SANDIA REPORT
SAND2008-6192
Unlimited Release
Printed September 2008

Cyber and Physical Infrastructure Interdependencies

Andjelka Kelic, Drake E. Warren, and Laurence R. Phillips

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.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2008-6192
Unlimited Release
Printed September 2008

CYBER AND PHYSICAL INFRASTRUCTURE INTERDEPENDENCIES

Andjelka Kelic
Infrastructure Modeling and Analysis Department
Drake E. Warren
Infrastructure and Economic Systems Analysis Department
Laurence R. Phillips
Critical Infrastructure Systems Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-1137

ABSTRACT

The goal of the work discussed in this document is to understand the risk to the nation of cyber attacks on critical infrastructures. The large body of research results on cyber attacks against physical infrastructure vulnerabilities has not resulted in clear understanding of the cascading effects a cyber-caused disruption can have on critical national infrastructures and the ability of these affected infrastructures to deliver services. This document discusses current research and methodologies aimed at assessing the translation of a cyber-based effect into a physical disruption of infrastructure and thence into quantification of the economic consequences of the resultant disruption and damage. The document discusses the deficiencies of the existing methods in correlating cyber attacks with physical consequences. The document then outlines a research plan to correct those deficiencies. When completed, the research plan will result in a fully supported methodology to quantify the economic consequences of events that begin with cyber effects, cascade into other physical infrastructure impacts, and result in degradation of the critical infrastructure's ability to deliver services and products.

This methodology enables quantification of the risks to national critical infrastructure of cyber threats. The work addresses the electric power sector as an example of how the methodology can be applied.

This page intentionally left blank.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS, INITIALISMS, AND ABBREVIATIONS

AC	alternating current
API	application programming interface
BioDAC	Biological Decision Analysis Center
COM	component object model
CEII	Critical Energy Infrastructure Information
DHS	U.S. Department of Homeland Security
DIISA	Dynamic Infrastructure Interdependency Simulation and Analysis
DIS	distributed interactive simulation
DLL	dynamic-link library
DOE	U.S. Department of Energy
DOE-OE	U.S. Department of Energy’s Office of Electricity Delivery and Energy Reliability
EMCAS	Electricity Market Complex Adaptive System (model)
EMS	Energy Management System
FAIT	Fast Analysis and Simulation Team (FAST) Analysis Infrastructure Tool
FAST	Fast Analysis and Simulation Team
FEP	Front-end processor
FERC	Federal Energy Regulatory Commission
FSM	Finite-State-Machine
GAO	Government Accountability Office
GIS	Geographic Information System
GUI	graphical user interface
Hz	hertz
IDSim	Interoperable Distributed Simulation
IEEE	Institute of Electrical and Electronics Engineers
ISO	independent service operator
IEISS	Interdependent Energy Infrastructure Simulation System
kV	kilovolts
LDRD	laboratory-directed research and development
LMP	locational marginal prices
MTTA	mean time to (successful) attack
MTTF	mean time to failure

MTTR	mean time to recovery
MW	megawatts
MWh	megawatt-hours
N-ABLE™	NISAC Agent-Based Laboratory for Economics
NISAC	National Infrastructure Simulation and Analysis Center
NPPD	National Protection and Programs Directorate
NSTB	National SCADA Test Bed
OPTNET®	OPTNET Technologies, Inc.
PCII	Protected Critical Infrastructure Information
PCS	process control systems
RAM	risk assessment methodology
REMI	Regional Economics Models, Inc. (model)
REAcct	Regional Economic Accounting (tool)
RIMSII	Regional Input-Output Modeling System II
RTS	Reliability Test System
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
T-to-C	threat-to-consequence
VCSE	Virtual Control System Environment
WECC	Western Electric Coordinating Council
WISE	Water Infrastructure Simulation Environment
XML	extensible markup language

This page intentionally left blank.

1 INTRODUCTION

There has been a great deal of research related to cyber attacks and vulnerabilities and critical infrastructure, but there is an incomplete understanding of the cascading effects a cyber-caused disruption could have on other critical national infrastructures and the ability of the affected infrastructures to deliver services. Sandia National Laboratories (Sandia) has developed methodologies that translate a cyber-based disruption to a physical disruption of infrastructure and economic methodologies that can provide an understanding of the national-level risk from cyber attacks on critical infrastructure. This report discusses these methodologies and addresses these methods' gaps for correlating cyber attacks with physical and economic consequences in the nation's critical infrastructures. This report outlines a roadmap to fill the methodological gaps, beginning with the electric power sector and then extending to other infrastructures.

Section 1.1 provides a background about critical infrastructure control systems and discusses why infrastructure disruptions due to cyber problems can harm infrastructure and the economy. Section 1.2 describes the purpose and goals of this laboratory-directed research and development (LDRD) report. Section 1.3 introduces the cyber-attack-consequence assessment process and 1.4 outlines the organization of this report.

1.1 Background

Process control systems (PCS) are distributed mechatronic[1] information systems used in every critical infrastructure industry to monitor and control processes. The information element of nearly every PCS currently in use is networked and digital in nature. Because of this near-universal networked digital basis, the modern PCS is at risk of cyber attacks, which can degrade or prevent control system function and cause critical infrastructures to fail. Failures may jeopardize health and safety and bring economic activity to a halt.

1.1.1 Description

The two primary types of control systems are distributed control systems, which are used over a small geographic area (such as a single plant), and supervisory control and data acquisition (SCADA) systems, which are used for larger, geographically dispersed operations ([1] p. 7). SCADA systems are cyber systems; the definitive elements are digital electronics. SCADA systems generally have six components ([1] pp. 7-8):

- **Instruments** sense conditions; for example, in electric power, a voltmeter measures voltage and the measurements can be sent to a controller.
- **Operating equipment** comprises machines that are central to the system and that can be controlled; for example, a circuit breaker in electric power can be tripped by a controller or automatically in response to system conditions.

[1] *Mechatronic* is a coined word combining *mecha*nical and elec*tronic*. A digital basis is so commonly found in modern mechatronic systems that their digital nature can be assumed.

- **Local processors** are the gateways to a site's instruments and operating equipment. One type of local processor, the remote terminate unit (RTU), communicates between remote instruments and operating equipment; for example, between a generator and a host computer. Local processors may be vulnerable to cyber attacks.
- **Short-range communication** consists of short connects between local processors and the instruments or operating equipment. Communication pathways can provide access for cyber attack.
- **Host computers** are the central point of monitoring and control where human operators can interact with the system. They may be located far from the local processors, instruments, and operating equipment. The human operators or logic imbedded in the host computer may control the local processors. For example, if frequency changes in an electric power grid, a host computer may automatically trip a breaker to prevent damage to a generator. A host computer is also vulnerable to cyber attacks.
- **Long-range communication** is the way local processors and host computers communicate over long distances. Common methods of communication are leased phone lines, satellite, microwave, and cellular packet data. Again, communication pathways can provide access for cyber attack.

SCADA systems have allowed increasingly efficient and coordinated critical infrastructure management. The primary benefit of using a SCADA system is that data about system function can be collected from a large geographic area, which allows decision makers to observe and make decisions based on the condition of a large fraction of the infrastructure, if not its entirety. This permits substantially more effective decisions; because, in all sectors, the infrastructures are highly interconnected. Furthermore, these decisions can be implemented easily once made; because, in general, SCADA systems are designed so that commands can be sent and executed to the same large area being sensed. This is not only more effective and efficient, but also more convenient. SCADA technology allows informed decision-making and control at a centralized location far from remote locations and far from the noise and danger of the power plants, production facilities, refineries, and pipelines that make up the various sectors.

Unfortunately, the digitized centralization that makes SCADA technology so cost-effective and convenient induces vulnerability. The centralization that defines SCADA operations means that if the SCADA system is compromised, a large fraction of the infrastructure—the same large fraction discussed above that is so advantageously and efficiently controlled—can be placed at risk. SCADA systems are constructed from networked digital communication and processing elements and are, therefore, cyber systems.

Cyber attacks target the digital information elements of PCS. An adversary who has penetrated an infrastructure's PCS may be able to degrade infrastructure function by issuing false commands, replaying commands at inappropriate times, or preventing authorized commands from reaching their destinations. For example, a man-in-the-middle attack on a local processor could compromise it so that false instrument readings are sent to the host computer, or an unauthorized command to an RTU could cause a circuit breaker to incorrectly trip.

Cyber attacks may originate anywhere an adversary can gain unauthorized access to digital information being used by the PCS. In 2000, an Australian sewage treatment facility was disrupted by a rejected job applicant who used a radio transmitter to break into the controls ([1] p. 15). Insiders may also threaten control systems through their knowledge and access to the control systems. The Internet is a common source of nontargeted attacks that can compromise control systems. For example, in 2003, a worm known as Slammer infected a computer network and disabled a safety monitoring system at the David-Besse nuclear power plant in Oak Harbor, Ohio ([1] p. 16). This approach is of interest because of the large fraction of digital PCS that are accessible via the Internet and the speed with which worms and other malware can propagate (see [2], concerning the spread of the *Code Red* worm).

There are three main challenges to securing control systems that are cited in [1] (pp. 17-20). First, many operational control systems, which in some cases have been in use for decades, have limited computational capabilities that prevent using modern digital security technologies. Second, the need for real-time operations has impeded the use of security technologies for fear that they will hinder the operations, especially during an emergency. Third, design limitations prevent security technologies from being enacted. Control systems were not designed with security in mind, customized systems prevent software patches from being efficiently developed, and some control systems must operate continuously, thus preventing software from being updated.

1.1.2 Historical Information

Critical infrastructure control systems are more vulnerable today than in the past because of “increased standardization of technologies, the increased connectivity of control systems to other computer networks and the Internet, insecure connections, and the widespread availability of technical information about control systems” ([1] p. 14). Control systems can commonly be accessed remotely via dial-up modems or the Internet with gateways that are often insecure.

Many groups have enacted initiatives to improve control system security. Among them are private, industry-specific organizations, federal agencies (principally the U.S. Department of Homeland Security (DHS) and the U.S. Department of Energy (DOE), and the national laboratories. While multiple initiatives are underway, the Government Accountability Office (GAO) has emphasized the need for DHS to coordinate the various efforts to avoid duplication ([1]).

1.1.3 Significance

Sandia currently has modeling tools that analyze cyber effects and how those cyber effects lead to physical impacts. Sandia also has modeling and simulation capabilities to understand the economic consequences of the loss of a critical physical asset. A method is needed that will allow the bridging of these two capabilities and provide analysts with the ability to understand the national-level risk from cyber attacks. The effort, as documented in this report, for the fiscal year (FY) 2008 was to outline a method to correlate cyber disruptions to physical disruptions in interdependent infrastructures and assess the economic consequences associated with those disruptions.

This work benefits the DHS mission by allowing economic quantification of the effects and risks associated with cyber attacks on the ability of the nation's critical infrastructure to meet its mission and deliver key services. The method described will allow quantification of the risks associated with cyber threats to the nation's critical infrastructure so that that risk can be appropriately managed and potentially mitigated. This will allow DHS to prioritize infrastructure-protection activities. DHS has seen this as a pressing research need.

1.1.4 Literature Review

References throughout this report provide access information for source material. Because a primary purpose of this document is to describe gaps in Sandia's existing cyber risk assessment methodology, the most relevant information source has been documents and reports written by Sandians and their non-Sandia colleagues working to develop elements of that methodology. This is supplemented by material describing the infrastructure, infrastructure risk and its assessment, and techniques for simulating and measuring infrastructure function. A list of source citations appears as Appendix B: References.

The GAO reviewed efforts to improve control system security by private and public entities in *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* [1]. They concluded that a lack of coordination between the different groups risks duplication of efforts.

The *Roadmap to Secure Control Systems in the Energy Sector* ([3]) was developed to improve control system security in the electricity, natural gas, and petroleum industries. Funded by DOE and DHS, the Roadmap was developed in conjunction with other government agencies, national laboratories, and industry asset owners and operators. The Roadmap has three purposes:

- "Define a consensus-based strategy that articulates the cyber security needs of owners and operators in the energy sector."
- "Produce a comprehensive plan for improving the security, reliability, and functionality of advanced energy control systems over the next 10 years."
- "Guide efforts by industry, academia, and government and help clarify how each key stakeholder group can contribute to planning, developing, and disseminating security solutions."

1.2 Purpose

This LDRD is designed to characterize and identify gaps in the process by which cyber effects on the critical infrastructure are quantified. The results of this study show what sort of efforts need to be applied to quantify the risk due to adversarial exploitation of vulnerabilities in the critical infrastructure's cyber subsystems.

For the purposes of this report, the cyber subsystem(s) of a system (or a system of systems) is defined as the hardware[2], software, and facilities by which digital information is created, destroyed, modified, stored, and transmitted. From an operational perspective, cyber means are used to execute the control process by which the system is made to execute its design functions. Historically, mechanical means were used to achieve this, which meant that operators needed to be physically proximate to the devices they were operating. This is a primary benefit of cyber mechanisms. They allow remote operation of the infrastructure, to the extent that the hardware elements of a system can remain untouched and unseen by system operators, often for their entire operational life. Most modern systems of any complexity have a significant cyber component. In particular, the critical infrastructure is managed almost entirely via cyber means.

To the extent that proper system function depends on cyber function, penetration of the cyber regime by an adversary directly subverts system function by replacing authorized control with adversarial intent. At worst, the adversary gains control of system function, and even trivial interruptions can prevent the system from performing correctly. This is the essential impact of cyber attack.

1.2.1 Reason for Investigation

The goals of this LDRD are to describe the gaps in Sandia's process for analyzing attacks to cyber-based control systems and estimating the consequences of the resulting disruptions to the infrastructure, and to outline the path to filling those gaps. Currently, Sandia and other government agencies have tools and methodologies for assessing cyber *threats*[3] to control systems. Sandia also has capabilities in modeling electric power control systems to allow researchers to assess the possible *effects* of a cyber attack on the particular control system that is attacked as well as the *impacts* of those disruptions on the infrastructure as a whole. The National Infrastructure Simulation and Analysis Center (NISAC) has the capabilities to assess the *consequences* of infrastructure disruptions on other infrastructures and the economy.

The methods recommended in this report will allow researchers to assess how cyber attacks on critical infrastructure control systems correlate to disruptions in other infrastructures and to quantify the economic consequences of these cyber attacks.

The *Roadmap to Secure Control Systems in the Energy Sector* ([3]) explains that the costs of developing and integrating security advances into SCADA architectures can be high and difficult to justify due to the uncertainty in the identification and evaluation of risks. The quantification of the economic consequences of cyber attacks is important in the energy sector because "Some decision-makers see no economic penalty associated with minimizing funding for cyber threat deterrence" ([3] p. A-4). Additionally, private infrastructure owners have "difficulty in

[2] Note: "Hardware" refers to all physical components, not just computational assets.

[3] The italicized language, used throughout this report, follows that of the threat-to-consequence (T-to-C) framework, which is discussed in Appendix A.

developing a compelling business case for improving control systems security" due to the lack of a business case and market incentive ([1] p. 20).

The development of a methodology to correlate cyber attacks with economic consequences will motivate decision makers to take steps to improve control system security.

1.2.2 Roadmap Challenges

The *Roadmap to Secure Control Systems in the Energy Sector* ([3]) lists "Identifying Strategic Risks" ([3] p. A-2) as a key challenge. The Roadmap says, "Identification of energy sector cyber threats, vulnerabilities, and consequences will facilitate development of standards for cyber security best practices, performance criteria for baseline control system security, and design requirements for hardware and software," ([3] p. A-2). This report provides a methodology to assess the consequences of cyber attacks on critical infrastructure control systems, on other infrastructures, and on the economy, thus facilitating strategic risk assessment.

The roadmap also stresses the need for making a business case for improving control system security. It says, "Without sufficient means to fully quantify and demonstrate the potential impacts of cyber attacks on energy sector control systems, asset owners are hard pressed to justify SCADA control system security as a top funding priority. The result is a reactionary policy to cyber security that places our bulk electric and critical oil and gas assets at greater risk to emergent cyber threats" ([3] p. A-4). Similarly, without the means to quantify the consequences of cyber attacks to other infrastructure and the economy, the public sector may not be able to justify control system security as a top funding priority. The consequences of a cyber attack on a critical infrastructure control system extend beyond the stakeholders of the attacked infrastructure. Even if asset owners can quantify risks of cyber attacks to themselves, they may under invest in security measures in the face of such externalities (see [4]). The methods recommended in this report enable assessment of widespread consequences of cyber attacks, which may be used to make a business case for public efforts to mitigate against specific cyber threats.

1.2.3 Audience

This report is expected to benefit DHS and DOE by enabling the economic quantification of the consequences of cyber attacks on the nation's critical infrastructure. It will also benefit asset owners and operators by quantifying the possible consequences of cyber attacks against their security vulnerabilities, for which they may be held financially responsible.

1.2.4 Desired Response

After reading this report, researchers at Sandia will have a roadmap for integrating infrastructure effects analysis and economic impact analysis to quantify the consequences of cyber attacks on critical infrastructure. While capabilities in assessing the effects of cyber attacks currently exist, primarily in electric power, this report details how the capabilities can be extended into other infrastructures and how capabilities can be further integrated to facilitate consequence assessment.

1.3 Steps in the Cyber-Attack-Consequence Assessment Process

The cyber-attack-consequence assessment process is a five-step process for assessing the infrastructure impact and economic consequences of cyber attacks on critical infrastructure control systems. Section 2 discusses the process and lists tools that can be used in the process, while later sections describe these capabilities in more detail.

This report focuses on the third, fourth, and fifth steps of the process (see Section 2, Figure 1), assuming that the first two steps (the development of a cyber attack and assessment of control system vulnerabilities) will be accomplished beforehand. The third step assesses control system effects by examining how a particular cyber attack will affect the operation of control systems. The fourth step assesses how the attack's effects on the control system produce impacts to both the system's own infrastructure and other, related infrastructures. The fifth step assesses how the infrastructure impact culminates in economic consequences.

1.4 Organization of the Report

This report is organized into seven sections. This initial section introduces the LDRD and provides background information about process control systems and their cyber vulnerabilities. Section 2 discusses the cyber-attack-consequence assessment process. Section 3 provides a walk-through of the process with electric power using the existing capabilities that can most easily be incorporated into the process. Section 4 identifies gaps in the walk-through and suggests capabilities that could be integrated into the process to close the gaps. Section 5 explains how the process can be extended to infrastructures other than electric power and identifies some capabilities to support these extensions. Section 6 suggests how the steps in the process can be further integrated to make the process more efficient. Section 7 offers the authors' conclusions.

This page intentionally left blank.

2 CYBER-ATTACK-CONSEQUENCE ASSESSMENT PROCESS

This section describes a cyber-attack-consequence assessment process developed to coordinate Sandia's capabilities in assessing the effects of a cyber attack and in assessing the infrastructure impacts and economic consequences of those attacks. Figure 1 illustrates a conceptual view of this process. The yellow boxes in the illustration are the focus of the efforts of this report.

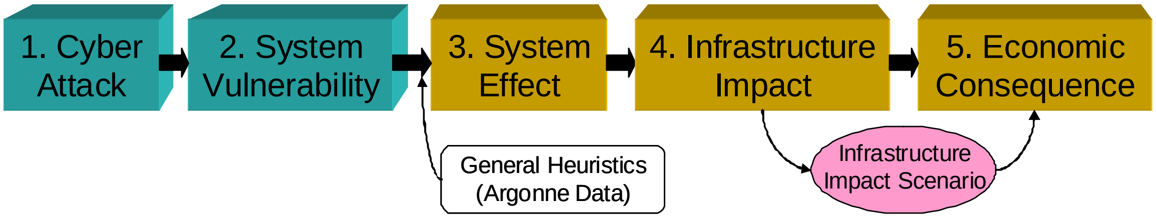

Figure 1: A Conceptual View of the Cyber-attack-consequence assessment Process

Step 1 of this process identifies a cyber attack, and Step 2 identifies a system vulnerability that will allow a cyber attack to be successful. These two steps may occur simultaneously because a cyber attack is likely to attempt to exploit a system vulnerability to ensure success.

Step 3 of this process is the assessment of the effects of a successful cyber attack on a critical infrastructure control system. This step answers the question "How does the attack affect the control system and the components that are connected to the system?" Simulators that model control systems can be used to assess how the control system will react to the attack. This step can be informed by general heuristics, or rules-of-thumb, about the structure of the control systems to help inform the assessment. Table 1 lists some examples of heuristics that may be found and gives examples of questions that they can answer that will be useful for determining the effects of cyber attacks to control system. These heuristics can be found from such sources as Argonne's Protected Critical Infrastructure Information (PCII) data (see Section 3.1.2.1).

Table 1: Some Examples of Hypothetical Heuristics and Questions they Might Answer

Heuristic	Example of a Question Answered
A component of an electric power control system is networked to computers that are connected to the Internet.	Can an Internet-based cyber attack on a control center affect a control system?
A water treatment control system monitors instruments but cannot directly control operating equipment.	Can a cyber attack possibly take direct control of infrastructure components?
A component of a gas pipeline control system uses a particular operating system.	Can a certain virus that infects a particular operating system be used to disable the control system?

During Step 4 of the process, the impact of the control system effects to the critical infrastructure being attacked (and possibly other, related infrastructure) is assessed. Infrastructure models are used to determine how the control system effects might spill over to other parts of the infrastructure that are not controlled by the attacked system. The result of this step is an infrastructure-impact scenario, which is a specific scenario of how the infrastructure is affected by the cyber attack. The scenario should specify the particular components of the infrastructure that are affected, as well as the details (time, severity, etc.) of the impacts.

Finally, during Step 5 of the process, the economic consequences of the infrastructure disruptions are found using the infrastructure-impact scenario. If the infrastructure-impact scenario constructed in Step 4 finds that the cyber attack may create disruptions in infrastructure, there will likely be economic ramifications to the loss. Economic models are available that can be used to assess the economic consequences of infrastructure disruptions caused by cyber attacks.

Table 2 lists existing capabilities and explains how they will be used in the cyber attack consequence assessment process for electric power. Table 3 illustrates tools that can be used to extend and refine the process in the case of electric power. Table 4 lists the capabilities that can be used to extend the process to other infrastructures.

Table 2: Capabilities Used in the Process Walk-Through for Electric Power

Process Step	Tool	Description
System Effect	Protected Critical Infrastructure Information (PCII)	PCII information can assist in providing heuristics for how likely the attacks are to have any particular effects on the system.
	Virtual Control Systems Environment (VCSE)	The VCSE is a test-bed environment that integrates real, emulated, and virtual entities to simulate control systems.
Infrastructure Impact	VCSE Steady-State Simulator	The steady-state simulator solves for the steady state of an electric power grid within the VCSE environment.
	IEEE RTS-96 Model	RTS-96 is a standardized model of an electric power system that facilitates comparison and benchmarking of reliability studies.
	FAST Analysis Infrastructure Tool (FAIT)	FAIT is a database of infrastructure assets that identifies relationships between assets.
Economic Consequence	Regional Economic Accounting (REAcct)	REAcct uses input-output multipliers to calculate impacts of economic disruptions to the entire economy.

Table 3: Capabilities Used to Fill Gaps in the Process or Extend the Process for Electric Power

Process Step	Tool	Description
Infrastructure Impact	Critical Energy Infrastructure Information (CEII)	CEII information is details about electric power infrastructure provided to FERC that can assist in building models of real power grids.
	VCSE transient power simulator	The transient power simulator is a dynamic electric power model in the VSCE environment that is uses differential equations.
	Finite-State-Machine (FSM) Representation of Dynamical Power System Behavior	The FSM model is a dynamic electric power model that uses graph-based methods.
	PowerWorld Simulator	PowerWorld Simulator is a commercial package with extensive visualization and geographic capabilities that can solve for the steady state of large power grids.
	Interdependent Energy Infrastructure Simulation System (IEISS)	The IEISS solves for the steady state of electric power systems and models natural gas distribution systems and the interdependencies between the two systems.
	Models of Actual Power Grids	Energy Visuals and Platts are commercial sources of models that represent real-world grids.
	Steady-State Load-Shedding Model	The steady-state load-shedding model solves for the steady state of an electric power grid and determines the optimal load-shedding strategy when supply cannot meet demand.
Economic Consequence	Consequence Modeling Tool	The Consequence Modeling Tool is a tool under development that helps stakeholders, such as utilities, weigh the various consequences of a cyber attack on an electric power control system.

Table 4: Other Capabilities to Extend the Process for Other Infrastructures

Process Step	Tool	Description
System Effect	OPNET Modeler	OPNET Modeler is a commercial tool for simulating networks.
Infrastructure Impact	Matlab	Matlab is a commercial numerical computing environment that can be used to create other tools and interface with the VCSE.
	Water Infrastructure Simulation Environment (WISE)	WISE is an extension of the IEISS that models water infrastructure such as water treatment and wastewater.
Economic Consequence	Consequence Modeling Tool	The Consequence Modeling Tool is a tool under development that helps stakeholders, such as utilities, weigh the various consequences of a cyber attack.
	REMI	REMI is a commercial tool that models long term changes in the economy using input-output and general equilibrium methodologies.
	NISAC Agent-Based Laboratory for Economics (N-ABLE™)	N-ABLE™ is a high-fidelity, agent-based simulator that models regional and national value chains.
	Dynamic Systems Modeling	Dynamic systems modeling produces analyses of complex, nonlinear systems (such as the economy) using feedback loops, stocks, and flows.

3 PROCESS WALK-THROUGH WITH ELECTRIC POWER

This section provides a walk-through of the cyber-attack-consequence assessment process, using electric power as an example. Sandia's existing capabilities are shown in Table 2. Sandia's existing capabilities make this process relatively straightforward to accomplish for electric power.

Sandia has developed extensive capabilities for simulating electric power control systems through its participation in the National SCADA Test Bed (NSTB). NSTB is a multinational laboratory facility created by the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE-OE). A mission of NSTB is "identify[ing] and correct[ing] critical security flaws in SCADA control systems and equipment" [5]. Facilities are concentrated at the Center for Control System Security at Sandia and the Critical Infrastructure Test Range at Idaho National Laboratory.

The NSTB was created "to assist the energy sector and equipment vendors in improving the security of control systems hardware and software" and "has closely aligned its activities with the industry-defined priorities identified in the Roadmap to Secure Control Systems in the Energy Sector" ([6] p. i). This section will show how the capabilities that the NSTB has developed to model the effects of cyber attacks on physical assets can be extended to explore how physical disruptions may cascade across infrastructures and assess the economic consequences of those disruptions.

3.1.1 Cyber-Attack and System-Vulnerability Steps

In the first two steps of the process, a cyber attack is identified along with the vulnerabilities in the control system that it may exploit. Because this report is most concerned with creating a roadmap for the final three steps of the process,[4] it is assumed that these steps have been completed, and the results are available to inform the remaining steps of the process.

An example of results that may come from this step for an attack on electric power control systems is given in a scenario developed in the *National SCADA Test Bed Threat Development Team, Threat case scenario* [7]. In the scenario, multiple malevolent front-end processors (FEPs) have been compromised at the manufacturer or through software updates. An FEP is a computer that provides a bridge between client computers of human operators and power system hardware clients such as RTUs. The FEP passes commands from the users to the hardware and provides the user with data from the power system hardware. The rogue FEPs are programmed to send breaker trip commands to generators to induce widespread under-frequency load shedding during periods where power reserves are low (Stage 2 alerts), thus causing blackouts.

[4] Threat analysis, which is necessary for risk analysis and may aid in identification of cyber attacks and system vulnerabilities, is discussed at greater length in the appendix.

The scenario presented in [7] is unlikely to occur. The scenario was constructed so that it could be presented in unclassified audiences as an illustration of a cyber-attack scenario. Realistic scenarios are likely to be classified.

3.1.2 System Effect

Step 3 of the process assesses the effects of the cyber attack on the control systems being attacked. This step can be informed by heuristics about infrastructure interdependencies that may facilitate the cyber attack. For example, if a utility's control systems were networked to computers that had Internet access, it would be possible that a cyber attack against that utility might affect the control systems, even if the attack was not directly aimed at those systems. PCII information collected from DHS site-assist visits is a source of these data. These data are stored at Argonne National Laboratories.

The effects of cyber attacks against control systems can currently be assessed for electric power using the Virtual Control Systems Environment (VCSE), developed by Sandia as part of the NSTB program. The focus of VCSE modeling has been electric power control systems.

3.1.2.1 Protected Critical Infrastructure Information (PCII)

The DHS National Protection and Programs Directorate (NPPD) maintains databases of PCII that are shared between the private and public sector. The PCII program started following the passage of the *Critical Infrastructure Information Act* of 2002 as a way for the private sector to share sensitive information that may be useful in homeland security. PCII is submitted voluntarily and is exempt from the *Freedom of Information Act*, state and local disclosure laws, use in civil litigation, and use in regulatory purposes.

Handling of PCII data follows strict procedures to ensure the privacy of the submitted information. Only federal, state, and local government employees, who are trained in the handling of PCII data, who have homeland security responsibilities, and who have a need-to-know, are permitted to access PCII data. Government agencies participate in the PCII accreditation program to gain access to PCII data, and employees participate in PCII Officer Training (a day-long instructor-led course) or PCII Authorized User Training (a two hour computer-based course).

PCII data from Argonne National Laboratories contain information gathered from site visits by the DHS Protective Security Coordination Division. These data contain information about site vulnerabilities, including answers to several questions about cyber attack vulnerabilities. It is important to gather a consistent set of PCII data for every type of infrastructure that is analyzed to assess whether it is really possible for an identified cyber threat to successfully attack a control system and harm the components that the system controls. The following are examples of some potentially useful data:

- Are control systems connected to the Internet? An Internet-based attack will require that the control system somehow be connected to the Internet. If the control system is not networked to any computers that can access the Internet, an Internet-based attack cannot be successful.

- Does the control system actually have control of the operating equipment or does it merely monitor instruments? A control system that does not have direct control over the operating equipment can create problems (e.g., a man-in-the-middle attack), but human intervention can prevent many serious problems.
- Can the control system be overridden through physical controls? If human operators see that the control system is causing the operating equipment to behave abnormally, can they take control of physical controls with minimal disruption? For example, if a wastewater treatment control system releases raw sewage, an operator might notice this and quickly close a valve, thus preventing much damage.

3.1.2.2 Virtual Control Systems Environment (VCSE)

Sandia has developed the VCSE, a test bed environment that combines real, emulated, and virtual entities in the power generation and distribution industries, with future extensibility to other infrastructures [8]. Analysts can use the VCSE to learn about system dependencies and identify threat attack paths that can be used to exploit vulnerabilities. The VCSE can also be used to explore the consequences of attacks, analyze the effects of mitigating threats, and test prototypes of systems prior to deployment.

The VCSE is the glue that connects all of the components in the simulation to allow the analyst to analyze the control system and overall system (e.g., the power system) from command to resulting effects. The VCSE contains a number of models for “control centers, network communications (including wireless), PCS/SCADA elements, and infrastructures.” These models act as virtual machines, but the VCSE can also interface with actual, physical components (hardware in the loop) using real software [8]. Commercially available software, such as OPNET Modeler, Matlab, and PowerWorld, can be easily integrated to the VCSE to assess the behavior of the external systems in response to the control systems. The VCSE’s application programming interface (API) can be used to connect new software through the use of dynamic-link library (DLL) files. For example, plug-ins can be written in C++ to communicate with the VCSE through its API. Recent development allows VSCE to also interface with distributed interactive simulation (DIS) protocols, which is a standard for conducting real-time war-gaming.

Cyber attacks on a control system can be simulated through the addition of a rogue software model in the VCSE or through manual intervention. As mentioned previously, in simulations of a hypothetical cyber attack of an electric utility developed in the *National SCADA Test Bed Threat Development Team*, *Threat case scenario* [7], a rogue software attack simulator is created to represent the malevolent FEPs.

The result of VCSE simulation will be a set of actions of the simulated components. These actions can be summarized qualitatively (e.g., “this attack can disable the operating equipment”), summarized numerically (e.g., “this attack can disable 30 percent of generation”), or feed all simulation results to other tools directly through a software interface. The VCSE is currently capable of feeding output to an infrastructure-impact tool (the electric power steady-state simulator discussed in the next section), so this walk-through will primarily take advantage of that capability.

At this step of the process, researchers can use the heuristics developed with the Argonne PCII data to verify that the identified cyber attack, system vulnerability, and system effect are realistic. For example, if the VCSE simulation showed that the control system behaved in a way that would have been overridden by a human operator before any damage had been done, the actual system effects might be minimal.

3.1.3 Infrastructure Impact

Cyber attacks can impact not only the entity that they attack, but other entities within the same infrastructure. These impacts can cascade into other infrastructures. The cumulative effect of these infrastructure disruptions will likely have an impact on the economy.

Disruptions in electric power are especially susceptible to spillovers. There are a limited number of alternating-current (AC) power grids in the contiguous United States. All components of each grid must operate in concert with one another, at the same frequency. Deviations in frequency or voltage may cause circuit breakers to open to protect equipment, which may further exacerbate the deviations, thus leading to a cascade of failures.

The NSTB currently has capabilities for assessing the impacts of cyber attacks on the electric power grid. The VCSE has the ability to interface with external software that simulates infrastructure systems. For example, in the cyber attack scenario developed in the *National SCADA Test Bed Threat Development Team, Threat case scenario* [7], a steady-state, load-shedding model is used to simulate the effects on a power grid. The VCSE also has the capability to interface with other software that can simulate infrastructures beyond power.

In this walk-through, the result of the system-effect step, coupled with the results from the VCSE, can be used to construct an infrastructure impact scenario for the impacts of a cyber attack on electric power. This scenario can be augmented to include the impact on other infrastructure through the use of the Fast Analysis and Simulation Team (FAST) Analysis Infrastructure Tool (FAIT).

3.1.3.1 Virtual Control Systems Environment (VCSE) Steady-State Simulator

The NSTB has written two power simulators that directly interface with the VCSE. The steady-state simulator is discussed here, while a dynamic simulator is discussed in 4.2.1. Additionally, PowerWorld—a commercial power simulator (see 4.2.3)—can currently interface with the VCSE.

In a cyber attack such as that simulated in the *National SCADA Test Bed Threat Development Team, Threat case scenario* [7], or any other event that could remove generation from a power grid, the state of the power grid will change to reflect the reduction in generation, which no longer matches the load. If available reserves are too low, the load will be larger than the generation, which will cause frequency to drop. Frequency drops are dangerous to many types of generation; hence, frequency has to be maintained to keep generation online. Frequency is maintained through load shedding, which means that some customers will be cut off from the grid and will experience blackouts.

The steady-state, load shedding model is a plug-in for the VCSE system that calculates steady-state conditions for an electric power grid and accounts for changes caused by load shedding that occur as a result of generation outages that prevent generation from meeting the load demand. The plug-in is written in C++ and uses a Newton-Raphson method ([9], Section 3.8.1) to solve for the state of the electrical grid (i.e., voltages and phase angle) given a grid topology, generation, and load.

Because the tool only calculates the steady state of the system, transitions between steady states are ignored—changes are assumed to be instantaneous. Dynamic models (Sections 4.2.1 and 4.2.2) can model changes between the steady states, thus modeling the transition, which may be especially important when analyzing cyber attacks that may attack an electric power grid by changing parameters that affect its dynamic behavior.

The steady-state, load-shedding model was used in the NSTB workshop to estimate how the simulated power grid reacted to the rogue FEP cyber attacks. The simulation assumed a hypothetical power grid topology called the Institute of Electrical and Electronics Engineers (IEEE) Reliability Test System (RTS)-96, which is commonly used as a benchmark to standardize power grid simulations. The attacks varied in their intensity; i.e., the number of generators whose FEPs were compromised. The simulation varied the number of generators that were affected by the rogue software and the amount of reserves available to arrive at simulated loads that were shed.

Because the steady-state simulator operates within the VCSE framework, the steady state can be continuously calculated and updated given changes in the status of the various control system components that are simulated in the VCSE. The results of this tool can be used to construct the infrastructure-impact scenario. Like the VCSE output, the steady-state simulator output can be summarized qualitatively, summarized numerically, or interfaced directly with other tools. Because the tool currently uses the IEEE RTS-96 model of an electric power system, direct integration with economic-consequence-assessment tools is difficult (this extension is discussed in Section 6.2), the infrastructure-impact scenario will be constructed with a combination of qualitative and quantitative summaries for the region of interest. For example, the simulator may show that an attack leads to 80 percent of load being shed near an attacked generator in the IEEE RTS-96 framework. A scenario for a specific generator could be constructed where 80 percent (or some other number that the analyst believes reasonable for an attack on a real power grid) of load is shed. If real power grids were used in place of IEEE RTS-96 (Section 4.1 discusses the gap caused by using unrealistic models of power grids), then the analysis can rely less on qualitative summaries and more on quantitative summaries of infrastructure impacts in real locations.

3.1.3.2 Institute of Electrical and Electronics Engineers (IEEE) Reliability Test System (RTS)-96 Model

The IEEE RTS-96 Model [10] is a model of an electric power system used to compare and benchmark bulk power reliability studies. Therefore, the model is designed to be standardized, with no intention of developing a system that is representative of a specific or typical power system (p. 1010). There are different variants of the model (i.e., one-, two-, and three-area models), but the configurations and data driving the systems are fixed.

IEEE RTS-96 is not software or a tool, but rather a set of specifications for a hypothetical power system. For example, the data include a topology for connecting the components on the grid. System load is specified for every hour of every day of a year. Different types of generators exist, with specifications such as total capacity and startup costs.

The IEEE RTS-96 model specification was used in an NSTB workshop [11] to perform reliability analysis (Section 6.1.1) using the steady-state, load-shedding model (Section 6.1.2). The advantage of using the IEEE RTS-96 as a model of an electric grid is that it provides a standardized specification that can be reproduced in relatively inexpensive simulations. The standardization facilitates the comparison of system behavior under different circumstances, such as different types of cyber attacks and different mitigation techniques.

3.1.3.3 Fast Analysis and Simulation Team (FAST) Analysis Infrastructure Tool (FAIT)

The FAST team at NISAC provides DHS with answers to questions about threats to national infrastructure. FAST analyses are often conducted in response to specific threats and, therefore, must be conducted quickly. For example, in advance of a major hurricane, the FAST team may have just hours to answer questions about the possible consequences of the hurricane. In the event of a major cyber attack that disabled power to a large area, the FAST team may be asked by DHS to answer questions about the consequences of that attack to other infrastructures and the economy.

FAIT ([12]) was developed to aid the FAST analyses. It contains an extensive spatial database of infrastructure that can be used to ascertain infrastructure interdependencies and collocation. FAIT is designed to facilitate the rapid analysis of these infrastructures through its translation of data into natural language, its mapping capabilities, and its features that allow users to attach their own data to specific assets.

Dependencies in FAIT are defined by a rule-based engine called Jess, developed at Sandia. The engine takes into account the available attributes for each infrastructure and specific relationships inherent in the infrastructures. For example, an electrical generator that uses natural gas as a fuel is likely to connect to a nearby natural gas pipeline. Connections between assets and electrical power substations are uncertain, but can be estimated by proximity.

FAIT contains extensive visualization capabilities, using third-party tools such as Google Earth. Assets can be selected by location via a web-based interface that includes an interactive mapping tool. Users can easily see what assets are in a specific area, which is useful if the location of a threat is known.

The results from the previous steps of the process and the analysis of electric power infrastructure assets using the VCSE steady-state simulator can be used to inform an analysis with FAIT. In this walk-through, the VCSE steady-state simulator produced estimates of the loads that are shed in the simulated cyber attacks. Although the IEEE RTS-96 model of the grid topology used in that simulation does not represent a real topology, the quantity of load shed can be compared to the total load in the system to estimate the severity of the impact of the attack to the entire electric power system.

Analysts can combine the infrastructure-impact scenario developed with the VSCE steady-state simulator with the results of FAIT, which can then be used to augment the infrastructure impact scenario by determining other infrastructures that are in the same geographic area as the outage caused by the cyber attack. For example, a natural gas pipeline may use electric compressors, which can be disrupted by an electrical outage. In such a situation, gas customers that rely on the compressor for natural gas delivery, which can be determined by the data on pipelines in FAIT, may not be able to operate.

3.1.4 Economic Consequences

A cyber attack on a control system may have effects beyond those of the attacked infrastructure identified in the infrastructure-impact step of the process. Infrastructures are interdependent, which means that a failure in one component may spill over to other components of the same infrastructure as well as associated infrastructures and industries. This interdependence is clear in the electrical power industry because almost all industries require electrical power in some manner. Disruptions of infrastructure may also spill over to economies. Economic activity depends on the infrastructure. A sustained loss of electric power, for example, may cause economic activity to nearly stop.

The consequences of infrastructure disruptions are complicated and difficult or impossible to measure in many cases and may vary greatly in their consequences. An outage at a single generator during a period with adequate reserve capacity is unlikely to disrupt service. Spot prices (which can be modeled by PowerWorld, see Section 4.2.3) might be affected by the outage, but there will likely be little change to overall economic activity. The consequences of an outage that results in unserved load are more difficult to measure. For a short load-shedding event, the economic consequences will likely be light because many short-term economic losses are recoverable. For example, consumer purchases can be delayed to another day or time, and interrupted manufacturers can draw on inventories that can be replenished over time. Many of the losses that do occur may be difficult to quantify. For example, short losses of power chemical plants sometimes cause the release of chemicals and have the potential to cause accidents.

In the case of electric power, smaller outages are likely to affect a small area and last a short time. Consequences of the power outage are likely to be relatively small and affect a small number of parties. Identification of the consequences will, therefore, be difficult. On the other hand, a large blackout that lasts a long time will have larger consequences that affect nearly all infrastructures and individuals. Consequences identification will be much easier because of the importance and ubiquity of electric power.

In the NSTB workshop [12], some informal methods of assessing the economic consequences of cyber attacks to electric power systems were developed using the scenario in the *National SCADA Test Bed Threat Development Team, Threat case scenario* [7]. The purpose of the exercise was to estimate the consequences of a cyber attack on a single utility company, rather than estimating the economic effects to the entire economy. A low-fidelity proxy for the cost of lawsuits due to a day-long blackout to the utility's entire service territory was created by calculating all of the direct and indirect economic impacts in the service territory. In reality, the effects of a cyber attack are likely to be more complex in terms of the coverage and duration of the blackout. Furthermore, the economic impact of the blackout is unlikely to be a complete loss of all economic activity, especially for short-duration blackouts. However, economic losses may propagate beyond the immediate service area.

3.1.4.1 Ad Hoc Analysis of Economic Consequences

The simplest way of assessing the economic consequences of a cyber attack is an ad hoc, back-of-the-envelope estimation using available data and an infrastructure-impact scenario created using qualitative and quantitative summaries of the results of the infrastructure-impact tools. This is the approach used to estimate the economic consequences of the simulated cyber attack in the NSTB workshop ([12]). The estimates of the workshop focused on the possible liabilities of utilities for lost power by calculating the total economic activity within each utility's service area for a single day from estimates of annual economic activity. This analysis assumed that electric power was lost throughout the utility's entire service area and that all economic activity was lost within the area due to the loss of power. In reality, the loss of power would likely be more complicated and the loss of economic activity would depend on who and what lost power and for what period of time the power was lost.

The ad hoc analysis of economic consequences requires an infrastructure-impact scenario developed Step 4, Infrastructure Impact, of the process; however, this scenario does not need to be detailed and can be constructed with minimal effort. For example, the scenario used for economic consequences in the NSTB workshop may be stated simply as, "All electric power within utility XYZ's service territory is lost for a day, thus inhibiting all economic activity."

3.1.4.2 Regional Economic Accounting (REAcct)

Regional Economic Accounting (REAcct) is a tool used for calculating losses of economic activity in a county. REAcct computes the economic impacts of interruptions to the businesses in the disruption region (called direct impacts) and outside the disruption region (called indirect impacts). Economic losses occur not only within an affected county, but spill over to other counties. A manufacturing firm that halts production due to an electricity outage may permanently reduce output due to the halt. This reduction is a direct economic impact of the outage. Because the firm produces fewer goods, it requires fewer inputs. Thus, its suppliers, who may be located anywhere in the world, also reduce output. These reductions form the indirect economic impact. The loss of business for these firms may mean that workers experience a reduction in pay. These workers may reduce their spending due to their lost income, which reduces economic activity even more. These reductions are the induced economic impacts of the outage.

The REAcct methodology is described in *REAcct 1.0: an Initial Methodology for Estimating and Reporting Economic Impacts* [14]. REAcct measures direct, indirect, and induced economic impacts (the indirect and induced impacts are combined and reported together). It is based at the county level and uses Regional Input-Output Modeling System II (RIMSII) multipliers to calculate the combined indirect and induced economic impacts. REAcct works within the FAIT environment. Economic losses throughout an economy that are caused by economic losses within the entire county containing a specific asset can be calculated from an analysis page for the asset. Also, economic losses can be calculated for (portions of) multiple counties by submitting an Excel sheet with the affected counties and parameters for a scenario. Each county has a number of days of economic disruption, a fraction of the county that is affected by the disruption, and a fraction of the affected area that is actually disrupted (the total fraction of the county that is disrupted is the product of the latter two fractions).

The REAcct methodology is a tool that is useful for determining the economic activity from a county if a fast estimate is needed and accuracy is not of the highest importance (see Section 4.3 for limitations). To use the REAcct methodology within the cyber-attack-consequence assessment process, the infrastructure impact scenario must specify counties that are affected as well as the number of days that the impact occurs and the two fractions mentioned in the previous paragraph. REAcct can handle complicated scenarios where different counties, or even different parts of the same county, have different fractions of disruptions.

Figure 2 gives an example of an infrastructure-impact scenario that might be generated from the infrastructure-impact step of the process. In this scenario, infrastructure has been disrupted across four counties in different levels of severity.

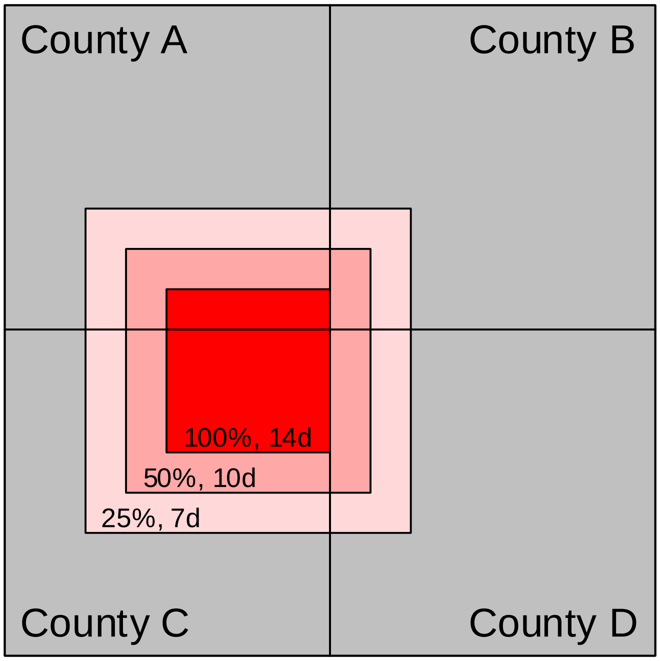

Figure 2: Hypothetical Infrastructure Impact Scenario

If a model of a real electric power grid were used, this infrastructure-impact scenario could be created using the quantitative results of the infrastructure-impact step of the process. However, in this walk-through, the IEEE RTS-96 model is used, so the scenario must be constructed by also relying on a qualitative assessment of the results of infrastructure-impact tools.

Table 5 shows how the infrastructure-impact scenario shown in Figure 2 is translated so that it can be used as an input in REAcct. This translation assumes that economic activity is spread evenly throughout a county, thus the fraction of the county that is affected by a disruption is the same as the fraction of the economic activity affected from the disruption.

Table 5: REAcct Input for Hypothetical Infrastructure Impact Scenario

County	Days	Affected (%)	Disruption (%)
A	14	6.3	100
A	10	9.4	50
A	7	12.5	25
B	10	3.1	50
B	7	6.3	25
C	14	18.8	100
C	10	12.5	50
C	7	15.6	25
D	10	6.3	50
D	7	9.4	25

3.2 Gaps in Capabilities

The steps of the cyber-attack-consequence assessment process can be accomplished for electric power using the capabilities discussed in the walk-through. These capabilities have several gaps that inhibit the accuracy and precision of the consequence assessment process. The most noticeable gap for electric power is that the grids currently being used by the steady-state simulator are not real, which inhibits the ability to construct a realistic infrastructure impact scenario. Furthermore, both the steady-state simulator and REAcct are limited. Section 4 discusses ways that these gaps can be filled by using existing capabilities or capabilities under development.

Section 5 discusses the gaps that must be filled to extend the consequence-assessment process to infrastructures other than electric power. The consequence-assessment tools are flexible to assessing the consequences of disruptions in other critical infrastructures caused by cyber attacks. The control-system-effect and infrastructure-impact steps, on the other hand, require greater development to enable the creation of realistic and detailed infrastructure-impact scenarios. The VCSE is flexible and can support new models of control systems in other infrastructures. Infrastructure-simulation tools for specific infrastructures are necessary to model the impacts of cyber attacks on different infrastructures. These individualized tools are necessary to construct infrastructure-impact scenarios and translate them into a format that can be used by economic-consequence tools.

3.3 Extensions to Process

The cyber-attack-consequence assessment process, as described in the walk-through, connects the steps of the process informally. Section 6 describes two extensions that can formalize the connections between steps. The first extension uses probabilistic modeling to assess both the infrastructure impacts and the economic consequences of cyber attacks. The second extension integrates the tools so that the process can be accomplished efficiently in a single environment. These two extensions—especially the latter—might require substantial development efforts to implement. The products of these extensions, however, would make the process simpler and more efficient.

This page intentionally left blank.

4 GAPS IN THE PROCESS FOR ELECTRIC POWER

There are several limitations to the capabilities described in the walk-through of the cyber-attack-consequence assessment process for electric power. These gaps can be closed using capabilities that currently exist or are under development at Sandia. Closing these gaps will often add complications to the process because the gap-closing tools are more complex than those used in the walk-through. Researchers will need to decide whether the improvements to the results of the process (i.e., the infrastructure impact scenario and the measurement of the economic consequences) are worth the costs of the increased complexity.

4.1 Use of Unrealistic Power Grids

The IEEE RTS-96 power grid model, which is currently used by the VCSE steady-state simulator, is not a representation of a true power grid. The IEEE RTS-96 specification is just one possible specification, and it is chosen so that it simulates most features that exist throughout power grids. However, this specification is not a realistic representation of any actual grid. The IEEE RTS-96 specification contains generators with a total generating capacity of 10,215 megawatts (MW), which is much smaller than actual power grids. For example, the load that was lost in the Northeast Blackout of 2003 was 22,984 MW in the state of New York, alone ([15]). As with the power grid test bed, there are no associated infrastructures or economies; therefore, it is difficult to create infrastructure-impact scenarios that can be used to map power system impacts to infrastructure and economic consequences. Rules-of-thumb for the costs of outages to customers can be developed (see, for example, [16]) but these rules are not specific to any particular scenario and include only direct economic impacts.

Other electric power models, in use or being developed by the NSTB at Sandia (mentioned in later sections of this report), use IEEE RTS-96 or specifications that are even more limited than IEEE RTS-96. While these models are useful for conducting experiments to see how cyber attacks affect electric power control systems, it is difficult to construct infrastructure-impact scenarios. Thus the models in use create a barrier to accurate consequence assessments.

The use of true-to-life power grid models would allow improved infrastructure-impact scenarios that would rely less on researchers' intuition. The steady-state model applied to IEEE RTS-96 produces estimates of hypothetical loads loss. A researcher has to decide how that maps to real world loads. If the steady-state model were applied to a real power grid, the output of the infrastructure simulation would show which loads were really lost. These areas could be mapped to counties and inputted into REAcct with a minimal number of additional assumptions.

4.1.1 Realistic Electric Power Grid Models

The simulation of electric power grids requires a specification of a topology of the grid along with generation and loads. Topologies show how the generators and loads are connected to one another. Basic building blocks of these topologies are buses where conductors (e.g., power lines) connect to one another. Models of electric power grids model the state of the grid (e.g., voltage) at each of these buses and power flow between the buses. Power generation/consumption for generators and loads must be specified, as well as other attributes such as the resistance of the conductors.

Electric power grids are commonly represented in one-line diagrams, which are schematics that illustrate the three-phase power system (which requires three separate conductors) as a single line. One-line diagrams can be combined with Geographic Information Systems (GISs) if the components of the diagrams are given geographic attributes. For example, PowerWorld software (Section 4.2.3) can combine geographic maps and one-line diagrams to show where generation and transmission equipment is located, which could be advantageous when assessing the consequences of power failures on other connected infrastructures.

4.1.2 Models of Actual Power Grids

While standardized power grids such as IEEE RTS-96 are useful for experimenting with cyber-attack scenarios, models of actual power grids would be more useful for assessing the consequences of cyber attacks on actual infrastructures and economies.

These models can be constructed from scratch using information such as Federal Energy Regulatory Commission (FERC) 715 filings, which have been Critical Energy Infrastructure Information (CEII) since 2001. They contain power-flow data for any utility that operates transmission facilities that are above 100 kilovolts (kV).

Models may also be obtained from commercial vendors. Energy Visuals ([17]), which is a partner of PowerWorld ([18]) (Section 4.2.3), maintains the Transmission Atlas. The atlas contains models of real electric power grids that are compatible with PowerWorld. Besides containing data about topologies, these models contain geographic information about the components of the grids. Data were originally created using FERC 715 filings and have been updated with models obtained from regional reliability councils and independent system operators (ISOs). The atlas contains all buses, substations, transmission lines, generators, and loads that exist in those models.

Platts ([19]) is another source of data about electrical power grids that is currently incorporated into the FAIT (Section 3.1.3.3). GIS data, which includes power plants, transmission lines, substations, and transmission line taps, is available from Platts ([19]), with quarterly updates. While the Platts data are comprehensive, they are not in a format that can be easily used by power system models, and Platts does not contain data that are necessary to use those models. Most notably, Platts does not contain information about loads nor does it contain information about generators’ reactive power. The GIS data could be useful when combined with other data sources.

4.1.3 Critical Energy Infrastructure Information (CEII)

CEII is a classification maintained by the FERC that is similar to the DHS PCII classification. The FERC website provides the following definition for CEII ([20]):

CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

- Relates details about the production, generation, transmission, or distribution of energy;
- Could be useful to a person planning an attack on critical infrastructure;
- Is exempt from mandatory disclosure under the Freedom of Information Act; and
- Gives strategic information beyond the location of the critical infrastructure.

Access to CEII is not as restricted as access to PCII. Individuals can request access to CEII data and must complete a nondisclosure agreement to obtain the data. FERC staff verifies that requesters have a legitimate request and do not pose a security risk. Requesters are verified for the remainder of the calendar year. Individual requesters can also request CEII access on behalf of an entire organization.

4.2 Models of Electric Power Grids are Limited

The VCSE steady-state electric power model used in the walk-through (Section 3.1.3.1) does not model the dynamic behavior of the power system, which may suppress power grid behavior that may be targeted by cyber attacks. Sandia is presently developing dynamic power models; however, their complexity may pose a barrier to using them with large, complex models of power grids.

While the VCSE steady-state model currently works with the IEEE RTS-96 power grid, two other steady-state power grid models (PowerWorld and the Interdependent Energy Infrastructure Simulation System) use models of real power grids.

4.2.1 Virtual Control Systems Environment (VCSE) Transient Power Simulator

One disadvantage of the VCSE steady-state model is that it assumes an immediate transition between steady states, which is unrealistic. This is especially the case when analyzing the effects of cyber attacks that affect the dynamic operation of the electric power system. For example, an attack may target the frequency of the AC system, which is a dynamic behavior of AC generators and transmission equipment.

The transient power simulator is being developed at the Missouri University of Science and Technology in cooperation with Sandia. It is a more realistic representation of the response of the power grid accounts for gradual changes between the steady states. The transient power simulator uses differential equations, which is the most common method of dynamically modeling a power system. For each generator, one equation models the speed rotor of the generator and one equation models the speed governor, which tries to keep the system frequency at 60 hertz (Hz). Two constraints for each bus in the system ensure that the net power and reactive power flows through the bus are zero.

The simulator is written in Matlab, but can interact with the VCSE by converting the Matlab model into C++ code or by using Matlab's API. Because C++ code is optimized during compilation, it runs much more efficiently and can be run at real-time. However, the Matlab code is easier to modify. Nevertheless, a very large scale differential equations model, as would be required to model a real electric power grid, would likely be computationally infeasible due to the high computational demands of nonlinear differential equations models.

4.2.2 Finite-State-Machine (FSM) Representation of Dynamic Power System Behavior

The VCSE transient power simulator models electric power grid dynamics using nonlinear differential equations. Unfortunately, power systems can be modeled by many nonlinear equations for a single generator. (The transient power simulator uses two, but many more are possible if assumptions are relaxed.) Combining many generators, plus loads, control systems, and other components of an electric power grid leads to an intractable system of nonlinear differential equations.

A possible solution to this intractability is the use of graph-based methods. Finite-state-machine (FSM) methods are graph-based methods that descretize the continuous-time behavior of the power system to make the problem computationally tractable. Nodes of the graph represent states of the system, while lines between the nodes represent transitions between the states. Graph-based methods such as FSM are commonly used in the design of microprocessors, which may have billions of transistors.

The FSM model currently uses two relatively simple models of electric power grids. The simple model uses 2 buses, while another model (still under development) uses 20 buses. Preliminary analysis of the FSM models suggests that the models are valid and that the simple model demonstrates the correct dynamics ([11]). Because the FSM model is in its infancy, it is uncertain whether it can scale up to be able to simulate real electric grids. The FSM model does not currently interface with the VCSE, but the transient power simulator has proven that the VCSE can interface with dynamic models.

4.2.3 PowerWorld Simulator

PowerWorld Simulator ([18]) is a commercial software package, which can interface with the VCSE, for simulating steady-state electric power grids. This graphical user interface (GUI)-based software allows users to visualize and solve high-voltage power grids that have up to 100,000 buses. The simulator allows analysis at different levels of detail. For example, individual buses can be analyzed or the system can be viewed at a level that is aggregated to separate control areas and interconnections among those areas. One of PowerWorld's strengths is the ability to perform “what if” scenarios and analyze them graphically in a way that makes the results understandable to a nontechnical audience.

A partner company called Energy Visuals ([17]) produces the Transmission Atlas, which provides data on the location and topology of components of real power grids. Data are based on annual FERC 715 filings, but have been expanded from additional sources. These data can be used within the PowerWorld Simulator to analyze power systems or provide geographical visualization of the locations of power grid components.

PowerWorld has developed several extensions to the Simulator that may be useful for analyzing the infrastructure impacts and economic consequences of cyber attacks on the power system. The Optimal Power Flow tools determine locational marginal prices (LMP) at each bus. When combined with the Simulator, changes in prices due to changing system conditions (such as power outages) can be analyzed over time. The SimAuto extension allows the program to interface with programs that support component object model (COM) compatibility. Interfaced programs (such as the VCSE) can run the Simulator and access results. The Retriever can be used to create simulations using historic or real-time data (e.g., Energy Management System [EMS] data).

PowerWorld appears to be a promising method to construct infrastructure-impact scenarios. It can easily use models of real power grids. It has the ability to solve very large power grids. It is also integrated with the VCSE, which means that the system effects and infrastructure-impact steps are seamlessly integrated, similar to how the VCSE steady-state model is currently integrated. PowerWorld’s chief downside is that it is not a dynamic model.

4.2.4 Interdependent Energy Infrastructure Simulation System (IEISS)

The Interdependent Energy Infrastructure Simulation System (IEISS) ([21]) is a system that has been developed by the NISAC group at Los Alamos National Laboratory. It models both electric power grids and the natural gas transmission systems. It also models the interdependencies between the two systems. For example, many generators use natural gas as their fuel, and natural gas pipelines have electric powered compressors to maintain pressure.

The power simulator has a number of different algorithms to solve for the steady state of the grid. Like PowerWorld’s Optimal Power Flow tools, the IEISS can also solve for the optimal dispatch of generators and optimal load-shedding schemes when generation is unable to meet loads. The natural gas component of the IEISS has a similar ability to solve for the physical state of the system, the optimal dispatch of resources, and optimal load-shedding.

Data within the IEISS have geographic attributes, which means that the locations of the power and natural gas resources are known. The IEISS has a service and outage area module that estimates service areas for known delivery points on both the power grid and the natural gas distribution network. The estimation of service areas allows the analysis of the consequences of disruptions to infrastructure. Therefore, the IEISS is not only a tool for assessing impacts at the electric power infrastructure level, but it also can be used to assess the consequences of those impacts on other infrastructures. For example, the IEISS is able to identify facilities, such as hospitals and police stations, within the outage areas.

The IEISS can be used within the cyber-attack-consequence assessment process to construct a more complete infrastructure-impact scenario. While the other power grid models mentioned in this section would need to be used with another tool, like FAIT, to assess the impact of electric power disruptions, IEISS can be used alone to assess many of these impacts. Like PowerWorld, the IEISS can solve very large power grids, and it shares the downside of being a steady-state simulator. Although, PowerWorld is integrated with the VCSE while the IEISS is not, it is likely that the flexibility of the VCSE would allow the two tools to be integrated, which could facilitate the integration of the system effects and infrastructure-impact steps of the process.

4.3 Economic Models are Limited

The REAcct methodology, which was discussed in the walk-through of the cyber-attack-consequence assessment process, is coarse due to the use of limiting assumptions. First, REAcct assumes that economic activity is spatially evenly distributed across a county. For example, if a disruption covers 5 percent of the area of a county and disrupts 50 percent of economic activity, REAcct assumes that 2.5 percent of economic activity is disrupted. However, if the county is sparsely populated, most economic activity could fall within the 5 percent of the county that receives the disruption. In this case, the parameters used by REAcct as inputs should be adjusted to reflect the uneven distribution of economic activity.

Second, REAcct calculates losses in gross regional product and income by assuming that all workers across the country have the same productivity. Data on county employment per industry are multiplied by average national productivity to generate estimates of gross regional product in each county. Because worker productivity varies by county, these estimates contain a degree of inaccuracy.

Third, the REAcct methodology is only valid for interruptions that last from about a week to a month. Depending on the nature of the disrupted asset, only some economic activity in an affected area may be lost. For example, a temporary power outage would not significantly affect businesses that had sufficient backup generation, nor would it significantly impact manufacturers who can continue to meet demand with on-site or in-transit inventories.

Finally, REAcct assumes little about how the economy will adjust structurally to the disruption which may change the multiplier effects. For example, firms outside the disrupted area may pick up the slack in supply caused by the disruption, former suppliers to the disrupted firms may find new customers, and workers in the disrupted areas may move to find employment. More sophisticated economic models and tools which capture many of these long-term adjustment effects, such as the Regional Economics Models, Inc. (REMI), model, are more appropriate than REAcct for assessing long-term economic consequences that involve structural adjustments.

The following sections discuss some other economic consequence assessment tools that are in use or under development at Sandia. Many of these fill gaps that exist in the use of REAcct. Most of these tools are more complex than REAcct, and many have drawbacks.

4.3.1 Consequence Modeling Tool

The Consequence Modeling Tool (see [12]) is being developed by NSTB to help stakeholders, such as utilities, assess the consequences of a cyber attack. The consequences that are assessed are specific to stakeholders rather than generalized to the entire economy. The four categories of consequences are economics (the costs to the stakeholder itself), image (fallout from unhappy customers and politicians), health and safety (dangers to workers and the public), and environment (damage to fauna). Consequences can be rated numerically and weighted to allow stakeholders to prioritize cyber defense mitigations to high priority risks.

Because the tool focuses on the costs of cyber attacks to stakeholders, it is not directly applicable to assessing the consequences of cyber attacks to an entire economy. However, the tool can provide an example of how a number of different types of consequences can be assessed together. REAcct, as well as the other tools mentioned in this section, measures a narrow set of economic consequences. The modification of the Consequence Modeling Tool could enable hard-to-measure consequences to be included in an economy-wide consequence assessment.

4.3.2 Regional Economics Models, Inc. (REMI)

The commercial software, REMI ([22]), used by NISAC at Sandia, as well as widely across the United States, is modeling software that estimates the long-term macroeconomic impacts of disruptions. Like REAcct, REMI is based at the county-level and uses input-output methodology to establish the links between different sectors of the economy. Pure input-output models do not account for prices of structural changes in an economy because the model is based on the accounting of observed flows between industries and counties. Changes in economic activity are a result of changes in final demand, which are exogenous. REMI augments an input-output model with general equilibrium methodology, which is a more traditional economic methodology where prices, production, consumption, etc., adjust to clear markets (i.e., supply equals demand). Underlying equations are estimated econometrically with historic data. Therefore, REMI is also able to model prices and changes in behavior that result because of price changes, and it better simulates long-term changes in an economy.

REMI is more flexible than REAcct, allowing users to simulate the economic consequences of a wider set of disruptions, such as labor shortages caused by a pandemic, loss of international trade caused by a port closure, or economic consequences of a power outage that affected only a certain industry. However, REMI takes more time than REAcct to compute estimates; so across-the-board, medium-term disruptions (weeks to a months) can be handled in REAcct in much less time, and with greater ease.

Because REMI software is customized for each customer, interfacing the software directly with other programs, such as the VCSE, may be difficult. Nevertheless, scenarios in REMI could be built to correspond to forecast changes in infrastructure that may result from a threat, as is the current practice in NISAC.

Most of the infrastructure-impact scenarios for electric power are likely to be short- or medium-term, thus REMI may not be a major improvement in the analysis. Nevertheless, long-term disruption scenarios can conceivably be constructed in electric power and other infrastructures; and in these cases REMI may improve markedly on the modeling done by REAcct.

4.3.3 NISAC Agent-Based Laboratory for Economics (N-ABLE™)

The NISAC Agent-Based Laboratory for Economics (N-ABLE™) is an agent-based economic simulation tool ([23]). It models the economy using thousands to millions of synthetic firms (called "EconomicAgents") to create a high-fidelity simulation of national and regional value chains and market dynamics. Each synthetic firm is an enterprise with buyers, production supervisors, sellers, and strategic planners who interact with each other within and across enterprises. These economic firms (along with households and government actors) interact with one another through infrastructures and markets. EconomicAgents are individually tailored with public and industry data to represent different types of agents. Firms in different industries, for example, will have different production functions and different buying and selling behavior. N-ABLE™ uses stochastic, Markov processes to model the system. N-ABLE™ currently includes models of the chlorine, dairy, petrochemical, and manufactured food sectors.

EconomicAgents in N-ABLE™ rely upon specific infrastructures, like transportation, to interact with each other and rely on other infrastructures, like electric power, to operate. Infrastructure in N-ABLE™ can be modeled within the simulation or interfaced externally. Electric power has been modeled using a dynamic systems model of California's energy systems (see Section 4.3.4) and the Electricity Market Complex Adaptive System (EMCAS) model—an agent-based model of competitive electricity markets developed by Argonne National Laboratory. Several N-ABLE™ projects have analyzed electric power ([24]). One project analyzed how some chemical producers on the Gulf Coast responded to a 3-day to 8-week regional power outage. Use of N-ABLE™ allowed analysts to see that even shorter term power outages resulted in permanent economic losses to power companies and the economy at large due to constraints in production and transportation capacity.

N-ABLE™ produces high fidelity simulations that provide results and insights that are of much greater fidelity than those produced by REAcct. N-ABLE™ is limited, however, to a small set of industries that are currently modeled. Therefore, N-ABLE™ would be useful for assessing the economic consequences of an infrastructure-impact scenario in some industries, but would be unable to provide assessments for most industries without building new models, which is a lengthy process. If N-ABLE™ were used to provide some assessments, tools such as REAcct would be necessary to assess the consequences in other industries. Furthermore, because N-ABLE™ is agent-based, it is computationally intensive and compared to REAcct and REMI, takes a long time to compute impacts.

4.3.4 Dynamic Systems Modeling

The Dynamic Infrastructure Interdependency Simulation and Analysis (DIISA) team at NISAC develops dynamic models in response to requests from DHS. DIISA products are analyses rather than tools ([25]). Dynamic systems modeling attempts to understand complex, nonlinear systems (such as the economy) by examining the flows between interdependent pieces of the system that cause feedback loops. Additionally, stocks (such as inventories) are modeled. The building blocks of these models are the individual actors. Typically, simple equations describe the behavior of these actors. For example, a manufacturer may make decisions on production and inventories based upon the demand from consumers. The models assemble the actors to show how their flows interact with each other, which means that dynamic systems models are enlargeable.

Current modeling at DIISA focuses on natural gas, telecommunications, petroleum, and port operations. Previous efforts looked at energy interdependencies in the Western Electric Coordinating Council (WECC) ([26]), which covers North America's western electric power grid. In those models, supply and demand at state/provincial-level aggregates (except for California, which was previously modeled at the ISO level) were modeled for a number of industries including electric power, natural gas, fuel, and water. The model allows analysts to answer a number of questions about what is driving the observed behavior. For example, critical pieces of infrastructure can be identified whose restoration, in the event of an outage, should be prioritized.

Dynamic systems models that include electric power, such as the WECC model, can be used with an infrastructure-impact scenario to develop in-depth economic consequence assessments. However, the models are not comprehensive, thus they will only model a portion of the economic consequences. Like N-ABLE™, dynamic systems models would need to be augmented by a more comprehensive, but lower fidelity, economic consequence tool, such as REAcct.

This page intentionally left blank.

5 EXTENSION OF THE CYBER-ATTACK-CONSEQUENCE ASSESSMENT PROCESS TO OTHER INFRASTRUCTURES

This report focuses on Sandia's capabilities in carrying out the cyber-attack-consequence assessment process using electric power control systems as an example. The process can be used with other critical infrastructure control systems with modifications to existing capabilities and the addition of infrastructure-impact simulations for new infrastructures.

Of the three steps of the cyber-attack-consequence assessment process focused upon in this report, the systems-effects step and the infrastructure-impact step need to be modified from the electric power walk-through of Section 3. For the final step (economic consequence assessment), the REAcct tool can continue to use the same type of infrastructure-disruption scenario as an input (i.e., specifications of which counties are affected, how long the disruption lasts, what fraction of their area is affected, and what fraction of economic activity is disrupted) provided the necessary mappings of infrastructure disruptions to economic disruptions are made. Many of the economic assessment tools that filled the gaps of REAcct are similarly flexible or can include new infrastructures by expanding their models.

This section provides a general explanation of how the electric power walk-through for the systems-effects step and the infrastructure-impact step would need to be modified to accommodate infrastructures other than electric power.

5.1 System Effect

The process walk-through detailed methods and tools that can currently be used to simulate a cyber attack on an electric power control system and assess the impacts to the electric power grid. Although these tools are tailored to the electric power industry, some tools, such as the VCSE, can be modified to different infrastructures. Other types of physical infrastructure can be simulated by either interfacing existing tools with the VCSE or creating new tools.

5.1.1 Virtual Control Systems Environment (VCSE)

The VCSE (Section 3.1.2.2) is a flexible environment for simulation of control systems. While most current work in the VCSE addresses electric power control systems, control systems for other infrastructures can also be simulated. New infrastructures may require new simulators to be created and added to the VCSE library that represent components of the new control systems or methods of cyber attack (much like the addition of the rogue software attack simulator in the workshop scenario). Actual components of control systems in other infrastructures can also be interfaced with the VCSE, just as real components of electric power control systems can currently be interfaced.

New tools can be written as VCSE plug-ins in the C++ language, communicating through the VCSE's API. Existing tools with a public API can be integrated with the VCSE by creating an adaptor that plugs into the VCSE and allows the two tools to communicate.

5.1.2 OPNET Technologies, Inc. (OPNET®) Modeler

Networks and network traffic in the VCSE can be simulated with the OPNET Technologies, Inc. (OPNET®) Modeler. In the case of electric power, the simulated network connects the FEP to the RTUs, which are connected to the generators. Other infrastructures that are subject to cyber attacks are likely to use networks that can also be simulated using OPNET® Modeler.

5.2 Infrastructure Impact

The infrastructure-impact step of the process maps changes in critical infrastructure control systems that are caused by cyber attacks to overall changes in infrastructure. The tools necessary to assess the infrastructure impact of cyber attacks will vary depending on the infrastructure being simulated, especially for infrastructures that have complex interdependencies among components. Thus, models of the specific infrastructure will be useful for developing a detailed and reliable infrastructure-impact scenario that shows how cyber attacks against a control system affect an infrastructure.

The following sections discuss how tools used to assess infrastructure impacts in the electric power walk-through and other strategies can be used to assess impacts in other infrastructures.

5.2.1 Fast Analysis and Simulation Team (FAST) Analysis Infrastructure Tool (FAIT)

FAIT, which was originally discussed in Section 3.1.3.3, is essentially a database that contains heuristics about connections among components of infrastructure. Analysts may use the information about infrastructure relationships—especially interdependencies among different types of infrastructure—to develop infrastructure-impact scenarios that detail how control-system effects lead to infrastructure impacts.

The information in FAIT is limited, especially when cyber attacks will lead to a detailed change in the state of the infrastructure. For example, a cyber attack against a natural gas pipeline control system might affect how a specific compressor works. The changes in this compressor might affect attributes such as pipeline pressure, but assessing these changes would require a specific model of pipelines. In this case, FAIT does not have the information or the tools necessary to model the state of the infrastructure. Higher fidelity modeling of infrastructure impacts will require specific infrastructure models.

While current associations in FAIT are at the asset level (e.g., the assets that are associated with a specific power plant), development is underway to define relationships at the infrastructure level. Additionally, associations will be sensitive to the type of interruption. For example, the consequences of the loss of a single generator in a cyber attack are likely much less than the consequences from the loss of many generators. Associations will also be sensitive to the timing of the threat.

5.2.2 Interdependent Energy Infrastructure Simulation System (IEISS)

As mentioned in Section 4.2.4, the IEISS simulates both electric power and natural gas distribution. In addition, the Water Infrastructure Simulation Environment (WISE) ([27]) is an analytic framework for modeling the water infrastructure (e.g., water treatment, wastewater). Interdependencies with electric power and natural gas distribution in urban areas can be modeled using the IEISS water extension.

If IEISS is used for assessing the impacts and consequences of cyber attacks to electric power, it would be straightforward to extend it to both natural gas distribution and water. Because both infrastructures already operate within IEISS, additional effort could be focused on modeling natural gas distribution or water control systems.

IEISS has shown itself capable of extensions to other infrastructures, thus providing a framework for analyzing infrastructures such as telecommunications, petroleum, and chemicals.

5.2.3 Commercial Software

Like the other infrastructure models, the PowerWorld Simulator is written specifically for modeling electric power. Other commercial infrastructure models could be interfaced with the VCSE in a similar manner to perform simulations of how cyber attacks on the control systems of those industries affects the actual infrastructure.

Many other infrastructures will not require a model that is as extensive or powerful as PowerWorld due to the greater isolation of other infrastructures and decreased complexity. For example, sewage treatment is performed locally, not nationally like electric power.

5.2.4 Matlab

Matlab is a numerical computing environment that is popular with engineers. Matlab can interface with the VCSE either by converting the Matlab code into C++ or using Matlab’s API. Just as the VCSE transient power simulator was created using Matlab to simulate an electric power grid, Matlab can be used to simulate other infrastructures and interfaced with the VCSE.

5.3 Economic Consequence

As mentioned earlier, the economic consequence tools are very flexible and can accommodate a variety of infrastructures, provided that the infrastructure-impact scenario can be mapped to a specific economic disruption. This mapping may be more difficult in infrastructures other than electric power. Most economic activity is highly dependent on electric power, but the same cannot be said for many other infrastructures. For example, a cyber attack on water treatment that resulted in a boil order would likely be more of an inconvenience than an event that halts all economic activity. In the extreme case of an infrastructure impact scenario where all water service was disrupted for a municipality, all economic activity would not be halted; much economic activity does not require water, and there are many common, alternative ways of obtaining water (such as wells).

More detailed economic consequence models, such as N-ABLE™, may be able to better model infrastructure disruptions that lead to more subtle economic disruptions than do interruptions in electric power. Heuristics can be used (or developed) to aid REAcct in mapping an infrastructure disruption to an economic disruption.

6 RECOMMENDATIONS FOR PROCESS EXTENSIONS

The walk-through of the cyber-attack-consequence assessment process in Section 3 showed how the process can be easily applied to electric power. Section 4 explained how some of the gaps in the process for electric power can be closed. This section discusses two extensions that can better integrate the different steps of the process.

The first extension uses probabilistic modeling, which is currently being used for reliability analysis of electric power, to assess economic consequences. The second extension more fully integrates the final three steps of the process at the software level by interfacing various tools so that the process can be conducted more efficiently.

6.1 Probabilistic Modeling

Critical infrastructures consist of complex engineering systems with many components. All of these components can fail, but the failure of individual components does not necessarily mean that the entire system will fail. A system, or parts of the system, is more likely to fail completely when multiple components fail at once.

Probabilistic analysis using Monte Carlo simulation is often used in reliability engineering (e.g. [28]) to assess the reliability of the system. The most basic simulation assumes that all components fail at random independently of one another. The failure of individual components of the system can be simulated by assuming a probability distribution for the failure of that component and drawing random numbers to determine whether the component has failed. For example, the exponential distribution is assumed if it is believed that a component has an equal chance of failing at any given time. Thus, failure of a component could be simulated when a randomly drawn number was below a given threshold during a specific period.

The exponential distribution has one parameter that must be specified for each component. The mean time to failure (MTTF) is, on average, how long a component will operate until it fails. If the recovery time of a component is also assumed to follow the exponential distribution then another parameter—the mean time to recovery (MTTR)—must also be specified.

At each step, the state of the system is recalculated to reflect failures of individual components. Metrics about the state of the system are recorded. For example, in an electric power grid, the state of a bus (whether or not it is receiving power) could be recorded. After simulating the system for a long time, the recorded metrics can be analyzed to determine overall reliability. Because the Monte Carlo simulation operates over a long time, the results are most useful for determining the long-term costs of failures in the system.

6.1.1 Electric Power Reliability Analysis

While Monte Carlo simulation is often used to assess the reliability of electric power, the vulnerabilities that exist because of possible cyber attacks are usually ignored. Sandia has developed a methodology for performing reliability analysis on electric power systems that accounts for failures in electric power control systems caused by cyber attacks (see [11]). The failure of the control systems due to attacks is acknowledged with the assumption that cyber attacks will occur randomly throughout time and with equal probability. Rather than specifying the MTTF, each control system has a mean time to (successful) attack (MTTA). To simulate cyber attacks that are coordinated against a number of control systems (such as in the scenario in the *National SCADA Test Bed Threat Development Team, Threat case scenario* [7]), a parameter that indicates the percentage of affected systems can also be specified.

To simulate impacts of cyber attacks, the topology of the electric power grid must be specified. The probabilistic analyses currently being performed assume the IEEE RTS-96 model (Section 3.1.3.2), but other specifications are possible. For example, the analysis could use a representation of a real grid.

For each time period the state of each component is determined using random numbers, then the state of the entire grid is calculated using the steady-state, load-shedding model discussed in Section 6.1.2. After metrics for the grid are recorded, the simulation moves to the next time period when the random numbers are again generated to determine the status of the components, and the state of the entire grid is recalculated. After a sufficiently long simulation, summary measures of the metrics can be recorded. For example, “Impact Analysis from Cyber Intrusion for Electric Power Systems” [11] calculates the mean number of megawatt-hours (MWh) of load that are unserved every year due to the cyber attacks by simulating the system for a large number of years, summing the total MWh or unserved load, and dividing by the number of years.

6.1.2 Electric Power Reliability Analysis: Steady-State, Load-Shedding Model

In the probabilistic analysis of an electric power system, the state of the electric power grid is solved whenever there are changes in the status of any component of the system. To solve for the steady-state solution to the system, a steady-state model is used that uses a similar methodology as the steady-state plug-in for the VCSE (Section 3.1.3.1); however, this model does not interface with the VCSE. This program is written in the Ruby programming language. Like the previous steady-state model, it uses a Newton-Raphson iterative method ([9], Section 3.8.1). The program invokes PowerWorld’s (see Section 4.2.3) Optimal Power Flow tool, which determines the optimal way to restore or minimize load loss given physical and regulatory constraints. The use of the Optimal Power Flow simulates the operators of the system who will respond to outages caused by the cyber attack.

This tool is currently slow because it has not been optimized. While speed is not critical when using the IEEE RTS-96 model, it could be a bigger issue when simulating a real grid with a large number of buses.

6.1.3 Extending the Electric Power Reliability Analysis to Economic Consequence Analysis

While the probabilistic analysis methodology used in "Impact Analysis from Cyber Intrusion for Electric Power Systems" [11] does not currently assess the consequences of cyber attacks to other infrastructures and the economy, this extension is straightforward if a real electric grid with historic loads is used to model the system-wide impact of cyber attacks and dependencies on the components of the grid are known. For example, if it is known that a manufacturing facility was connected to a certain bus, the average amount of time each year that the facility is without power could be calculated by monitoring the status of the bus. Furthermore, using knowledge about interdependencies of other infrastructures to individual buses would enable economic costs to be calculated throughout the simulation, thus providing another metric that could be analyzed.

If a representation of a real electric grid is not used, economic consequences could be simulated in a fashion similar to the walk-through, although some automation would be necessary to enable the Monte Carlo process to operate efficiently. For example, heuristics about the cost of electricity outages could be used to automatically assign economic consequences to outages based on the lengths of the outages (see [16]).

The reliability analysis is unconnected to the VCSE. Control system effects found through simulation in the VCSE can be used to inform the inputs for the model; i.e., MTTA, MTTR, and the fraction of components that are affected by the cyber attack. Unfortunately, these variables are rather limited and do not reflect the variety and complexity of cyber attacks and their possible effects. However, an advantage of this type of reliability analysis is that it is relatively simple to map cyber attacks to economic and infrastructure consequences.

6.1.4 Extension to Other Infrastructures

Extending probabilistic analysis to other infrastructures is relatively straightforward if another infrastructure simulation tool is used in the same manner as the steady-state, load-shedding model in the electric power reliability analysis. The Monte Carlo analysis would determine, in each time step, the status of each component (using MTTA and MTTR parameters that were informed by the system-effect step of the process) and calculate the state of the system using the infrastructure simulation tool. Economic consequences could be incorporated in analysis of infrastructures, using heuristics about the economic costs of outages in the other infrastructures.

6.2 Full Integration of Process Steps/Tools

A long-term goal may be to fully integrate the system-effect, infrastructure-impact, and economic-consequence steps of the process. Full integration might consist of a single user interface to conduct all three steps simultaneously using tools that are interfaced.

The system-effect and infrastructure-impact steps of the process are already interfaced for electric power using the VCSE. The VCSE simulates the control system, but also interfaces to electric power grid models, which allows it to assess how a cyber attack affects control systems and how those effects propagate throughout the electric power grid. Furthermore, implementation of probabilistic analysis for economic consequences would likely require the infrastructure-impact and economic-consequence steps to be formally integrated so that Monte Carlo analysis could run quickly.

The following sections discuss how specific, previously mentioned tools can be integrated.

6.2.1 Virtual Control Systems Environment (VCSE)

Because the VCSE acts as glue that links many components together in a simulation, it should be relatively straightforward to link software that assesses economic consequences. Infrastructure impact tools such as the steady-state, load-shedding model map changes in individual components to changes in an entire electric grid. Likewise, economic analysis software could be integrated into the VCSE to map the changes in the entire electric grid to economic consequences. Intermediate software could also be integrated into the VCSE that maps changes in one infrastructure, such as the electric grid, to many infrastructures.

6.2.2 Regional Economic Accounting (REAcct)

REAcct could be used in the fully integrated process to assess economic consequences. The VCSE could be used to simulate the system effects of the cyber attack and calculate the new system state, thus forming an infrastructure-impact scenario. Software to interface REAcct to the VCSE could map this scenario to detailed economic disruptions by county, which would be inputted into REAcct to produce estimates of economic consequences. For example, VCSE would use an infrastructure-impact tool to produce an infrastructure-impact scenario like that in Figure 2, and the interface between the VCSE and REAcct would be responsible for translating it into an input like Table 2.

REAcct would be a good candidate for Monte Carlo analysis—and integration, in general—because it is a fast and simple program. Therefore, it can be run repeatedly with a relatively small computational burden, unlike other tools like N-ABLE™ (see next section).

6.2.3 NISAC Agent-Based Laboratory for Economics (N-ABLE™)

The ability of N-ABLE™ to interface with other simulations was demonstrated in an LDRD in 2005 ([29]). A process that emulated N-ABLE™ was interfaced with Biological Decision Analysis Center (BioDAC), a crisis management simulation for biological weapons of mass destruction developed at Sandia in California. The Interoperable Distributed Simulation (IDSim) framework, which was developed at Sandia and the Georgia Institute of Technology, connects the N-ABLE™ and BioDAC engines over a network. The two simulators communicate with each other using extensible markup language (XML) through the IDSim framework. Collaboration between users using the two simulators was enabled through the use of

GroupMeld, which is a Java GUI developed at Sandia. GroupMeld's capabilities allow collaborating users to chat, share screen images, and share a whiteboard.

GroupMeld is an example of how different tools can be integrated in a single user interface. This interface, or something similar, could be used to integrate the different tools that accomplish the various steps of the process. N-ABLE™ can be integrated with the VCSE in the background by combining the IDSim framework with a VCSE plug-in.

This page intentionally left blank.

7 CONCLUSIONS

Process Control Systems (PCS) such as supervisory control and data acquisition (SCADA) systems are systems of computers that are used to monitor and control many critical infrastructures. These control systems are increasingly vulnerable against cyber attacks. The effects of cyber attacks on control systems can be severe enough to disrupt an infrastructure. While Sandia currently has capabilities to assess the effects of these attacks on control systems and assess the impacts on the infrastructure, there is no process for linking these effects and impacts to the economic consequences that result from infrastructure disruptions.

This report develops a cyber-attack-consequence assessment process to coordinate Sandia's capabilities in assessing the control system effects of cyber attacks, the impact of the effects to infrastructures, and the economic consequences of these impacts. A walk-through of this process is conducted to show how the steps can be accomplished quickly using electric power as an example. Electric power is chosen to be an example due to Sandia's expertise in modeling electric power control systems. The final three steps of the process are detailed in the walk-through; it is assumed that a cyber attack and system vulnerabilities have already been identified.

In the system-effect step of the process, Protected Critical Infrastructure Information (PCII) obtained during U.S. Department of Homeland Security (DHS) Protective Security Coordination Division site visits to critical infrastructure sites (stored at Argonne National Laboratories) is used to verify that the cyber attacks have the ability to substantially interfere with the operation of the infrastructure. The Virtual Control Systems Environment (VCSE), which combines real, emulated, and virtual entities, is used to simulate how cyber attacks affect simulated electric power SCADA systems.

The infrastructure-impact step of the process assesses how cyber attacks' effects on control systems lead to impacts across infrastructures. The VCSE steady-state simulator solves for the steady state of power systems by interfacing directly with the VCSE. The Institute of Electrical and Electronics Engineers (IEEE) Reliability Test System-96 (RTS-96) model is used to represent the physical layout of an entire interconnected power grid. The Fast Analysis Simulation Team (FAST) Analysis Infrastructure Tool (FAIT) identifies components of other infrastructures that are dependent upon elements of electric power.

In the economic-consequence step of the process, the Regional Economic Accounting (REAcct) tool is used to measure the total economic losses to the country due to economic disruptions caused by the cyber attack.

While the process walk-through will enable an economic consequence assessment of simulated cyber attacks in electric power, there are several gaps that, if filled, will lead to better estimates of the economic consequences of cyber attacks. This report identifies several of these gaps and recommends solutions using data sources and tools that are available to, in use at, or under development at Sandia.

One of the major gaps is that the electric power infrastructure impact models mentioned throughout this report, such as IEEE RTS-96, use unrealistic power grids. While these grids facilitate the comparison of different cyber attacks' infrastructure impacts, they make it difficult to create a realistic infrastructure-impact scenario that bridges the infrastructure-impact and the economic-consequence steps. Models of real power grids can be obtained commercially from Energy Visuals or Platts, or constructed using Critical Energy Infrastructure Information (CEII) from the Federal Energy Regulatory Commission (FERC).

The limited abilities of the VCSE steady-state simulator used in the walk-through infrastructure-impact step is another identified gap. The VCSE transient power simulator can be used to simulate the dynamic behavior of a power system within the VCSE; however, it is unlikely to be able to simulate large power grids. The Finite-State-Machine (FSM) Representation of Dynamical Power System Behavior is a tool under development that will simulate dynamic behavior and may be expanded to large power grids. PowerWorld Simulator is a commercial package that solves for the steady state of large grids and provides extensive visualization capabilities. The Independent Energy Infrastructure Simulation System (IEISS) solves for the steady state of real power grids and can be used to assess the impact of electric power outages on natural gas transmission systems.

The third gap is the limited abilities of REAcct. The Consequence Modeling Tool is being developed to assist stakeholders, such as utilities, weigh a variety of consequences of a cyber attack. REMI (developed by Regional Economics Models, Inc.) combines the input-output methodology used by REAcct with general equilibrium methods that allow it to simulate long-term economic consequences. The NISAC Agent-Based Laboratory for Economics (N-ABLE™) can be used in high-fidelity simulation of the economic consequences of cyber attacks to several national and regional value chains. Dynamic systems models, created by the Dynamic Infrastructure Interdependency Simulation and Analysis (DIISA) team at NISAC, can be used to analyze the behavior of complex, nonlinear relationships between infrastructures and the economy.

The process walk-through focuses on electric power, but the process can be extended to other infrastructures with the appropriate modifications and substitutions of tools. To conduct the system-effect step of the process for other infrastructures, the VCSE must be customized for other infrastructures. The OPNET® Modeler is a commercial network simulation tool that can be used to model networks used in other infrastructures' control systems. Both FAIT and the IEISS can be used to assess the infrastructure impact of cyber attacks in other infrastructures. However, new infrastructure impact models specific to those infrastructures should be used (or developed if they do not exist) for accurate impact modeling. These models may be obtained from commercial sources or constructed using tools such as Matlab, a numerical computing environment that can interface with the VCSE.

Section 6 recommended two extensions that better integrate the steps of the process. While these extensions would likely require substantial development efforts, integration would make the process simpler and more efficient.

The first extension is the use of probabilistic modeling. Capabilities currently exist to conduct probabilistic modeling of cyber attacks by slightly modifying electric power reliability analysis. The modification uses a steady-state, load-shedding model to calculate the infrastructure impacts of the cyber attacks. The current capabilities can be extended to economic consequences by developing heuristics about the costs of outages or by interfacing existing consequence tools to directly calculate economic impacts for simulated states of the power grid.

The second extension is the full integration of the process steps and tools. Full integration would make analyses more efficient because it would allow all steps to be conducted together to improve the efficiency of the process. The VCSE currently integrates the system-effect step with the infrastructure-impact step by interfacing directly with the VCSE steady-state simulator. These capabilities could be extended by interfacing the tools directly to economic consequence tools. Both REAcct and N-ABLE™ have demonstrated interfacing capabilities that could be used to fully integrate the process.

APPENDIX A: THE THREAT-TO-CONSEQUENCE FRAMEWORK

The threat-to-consequence (T-to-C) framework ([30]) includes the components of a risk assessment of cyber risk to critical infrastructure control systems. The framework is illustrated in Figure 3.

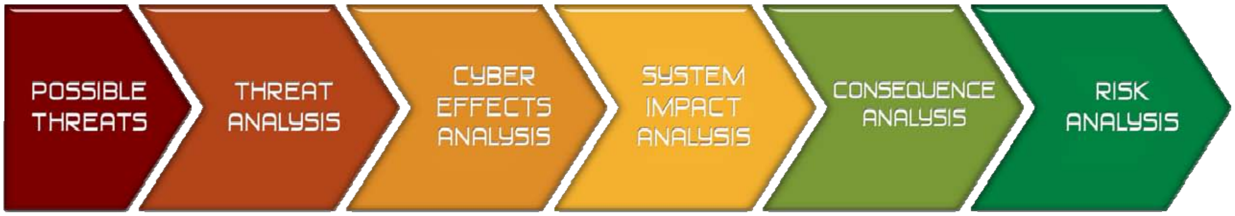

Figure 3: A Conceptual View of the Threat-to-Consequence Framework

Specific tools can be used to conduct each step of the analysis. Tools have been developed (or are under development) that would allow all steps to be completed for a cyber attack on an electric power control system. Conducting the analysis for control systems in other critical infrastructures may require the development of new tools or the modification of existing tools. The various steps of the consequence can be fit together informally or be integrated.

The following sections give an overview of the steps of the T-to-C framework. Capabilities to conduct cyber effects analysis, system impact analysis, and consequence analysis are expanded upon in later sections.

A.1 THREAT

Sandia National Laboratories (Sandia) has developed a threat analysis framework for cyber attacks, which is documented in *A Threat Analysis Framework as Applied to Critical Infrastructures in the Energy Sector* [31]. The first step of the analysis is the identification of the threat. A generic threat matrix is developed in *Categorizing Threat: Building and Using a Generic Threat Matrix* [32] to categorize malevolent threats. This matrix enables the identification of levels of threat in an unclassified environment, thus allowing stakeholders to prioritize mitigation of threats. Furthermore, the matrix gives government agencies the ability to map classified threat information into the unclassified matrix, which can be used to communicate threat information with stakeholders. The threat profiles in the matrix also allow these government agencies to “identify potential attack paths and initial mitigation strategies” ([32] p. 23).

Threats are measured across several attributes in two broad categories. Commitment attributes “quantify the threat’s willingness to pursue its goal” ([32] p. 19), while resource attributes measure “the characteristics of a threat that quantify the people, knowledge, and access available to a threat for pursuing its goal” ([32] p. 20). The attributes of the threat are matched to one of eight sequential threat levels, where Level 1 threats are most capable and Level 8 threats are least capable.

The second step of the threat analysis outlined in *A Threat Analysis Framework as Applied to Critical Infrastructures in the Energy Sector* [31] is the identification of threat attack paths. Identification is facilitated through the use of reference models that describe control systems. Reference models may be specific to a particular infrastructure, but abstract models that may apply to more general classes of infrastructure may be used. The Argonne data described in Section 3.1.2.1 could be used to construct such a reference model. The Virtual Control System Environment (VCSE) described in Section 3.1.2.2 is an example of an implementation of a detailed reference model that can be used to find threat attack paths with high assurance.

The third step of the threat analysis expands on the second step through the generation of a realistic threat scenario. Specific components of the system are analyzed in viable scenarios that may use tangible elements of operation and architecture. Outside experts, such as system operators, help validate the system and receive results of the threat analysis. In the case of electric power, the use of the standardized Institute of Electrical and Electronics Engineers (IEEE) Reliability Test System (RTS)-96 ([10], Section 3.1.3.2) model along with the VCSE could be used to model the impacts of local events on the electricity grid and develop the realistic threat scenario. Tools being developed at Sandia can be used to expand the scenario to other infrastructures and evaluate economic impacts.

Step four of the threat analysis is conducting a real-time vulnerability analysis. Given an attack path, analysts must evaluate the likelihood that an identified threat has identified the vulnerability. To conduct the analysis, *A Threat Analysis Framework as Applied to Critical Infrastructures in the Energy Sector* [31] poses two questions:

- Are any threats discussing aspects of exploiting a specific vulnerability?
- Could the threat find enough information about a vulnerability to develop an attack?

Answers to these questions may be found in open-source data sets, such as the World Wide Web (WWW) or the intelligence community. A suggested repository for WWW research of threats is the Dark Web Portal [33]. A graph-based concept discovery tool (see [34]) uses information on the WWW to assess whether there are adversaries who are interested in exploiting identified threat attack paths and whether these paths are discoverable with available information.

The final step of the threat analysis is the development of protection strategies to mitigate the identified threats.

A.1.1 Effect

A cyber effects analysis can be conducted to assess how a cyber attack that is identified by a threat analysis will affect the attacked control system. The effects of a cyber attack against an electric power control system can be assessed using the tools of the National Supervisory Control And Data Acquisition (SCADA) Testbed (NSTB). The VCSE provides an environment where real and virtual components of a control system can interact, and attacks can be simulated to gauge their effects on the operation of the control system. The VCSE is flexible and can be modified to simulate control systems in other critical infrastructures.

A.1.2 Impact

The next step of the T-to-C framework is assessing the impact that a cyber attack can have on an entire infrastructure. Different components of an infrastructure interact with each other. A disruption in one component caused by a cyber attack may spill over to another infrastructure.

System impacts can be assessed by modeling a collection of components that make up the infrastructure. The results of the effects analysis of the previous section are used to assess how the effects of the cyber attack in one component spill over to affect other parts of the infrastructure.

A.1.3 Consequence

Consequences are the costs of impacts. Consequence analysis maps disruptions to an infrastructure to disruptions across other infrastructures and, ultimately, an overall cost. For the purposes of this report, the overall cost is expressed in economic consequences such as dollars of gross regional production lost; however, other metrics like loss of lives are possible.

There are a variety of consequence analysis tools that are in use at the National Infrastructure Simulation and Analysis Center (NISAC), which is housed (in part) at Sandia.

A.1.4 Risk

The use of the T-to-C framework allows an assessment of risk. Sandia has developed a variety of risk assessment methodologies (RAMs) to calculate the expected loss from attacks ([35]). (One application is to cyber threats to assess the risk of critical infrastructure systems [36]) RAM methodologies use the following risk equation ([35]):

$$\text{Risk} = PA * (1 - PE) * C$$

In this equation, PA is the probability that an adversary will conduct an attack. This quantity is assessed in the threat analysis. PE is the probability that a security system will be effective against an attack, which can be assessed in the analysis of cyber effects. C is the consequence—the loss due to a successful attack. This quantity can be assessed through the impact analysis and consequence analysis of the T-to-C framework.

Risk assessment provides a framework for determining what threats are most important to mitigate. The threats that have the high chances of occurring, high chances of being successful, and may cause extreme consequences should receive the highest mitigation priority. This report enables better risk assessment of cyber attacks to critical infrastructure control systems by better integrating the simulation of consequences of threats to the cyber effects and impacts of those threats.

APPENDIX B: REFERENCES

[1] United States General Accountability Office, “Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,” GAO-07-1036, September 2007.

[2] S. Staniford, V. Paxson, and N. Weaver, “How to 0wn the internet in your spare time,” in *Proc. 11th Usenix Security Symposium*, pp. 149 – 167, 2002.

[3] Eisenhauer, J., P. Donnelly, M. Ellis, and M. O’Brien, “Roadmap to Secure Control Systems in the Energy Sector,” U.S. Department of Energy tech. rep., January 2006, http://www.controlsystemsroadmap.net/pdfs/roadmap.pdf

[4] Kunreuther, H., and E. Michel-Kerjan, “The Economics of Security Externalities: Assessing, Managing and Benefiting from Global Interdependent Risks,” Annual Meeting of the Allied Social Science Associations, New Orleans, Louisiana, January 4 – 6, 2008, http://www.aeaweb.org/annual_mtg_papers/2008/2008_175.pdf.

[5] “National SCADA Test Bed Fact Sheet,” Department of Energy Office of Electricity Delivery and Energy Reliability, November 5, 2007, http://www.oe.energy.gov/DocumentsandMedia/NSTB_Fact_Sheet_11-5-07.pdf.

[6] “NSTB Fiscal Year 2006 Work Plan,” Department of Energy Office of Electricity Delivery and Energy Reliability, November 17, 2006, http://www.oe.energy.gov/DocumentsandMedia/NSTB_Work_Plan__11-17-06__External4.pdf.

[7] “National SCADA Test Bed Threat Development Team, Threat case scenario,” Tech. Rep. SAND2008-2676, May 2008,

[8] “Virtual Control Systems Environment Fact Sheet,” Department of Energy Office of Electricity Delivery and Energy Reliability.

[9] L. Grigsby, J. Harlow, and J. Douglas, *Electric Power Engineering Handbook*, CRC Press, Boca Raton, FL, 2007.

[10] Grigg, C., P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, and C. Singh, “The IEEE reliability test system-1996: A report prepared by the reliability test system task force of the application of probability methods subcommittee,” in *IEEE Transactions on Power Systems*, vol. 14, pp. 1010–1020, August 1999.

[11] Stamp, J., “Impact Analysis from Cyber Intrusion for Electric Power Systems,” Cyber Attacks on Control Systems: Evaluating the Real Risk Workshop, Albuquerque, New Mexico, June 24, 2008, http://www.sandia.gov/scada/workshop_presentations/workshop_presentations.htm.

[12] “NISAC: FAST Analysis Infrastructure Tool,” http://www.sandia.gov/nisac/fait.html, accessed 8/29/08.

[13] Stamber, K., and B. Richardson, “Consequence Modeling and Analysis,” Cyber Attacks on Control Systems: Evaluating the Real Risk Workshop, Albuquerque, New Mexico, June 24, 2008, http://www.sandia.gov/scada/workshop_presentations/workshop_presentations.htm.

[14] Cooperstock, L., M. Ehlen, and V. Loose, “REAcct 1.0: an Initial Methodology for Estimating and Reporting Economic Impacts,” Tech. Report, National Infrastructure Simulation and Analysis Center, October 2006.

[15] New York Independent System Operator, “Interim Report of the August 14, 2003 Blackout,” January 8, 2004, http://www.hks.harvard.edu/hepg/Papers/NYISO.blackout.report.8.Jan.04.pdf.

[16] Billinton, R., S. Kumar, N. Chowdhury, K. Chu, K. Debnath, L. Goel, E. Khan, P. Kos, G. Nourbakhsh, and J. Oteng-Adje, “A Reliability Test System for Educational Purposes—Basic Data,” in *IEEE Transactions on Power Systems*, vol. 4, pp. 1238–1244, August 1989.

[17] Energy Visuals, Inc. “Energy Visuals, Inc.,” http://www.energyvisuals.com, retrieved August 25, 2008.

[18] PowerWorld Corporation, “PowerWorld Corporation, Simulator,” http://www.powerworld.com/products/simulator.asp, accessed August 25, 2008.

[19] “GIS Data from Platts,” Platts, http://www.platts.com/Analytic%20Solutions/Custom/gis/index.xml, accessed August 27, 2008.

[20] “FERC: CEII,” Federal Energy Regulatory Commission, http://www.ferc.gov/legal/ceii-foia/ceii.asp, accessed August 27, 2008.

[21] “NISAC: Interdependent Energy Infrastructure Simulation System," http://www.sandia.gov/nisac/ieiss.html, accessed August 28, 2008.

[22] “The REMI Model,” Regional Economics Modeling, Inc., http://www.remi.com/index.php?page=model, accessed August 29, 2008.

[23] “NISAC Agent-Based Laboratory for Economics,” http://www.sandia.gov/nisac/nable.html, accessed August 29, 2008.

[24] Ehlen, M., and A. Scholand, “Modeling Interdependencies between Power and Economic Sectors using the N-ABLE Agent-Based Model,” IEEE Power Engineering Society General Meeting, June 2005, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1489715

[25] “NISAC Summary of Internal Documentation for Dynamic Simulation Models: Telecom Operations, Natural Gas, National Petroleum, and Port Operations,” National Infrastructure Simulation and Analysis Center, December 21, 2007.

[26] Brown, T., W. Beyeler, S. Conrad, and T. Corbet, Jr., “DOE Office of Energy Assurance Projects FY02 Final Report,” SAND 2002-4140P, November 18, 2002.

[27] “NISAC: Water Infrastructure Simulation Environment," http://www.sandia.gov/nisac/wise.html, accessed August 28, 2008.

[28] Salehfar, H., and S. Trihadi, “Animated Monte Carlo Simulatoin for Teaching Power Generating System Reliability Analysis,” in *IEEE Transactions on Education*, vol. 41, pp. 130-140, May 1998.

[29] Linebarger, J., D. Fellig, P. Moore, M. Goldsby, M. Hawley, and T. Sa, "Integrating Software Architectures for Distributed Simulations and Simulation Analysis Communities," Sandia National Laboratories, SAND2005-6642, October 2005.

[30] Phillips, L., "Using the Threat-to-Consequence Process to Reduce Risk of Cyber Attacks on Critical Infrastructure," Cyber Attacks on Control Systems: Evaluating the Real Risk Workshop, Albuquerque, New Mexico, June 24, 2008, http://www.sandia.gov/scada/workshop_presentations/workshop_presentations.htm.

[31] Duggan, D., and J. Michalski, "A Threat Analysis Framework as Applied to Critical Infrastructures in the Energy Sector," Tech. Rep. SAND2007-5792, September 2007.

[32] D. Duggan, S. Thomas, C. Veitch, and L. Woodard, Categorizing Threat: Building and Using a Generic Threat Matrix, Tech. Rep. SAND2007-5791, September 2007.

[33] University of Arizona, Artificial Intelligence Lab, "Dark Web Terrorism Research," http://ai.arizona.edu/research/terror/index.htm, accessed August 2008.

[34] Colbaugh, R., and J. Michalski, "Threat Analysis," Cyber Attacks on Control Systems: Evaluating the Real Risk Workshop, Albuquerque, New Mexico, June 24, 2008, http://www.sandia.gov/scada/workshop_presentations/workshop_presentations.htm.

[35] DePoy, J., J Phelan, P. Sholander, B.J. Smith, G.B. Varnado, G.D. Wyss, J. Darby, and A. Walter, "A Risk Assessment Methodology (RAM) for Physical Security," White Paper, Sandia National Laboratories, 2005, http://www.prod.sandia.gov/cgi-bin/techlib/access-control.pl/2006/066399.pdf.

[36] DePoy, J., J. Phelan, P. Sholander, B. Smith, G. Varnado, G. Wyss, J. Darby, and A. Walter, Critical Infrastructure Systems of Systems Assessment Methodology, Tech. Rep. SAND2006-6399, October 2006.

DISTRIBUTION LIST

1	MS 0899	Technical Library, 9536 (electronic copy)
2	MS 0123	D. Chavez, LDRD Office, 1011

Sandia National Laboratories