SANDIA REPORT
SAND2010-1845
Unlimited Release
Printed April 2010

Methodology for Prioritizing Cyber-vulnerable Critical Infrastructure Equipment and Mitigation Strategies

Lon A. Dawson and Jennifer Stinebaugh

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: 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.

SAND2010-1845
Unlimited Release
Printed April 2010

Methodology for Prioritizing Cyber-vulnerable Critical Infrastructure Equipment and Mitigation Strategies

Lon Dawson and Jennifer Stinebaugh
Critical Infrastructure Systems
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0671

ABSTRACT

The Department of Homeland Security (DHS), National Cyber Security Division (NSCD), Control Systems Security Program (CSSP), contracted Sandia National Laboratories to develop a generic methodology for prioritizing cyber-vulnerable, critical infrastructure assets and the development of mitigation strategies for their loss or compromise. The initial project has been divided into three discrete deliverables: 1) A generic methodology report suitable to all Critical Infrastructure and Key Resource (CIKR) Sectors (this report); 2) a sector-specific report for Electrical Power Distribution; and 3) a sector-specific report for the water sector, including generation, water treatment, and wastewater systems.

Specific reports for the water and electric sectors are available from Sandia National Laboratories.

ACKNOWLEDGMENTS

Sandia Labs acknowledges the Control Systems Security Program at the Department of Homeland Security for sponsoring this program. This work would not have been possible without dedicated and expert support from:

- OPUS Consulting Group – Dennis Holstein and John Tengdin
- GHD – Doug Dailey
- Schweitzer Engineering Laboratories – Jeff Butler, Allen Risley, Ajay Sitaula and Bill Dull
- Albuquerque Bernalillo County Water Utility Authority (ABCWUA)
- The American Water Works Association (AWWA) – Kevin Morley and Alan Roberson

TABLE OF CONTENTS

Figures

Tables

1. EXECUTIVE SUMMARY

Critical Infrastructure and Key Resource (CIKR) sector systems are highly reliant on industry-specific automation systems and physical components that can have long lead-times and a small number of associated suppliers. Given these supply chain limitations, CIKR systems could be taken offline for months or years by successful cyber attacks and other catastrophic cyber failures that damage essential components. Because it is not practical to secure all CIKR systems, a risk management approach is needed to protect the systems of greatest concern (i.e., mission-critical components/systems).

However, the present state of computer security assessment is insufficient to fully account for all potential risks. Therefore, CIKR sectors continue to struggle with making informed decisions about how to mitigate the potential failure of essential control system components due to cyber attack or catastrophic natural events. DHS has taken a lead role in proactively identifying methods to measure the risk for this equipment and develop strategies to mitigate that risk.

Sandia National Laboratories (Sandia) was contracted by the Department of Homeland Security (DHS) to develop a methodology for prioritizing cyber-vulnerable, critical infrastructure assets and mitigation strategies for the loss or compromise of those assets. DHS required that the Methodology be applicable across all Critical Infrastructure and Key Resource (CIKR) sectors. This report documents the generic methodology.

During development, the methodology was applied to a pilot program that focused on two CIKR sectors – water and electrical distribution. The water system report: *Applying a Methodology for Prioritizing Cyber-Vulnerable Critical Infrastructure Equipment and Mitigation Strategies to the Water Sector* [1] and the electrical power distribution system report: *Applying a Methodology for Prioritizing Cyber-Vulnerable Critical Infrastructure Equipment and Mitigation Strategies to the Electrical Distribution Sector* [2] were prepared by Sandia.

This report explains the tasks, resources, and key individuals necessary to identify and prioritize critical sector assets that could be damaged by the failure of automated control systems. The report also scrutinizes the assets in terms of how they could be lost or compromised and the development of mitigation strategies to minimize the associated probability and/or consequences of such events.

For the process control systems of a given sector, similar sub-systems at different facilities/utilities could be attacked simultaneously, causing that which would normally be considered an isolated, low-consequence event to become a consequence of concern. Therefore, the “scalability” associated with cyber-related attacks is also considered in the report.

Cyber attacks are not as common as natural, physical threats; but, some of the methods used to prevent cyber attacks often involve well-known and easy-to-implement “cyber-hygiene;” e.g., strong passwords, appropriate access control for users, etc. Other mitigation strategies can be more involved, such as multi-factor authentication, encryption, patch management, or configuration control. By following the methodology presented in this report, a team analyzing any CIKR sector will discover both new and already-established mitigation strategies.

Finally, the methodology developed herein can provide support for a specific milestone in the DHS and American Water Works Association (AWWA) Roadmap [6] requirements (herein: "the Roadmap"). The Roadmap had several goals, including the ability of the water sector to be able to “Assess Risk.” One near-term milestone of that goal was to develop Industrial Control Systems (ICS) risk assessment tools, such as end-to-end threat-vulnerabilities-consequence analysis capability for the water sector. The methodology developed and applied here, with some adjustments and industry input, could play a key part in support of this milestone.

2. PURPOSE

This report describes the methodology, resources, and key individuals necessary to identify and prioritize in a given sector those critical assets that could be damaged by the failure of automated control systems. The report also describes techniques for understanding how those assets could be lost or compromised and the mitigation strategies necessary to minimize the associated probability and/or consequences of such events.

The report provides sector stakeholders with tools and analytical techniques that can assist them in better understanding the scope of threats to cyber-connected, sector assets and how to better manage and reduce the risks from such threats.

3. SCOPE

The scope of this report is limited only to a description of the methodology. How the methodology was applied to the water and electrical distribution sectors and the specific results for those sectors are separate reports, as referenced in the executive summary.

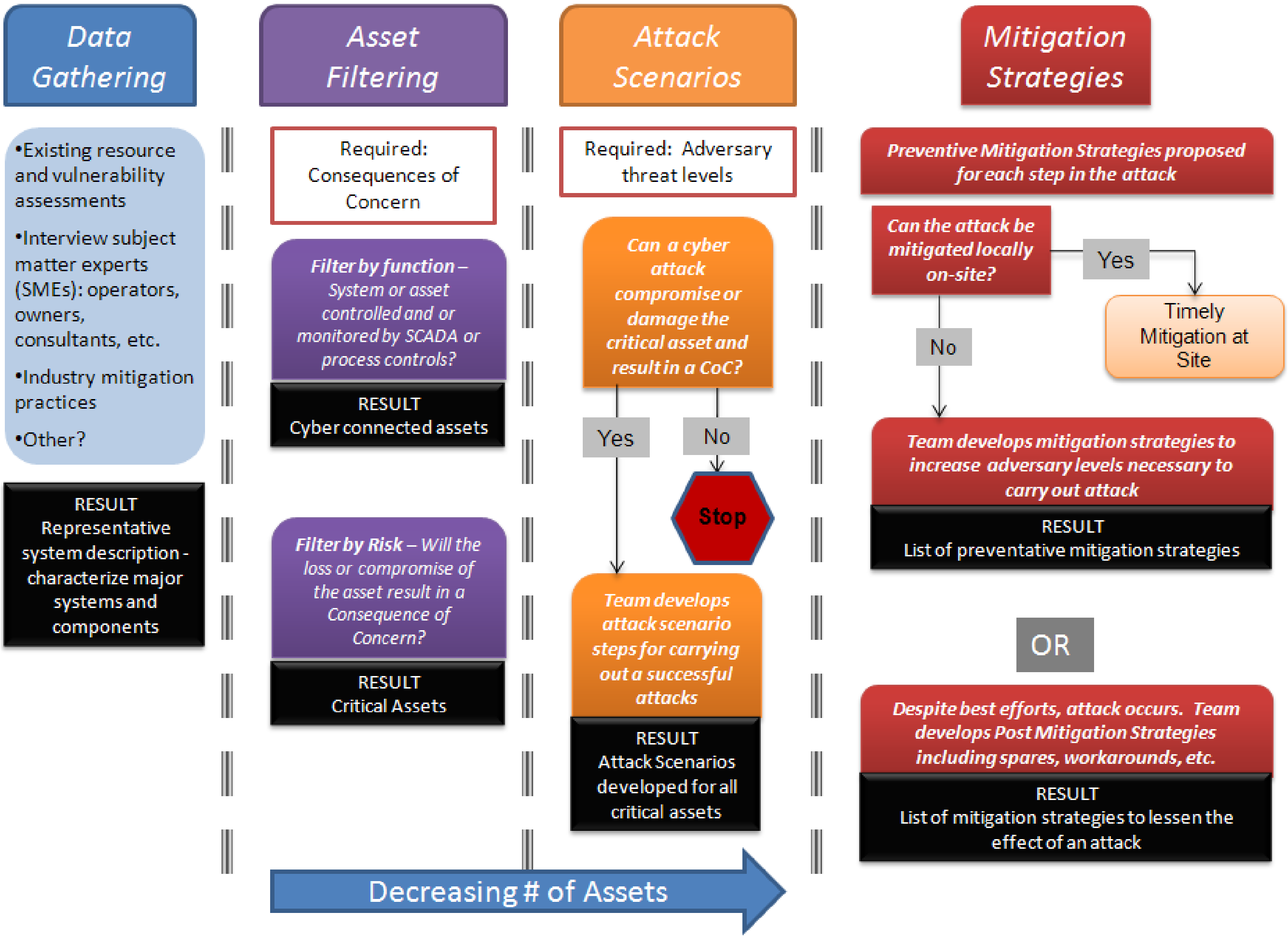
4. CRITICAL INFRASTRUCTURE AND KEY RESOURCE ASSET ASSURANCE METHODOLOGY

This section presents an overview of the methodology (Methodology) developed by Sandia to prioritize critical assets in CIKR Sectors and the development of mitigation strategies that can prevent cyber attacks from occurring and/or reduce the consequences from a successful attack. The Methodology was developed by using expertise at Sandia National Laboratories, gathering input from internal and external subject matter experts, and incorporating knowledge/experience gained from similar projects.

The Methodology is designed to be applied across any CIKR sector, with the understanding that some modifications will be necessary to conform to the needs of each industry. The process steps are broadly categorized below, as shown in Figure 1.

- Team Organization and Data Gathering,
- Development of Representative System Description,
- System review and cyber-connected asset identification,

- Consequence of Concern and Critical Asset Determination,
- Threat-level Determination and Attack Scenario Development,
- Develop Mitigations - Protective Actions and Post-consequence Strategies,
- Industry Verification and Validation, and
- Final report.



Data Gathering
Asset Filtering
Attack Scenarios
Mitigation Strategies
•Existing resource and vulnerability assessments
•Interview subject matter experts (SMEs): operators, owners, consultants, etc.
•Industry mitigation practices
•Other?
RESULT Representative system description - characterize major systems and components
Required: Consequences of Concern
Filter by function – System or asset controlled and or monitored by SCADA or process controls?
RESULT Cyber connected assets
Filter by Risk – Will the loss or compromise of the asset result in a Consequence of Concern?
RESULT Critical Assets
Required: Adversary threat levels
Can a cyber attack compromise or damage the critical asset and result in a CoC?
Yes
No
Stop
Team develops attack scenario steps for carrying out a successful attacks
RESULT Attack Scenarios developed for all critical assets
Preventive Mitigation Strategies proposed for each step in the attack
Can the attack be mitigated locally on-site?
Yes
Timely Mitigation at Site
No
Team develops mitigation strategies to increase adversary levels necessary to carry out attack
RESULT List of preventative mitigation strategies
OR
Despite best efforts, attack occurs. Team develops Post Mitigation Strategies including spares, workarounds, etc.
RESULT List of mitigation strategies to lessen the effect of an attack
Decreasing # of Assets

Figure 1. Methodology Overview

The Methodology was vetted by applying it to the distribution function of electrical power and water/wastewater treatment sectors. The results of the sector-specific applications of the methodology are available as Sandia reports [1, 2].

Each process step is defined in the following sections, and examples generated by the pilot project are provided, where applicable. Feedback on the Methodology approach was provided by the sector asset owners that participated in the pilot project.

4.1 Team Organization and Data Gathering

The Methodology developed for the DHS project is based on the assumption that resources are available to assemble the appropriate Team. Team members should include:

- Sector Subject Matter Experts (SMEs). For example: operators, engineers, consultants, industry partners, etc.,
- Cyber security and threat analysis SMEs,
- Control system and communications SMEs, and
- A Project Lead.

Industry partnerships are invaluable to the information gathering process, as they provide sector-specific information and can validate Team results throughout the process; although, in some industries, it might be difficult to develop partnerships, due to privacy and competitive concerns. Consultants are an excellent method for fostering industry partnerships and can provide excellent insight into industry operations. Assembling a proper Team ensures that much of the data required is readily available and that, where gaps exist, Team members are able to generate the required information.

For both the water and electrical projects, the Team included consultants that were sector experts with in-depth knowledge of sector assets and vendors, the functions and interactions of sector assets, typical communications protocols employed, and general control system layouts.

In many cases, reports are available that can provide much of the necessary information (e.g., existing risk and vulnerability assessments, Sector Information Sharing and Analysis Centers [ISACs], industry best practices for operations and security, and mitigation plans). To benefit from existing information, the first step in the data gathering process is to find and review existing data, and ensure that required information is readily available to the Team. Table 1 lists required data and possible information sources.

Table 1. Required Data and Potential Sources

Data or Information Required	*Possible Source*	*Comments*
List of major sector components and functions	Sector SME Sector ISAC	
Cyber controlled assets	Sector SME (control system SME) SCADA tag sets	
Security best practices	Cyber SME Industry best practice documents	
Mitigation Plans	Sector SME Existing mitigation plans	Existing risk and vulnerability assessments
Mitigation Strategies	Sector SME Existing Mitigation Strategies	Existing risk and vulnerability assessments
Potential attack vectors	Cyber SME Existing security best practices	
Validation and verification	Sector SME On-site visits	

4.2 Development of Representative System

As noted in Table 1, the first data-gathering requirement is to assemble a list of the major components in a sector and their functions. The purpose of this effort is to establish a holistic understanding of the major systems and components of the infrastructure, and determine how they interact (both physically and via cyber connections). This compilation is called the *representative system* description. The description is designed to represent a cross-section of those systems in place across the country and can include several sub-system alternatives that accomplish the same mission, but with different processes.

To develop the representative system, the Team begins with a list or drawing of the major assets in the system. To verify that this list is accurate and complete, system functions can be listed; assets that are used to carry out these functions can then be catalogued.

Another acceptable method is to determine the functions of the sector, and then determine the assets associated with each function. This process is somewhat redundant; but, it ensures that the representative system includes interdependencies. For example, when compiling the assets for water treatment, the Team intuitively listed and described the major treatment system components; but, when the *function* of water treatment was reviewed closely, the Team realized that bulk chemicals, electrical power, and transportation sector interdependencies should be included.

In order to discern the potential, integrated effects of cyber attacks on all component parts, it is necessary to develop a representative system that includes all major sector components, including those that are not cyber connected; although, the process eventually filters out non-cyber-connected assets.

Once the representative system description is developed, a system review is then performed to filter out those assets not controlled or monitored by SCADA or Process Control Systems; and the remaining assets are termed *cyber-connected assets*. In most cases, sector asset management is robust and adequately accounts for natural events and typical causes of asset loss. Accordingly, Team efforts primarily included verifying the adequacy of asset management programs for losses due to normal causes, and then focused on attack vectors with a cyber component.

4.3 Consequences of Concern and Critical Asset Determination

The maintenance of critical infrastructure and sector response to local outages is an ongoing process, and local sector experts have the capabilities for mitigating these outages quickly and efficiently. For this project, however, a filter was needed to appropriately scale the engagement to those outages and any resulting consequences that are beyond recovery by local resources.

Therefore, a set of *consequences of concern* must be developed for each sector. As part of the pilot project, a national-level focus was specified. In the future, consequences of concern should be defined by the sector stakeholders and, therefore, might have more local characteristics.

Simply stated, *consequences of concern* are those resulting from damage to a system or assets that have results so severe, so long-lasting, so geographically dispersed, or so harmful to public health that national-level action is warranted.

The consequences of concern should be developed specifically for the sector being analyzed. They should be as explicit as possible and include metrics such as percentage of population disrupted by the service outage, size of the geographical area affected, and percentage of population facing health effects or death due to the disruption.

As shown in Figure 2, these consequences of concern allowed the Team to identify “critical assets” – components that, if damaged or shut down by a cyber attack, would result in one or more consequences. Cyber-attack scenarios that could be carried out on these critical assets and result in a consequence of concern, and that could not be mitigated locally, were developed in further detail.

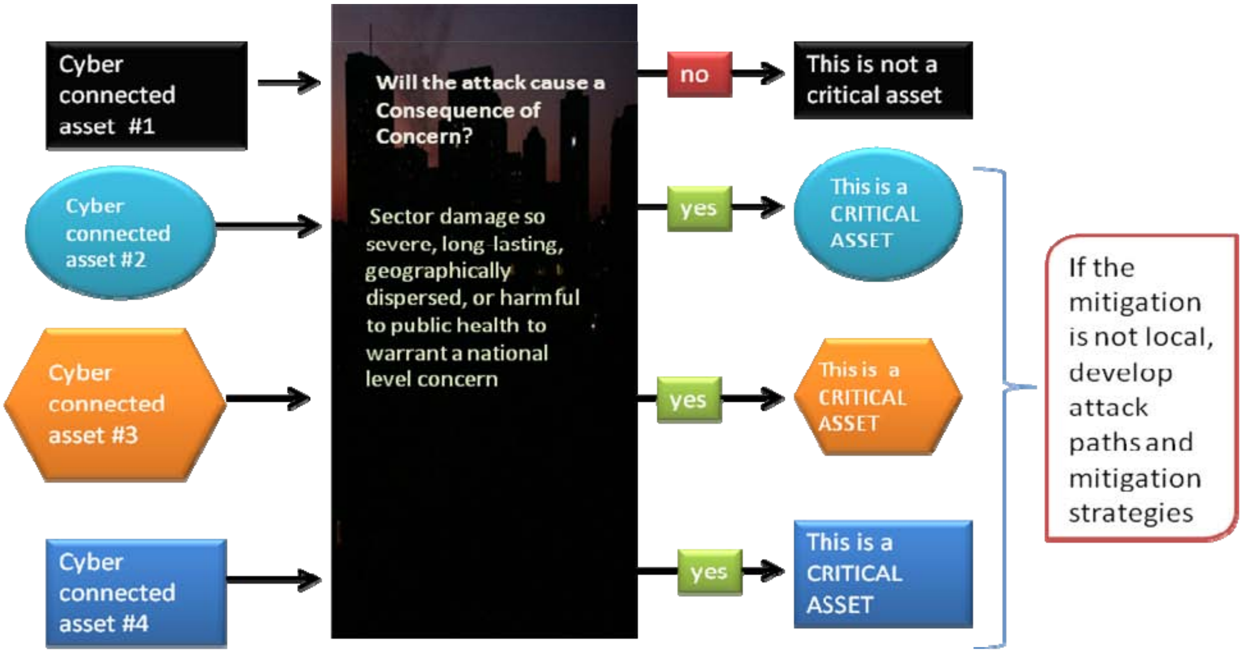

Cyber connected asset #1
Cyber connected asset #2
Cyber connected asset #3
Cyber connected asset #4
Will the attack cause a Consequence of Concern?
Sector damage so severe, long-lasting, geographically dispersed, or harmful to public health to warrant a national level concern
no
This is not a critical asset
yes
This is a CRITICAL ASSET
yes
This is a CRITICAL ASSET
yes
This is a CRITICAL ASSET
If the mitigation is not local, develop attack paths and mitigation strategies

Figure 2. Filter for Critical Assets

4.3.1 Definition of Risk

The risk to a cyber-controlled asset from a particular attack scenario is a quantification of the possibility that a particular threat will adversely affect the target by exploiting a particular vulnerability. The risk equation below can be used as a guideline for understanding and assessing risk from an overall, system-level perspective, as well as for individual assets. This equation has been used to evaluate risks to non-cyber threats imposed by natural failure modes; but, in this project, the Team was concerned chiefly with threats to cyber-controlled assets.

R = C x T x V

R = **Risk** associated with an attack that results in a system/asset failure

C = **Consequences** − the negative outcomes associated with degradation or failure of the system or assets. Consequences of an attack can be measured by metrics such as loss of life, economic impact, loss of public confidence, etc. The consequences of concern developed in this document are described below.

T = **Threats** − the probability or likelihood that a given attack scenario will occur, with the potential to disrupt systems or assets and cause undesirable consequences. Credible Threats are characterized by defined threat levels that consider adversary attributes and capabilities to carry out cyber attacks.

V = **Vulnerability** − a weakness in the system or asset, or supporting systems/assets (e.g., security systems), exploitable by the threat (T) and resulting in a successful attack.

Some consequences of failure can be quantified, such as the number of customers who lose service; but others, such as loss of public confidence, are less quantifiable (and usually expressed in qualitative terms).

Reducing risk entails managing each of the factors in the risk equation. Mitigation strategies are used to reduce “C” values. Protection strategies (e.g., enhanced cyber security) increase system effectiveness and reduce vulnerabilities. If high consequences are still considered possible, post-mitigation strategies can be employed that accelerate responses to attacks, thus reducing the impact and lessening the consequences.

4.3.2 Consequences of Concern Resulting from Cyber Attacks

Long-term sector failures can result in more than economic losses. Depending on the targeted sector, public confidence can be eroded and/or significant health problems can result. Other critical infrastructures can be affected as well. The following list of consequence types was taken from a DHS Water Sector Roadmap [6], and provides a general categorization of consequences that should be considered by all CIKR sectors:

- **Economic –** Loss of equipment in many CIKR sectors can reach millions of dollars.
- **Health and Safety –** Depending on the sector, an attack could result in harm to human health and safety.
- **Public Confidence –** A successful attack could erode public confidence in any CIKR sector.
- **Critical Infrastructure Interdependencies –** For example, loss of a water supply can affect energy, transportation, emergency services, and food and agriculture infrastructures.

When the methodology developed in this report was applied to the water sector, the Team began with reference guidance to develop the Consequences of Concern in Table 2 [3]; but also relied on expert judgment, including the advice of consultants.

Table 2. Example Consequences of Concern Developed for the Water Sector

➢ Attacks that result in any prompt fatalities or >100 related illnesses
➢ Attacks with long-term impacts (> 3 days recovery time) that can be replicated beyond one utility
➢ Attacks with economic Loss to Owner/Operator or to the Community or >$25M
➢ Attacks resulting in Psychological Impact (Public Confidence) of moderate level of fear, stress; causes regional change of lifestyle/ behavior
➢ Attacks that cause significant interruptions (>1 day of service loss per interruption) and can be easily replicated.

These consequences of concern were developed mainly to determine which cyber-connected assets are critical (the loss or compromise of the asset could result in a consequence of concern). The criteria for the consequences of concern should be developed to meet the needs and requirements of different customers in all sectors. For example, a small rural utility will have different thresholds, and possibly different metrics, than a large urban, regional, or national-level entity.

It might appear that some of these water sector example consequences do not require national-level action. However, the water Team felt that rigorous, repeated, cyber attacks replicated across many utilities could be considered so disruptive that results could prompt significant concern. The water Team did not further explore cases where mitigations could be accomplished locally or were fairly simple to implement.

4.4 Threat level Determination and Attack Scenario Development

An attack on the information technology of a sector control system exposes sector assets to security vulnerabilities and sets up many opportunities for disruption of services. Attacks are composed of a series of steps, each of which exploits a vulnerability (V) of the protection elements leading to the target of interest (i.e., critical asset) open to a particular threat (T), as defined by the risk equation in Section 4.3.1. Specific vulnerabilities depend upon the attributes and functions of the protection elements involved in protecting the critical asset.

Before examining attack steps, however, it is necessary to understand system vulnerabilities and adversary threat profiles. Following is a discussion of the development of threat profiles and generic attack scenarios against critical assets, including a description of how attack steps, adversary capabilities, and possible mitigations are proposed in sector-specific reports. How an adversary conducts an attack step is covered, as well as the type of adversary necessary to carry out that step.

4.4.1 Threat Level Determination

Adversary Threat Profile Development

Because threats are variable, difficult to quantify, and dependent upon particular vulnerabilities, one way to consider them is to create a range of credible threat profiles. This technique should be used with caution, because the understanding of threats to control and IT systems is relatively new and continually evolving. Developed threat profiles should be considered only as guidelines. They are useful for initiating discussions with industry stakeholders; but, they do not represent a formal, specific threat analysis (and they might not represent the actual threat).

Table 3 is from a Sandia report [4]. The compilation is based on case studies, informed judgment, and experience of both control and IT experts, and was deemed by the Team to be a valid guideline for use in developing threat profiles for this project. The table presents a spectrum of possible adversaries and characterizes their likely attributes of concern.

For example, the category **Stealth** represents the adversary’s willingness to be detected. The category **Intensity** represents the commitment of the adversary to physical violence - are they willing to sacrifice their lives or the lives of others? Thus, threat level 1 is the highest possible threat (e.g., terrorist) and threat level 8 is the lowest threat (e.g., novice hacker).

Table 3. Generic Adversary Definitions and Threat Levels

Threat Level	Threat Profile						
	Commitment			Resources			
	Intensity	Stealth	Time	Technical Personnel	Cyber	Kinetic	Access
1	H	H	Yrs to Decades	Hundreds	H	H	H
2	H	H	Yrs to Decades	Tens	M	H	M
3	H	H	Months to Years	Tens	H	M	M
4	M	H	Wks to Months	Tens	H	M	M
5	H	M	Wks to Months	Tens	M	M	M
6	M	M	Wks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

It should be noted that departing from the intact reference can result in a loss of understanding of the full range of credible adversaries and their capabilities, and there is also a danger in assigning names to any single level. For example, Threat Level II, in Table 4, was assigned the name "Insider Threat." However, the full spectrum of insider threat capabilities and attributes can be above or below Level II.

Table 5 assigns names and attributes to the threat levels in Table 4. The Team realized that, although there is the danger of using specific labels to define something that is variable, the benefit of the simplification and name assignment is that adversaries become more tangible to the sector experts and allow easier input into adversary recognition and capability definition.

For the electric and water sector, three levels of adversaries were encouraged by the DHS – *Garden Variety Hacker*, *Mercenary*, and *Nation State*. The fourth level – *Insider Threat* – was suggested by SME input and verified with industry contacts. Tables 4 and 5 present the four threat levels used in the project and were derived from Table 3.

Table 4. Project Adversary Threat Level Profiles

Threat Level	Threat Profile						
	Commitment			Resources			
	Intensity	Stealth	Time	Technical Personnel	Cyber	Kinetic	Access
IV	H	H	Yrs to Decades	Hundreds	H	H	H
III	M	H	Wks to Months	Tens	H	M	M
II	M	M	Months to Years	Ones	M	L	H
I	L	L	Days to Weeks	Ones	L	L	L

Table 5. Adversary Threat Levels, Names, and Attributes

ADVERSARY NAME	ATTRIBUTES
Threat Level I – “Garden Variety”	• Common hacker, script kiddies; joy hunting
Threat Level II – “Insider”	• High level of access and knowledge • Targeting known vulnerabilities • Acts alone • Target equipment and operations • Difficult to detect • Main interests in disrupting operations, causing public embarrassment
Threat Level III – “Mercenary’	• Higher level of skills • Organized crime • Targeting known vulnerabilities • Detectable but hard to attribute • Uses viruses, worms, etc
Threat Level IV – “Nation State”	• Very sophisticated, highly skilled • Backed by intelligence agencies • Well-financed • Target technology and data • Difficult to detect • Main interests are still with kinetics • Focused on cyber for data exportation

4.4.2 Attack Scenario Development

A given threat profile can be applied to vulnerabilities in individual attacks in order to obtain a sense of the capabilities required to carry out a successful attack. This can then be used to develop protection and mitigation strategies designed to make the attack step more difficult, or eliminate the ability of an attacker to implement the step.

In other words, with the new protection/mitigation strategies in place for each attack, the level of adversary required to implement the steps will be increased; therefore, both the vulnerability to attack (**V)** and threat (**T)** will be reduced, lowering the overall risk (**R**) of a successful attack being carried out, even if the consequence of concern (**C)** still exist.

4.4.3 Critical Asset Attack Scenarios

Attack scenarios can be created utilizing adversarial-based techniques involving all cyber-connected, critical assets in a sector. Those scenarios that could lead to one or more of the consequences of concern are then selected for further development, which includes listing the steps necessary to successfully carry out the attack and deriving countermeasures that could be applied to stop each attack step. These mitigation strategies reduce the risk of the attack. The scenarios should be reviewed by the entire Team, including industry experts, for input and validation.

The development of a potential attack path process begins with determining access points (e.g., internet or communication systems) to cyber-connected, critical components and includes a review of standard and emergency asset functions for determining how an asset might be shut down or compromised. It can require input from SMEs and system operators, actually performing site assessments, or researching existing plans.

For each step, a threat profile should be applied based on the capabilities required to successfully carry out that particular step. The threat level should be assessed pre- and post-mitigations. In other words, what effect does the proposed protective action have on the attack level? Figure 3 depicts the process flow for mitigation development and threat-level assignment.

The outcome of this assessment is a better understanding of how the systems are impacted, what sub-sets of components fail, how they are damaged, and the resulting impacts to the sector mission(s). An example developed by the pilot project is provided to better emphasize the process steps in the Methodology.

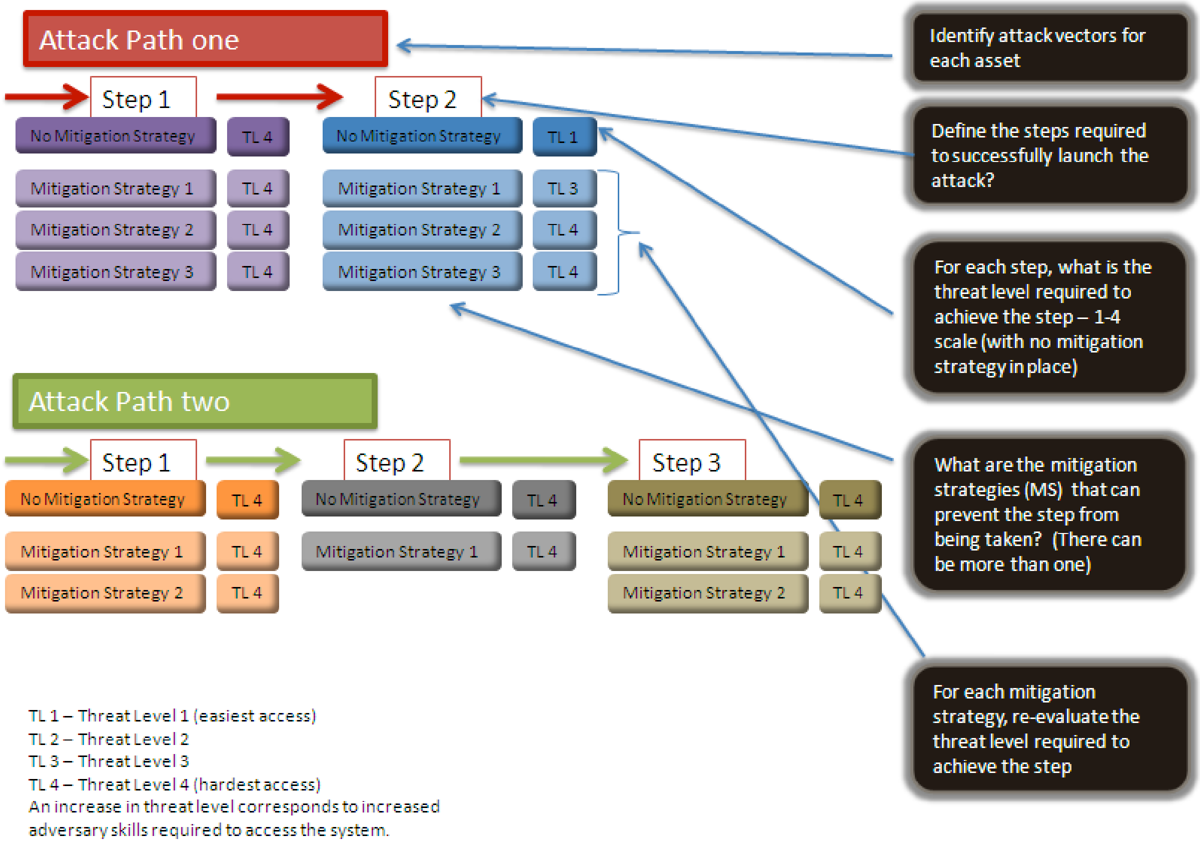

Attack Path one
Step 1
Step 2
No Mitigation Strategy
TL 4
Mitigation Strategy 1
TL 4
Mitigation Strategy 2
TL 4
Mitigation Strategy 3
TL 4
No Mitigation Strategy
TL 1
Mitigation Strategy 1
TL 3
Mitigation Strategy 2
TL 4
Mitigation Strategy 3
TL 4
Attack Path two
Step 1
Step 2
Step 3
No Mitigation Strategy
TL 4
Mitigation Strategy 1
TL 4
Mitigation Strategy 2
TL 4
No Mitigation Strategy
TL 4
Mitigation Strategy 1
TL 4
No Mitigation Strategy
TL 4
Mitigation Strategy 1
TL 4
Mitigation Strategy 2
TL 4
Identify attack vectors for each asset
Define the steps required to successfully launch the attack?
For each step, what is the threat level required to achieve the step – 1-4 scale (with no mitigation strategy in place)
What are the mitigation strategies (MS) that can prevent the step from being taken? (There can be more than one)
For each mitigation strategy, re-evaluate the threat level required to achieve the step
TL 1 – Threat Level 1 (easiest access)
TL 2 – Threat Level 2
TL 3 – Threat Level 3
TL 4 – Threat Level 4 (hardest access)
An increase in threat level corresponds to increased adversary skills required to access the system.

Figure 3. Attack Path and Mitigation Development

4.4.4 Example Attack Scenario – Electric Distribution Sector

Table 6 shows one attack example developed by the electrical Team. All asset names and specific details have been removed (Refer to sector-specific reports for actual attack details). The cyber-connected, critical asset is shown, along with a short attack description and the potential consequences. Because the potential consequence is a Consequence of Concern, the attack was developed further, and the results are summarized in Table 7.

Table 6. Distribution System Critical Asset Attack Scenarios with High Consequences

Asset	Attacks Summary	Potential Consequences
Asset Name and description	Cause distribution system event via command or input to remote controller	(Consequence of Concern #4) A > 10% load loss per interruption can be achieved (4) due to loads being disconnected unnecessarily.

4.5 Attack Steps Development

Included in Table 7 is the list of attack steps that must be carried out to execute an attack. The information is generic, to protect specific information and because there are multiple vendors, equipment types, communication media, applications, protocols, etc., that might be affected.

Threat-level profiles of adversaries necessary to carry out an attack step are listed (Tables 4 and 5), along with one or more recommended mitigations. The mitigations are designed to prevent or diminish the likelihood of the threat being carried out.

Finally, as a result of the mitigation, the “post mitigation” threat level necessary to carry out the attack is determined. For example, an attack step that might be carried out by a Threat Level I *Garden Variety* adversary, might be increased to a Threat Level II *Insider* adversary after the mitigation strategies are implemented. This would require an increase in the level of adversary required to carry out the attack, thus increasing the threshold for the attack step to be successful.

Each attack step includes an abbreviated description of recommended mitigations applicable to the step. In 2009, DHS produced a report geared primarily towards large, industrial control systems (ICS) [5]. In Table 7, the terms in italics refer to terms defined in that DHS report, which are available in the Appendix.

4.5.1 Example Attack - Description

Cyber-connected Critical Asset: name of the asset

*Assets Impacted***:** distribution system remote site devices

Consequence: cyber attacks that cause significant interruptions (>10% or worse load loss per interruption) and can be easily replicated (a consequence of concern that was developed by the electrical distribution Team).

Table 7. Example Attack Scenario

Attack Steps	**Threats (pre-mitigations)**	**Abbreviated Mitigations (Note 1)**	**Threats (post-mitigations)**
1. Reconnaissance - Determine access path to remote controller in the control center Limited by firewall, on private network, open to Internet, etc.	**Level I** May be connected to Internet or enough information maybe openly available	Protect sensitive data, such as network architecture and firewall rules *Information Disclosure*	**Level II**
2. Gain access to appropriate network	**Level II** May be Level III if communications medium is fiber...	Implement strong firewall rules *Lack of Network Segmentation* *Firewall Bypassed* *Access to Specific Ports on Host Not Restricted to Required IP Addresses*	**Level III**
		Implement strong physical protection of communications medium	**Level III**
3. Reverse engineer network data to remote controller Need to understand conditions necessary for system initiation, may include adversary monitoring network traffic waiting for a an event.	**Level I**	Data encryption of sensitive control messages *Information Disclosure*	**Level III**
4. Send well-formed data to remote controller. Repeat for multiple attacks.	**Level I**	Authenticate data in sensitive control messages *SCADA Protocol Uses Weak Authentication and/or Data Integrity Checks*	**Level III**
		Require human confirmation for System actions	**Level II**

First Attack Step

The first attack step in this scenario is ***reconnaissance***, which consists of determining the access path to the remote controller within the control center. The remote controller can be on a network that is limited by a firewall, on a private network, or even on an open network with internet connections.

If the remote controller is on an open network with internet connections, and enough information is openly available about the network architecture and/or firewall rules; or, if information is not adequately protected from theft or "dumpster diving" for discarded documents containing this critical information, then this first attack step would be simple enough for a Level I adversary.

This attack step exposes *information disclosure* vulnerabilities. If sensitive information such as network architecture and/or firewall rules is better protected (e.g. administration/passwords, logging of access, locked cabinets, etc.), a Level II adversary *Insider* who has access to this information would be required to achieve this first attack step.

Second Attack Step

The second attack step consists of ***gaining access to the appropriate network within the control center.*** Depending on the nature of the system, several vulnerabilities such as Lack of Network Segmentation, Firewall Bypassed, and Access to Specific Ports on Host Not Restricted to Required IP Addresses can be exploited.

For this step, a Level II or Level III adversary is required, depending on the type of communications media. For example, fiber-optic communications are typically more secure than other types of communications because they require, among other factors, specialized fiber equipment to access the data stream. By establishing strong firewall rules and/or strong physical protection within the communications medium, the level of adversary required to achieve this attack step could possibly move from a Level II to a Level III, because there would no longer be easy access to ports or tunnels with connections to the remote controller.

Third Attack Step

The third step is to ***reverse engineer the network data to the remote controller***. This is necessary to understand the conditions required to trigger the automatic control algorithm, and is another example of *Information Disclosure*. Some adversary levels (e.g. Level II *Insider*) might already have knowledge of this information. If such is not the case, the adversary would be required to monitor the traffic within the network and wait for an event to occur in order to determine the data signature of the event that would be used in the attack. A Level I adversary would be sufficient to achieve this attack step. However, if sensitive control messages were encrypted, at least a Level III adversary would be required.

Fourth Attack Step

The fourth step in this attack is to **s*end out well-formed data to the remote controller*** instructing it to cause the distribution system event, and to repeat the action several times. (This is an example of SCADA *Protocol Uses Weak Authentication and/or Data Integrity Checks* vulnerability). The adversary level required for this is Level I.

If human confirmation were required for all system action, the level of adversary would shift from a Level I to a Level II. By incorporating data authentication of sensitive control messages, it would be possible to shift to a Level III adversary.

The four attack steps illustrated above can be used in all sectors to create attacks based on first selecting only those scenarios that could lead to consequences of concern, and then performing the steps necessary to successfully carry out an attack. From this, mitigations for each step can be developed to reduce the risk of an attack.

Because an attack usually contains multiple steps, and there might be more than one way to mitigate each specific step, further analysis would be required to determine both the cost effectiveness and necessary policy and procedural changes required to implement the best set of mitigations.

5. MITIGATIONS — PROTECTIVE ACTIONS AND POST-CONSEQUENCE STRATEGIES

Originally, the primary focus of this project was to develop and improve regional and/or national mitigation strategies that could be implemented to reduce the impact of an event, or reconstitute the critical functions within a sector. However, as the Team considered cyber-connected components and associated vulnerabilities, the need to expand the focus of the project to include defensive or protective actions became apparent.

Unlike physical events or purely kinetic attacks, cyber attacks are relatively new and, although technically complex, might offer an adversary the option of scalability – a single attack might be easily repeated or simultaneously targeted at multiple, unprotected, cyber assets. Therefore, the Team took a more comprehensive approach and included steps to prevent cyber attacks from occurring by making access more difficult, or ensuring that unauthorized intrusions are more easily detected.

To ensure the entire system was analyzed, the Team assumed a two-pronged approach. First, protective actions were developed to prevent an attack from happening in the first place. Second, post-consequence mitigation strategies were considered for each critical asset in the event that an attacker is able to successfully penetrate the system.

5.1 Protective Actions

Protective actions combine strategies and best practices to prevent or reduce potential attacks from occurring by increasing the skill set necessary for an adversary to carry out an attack.

The process for the development of a potential attack path begins with a determination of the access points (e.g., internet or communication systems) to cyber-connected, critical components, and it includes a review of standard and emergency asset functions to determine how an asset can be shut down or compromised. Once the vulnerability assessment has been completed and attack paths determined, the developed mitigations can be added to existing risk assessment methods and security policies.

Mitigations can include both technical and organizational controls, such as preventing access to resources or control systems, use of cyber assessment tools, metrics to evaluate and assess vulnerabilities, new policies for implementing security enhancements, incident detection and response, and training for mitigation and risk assessment both for new risks and as part of an ongoing process.

Although the focus of this report is on cyber-based attacks, utilities should consider some physical security measures to protect cyber resources, including:

- Secured perimeter of buildings that house cyber-connected assets,
- Locked doors to buildings (or keypad entries),
- Security checks for people entering the plant (deliveries, contractors),
- Cameras to monitor especially critical areas such as chlorine storage and chlorinators, and
- For systems that involve dangerous chemicals, local alarms that are not connected to control systems (i.e., cannot be disabled by a cyber attack).

In 2009, DHS produced *Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments* [5], which is oriented toward large, industrial, control systems (ICS such as water and wastewater systems). That document presents a list of common vulnerabilities and recommended mitigations found in multiple systems.

The Appendix contains a table derived from this reference that provides summary descriptions and recommended mitigations for generic vulnerabilities. Team members referred to this table when determining vulnerabilities for the attack scenarios.

An analysis of the project scenarios revealed that the most common vulnerabilities found by analyzing the generic attack scenarios in both sectors included:

- Information disclosure,
- Weak passwords,
- Lack of network segmentation,
- Firewall bypassed,
- Access to specific ports on host not restricted to require IP addresses, and
- SCADA protocol uses weak authentication and/or data integrity checks.

The second, most common set of vulnerabilities found in the generic attack scenarios occurred in fewer than three instances, but is important to mention nonetheless:

- Firmware upgrades,
- Poor patch management,
- Unpatched operating system,
- Services running with unnecessary privileges, and
- Poor code quality.

Other vulnerabilities listed in the Appendix are important to consider as part of securing a control system. Although they have not been found to be primary considerations in the two sectors studied, the other vulnerabilities are commonly found and should be given consideration when implementing security measures to further mitigate risk from potential attacks.

5.2 Post-consequence Mitigation Strategies

To lessen the effect of an attack, and potentially prevent the escalation of damage that could lead to a consequence of concern, post-consequence mitigation strategies must be developed.

By developing and implementing protective actions, the barriers to attacks are strengthened; therefore, the likelihood of a successful attack is reduced. In some cases, the costs of implementing protective actions might be prohibitive; therefore, less effective measures are implemented, or no action is taken. Regardless, it is still possible that a cyber attack by a high-level adversary can be successful and potentially damage a critical asset.

As discussed previously, the first step is to consider the contingency plans in place for expected equipment failures. To the extent that the failures imposed by cyber attacks are comparable to other failure modes, the same types of emergency contingency plans and operations can be used. Where they differ, new contingencies should be added to existing plans.

A list of some immediate, post-consequence mitigation strategies might include:

- Providing the same service on a temporary basis, possibly at higher cost or with lower efficiency and/or reliability and with different equipment, until the critical piece of required equipment can be installed;
- Using available workarounds, such as running in manual mode, in lieu of taking the time to replace the loss of a critical piece of equipment, until the equipment can be replaced; or
- Working with vendors and other utilities in the region to develop specific agreements for obtaining equipment on a temporary basis, if it doesn’t exist in-house.

Longer term, post-consequence mitigation strategies can include:

- Employing redundant equipment, wherever possible,
- Maintaining a stockpile of critical spares;
- Re-engineering equipment to have greater resiliency to cyber attacks, and
- Employing outside consultants to aid in developing mitigation strategies.

6. MITIGATION PRIORITIZATION — RISK AND COST BENEFIT TRADE-OFF ANALYSIS

Each mitigation strategy yields risk reduction at some associated cost. Based on unique vulnerabilities, mitigations might be readily apparent and relatively low cost. Conversely, some mitigation strategies might be very expensive and/or difficult. Mitigation strategies must be evaluated relative to the risk reduction.

For the pilot project, mitigations fell into two basic categories – protective actions and post-consequence mitigation strategies. The control system security focus of this project resulted in protective actions that consisted primarily of implementing common cyber-security measures specific to the control systems involved. Such actions are not viewed as additional requirements; rather, they are considered as using the existing staff and systems more effectively.

A host of possible post-consequence mitigation strategies are proposed; but the scope of this project does not allow examination of a specific application. That activity is proposed for subsequent work, during which the Team proposes to partner with a specific utility.

During that phase, the next step will be to conduct analyses to improve the understanding of the risk reduction/cost relationship. Such analyses might take the form of a simplified, relative-risk analysis. Thus, the key, high-level stakeholders can evaluate the costs and benefits of mitigation options relative to other investment needs.

7. INDUSTRY VERIFICATION AND VALIDATION

In the formal Methodology, *Verification and Validation* (V&V) is the approval of the data generated during each phase of the Methodology. Industry input is essential throughout the process. In the formative stages, sector SME’s are required to build the Representative System. Throughout Critical Asset Determination and Red Teaming, industry feedback ensures that the process is thorough and that technical details are correct.

A formal, industry V&V was completed at the conclusion of the pilot project. The V&V included:

- A review of project assumptions and methodology;
- Initial findings, including cyber-connected critical components, vulnerabilities, and proposed mitigations; and
- An understanding of standard local response and recovery plans for physical and natural incidents within the sector.

8. CONCLUSIONS

To satisfy an urgent need for mitigating the risk of potential cyber attacks on CIKR systems, the duration of this project was intentionally kept very short, which limited the Team's ability to gather thorough feedback from industry on specific milestones (e.g., Consequences of Concern). The fast turnaround also prevented any opportunity for the Team to examine the specifics for any particular sectors/utilities.

Even so, when applied to the electrical distribution and water sectors, the Methodology developed and presented in this report worked extremely well for identifying the most critical, cyber-vulnerable systems and mitigating the associated risks. The Team identified several key items that should be considered when applying the methodology to other CIKR sectors.

The *representative system* description used in this report represents a cross-section of systems currently in place across the nation and was designed to be flexible enough to ensure the process is applicable to all critical systems in a sector. Breaking down that system into its physical components and then describing its functions ensured that the representative description was accurate, thorough, and characteristic of sector systems. This provided a mechanism that ensured every necessary component of the system was analyzed.

Although, initially, both the water and electrical sector Teams struggled with taking the time to develop the representative system (the natural inclination was to immediately start working on attack vectors), they realized quickly that this part of the process could not be skipped.

The attack scenario development worked best when both sector and cyber experts worked together in the same room. Input from each was necessary to think through each attack fully. Doing so caused them to identify several, potential attack scenarios that were unachievable.

Several attack scenarios considered by the group, in both water and electrical distribution, were enhanced by feedback from industry members of the Team. Industry Team members pointed out common local mitigations already in place (local security features) that made attacks more difficult or ineffective.

Physical threats, such as natural disasters or operational failures, are common in any industry, as are the strategies and operational practices designed to mitigate such situations. So it is not surprising that this methodology might identify already-established vulnerabilities and risk mitigation strategies as well as new ones.

An example of this occurred in the water sector, in which Team findings and proposed mitigations paralleled the DHS and AWWA Roadmap requirements [6]. The Roadmap had several goals, including the ability for the water sector to "Assess Risk." One near-term milestone of that goal was to develop ICS risk assessment tools, such as end-to-end threat-vulnerabilities-consequence analysis capability for the water sector. Many Team members concluded that the methodology developed and applied here, with some adjustments and industry input, could play a key role in achieving this milestone.

Cyber attacks are not as common as physical threats; but, some of the methods used to prevent them often involve well-known and easy-to-implement “cyber hygiene;” (e.g., strong passwords, appropriate access for users, etc.). Other, more involved mitigation strategies, such as double authentication, encryption, patch management and control, etc., can be applied where necessary.

If a cyber attack leads to the loss or damage of an asset, many of the mitigation strategies are similar to those for physical threats; e.g., providing the same service at higher cost or with lower efficiency and/or reliability, using available workarounds, keeping a stockpile of critical spares, or working with vendors and other utilities in the region to develop specific agreements to obtain equipment on a temporary basis, if it doesn’t exist in-house. Longer term, post-consequence, mitigation strategies can include employing redundant equipment or employing outside consultants to aid in the development of mitigation strategies.

In future studies, specific protective actions will be recommended and post-consequence mitigation strategies will be prioritized by conducting a risk reduction/cost benefit analysis.

9. RECOMMENDATIONS

To enhance the quality and depth of this proposed Methodology, it is recommended that further efforts be made to implement and improve the Methodology with respect to particular sectors and/or utilities.

The Methodology should be promoted to water and electrical sector stakeholders. By doing so, the Methodology will benefit from their expertise and more fully guarantee that the results of this project are understood and implemented correctly. By specifically applying the Methodology and involving sector stakeholders in the process, each deliverable produced by the Methodology becomes more specific and more useful.

For example, Consequences of Concern become specific to the concerns of site stakeholders, thus enhancing buy-in. To facilitate further development of attack scenarios, assets will be more carefully described. Attacks will evolve from generic, theoretical attacks to specific demonstrations on test systems. Finally, specific protective actions will be recommended by the analyzing Team; plus post-consequence mitigation strategies that will be prioritized with a risk reduction/cost benefit analysis.

Maximum benefit of the Methodology can be achieved by conducting follow-on work that leverages what has been learned in this study and applied to a review of more critical infrastructure sectors.

GLOSSARY

consequences of concern – repercussions from malicious attacks that result in sector damage so great, long-lasting, geographically disperse, or harmful to public health that loss of critical function is seen on a national level. Example: An attack on a water treatment system that results in a large metropolitan area having to import water for several weeks.

control systems – a general term, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), remote terminal units (RTU), programmable logic controllers (PLC), intelligent electronic devices (IED), and others.

critical assets – physical and software components in a sector facility that are required for the system to operate, and whose loss or compromise would result in a consequence of concern. Critical assets are determined using the asset filtering process steps.

cyber attack – any unauthorized access to computer networks and equipment with actions resulting in some form of negative consequence to the asset owners. Damage might include stolen data, exposure of private or business sensitive information, interruption of key services, a shutdown of production operations, and damage to physical equipment and the environment. From an all hazards perspective, a cyber incident occurs when a terrorist attack, other intentional act, natural disaster, or other hazard destroys, incapacitates, or exploits all or part of a control system and its networks

cyber-connected assets – physical and software components in a sector facility that are manipulated (turned on or off, turned up or down, etc.) or monitored by a control system including SCADA, DCS, PLC, etc.

(DCS) – Distributed Control System – a control architecture that supervises multiple, integrated sub-systems responsible for controlling the details of a localized process, such as water and wastewater treatment systems. The processes may be spread among several different unit processes that may be related (such as in a water treatment facility) or unrelated, as in a manufacturing plant where many different products are fabricated.

(IED) – Intelligent Electronic Device – a term used in the electric power industry to describe microprocessor-based controllers of power system equipment, such as circuit breakers, transformers, and capacitor banks.

insider threat – For the purposes of this report, an insider is either someone who works at the facility and has access to company computing equipment, or a person that gains access to the "inside" of the facility. This could be someone that enters the property as a consultant, a vendor, a delivery person, etc. It could also be someone that is allowed access to the facility's computing system, such as a vendor doing remote technical support of their computer systems.

(ISAC) – Information Sharing and Analysis Center – CIKR sector-specific centers formed to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government.

major sector components – physical and software system components that are required to keep the system running at a level so that an acceptable level of service is maintained.

protective actions – mitigation strategies that are put into place to prevent an attack from occurring, such as firewalls, physical security, strong passwords, encryption, etc.

post-consequence mitigation strategies – mitigation strategies that can lessen the effects of a successful attack, such as having the correct spares on hand, running in manual mode, etc.

(RTU) – Remote Terminal Unit – an intelligent electronic device which interfaces objects in the physical world to a distributed control system or SCADA system by transmitting data to the system or altering the state of connected objects based on feedback received from the system.

representative system – a list of all assets and functions in an infrastructure system that are critical for the infrastructure's operation. The representative system lists cyber-connected and non cyber-connected assets.

(SCADA) – Supervisory Control and Data Acquisition – highly distributed systems used to control geographically dispersed assets, where centralized data acquisition and control are critical to system operation. In the water sector, SCADA is used in water distribution and wastewater collection systems. A SCADA system gathers information, transfers the information back to a central site, carries out necessary analysis and control, and displays the information in a logical and organized fashion.

APPENDIX

Common Control System Vulnerabilities and Recommended Mitigations

Reference - DHS Control Systems Security Program. “Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments.” (2009) [6]

Vulnerability Description	**Recommended Mitigation**
Poor Code Quality SCADA code review and reverse engineering exercises indicate that SCADA software has not been designed or implemented using secure software development concepts in general.	SCADA-specific protocols should be redesigned to include strong authentication, integrity checks, and proper function calls. IT products deployed on the SCADA network should also have passed a security review. Asset owners should explicitly address the security of these products during the procurement process.
Vulnerable Web Services Many SCADA systems have recently incorporated Web applications and services to allow remote supervisory control, monitoring, or corporate SCADA data analysis. SCADA system assessments have found unauthorized directory traversal and authentication problems with SCADA Web implementations.	The file permissions on the Web server must be set to grant the least privileges necessary. The system design must be evaluated to reduce necessary file access as much as possible. Features on the Web server, such as unrestricted browsing, must be disabled; additional security of HTTP can be gained by utilizing the Secure Sockets Layer (SSL), where possible. The Web server should filter input to screen incoming filenames and exclude the “..” string. Disabling unused ports and keeping the Web server patched to current standards are good practices.
Unauthenticated Access to Web Server Web services developed for the SCADA system tend to be vulnerable to attacks that can exploit the SCADA Web server to gain unauthorized access.	SCADA applications should use well known and tested third-party Web servers to serve their Web applications. Web applications should be thoroughly tested for malformed input and other vulnerabilities that could lead to a compromise of the SCADA Web server.
Poor Network Protocol Implementations Services that employ weak authentication methods can be exploited to gain unauthorized privilege. Poorly protected credentials can be found in documentation or code, sniffed “off the wire,” cracked, or guessed.	All code should be written to validate input data. All programmers should be trained in secure coding practices, and all code should be reviewed and tested for input functions that could be susceptible to buffer overflow attacks. All input should be validated for length, and buffer size should not be determined based on an input value. Perform a code review of all SCADA applications responsible for handling network traffic. Network traffic cannot be trusted therefore, better security and sanity checks need to be implemented so fuzzing attempts will not

	cause crashes or a Denial of Service attack.
SCADA Protocol Uses Weak Authentication and/or Data Integrity Checks The integrity and timely delivery of alarms and commands are critical in a SCADA system.	The system design must implement strong authentication into SCADA communication protocols and encrypt communications, if appropriate and possible. Secure authentication and data integrity checks should be used to ensure that process commands and updates have not been altered in transit.
Firmware Updates	Physical access to the controller while the controller is disconnected from a production Ethernet network should be required for firmware updates. Ensuring that updates occur in this environment will help prevent possible exploitation and will prevent the information disclosure of the device's firmware. Authentication and data integrity checks should also be used to protect against unauthorized physical access and manipulation of firmware files.
Information Disclosure Credentials sent across the network in clear text leave the system at risk to the unauthorized use of a legitimate user's credentials. If attackers are able to capture usernames and passwords, they will be able to log onto the system with that user's privileges. Any un-encrypted information concerning the SCADA source code, topology, or devices is a potential benefit to an attacker and should be limited.	When possible, standard secure versions of protocols should be used. Ideally, when proprietary protocols are used, they should be encrypted and every message's integrity validated. In situations where encryption of messages or provision for encrypted channels is not feasible, access to the proprietary protocols and associated communications should be kept to a minimum level and, preferably, kept within the confines of a well-protected SCADA security zone. Future protocols should be designed with greater security, including encrypted messaging. If possible, immediate application of encrypted channels would be beneficial. If supported by the field devices, configure the field equipment to allow only connections from the IP addresses of the systems that are expected to connect to those devices. Although unable to prevent information leaks, this mitigation could make a successful attack more difficult. Where possible, unsecure versions of common IT services should be replaced by their secure versions. SCADA use common IT protocols for common IT functionality, such as network device management, remote logins, or file transfers. Because they are not used for real-time functionality, they can be replaced with their secure counterparts, in most cases. SSH can replace all file transfer and remote login protocols such as FTP, telnet, and rlogin with encrypted versions. Any communication can be "tunneled" through SSH. HTTP can be sent over the Secure Socket Layer (HTTPS). Share files with only the computers and accounts that require them. Restrict the read and write permissions of

	these shared files and directories to the minimum required for each user. Restrict ability to create network shares to the users that need this functionality (generally administrators). Use network segmentation and firewall rules that block access to file sharing ports (e.g., TCP Port 139 and 445 on Windows systems).
Poor Patch Management The number of publicly announced vulnerabilities has been steadily increasing over the past decade to the extent that patch management is a necessary part of maintaining a computer system. Although patching might be difficult in high-availability environments, unpatched systems are often trivial to exploit due to the ease of recognizing product version and the readiness of exploit code.	The vendor bears responsibility for incorporating the latest versions of third-party (and OS) software into the current version of the SCADA software product. The vendor should also support customers in patch testing and providing patches for their own software.
Use of Standard IT Protocol with Clear-text Authentication Clear-text authentication credentials can be captured and used by an attacker to authenticate the system.	Reduce the number of necessary services as much as possible. If necessary services are vulnerable to attack, these services should be replaced with more secure counterparts. For example, the clear-text protocols FTP, telnet, rshell, rexec, and rlogin can be replaced with SSH and secure FTP (a straightforward procedure for system access). This effort is not trivial if these services are integrated into the system functionality and might require a code rewrite, architecting secure authentication, or even re-engineering system communications.
SCADA System Uses Standard IT Protocol with Weak Encryption Some standard IT encryption protocols used in assessment systems were exploited due to encryption weaknesses.	Perform the necessary background research before choosing and properly implementing an encryption solution. Stay informed on published vulnerabilities and weaknesses of the deployed protocols and ensure patches are up-to-date.
Client-Side Enforcement of Server-Side Security Applications that authenticate users locally trust the client that is connecting to a server to perform the authentication. Because the information needed to authenticate is stored on the client side, a moderately skilled hacker can easily extract that information or modify the client to not require authentication.	Implement robust authentication by the server or component that is granting access.

Unauthorized Directory Traversal Allowed Findings were reported that directory traversal was allowed beyond intended file access. Either remotely connecting to a Web server, database, open network share or proprietary SCADA application can accomplish this task.	Ensure that share permissions for nonessential folders are removed. Whenever possible, shared folders should only allow read access. Ensure that even read-only shares are not providing critical information to public queries.
Services Running with Unnecessary Privileges Services are restricted to the user rights granted through the user account associated with them. Exploitation of any service could allow an attacker a foothold on the SCADA network with the exploited service's permissions. Privilege escalation can be accomplished by exploiting a vulnerable service running with more privileges than the attacker has currently obtained.	Running with minimum privileges is a recommended practice because it reduces the potential harm that a service can cause due to a bug, accident, or malicious exploit. The most secure service available should be used for a given functionality and then kept patched and up-to-date to help prevent exploitation.
Unpatched Operating System (OS) Unpatched operating systems open SCADA to attack through known operating system service vulnerabilities.	A timely patch management process is critical to reduce vulnerabilities. OS patches repair vulnerabilities in the OS that could allow an attacker to exploit the computer. The importance to system security of keeping OS patches up-to-date cannot be over-emphasized. However, patching SCADA machines can present unique challenges. Among the factors to consider are system functionality, security benefit, and timeliness. This process requires elements of IT, IT security, process control engineering, and senior management, and incorporates elements of an Incident Response Plan, a Disaster Recovery Plan, test bed testing, and a Configuration Management Plan. Where patching is not an option, work-arounds and defense-in-depth techniques can be used.
Improper Security Configuration A common problem found during assessments was that, even though secure authentication applications were used, installations and configurations were not correct.	Instructions for secure installation and proper configuration for each application must be followed and tested. Do not allow login information to be hard-coded into scripts and user programs or stored so that re-authentication on that computer is never required again.
Weak Passwords Poorly chosen passwords can easily be	Strong passwords must be required and deployed on networking, client, and server equipment. Passwords should

guessed by humans or computer algorithms to gain unauthorized access. The longer and more complex a password, the longer the time to or crack the password.	be implemented on SCADA components to prevent unauthorized access. A policy mandating the use of strong passwords for all cyber assets inside the electronic perimeter with a reasonable lifespan limit must be mandated and enforced. Use of common administrative passwords must be discouraged. Password policies should be developed as part of an overall SCADA security program, taking into account the capabilities of the SCADA and its personnel to handle more complex passwords. System administrators should enforce the use of strong passwords. A password strength policy should contain the following attributes: (1) minimum and maximum length (2) require mixed character sets (alpha, numeric, special, mixed case); (3) do not contain user name; (4) expiration; and (5) no password re-use. Authentication mechanisms should always require sufficiently complex passwords and require that they be periodically changed.
Information Leak through Insecure Service Configuration Information that can be used in determining system vulnerabilities can be gathered from services that have been configured to reply with debug or other information.	Any information that is not necessary to the functionality should be removed in order to lower both the overhead and the possibility of security sensitive data being sent.
Lack of Network Segmentation Minimal or no security zones allows vulnerabilities and exploitations to gain immediate full control of systems, which could cause high-level consequences.	At a minimum, the SCADA network should be separated from the corporate network by a firewall, and a DMZ should be implemented to provide the corporate network access to the required information from the SCADA network. The systems located in the DMZ are not production systems and should be treated as hostile. Exceptions between the DMZ and the SCADA networks should be kept to an absolute minimum, and exceptions from the corporate to the SCADA should be eliminated. Additional security zones can be created within these segments.
Firewall Bypassed Backdoor network access could cause direct access to SCADA for attackers to exploit and take full control of the system.	A firewall should limit access to the different LAN segments to only necessary communication. The SCADA network should be separated from the corporate network by a firewall, and a DMZ implemented to provide the corporate network access to the required information from the SCADA network. The systems located in the DMZ are

	not production systems and should be treated as hostile. Exceptions between the DMZ and the SCADA networks should be kept to an absolute minimum, and exceptions from the corporate to the SCADA should be eliminated.
Access to Specific Ports on Host Not Restricted to Required IP Addresses Improperly configured firewalls can allow direct access to SCADA systems for attackers to exploit and take full control of the system.	Firewall rules that apply to functional groups should use defined, finite groups that are restricted to required IP addresses. Firewall rules that are no longer needed should be removed as part of a change management procedure, periodic system review, or audit. Access control lists should be used to limit management access of network equipment to only those who require it.
Port Security Not Implemented on Network Equipment A malicious user who has physical access to an unsecured port on a network switch could plug into the network behind the firewall to defeat its incoming filtering protection.	Port security should be implemented to limit connectivity to hardware interfaces. Given the static nature of SCADA environments, port security can be used to ensure that MAC addresses do not change and new devices are not introduced to the network. Actions, such as limiting known MAC addresses to specific interfaces and disabling unused interfaces, should be implemented to assist in network security.

REFERENCES

1. Clem, John; Dailey, Doug; Dawson, Lon A.; Finley, Ray; Jaeger, Cal; Pollock, Robert; Schwalm, Keith; Stinebaugh, Jennifer; Torres, Teresa M. *Applying a Methodology for Prioritizing Cyber-Vulnerable Critical Infrastructure Equipment and Mitigation Strategies to the Water Sector* (Apr 2010).
2. Baca, Michael J.; Dawson, Lon A.; Munoz, Karina; Parks, Ray; Pollock, Robert; Richardson, Bryan; Stamp, Jason; Schwalm, Keith T.; Stinebaugh, Jennifer; *Applying a Methodology for Prioritizing Cyber-Vulnerable Critical Infrastructure Equipment and Mitigation Strategies to the Electrical Distribution Sector,*" Sandia National Laboratories (Apr 2010).
3. Jaeger, C. and Torres, T. *RAMCAP Compliant Risk Assessment Methodology for Water and Wastewater Utilities (RC RAM-W),* Sandia National Laboratories: SAND2007-5581 (Aug 2007).
4. Duggan, David P., et. al. *Categorizing Threat - Building and Using a Generic Threat Matrix.* Sandia National Laboratories: SAND2007-5791 (Sept 2007).
5. DHS Control Systems Security Program. *Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments* (2009).
6. Water Sector Coordinating Council Cyber Security Working Group. *Roadmap to Secure Control Systems in the Water Sector.* American Water Works Association, Department of Homeland Security (2008).

DISTRIBUTION

1 U.S. Department of Homeland Security (DHS)
Attn: Mr Sean McGurk, Director, DHS Control Systems Security Program
1110 North Glebe Road
Arlington, VA 22201

1	MS0671	Jennifer Depoy	05628
1	MS0671	Robert Pollock	05633
1	MS0672	Robert Hutchinson	08960
1	MS9151	James Costa	08950
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories