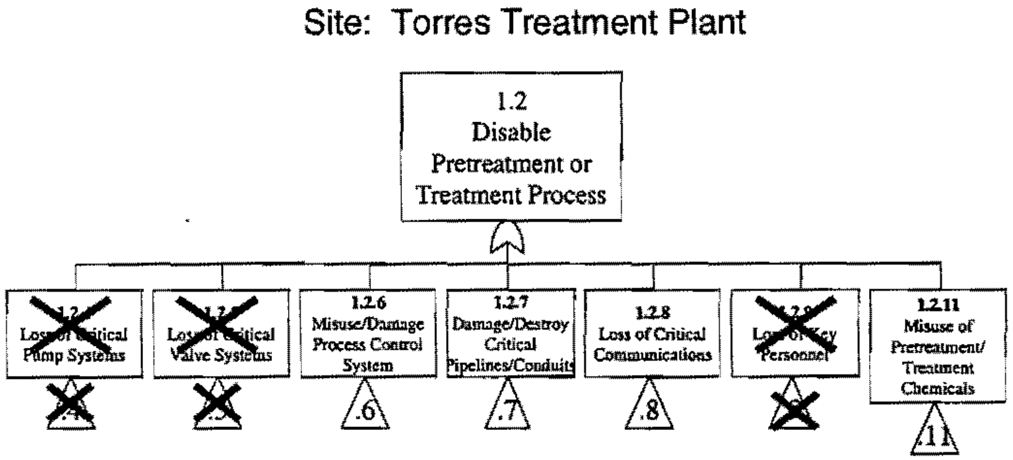
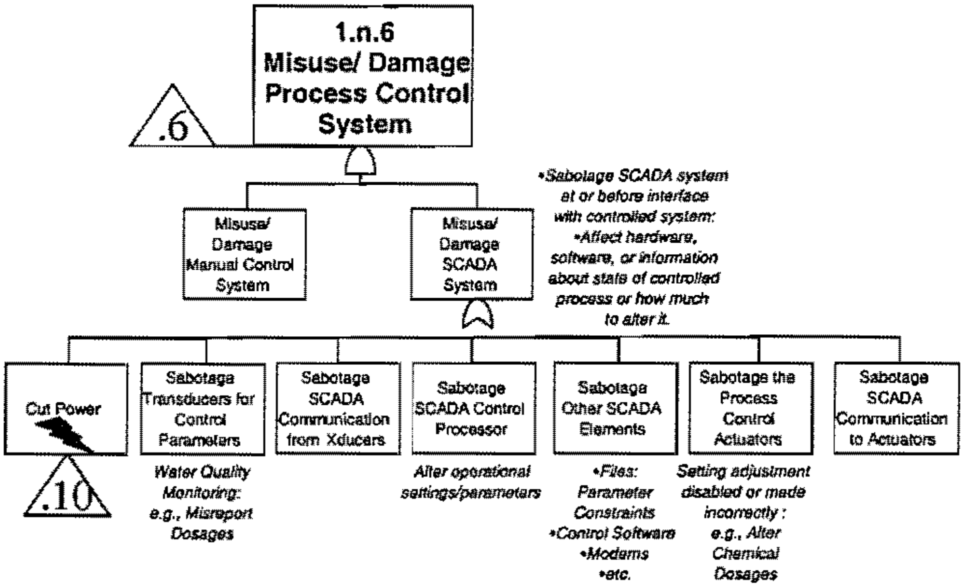


Figure 3b. Site-Specific Fault Tree Element for "Disable Pretreament or Treatment Process" for the Torres Treatment Plant

Notes are added onto the fault tree to indicate areas of concern and to capture important data. For example, notes on chlorine disinfection would prompt additional questions to analyze how much is stored on site at any one time and the potential impact to surrounding communities if the cylinders were to become an adversary target.

See the questionnaires in Appendix F of the methodology document.

The triangles with numbers in them note ties to sub-trees to further the analysis. Figures 3c - 3g show these sub-trees. The same process is followed to prune/graft other elements that exist/do not exist at the site.


1.n.6
Misuse/ Damage
Process Control
System
.6
Misuse/ Damage Manual Control System
Misuse/ Damage SCADA System
Cut Power
.10
Sabotage Transducers for Control Parameters
Sabotage SCADA Communication from Xducers
Sabotage SCADA Control Processor
Sabotage Other SCADA Elements
Sabotage the Process Control Actuators
Sabotage SCADA Communication to Actuators

•Sabotage SCADA system at or before interface with controlled system:
•Affect hardware, software, or information about state of controlled process or how much to alter it.

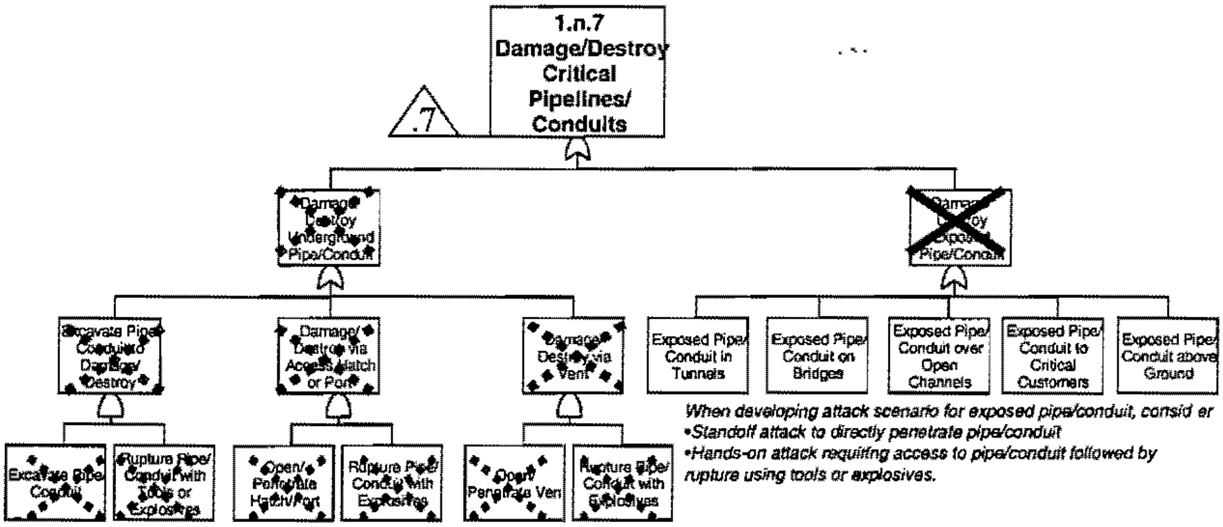
Water Quality Monitoring: e.g., Misreport Dosages

Alter operational settings/parameters

•Files: Parameter Constraints
•Control Software
•Modems
•etc.

Setting adjustment disabled or made incorrectly: e.g., Alter Chemical Dosages

Figure 3c. Site-Specific Fault Tree Element for "Misuse/Damage Process Control System" for the Torres Treatment Plant


1.n.7
Damage/Destroy
Critical
Pipelines/
Conduits
.7
Damage/ Destroy Underground Pipe/Conduit
Damage/ Destroy Exposed Pipe/Conduit
Excavate Pipe/ Conduit to Damage/ Destroy
Damage/ Destroy via Access Hatch or Port
Damage/ Destroy via Vent
Excavate Pipe/ Conduit
Rupture Pipe/ Conduit with Tools or Explosives
Open/ Penetrate Hatch/Port
Rupture Pipe/ Conduit with Explosives
Open/ Penetrate Vent
Rupture Pipe/ Conduit with Explosives
Exposed Pipe/ Conduit in Tunnels
Exposed Pipe/ Conduit on Bridges
Exposed Pipe/ Conduit over Open Channels
Exposed Pipe/ Conduit to Critical Customers
Exposed Pipe/ Conduit above Ground

When developing attack scenario for exposed pipe/conduit, consid er
•Standoff attack to directly penetrate pipe/conduit
•Hands-on attack requiring access to pipe/conduit followed by rupture using tools or explosives.

Figure 3d. Site-Specific Fault Tree Element for "Damage/Destroy Critical Pipelines/Conduits" for the Torres Treatment Plant

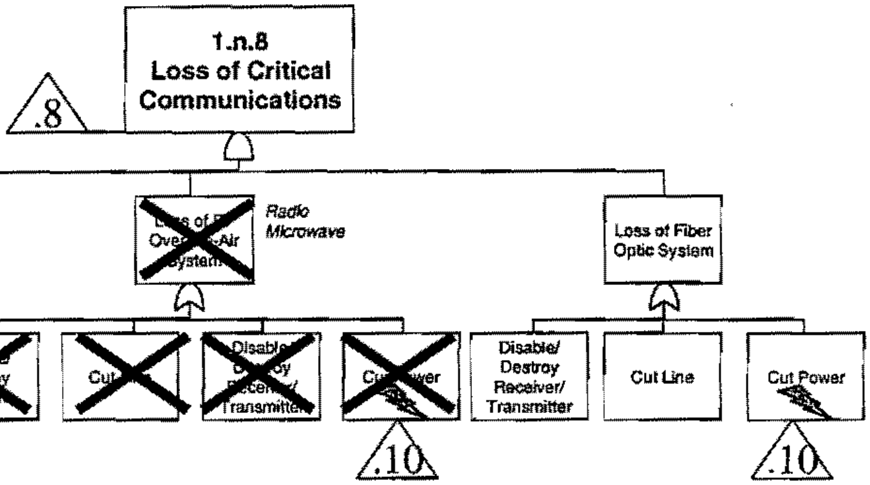


Figure 3e. Site-Specific Fault Tree Element for "Loss of Critical Communications" for the Torres Treatment Plant

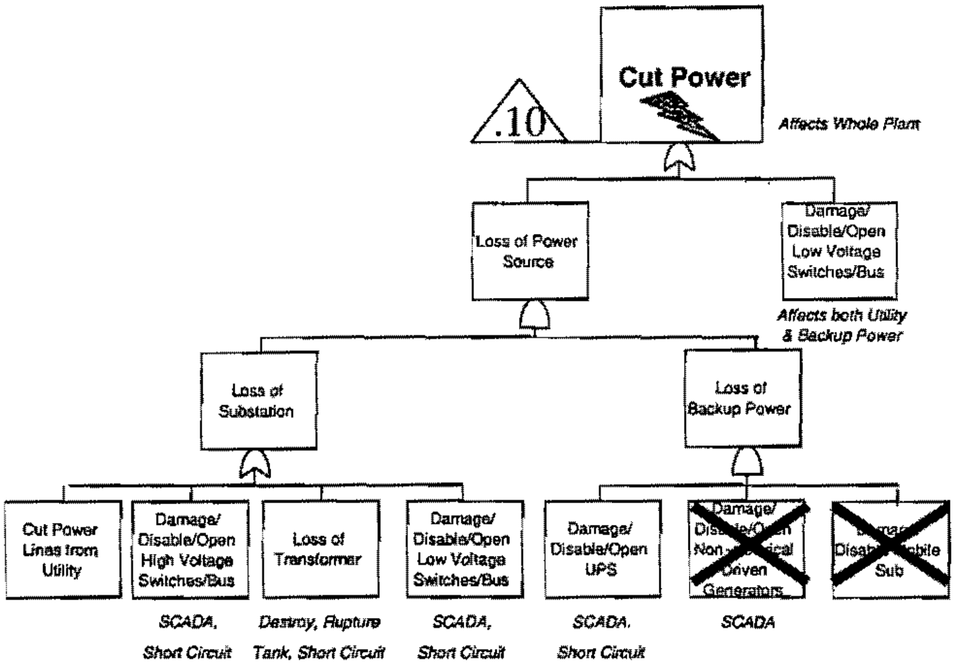

Cut Power
.10
Affects Whole Plant
Loss of Power Source
Damage/ Disable/Open Low Voltage Switches/Bus
Affects both Utility & Backup Power
Loss of Substation
Loss of Backup Power
Cut Power Lines from Utility
Damage/ Disable/Open High Voltage Switches/Bus
Loss of Transformer
Damage/ Disable/Open Low Voltage Switches/Bus
Damage/ Disable/Open UPS
Damage/ Disable/Open Non- ical Driven Generators
Damage Disable Mobile Sub
SCADA, Short Circuit
Destroy, Rupture Tank, Short Circuit
SCADA, Short Circuit
SCADA, Short Circuit
SCADA

Figure 3f. Site-Specific Fault Tree Element for "Cut Power" for the Torres Treatment Plant

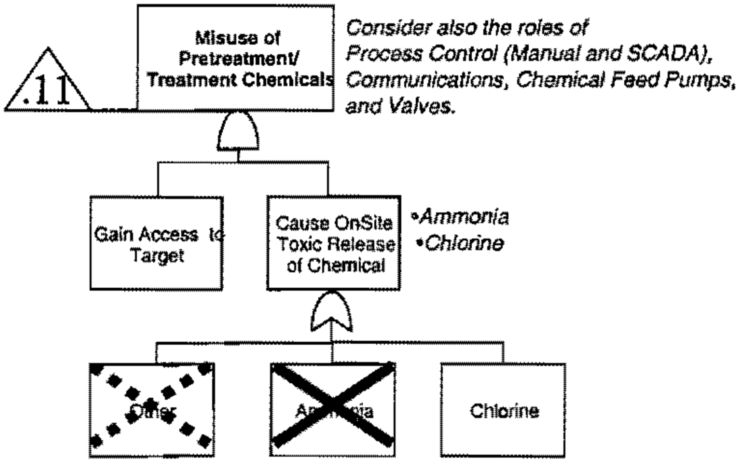

.11
Misuse of Pretreatment/ Treatment Chemicals
Consider also the roles of Process Control (Manual and SCADA), Communications, Chemical Feed Pumps, and Valves.
Gain Access to Target
Cause OnSite Toxic Release of Chemical
•Ammonia
•Chlorine
Other
Ammonia
Chlorine

Figure 3g. Site-Specific Fault Tree Element for "Misuse of Pretreatment/Treatment Chemicals" for the Torres Treatment Plant

4. CONSEQUENCE MEASURES

Table 8 has been developed for MCWD. The consequence matrix includes four columns (In the methodology document we've shown an extra column to distinguish between High and Very High consequences – either system works fine to denote WMD-type events). The first column lists the measures of consequence including economic loss, duration of loss, number of users impacted, loss of fire protection (in terms of duration), deaths, and illnesses. The remaining columns indicate the threshold levels for evaluation of the undesirable events. The measures of consequence were determined by the expert judgment of the MCWD assessment team and approved by upper management.

Table 8. MCWD Consequence Matrix

Measure of Consequence	High	Medium	Low
Human effects (sickness, death, etc.)	>5 persons	2–5 persons	<2 persons
Impact on MCWD ratepayers	>$100 million	$25–100 million	<$25 million
Impact on region's economic base	>$5 billion	$100 million to $5 billion	<$100 million
Duration of widespread loss of fire protection	>8 hours	4–8 hours	<4 hours
Duration of widespread loss of water potability	>72 hours	6–72 hours	<6 hours

4.1. Consequence Assessment

The consequence matrix, the pairwise ordering, and the site-specific fault tree identify specific assets at all the facilities and provide a means to estimate the consequence of the loss of those assets. "Assets" can be thought of synonymously as "targets" from an adversary's point of view. From this point forward in this example, the focus will be on assets. Facilities are mentioned only as a means of identifying the physical location of the assets. In some cases, the facility itself is the asset if a grouping of lower level assets is best described at the facility level. Refer to Section 5 of the methodology document.

Many of the facilities that make up MCWD support more than one of the major branches of the site-specific fault tree. Table 9 summarizes the assets at each of the facilities and also displays the results of the consequence evaluation. The table is constructed with consideration of the three top-level undesirable events from the fault tree. The undesired events from the fault tree are as follows:

- Interrupt or Impair Water Flow in the System,
- Contaminate Water,
- Weapon of Mass Destruction (WMD) Event

Each sub-table has four columns that list (1) the facility-asset-effect, (2) the high-medium-low magnitude of the consequence based on the measures defined in the consequence matrix, (3) a numerical value associated with that magnitude, and (4) brief explanatory comment(s). The numerical value in column 3 will be used later in the analysis. The items in the table were derived by summarizing the remaining undesired events found on the customized fault tree segments for each facility.

The facilities are evaluated for the undesired events that apply to their main functions. Naturally, there are commonalties between many of these facilities and the undesired events. It is important to divide the facilities and assets into the most logical subgroups to aid in making the difficult decisions necessary to carry on with the analyses. Within each of the identified facilities are numerous "assets" that allow the main functions to be performed and the mission objectives of MCWD to be completed. Finally, these assets (or the *loss* of these assets) are compared to the consequences measures listed in Table 8. Engineering judgment is used to assign values of consequence for the loss of each of the identified assets and a description of why that consequence was assigned. The justification allows for review and concurrence of these consequence values. Later, the assigned consequence values are used in the risk equation to calculate the relative risk associated with the loss of specific assets due to malevolent attack(s). It should be noted that the estimated consequences in Table 8 may change with time because of changes in the design and/or operation of the water system.

Table 9a. Consequence Table

Metrocity Water District

Consequence Table (C)

Note: There are three possible WMD-type events (noted in ***Bold Italics***) identified; (1), the breach of the Santa Inez dam with resulting damage to residences below, (2), the release of a large cloud of chlorine gas from the TTP, and (3), biological agent water contamination.

Facility: Santa Inez Asset (effect):	Consequence:	Consequence Factor:	Justification:
Dam (damage, destroy)	HI	0.9	> $100M cost, > 8 hrs loss of fire protection, > 72 hrs loss of water
Intake (damage, destroy)	LO	0.1	
Spillway (damage, destroy)	LO	0.1	
Watershed (burn)	HI	0.9	>72 hrs loss of water potability
Water (contaminate)	MED	0.5	Clean up costs

Facility: Corona Hydro Plant Asset (effect):	Consequence:	Consequence Factor:	Justification:
Structure (damage, destroy)	LO	0.1	
Corona Bypass (damage, destroy)	LO	0.1	
Plant & Bypass (damage, destroy)	MED	0.5	Repair costs
Bypass valves (damage,destroy)	LO	0.1	
Water (contaminate)	HI	0.9	> $100M cleanup cost, poss loss of fire prot, > 72 hrs loss of water, likely human effects.

Facility: McGrath Tunnel Asset (effect):	Consequence:	Consequence Factor:	Justification:
Structure (damage, destroy)	MED	0.5	$25M - $100M
Shafts (damage, destroy)	MED	0.5	$25M - $100M
Water (contaminate)	HI	0.9	Replacement costs

Facility: TTP Asset (effect):	Consequence:	Consequence Factor:	Justification:
Structure (damage, destroy)	HI	0.9	> 72 hrs loss of potability, poss loss of life
Pipes/treatment pumps (damage, destroy)	LO	0.1	
Control System (damage, destroy)	LO	0.1	
BP1 (damage, destroy)	LO	0.1	
BP2 (damage, destroy)	LO	0.1	
Water (contaminate with on-site chemicals)	LO	0.1	See analysis
Chlorine (release gas cloud)	HI	0.9	Significant human effects
Water (contaminate)	HI	0.9	> $100M cleanup cost, poss loss of fire prot, > 72 hrs loss of water, likely human effects.

Table 9b. Consequence Table

Facility: Newman Reservoir		Consequence	
Asset (effect):	Consequence:	Factor:	Justification:
Structure (damage, destroy)	HI	0.9	Flooding & repair damage costly, extended loss of water potability
Intake (damage, destroy)	MED	0.5	>72 hrs loss of water
Outlet (damage, destroy)	HI	0.9	>72 hrs loss of water
Water (contaminate)	HI	0.9	Likely human effects.

Facility: Monroe Aqueduct		Consequence	
Asset (effect):	Consequence:	Factor:	Justification:
Structure (damage, destroy)	HI	0.9	Flooding & repair damage costly, extended loss of water potability
Intake (damage, destroy)	HI	0.9	> 8 hrs loss of fire protection
Outlet (damage, destroy)	HI	0.9	> 8 hrs loss of fire protection
Water (contaminate)	HI	0.9	> $100M cleanup cost, poss loss of fire prot, > 72 hrs loss of water, likely human effects.

Facility: Valveworks		Consequence	
Asset (effect):	Consequence:	Factor:	Justification:
Structure (damage, destroy)	HI	0.9	Flooding & repair damage costly, extended loss of water potability
Manifold (damage, destroy)	HI	0.9	> 8 hrs loss of fire protection
Generic Valve (damage, destroy)	HI	0.9	> 8 hrs loss of fire protection
Water (contaminate)	HI	0.9	Likely human effects.

Facility: Control Center		Consequence	
Asset (effect):	Consequence:	Factor:	Justification:
Structure (damage, destroy)	MED	0.5	Poss loss of life
SCADA (disable, control)	HI	0.9	SCADA control can cause extensive damage (water hammer)
Security System (disable, control)	MED	0.5	Enables access for coordinated attack

Facility:Municipal Reservoirs		Consequence	
Asset (effect):	Consequence:	Factor:	Justification:
Structure (damage, destroy)	MED	0.5	Repair and collateral costs > $25M
Intake (damage, destroy)	LO	0.1	
Outlet (damage, destroy)	LO	0.1	
Valves (damage, destroy)	LO	0.1	
Disinfection equip (damage, destroy)	LO	0.1	
Water (contaminate)	HI	0.9	Likely human effects.

Facility: Pump Stations		Consequence	
Asset (effect):	Consequence:	Factor:	Justification:
Structure (damage, destroy)	MED	0.5	Repair and collateral costs > $25M
Valves (damage, destroy)	LO	0.1	
Pumps (damage, destroy)	LO	0.1	Merely lowers presssure to customers
Water (contaminate)	HI	0.9	Likely human effects.

A few important points should be recognized from the consequence values assigned to the identified assets in Table 9. First, the tables contain a fairly good distribution of LO, MED, and HI consequence values. This derives from the threshold levels assigned by MCWD to the consequence measurements table, and indicates that the levels were appropriate to achieve good resolution (or distribution) across the consequence spectrum. This should be a goal in the analysis because the vulnerability assessment must discriminate between the relative risks for the assets. Also, the HI consequence events are associated with contamination, major structure damage, and catastrophic attacks, which should be expected.

5. SYSTEM EFFECTIVENESS

This section presents an analysis of the existing system effectiveness based on the capabilities of the DBT. The outcome of this analysis is an estimate of the effectiveness, P_E, of the existing security and operational systems at each facility. Refer to Section 7 of the methodology document.

5.1. Identification of Adversary Strategies

The DBT for MCWD was previously defined to include an Insider, an Outsider(s), and a Hacker. In addition, the adversary was identified to have specific tools that would be used to attempt to accomplish the objective of defeating/damaging each of the critical assets. The DBT will be used as input to define potential strategies and adversary paths. The threats are all given the number(s), tools, or capability to potentially cause significant damage to equipment/facilities.

Presented here are potential adversary strategies, tactics, and adversary path diagrams for selected facilities and assets. This technique defines the path that the adversary will likely take to reach the asset, thereby achieving the objective of defeating at least one of the mission objectives of MCWD. Because of the relative simplicity of the existing security measures and because the structures that normally house the critical assets are not generally hardened, the paths are simplistic. They do, however, illustrate the thought process necessary to design upgrades to improve security. The optimal adversary strategy is derived from expert opinion based on team members' knowledge and the existing protection system and operational design features. Several weaknesses in the existing security system(s) are considered in judging which strategies may be the most successful:

- Least protected paths,
- Easiest system features to defeat,
- No detection,
- Very little delay, and
- Long response times.

The scenarios and paths must be consistent with the attributes and tools already defined for the adversary. Table 10 provides brief descriptions of potential adversary strategies and tactics for a range of undesired events for the facilities evaluated during the assessment. Note that the strategies/tactics given in the table are not considered exhaustive, but rather identify what to consider in defining adversary strategies and tactics. Figure 4 indicates an ASD for TTP.

Table 10. Possible Adversary Tactics

Metrocity Water District Adversary Tactics Table	Possible Adversary Tactic
Facility: Santa Inez	Damage various parts of dam Burn watershed Contaminate water
Facility: Corona Hydro Plant	Damage various parts of structure Contaminate water
Facility: McGrath Tunnel	Damage the shafts Contaminate water
Facility: TTP	Damage various parts of structure Contaminate water Contaminate water (on-site chemicals) Damage Bypasses Cause chlorine gas release
Facility: Newman Reservoir	Damage various parts of the dam Contaminate water
Facility: Monroe Aqueduct	Damage various parts of exposed tunnel at overpass Contaminate water
Facility: Valveworks	Damage valves and/or pipelines Contaminate water
Facility: Control Center	Damage various parts of structure Contaminate water Disable SCADA Disable Security System
Facility: Municipal Reservoirs	Damage various parts of containment structure Contaminate water
Facility: Pump Stations	Damage various parts of structure Contaminate water

5.2. Adversary Path and Sequence Diagrams

Illustrated below(Figures4, 5, 6) are notional diagrams associated with a scenario to breach the TTP and explode the chlorine cylinders. The rudimentary security features of the facility make these diagrams quite simplistic.

Refer to Section 7 of the methodology document.

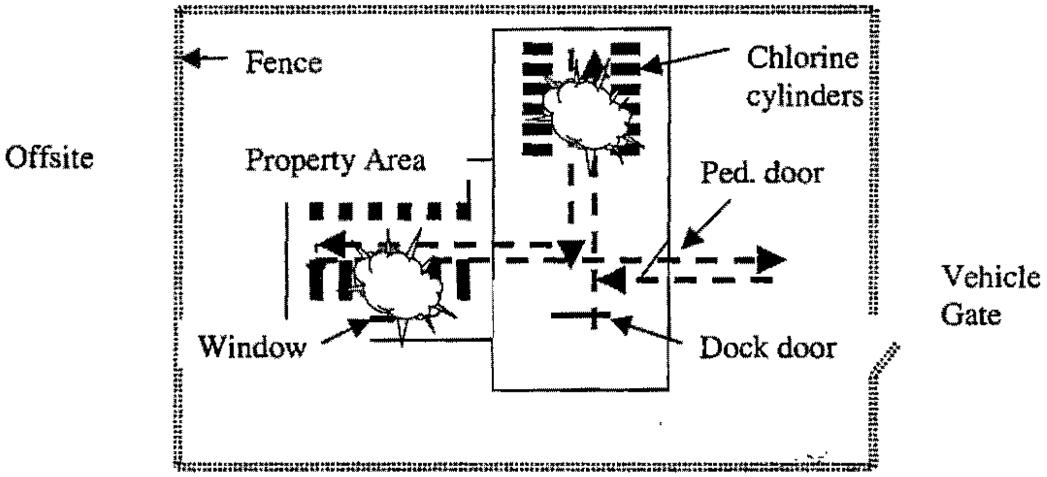


Figure 4. Adversary Path Development for the Chlorine Cylinders at the TTP

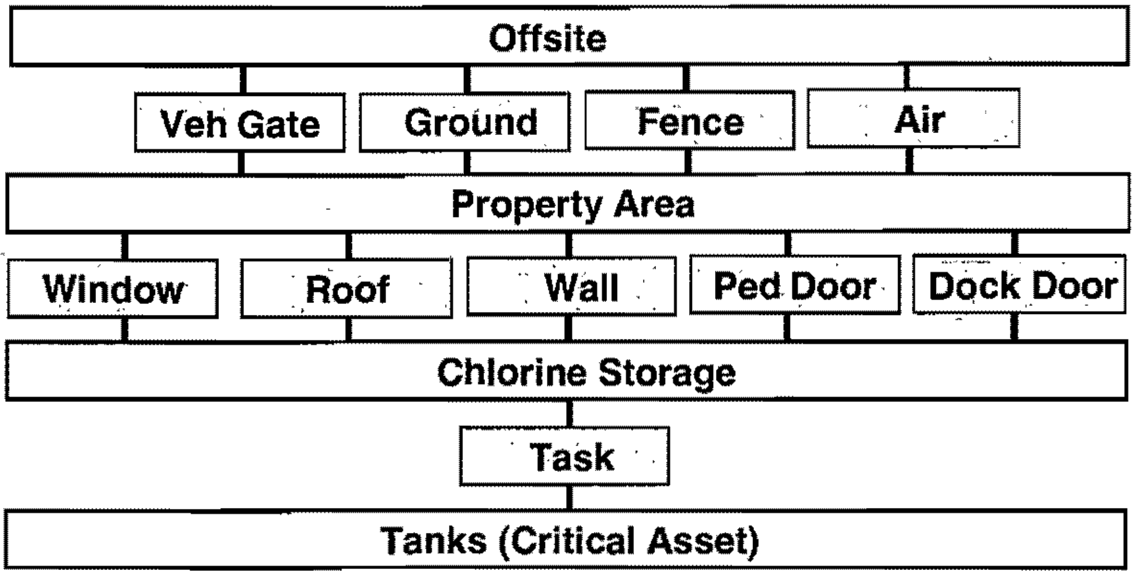


Figure 5. Adversary Sequence Diagram for the Chlorine Cylinders at the TTP

5.3. System Effectiveness Tables

In a manner similar to the assessment of consequence, the System Effectiveness also uses values of LO, MED, and HI for characterization. Table 11 indicates the results of the analysis for each element of the DBT (Outsider Medium, Insider Medium, and Hacker Medium). The table also contains a brief comment explaining the valuation. An example scenario timeline is shown in Figure 6.

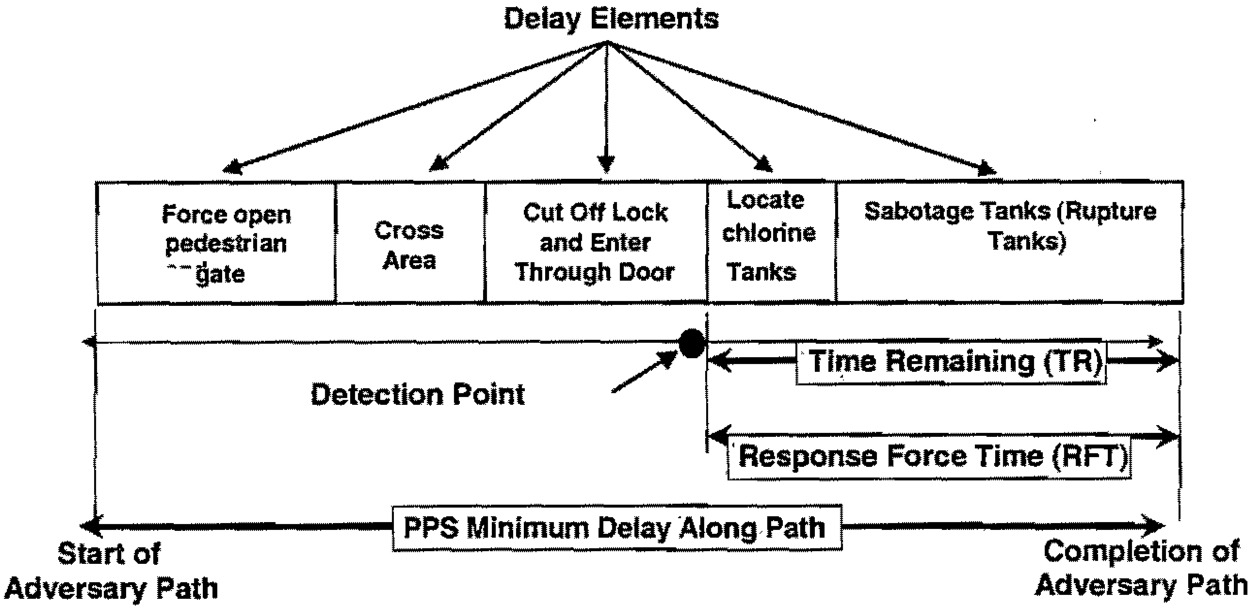

Delay Elements
Force open pedestrian gate
Cross Area
Cut Off Lock and Enter Through Door
Locate chlorine Tanks
Sabotage Tanks (Rupture Tanks)
Detection Point
Time Remaining (TR)
Response Force Time (RFT)
PPS Minimum Delay Along Path
Start of Adversary Path
Completion of Adversary Path

Figure 6. Scenario Timeline for the Chlorine Cylinders at the TTP (Insider Medium)

As an example, Figure 6 shows a notional timeline associated with the chlorine cylinder attack as mentioned above for the Insider Medium adversary [response time is approximately equal to delay (after detection) time]. Note that the Insider Medium does not have explosives; therefore, he is limited to somehow rupturing a tank or tanks. This timeline is used to evaluate the effectiveness of the existing system (i.e., determine LO, MED, HI) for each level of the DBT for this particular event. Such a timeline diagram may be necessary for each critical asset and each level of adversary. Refer to Section 7 of the methodology document.

Table 11a. System Effectiveness Against Threats

Metrocity Water District **Effectiveness Table (P_E)**							Note: This table includes the combined effectiveness of the Physical Protection System (PPS), and the System Design Effectiveness or asset "Robustness".		
Facility: Santa Inez	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Dam (damage, destroy)	HI	0.9	HI	0.9	HI	0.9	Explosive quantity insufficient	Insufficient tools/equipment	No access
Intake (damage, destroy)	MED	0.5	HI	0.9	HI	0.9	Difficult access	Insufficient tools/equipment	No access
Spillway (damage, destroy)	MED	0.5	HI	0.9	HI	0.9	Difficult to damage	Insufficient tools/equipment	No access
Watershed (burn)	LO	0.1	LO	0.1	HI	0.9	Poor PPS	Poor PPS	No access
Water (contaminate)	HI	0.9	HI	0.9	HI	0.9	Large dilution factor	Insufficient tools/equipment	No access
Facility: Corona Hydro Plant	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Structure (damage, destroy)	LO	0.1	HI	0.9	HI	0.9	Explosives effective	Insufficient tools/equipment	No access
Corona Bypass (damage, destroy)	LO	0.1	MED	0.5	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Plant & Bypass (damage, destroy)	MED	0.5	HI	0.9	HI	0.9	Explosives unlikely to affect both	Unlikely to affect both	Unlikely access
Bypass valves (damage,destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Water (contaminate)	HI	0.9	HI	0.9	HI	0.9	Large dilution factor, high pressure	Insufficient tools/equipment	No access
Facility: McGrath Tunnel	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Structure (damage, destroy)	HI	0.9	HI	0.9	HI	0.9	Asset robust	Asset robust	No access
Shafts (damage, destroy)	MED	0.5	HI	0.9	HI	0.9	Explosives effective	Asset robust	No access
Water (contaminate)	HI	0.9	HI	0.9	HI	0.9	Large dilution factor	Insufficient tools/equipment	No access
Facility: TTP	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Structure (damage, destroy)	LO	0.1	HI	0.9	HI	0.9	Explosives effective	Insufficient tools/equipment	No access
Pipes/treatment pumps (damage, destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	Manipulation of controls	No access
Control System (damage, destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	Manipulation of controls	No access
BP1 (damage, destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	Manipulation of controls	Unlikely access
BP2 (damage, destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	Manipulation of controls	Unlikely access
Water (contaminate with on-site chemicals)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	Manipulation of controls	No access
Chlorine (release gas cloud)	LO	0.1	MED	0.5	HI	0.9	Poor PPS, easy access	Difficult but possible for determined adversary	No access
Water (contaminate)	HI	0.9	HI	0.9	HI	0.9	Large dilution factor	Insufficient tools/equipment	No access

Table 11b. System Effectiveness Against Threats

Facility: Newman Reservoir	Outsider Med		Insider Med		Hacker Med		Justification:		
Asset (effect):	Rank	Factor	Rank	Factor	Rank	Factor	Outsider Medium	Insider Medium	Hacker Medium
Structure (damage, destroy)	HI	0.9	HI	0.9	HI	0.9	Explosive quantity insufficient	Insufficient tools/equipment	No access
Intake (damage, destroy)	MED	0.5	HI	0.9	HI	0.9	Difficult access	Insufficient tools/equipment	No access
Outlet (damage, destroy)	MED	0.5	HI	0.9	HI	0.9	Difficult to damage	Insufficient tools/equipment	No access
Water (contaminate)	HI	0.9	HI	0.9	HI	0.9	Large dilution factor	Insufficient tools/equipment	No access
Facility: Monroe Aqueduct	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Structure (damage, destroy)	LO	0.1	HI	0.9	HI	0.9	Explosives effective	Asset robust	No access
Intake (damage, destroy)	MED	0.5	HI	0.9	HI	0.9	Explosives effective	Asset robust	No access
Outlet (damage, destroy)	MED	0.5	HI	0.9	HI	0.9	Explosives effective	Asset robust	No access
Water (contaminate)	MED	0.5	HI	0.9	HI	0.9	Moderate dilution factor, high pressure	Insufficient tools/equipment	No access
Facility: Valveworks	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Structure (damage, destroy)	LO	0.1	MED	0.5	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Manifold (damage, destroy)	LO	0.1	MED	0.5	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Generic Valve (damage, destroy)	LO	0.1	MED	0.5	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Water (contaminate)	HI	0.9	HI	0.9	HI	0.9	Large dilution factor, high pressure	Insufficient tools/equipment	No access
Facility: Control Center	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Structure (damage, destroy)	LO	0.1	HI	0.9	HI	0.9	Explosives effective	Insufficient tools/equipment	No access
SCADA (disable, control)	LO	0.1	LO	0.1	MED	0.5	Poor PPS	SCADA exploitation	Possible disruption if accessed
Security System (disable, control)	LO	0.1	LO	0.1	MED	0.5	Poor PPS	Has knowledge & access	Possible disruption if accessed
Facility: Reservoirs	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Structure (damage, destroy)	LO	0.1	HI	0.9	HI	0.9	Explosives effective	Asset robust	No access
Intake (damage, destroy)	LO	0.1	HI	0.9	HI	0.9	Explosives effective	Asset robust	No access
Outlet (damage, destroy)	LO	0.1	HI	0.9	HI	0.9	Explosives effective	Asset robust	No access
Valves (damage, destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Disinfection equip (damage, destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Water (contaminate)	MED	0.5	HI	0.9	HI	0.9	Dilution factor marginal, poor PPS	Insufficient tools/equipment	No access
Facility: Pump Stations	**Outsider Med**		**Insider Med**		**Hacker Med**		**Justification:**		
Asset (effect):	**Rank**	**Factor**	**Rank**	**Factor**	**Rank**	**Factor**	**Outsider Medium**	**Insider Medium**	**Hacker Medium**
Structure (damage, destroy)	LO	0.1	HI	0.9	HI	0.9	Explosives effective	Asset robust	No access
Valves (damage, destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Pumps (damage, destroy)	LO	0.1	LO	0.1	HI	0.9	Explosives effective	SCADA exploitation	Unlikely access
Water (contaminate)	MED	0.5	HI	0.9	HI	0.9	Moderate dilution factor, high pressure	Insufficient tools/equipment	No access

6. RISK CALCULATION

This section presents the risk analysis. The analysis uses the estimates of the effectiveness of the existing system (P_E) and the associated consequence(C) values determined in prior sections to calculate the risk value for each undesired event for specific adversaries at each critical asset. Refer to Section 8 of the methodology document.

In Table 12, the relative risk is calculated for each of the identified assets at MCWD. The leftmost column lists the facilities and their assets. The next column to the right lists the consequence (factor) for loss of each of the assets. This consequence value is identical to the consequence defined in that section for each of the assets with High equal to 0.9, Medium equal to 0.5, and Low equal to 0.1. The next three columns represent the current security system "ineffectiveness" (that is 1 minus the system effectiveness). The range of threat described by the DBT is included in this part of the table. Finally, the relative risk of the *loss* of each asset is calculated for the range of threat listed. The right portion of the table is also shaded to highlight those relative risk values that are high (.81) compared to the remainder of the water system. Careful examination of the table can be insightful. For example, it is interesting to note that in a few cases, the same corrective actions can thwart more than one level of threat.

Table 12a. Risk Calculation

Metrocity Water District **Risk Analysis (R)**	Note 1: The **System Ineffectiveness** is equal to (1 - P_E) Note 2: O-M = Outsider Medium, I-M = Insider Medium, H-M = Hacker Medium

Facility: Santa Inez	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Dam (damage, destroy)	0.9	0.1	0.1	0.1	0.09	0.09	0.09
Intake (damage, destroy)	0.1	0.5	0.1	0.1	0.05	0.01	0.01
Spillway (damage, destroy)	0.1	0.5	0.1	0.1	0.05	0.01	0.01
Watershed (burn)	0.9	0.9	0.9	0.1	0.81	0.81	0.09
Water (contaminate)	0.5	0.1	0.1	0.1	0.05	0.05	0.05

Facility: Corona Hydro Plant	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.1	0.9	0.1	0.1	0.09	0.01	0.01
Corona Bypass (damage, destroy)	0.1	0.9	0.5	0.1	0.09	0.05	0.01
Plant & Bypass (damage, destroy)	0.5	0.5	0.1	0.1	0.25	0.05	0.05
Bypass valves (damage,destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
Water (contaminate)	0.9	0.1	0.1	0.1	0.09	0.09	0.09

Facility: McGrath Tunnel	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.5	0.1	0.1	0.1	0.05	0.05	0.05
Shafts (damage, destroy)	0.5	0.5	0.1	0.1	0.25	0.05	0.05
Water (contaminate)	0.9	0.1	0.1	0.1	0.09	0.09	0.09

Facility: TTP	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.9	0.9	0.1	0.1	0.81	0.09	0.09
Pipes/treatment pumps (damage, destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
Control System (damage, destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
BP1 (damage, destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
BP2 (damage, destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
Water (contaminate with on-site chemicals)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
Chlorine (release gas cloud)	0.9	0.9	0.5	0.1	0.81	0.45	0.09
Water (contaminate)	0.9	0.1	0.1	0.1	0.09	0.09	0.09

Table 12b. Risk Calculation

Facility: Newman Reservoir	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.9	0.1	0.1	0.1	0.09	0.09	0.09
Intake (damage, destroy)	0.5	0.5	0.1	0.1	0.25	0.05	0.05
Outlet (damage, destroy)	0.9	0.5	0.1	0.1	0.45	0.09	0.09
Water (contaminate)	0.9	0.1	0.1	0.1	0.09	0.09	0.09

Facility: Monroe Aqueduct	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.9	0.9	0.1	0.1	0.81	0.09	0.09
Intake (damage, destroy)	0.9	0.5	0.1	0.1	0.45	0.09	0.09
Outlet (damage, destroy)	0.9	0.5	0.1	0.1	0.45	0.09	0.09
Water (contaminate)	0.9	0.5	0.1	0.1	0.45	0.09	0.09

Facility: Valveworks	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.9	0.9	0.5	0.1	0.81	0.45	0.09
Manifold (damage, destroy)	0.9	0.9	0.5	0.1	0.81	0.45	0.09
Generic Valve (damage, destroy)	0.9	0.9	0.5	0.1	0.81	0.45	0.09
Water (contaminate)	0.9	0.1	0.1	0.1	0.09	0.09	0.09

Facility: Control Center	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.5	0.9	0.1	0.1	0.45	0.05	0.05
SCADA (disable, control)	0.9	0.9	0.9	0.5	0.81	0.81	0.45
Security System (disable, control)	0.5	0.9	0.9	0.5	0.45	0.45	0.25

Facility: Municipal Reservoirs	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.5	0.9	0.1	0.1	0.45	0.05	0.05
Intake (damage, destroy)	0.1	0.9	0.1	0.1	0.09	0.01	0.01
Outlet (damage, destroy)	0.1	0.9	0.1	0.1	0.09	0.01	0.01
Valves (damage, destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
Disinfection equip (damage, destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
Water (contaminate)	0.9	0.5	0.1	0.1	0.45	0.09	0.09

Facility: Pump Stations	**Consequence**	**System Ineffectiveness**			**Relative Risk**		
Asset (effect):	**Factor**	**O-M**	**I-M**	**H-M**	**O-M**	**I-M**	**H-M**
Structure (damage, destroy)	0.5	0.9	0.1	0.1	0.45	0.05	0.05
Valves (damage, destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
Pumps (damage, destroy)	0.1	0.9	0.9	0.1	0.09	0.09	0.01
Water (contaminate)	0.9	0.5	0.1	0.1	0.45	0.09	0.09

7. RISK REDUCTION

In Table 13, suggestions are made to reduce all high risks (.81). This action reflects the management decision to pursue such a policy for risk reduction. The table is essentially a reproduction of Table 12 with the addition of three more columns to show the effect of the upgrade on risks that were previously rated a value of .81 and any collateral effects. Also included is a brief note describing the action in each case.

Assume that the PPS for the TTP was improved to allow reliable detection and assessment at an earlier stage in the adversary path. The timeline exemplified earlier now looks like Figure 7. This allows the system effectiveness to change from "MED" to "HI," thereby lowering the risk for that particular scenario. Refer to Section 9 of the methodology document.

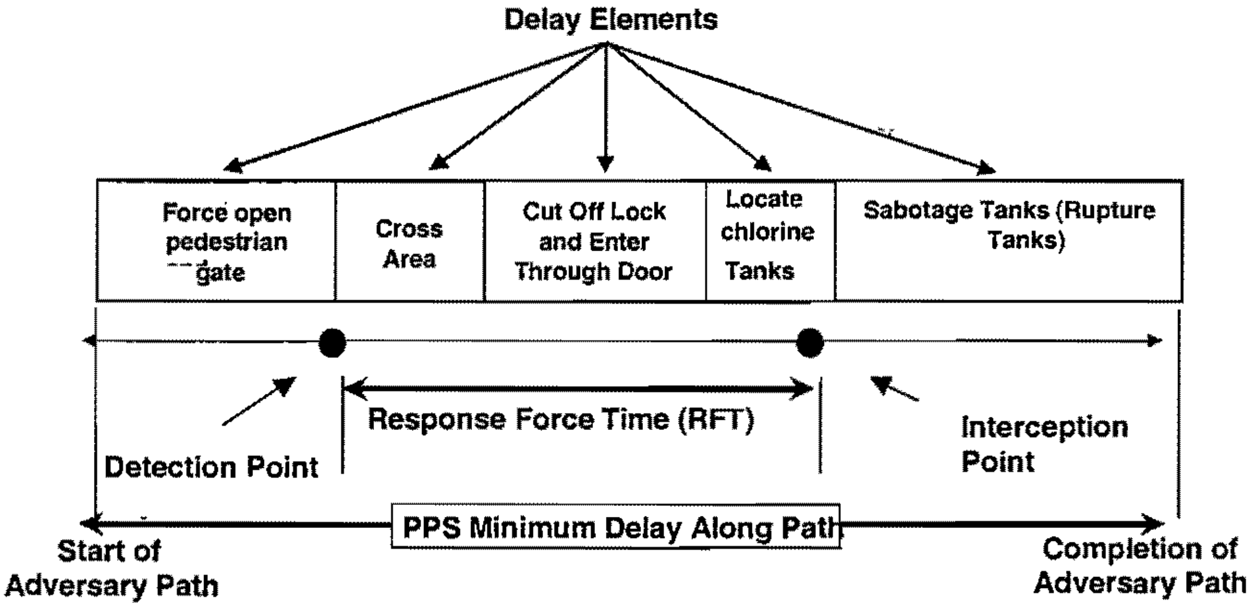

Delay Elements
Force open pedestrian gate
Cross Area
Cut Off Lock and Enter Through Door
Locate chlorine Tanks
Sabotage Tanks (Rupture Tanks)
Response Force Time (RFT)
Detection Point
Interception Point
PPS Minimum Delay Along Path
Start of Adversary Path
Completion of Adversary Path

Figure 7. Scenario Timeline for the Chlorine Cylinders at the TTP (Insider Medium) with Improvement in PPS

Table 13a. Risk Reduction Comparison for High-Risk Assets

Metrocity Water District

Risk Reduction (R_{NEW})

Note: This table contains upgraded risk values resulting from suggested actions. It reflects a risk reduction strategy of reducing the high level risks (.81) to a lower value. Only these effects and significant collateral reduction effects (at the same facility, if appropriate) are shown in the "Reduced Relative Risk" columns. A different reduction strategy would result in different values.

Facility: Santa Inez	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	Develop response policy with law enforcement. Mitigate with fire response plans & agreement with local firefighting forces. Develop plan to deal with run-off. Reduce deadwood in watershed.
Dam (damage, destroy)	0.09	0.09	0.09				
Intake (damage, destroy)	0.05	0.01	0.01				
Spillway (damage, destroy)	0.05	0.01	0.01				
Watershed (burn)	0.81	0.81	0.09	0.45	0.45		
Water (contaminate)	0.05	0.05	0.05				
Facility: Corona Hydro Plant	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	
Structure (damage, destroy)	0.09	0.01	0.01				
Corona Bypass (damage, destroy)	0.09	0.05	0.01				
Plant & Bypass (damage, destroy)	0.25	0.05	0.05				
Bypass valves (damage,destroy)	0.09	0.09	0.01				
Water (contaminate)	0.09	0.09	0.09				
Facility: McGrath Tunnel	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	
Structure (damage, destroy)	0.05	0.05	0.05				
Shafts (damage, destroy)	0.25	0.05	0.05				
Water (contaminate)	0.09	0.09	0.09				
Facility: TTP	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	**Structure:** improve PPS with sensors & immediate alarm assessment. Compartmentalize access to area. Develop response policy with law enforcement. **Chlorine:** Convert disinfection system to eliminate use of chlorine gas. See recommendations section.
Structure (damage, destroy)	0.81	0.09	0.09	0.45			
Pipes/treatment pumps (damage, destroy)	0.09	0.09	0.01				
Control System (damage, destroy)	0.09	0.09	0.01				
BP1 (damage, destroy)	0.09	0.09	0.01				
BP2 (damage, destroy)	0.09	0.09	0.01				
Water (contaminate with on-site chemicals)	0.09	0.09	0.01				
Chlorine (release gas cloud)	0.81	0.45	0.09	N/A	N/A		
Water (contaminate)	0.09	0.09	0.09				

Table 13b. Risk Reduction Comparison for High-Risk Assets

Facility: Newman Reservoir	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	
Structure (damage, destroy)	0.09	0.09	0.09				
Intake (damage, destroy)	0.25	0.05	0.05				
Outlet (damage, destroy)	0.45	0.09	0.09				
Water (contaminate)	0.09	0.09	0.09				

Facility: Monroe Aqueduct	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	
Structure (damage, destroy)	0.81	0.09	0.09				
Intake (damage, destroy)	0.45	0.09	0.09				
Outlet (damage, destroy)	0.45	0.09	0.09				
Water (contaminate)	0.45	0.09	0.09				

Facility: Valveworks	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	Improve PPS with sensors & immediate alarm assessment. Compartmentalize access to area. Develop response policy with law enforcement. Mitigate C by developing evacuation procedures for local neighborhoods. Install bypass P/L's
Structure (damage, destroy)	0.81	0.45	0.09	0.45	0.25		
Manifold (damage, destroy)	0.81	0.45	0.09	0.45	0.25		
Generic Valve (damage, destroy)	0.81	0.45	0.09	0.45	0.25		
Water (contaminate)	0.09	0.09	0.09				

Facility: Control Center	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	Improve PPS with sensors & immediate alarm assessment. Compartmentalize access to area. Develop rapid response policy with law enforcement. Require background checks on personnel, Implement 2-person control policies.
Structure (damage, destroy)	0.45	0.05	0.05	0.25			
SCADA (disable, control)	0.81	0.81	0.45	0.45	0.45		
Security System (disable, control)	0.45	0.45	0.25	0.25	0.25		

Facility: Municipal Reservoirs	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	
Structure (damage, destroy)	0.45	0.05	0.05	0.25			
Intake (damage, destroy)	0.09	0.01	0.01				
Outlet (damage, destroy)	0.09	0.01	0.01				
Valves (damage, destroy)	0.09	0.09	0.01				
Disinfection equip (damage, destroy)	0.09	0.09	0.01				
Water (contaminate)	0.45	0.09	0.09	0.25			

Facility: Pump Stations	Relative Risk			Reduced Relative Risk			Comments
Asset (effect):	O-M	I-M	H-M	O-M	I-M	H-M	
Structure (damage, destroy)	0.45	0.05	0.05				
Valves (damage, destroy)	0.09	0.09	0.01				
Pumps (damage, destroy)	0.09	0.09	0.01				
Water (contaminate)	0.45	0.09	0.09				

8. RECOMMENDATIONS

The recommendations below are hypothetically appropriate to this exercise, but are merely brief examples. An actual assessment would contain many more specifics.

8.1. General Recommendations

There are a number of good practices under way at MCWD. Unusual occurrences are being captured and reviewed, but several questions arise concerning how the information is being recorded. Do the instructions for completing the forms on an unusual occurrence specifically ask the person completing the report to look for malevolent or intentional acts that may have caused the condition? It is highly recommended that this log be expanded to include potential malevolent activities. Are all employees trained on the use of the Unusual Occurrence log?

Having a Security Incidents Log is another good business practice. It is recommended that all employees be trained on the use of this log and that summaries of incidents be produced for trend analysis. Employ uniform descriptions for the security incidents to assist in the analysis.

The Alarms Log indicated an unusual number of alarms for the short period reviewed during the assessment. Notes on the follow-up for every alarm should be captured in the log. This information can then be used for maintenance, system performance, and trend data.

A security system testing program has to be developed to exercise all components of the system to ensure proper operation. Performance testing has to be instituted at the level of the DBT to build confidence that the system will work as designed.

While not tied to a specific adversary, there are several good business practices that could be undertaken by MCWD to lower risks from lower level adversaries. Factors to consider for improvement include the following:

- Developing/upgrading security policies and procedures.
- Developing a training program to provide security training for employees including refresher courses and test-out provisions (tests to assure understanding).
- Developing and enforcing more stringent badge policies.
- Conducting "Table-Top" exercises regularly (such as conducted during Y2K and following 9/11) on malevolent events and emergency response.
- Continuing to develop/exercise memorandums of understanding with other governmental agencies (cooperation and education with law enforcement agencies has been excellent).
- Performing background checks on key employees and key contractor employees.
- Developing testing procedures for how to respond to all security alarms.
- Enforcing employee separation policies.
- Following up and writing a disposition on all security alarms.
- Compartmentalizing facilities—providing access on "as-needed" basis.
- Creating and enforcing a key control policy.
- Training all employees on the use of the Unusual Occurrence Log and insisting that it be completed.
- Controlling the access of all visitors, contractors, and vendors.
- Creating and enforcing a vehicle control policy.
- Maintaining a supply of critical replacement parts.
- Developing a robust security system testing program.
- Reviewing, updating, and/or eliminating policies and procedures annually.

8.2. Toxic/Biological Contaminants General Recommendations

Monitoring for contamination events is a concern for MCWD, from the perspective of impacting the drinking water as well as potentially contaminating a facility. Instrumentation in use to measure pH, chlorine residual, total organic carbon, conductivity, and other parameters may also be employed to detect impacts on water quality from malevolent acts. MCWD may want to consider installing some of this available instrumentation in critical locations in the distribution system and monitoring the data in real time. It is important to know the range of these measurements outside a contamination event in order to identify significant state changes in the system. Policies, procedures, and emergency response plans will also be required to effectively deploy real-time monitoring instrumentation. Knowing what to do and how to do it in an emergency will be critical to successfully defeating an event. Changes to the system may also be required to allow a quick response and the ability to isolate sections when contamination is indicated.

8.3. WMD-Type Event Recommendations

Although the MCWD management team considers the most important mission objective to be the provision of adequate water volume for firefighting, several WMD-type events should be addressed that potentially have a large impact on public safety. The potential WMD-type events were indicated in bold italics in the tables and include the following:

- Breach of the Santa Inez Dam
- Water contamination by a biological agent
- Release of chlorine gas from TTP

For the DBT adopted by MWD, the breach of the dam is not considered a viable risk as indicated in the tables. However, a revision of the DBT would change this - possibly to a matter of grave concern. The most significant public safety risk concerns the chlorine at TTP. The obvious remedy for this is to modify the treatment process and eliminate the gaseous chlorine altogether. This is a costly approach, but very effective and also reduces the risk of a catastrophic accident. MCWD may choose to accept the risks associated with the chemicals and take other steps to simply mitigate the risk. It is recommend that a detailed analysis of the consequences of all ten chlorine cylinders being breached simultaneously be undertaken for MCWD to understand the full extent of the risk.

8.4. Detailed Facility/Asset Recommendations

This section contains one example of an upgraded PPS for improving system effectiveness. The assumption is made that MCWD would like to continue using gaseous chlorine as a disinfection agent due to its efficacy and lower operating costs. The DBT for MCWD has up to three adversaries with the capability to attack with explosives and weapons.

MCWD would like to defeat this adversary and significantly lower the risk to public safety of a catastrophic chlorine release. The chlorine storage facility is a concrete block building with eight personnel and three roll-up doors for access. The facility is surrounded by a chain link fence with two access gates. In general, to have an effective PPS, the following items are necessary:

- Balanced protective layer that serves as the first point of detection.
- Detection system that has a high probability of detecting intrusions at this outer protective layer.
- Additional delay elements after detection.
- Selectively hardened and alarmed vital targets inside the outer protective layer.
- Well-equipped, trained, and authorized 24/7 response force of 2 to 6 persons located at the site.

The existing facility was not built to withstand this level of threat and significant changes will be required to upgrade the PPS. The fence will need to be replaced with a much sturdier version that includes sensors to detect whether or not someone is climbing. Since adversaries can jump a sensored fence, the next item is to put a second layer of protection inside the fence. A microwave sensor field and a buried cable are included. Unless the adversary brings tools beyond their present capability, or is able to defeat the detection elements in some other way, detection probability will increase dramatically. Lights are added around the perimeter and a CCTV camera system installed to provide assessment of all alarms. Finally, a second fence is constructed with a barrier that will prevent anyone from driving through the detection perimeter and reaching the chlorine storage facility.

The next item is to increase delay. The decision is made to harden all the openings to the building and permanently seal all but a couple of the doors. Balanced magnetic switches are already installed on the doors. A new wall is designed to surround the chlorine tanks that will survive the blast from the amount of explosives available to the adversary. The access door is hardened, but will not be able to survive the explosives. To further delay the adversaries, enclosures are designed for the chlorine cylinders that will each require explosives to destroy. With these elements in place, MCWD estimates the delay time is now several minutes for the DBT. A blast consultant confirms that the amount of explosives necessary to breach the chlorine room door and each of the chlorine cylinder enclosures is beyond the amount the adversaries could carry on-site.

The final element is response. MCWD decides to take a two-pronged approach. A security guard is stationed inside the facility in a protected area. The guard will not be able to stop the adversaries, but will be able to assess the situation and delay them further. MCWD alerts local law enforcement of the situation and asks for their support. Drills are conducted and the response time is consistently less than 5 minutes. Adversary sequence diagrams are constructed on the updated PPS. It's estimated the system effectiveness has improved from low to medium.

The life-cycle costs of this upgraded PPS has to be weighed against the costs of eliminating the gaseous chlorine and a final decision reached as to the best course of action.

8.5. SCADA Recommendations

This section contains SCADA mitigations for MCWD. The critical vulnerabilities previously identified and categorized for MCWD are repeated here for reader convenience. Each vulnerability is followed by a corresponding recommendation/mitigation.

8.5.1. SCADA Policy/Procedure/Configuration Management Vulnerabilities

Vulnerability: The system has no security policy or security plan. There is very little security awareness, security implementations and administration are lax, and there exists a general lack of recognition that security is important.
Mitigation: The basic solution is to start developing these policies, procedures, and plans. Guidelines for these efforts are found in the SCADA Security Policy Framework. It is important to note that these activities, particularly the security policy development, should take place before technology solutions are incorporated into the system to avoid redoing the technology solutions that conflict with the decided security policy.

Vulnerability: SCADA personnel do not receive regular formal security training.
Mitigation: Formal security training for SCADA personnel must be done on an ongoing basis.

Vulnerability: The dial-up access into the SCADA network for the system administrators utilizes shared passwords and shared accounts. Shared accounts and passwords are weak. In addition, activity logging on remote activities becomes impractical.

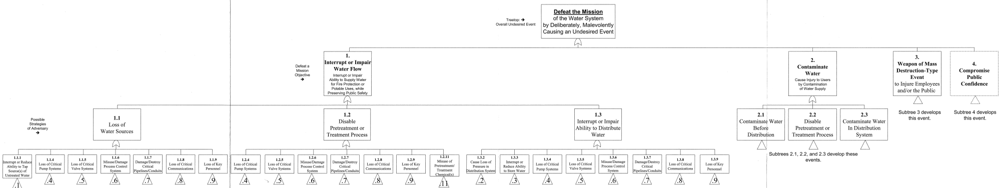
Mitigation: Create individual accounts for all personnel that login into the SCADA network remotely, including system administrators. Utilize a stronger authentication process, i.e. dial-back, Smart Cards, etc. Audit activities on the remote connection via logging, and review the audit logs as part of the security program on a regular basis.

Vulnerability: Inadequate data protection exists as the SCADA data traverses MetroCity network, both as it transferred to other SCADA segments, and as the data is sent to servers on the administrative network. This data is used for a variety of purposes, including public display and engineering efforts.

Mitigation: MCWD needs to determine the level of sensitivity associated with particular types of data (i.e.: SCADA sensor data versus control data versus historical data). Appropriate data protection methods can then applied. Technologies of data protection and separation include, encryption, strong authentication, filtering, etc.

Generic Fault Tree for Water System

FOR OFFICIAL USE ONLY
(Proprietary)


Treetop: ➔
Overall Undesired Event
Defeat the Mission
of the Water System
by Deliberately, Malevolently
Causing an Undesired Event
Defeat a Mission Objective ➔
1.
Interrupt or Impair Water Flow
Interrupt or Impair Ability to Supply Water for Fire Protection or Potable Uses, while Preserving Public Safety
2.
Contaminate Water
Cause Injury to Users by Contamination of Water Supply
3.
Weapon of Mass Destruction-Type Event
to Injure Employees and/or the Public
4.
Compromise Public Confidence
Possible Strategies of Adversary ➔
1.1
Loss of Water Sources
1.2
Disable Pretreatment or Treatment Process
1.3
Interrupt or Impair Ability to Distribute Water
2.1
Contaminate Water Before Distribution
2.2
Disable Pretreatment or Treatment Process
2.3
Contaminate Water In Distribution System
1.1.1 Interrupt or Reduce Ability to Tap Source(s) of Untreated Water
1.1.4 Loss of Critical Pump Systems
1.1.5 Loss of Critical Valve Systems
1.1.6 Misuse/Damage Process Control System
1.1.7 Damage/Destroy Critical Pipelines/Conduits
1.1.8 Loss of Critical Communications
1.1.9 Loss of Key Personnel
1.2.4 Loss of Critical Pump Systems
1.2.5 Loss of Critical Valve Systems
1.2.6 Misuse/Damage Process Control System
1.2.7 Damage/Destroy Critical Pipelines/Conduits
1.2.8 Loss of Critical Communications
1.2.9 Loss of Key Personnel
1.2.11 Misuse of Pretreatment/ Treatment Chemical(s)
1.3.2 Cause Loss of Pressure in Distribution System
1.3.3 Interrupt or Reduce Ability to Store Water
1.3.4 Loss of Critical Pump Systems
1.3.5 Loss of Critical Valve Systems
1.3.6 Misuse/Damage Process Control System
1.3.7 Damage/Destroy Critical Pipelines/Conduits
1.3.8 Loss of Critical Communications
1.3.9 Loss of Key Personnel
.1
.4
.5
.6
.7
.8
.9
.4
.5
.6
.7
.8
.9
.11
.2
.3
.4
.5
.6
.7
.8
.9

Subtrees .1, .4, .5, .6, .7, .8, and .9 develop this event.

Subtrees .4, .5, .6, .7, .8, .9, and .16 develop this event.

Subtrees .2, .3, .4, .5, .6, .7, .8, and .9 develop this event.

Subtrees 2.1, 2.2, and 2.3 develop these events.

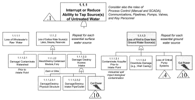
Subtree 3 develops this event.

Subtree 4 develops this event.

Generic Subtrees That Develop Event 1. "Interrupt or Impair Water Flow in the System":

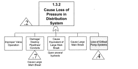
1.1.1 Interrupt or Reduce Ability to Tap Source(s) of Untreated Water

Identify Source(s): ______________________


1.1.1
Interrupt or Reduce Ability to Tap Source(s) of Untreated Water
.1
Consider also the roles of Process Control (Manual and SCADA), Communications, Pipelines, Pumps, Valves, and Key Personnel
1.1.1.1 Loss of Wholesaler's Raw Water
1.1.1.2 Loss of Surface Water Source(s): Lakes, Streams, Reservoirs
Repeat for each essential surface water source
1.1.1.3 Loss of Well to Draw from Ground Water Source(s)
Repeat for each essential ground water source
1.1.1.2.1 Damage/ Contaminate Watershed
Prior to Intake Point
1.1.1.2.2 Breach/Destroy Containment Structure, if any
Dam or Dike
1.1.1.2.3 Damage/ Destroy Access: Intake
1.1.1.2.3.1 Damage/Destroy Physical Structure
1.1.1.2.3.2 Damage/Destroy Intake Pipe/Outlet
Cut Power
.10
1.1.1.3.1 Contaminate Acquifer Prior to Intake Point
•Industrial spill •Inject biological contamination
1.1.1.3.2 Downhole Damage (e.g., Well Casing)
Loss of Critical Pump Systems
.4
Cut Power
.10

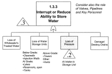
1.3.2 Cause Loss of Pressure in Distribution System

Identify Location of Pressure Loss: ______________________


1.3.2
Cause Loss of Pressure in Distribution System
.2
Improper Valve Operation
Damage/ Destroy Pipelines/ Conduits
.7
Cause Large Main Break
Cause Equivalent of Large Main Break
Open several hydrants
Cause Large Main Break
Loss of Critical Pump Systems
.4

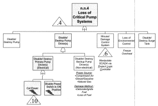
1.3.3 Interrupt or Reduce Ability to Store Water

Identify Storage Unit: ______________________


1.3.3
Interrupt or Reduce Ability to Store Water
.3
Consider also the role of Valves, Pipelines and Key Personnel
Loss of Wholesaler's Treated Water
Loss of Water Storage Units
Below Grade: •Clearwells •Injection Wells At Grade: •Lakes •Reservoirs, open •Tanks
Above Grade: •Towers Other: •Vents
Loss of Pressure
.2
At Intake to Storage Unit
Damage/ Destroy Drains

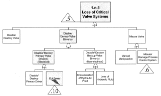
n.n.4 Loss of Critical Pump Systems

Identify Pump(s): ______________________


n.n.4
Loss of Critical Pump Systems
.4
Disable/ Destroy Pump
Disable/ Destroy Pump Driver(s)
Misuse/ Damage Control System
.6
Manipulate SCADA via Project Logic Controller
Loss of Environmental Control
Freeze Overheat
Disable/ Destroy Surge Tank
Disable/ Destroy Primary Pump Driver(s) (Electrical)
Disable/ Destroy Backup Pump Driver(s) (Non-electrical)
Power Source: •Compressed Air •Diesel/Gasoline •Natural Gas
Damage Method: •Detonate/Ignite Fuel •Loss of Fuel
Cut Power
.10
Disable Power Switch in ON Position

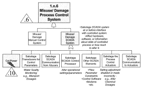
1.n.5 Loss of Critical Valve Systems

Identify Valve(s): ______________________


1.n.5
Loss of Critical Valve Systems
.5
Disable/ Destroy Valve
Disable/ Destroy Valve Driver(s)
Misuse Valve
Disable/ Destroy Primary Valve Driver(s) (Electrical)
Disable/ Destroy Backup Valve Driver(s) (Non-electrical)
Manual Manipulation
Misuse/ Damage Process Control System
.6
Disable/ Destroy Primary Driver
Cut Power
.10
Contamination of Hydraulic Fluid
Loss of Hydraulic Fluid

1.n.6 Misuse/Damage Process Control System

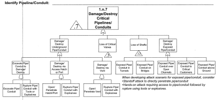
Identify Control System: ______________________


1.n.6
Misuse/ Damage Process Control System
.6
Misuse/ Damage Manual Control System
Misuse/ Damage SCADA System
•Sabotage SCADA system at or before interface with controlled system: •Affect hardware, software, or information about state of controlled process or how much to alter it.
Cut Power
.10
Sabotage Transducers for Control Parameters
Water Quality Monitoring: e.g., Misreport Dosages
Sabotage SCADA Communication from Xducers
Sabotage SCADA Control Processor
Alter operational settings/parameters
Sabotage Other SCADA Elements
•Files: Parameter Constraints •Control Software •Modems •etc.
Sabotage the Process Control Actuators
Setting adjustment disabled or made incorrectly: e.g., Alter Chemical Dosages
Sabotage SCADA Communication to Actuators

SCADA - Supervisory Control and Data Acquisition

1.n.7 Damage/Destroy Critical Pipelines/Conduits

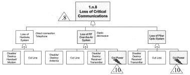
Identify Pipeline/Conduit: ______________________


1.n.7
Damage/Destroy Critical Pipelines/ Conduits
.7
Damage/ Destroy Underground Pipe/Conduit
Loss of Critical Valves
.5
Loss of Shafts
.12
Damage/ Destroy Exposed Pipe/Conduit
Excavate Pipe/ Conduit to Damage/ Destroy
Damage/ Destroy via Access Hatch or Port
Damage/ Destroy via Vent
Exposed Pipe/ Conduit in Tunnels
Exposed Pipe/ Conduit on Bridges
Exposed Pipe/ Conduit over Open Channels
Exposed Pipe/ Conduit to Critical Customers
Exposed Pipe/ Conduit above Ground
Excavate Pipe/ Conduit
Rupture Pipe/ Conduit with Tools or Explosives
Open/ Penetrate Hatch/Port
Rupture Pipe/ Conduit with Explosives
Open/ Penetrate Vent
Rupture Pipe/ Conduit with Explosives

When developing attack scenario for exposed pipe/conduit, consider
- Standoff attack to directly penetrate pipe/conduit
- Hands-on attack requiring access to pipe/conduit followed by rupture using tools or explosives.

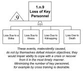
1.n.8 Loss of Critical Communications

Identify Communications System: ______________________


1.n.8
Loss of Critical Communications
.8
Loss of Hardwire System
Direct connection Telephone
Loss of RF Over-the-Air System
Radio Microwave
Loss of Fiber Optic System
Disable/ Destroy Handset/ Modem
Cut Line
Disable/ Destroy Antenna
Cut Line
Disable/ Destroy Receiver/ Transmitter
Cut Power
.10
Disable/ Destroy Receiver/ Transmitter
Cut Line
Cut Power
.10

1.n.9 Loss of Key Personnel

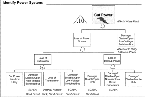
Identify Position & Location: ______________________



These events, malevolently caused, do not by themselves defeat mission objectives; they would impair ability to cope with a crisis or recover from it in the most timely manner. Minimizing the number of key personnel, for example by cross training is desirable.

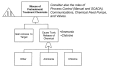
. . .10 Cut Power

Identify Power System: ______________________


Cut Power
.10
Affects Whole Plant
Loss of Power Source
Damage/ Disable/Open Low Voltage Switches/Bus
Affects both Utility & Backup Power
Loss of Substation
Loss of Backup Power
Cut Power Lines from Utility
Damage/ Disable/Open High Voltage Switches/Bus
SCADA, Short Circuit
Loss of Transformer
Destroy, Rupture Tank, Short Circuit
Damage/ Disable/Open Low Voltage Switches/Bus
SCADA, Short Circuit
Damage/ Disable/Open UPS
SCADA, Short Circuit
Damage/ Disable/Open Non-electrical Driven Generators
SCADA
Damage/ Disable Mobile Sub

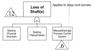
n.n.11 Misuse of Pretreatment/Treatment Chemical(s)

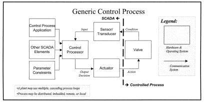
Identify Chemical, Quantity and Location: ______________________


Misuse of Pretreatment/ Treatment Chemicals
.11
Consider also the roles of Process Control (Manual and SCADA), Communications, Chemical Feed Pumps, and Valves.
Gain Access to Target
Cause Toxic Release of Chemical
•Ammonia •Chlorine
Other
Ammonia
Chlorine

n.n.12 Loss of Shaft(s)

Identify Shaft: ______________________


Loss of Shaft(s)
.12
Applies to deep rock tunnels.
Destroy Physical Structure
Destroy Piping/Valves
Misuse/Damage Process Control System
.6



- A plant may use multiple, cascading process loops
- Process may be distributed, imbedded, remote, or local

Generic Fault Tree for Water System

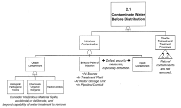
FOR OFFICIAL USE ONLY

(Proprietary)

Generic Subtrees That Develop Event 2. "Contaminate Water":

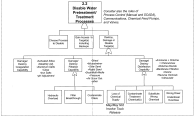
2.1 Contaminate Water Before Distribution

Site of Contamination: ______________________________


2.1
Contaminate Water Before Distribution
Introduce Contamination
Disable Pretreatment/ Treatment Processes
2.2
Natural contaminants are not removed.
Obtain Contaminant
Bring to Point of Injection
← Defeat security → measures, especially detection.
Inject Contaminant
•At Source
•In Treatment Plant
•At Water Storage Unit
•In Pipeline/Conduit
Biological Pathogens/ Toxins
Chemicals: Organic/ Inorganic
Radionuclides
Consider Hazardous Material Spills, accidental or deliberate, and beyond capability of water treatment to remove

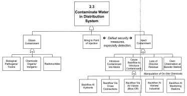
2.2 Disable Pretreatment / Treatment Processes

Identify Site of Treatment/Pretreatment: ______________________________


2.2
Disable Water Pretreatment/ Treatment Processes
Consider also the roles of Process Control (Manual and SCADA), Communications, Chemical Feed Pumps, and Valves.
Choose Process to Disable
Gain Access to Target(s) Including Backups
Destroy, Damage or Disable Target(s)
Damage/ Destroy Coagulation Capability
•Activated Silica
•Alkalinity Adj.
•Aluminum Salts
•Clays
•Iron Salts
•pH Adjustment
Damage/ Destroy Filtration Capability
•Direct
•Microstrainer
•Slow Sand
•Rapid Sand
•Dual/Multi-Media
•Pressure
•Air Scour Sys.
•other
Damage/ Destroy Disinfection Capability
•Ammonia + Chlorine = Chloramines
•Chlorine Dioxide
•Membrane Filtration
•Ozone
•Reverse Osmosis
•Ultraviolet
Hydraulic Overload
Filter Breakthrough
Contaminate Filters
Loss of Chemical Supply
May/May Not Involve Toxic Release
Contaminate Treatment Chemical(s)
Substitute Wrong Chemical
Wrong Dose: Underdose/ Overdose

2.3 Contaminate Water in Distribution System

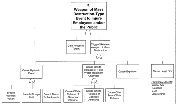
Site of Contamination: ______________________________


2.3
Contaminate Water in Distribution System
Obtain Contaminant
Bring to Point of Injection
← Defeat security → measures, especially detection.
Inject Contaminant
Biological Pathogens/ Toxins
Chemicals: Organic/ Inorganic
Radionuclides
Introduce Contaminant into Mains
Cause Backflow to Introduce Contaminants
Loss of Chlorine Residual
Over-Chlorination at Booster Station
Manipulation of On-Site Chemicals
Backflow At Hydrants
Backflow Via Cross Connections
Backflow Via Air Valves (Blow Off)
Backflow At Homes/ Industrial
Backflow At Monitoring Stations

Generic Subtrees That Develop Event 3. "Weapon of Mass Destruction-Type Event to Injure Employees and/or the Public":

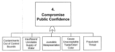
3. Weapon of Mass Destruction-Type Event to Injure Employees and/or the Public

Site of the Event: ______________________________


3.
Weapon of Mass Destruction-Type Event to Injure Employees and/or the Public
Gain Access to Target
Trigger/ Release Weapon of Mass Destruction
Cause Hydraulic Event
Cause Offsite Release of Toxic Water Treatment Chemical
Cause Explosion
Cause Large Fire
Flammable Agents:
•Diesel fuel
•Gasoline
•LOX
•Accelerants
Breach Pipelines, Valves
Breach Storage Unit
Breach Dams, Embankments
Cause Offsite Release of Gaseous Chlorine
Cause Offsite Release of Gaseous Ammonia
Cause Other Toxic Offsite Release

Generic Subtrees That Develop Event 4. "Compromise Public Confidence":

4. Compromise Public Confidence


4.
Compromise Public Confidence
Contaminants Out of Control Bounds
Insufficient/ Unreliable Supply of Water
Journalistic Misrepresentation
Cause Unacceptable Taste/Odor/ Color
Fraudulent Threat