SANDIA REPORT
SAND2008-5954
Unlimited Release
Printed September 2008

Cyber Effects Analysis Using VCSE

Promoting Control System Reliability

Michael J. McDonald, Gregory N. Conrad, Travis C. Service, Regis H. Cassidy

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.

Approved for public release; further dissemination unlimited.

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

SAND2008-5954
Unlimited Release
Printed September 2008

Cyber Effects Analysis Using VCSE

Promoting Control System Reliability

Michael J. McDonald
Effects-Based Studies Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1235

Travis C. Service, Regis H. Cassidy
Networked Systems Survivability & Assurance Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0672

Gregory N. Conrad
Threat Analysis Technologies Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1235

Abstract

This report describes the Virtual Control System Environment (VCSE) technology—developed at Sandia National Laboratories—to investigate Supervisory Control And Data Acquisition (SCADA) vulnerabilities associated with energy systems; and it describes a set of experiments with findings from using that environment. The report explains how VCSE can be used to analyze and develop an understanding of cyber attacks. Specific analyses in this report focus on unencrypted, unsecured data channels on Internet protocol (IP)-routed computer networks within electric power systems.

Acknowledgments

The authors would like to acknowledge that the work, which produced the results presented in this paper, was funded by the U.S. Department of Energy/Office of Electricity Delivery and Energy Reliability (DOE/OE) as part of the National SCADA Test Bed (NSTB) Program.

Special acknowledgements are given to the individuals of the Virtual Control Systems Environment (VCSE) software development team: Brian J. Stinar, Bryan T. Richardson, David Burton, Erik J. Lee, John Mulder, Jonathan Margulies, Mario Urrea, Pengchu Zhang, Ryan P. Custer, and William Atkins.

Executive Summary

Control systems encompass vast networks of interconnected electronic devices that are essential in monitoring and controlling the production and distribution of energy in the electric grid, as well as in the oil and gas infrastructure. While these control systems provide great benefit, they also expose energy systems and their dependent infrastructures to potential harm from malevolent cyber attack [1]. The consequent need to safeguard our energy networks is readily apparent: Any prolonged or widespread disruption of energy supplies could produce devastating human and economic consequences. New tools are needed to uncover and address the vulnerabilities of sophisticated, targeted attacks.

This paper describes the Virtual Control System Environment (VCSE), developed by Sandia National Laboratories as a new and unique way to address many of these needs. VCSE is a system for studying cyber threats on control-system dependent infrastructures. It is a hybrid system to support Simulated, Emulated, and Physical components for Investigative Analysis (SEPIA). More than a particular model or particular set of modeling components, VCSE is best described as a suite of modeling components. It uses simulated, emulated, and physical components for in-depth yet broad-reaching analyses. In describing VCSE, this paper describes tools developed for VCSE analysis, and a variety of analyses performed using it.

This paper describes a variety of tools that have been developed to represent different parts of control systems. In several areas multiple models were developed to represent the same types of parts (e.g., remote terminal units [RTUs], power systems, human-machine interfaces [HMIs] and malware) that may exist in control systems. This paper shows different ways to represent these different parts of the control systems. These multiple representations expose different aspects of the vulnerabilities. In other areas, the same tools were used to model the infrastructure elements at different scales (e.g., the 4- and then 24-bus electric power systems). This scale difference allows the analysts to better understand how threats operate at different scales.

This paper highlights details from several analyses performed using VCSE. Each analysis is focused on understanding the mechanisms used in cyber attacks and the effects that these attacks have upon the systems. In modeling the systems, some cyber threats are represented using functioning malware codes and penetration testing software that has been collected from the Internet. In addition, real HMI monitoring software is used to interface with the control environments. Networks that contain physical and either simulated or emulated network segments are used to represent the control system networks. Simulated RTUs with realistic cyber interfaces are used to represent the control system interfaces. These simulated RTUs interact with simulated power systems (two different power models are used).

VCSE is presently a new and emerging technology. Its toolset library supports a limited number of analyses, yet initial results using VCSE show that the approach is promising and has the potential for allowing analysts to cost-effectively discover, understand, and mitigate control system vulnerabilities that will otherwise be left for our adversaries to exploit. This paper recommends continued investment into expanding and refining the VCSE toolset through an effort that is focused by ongoing relevant studies.

—This page intentionally left blank —

Table of Contents

Table of Figures

Table of Tables

1 Introduction

Control systems form the central nervous system of the North American energy infrastructure. They encompass vast networks of interconnected electronic devices that are essential in monitoring and controlling the production and distribution of energy in the electric grid as well as the oil and gas infrastructure. The ability of these cyber systems to provide automated control over a large, dispersed network of assets and components has helped to create the highly reliable and flexible energy infrastructure that exists today. However, this span of control requires control systems to communicate with thousands of nodes and numerous information systems, thus, exposing energy systems and other dependent infrastructures to potential harm from malevolent cyber attack or accidents [2].

Efforts by the energy sector to uncover system vulnerabilities and develop effective countermeasures have so far prevented serious damage. However, attacks on energy control systems have been successful [3, 4]. The need to safeguard our energy networks is readily apparent: energy systems are integral to daily commerce and the safe and reliable operation of our critical infrastructures. Any prolonged or widespread disruption of energy supplies could produce devastating human and economic consequences.

New tools are needed to uncover and address the vulnerabilities of sophisticated, targeted attacks. Cyber-control systems are characterized by the close interplay between the cyber systems, control systems, operators, infrastructure, and adversaries. It is easy to miss or over-state key vulnerabilities and, consequently, to under- or over-design protections without addressing the bigger picture.

This paper describes the Virtual Control System Environment (VCSE), which Sandia National Laboratories developed as a new and unique way to address these needs. The work reported in this paper results from the Department of Energy Office of Electricity Delivery and Energy Reliability [5] (DOE/OE)-funded studies designed to better understand these cyber vulnerabilities to better implement protections against them. Studies reported here show how VCSE is used to investigate Supervisory Control And Data Acquisition (SCADA) vulnerabilities that stem from using unencrypted, unsecured data channels on internet protocol (IP)-routed computer networks.

1.1 Background

For several years, the DOE/OE has worked to reduce the chances and consequences of malicious cyber attacks that could produce catastrophic disruptions to our critical national infrastructures.

In January 2006 the *Roadmap to Secure Control Systems in the Energy Sector* was published. The Roadmap states the following vision: “In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.” The Roadmap further states challenges to achieving that vision. Among them are the following:

- Limited ability to measure and assess cyber security posture
- Hard to quantify and demonstrate threats
- Possible performance degradation from security upgrades to legacy systems
- Increasingly sophisticated hacker tools
- Poor understanding of cyber risks.

The Roadmap continues by articulating a set of goals. The first Roadmap goal that cyber effects analysis seeks to achieve is to “Measure and assess security posture. Companies should thoroughly understand their current security posture to determine system vulnerabilities and the actions required to address them.” The Roadmap goes on to state, “Within 10 years, the sector will help ensure that energy asset owners have the ability and commitment to perform fully automated security-state monitoring of their control system networks with real-time remediation capability.”

The second Roadmap goal is to “Develop and integrate protective measures.” A key challenge is defined as, “Security upgrades are hard to retrofit to legacy systems, may be costly, and may degrade system performance.”

From this roadmap, DOE/OE developed an overall strategy and instituted a program to meet these goals. The Sandia-developed VCSE technology addresses key technical aspects of both Roadmap goals.

1.1.1 Description

The VCSE toolset will enable collaborative analysis to determine the robustness of a system’s security posture. This is accomplished by performing analyses on the modeled SCADA or control system. VCSE will support the design, integration, and evaluation of security solutions used in legacy systems.

Modeling capabilities, such as the VCSE, are needed to combat the challenging technological complexities associated with securing not only legacy systems but also for the integration of emerging control system components and system architectures. Control system architectures will grow in complexity and interconnectivity with other networks. Control systems will be exposed to more sophisticated threats. Also, there is a trend toward incorporating conventional information technology (IT) solutions into control system networks. As these challenges unfold, asset owners will need modeling and simulation tools to make better-informed decisions in the selection of security solutions for their current and next-generation systems.

The VCSE is a hybrid simulation environment that analysts use to study and analyze cyber threats to—and to assess their effects on—large-scale infrastructures. VCSE uses a mix of real, simulated, and emulated control systems software/hardware components in a flexible way that lets analysts dial up fidelity in areas of great interest, while dialing down fidelity in areas of peripheral interest. This allows analysts to apply techniques of aggressive abstraction to identify system dependencies and system vulnerabilities, to estimate failure consequences, and to assess performance impacts of security approaches. Results from this simulation environment provide mechanisms to—

- Assess and measure the cyber security posture of control systems
- Demonstrate and quantify threats

- Understand the effects of emerging hacker tools
- Understand the cyber risks of modern control systems
- Assess and design risk mitigations and system upgrades.

1.1.2 Historical Information

1.1.2.1 The Problem Environment

Large segments of U.S. infrastructures are controlled through computer-based SCADA control systems. The systems effects propagate across many functional domains at the systems level. Figure 1 shows a notional SCADA control system for an electrical power system among functional domains. Some questions, such as potential adversary reach, can be addressed by treating the various domains in isolation. Here, reach can often be analyzed at the cyber level. Other questions require considering these domains as a system. For example, understanding how various attack forms might produce different power outages requires a combined understanding of the cyber, the control, and the power system dynamics. Understanding threat vectors requires also addressing the cyber-social domain. Understanding outage impacts requires expanding the study to the social (economic) domains.

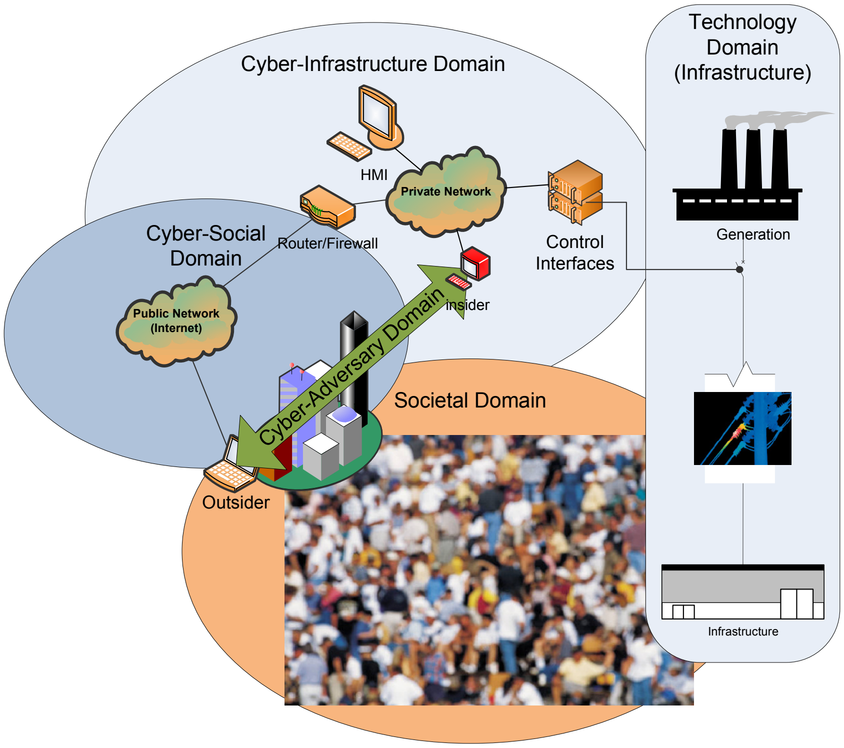


Figure 1. SCADA environment

The VCSE tools described here are designed primarily to address the cyber-infrastructure and control domains. In some cases, they can interface with other tools for combined analyses that address the other domains.

SCADA systems are a form of distributed control systems. In these SCADA systems, human operators interact with the controlled equipment through computer-based operator control units or human–machine interfaces (HMI). Operators utilize these supervisory systems to monitor and control remotely located physical systems and components using intelligent electronic devices (IEDs) interconnected over a network fabric; they include remote terminal units (RTUs) and programmable logic controllers (PLCs). These IEDs connect to physical systems and to components through analog and digital interface devices. The devices convert real world signals, device readings, and settings into and from digital computer messages. Control information, in the form of these messages, is transmitted in between the IEDs and the HMIs across computer networks.

The exact configurations of SCADA systems vary greatly between installations. For example, legacy SCADA systems largely use serial connections (e.g., RS232) with simpler protocols to support communications. More modern SCADA systems use Ethernet-based connections and transmit the messages using one of many Internet protocol (IP) formats popular in the control industry. In some systems, front-end processor (FEP) units are used to distribute control or to provide IP front-ends to the serial connections. HMIs often communicate with the FEPs using a different protocol than that used between the FEPs and the IEDs. In some installations, high-security measures including encryption and authentication are used to protect all data being transmitted and all transmission links. In others, the data channels may be physically protected, but the actual data are transmitted without encryption, and access is not secured. Still others may use a mix of security measures, protecting some links while leaving some links unsecured.

Figure 2 shows a typical SCADA for electrical power system infrastructure. This system connects through a firewall (or through a series of firewalls) that provides a main barrier of defense. Operators control the infrastructure through the HMI, which, in turn, transmits commands through the network to the RTUs. The communication system includes an Ethernet network near the HMI, which connects—through a communications server and through a private switched telephone system—to hubs. They connect to the RTUs. This control system (showed in Figure 2) is augmented with an energy management system that stores information to a database. Other computers (not shown) may be on the network to support control and non-control functions. When under attack, adversaries might place software on hosts located near the host or near various RTUs. They might even place software on the HMI or other control equipment directly. Advanced adversaries might control these programs from remote sites located on the Internet.

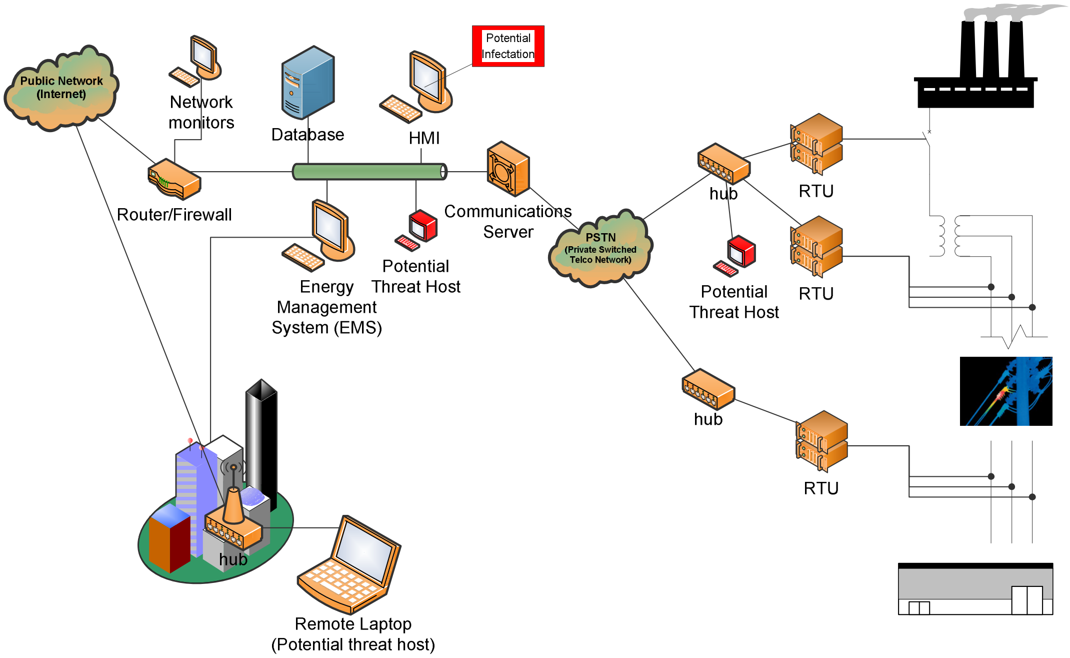


Figure 2: Typical SCADA for electrical power system

1.1.2.2 Trends Driving the Changes in Cyber Security

Energy control systems are subject to targeted cyber attacks [6]. Potential adversaries have pursued progressively devious means to exploit flaws in system components, telecommunication methods, and common operating systems found in modern energy systems. These adversaries intend to infiltrate and sabotage vulnerable control systems. Sophisticated cyber attack tools require little technical knowledge to use and can be found on the Internet, as can manufacturers' technical specifications for popular control system equipment. Commercial software used in conventional IT systems offer operators good value and performance, but poor security. Such software is beginning to replace custom-designed control system software. In addition readily available engineering software designed for control system installation and diagnostic purposes can bypass the control software to provide malicious insiders with nearly unlimited access to all aspects of the control systems.

1.1.2.3 Cyber Communications for Control Systems

Utilities and energy companies recognize it is not feasible to fully protect all energy assets from external threats. The industry's vision for securing energy control systems focuses on critical functions of the most critical applications—functions that, if lost, could result in loss of life, public endangerment, environmental damage, loss of public confidence, or severe economic damage. This risk-based approach builds on established risk management principles now in use in the energy sector. However, many energy companies have a limited ability to measure and assess their cyber security.

This lack consists of metrics or reliable tools for measuring risks and vulnerabilities. Threats, when known, may be difficult to demonstrate and quantify for decision-makers. Control systems are increasingly interconnected and often operate on open software platforms with known vulnerabilities and risks. Poorly designed connections between control systems and enterprise networks introduce further risks. Security upgrades for legacy systems may degrade performance due to limitations of existing equipment and architectures. New architectures with built-in, end-to-end security will take years to develop and even longer to deploy.

1.1.2.4 External Threats

In addition to natural and accidental threats, intentional threats are increasingly sophisticated [7]. When attacks occur, information about the attack, consequences, and lessons learned are often not shared beyond the company. Outside the control system community, there is poor understanding of security problems, their implications, and need for solutions. Coordination and information sharing between industry and government is also inadequate, primarily due to uncertainties in how information will be used, disseminated, and protected. Finally, even when risks, costs, and potential consequences are understood, it is difficult to make a strong business case for cyber security investment because attacks on control systems so far have not caused significant damage.

1.1.3 Significance

By 2015, the four Roadmap goals—1) measure and assess security posture, 2) develop and integrate protective measures, 3) detect intrusion and implement response strategies, and 4) sustain security improvements—will be achieved. At that point, energy owners will be able to perform fully automated security state monitoring of their control system networks with real-time remediation. Next-generation control system components and architectures will offer built-in, end-to-end security that will replace older legacy systems. Control system networks will automatically provide contingency and remedial actions in response to attempted intrusions, and energy asset owners and operators will work collaboratively with government and sector stakeholders to accelerate security advances.

1.1.4 Literature Review

The following literature review lists related emerging technologies:

- RINSE [8, 9]

> The Real-time Immersive Network Simulation Environment for Network Security Exercises (RINSE) is a tool for realistic emulation of large networks as well as network transactions, attacks, and defenses.
>
> RINSE has unique capabilities, which make it suitable for cyber security and game-playing exercises including large-scale real-time human/machine-in-the-loop network simulation support, multi-resolution network traffic models, and novel routing simulation techniques.
>
> RINSE consists of five components:
> - iSSFNet network simulator
> - Simulator Database Manager
> - Database
> - Data Server
> - Client-side Network Viewers

- RTDS

The Real Time Digital Simulator or RTDS provides power systems simulation technology for fast, reliable, accurate, and cost effective study of power systems with complex High Voltage Alternating Current (HVAC) and High Voltage Direct Current (HVDC) networks. The RTDS Simulator is a fully digital electromagnetic transients power system simulator that operates in real time.

Since the simulator functions in real-time the power system algorithms are calculated quickly enough to continuously produce output conditions which realistically represent conditions in a real network. Real-time simulation is significant for two reasons—the user can test physical devices and the user is more productive by completing many studies quickly with real-time simulation.

Since the simulator is real time, it can be connected directly to power system control and protection equipment. For example, it can be used to test HVDC (High Voltage Direct Current) controllers or protective relays. Testing on an RTDS Simulator is more thorough than other test methods because the user is able to subject the equipment to many severe but realistic conditions, which could not possibly be achieved when it is installed on the physical system [10, 11].

- CIPR/sim

Critical Infrastructure Protection and Resiliency Simulator (CIPR/sim)

In cooperation with the Department of Defense, scientists and engineers at Idaho National Laboratory have developed an advanced simulation technology called CIPR/sim which allows emergency planners to visualize the real-time cascading effects of multiple infrastructure failures before an actual emergency occurs. By using CIPR/sim, responders are better prepared and more responsive and accurate when analyzing critical incident data.

In 2007, several INL critical infrastructure protection engineers, geospacial technology experts and software developers began designing CIPR/sim to help first responders plan, prepare and predict the cascading effects that natural disasters or terrorist attacks have on infrastructure resources such as the electric power grid and telecommunication networks.

Today, CIPR/sim has become the first critical infrastructure simulation tool to be designed with a common operating framework that adheres to national Institute of Electrical and Electronics Engineers (IEEE) 1516 standards. This advancement allows the tool to import real-time data from numerous existing analysis modules, including RTDS (Real Time Digital Simulator) for electric grid analysis, QualNet for telecommunications analysis, and PC Tide for wind speed and flood surge analysis [12].

1.2 Purpose

Sandia developed VCSE as a unique way to analyze cyber effects. In keeping with needs cited in the Roadmap, VCSE provides a means to discuss and explain vulnerabilities to system operators. VCSE also addressed the following needs:

- Reduce energy system exposure to harm, cyber attacks, and accidents
- Uncover system vulnerabilities that stem from unencrypted, unsecured data on IP routed computer networks
- Develop, test, and validate counter measures to prevent system damage and safeguard energy networks
- Prevent disruptions.

1.2.1 Roadmap Challenges

VCSE is part of an overall program to address the control system vulnerabilities cited in the Roadmap [13]. Table 1 describes the relationship between VCSE features and key challenges set out in the roadmap.

Table 1 VCSE Response to Roadmap Challenges

Challenge	VCSE Response
Limited ability to measure and assess cyber security posture	VCSE provides the ability to model the security aspects of a control system and analyze the impacts of specific attacks on the system.
No consistent cyber security metrics	VCSE can aid engineers as they develop metrics and analyze how those metrics are calculated and utilized within the control system.
Hard to quantify and demonstrate	VCSE provides a mechanism to model, demonstrate, and analyze the impacts of control system threats.
Growing risks from interconnected systems	VCSE can provide control system impacts analysis information for other analysis tools that model interconnections between power and other national infrastructures.
Poorly designed connections of control systems and business networks	VCSE can be federated with business network models to analyze the impact on the infrastructure resulting from threats against connected business networks.
Lack of clear design requirements	VCSE can be used to model competing design models to allow engineers to analyze and develop design strategies.
Possibility that performance may degrade from security upgrades to legacy systems	VCSE provides the ability to model and analyze the performance degradations as a result of security upgrades before such changes are affected in real control system.
Increasingly sophisticated hacker tools	As emerging threats are identified, they can be incorporated or simulated within a VCSE simulation model to analyze their potential impacts.
Insufficient information sharing	The primary analysis methodology—that Sandia envisions for VCSE and the NSTB analysis tool suite—brings together stakeholders from government, industry, and the national laboratories to understand threats and work for their mitigations. This provides a forum for information sharing.
Poor industry/government coordination	The primary analysis methodology—that Sandia envisions for VCSE and the NSTB analysis tool suite—brings together stakeholders from government, industry, and the national laboratories to understand threats and work for their mitigations. This provides a natural forum for coordination to occur.
Weak business case for cyber security	VCSE provides an analysis mechanism to study the impacts from cyber threats to control systems. When this is coupled with consequence analysis tools, it provides compelling arguments for appropriate and reasoned investment in control-system cyber security.

1.2.2 Reason for Investigation

SCADA systems have certain vulnerabilities. Sandia developed the VCSE model and simulation environment to assess security vulnerabilities of infrastructures. At present, VCSE supports SCADA for electrical power systems.

1.2.3 Audience

This report should be of interest to 1) U.S. government agencies including the departments of Energy (DOE), Defense (DoD), Homeland Security (DHS) and others; 2) branches of U.S. military; 3) utility companies including owners and operators of energy systems; 4) city, county, and state government offices associated with Homeland Security; and 5) researchers studying cyber security, modeling and simulation, and other topics.

1.2.4 Desired Response

As the audience reviews this report, it is hoped that they will understand what VSCE is and what this technology is designed to accomplish. A project objective is to build the VCSE testbed so that it allows industry and government to work together to explore and analyze control system issues and find solutions to these problems. To be most effective, these types of analysis methodologies utilize expertise in 1) the infrastructure under analysis (i.e., power, oil, and gas, etc.), 2) control systems, 3) computer networking, 4) cyber security and vulnerability, and 5) modeling and simulation. It is hoped readers will understand how they might utilize and participate in analyses using VCSE to strengthen our nation's infrastructures. This participation will be in the form of providing feedback and analysis scenarios, as well as participation in analysis working sessions.

1.3 Scope

The project conducted three sets of experiments: An initial set used a VCSE system configured with a real HMI, a hybrid simulated/physical network, simulated IEDs, and a simulated power system. A second set replaced the simulated network with an emulated network. A third set enlarged the power system to study potential effects of a third malware package at a larger scale. Experiments were conducted to simulate the following attacks: Man-in-the-middle (MITM), precision insider, MITM attack on multiple remote terminal units (RTUs), and a rogue software attack. Also, a VCSE experiment used a dynamic power simulator.

1.3.1 Extent and Limits of Investigation

It should be recognized that VCSE is a hybrid simulation environment; as a result there are a number of real software and hardware components that can be incorporated into a given scenario. The simulated components are just that—simulated—and must be configured or modified to perform realistic behaviors. Each new scenario must be analyzed to determine how it can be modeled to provide the analysis required.

The VCSE modeling methodology uses a principle called aggressive abstraction. Aggressive abstraction suggests that it is unproductive to model large systems at the full fidelity needed to answer many specific questions. Rather, it recommends modeling aspects of the model that specifically touch the particular aspects of the system in sufficient detail to address those questions, while abstracting extraneous aspects to the maximum extent possible. Models at medium levels of fidelity are used to bridge the extremes. In VCSE, aggressive abstraction lets modelers mix, for example, live cyber threats attacking emulated control equipment that, in turn, controls simulated electrical power systems that serve highly abstracted customer demands. A contrasting approach for analyzing similar problems would be to analyze live cyber threats on functioning portions of the electrical power grid. Aggressive abstraction is best used when this contrasting approach is cost- and time-prohibitive or overly dangerous.

1.3.2 Goal

The VCSE project goal is to provide a security evaluation toolset for analysis of cyber vulnerabilities on control systems. The goal of this paper is to describe the capabilities built to date

1.3.3 Objectives

The VCSE simulation environment will provide functionality in four capability areas—simulation framework, simulation configuration, simulation execution, and analysis tools. These capabilities translate into the following objectives:

1. Create a simulation framework
2. Develop simulation-configuration user interfaces
3. Develop simulation-execution user interfaces
4. Develop or employ analysis tools.

—This page intentionally left blank —

2 Approach

Given plausible threats, the VCSE will help asset owners and analysts understand the scope and scale of effect that each threat might reach if it were actually launched. In doing so, the tool will provide valuable insight into how the threats propagate and how operators might observe threats in action. Finally, the tool will provide a testbed on which to evaluate the effectiveness of selected mitigation options.

VCSE will permit end-users to configure simulation environment of control system devices and network communication protocols and will enable real-time, hardware-in-the-loop connectivity to understand the effects of cyber-vulnerabilities on the control system. The VCSE will reduce the risk of energy disruption by providing a realistic setting designed to replicate portions of a vulnerable infrastructure against which cyber attacks can be played out and effective mitigation tactics developed with no threat to the actual infrastructure.

A robust architecture, the VCSE environment is a collection of hardware and constructive capabilities to assess security vulnerabilities of infrastructures for the Supervisory Control And Data Acquisition Systems (SCADA). These VCSE tools primarily address the cyber-infrastructure and control domain, with some potential to interface with other tools for combined analyses of domains.

To threaten a SCADA system, adversaries must overcome and execute code behind protective barriers, while subverting the control system. Because the control systems operate over a cyber-control domain, many cyber and control-related vulnerabilities cannot be studied separately. To examine the combined problem, researchers might—

- Study the threats *in-situ*
- Predict large-scale system impacts by studying affordable small-scale systems
- Study the threats through simulation alone.

In practice, each of these approaches is problematic. *In-situ* studies involving infrastructures become unreasonably expensive when performed at even modest scale. It is, likewise, difficult to understand how various large-scale threats operate and to predict their impacts by studying small-scale threat vectors. While simulation models alone are useful, the results of using simulation are often not conclusive, as today's models are not sufficiently advanced to highlight and expose key threats.

To overcome these individual limits, this work takes a hybrid approach as described below.

2.1 Methods

VCSE combines Simulated, Emulated, and Physical components for Investigative Analysis (SEPIA). The SEPIA method allows analysts to use aggressive abstraction to simplify the analytic task. Aspects requiring high resolution are analyzed using actual components. Driving system issues are represented by using simulation models. Emulation allows for cost-effectively representation of systems with modest impact.

Just as the infrastructures work in the context of the larger social environments, key cyber vulnerabilities exist within the context of the larger application. By analogy, key banking vulnerabilities exist in the context of the how money might be diverted. In SCADA systems, the key is in protecting the infrastructure, its products, and the monitory value derived from operating it. To threaten the control actions within a SCADA system, adversaries must overcome the cyber protective barriers and subvert the control system itself.

This work posits that, for SCADA systems, the overlaps between the application (infrastructure dynamics) and cyber domains are significant. For this reason, it is insufficient to study cyber and control vulnerabilities separately. Combined study environments are needed.

Unfortunately, it is quite difficult to study the threats *in-situ*. Few operators wish to subject their systems to penetration tests that actually affect the control systems. The cost of producing and subjecting even relatively small-scale physical replicas to meaningful threats is high. Worse, it is difficult to predict large-scale system impacts by studying affordable small-scale systems. Likewise, it is also difficult to study the threats through simulation alone, as today’s models are not sufficiently advanced to highlight and expose key threats.

To overcome these limits, this work uses SEPIA, a hybrid approach. These SEPIA environments allow analysts to use aggressive abstraction. Details requiring high resolution, such as the ways traffic passes on the network, are analyzed in full realistic detail using actual (physical) components. Driving system issues, including control system dynamics that affect SCADA traffic patterns, are represented using simulation models. In-between, emulation is used to cost-effectively represent systems that have modest impact on the control systems.

2.2 Assumptions

In developing hybrid models, several assumptions must be made. Analysts must be careful to operate the models within the bounds set by the characteristics of the various model elements. For example, some experiments use emulated components as a cost-effective way to represent various system components such as network routers. These emulators execute the same code as real equipment, but are often performance limited. As a result, emulators are much more sensitive to denial of service attacks than the actual equipment that they model. It is, therefore, not valid to use these emulators for studying denial of service or threats that otherwise try to overwhelm the components being emulated. The analyst must, therefore, assume that this form of denial of service will not be used in the particular studies that use those emulated components.

Similarly, VCSE adds cyber interfaces to its simulated remote terminal unit (RTU) models to represent the cyber-to-control bridge. These interfaces reproduce the network protocols that are present between the human-machine interface (HMI) and the RTUs and, thus, are subject to the same MITM attacks as real systems. However, they are not vulnerable to particular buffer overflow and related attacks that may be problematic on some real RTUs. For this reason, the analyses that depend on simulated RTUs assume that the threats do not use buffer overflow as a mechanism for gaining cyber control at those RTUs.

In the experiments reported here, several particular assumptions are made. For the precision-insider-attack experiment, it is assumed that the insider could execute changes at will. This may not be valid in controlled settings. To simulate a model for the rogue-software-attack experiment, it was assumed that the front-end processor (FEP) was developed overseas by a programmer with ties to a U.S. adversary. In the same experiment, it was assumed that the FEP malware could determine, by searching internal data structures, which breakers to trip, and which commands would cause a trip. In contrast, the analytic model uses in-house developed software that operates just outside the FEP and directly incorporates the information that the assumed threat would need to derive. It then uses a statistical model to model how well the real threat would derive the information through database queries on the FEP and launches the attack based on these statistical estimates.

2.3 Procedures

2.3.1 Analytic Methodology

Just as the infrastructures work in the context of the larger social environments, key cyber vulnerabilities exist within the context of the larger application. By analogy, key banking vulnerabilities exist in the context of the how money might be diverted. In SCADA systems, the key is in protecting the infrastructure, its products, and the monitory value derived from operating it. To threaten the control actions within a SCADA system, adversaries must overcome the cyber protective barriers and subvert the control system itself.

This work posits that, for SCADA systems, the overlaps between the application (infrastructure dynamics) and cyber domains are significant. For this reason, it is insufficient to study cyber and control vulnerabilities separately. Combined study environments are needed.

As noted above, studying threats *in-situ* is difficult. Operators prefer not to subject systems to penetration tests because these can affect the control systems. Further, producing and subjecting small scale physical replicas to threats is not cost effective; and predicting large scale system impacts by studying affordable small scale systems is often not helpful either. Finally, studying threats through simulation alone is difficult because current models are not advanced enough to reveal key threats.

To address these considerable challenges, a hybrid approach is applied, using SEPIA. SEPIA environments enable researchers to use aggressive abstraction. Where high resolution is required, analyses are conducts in full realistic detail (using SEPIA's physical component). Driving system issues are represented with simulation models. Systems with modest impact on control systems use the more cost effective emulation component.

2.3.2 Tool and Methodology Development

The VCSE project develops a modeling and simulation tool to analyze and assess threats and cyber vulnerabilities on control systems without risking disruptions to critical operations. The following discussion addresses work conducted to achieve each the four objectives:

Objective 1: Simulation Framework.

This work creates the software that is associated with the core/kernel elements of the VCSE architecture. That consists of the following elements:

- Simulation engine {scheduler, configuration, execution}—This feature is the heart of the tool and provides the environment for running simulations.
- Interoperability-federation interface—This mechanism enables third party simulators/models to interact with VCSE (power simulators, both static and dynamic, custom models provided by asset owners, etc.).
- External integration {emulated devices, simulated devices, and real hardware devices}—This feature provides the fusion of various levels of modeling fidelity.

Objective 2: Simulation Configuration.

Developing this capability allows the analyst access to the VCSE toolbox for building the targeted control-system environment under investigation. This includes identification of data inputs/outputs; control-system simulated or emulated devices, and communication protocol models. This capability consists of the following elements:

- User interface (UI)—allows the configuration and management of the simulation environment (i.e., devices, models, probes, data input/output, etc.).
- Control-system simulated/emulated devices—provide a suite of simulated and emulated control-system equipment/components.
- Network protocol simulators—provide a suite of network protocol models (ModBus, transmission control protocol/Internet protocol (TCP/IP), DNP3, ICMP, ICCP, etc.).

Objective 3: Simulation Execution.

Creating this capability allows analysts to run and manage the simulation runs; it includes a statistics collection of data measurements for post-run analysis. The output generated from this capability will be used by several end-users, including control-system operators/engineers, security operators/engineers, network analyst/designers, and control-system product designer/engineers. This capability consists of the following elements:

- Setting data probes in the simulation environment for gathering post-analysis data
- Managing the simulation runs (set static parameters, pause, resume, change run-time parameters, direct running output to visualization tools, etc.)
- Simulation environment library (store and recall a simulation environment for future use).

Objective 4: Analysis tools.

Developing this capability creates an extension of the VCSE toolbox and allows the end-users to perform post-simulation analysis. This capability provides a mechanism for viewing the results of the simulation. It is anticipated that several visualization tools will be available to the user (i.e., 2-D/3-D views, data tables, graphs, charts, etc). Analytic tools consist of the following elements:

- Graphical user interface for post-simulation data graphics display capability (2-D, 3-D, etc)
- Data reduction analysis library.

3 Results and Discussion

3.1 VCSE Architecture

The Virtual Control System Environment (VCSE) was designed to use the Simulated, Emulated, and Physical components for Investigative Analysis (SEPIA) approach to assess security vulnerabilities in Supervisory Control And Data Acquisition (SCADA) systems. It is an analytical environment designed to allow researchers to model any and all the aspects of SCADA systems mentioned in sections 1 and 2 of this report. Researchers develop and integrate simulation models, emulated and virtualized devices, and real physical hardware representing various control system elements into combined SEPIA environments. Sandia's VCSE includes commercial-off-the-shelf components, custom physical devices, and constructive software components.

While the VCSE project has developed, incorporated and used many tools and modeled many systems, VCSE itself is not a tool. Rather it is an environment within which tools are brought together to study control systems. In a typical VCSE analysis, modelers use VCSE to build a virtual control-system network that represents the key issues of the problem at hand. For example, in analyzing particular threat codes, they build virtual control-system models that use real (physical) software to represent the cyber portions of the system that the code interacts with; and they simulate elements to represent the systems that the threatened control-system elements interact with. Conversely, when the threat software under study works within the network fabric, the analysts configure systems that produce real network traffic, and then they use simulation and emulation to represent those pieces that are indirectly impacted. Figure 3 shows the factors or components involved in a VCSE analysis.

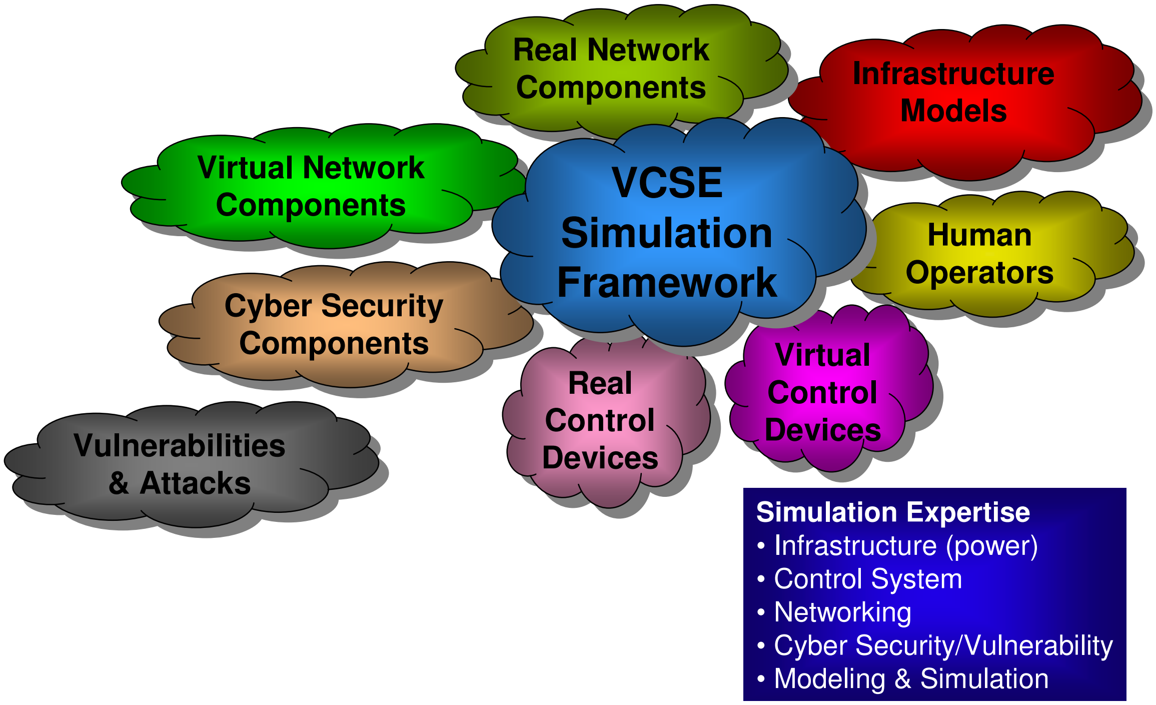
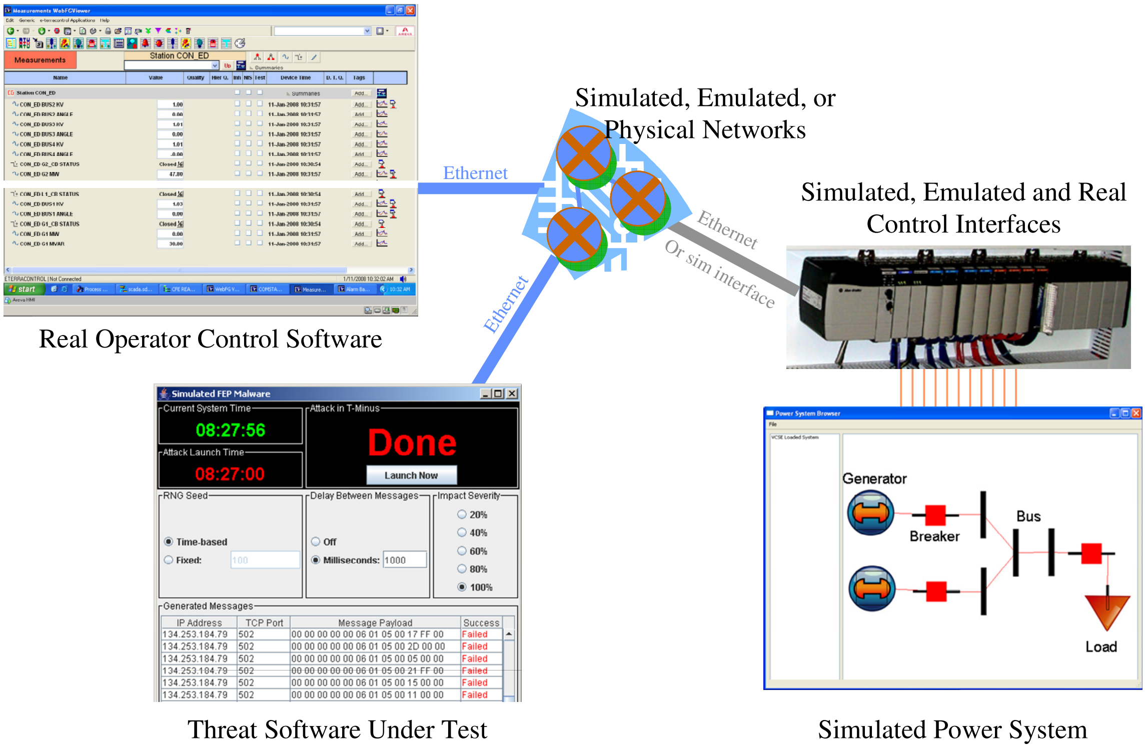


Figure 3: VCSE is an environment and methodology

Figure 3 categorizes some of the tools or elements used in VCSE analyses. These include real and virtual network components, infrastructure models, human operators, real and virtual control devices, cyber security components, and vulnerability and attack codes and models. Because simulation enables the analysis of large systems, the VCSE simulation framework (SF) is a central element in any VCSE analysis. Likewise, because human expertise is the driving force in any analysis, the VCSE architecture directly addresses the multiple expertises that it draws from, and it addresses different ways that these areas of expertise are expressed in any system analysis. Beyond VCSE-SF, specific components developed or used within VCSE to date include—

- Infrastructure Models
  - A Sandia-developed Newton–Raphson Steady State Power Simulator
  - University of Missouri (UMR)-developed Dynamic Power Simulator
  - PowerWorld [14] Steady State Power Simulator
- Network Components
  - OPNET [15] Network Simulator
  - Network-In-a-Box (NIB) Network Simulator [16]
  - Real Network Devices (routers, switches, etc.)
- Control-System Interfaces
  - Remote terminal unit (RTU) simulation models with ModBus [17] interfaces
  - Telvent SAGE 1330 RTU using a National Instruments (NI) PXI-1042 with NI PXI-8196 digital to analog converter to connect to VCSE
- Human Machine Interfaces (HMIs)
  - Areva E-TERRACONTROL based operator's consol (HMI) [18]
  - A Sandia-developed Web-based HMI
- Cyber Security Components
  - An Open Process control system Security Architecture for Interoperable Design (OPSAID) prototype security device
- Vulnerabilities and Attacks
  - Man-in-the-middle (MITM) attack (see section 3.5.1 below)
  - ModBus vulnerabilities (see section 3.5.2 below)
  - Rogue software attack—a simulated software life cycle attack (see section 3.5.3 below)
  - Simulated directed energy attack.

Figure 4 diagrams a typical VCSE model designed to assess software and network-level vulnerabilities while also highlighting the plug-and-play nature of the modeling problem. Typical control systems include control software in the form of HMIs, networks, control interfaces (i.e., RTUs and programmable logic controllers [PLCs]) and a controlled system. Cyber threats typically act at either the software (e.g., by directly interacting with the HMI software) or at the network (e.g., by manipulating network packets) level. Models that focus on threat software analysis have interfaces that these threat programs can interact with directly. This is illustrated in Figure 4 by having the operator control and threat software interact through physical Ethernet interfaces.



Measurements WebFGViewer

Station CON_ED

Name	Value	Quality	Hier Q.	Inh	NIS	Test	Device Time	D. T. Q.	Tags
Station CON_ED				□	□	□	Summaries		Add...
CON_ED BUS2 KV	1.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS2 ANGLE	0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS3 KV	1.01			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS3 ANGLE	0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS4 KV	1.01			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS4 ANGLE	-0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED G2_CB STATUS	Closed			□	□	□	11-Jan-2008 10:30:54		Add...
CON_ED G2 MW	47.80			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED L1_CB STATUS	Closed			□	□	□	11-Jan-2008 10:30:54		Add...
CON_ED BUS1 KV	1.03			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED BUS1 ANGLE	0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED G1_CB STATUS	Closed			□	□	□	11-Jan-2008 10:30:54		Add...
CON_ED G1 MW	0.00			□	□	□	11-Jan-2008 10:31:57		Add...
CON_ED G1 MVAR	30.80			□	□	□	11-Jan-2008 10:31:57		Add...

ETERRACONTROL | Not Connected   1/11/2008 10:32:02 AM

Real Operator Control Software

Simulated FEP Malware

Current System Time: 08:27:56

Attack Launch Time: 08:27:00

Attack in T-Minus: Done

Launch Now

RNG Seed: ● Time-based ○ Fixed: 100

Delay Between Messages: ○ Off ● Milliseconds: 1000

Impact Severity: ○ 20% ○ 40% ○ 60% ○ 80% ● 100%

Generated Messages

IP Address	TCP Port	Message Payload	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 17 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2D 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 05 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 21 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 15 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 11 00 00	Failed

Threat Software Under Test

Simulated, Emulated, or Physical Networks

Simulated, Emulated and Real Control Interfaces

Simulated Power System

Figure 4: Typical VCSE model designed to assess software and network-level vulnerabilities

Depending upon the particular study, the network with which the threat interacts can be represented using simulated, emulated, or physical network elements and is typically implemented using combinations of all three. In some cases, the threats also interact with physical control interfaces that are brought into the system in the same way. However, in most cases, the control systems have large numbers of control interfaces. Here, the VCSE models use simulated control interfaces that can be inexpensively replicated. For consistency and integration with the HMI, these simulated control interfaces are designed to appear on the network as if they were collections of real control interfaces. In these models, the infrastructures themselves are modeled in simulation to avoid the physical and societal costs, as well as the risk of life; these costs and risks—associated with performing scale-level cyber threat experiments on the live equipment—are a focus of concern.

VCSE currently models SCADA systems for electrical power grids. The SCADA is modeled based on a three-layer physical, control, and network topology. Figure 5 provides an example of how a typical model is arranged in this topology. The physical layer includes models of the power system's generators, loads, and associated transmission, distribution, and control components. The control layer is the command and control structure for the power grid SCADA. This includes the HMIs, the RTUs, the energy management systems, and all other control elements. The network layer is the communication and control network fabric associated with the control system. This includes the physical computers, network devices, and data transmission lines. Cyber adversaries typically operate at the network layer.

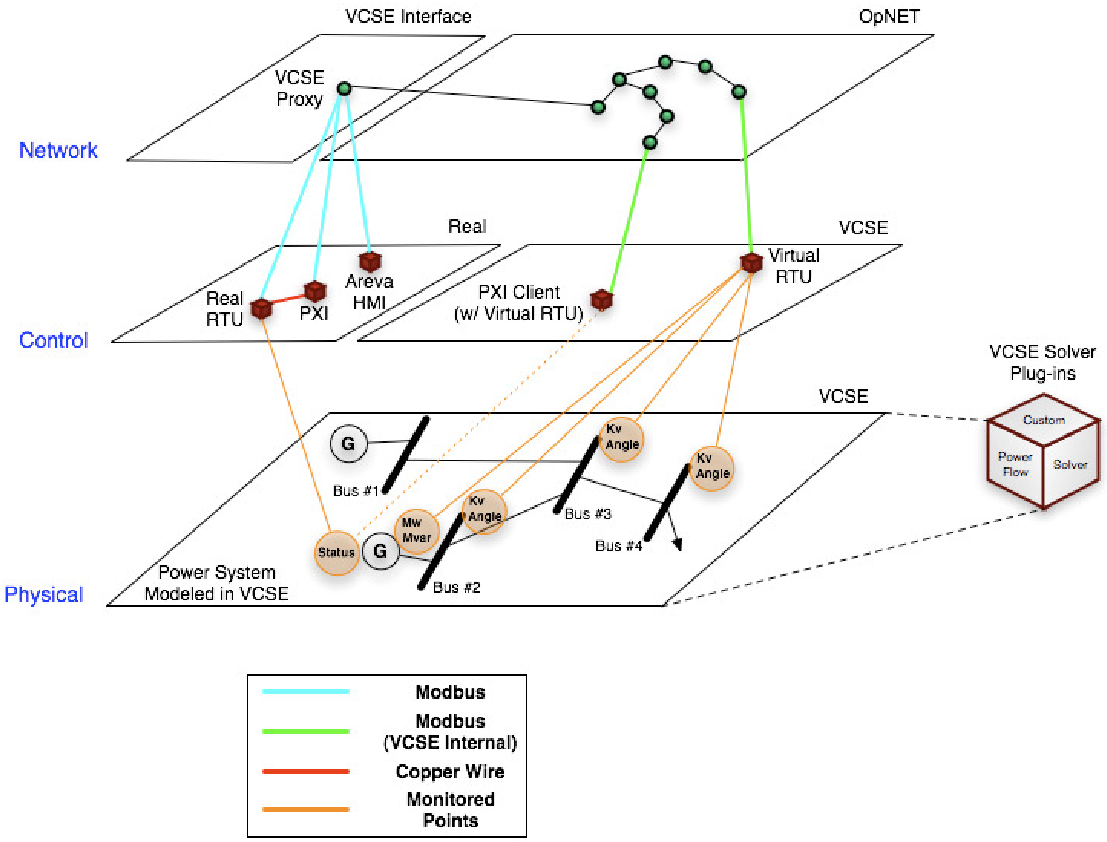


Figure 5: VCSE model arranged along three-layer physical, control and network topology

VCSE simulation models are developed using the VCSE-SF. Model execution is centered on a discrete event simulation (DES) engine. VCSE-SF models control-system infrastructures based on the three-layer physical, control, and network topology. It integrates disparate modeling and simulation capabilities across the VCSE-SF boundary through a software plug-in architecture. In addition, it can interface with external models through VCSE-SF-based network proxy interface modules (a.k.a., class instances). Generally, VCSE-SF was designed to support—

- Modeling
- Model/code integration
- Real to simulation integration
- Experiment support.

Figure 6 diagrams a VCSE model that was used to analyze a particular suite of MITM malware code. Here, the physical HMI and threat software (roadblock and threat hosts) interact through a simulated network with simulated control-system components, which, in turn, control simulated power system elements. In the experiment diagrammed here, the HMI is implemented using Areva E-TERRACONTROL, a commercial HMI tool, running on a dedicated computer. The malware consisted of appropriately configured threat software that had been collected from the Internet. This software was run from virtual machines (VMs). All other elements were implemented within VCSE-SF. Here, the network was implemented using the commercial OPNET modeling package. (VCSE-SF encapsulates this software as an integrated module.) The RTUs and power grid simulator were implemented directly within VCSE-SF.

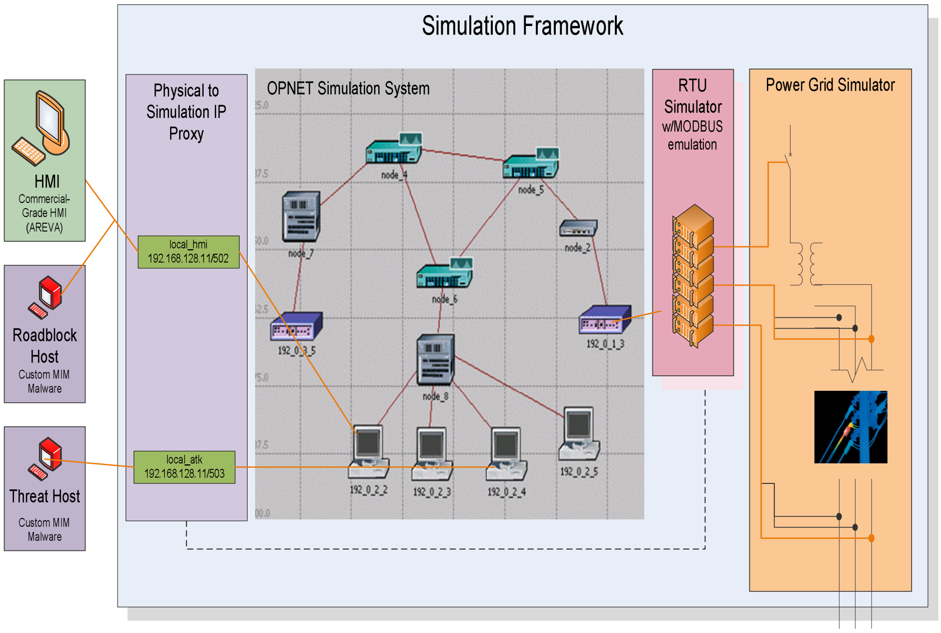


Figure 6: VCSE model of a notional SCADA system for an electrical power grid

As discussed, VCSE is an environment and not a single simulation model. In researching control-system vulnerabilities, analysts must often adjust the various models to shift their focus. VCSE allows analysts to dial in resolution where needed to study SCADA vulnerabilities and aggressively abstract the rest of the system. For example, in further investigating the implications of the aforementioned threat's ability to reach various parts of the network, analysts found it necessary to increase the fidelity of the real network traffic. To facilitate this, they replaced the OPNET simulated network with an emulated network based on Sandia's NIB technology.[1] The resultant implementation is diagrammed in Figure 7. Here, the RTU and power grid models are still implemented within VCSE-SF. However, the network is implemented as a network of four emulated routers that connect between the HMI and threat and the simulated control system. Using NIB, network protection rules can be implemented within the routers and the threat can be moved to various locations on the network. In this way, researchers could determine the effect that various router configurations would have on both the operational network and on reducing threat impacts.

In addition to changing network representations, analysts can currently choose from three different types of power system simulation models to represent the infrastructure systems. Real and simulated intelligent electronic devices (IEDs) can be used side-by side, and a commercial-based HMI is used to control the system. Analysts can bring in new threats, change system configurations, and evaluate these threats against different conditions to develop a better understanding of threat dynamics and consequences or effects.

[1] McDonald, Michael J., Sholander, Peter E., Tarman, Thomas D., Hybrid Simulation And Virtualization Research For Information Assurance Analysis; presented at the 76th MORS Symposium Session on Information Assurance Analysis, 10–12 June 2008 United States Coast Guard Academy, New London, CT.

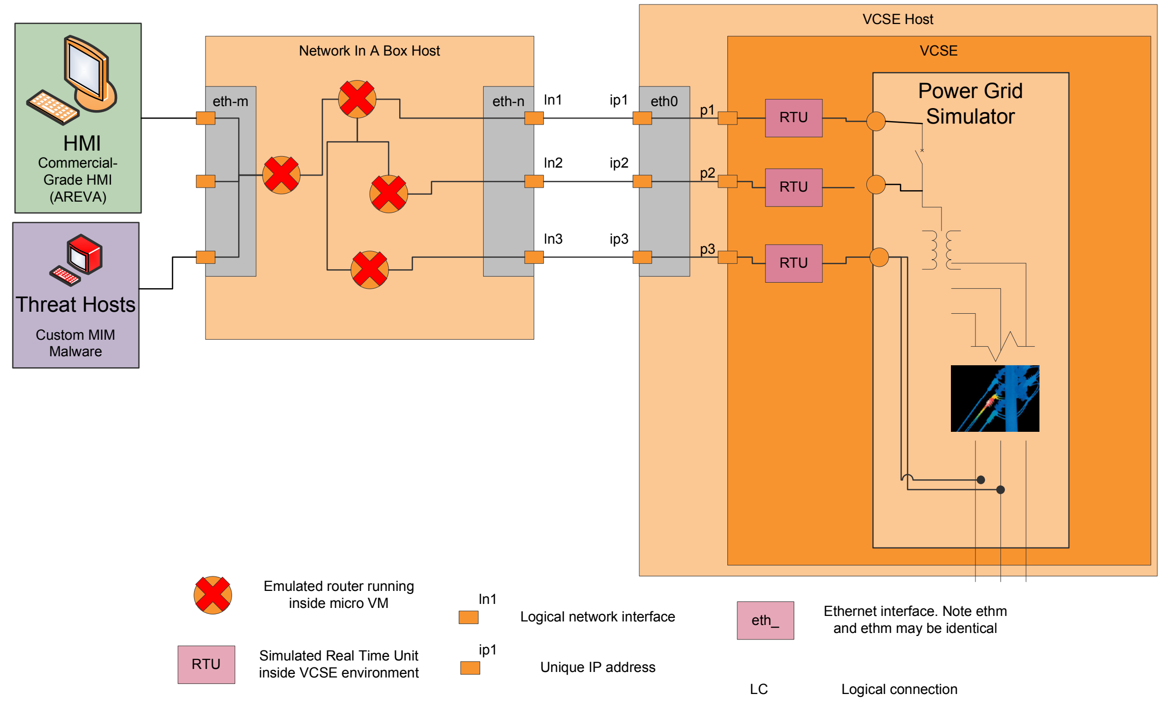

HMI
Commercial-Grade HMI (AREVA)
Threat Hosts
Custom MIM Malware
Network In A Box Host
eth-m
eth-n
In1
In2
In3
ip1
ip2
ip3
eth0
VCSE Host
VCSE
p1
p2
p3
RTU
RTU
RTU
Power Grid Simulator
Emulated router running inside micro VM
In1
Logical network interface
eth_
Ethernet interface. Note ethm and ethm may be identical
RTU
Simulated Real Time Unit inside VCSE environment
ip1
Unique IP address
LC
Logical connection

Figure 7: VCSE model using Network-in-a-Box

3.1.1 VCSE-SF

VCSE-SF is a simulation framework written to allow analysts to develop new and integrate existing simulation models for VCSE studies. It is an object-oriented framework written in C++. It provides a plug-in architecture that allows the framework to dynamically load models with different features for plug-and-play model re-use. It also includes a DES engine with a signals and slots communication system that allows the plug-ins to communicate through the DES.

Model developers can use VCSE-SF directly to represent system components as individual elements and then plug the systems together into integrated systems. VCSE-SF includes an interface class that allows program elements to communicate across plug-ins. Modelers can also integrate or encapsulate models and whole modeling environments into VCSE-SF as if they were VCSE-SF simulation components or systems of components. In some cases, such as with OPNET, VCSE-SF directly loads the simulation environments as Dynamic Link Libraries and interacts with the external models through library calls. In other cases—such as with integrating external power simulation systems to VCSE—VCSE-SF communicates with the models through transmission control protocol (TCP)/Internet protocol (IP) interfaces and Structured Query Language (SQL) databases to coordinate program execution and transfer data. A Distributed Interactive Simulation (DIS) interface has also been developed and native DIS interfaces are being developed for this type of integration.

VCSE-SF can also interact with physical and emulated systems that are external to it through VCSE-SF-based network proxy interface modules. Here, VCSE-SF presents itself as if it were a real-world system of devices with native TCP/IP interfaces. These devices then interact with VCSE-SF using their native protocols.

VCSE-SF was designed to make it easy for model developers to build models that could be saved and restored at any point in executing a simulation. While not all models that integrate with VCSE-SF have this capability, VCSE-SF can save and restore state in configurations that only contain compliant models.

To summarize, the VCSE-SF core includes a/an—

- Plug-in or extension loader system
- Interface representation for bridging plug-ins
- DES engine
- Signals and slots-based instance-to-instance communication system
- System for saving and restoring state
- Test framework.

3.2 Analyses using VCSE

To illustrate the use of VCSE, this section describes three sets of experiments that were performed using it. An initial set of experiments was performed using a VCSE system configured with a real HMI, a hybrid simulated/physical network, simulated IEDs, and a simulated power system. The network simulator used OPNET. The power model used a semi-static Newton-Raphson iterative solver based upon the Bryan Richardson's JPowerFlow model [19]. The HMI was based upon the Areva E-TERRACONTROL. A second set of experiments replaced the simulated network with an emulated network based upon the Dynamips emulator [20]. A third set of experiments enlarged the power system to study potential effects of a third malware package at a larger scale.

In operation, HMIs like Areva E-TERRACONTROL continuously poll and occasionally send control messages to the simulated IEDs across an Ethernet network. (In this model, all traffic is transmitted as ModBus messages.) As is typical in many control systems, the data channels passing the ModBus traffic are neither encrypted nor secured. These experiments analyzed various ways that a malicious cyber attacker could take control of the network through these protocol streams.

3.2.1 Man-In-The-Middle (MITM) Attack Scenario Experiment

The initial VCSE experiment tested the effectiveness of a widely distributed vulnerability test software, which executes an MITM attack upon a control system. Here, Ettercap [21] was used to build an MITM that could fool the operator into thinking the system was operating normally. A simple TCP/IP program was used to quickly connect to a specific RTU, send a disabling control message, and then disconnect.

When first activated, the MITM roadblock intercepts messages between the HMI and IEDs to capture *normal* control values. Technically, it accomplishes this interception using a technique called address resolution protocol (ARP) poisoning [22]. Once it captures enough data, the MITM roadblock switches into a deception phase where it modifies messages from the IEDs with fabricated data based on the monitored values.

For this experiment, the VCSE testbed was configured with VCSE and the MITM codes running on separate VMs that were hosted on a Windows 2003 server. The HMI ran on a freestanding Dell computer running Windows XP. Within this laboratory configuration, the communications between the HMI, VCSE, and the MITM were monitored using WireShark

[23]. WireShark monitors were placed throughout the system to ensure that traffic moving between components, especially VMs, could be monitored. As the network contained a significant amount of background traffic, special filters were then applied in WireShark to allow the analysts to focus in on particular packets.

After performing the attack with several variations, analysts reviewed the WireShark data to identify and carefully document the signature of the attacks. In this way, the analysts could see the exact ARP poisoning messages and gather signature data on them. It became evident through analysis that it is difficult to record this type of attack from WireShark. A particular problem exists in completely matching the data streams from two monitoring points. For example, switches and routers cause messages on one part of a network to not appear at other points. For this reason, the experiment was (as is often the case) repeated several times to acquire a full signature collection.

This experiment set verified that this standard penetration software could be used as malware to change values in a control system while simultaneously hiding the changes and their effects from the operators. In conducting the experiment on a functioning virtual control system, it was observed that, for the attack to cause harm, the attackers would need to adjust control values in specific ways. For example, in this experiment, the attack turned off the generator by executing a *set register* ModBus command to set register 1006 on a particular RTU to zero. (The ModBus message, which is encoded according to [24], is 0603EE0000). Had the attack tried setting values on registers 0-999 or higher than 1008, the attack would have had no effect because those registers were not in use. Had it set values to registers near 1006, the effect would be completely different. Similarly, digital values are indicated with a 1 or 0. Attackers trying to turn digital values on or off, need to know the both the register numbers and the normal states of those registers. For example, some breakers in a system might use 1 to indicate *open* while others in the same system might use 0 to mean *open*. The attacker would need to know which meaning had been used in the targeted part of the system's implementation. In practice, many systems use thousands of registers and digital I/O points on RTUs spread across a wide geographic area. Any attacker would have to perform the practical job of sorting out which register causes which effect before launching any precision attack.

One subtle finding made in this investigation was in discovering flaws in the data gathering phase of the MITM roadblock that would cause the malware to fail in switched networks. In particular, while the roadblock code used active ARP poisoning to deceive the operator, it used passive monitoring to collect data. Had this software been launched in a switched network, the first phase would have failed. Of course, the software did include the capability to use ARP poisoning in each phase of the attack. The malware programmer had simply not turned on the feature for that phase of the attack.

The specific things that the VCSE aided in understanding for the MITM are as follows:

- Understanding how the attack operated and impacted the control system
- Recognizing that the actual location of the attack software made a difference
- Recognizing that the actual location of the monitoring software made a difference
- Discovering that this attack script's monitoring software would have failed in a switched network
- Recognizing that attack/threat success requires detailed knowledge about system configuration that may not be easy to acquire.

3.2.2 Precision Insider Attack Scenario Experiment

This experiment set was executed to investigate the difficulty that a malevolent actor would face in attacking this unsecured system with precision. As noted in the first experiment, it is difficult to sort out which register and I/O point will cause which effect. While a variety of harmful acts could be accomplished by blindly adjusting control values, blind attacks may have limited effects. This experiment postulates that somebody with inside access (i.e., an insider) who, out of curiosity, first seeks to determine whether the access controls on the HMI could be bypassed. They do this by using generic monitoring and control software that is readily available to networking and control system engineers, while simultaneously looking at the HMI. It then suggests that the insider develops a way to remotely access the software that they execute at a time of their choosing. The experiment attempts to determine the difficulty that this insider would face in deriving sufficient information to cause targeted, crippling harm. To validate the finding, it then strikes overtly at the system to gain control.

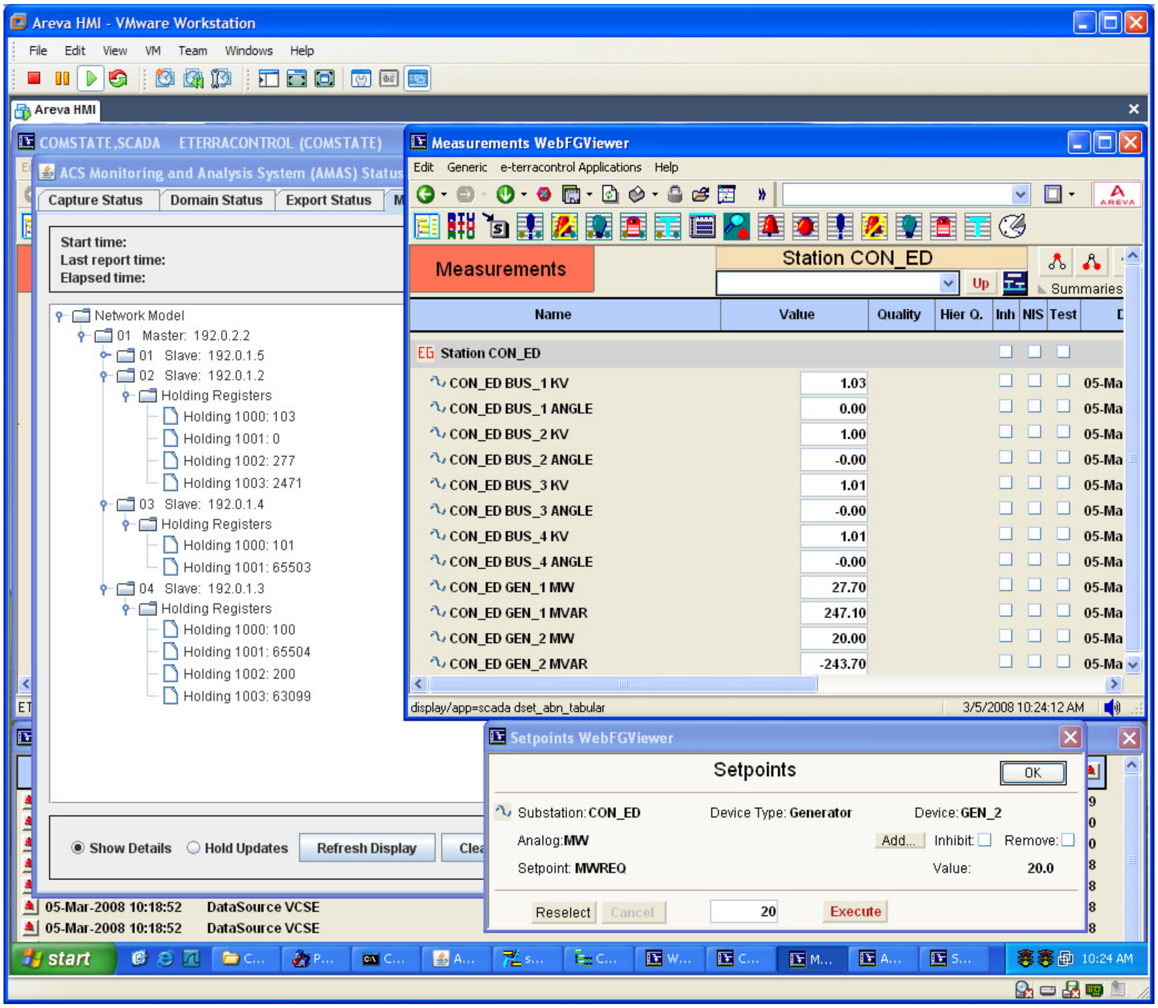
The virtual control system in this experiment set was configured using the NIB technology. The control system had four virtual IEDs, each with a different IP address. Overall, the system was configured using three VMs running on two hosts.

- The first VM ran the VCSE code on Dell Precision 650 (3.06 GHz dual-core Xeon processor with 4 GB RAM). The VM was configured to represent a 4-bus power system controlled through four RTUs operating on the 192.0.1 network.
- The second VM ran both the Areva HMI and the threat software.
- The third VM ran the NIB code on a Dell Latitude D600 laptop computer (1.7 GHz Pentium M with 1 GB RAM).
- WireShark data was collected through the Dell Precision 650 host operating system.

In these experiments, passive monitoring tools were installed on the same computer as the HMI to monitor SCADA-specific network traffic. The first tool, WireShark, was described previously. The second, automatic control system (ACS) Monitoring and Analysis System (AMAS) is a Sandia-developed multipurpose tool. It is used here to simplify the job of converting the multiple ModBus messages into high-level data. In contrast to using ARP poisoning, passive monitoring restricts the number of computers that it can be effective on. These passive tools are easy to implement and difficult to detect. For example, tools with similar features as those used in AMAS for this report are widely used by control engineers. They are readily available both commercially and as open source software. It is not unlikely that control engineers may leave such tools on the HMI computers for their own critical control-system analysis work. As such, this toolset matches well to the insider threat being studied.

The experiments consisted of using WireShark and AMAS to capture network data while an operator changed generation set points on the HMI. After adjusting set points several times, the data was analyzed to determine how closely the HMI data could be reverse engineered. Figure 8 shows a screen image that simultaneously displays a key screen on the HMI and the output from the AMAS monitoring software.

Using either WireShark or AMAS, analysts were able to readily obtain control-system values. (It is noteworthy that AMAS dramatically simplified this task.) For example, the analysts could readily determine the addresses and active registers of each RTU. Additional effort was required to reverse-engineer the control system. In particular, the analysts had to monitor and compare values between the Areva HMI and those on the network. In some cases, data were only being exposed to the monitoring program when users at the HMI issued new control settings for the power system. In this case, because the postulated threat was an insider, it was assumed that they could execute these changes at will. Had the threat not been able to view and adjust various settings, this software would not have been sufficient to determine which control values mapped to which system control points.


Areva HMI - VMware Workstation
File Edit View VM Team Windows Help
Areva HMI
COMSTATE,SCADA ETERRACONTROL (COMSTATE)
ACS Monitoring and Analysis System (AMAS) Status
Capture Status
Domain Status
Export Status
Measurements WebFGViewer
Edit Generic e-terracontrol Applications Help
AREVA
Measurements
Up
Summaries
Setpoints WebFGViewer
Setpoints
OK
start
10:24 AM

Start time:
Last report time:
Elapsed time:

```
Network Model
  01  Master: 192.0.2.2
    01  Slave: 192.0.1.5
    02  Slave: 192.0.1.2
      Holding Registers
        Holding 1000: 103
        Holding 1001: 0
        Holding 1002: 277
        Holding 1003: 2471
    03  Slave: 192.0.1.4
      Holding Registers
        Holding 1000: 101
        Holding 1001: 65503
    04  Slave: 192.0.1.3
      Holding Registers
        Holding 1000: 100
        Holding 1001: 65504
        Holding 1002: 200
        Holding 1003: 63099
```

● Show Details ○ Hold Updates Refresh Display

05-Mar-2008 10:18:52 DataSource VCSE
05-Mar-2008 10:18:52 DataSource VCSE

Station CON_ED

Name	Value	Quality	Hier Q.	Inh	NIS	Test	D
EG Station CON_ED				□	□	□	
CON_ED BUS_1 KV	1.03			□	□	□	05-Ma
CON_ED BUS_1 ANGLE	0.00			□	□	□	05-Ma
CON_ED BUS_2 KV	1.00			□	□	□	05-Ma
CON_ED BUS_2 ANGLE	-0.00			□	□	□	05-Ma
CON_ED BUS_3 KV	1.01			□	□	□	05-Ma
CON_ED BUS_3 ANGLE	-0.00			□	□	□	05-Ma
CON_ED BUS_4 KV	1.01			□	□	□	05-Ma
CON_ED BUS_4 ANGLE	-0.00			□	□	□	05-Ma
CON_ED GEN_1 MW	27.70			□	□	□	05-Ma
CON_ED GEN_1 MVAR	247.10			□	□	□	05-Ma
CON_ED GEN_2 MW	20.00			□	□	□	05-Ma
CON_ED GEN_2 MVAR	-243.70			□	□	□	05-Ma

display/app=scada dset_abn_tabular 3/5/2008 10:24:12 AM

Substation: CON_ED Device Type: Generator Device: GEN_2
Analog: MW Add... Inhibit: □ Remove: □
Setpoint: MWREQ Value: 20.0
Reselect Cancel 20 Execute

Figure 8: Screen capture showing values at HMI and those derived by AMAS

In sum, this experiment set demonstrated that an operator with access to HMI display screens and the network can readily reverse engineer the SCADA system's control mapping. Attackers gaining this information can then bypass any security measures in the HMI software to take control of the system and perform any control action desired.

The specific things that the VCSE aided in understanding for the precision insider attack are as follows:

- It is relatively easy to determine the control mappings and execute a precision attack when the attacker has access to sophisticated engineering tools in conjunction with access to the HMI.
- Conversely, it is very difficult to determine the control-system mapping by only monitoring network traffic. (Additional information, such as the HMI display, is needed).

- The engineering tool for the maliciously directed reverse engineering used passive network monitoring. As such, it was only effective when run from the same computer as the HMI.

3.2.3 Rogue Software Attack Scenario Experiment

This scenario experiment was developed for a workshop sponsored by the National SCADA Test Bed (NSTB) program, entitled Cyber Attacks on Control Systems: Evaluating the Real Risk. The workshop was held at Albuquerque, NM, June 23–24, 2008. In preparation for the workshop, a threat analysis team posed an attack scenario, which formed the basis for several of the NSTB projects at Sandia National Laboratories. Each of these projects was to respond to the scenario utilizing their specific analysis capabilities.

Simulation Model

The essential elements of the workshop scenario are as follows: It was assumed that the front-end processor (FEP) software was developed at an overseas location and that there was a programmer involved in the project with ties to an organization that wished to inflict harm on the U.S. infrastructure. Specifically, that organization wanted to produce a catastrophic failure in regional power grids. This programmer inserted some malicious code that caused trip commands to be sent to the set of breakers that connected the power system generator to a regional grid. (It was assumed that that the malware would automatically identify generator-related breakers in the system configuration files.) Further, the programmer scheduled this program to run at a predetermined date and time when historical records indicate that the power system is at its greatest stress point. Finally, the programmer packaged the code so that the malicious software would be installed during regular FEP software installation.

Effective utilization of VCSE requires a determination of questions to be answered and a determination of how to configure VCSE to produce the answers. The salient question chosen to ask was this: How feasible is it that the rogue-software attack can produce a catastrophic failure in the regional power grid? VCSE modeling efforts are based on the principle of aggressive abstraction, meaning that analysts seek to simulate in degrees of fidelity only aspects of the problem needed to answer the given questions. Other aspects can be abstracted or ignored entirely. Figure 9 depicts a schematic of the simulation scenario. Within the scenario are the boundaries of the model that was actually simulated through VCSE. For this experiment even the concept of the operator workstation was minimized in that it provided only minimal benefit to analysis.

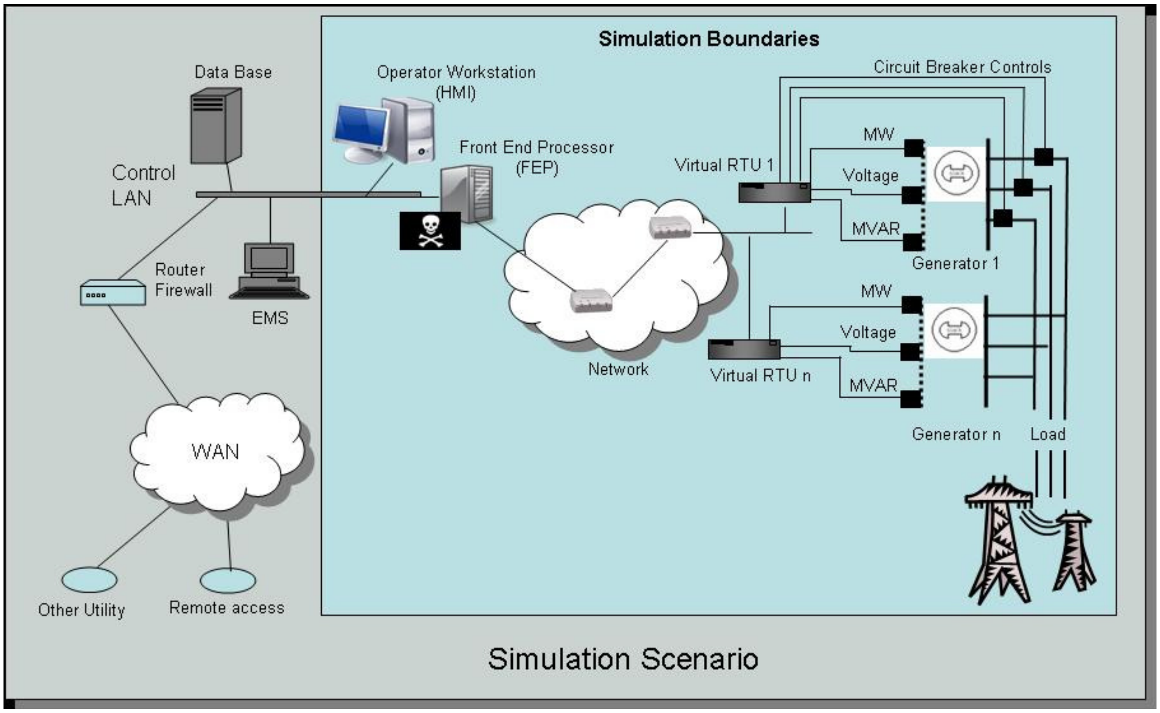
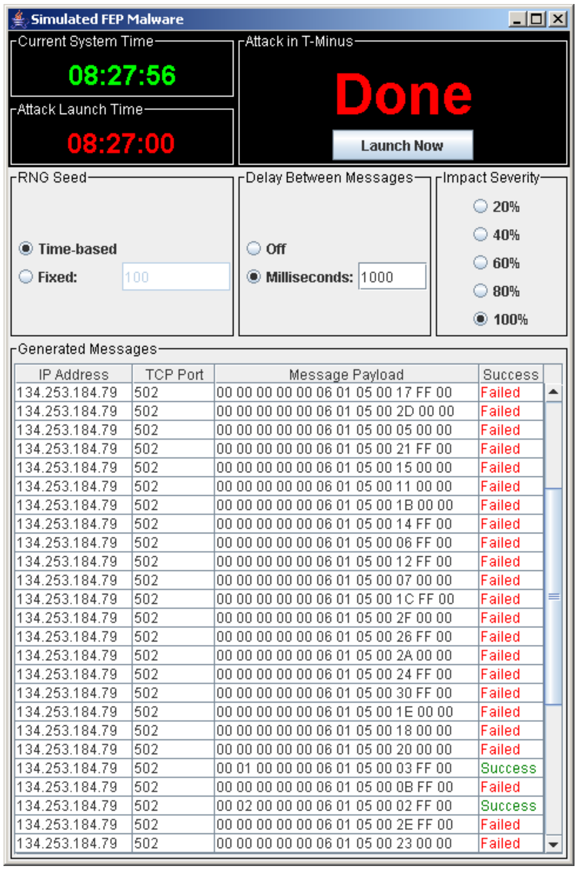


Figure 9: Rogue software scenario

Analysis

For this experiment, the power system was expanded to model a hypothetical power system representing one area of the Institute of Electrical and Electronics Engineers, Inc. (IEEE) RTS-96 system [25]. This is a 24-bus power system with 11 generators and 17 loads, representing an area approximately the size of San Diego. Rather than attempting to modify the FEP, a custom threat was developed that could send *trip* messages to a random subset of the breakers connecting various generators to the network. This custom attack simulator resided on the same computer as the FEP software. Figure 10 shows the user interface developed for this simulator. This interface allowed analysts to vary the numbers (impact severity %) of affected FEPs and to exactly replicate experiments as needed using the *RNG seed*. Additionally, a modification was made to the steady state power model that allowed for load shedding. The load shedding scheme employed was that, as generation was lost and there was insufficient spinning reserve, then the smallest loads in terms of megawatt usage were dropped first. A Monte Carlo approach was taken to execute the simulation and collect data. From this data, system effects were measured in terms of lost loads (customer areas that lost power).



Current System Time
08:27:56

Attack Launch Time
08:27:00

Attack in T-Minus
Done

RNG Seed
● Time-based
○ Fixed: 100

Delay Between Messages
○ Off
● Milliseconds: 1000

Impact Severity
○ 20%
○ 40%
○ 60%
○ 80%
● 100%

Generated Messages

IP Address	TCP Port	Message Payload	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 17 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2D 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 05 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 21 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 15 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 11 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1B 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 14 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 06 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 12 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 07 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1C FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2F 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 26 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2A 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 24 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 30 FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 1E 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 18 00 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 20 00 00	Failed
134.253.184.79	502	00 01 00 00 00 06 01 05 00 03 FF 00	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 0B FF 00	Failed
134.253.184.79	502	00 02 00 00 00 06 01 05 00 02 FF 00	Success
134.253.184.79	502	00 00 00 00 00 06 01 05 00 2E FF 00	Failed
134.253.184.79	502	00 00 00 00 00 06 01 05 00 23 00 00	Failed

Figure 10: The rogue software attack simulator user interface

These experiments varied two parameters—the impact severity (number of FEPs affected by the rogue software) and the spinning reserve. Spinning reserve was varied between 15% and 2.5% for the experiment. Figures 11 and 12 show the results of the testing. In the former, total lost load is compared to the percent of generators taken off line. The red dots represent 15% spinning reserve and the blue, 2.5%. From this plot it can determined that catastrophic effects can be produced even during times of higher spinning reserve if the higher producing generators are the ones affected. This point is reiterated in the latter figure by recognizing that the plots converge (15% or 2.5% spinning reserve) as more generation is lost.

It was apparent through this experimentation that the scenario, as articulated within VCSE, would produce a catastrophic failure within a regional grid. The simulation was for demonstration purposes only and was not a validated model. The desired objective was to provoke conversation with in the workshop, which it did.

A point of discussion in the workshop was that the demonstrated model utilized RTUs in the scenario; and a more realistic model would use PLCs instead.

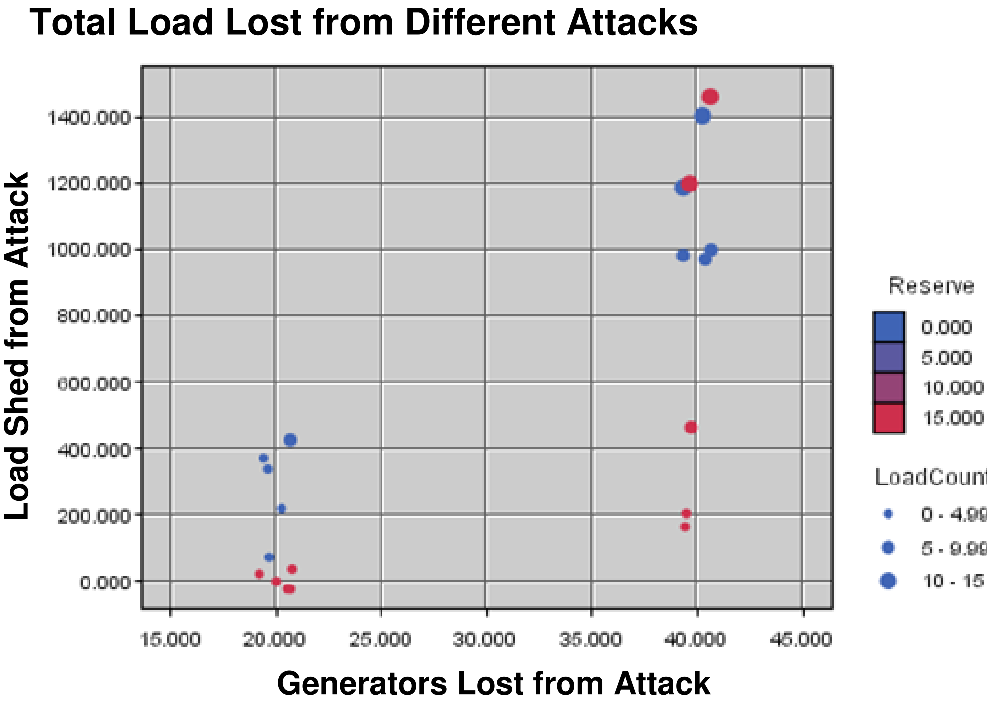


Figure 11: Load lost scatter plot

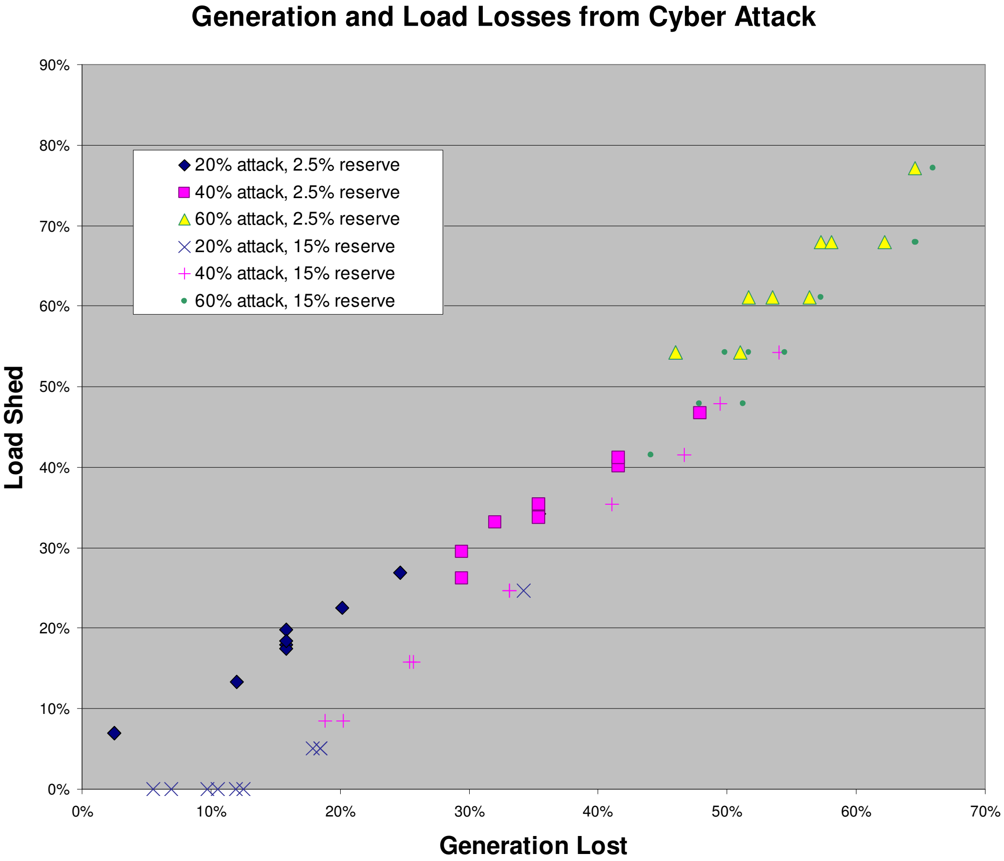


Figure 12: Generation vs. load losses

3.2.4 Dynamic Power Simulator Experiment

There is a set of experiments and scenarios that require a higher fidelity while observing the transient dynamic behaviors of the power system and its consequent effects to, or from, the control system. As a result VCSE has incorporated a dynamic power simulator as an alternative to the static simulator used for most experiments. The VCSE implementation is the University of Missouri-Rolla (UMR)[†] Transient Power Simulator that utilizes MATLAB as its base solver technology. The model implements power-flow-equations and a synchronous-machine model developed at UMR, and were augmented with a speed governor for VCSE purposes.

The purpose of this experiment was to determine whether the dynamic solver could be used within the VCSE and whether the effects could be propagated within a simulation. Specifically, the effects of disabling a generator in the IEEE 14-bus system on the remaining system generators were examined.

At the beginning of the simulation, Generator 1 is producing 232 MWs, Generator 2 is producing 40 MWs, and the three remaining generators are not producing any output. As the system is initialized to be in a steady state, these values remain constant until a change occurs.

At roughly 100 milliseconds into the simulation, Generator 1 is disabled from the attack. This represents a loss of about 85% of the current system generation. This loss forces the power drawn by the loads to be delivered by the remaining four generators and forces the control systems of those generators to respond.

Figure 13 shows how disabling Generator 1 affects the megawatt output of the remaining four active generators. Since the load on the system remains constant, at the moment Generator 1 is disabled, the power output of the remaining generators increases instantaneously to compensate for the sudden loss of power.

Initially, the additional power delivered by each generator comes primarily from energy in the rotation of the generator's rotors. As energy is removed from the rotating rotors in the active generators to compensate for the sudden loss of generators, the rotation of those rotors begins to slow. Figure 14 shows how the rotor frequency of Generator 2 changes in response to the deactivation of Generator 1. As the speed of the rotors determines the frequency of the resulting AC power; a decrease in rotor speeds results in a corresponding decrease in the frequency of the delivered AC power.

[†] UMR is now Missouri University of Science and Technology

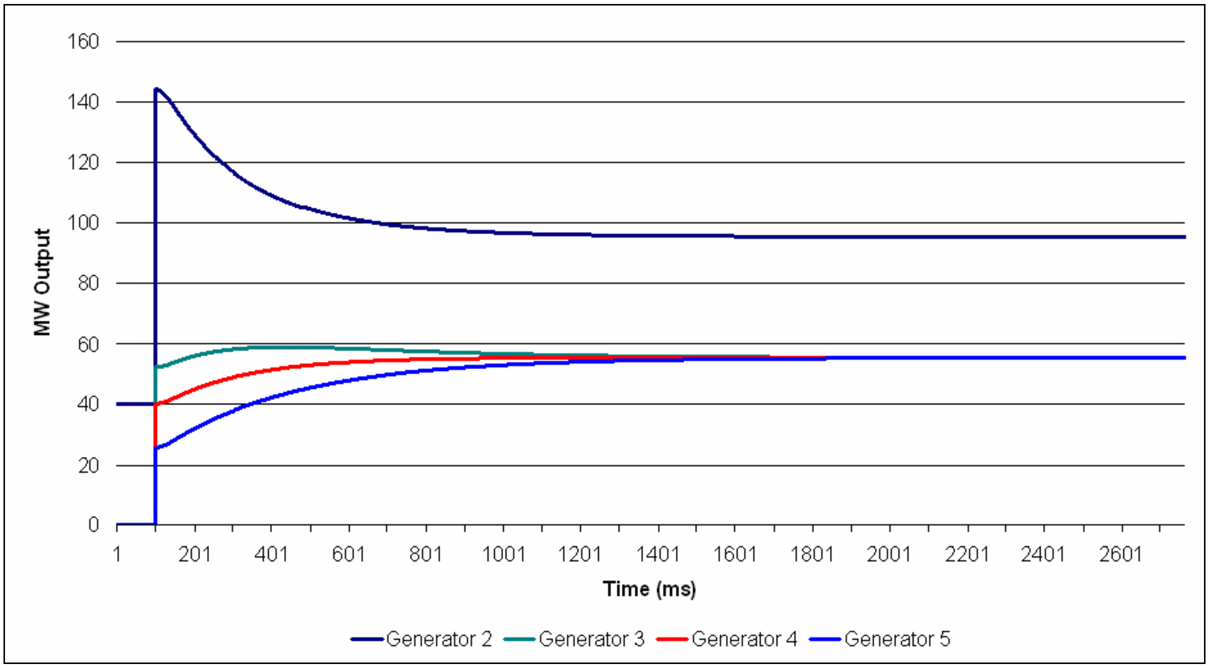


Figure 13: Generator megawatt output

The generator governor control systems are designed to keep the system frequency close to the nominal value of 60 Hz; therefore, as the system frequency decreases, these control systems begin to act by increasing the amount of mechanical power input (torque on the rotor due to the turbine; i.e., it increases the amount of steam fed into the turbine so that the generator speeds up). As the mechanical power input to the generator increases, the frequency's decline begins to slow and eventually to reverse.

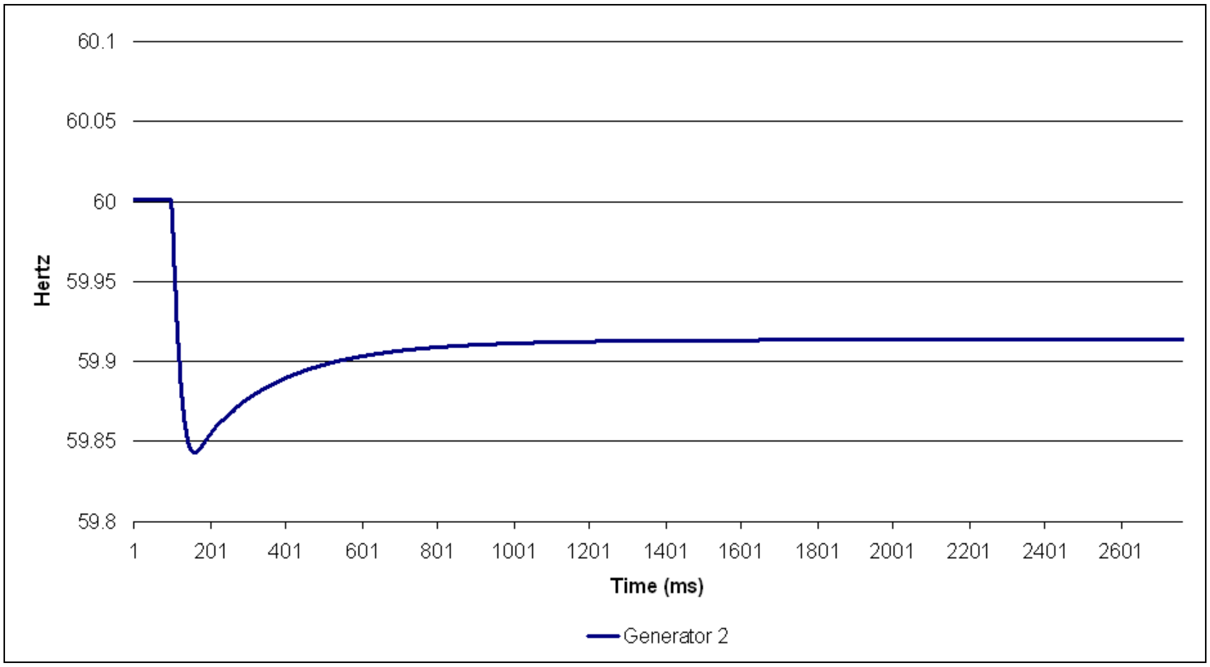


Figure 14: Generator 2 frequency

The difference between the initial steady state frequency and the final frequency (that the system converges to) is due to the speed droop characteristic of the generator speed governors [26]. Figures 14 and 15 show how the Generator 2 speed-governor control system responds to overcome the drop in frequency. The control system steadily increases the mechanical input power to the generator until the generator's frequency begins to increase; at that point it begins to decrease the input power until a steady state is reached. This ‘overshoot’ helps to restore losses in frequency.

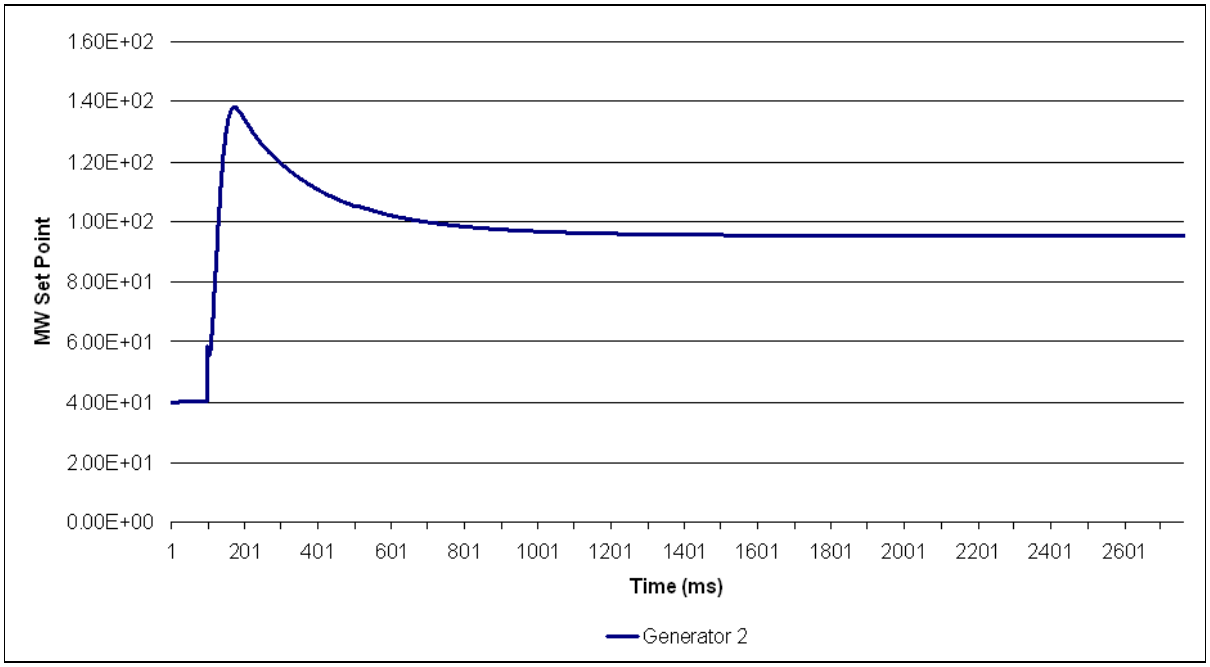


Figure 15: Generator 2 megawatt set point

—This page intentionally left blank —

4 Conclusions

The Virtual Control System Environment (VCSE) is a system for studying cyber threats on system infrastructures. It uses Simulated, Emulated, and Physical components for Investigative Analysis (SEPIA). This paper describes VCSE, tools developed for VCSE analysis, and a variety of analyses performed using VCSE. In discussing the tools and analyses, it is apparent that VCSE is best described as a suite of modeling components rather than a particular model or particular set of modeling components.

This paper describes a variety of tools that have been developed to represent different parts of control systems. In several areas, a multiplicity of models was developed to represent the same types of parts (e.g., remote terminal units [RTUs], power systems, human-machine interfaces [HMIs], and malware toolkits) that exist in control systems. This paper showed how the different ways of representing these different control-system parts could expose different aspects of the vulnerabilities. In other areas, the same tools were used to model the infrastructure elements at different scales (e.g., the 4- and then 24-bus power systems). This scale difference allows the analysts to better understand how the threats operated at different scales.

In explaining how VCSE is used, the paper highlights details of several analyses performed using VCSE. Here, each analysis was focused on understanding the mechanisms used in cyber attacks and the effects that these attacks had upon the systems. In modeling the systems, cyber threats were represented using codes that could actually be used to attack real control systems. In addition, real HMI monitoring software was used to interface with the control environments. Networks that contained physical and either simulated or emulated network segments were used to represent the control-system networks. Simulated RTUs with realistic cyber interfaces were used to represent the control-system interfaces. These simulated RTUs interacted with simulated power systems (two different power models were used).

Using VCSE, analysts first performed detailed analyses on the mechanisms employed in the cyber attacks. These initial studies uncovered a variety of issues demanding further study. In particular, the analysts wondered whether and how effectively the man-in-the-middle (MITM) attacks scaled when applied to increasingly realistic systems. Here the analysts found that, while MITM attacks could be readily executed, successful execution required detailed system knowledge that, these studies showed, could be obtained with varying degrees of difficulty through the combination of insider access and live monitoring software. In addition, the analysts showed that, while the MITM software under investigation hid some of the cyber effects from the operators, this hiding had diminishing effectiveness at larger scale. In particular, the deception algorithms produced outputs that looked suspicious for larger dynamic systems. Also, the analysis uncovered flaws in the deception software that had not been previously observed.

Scaling the systems further, the analysts simulated a modest-scale attack on a larger system to investigate effect propagation. Here, the analysts found that the simulated power system crashed in a fairly linear fashion. This prompted the desire for further analysis, and the paper described initial investigations performed using a higher-fidelity power model.

The rogue software experiment demonstrated VCSE's capability to demonstrate and analyze impacts of a sophisticated attack on a large scale power system. The experiments using dynamic power system simulators demonstrated VCSE's capability to capture transient behavior in power system dynamics. These experiments are important in demonstrating that VCSE can increase the scale and fidelity in different aspects of the simulation model.

5 Recommendations

The VCSE is presently a new and emerging technology. While its toolset library only supports a limited number of analyses, initial results using VCSE are promising. VCSE has the potential for allowing analysts to cost effectively discover, understand, and mitigate control-system vulnerabilities that will otherwise be left to our adversaries to exploit.

Regarding specific experiments described here, future VCSE experiments are needed to understand the extent to which dynamic representations of the power system change the nature or effectiveness of the cyber threats. It needs to be better understood whether cyber-induced power system crashes would behave in the linear fashion indicated with the semi-static power models. It is hoped that this increased insight will lead to a better understanding of the potential impact scale of various cyber threats. In addition, model upgrades are needed to understand the mechanisms of cyber threats applied against different control-system protocols. For example, it is desirable to better understand how—and whether—the more advanced protocols increase or decrease the difficulty that a malicious actor would have in attacking power systems.

Overall, cyber security researchers need to better understand how these and other systemic and imposed barriers constrain malicious actors. That is, there is a need to better understand how, whether, and where the scale and diversity of present-day cyber control systems establish self-protecting structures, increase vulnerabilities, or present opportunities for lower-cost security improvements. For example, researchers need to know where the principle of *security through obscurity* works and where it fails. An enhanced VCSE could address many of these issues.

With a better understanding of the threat dimensions, cyber security research is needed to understand and develop security and mitigation techniques for the cyber threats. For example, the systems studied use typical unsecured, unencrypted, and unauthenticated data connections. Analysts wish to understand the value that security, authentication, and encryption would have on computer-system security. This calls for both modeling the added protections and for investigating threats against them. An enhanced VCSE could provide a testbed for trying out those solutions and discovering whether, where, and how the enhancements help, hurt, or could be improved.

This paper recommends that the U. S. Government make continued investment into expanding and refining the VCSE toolset and approach. To sharpen the development, this paper recommends that all VCSE development efforts be performed in parallel with and focused on supporting relevant studies. By improving its model base, the VCSE project will be able to address problems at larger scale and higher fidelity. By grounding the work in ongoing threat analyses, the VCSE will produce earlier security-enhancing results and keep the modeling effort focused on real cyber-security needs.

This paper recommends that organizations using control-systems for infrastructure control evolve their security approach to leverage current and future simulation and analysis capabilities as represented by VCSE. Current options range from 1) collaborating with analysts to better focus the development of the methodology to 2) utilizing the results of general analyses to better understand and protect against known threats. Future options include utilizing these simulation environments for case-specific analyses and as a basis for operator training and awareness.

The paper recommends that organizations studying cyber security issues invest in modeling and simulation technologies to further and deepen their understanding and as a means of testing their security tools and approaches. This approach should, in particular, be applied to address cyber threats that operate over increasing scales and impacts.

Appendix A: References

[1] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, "The Roadmap to Secure Control Systems in the Energy Sector at http://www.controlsystemsroadmap.net/

[2] U.S. DOE Office of Electricity Delivery and Energy Reliability, Roadmap at http://www.controlsystemsroadmap.net

[3] CIA Says Hackers Have Cut Power Grid, Robert McMillan, IDG News Service, Saturday, January 19, 2008 6:00 AM PST (see also http://www.washingtonpost.com/wp-dyn/content/article/2008/01/20/AR2008012000056.html)

[4] Internet Law—CIA Report: Cyber Extortionists Attacked Foreign Power Grid, Disrupting Delivery, K. O'Connell, IBLS Editor, Wednesday, January 23, 2008 (http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1963)

[5] Office of Electricity Delivery and Energy Reliability at http://www.oe.energy.gov/

[6] U.S. DOE Office of Electricity Delivery and Energy Reliability, Roadmap at http://www.controlsystemsroadmap.net

[7] U.S. DOE Office of Electricity Delivery and Energy Reliability, Roadmap at http://www.controlsystemsroadmap.net

[8] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, SCADA Cyber Security Testbed Development, at http://www.iti.uiuc.edu/tcip/NAPS06.pdf

[9] M. Liljenstam, J. Liu, D. Nicol, Y. Yuan, G. Yan, and C. Grier, RINSE: the Real-time Immersive Network Simulation Environment for Network, Proceedings of the Workshop on Principles of Advanced and Distributed Simulation (PADS'05), 2005 (at http://ieeexplore.ieee.org)

[10] INEL Technologies: Real Time Digital Simulator at http://inl.gov/nationalsecurity/factsheets/docs/rtds.pdf

[11] RTDS Technologies at http://www.rtds.com

[12] INL Research Programs in National and Homeland Security at https://inlportal.inl.gov/portal/server.pt?open=514&objID=1707&parentname=Gateway&parentid=None&mode=2&in_hi_userid=200&cached=true

[13] U.S. DOE Office of Electricity Delivery and Energy Reliability, Roadmap at http://www.controlsystemsroadmap.net

[14] PowerWorld Corporation at http://www.powerworld.com/

[15] OPNET Network Simulation Tools at http://www.opnet.com

[16] T. Tarman, M. McDonald, Hybrid Simulation And Virtualization Research For Information Assurance Analysis, 76th MORS Symposium (MORSS), New London, CT, 06/10/2008

[17] Modicon ModBus Protocol Reference Guide (PI–MBUS–300 Rev. J) at http://www.modbustools.com/PI_MBUS_300.pdf

[18] Areva T&D Corporation, producers of Areva E-TERRACONTROL HMI software at http://www.areva-td.com/

[19] B. Richardson, JPowerflow at http://sourceforce.net/projects/jpowerflow

[20] Dynamips, a Cisco 7200 Simulator at http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator

[21] Ettercap suite for man-in-the-middle attacks on LANs at http://ettercap.sourceforge.net/

[22] http://en.wikipedia.org/wiki/ARP_spoofing

[23] http://www.wireshark.org

[24] Modicon ModBus Protocol Reference Guide (PI–MBUS–300 Rev. J) at http://www.modbustools.com/PI_MBUS_300.pdf

[25] C. Grigg, P. Wong. et al, Reliability Test System Task Force, The IEEE Reliability Test System—1996, IEEE Transactions on Power Systems, Vol. 14, No 3, August 1999.

[26] Speed Droop and Power Generation, Application Note 01302, Woodward Governor Company, 1991; at http://www.canadiancontrols.com/documents/technical/Speed%20Droop%20and%20Power%20Generation.pdf

Appendix B: Acronyms, Symbols, and Abbreviations

2-D	two-dimensional
3-D	three-dimensional
AC	alternating current
ACS	automatic control system
AMAS	ACS Monitor and Analysis System
ARP	address resolution protocol
DES	discrete event simulation
DHS	Department of Homeland Security
DIS	Distributed Interactive Simulation
DNP3	distributed network protocol
DoD	Department of Defense
DOE	Department of Energy
DOE/OE	DOE Office of Electricity Delivery and Energy Reliability
FEP	front-end processor
GHz	gigahertz
HMI	human-machine interface
HVAC	high voltage alternating current
HVDC	high voltage direct current
Hz	hertz
ICCP	inter-control center communications protocol
ICMP	internet control message protocol
IED	intelligent electronic devices
INL	Idaho National Laboratory
I/O	input/output
IP	Internet protocol
IT	information technology
MITM	man-in-the-middle
MW	megawatt
NI	National Instruments
NIB	Network-In-a-Box
NSTB	National SCADA Test Bed
OPSAID	Open Process control system Security Architecture for Interoperable Design
OPNET	(company providing network and application management software and hardware)
PLC	programmable logic controller
RINSE	Real-time Immersive Network Simulation Environment for Network Security Exercises
RTDS	Real-Time Digital Simulator
RTU	remote terminal units
SCADA	Supervisory Control And Data Acquisition
SEPIA	simulated, emulated, and physical components for investigative analysis
SF	simulation framework
SQL	Structured Query Language
TCP	transmission control protocol

UI	user interface
UMR	University of Missouri–Rolla
VCSE	Virtual Control System Environment
VCSE-SF	VCSE simulation framework
VM	virtual machine

Appendix C: Glossary

address resolution protocol. In computer networking, the address resolution protocol (ARP) is the method for finding a host's hardware address when only its network layer address is known.

adversary reach. In cyber threat analysis, it is important to understand how far into a network an adversary can effectively reach with a given suite of codes. For example, many threat tools can only reach the firewalls of well-protected networks while others may reach far inside the network.

automatic control system. This is any control system that uses automation technologies.

communication protocol. In the field of telecommunications, a communications protocol is the set of standard rules for data representation, signaling, authentication, and error detection required to send information over a communications channel.

control system networks. This is a computer network used to support control system cyber traffic.

core/kernel elements. Modern software systems are built using layered architectures. The software modules at the innermost layer of any architecture are called the core or kernel elements.

cyber. This term refers to *electronic* or computer-related counterparts of a pre-existing product or service.

cyber security posture. This term refers to how well an organization's cyber-security tools, techniques, and processes match the current threat environment.

discrete event simulation. In discrete-event simulation (DES), the operation of a system is represented as a chronological sequence of events. Each event occurs at an instant in time and marks a change of state in the system

distributed control system. A distributed control system refers to a control system usually of a manufacturing system, process or any kind of dynamic system, in which the controller elements are not central in location (like the brain) but are distributed throughout the system with each component sub-system controlled by one or more controllers. The entire system of controllers is connected by networks for communication and monitoring.

Distributed Interactive Simulation. Distributed Interactive Simulation (DIS) is an open standard for conducting real-time platform-level war-gaming across multiple host computers and is used worldwide especially by military organizations, but also by other agencies such as those involved in space exploration and medicine.

Dynamic Link Library. Dynamic-Link Library is Microsoft's implementation of the shared library concept in the Microsoft Windows and OS/2 operating systems.

emulated devices. An emulator duplicates (provides an emulation of) the functions of one system using a different system, so that the second system behaves like (and appears to be) the first system. An emulated device is one such device that exists within a system.

energy management system. An energy management system is usually a system of computer-aided tools used by operators of electric utility grids to monitor, control, and optimize the performance of the generation and/or transmission system.

Ethernet. Ethernet is a family of frame-based computer networking technologies for local area networks (LANs). The name comes from the physical concept of the ether. It defines a number of wiring and signaling standards for the physical layer, through means of network access at the Media Access Control (MAC)/Data Link Layer, and a common addressing format.

front-end processor. In this report, a front end processor (FEP) is a computer used for data and control message translation, aggregation, and possible automation of supervisory control between an HMI and RTUs. A FEP may also support other system functions such as data logging or historian systems.

human-machine interface. The user interface (or human-computer interface) is the aggregate of means by which people—the users—interact with the system. It is a particular machine, device, computer program, or other complex tools.

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

Internet protocol. The Internet protocol (IP) is the method or protocol by which data are sent from one computer to another on the Internet.

legacy systems. Legacy systems are those that were fielded prior to the establishment of current requirements. These systems do not typically meet the requirements that were established after they were produced. For cost reasons, they are often part of the newer systems.

malware. Malware, also known as *malicious software*, is software designed to infiltrate or damage a computer system without the owner's informed consent. The term is a portmanteau of the words malicious and software.

man-in-the-middle. The man-in-the-middle attack (MITM)—or bucket-brigade attack, sometimes Janus attack—is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

MATLAB. MATLAB is a numerical computing environment and programming language. MATLAB was created by The MathWorks Inc.

ModBus. ModBus is a serial communications protocol published by Modicon in 1979 for use with its programmable logic controllers (PLCs). It has become a de facto standard communications protocol in industry and is now the most commonly available means of connecting industrial electronic devices.

National SCADA Test Bed. The National SCADA Test Bed (NSTB) is a DOE multi-laboratory program that addresses the security challenges of control systems in the energy sector through control systems testing, research and development, advanced technology development, control systems requirements development, and industry outreach.

Network-In-a-Box. Product developed at Sandia to emulate networks that contain systems of several routers; literally, a network-in-a-box.

Newton-Raphson iteration. In numerical analysis, Newton's method (also known as the Newton–Raphson method, named after Isaac Newton and Joseph Raphson) is perhaps the best known method for finding successively better approximations to the zeros (or roots) of a real-valued function.

operator control units. See also human machine interface (HMI)

OPNET. OPNET Modeler, a network modeling and simulation software solution, is one of OPNET's flagship solutions.

OPSAID. OPSAID (Open PCS [Process Control System] Security Architecture for Interoperable Design) is a joint government/industry project to develop interoperable open system security architecture for potential use by electric utility companies.

power grid. A power grid is a set of high-voltage electrical transmission lines connected by direct-current lines. Dispatch centers maintain and control the flow of electricity over the grid, supplying electricity to meet the demand.

programmable logic controller. A programmable logic controller (PLC) or programmable controller is a digital computer used for automation of industrial processes, such as control of machinery on factory assembly lines. Unlike general-purpose computers, the PLC is designed for multiple inputs and output arrangements, extended temperature ranges, immunity to electrical noise, and resistance to vibration and impact.

PXI. PXI (PCI eXtensions for Instrumentation) is one of several modular electronic instrumentation platforms in current use. These platforms are used as a basis for building electronic test equipment or automation systems, such as might be used in a mobile phone manufacturing test environment. Based on industry-standard computer buses and loaded up with extra features to facilitate electronic test, they permit a great deal of flexibility in building the exact test equipment or automation system required.

remote terminal unit. A remote terminal unit (RTU) is a microprocessor controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA system by transmitting telemetry data to the system and/or altering the state of connected objects based on control messages received from the system.

SCADA. Supervisory Control And Data Acquisition (SCADA) generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility based.

simulated devices. A simulator models a subset of the functions of a system using a different system, so that the second system behaves roughly like the first system. A simulated device is one such device that exists within a system.

simulation framework. A framework is a basic conceptual structure used to solve or address complex issues. A simulation framework is a conceptual structure used to solve or address issues of simulation. The VCSE simulation framework is a suite of software that people use to write simulation models to represent various aspects of control systems.

spinning reserve. The spinning reserve is the extra generating capacity that is available by increasing the power output of generators that are already connected to the power system. For most generators, this increase in power output is achieved by increasing the torque applied to the turbine's rotor.

Structured Query Language. Structured Query Language (SQL) is a database computer language designed for the retrieval and management of data in relational database management systems (RDBMS), database schema creation and modification, and database object access control management.

transmission control protocol. The transmission control protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP is so central that the entire suite is often referred to as TCP/IP. Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet, TCP operates at a higher level, concerned only with the two end systems. TCP provides reliable, ordered delivery of a stream of bytes from one program on one computer to another program on another computer.

virtual machines. A virtual machine (VM) is a software implementation of a machine (computer) that executes programs like a real machine.

WireShark. WireShark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software, and communications protocol development, and education.

—This page intentionally left blank —

Distribution

1	MS1235	Gregory N. Conrad, 5631
1	MS1235	Michael J. McDonald, 5633
1	MS0672	Regis H. Cassidy, 5629
1	MS0671	Robert D. Pollock, 5633
1	MS0671	Jennifer M. DePoy, 5628
1	MS1108	Juan J. Torres, 6332
1	MS1202	Roxana Jansma, 5631
1	MS0899	Technical Library, 9536

Sandia National Laboratories