

Position Paper: Modeling and Simulation for Process Control System Cyber Security Research, Development and Applications

Michael J. McDonald and Bryan T. Richardson
Sandia National Laboratories ^{*†}
Albuquerque, NM
mack,btricha@sandia.gov

Abstract

This paper advocates for increasing the utilization of hybrid modeling and simulation technologies for understanding and developing mitigations for cyber threats upon industrial control systems (ICS). 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 VCSEs. It closes with recommendations to the ICS security community for applying this valuable technology.

1. Introduction

The greatest security challenge that ICS face over traditional Information Technology (IT) systems is that they interface with, and control, physical systems. At a cyber level (here, cyber references all technologies directly associated with computers and networks), this difference results in topological configurations, data characteristics and timing requirements that are unique to ICS. At a system level, this uniqueness is particularly important because cyber attacks on the system could lead to serious consequences ranging from loss of product up to large-scale loss of life.

^{*}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.

[†]Copyright 2009, Sandia Corporation. The submitted manuscript has been authored by a contractor of the U.S. Government under contract No. DE-AC04-94AL85000. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes. Sandia National Laboratories report TBD: UNCLASSIFIED UNLIMITED RELEASE — APPROVED FOR PUBLIC RELEASE.

2. Research Needs

Significant research is needed to provide new and improved component-level security and threat mitigation technologies to ICS. Moreover, new approaches and tools are needed to better understand the specific vulnerabilities of ICS at a system level so that we can successfully defend them against cyber attacks. The tight interplay between the human, physical and cyber aspects of these systems compounds the complexity of defending these systems. Additionally, serious attackers might well execute complex cyber battles plans in carrying out their attacks. The two recently reported national-level cyber attacks experienced by Estonia[1] and Georgia[2] may foreshadow future attacks upon the United States. We need to prepare ourselves to survive these cyber attacks at a system level.

We assert that the key system-level need is threefold. First, we need to improve our ability to analyze, in depth, ICS 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 an environment where engineers, security experts and operators can exercise their security systems and train for both large and small attacks upon ICS. 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 more secure ICS.

One promising area of research to address these needs is in hybrid analytic environments that serve as testbeds for analysis, design and training. Cyber security analyses traditionally utilize real systems (e.g., computers, network equipment), computer emulations (e.g., virtual machines) and simulation models separately to understand the interplay between cyber threats and safeguards. In contrast, new systems are being developed to combine these three into what we term simulated, emulated and physi-

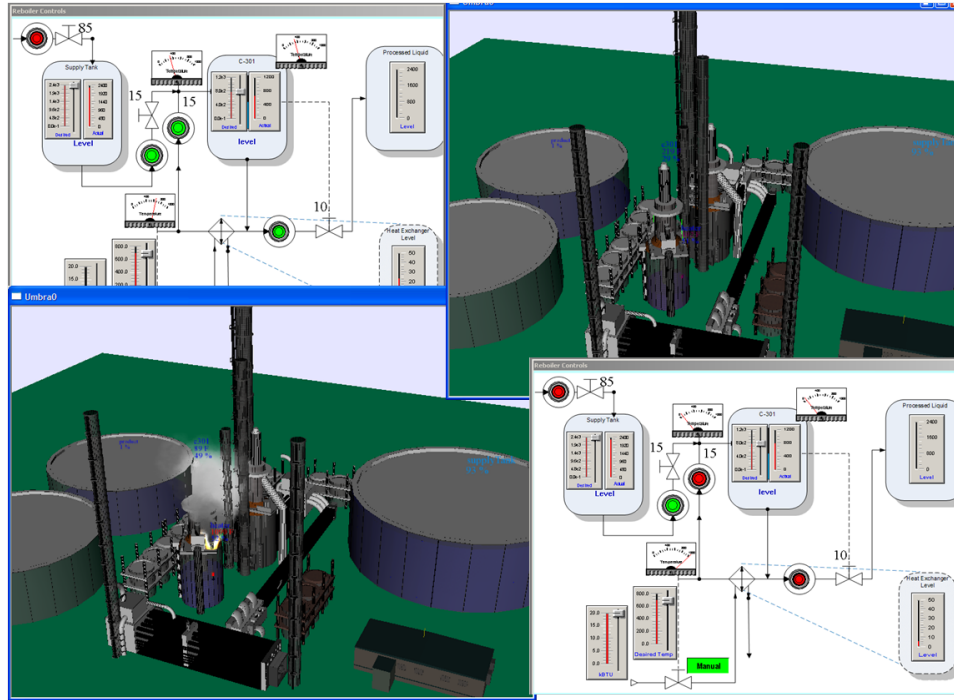


Figure 1. VCSE model of a small refinery before and after a damaging cyber attack.

cal environments for our investigative analysis (SEPIA)[3]. SEPIA environments provide relatively high fidelity representations of key system nodes while still leveraging the scalability and cost advantages of simulation tools for nodes that contribute to the analysis, but whose salient features for that analysis can be expressed at higher levels of abstraction. The need for these SEPIA environments is especially heightened when investigating large-scale ICS infrastructures and other critical systems that cannot be completely replicated in a lab. Sophisticated threats are best understood when the cyber, control and physical issues are addressed together.

Sandia[4] and UIUC[5] have each developed hybrid simulation environments to address ICS security to varying levels of maturity. These Virtual Control System Environments (VCSEs) can already be used as analytic, exercise and training testbeds for cyber control security work. They typically include actual supervisory control and data acquisition (SCADA) elements, including operator control stations, which run on real and virtualized computers. These control stations connect through simulated, emulated and physical (SEP) networks to SEP control equipment that uses real network interfaces to represent the cyber parts of the systems that are subject to attack. Thus, even though simulation and emulation is used as a cost-effective yet scalable way to represent portions of the network, these elements typically support native cyber interfaces (e.g., Modbus, DNP3

and IEC68150 over TCP/IP and serial lines) such that they can interface directly with cyber threat and protection elements. The control equipment connects to plant and infrastructure simulation models that are programmed to respond in the same ways that real systems would respond when under the stresses of attack. For some problems, these simulation models extend beyond the immediate system when doing so adds to the realism that operators would experience and analysts would use in performing their work.

3. Present Day Status of Sandia's VCSE Technologies

Figure 1 shows screen images from a recently developed VCSE physical system simulator that was developed to train cyber defense concepts to oil refinery operators. The top images show its WonderWare-based[6] 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 had been harvested from the Internet.

Sandia's VCSE physical system modeler is based upon Sandia's patented[7] Umbra Framework[8]. Umbra is a robust framework that was developed to model and, for some applications, control sophisticated systems. It has been used previously to develop and analyze a wide variety of automation systems including robotics, factory automation, mili-

tary systems, and security technologies. It is an ideal tool for modeling physical and control systems and for interfacing with actual equipment and SCADA system elements.

Sandia has developed a variety of ways to represent key portions of ICS networks. For some experiments, Sandia uses real Ethernet connections with real switches, firewalls and routers to represent the ICS networks. In other experiments, Sandia uses a combination of emulation and simulation technologies to represent portions of the network. Included here is Network in-a-Box (NIB), a Sandia tool that can instantiate and configure networks of emulated Cisco routers[9] through a Sandia-developed hypervisor. With it, complex emulated networks can be quickly defined in XML and then instantiated with the click of a mouse. In addition, Sandia has developed extensive experience in, and extended the capabilities of, OPNET and its System-in-the-Loop (SITL)[10] simulation capability. For example, Sandia can generate NIB network emulation configurations directly from the OPNET editor, along with additional configurations that integrate OPNET network simulations (via SITL) into the overall system.

Sandia has developed a variety of SEPIA approaches to represent controllers, plant floor interfaces, sensors, intelligent actuators and remote terminal units (RTUs). In the examples in Figure 1, 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 addition, Sandia has utilized and integrated a variety of commercial control equipment into its VCSE environment. In one effort, Sandia is utilizing both real and emulated SoftPLC Programmable Logic Controllers (PLCs) that can control elements within the physical system models, as well as be controlled through the SCADA system. The goal is to run a significant number of emulated PLCs on each host computer in large-scale ICS studies.

Finally, Sandia has tested a variety of cyber threat representations against VCSE environments. These include using Ettercap for Man-in-the-Middle exploits, the Metasploit framework for testing a variety of host exploits, and several ICS-specific tools for investigating concepts on malicious assumption of control.

For example, Figure 2 diagrams some threats upon a typical corporate-situated ICS network that Sandia has studied using a combination of VCSE and red-teaming exercises. As diagrammed, there are a variety of cyber threat injection points (black flags) that adversaries might use to enter these ICS networks. Once injected, these threats might move to other vantage points (red flags) to assume control of ICS functions. In one recent, for example, we showed how an adversary could use an exploit from the Metasploit framework to inject codes onto a Front End Pro-

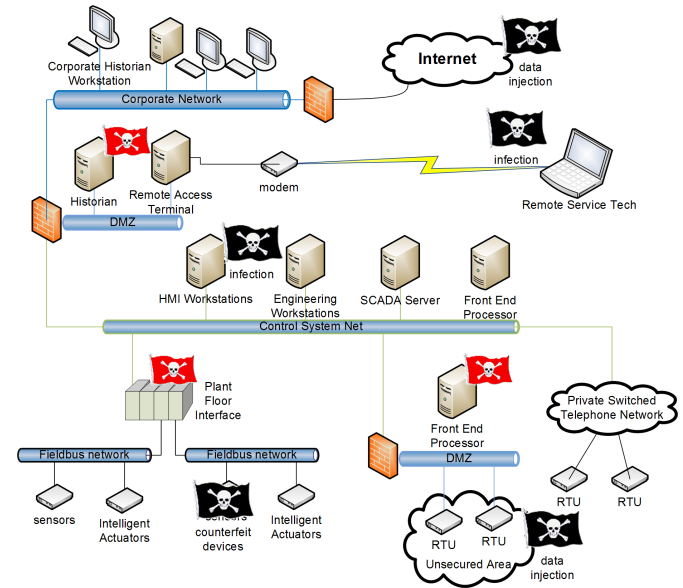


Figure 2. Threats upon a typical “corporate-situated” ICS network.

cessor that was using Microsoft Server 2000 with out-of-date security patches. From this point, we demonstrated how an adversary could connect back to their injection site and completely take over plant functions (overriding operator inputs). In another experiment, we demonstrated how an Ettercap-based MITM could be used to trick these same operators into believing that the plant was functioning normally. Our mitigation analysis is that these threats could be substantially reduced through frequent patching and the strategic use of well-designed Demilitarized Zones (DMZs).

For detailed engineering studies we could, for example, replace our experimentally configured computers and network devices and plant functions with simulated, emulated and real versions of the components from real sites. In this way, red team analysts could study and test vulnerability theories in detail while cyber security engineers could develop and test mitigations to these vulnerabilities. In this way, the most important vulnerabilities could be discovered, understood and mitigated before adversaries had a chance to deploy them.

While still in their prototype form, the published successes at both Sandia and UIUC testify 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 to fight threats that make it past our technical defenses.

4. Recommendations

The ICS security community needs to extend its use of the VCSE approach to design solutions to pressing ICS cyber security problems. This will allow:

- Organizations 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.
- Government policy makers to better determine which aspects of cyber security protection should be regulated and standardized, which should be encouraged, and which are best left to free enterprise to address.
- Technology developers to better fit their technologies and standards to the problem so that they can address the most pressing problems and develop the most cost-effective solutions possible.

ICS 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.

Acknowledgments

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.

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.

References

- [1] Mark Landler and John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, New York Times,

May 29, 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&oref=slogin

- [2] John Markoff, *Before the Gunfire*, Cyberattacks, New York Times, August 12, 2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html>
- [3] Michael J. McDonald, Uzoma Onunkwo, and Brian P. Van Leeuwen, *BGP Analysis using System-in-the-Loop (SITL) Testbed*, OPNETWORK 2008, Washington DC, 08/25/2008.
- [4] Michael J. McDonald, Gregory N. Conrad, Travis C. Service, and Regis H. Cassidy, *Cyber Effects Analysis Using VCSE: Promoting Control System Reliability*, Sandia Report SAND2008-5954, printed September 2008.
- [5] 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.
- [6] Invensys WonderWare, Lake Forest, CA <http://global.wonderware.com/EN/Pages/default.aspx>
- [7] Patrick G. Xavier, Eric J. Gottlieb, Michael J. McDonald, and Fred J. Oppel III, *Apparatus and method for interaction phenomena with world modules in data-flow-based simulation*, United States Patent 7,085,694, filed October 22, 2001, issued August 1, 2006.
- [8] Eric J. Gottlieb, Michael J. McDonald, Fred J. Oppel III, James B. Rigdon, and Patrick G. Xavier, *The Umbra simulation framework as applied to building HLA federates*, 2002 Winter Simulation Conference, December 8-11, 2002 in San Diego, CA (also Sandia Report SAND2002-0975C).
- [9] Using the Dynamips Cisco 7200 Simulator, http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator
- [10] Press Release, *OPNET Announces New System-in-the-Loop Software for Inter-operability Testing, Training, and Wargaming Exercises*, OPNET, Bethesda, MD December 13, 2005