SANDIA REPORT
SAND2010-0568
Unlimited Release
Printed February 2010

Modeling and Simulation for Cyber-Physical System Security Research, Development and Applications

Michael J McDonald, John Mulder, Bryan T Richardson, Regis H. Cassidy, Adrian Chavez, Nicholas D Pattengale, Guylaine M Pollock, Jorge Mario Urrea, Moses Daniel Schwartz, William Dee Atkins, Ronald D. Halbgewachs

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.

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

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

SAND2010-0568
Unlimited Release
Printed February 2010

Modeling and Simulation for Cyber-Physical System Security Research, Development and Applications

Michael J McDonald, John Mulder, Bryan T Richardson, Regis H. Cassidy, Adrian Chavez, Nicholas D Pattengale, Guylaine M Pollock, Jorge Mario Urrea, Moses Daniel Schwartz, William Dee Atkins, Ronald D. Halbgewachs

Information Systems Analysis Center
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1235

Abstract

This paper describes a new hybrid modeling and simulation architecture developed at Sandia for understanding and developing protections against and mitigations for cyber threats upon control systems. It first outlines the challenges to PCS security that can be addressed using these technologies. The paper then describes Virtual Control System Environments (VCSE) that use this approach and briefly discusses security research that Sandia has performed using VCSE. It closes with recommendations to the control systems security community for applying this valuable technology.

Acknowledgements

We wish to thank the National SCADA Test Bed (NSTB) program at the United States Department of Energy's Office of Electricity Delivery and Energy Reliability which provided the funding for the enabling research for this effort.

We wish to thank the Department of Homeland Security (DHS) and the Institute for Information Infrastructure Protection (I3P) for providing the major funding for our work in cyber security in the Oil and Gas sector and for sponsoring this paper.

Finally, we wish to thank the many researchers, team leaders and program managers at Sandia and our partner agencies who have produced the technologies used in the analyses described here. We especially thank Greg Conrad, Eric Lee, Ryan Custer and Jonathan Margulies for their initial work on VCSE. We thank Brian Van Leeween, David Burton, Vince Urias, Uzoma Onunkwo, and Tom Tarman for their work in hybrid network technologies. We thank Ray Parks, Rolf Carlson, and Ben Cook for their valuable insights in SCADA security.

Table of Contents

Background 10
Sandia's VCSE Framework and Architecture 11
Practical VCSE Application 15
Cyber Defense Training 15
Exploring Electrical Power System Vulnerabilities 17
Developing and Testing Protections and Mitigations 17
Understanding Possible Impacts of Particular Cyber Threats 19
Conclusions 22
Recommendations 23
References 24

Table of Figures

Figure 1: System diagram of a canonical cyber-physical system 12
Figure 2: VCSE Toolbox 14
Figure 3: VCSE model of a small refinery before and after a damaging cyber attack 16
Figure 4: VCSE model of an electric power distribution system before and after a cyber attack 17
Figure 5: VCSE model of a PLC-controlled burner before and after attack 18
Figure 6: Attack Initiated Through False Address Advertisement 20

This page intentionally left blank.

Introduction

The nation is greatly and appropriately concerned with computer and network vulnerabilities and the threats they pose to our infrastructures. Presidential-level concern dates back to 1998 (PDD-63). Public accounts of malicious attacks on supervisory control and data acquisition (SCADA) and distributed control systems (DCS) are appearing with increasing frequency. This paper describes advances Sandia has made in the science of protecting these cyber-physical systems.

The computer aspects of cyber-physical systems are much like traditional Information Technology (IT) systems. Similarities include the use of Transmission Control Protocol (TCP) and Internet Protocol (IP) over Ethernet, the use of standard Personal Computers (PCs) running mainstream operating systems for engineering workstations and control interfaces, and the use of IT network devices such as switches and routers. They also share vulnerabilities such as network protocols that are too trusting, software stacks with buffer overflows, indirect connectivity to the Internet, unsecured product cycle issues, and authentication control. At the surface, the technical differences seem mild. Differences include computer and network configurations, applications software, data exchange characteristics including timing issues, and unique end point devices.

Though similar in many respects, cyber-physical systems are different from IT systems, and, from a security perspective, they are dramatically different. Cyber attacks on physical systems can lead to serious consequences including product loss, damage, injury and death. Adversaries may need to make many unique technical steps to achieve these consequences. Operators might need to perform complex procedures to bring attacked physical systems to a safe state. As a result, defenders must be attuned to the unique patterns of these attacks so that they can defend against them and they must be attuned to the physicality of the systems so that they can respond appropriately. Addressing these differences drive the work behind this report.

Preparations to better secure America after the 9/11 attacks heightened our policy planners' awareness on of our dependence upon infrastructures including electrical power, water, oil, gas, and special material production and distribution systems. At the time, however, the focus was on adversaries who would attack these infrastructures physically. This translated to a focus on the few physical assets that terrorist cells could attack to produce the greatest effects. Over time, policy makers (110th Congress-2008) and analysts (CERT-CSSP) came to understand the important role that cyber-enabled control systems play in the vulnerability of these infrastructures.

Most people recognize how dangerous machines can become when put in the hands of unskilled operators. In one case, a whole nuclear power plant was inadvertently shut down through the simple act of installing control system updates on a corporate server (Krebs 2008). Analysts asked: What if whole infrastructures were put into the hands of terrorists through their control systems? Could cyber-skilled terrorists cause even more damage than operators? Could cyber-skilled terrorists

circumvent the safety and security mechanisms that protect systems from mistakes and abnormal conditions to drive the systems directly to ruin? They found that many of these control systems share a common architectural blueprint and are implemented with a common core of inter-compatible elements (CERT-CSSP). As a result, cyber-enabled terrorists could potentially use their malware in many places to simultaneously attack many systems at once (Saydjari-2007). Policy makers, analysts and cyber experts alike have thus become clear on the pressing need to keep terror's hands off the controls of the cyber controls of these physical systems.

Addressing this need is not easy. Analysts, engineers and stakeholders even disagree on how to approach the problem. One extreme course of action is to isolate these control systems from the larger world. Unfortunately today's infrastructures rely upon the very interconnectedness that drives the cyber vulnerabilities:

- Businesses rely upon the huge efficiencies gained by connecting control systems directly to the larger business world and their businesses to consumers through the Internet.
- Distance, data rate and timing requirements for tight coordinated control and human interfacing necessitate sophisticated technologies of integration that rely upon modern networking.
- The huge engineering efficiencies that made control systems possible derive from their use of common software, computer hardware, and network elements that are replicated, refined, exchanged and produced globally.

Disconnect the Internet or corporate network? The cost is business efficiency. Discontinue using common software, computers or networks? The cost may be a complete loss of function. In this light we see that even the best designers can only partially disconnect real cyber-control systems. Rather, they must leave them partly connected and consequently treat the systems as only partially secure. The current best practice is to first propagate protections through all the layers of connectedness to limit adversary reach. With protections in place, they must then augment these defenses with intrusion detection and monitoring systems to maximize the chance that breaches are detected and stopped. Finally, they must remain ever vigilant to new and emerging threats and understand the impacts that new threat-relevant technologies may have upon their security.

These realistic solutions are fraught with complexities and inherent complex vulnerabilities that security experts must understand. Additionally, analysts must understand how adversaries could take advantage of known and unknown security flaws and system features. Armed with this knowledge, analysts can then determine how these flaws and features combine at a system-level to give the adversaries dangerous levels of control. Knowing this, then, they can develop, analyze and prioritize methods for mitigating or reducing the chance that an adversary might gain control.

The remainder of this paper describes new modeling and simulation technologies that Sandia developed and is using to aid in this analysis. It describes Sandia's environment, called the Virtual Control System Environment (VCSE) that uses this

approach and briefly discusses security research that Sandia has performed using VCSE.

Background

Engineering science offers a variety of approaches or methods for analyzing complex problems and developing design solutions. As a science and engineering laboratory, Sandia's approach is to adapt and apply science and technology (S&T) to the security problem at hand.

The simplest, though least rigorous S&T methods uses descriptive models, such as diagrams with supporting text, to describe the systems for easy analysis and understanding. Network diagrams with accompanying descriptions of applicable malware methods and mitigation technologies are greatly used examples of this approach. For some aspects of the problems, software is available to analyze these descriptive models to automatically search for and prioritize solution concepts. Attack graph theory is an example of how this automation is applied in network security analysis (Phillips -1997), (Lippmann-2005).

At the other extreme, tests using physical test harnesses, working prototypes and live full-scale tests provide among the most rigorous tools for analysis. The community studying cyber-physical security has produced a variety of physical testbeds. Many researchers have connected laboratory-scale equipment to sophisticated control systems in order to study device-level vulnerabilities associated with the control system equipment and software. Some very sophisticated testbeds have also been built. The INL Aurora demonstration (MESERVE-07), for example, used a high fidelity, high-expense testbed. Unfortunately, practical limitations on approaches, measurement techniques and practical testbed sizes often restrict analysts to addressing overly narrow sets of problems. For example, aforementioned Aurora demonstration provided the last data point from that testbed.

At a middle ground, scientists and engineers use models that exhibit key characteristics of the systems under study for lower-cost studies. While cyber-physical system models can be fully synthetic or simulated, many aspects are best addressed using hybrid approaches. For example, (Lee-2006) describes Sandia's first effort to develop a hybrid model for SCADA system security analysis. (Davis-2006) describes a similar effort at UIUC. Since first developing the technologies, researchers have made dramatic progress to improve cyber-physical system representations and use the models for analysis (McDonald-2008), (Bergman-2009), & (McDonald-2009).

Sandia's VCSE Framework and Architecture

VCSE models represent the relevant portions of cyber-physical systems and their threats. They are instrumented to facilitate the analysis of the physical effects that the threats may have on the systems under study. The models are constructed from real, emulated[1] and simulated[2] components that are vulnerable to actual, representative and simulated malware and other hostile actions. Sandia's VCSE is, by its nature, a distributed tool-oriented environment. VCSE instantiations or models vary by the specific tools brought together and their configurations. Generally, Sandia's VCSE models combine real or representative SCADA systems, a mixture of real and emulated network components, emulated control interfaces, and simulated physical plant models. Cyber threats are represented with actual or representative malware. Physical threats are represented in the physical model and the analysis team members typically play the part of insiders and cyber terrorists.

Figure 1 diagrams the connectivity of the elements that form a typical cyber-physical system that VCSE modelers are concerned with. VCSE models can address each element within these systems or analysts can omit portions of the system if they are not relevant to the questions being addressed. Generally, modelers separately represent the physical systems, their control (including SCADA) systems, the supporting networks, the security appliances, and the threats that the analysts are concerned with through separate tools or separate models within a VCSE toolset.

Sandia has focused its VCSE work on several activities. First is in developing an understanding of and then integrating a variety of real system components into VCSE models. Components include commercial SCADA systems, intelligent electronic devices (IEDs),[3] computers and operating systems, networking devices and representative threat software (or malware). We have become expert at using and integrating a variety of commercial tools to serve our purposes. We have also developed our own stand-in SCADA software within which we can insert specific vulnerabilities and mitigation concepts. In this way, the representative malware that Sandia modelers use to study these particular concepts concerning SCADA systems cannot be used maliciously against fielded SCADA systems. It is also noteworthy that

[1] Emulators duplicate (provide 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. For purposes of this discussion, emulators include software-based emulators that emulate real computer hardware as well as simulation models that are configured to emulate computers and physical equipment.

[2] A simulation is the imitation of some real thing, state of affairs, or process. VCSE simulations are generally built as computer models. Most of the simulations have emulation interfaces to behave, on the outside, as an emulator

[3] Various industries use different terms to describe the different devices that form the cyber-to-physical bridge. In this paper, we borrow the term Remote Terminal Unit (RTU) as the most basic of these devices. A Programmable Logic Controllers (PLC) is a more sophisticated IED. In the electric power industry, the term Relay ranges from a basic mechanical switch to a sophisticated, programmable IED. Some modern thermostats are sophisticated, networked IEDs. The term IED covers all these types of devices.

Sandia typically uses Virtual Machine (VM) technologies to host real system components. In this way, for example, analysts can run a small network of SCADA tools on one host computer.

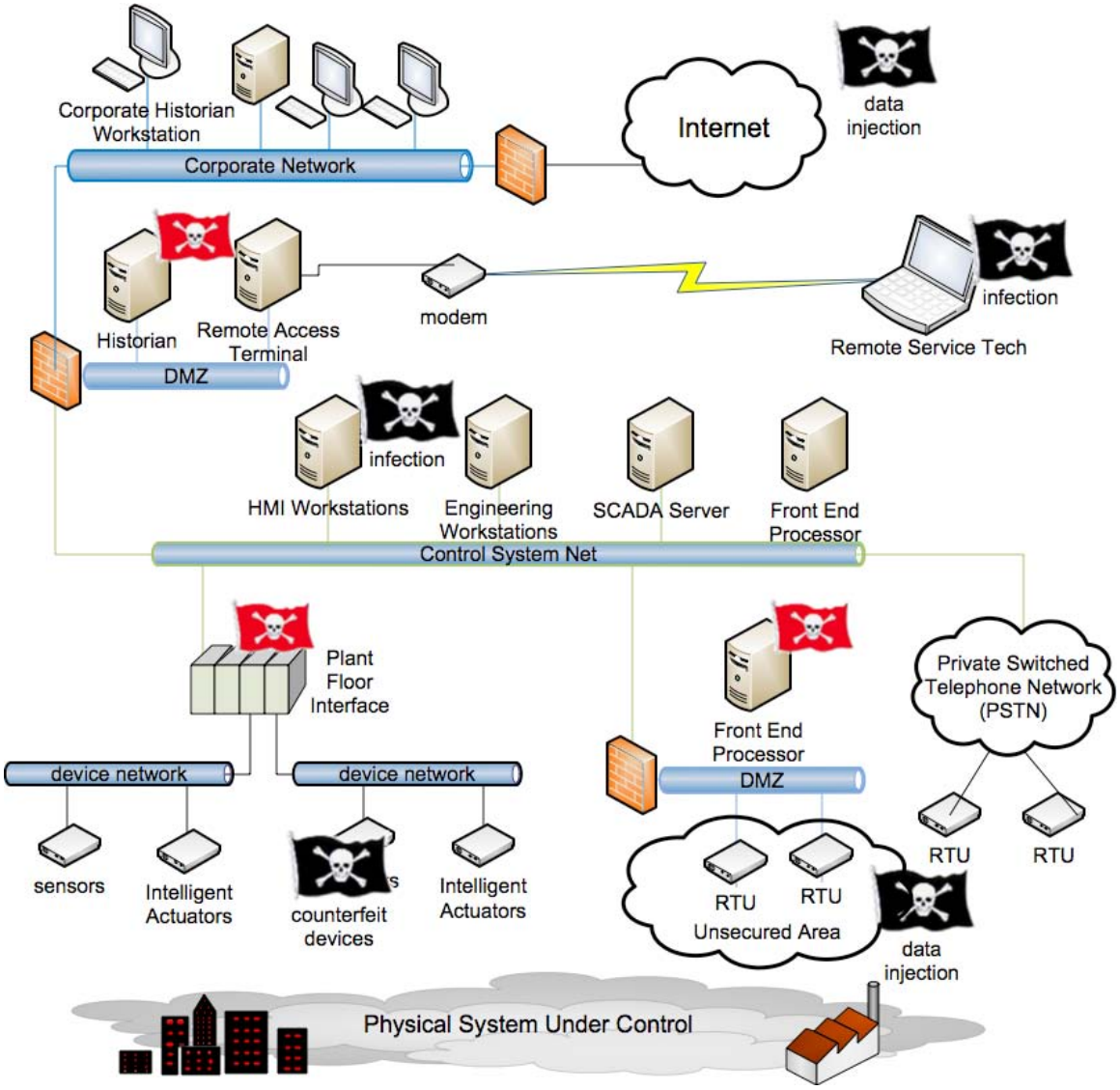

Figure 1: System diagram of a canonical cyber-physical system

Sandia's second contribution has been in developing technologies to more cost-effectively represent networks that host the SCADA systems. This work leverages separate Sandia Laboratory Directed Research and Development (LDRD) projects to develop a general hybrid modeling system for analyzing networks and their vulnerabilities (McDonald-8-2008), (Burton-2009). Using that work, VCSE modelers can configure networks of routers via a single XML file and then instantiate emulators to form these networks through a single hypervisor. In addition, modelers can efficiently utilize OPNET to model complex networks containing many devices and then use OPNET's System in the Loop (SITL) capability to run these

simulated networks as large network emulations. These hybrid networks then interact with real networking hardware, route and pass control system and any other Internet Protocol (IP) traffic, block network access using access control lists, and distribute router configurations and even respond accurately to malicious routing protocol attacks and misconfigurations as if the emulated components were real (Van Leeuwen-2009). In short, these hybrid networks look and act like large-scale real networks but are implemented at a fraction of their cost.

Sandia's third contribution is in developing simulation models of critical infrastructures and providing emulation interfaces so that they interoperate with SCADA systems and malware. Sandia's original work on simulating infrastructures focused on building a purpose-built prototype simulation framework and populating it with device models. By 2008, this prototype had reached a Technical Readiness Level (TRL) of between 4 and 5. To break through the next level of technical sophistication, Sandia used the prototype as a study and test environment for analyzing control system vulnerabilities. In addition to analyzing relevant problems, Sandia then used these efforts to study the simulation architecture itself and to develop a robust set of requirements for advancing the simulation architecture. Completing this work, Sandia then evaluated the applicability of other simulation tools in October 2008. As a result, Sandia adopted another tool, called Umbra (Gottlieb-2002), which another group at Sandia had developed for simulating, analyzing and controlling complex physical and human-involved systems.

Sandia's patented Umbra Framework is a TRL-7 tool that has been successfully applied both within and outside Sandia in a variety of national security, military, physical security, hazardous work, and industrial automation applications. It is an ideal tool for modeling physical and control systems and for interfacing with actual equipment and SCADA system elements. Because the low-level portions of the models are programmed in C++, Umbra scales very well in modeling large systems. Since Umbra includes a powerful scripting language and the ability to configure models using XML files, models can be readily built, used and adapted by analysts who have limited programming skills.

While Umbra serves as a fully capable simulation and visualization environment in itself, a key feature of Umbra is in its features that support effective integration with other simulation environments and tools. Using this capability, Sandia researchers also began using Umbra as a go-between to add emulation capabilities to other infrastructure simulation tools. Most notably, Sandia interfaced Umbra with PowerWorld (http://www.powerworld.com) to allow PowerWorld models to emulate electrical power systems that are controlled from traditional SCADA systems. In this integration, Umbra models the RTUs, the terrain, the breakers and the sensors while PowerWorld models the actual flow of electricity through the power system. Using the combined capability, analysts can simulate both cyber and physical attacks (e.g., physically breaking system elements) on the power system.

A final contribution to VCSE development has been extending the computer emulation concept to address control system elements. As a first step in that direction, Sandia worked with the SoftPLC Corporation (http://www.softplc.com) to develop and integrate an emulated version of their SoftPLC product for VCSE research. Using this technology, Sandia can launch a large number of emulated PLCs on a single workstation-class computer. Because the PLCs natively interoperate with commercial SCADA systems, no change was needed to make these PLCs interoperate with our SCADA systems. At the lower level, where the PLCs interface with the simulators, we choose to use these same protocols as a first method of integration. Here, for example, the PLCs interface with the Umbra simulations through a Modbus connection (as if they were communicating with RTUs in a distributed control system). It is notable that SoftPLC has proposed a variety of approaches for developing more efficient interfaces that are under consideration at Sandia.

Figure 2 illustrates these combined contributions as a VCSE toolbox. Within the toolbox, the Human element represents real operators along with the analysts and engineers we have trained to act as operators and malicious attackers. The Physical box represents the various devices, software and malware that we are skilled in successfully integrating into larger VCSE models. The Emulation box holds the hybrid networks, the control emulators and the emulation interfaces to the simulation software. Finally, the Simulation toolbox represents the models we have built in Umbra along with the models that we've integrated into VCSE through Umbra.

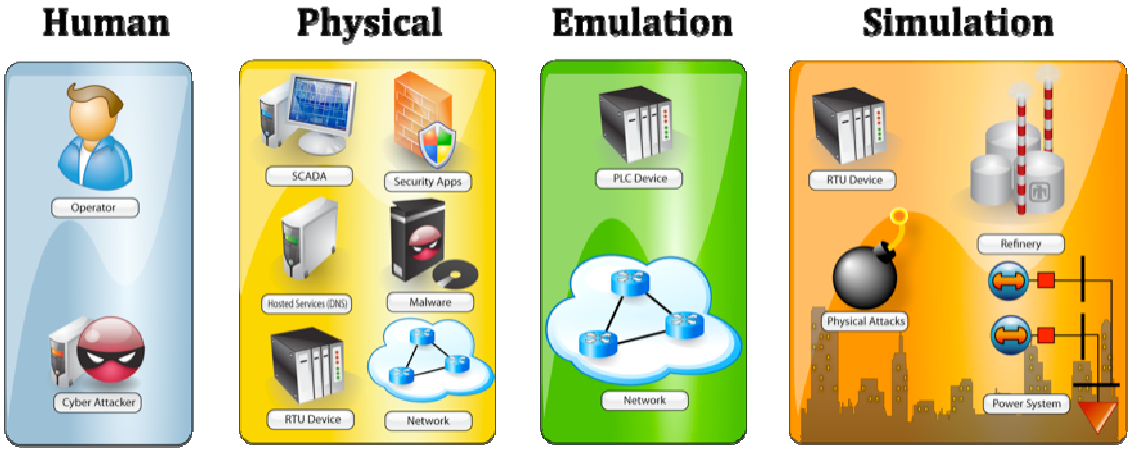

Figure 2: VCSE Toolbox

Practical VCSE Application

With its capability, expressibility, ease of use, and powerful graphics, VCSE has become a preferred tool at Sandia for analyzing the complex problems and developing design solutions in cyber-physical system security. Broadly, the applicable analysis and design functions fall into several categories.

- Discovery out of completeness: Developing working system models entails deep drill down and discovery of small details that can cause large system impacts. VCSE stimulates this process and provides a "proof of completeness" in terms of easily understood system models that can be effectively validated by domain experts.
- Concept exploration and validation: Because VCSE models operate as emulation analogs to the real systems, analysts can freely (and safely) execute any step that an adversary might take on the real system. In addition, due to the open nature of the VCSE structure, analysts can model in and test the impacts of undiscovered but theoretically possible flaws and vulnerabilities before any actual flaws are found.
- Mitigation design and testing: Analysts perform many design-implement-test iterations in developing and refining successful mitigation technologies. VCSE models that include real malware provide ideal environments for this activity.
- Red teaming: After collecting data on sites, red teams can build models to reason about attack scenarios. VCSE models provide significantly higher fidelity than the paper models that are traditionally used here.
- Cyber defense training: People are a key part of any cyber defense. Because VCSE models work like the real systems, they provide an ideal training environment for building the people skills. With VCSE, operators can experience the effects of cyber attacks and IT specialists can learn about the signatures of cyber-physical attacks and how defense failures can lead to disaster. VCSE-based cyber defense requires skills in IT networks, cyber-physical systems, SCADA, and the underlying physical systems and it is difficult to find personnel skilled in all areas. By addressing all of these areas, VCSE provides an ideal team-training environment where members can use their knowledge to help each other learn.

The remainder of this section details specific examples of how Sandia has used VCSE to support these analysis and design functions.

Cyber Defense Training

As a first example, Figure 13 shows screen images from a recently developed VCSE physical system simulator, called OPSAID, that Sandia developed to train cyber defense concepts to oil refinery operators. The top images show its WonderWare-based controls and plant model before a cyber attack and the bottom after attack. In operation, students could experience and attempt to defend against actual malware that researchers had found on the Internet.

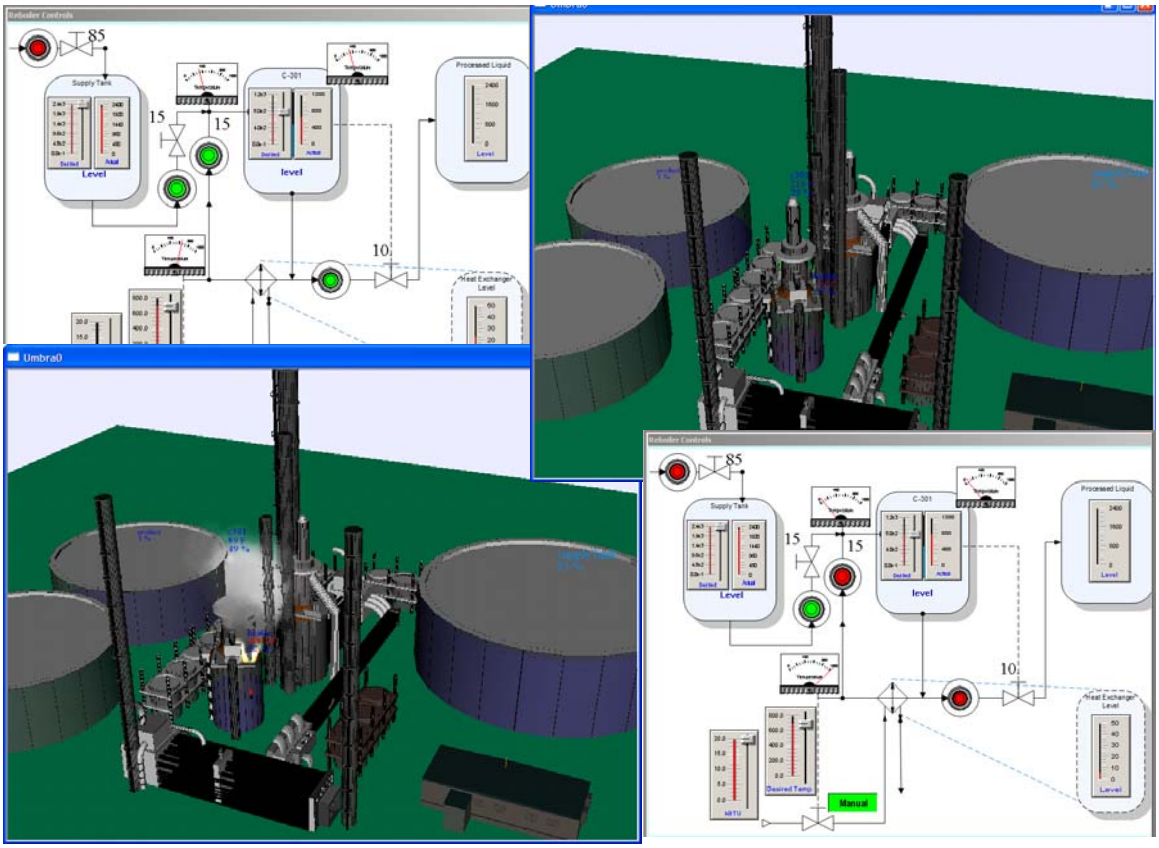

Figure 3: VCSE model of a small refinery before and after a damaging cyber attack

In this application, Sandia embedded simulated RTU models within its physical modeling environments. These simulated RTUs utilize commercial standard SCADA protocols (i.e., Modbus) and can accept real traffic from commercial SCADA systems and control equipment (e.g., other RTUs). In the training scenario, developers used an extended version of Sandia's Graphical Adversary Modeling Environment (GAME) tool to drive Metasploit (http://www.metasploit.com), which in turn launched various malware codes. The particular exploit used inserted malware on the SCADA computer that would redirect malicious control traffic from another computer through the SCADA host to the plant RTUs. In the training environment, operators would thus experience a realistic threat and be able to learn (in detail) about the early cyber and physical signatures of this style of attack.

It is interesting to note that while the OPSAID trainer is in a prototype form, its training attributes benefitted a second audience – cyber security experts. Sandia's Information Systems Analysis Center has a large staff of cyber security experts from a variety of backgrounds. We have begun using VCSE as a hands-on training tool for introducing staff to the unique issues of control system security. As an open-ended model, security experts explore the malware and mitigation technologies provided with the model and also apply other cyber security tools that they are familiar with. Thus, for example, staff use WireShark (www.wireshark.com) to view and

understand control system traffic and, as was done in one case, then apply their own intrusion detection software to understand its applicability to the modeled threats.

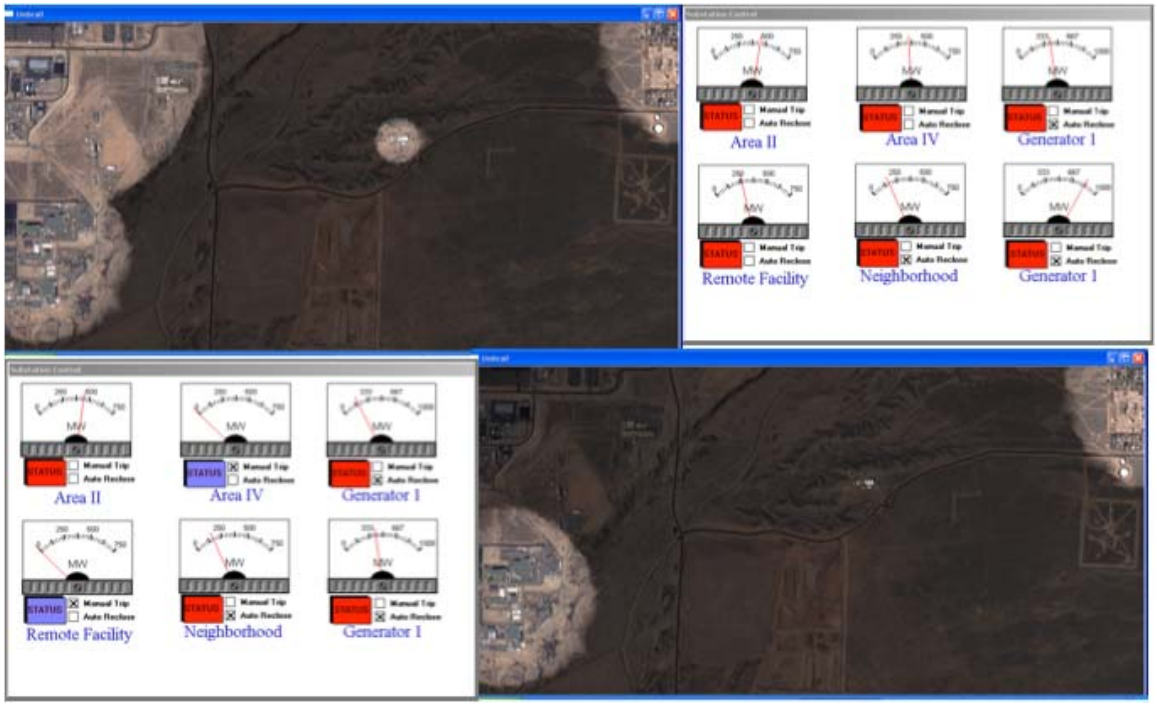

Figure 4: VCSE model of an electric power distribution system before and after a cyber attack

Exploring Electrical Power System Vulnerabilities

Figure 4 shows a similarly configured model designed to explore control system vulnerabilities in an electrical power system. In this experiment, analysts were wished to compare and contrast physical and cyber attacks upon control systems. Analysts used a modified version of the malware described with Figure 3 to simulate cyber attack. Here, adversaries could open breakers at either the generation or load sides of the distribution network to cause general load shedding or targeted effects. To simulate physical attacks, analysts used a commercial game controller (joystick) to drive a virtual vehicle up to switching substations and fire a virtual weapon that would physically disable the control system interface or release the breaker. By providing these two modes of attack, analysts could investigate impacts of physical and cyber defenses against separate or combined attacks.

Developing and Testing Protections and Mitigations

Programmable logic controllers (PLCs) are used in a variety of systems to assert or enforce key safety functions. Typically safety-critical systems are operated out of band from the main control system (e.g., not connected to the control system network). Increasingly, these computer-based safety systems are being integrated directly with control systems in ways that make them vulnerable to cyber attack through the Internet (Spiegel-2009). An open question is whether adversaries might attack these systems to reverse the safety functions of these critical devices and whether such threats can be mitigated through new cyber security technologies.

Figure 5 illustrates a VCSE system that Sandia developed to apply and test its Trust Anchor technology (Chavez-2009) in the protection of critical safety systems. For this study, engineers developed a detailed, though notional, physical model of a natural gas burner, interfaced it to a SoftPLC (using methods described earlier), and programmed the SoftPLC to assert all safety functions. In addition, the engineers integrated the system with a SCADA system. In use, the combined model was accurate enough to respond appropriately to subtle changes in the PLC program. The engineers demonstrated that the physical system could not be damaged through protocol SCADA attacks or through the operator workstation. A Sandia red team then implemented a hard to detect malicious change to the safety program that would reverse the safety function and cause the burner to explode.

To test its powerful threat mitigation capability to threats such as this, Sandia researchers installed the Trust Anchor software onto the SoftPLC. (As a Linux-based open architecture controller, the SoftPLC was readily updated to use the Trust Anchor software.) In its tests, researchers then demonstrated that the Trust Anchor software could detect the subtle program modification and shut down the system when it attempted to execute the malicious code.

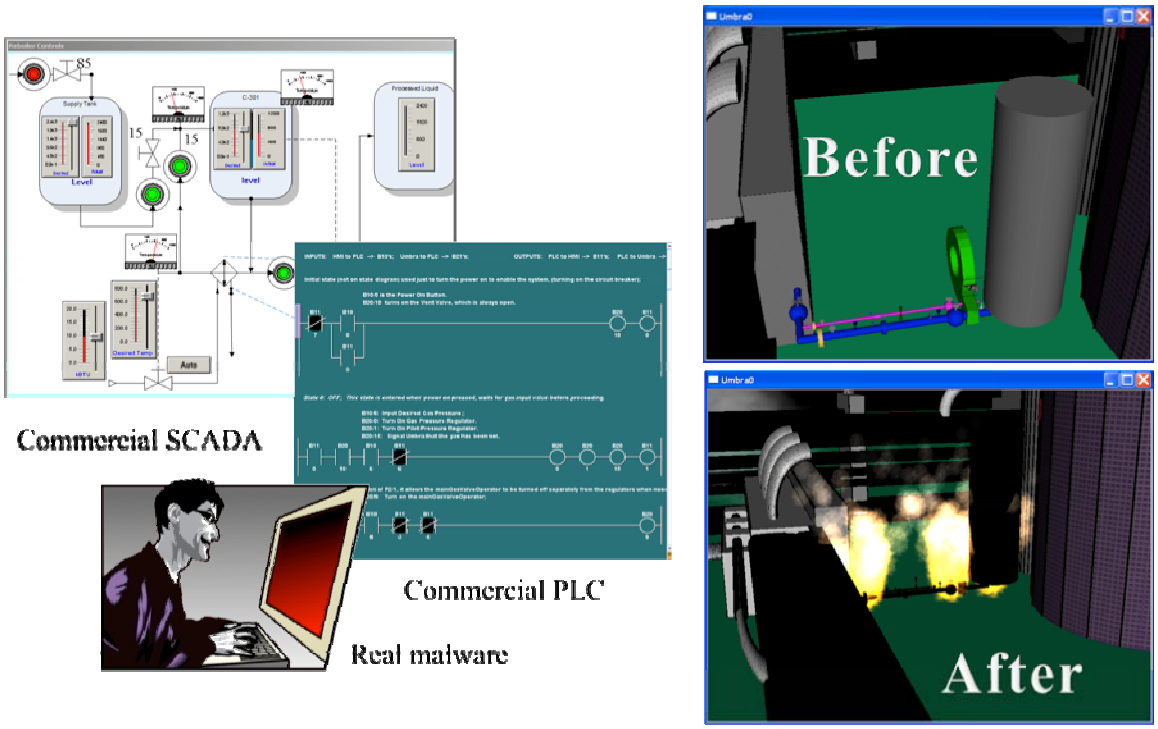

Figure 5: VCSE model of a PLC-controlled burner before and after attack

In a similar project called Detection and Analysis of Threats to the Energy Sector (DATES), researchers at Sandia and SRI International (www.sri.com) are using VCSE to develop and test control system intrusion detection, security event monitoring and large-scale threat analysis technologies. In this effort, Sandia provided SRI with a variety of VCSE models with threats that would be difficult to detect using existing

IT mitigation technologies. Applying their intrusion detection prototypes to the systems, SRI developers first operate the models in their quiescent (non-attacked) state to determine, for example, false alarm rates. Here, using different models operating under different conditions helps ensure that their solutions are general and not tuned to a particular model. Next, they transition through various stages of attack to determine the time to detect various attacks. Were the tool a real cyber-physical system, the analysts would need to significantly restrict the level of cyber attack that they could launch on the system. This is not the case with VCSE systems, where even the effects of attacks that destroy equipment, computer operating systems can be erased in a matter of seconds and the system restarted instantly for further studies. To determine how the security systems respond to zero-day attacks and other anomalies, Sandia modelers can introduce new attacks for these tests.

In the Factotum LDRD project, Sandia researchers are using VCSE to aid in developing a distributed agent systems for control system security. In this system, agent software is installed at a variety of listening points throughout a complex control system network. In one prototype, agents listen to control system traffic to develop an understanding of the physical state of the control systems. In a large system, the agents will be able to compare their models to determine anomalies that may be associated with malicious network activity. In future systems, the agents may form a final line of defense by coordinating, for example, safe isolating and shutdown strategies after human operators have lost control.

Researchers in these mitigation technology development efforts particularly like the features that VCSE provides for implementing a variety of complex cyber-physical systems. For example, by editing XML configuration files, researchers can repartition the networks with varying numbers of virtual routers, extend the underlying physical system to represent control systems of increasing size, and reconfigure the control points to determine how their systems respond to expected day-to-day changes on real-life systems. Because such flexibility is, in contrast, very difficult to achieve with lab or full-scale physical models, our VCSE modeling approach is allowing researchers to build more robust solutions than they could using best of class physical models.

Understanding Possible Impacts of Particular Cyber Threats

Figure 6 diagrams a vulnerability concept that VCSE was used to study. In the summer of 2008, Dan Kaminsky, a Director of Penetration Testing at IO Active (http://www.ioactive.com) discovered a security flaw categorized as a DNS cache poisoning attack (CERT VU#800113). This flaw allows an attacker to advertise false addresses for computers and gain control of systems by making users believe that they are connecting to one computer when, in fact, they are connecting a computer that the attacker controls. Subsequent to this finding, Sandia was asked to investigate whether and how this class of malware created control system vulnerabilities and, subsequently, whether the known mitigations were adequate.

Figure 6 diagrams how DNS poisoning could be used to take control of a SCADA system. Here, an attacker uses DNS poisoning to falsely advertise the addresses of

named RTUs in a control system. Once successful, the SCADA system terminates its connections to the real system and establishes connections to a false or simulated system that the attacker has established. (As an alternative, this system might be software that replays control system values that the adversary has previously recorded.) Once the diversion was created, the attacker would then connect to the real system to control it directly.

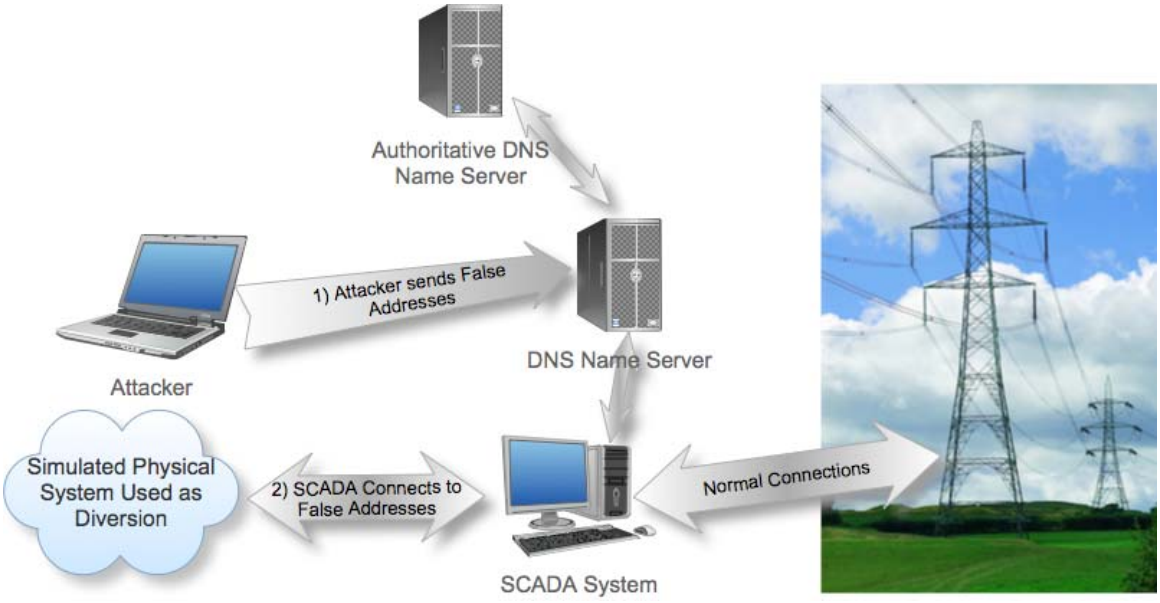

Figure 6: Attack Initiated Through False Address Advertisement

The VCSE model that Sandia developed to study this issue used simulated physical systems to represent both the real and adversary systems. In addition, it used Sandia's aforementioned hybrid network representations to provide an inexpensive computer network that was vulnerable to the Kaminsky codes. They used Metasploit to drive the DNS poisoning attack.

By building a simulated version of this attack, researchers were able to determine conditions under which the vulnerability was important, understand the degree of sophistication needed by an adversary to use the exploits, and validate that the published mitigations were adequate for protecting control systems. Using simulated model gave researchers confidence that they understood the issues. It also provided a teaching environment within which network experts on the team who had little understanding of control systems could quickly learn about the particular issues and contribute effectively.

In another related project, Sandia used VCSE to analyze a "war-dialing" exploit concept. The particular threat team's scenario consisted of an adversary breaking into power substations using wardialing and password guessing to obtain access. In the attack phase, the adversary then dialed in to trip breakers to cause rolling blackouts and, while attacking the breakers, the adversary launching a Denial of Service (DoS) attack on the control center.

To analyze this scenario analysts first modeled the steps of the attack as a formal attack graph using GAME. The analysts then calculated the cost and determined the technical feasibility of each step. Finally, they simulated the immediate consequences of this attack using the VCSE. Here they used VCSE to determine outage sizes for different attack scales.

This analysis highlights the fact that VCSE can be cost-effectively used as a relatively minor aspect of larger analyses. Here, the tasks of analyzing the cyber steps, such as determining whether war dialing could be done at low cost, dominated the analysis. Because the VCSE models were already in existence, analysts were able to use the models to determine effects of attack scales at a very low cost.

Conclusions

Significant and continuing research and a continuing stream of new security products are needed to mitigate cyber threats against our infrastructures. While threats operate at the component level, the tight interplay between the human, physical and cyber aspects of these systems compounds the complexity of defending these systems. Because very serious attackers might well execute complex cyber battles plans and carry out their attacks across many parts of the system, we need to prepare ourselves to survive these cyber attacks at a system level. VCSE provides an ideal platform on which this research can understand, address and train for infrastructure cyber-defense.

While still new, the successful use of VCSE testifies to the validity and practicality of VCSE for modeling and analysis. VCSE approaches provide new ways to conduct threat assessments that identify cyber-control system vulnerabilities, analyze the threat mechanisms and their potential effects, develop and test technologies to mitigate the threats, and train operators and cyber experts to fight the threats before they cause catastrophes.

Within the past year, VCSE has moved from a prototype, TRL level 4-5 tool to a proven, TRL level 6-7 production ready tool.

- Systems analysts are using VCSE to analyze cyber-security risks.
- Technology developers have begun to use VCSEs to better fit their technologies to the problem so that they can address the most pressing problems and develop the most cost-effective solutions possible.
- Cyber defense teams are now using VCSE as a training aid to bring their teams up to speed on the relevant issues and other researchers are using VCSE to train stakeholders on the threats and mitigations.
- Government policy makers have begun funding VCSE-enabled research to better determine which aspects of cyber security protection should be regulated, which should be encouraged, and which are best left to free enterprise to address.

Recommendations

We assert that the key need moving forward is threefold. First, we need to improve our ability to analyze, in depth, control system threat vectors and their potential impacts upon the systems they control. Second, we require a new means of performing deep vulnerability assessments of existing systems without having to perturb the on-line operations of those systems. Third, we need to improve our environments that allow engineers, security experts and operators to exercise their security systems and train for both large and small attacks upon control systems. By addressing these needs in concert, we assert that the combined analyze, exercise and train regime will result in increasingly valid understandings and responses that, in the end, produce dramatically more secure control systems.

Control systems security researchers additionally need to improve the VCSE technology base itself. A variety of technologies, including additional simulators, emulators, physical components, cyber protection devices and penetration testing technologies, are available that future VCSE models might effectively draw from. VCSE system solutions are needed to more rapidly bring together these elements to address realistic systems at more appropriate scales and fidelities. Also needed are better ways to represent the control and threat environments at diverse degrees of detail, the ability to scale the simulation to represent the key systems of interest, the ability to rapidly design and configure experiments, the ability to conduct realistic and meaningful analyses, exercises, and training events, and the ability to capture data from these events for meaningful post-event analysis.

Finally, VCSE needs to be brought out of the lab. With it, private organizations can begin applying VCSEs to better secure their systems and prepare themselves (through training) to survive future cyber attacks that adversaries might one day launch directly against their cyber-controlled infrastructure systems.

References

(Bergman-2009) David C. Bergman, Dong Jin, David M. Nicol, and Tim Yardley, "The Virtual Power System Testbed and Inter-Testbed Integration University of Illinois at Urbana-Champaign," CSET-09: 2nd Workshop on Cyber Security Experimentation and Test, Montreal, Canada, Aug 10, 2009.

(Burton-2009) David P. Burton, Michael J. McDonald, Uzoma A. Onunkwo, Thomas D. Tarman, Vincent E. Urias, Brian P. Van Leeuwen, "Simulated, Emulated, and Physical Investigative Analysis (SEPIA) of Networked Systems," Sandia Report SAND2009-5996, September and 2009

(CERT CSSP) US Computer Emergency Readiness Team (CERT), Control Systems Security Program (CSSP), Overview of Cyber Vulnerabilities, http://www.us-cert.gov/control_systems/csvuls.html.

(CERT VU#800113) Multiple DNS implementations vulnerable to cache poisoning US Computer Emergency Readiness Team (CERT) Vulnerability Note VU#800113 http://www.kb.cert.org/vuls/id/800113

(Chavez-2009) Adrian R Chavez, "Position Paper: Protecting Process Control Systems againstLifecycle Attacks Using Trust Anchors," Future Directions in Cyber-physical Systems Security, Newark, NJ, July 22-24, 2009.

(Davis-2006) C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA Cyber Security Testbed Development," Proceedings of the 38th North American Power Symposium, Carbondale, IL, September 2006, p. 613.

(Gottlieb-2002) Gottlieb, Eric Joseph; McDonald, Michael James; Oppel, Fred John III; Rigdon, James Brian; Xavier, Patrick Gordon, The Umbra simulation framework as applied to building HLA federates, 2002 Winter Simulation Conference, San Diego, CA December, 2002, SAND2002-4269P

(Krebs-2008) Brian Krebs "Cyber Incident Blamed for Nuclear Power Plant Shutdown," washingtonpost.com, June 5, 2008. (http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html)

(Lippmann-2005) Lippmann, R. P., Ingols, K. W., "An Annotated Review of past Papers on Attack Graphs," Lincoln Laboratory Project Report ESC-TR-2005-054, March 31, 2005.

(Lee-2006) Lee, Erik J., Michalski, John T., van Leeuwen, J. M. J., "National SCADA test bed: FY05 progress on virtual control system environment (VCSE)" by Sandia National Laboratories, Albuquerque, NM, July 2006, SAND2006-4083

(McDonald-8-2008) McDonald, Michael J., Onunkwo, Uzoma, Van Leeuwen, Brian P., "BGP Analysis using System-in-the-Loop (SITL) Testbed," OPNETWORK 2008, Washington DC, 08/25/2008.

(McDonald-10-2008) Michael. J. McDonald, Gregory N. Conrad, Travis C. Service, and Regis H. Cassidy, "Cyber effects analysis using VCSE." Tech. Rep. SAND2008-5954, Sandia National Laboratories, September2008.

(McDonald-2009) Michael J. McDonald and Bryan T. Richardson, "Position Paper: Modeling and Simulation for Process Control System Cyber Security Research, Development and Applications", Future Directions in Cyber-physical Systems Security, Newark, NJ, July 22-24, 2009.

(MESERVE-2007) MESERVE, J., Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid., CNN, September 26 2007 (http://www.cnn.com/2007/US/09/26/power.at.risk/index.html)

(Phillips -1997) Phillips, Cynthia, Swiler, Laura Painton, "A Graph-Based System for Network-Vulnerability Analysis," Proceedings of the 1998 workshop on New security paradigms, Charlottesville, Virginia, United States, 1999 (ACM 1-58113-168-2/99/0007)

(PDD-63) William J Clinton, "Critical Infrastructure Protection," Presidential Decision Directive 63, May 22, 1998

(Saydjari-2007) O. Sami Saydjari, (President, Professionals for Cyber Defense, a non-profit organization Chief Executive Officer, Cyber Defense Agency, LLC, Former Director's Fellow, National Security Agency, Former Program Manager of Information Assurance, Defense Advanced Research, Projects Agency Former Senior Executive Service, Defense Department, Founding Member, Cyber Conflict Studies Association, Department Editor, IEEE Security & Privacy Magazine), "Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action," Testimony before the House Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, April 2007 (http://hsc.house.gov/SiteDocuments/20070425145307-82503.pdf)

(Spiegel-2009) Rob Spiegel, "Integrated Safety Systems Winning Out," Automation World, May 2009. (http://www.automationworld.com/feature-5491)

(110th Congress-2008) "Implications Of Cyber Vulnerabilities On The Resilience And Security Of The Electric Grid," Hearing Before the Subcommittee On Emerging Threats, Cyber Security, And Science And Technology, of the Committee On Homeland Security House of Representatives One Hundred Tenth Congress Second Session, May 21, 2008, Serial No 110-117, U. S. Government Printing Office, Washington, DC.

(Van Leeuwen-2009) Brian Van Leeuwen, David Burton, Uzoma Onunkwo, Michael McDonald, Simulated, Emulated, And Physical Investigative Analysis (SEPIA) of Networked Systems, MILCOM 2009, Boston, MA, October 18-21, 2009


Sandia National Laboratories