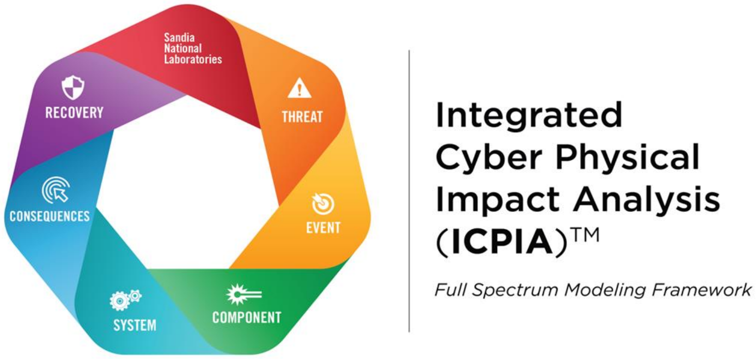
SANDIA REPORT
SAND2016-8046 C
Unlimited Release
Printed August 2016

Integrated Cyber/Physical Impact Analysis to secure US Critical Infrastructure

Lon A. Dawson, Marvin A. Cook



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

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. 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.

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@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/search

SAND2016-8046 C
Unlimited Release
Printed August 2016

Integrated Cyber/Physical Impact Analysis to secure US Critical Infrastructure

Lon A. Dawson, Advanced Nuclear Concepts
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1136

Abstract

Our nation's security and well-being is supported by complex critical infrastructure which is largely privately owned and operated. This infrastructure is reliant on advanced information, communications, and digital control technologies that may be compromised through cyber or physical attack or acts of nature. Our federal agency sponsors and system owners must decide what to invest in to increase the resiliency of our nation’s critical infrastructure to such hazards. Tools, technologies, and metrics that support cyber defense decision making are lacking and the analysis extends beyond a single area of expertise. We need to enable sponsors and owners to identify and evaluate a representative set of scenarios, prioritize events of concern, and make effective operational, investment, policy, and technology decisions. Further, we must be able to identify and evaluate scenarios that emerge from a focus on different domains. For example, an analysis may focus on the possible consequences of a particular threat or the focus could be on identifying attack vectors necessary to achieve a consequence of interest. These efforts must provide information at an appropriate level of fidelity for the decision making context.

Sandia National Laboratories has initiated an internally-funded effort to develop and demonstrate our cross-mission ability to model cyber-initiated events to our national energy infrastructure and manage the resulting impact to the system(s), community, state, and nation. Three attack scenarios targetting stationary energy components (transmission, distribution and nuclear) were used to demonstrate this capability. The scenarios focused on identifying the extended consequences of a cyber-attack from the initiating event to component/system level effects and ultimately the regional or national-level impacts. As specific scenarios were outlined and modeled, the team proposed a framework for Integrated Cyber-Physical Impact Analysis (ICPIA). The framework incorporated a holistic view of the causes, consequences, and potential mitigation strategies crossing five domains: threat, cyberattack, component effects, physical system impacts and extended consequences.

The investment demonstrated that Sandia has the capability to conduct end-to-end analysis of cyber-physical scenarios; however, current tools only analyze a limited set of scenarios at a time and analysts must manually connect the modeling and simulation from different domains. Our

sponsors need an analysis capability that can be used to explore a large number of cyber-physical scenarios that may include many threats, events, system designs and configurations, mitigating strategies and responses, potential investments, policy changes, and sensitivities. This will require a multi-objective constrained optimization capability that spans the domains of the ICPIA framework. Additionally, the results of the analysis will ideally be compatible with an "all hazards" perspective on risk, to enable comprehensive decision making.

This paper has been developed for the Energy Policy Institute's (EPI's) 6th Annual Energy Policy Research Conference scheduled for 8 & 9 September 2016 in Santa Fe, NM. This paper describes the ICPIA framework in further detail, explores a specific example of critical infrastructure cyberattack modeling, and describes future research opportunities.

CONTENTS

FIGURES

TABLES

NOMENCLATURE

EPI	Energy Policy Institute
COTS	commercial-off-the-shelf
DOE	Department of Energy
DMZ	Demilitarized Zone
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICPIA	Integrated Cyber-Physical Impact Analysis
IT	Information Technology
JTAG	Joint Test Action Group
LAN	Local Area Network
MITM	Man-in-the-Middle
PV	Photovoltaic
SSH	Secure Shell
SNL	Sandia National Laboratories
TLS	Transport Layer Security
TPM	Trusted Platform Module
VPN	Virtual Partner Network
WECC	Western Electricity Coordinating Council

1. THREAT TO CRITICAL INFRASTRUCTURE

Our national energy infrastructure is increasingly reliant on advanced information, communications, and digital control technologies. This "system-of-systems" infrastructure represents a complex architecture that is difficult to manage and defend against potential threats. Many domains are well-characterized with accurate computer modeling, but the integrated effects from a local cyber event to the associated system-level impacts that potentially involve other critical infrastructure sectors represents an opportunity for deeper analysis and better management. Multiple Cabinet-level agencies, e.g., DOE, NRC, DHS, and DOD, are trying to understand exactly how the introduction of digital technologies might impact critical infrastructures and national security.

Digital technology proliferation brings increased accessibility through electronic communication networks and migration from vendor proprietary technology and system isolation to generic commercial-off-the-shelf (COTS) components, interlinked business systems, and remote vendor support. As nuclear energy facilities become more dependent upon digital technology (sensors, instrumentation, controls, and communication systems), they have increased exposure to potential cyber attacks. These cyber attacks may manipulate data, extract data, induce unsafe conditions, cause system failures, or cause radiological release.

Examples of relevant attacks and trends include:

- STUXNET was launched against the uranium enrichment facility located at Natanz, Iran and altered industrial control systems to cause physical damage to the plant's operations. Forensic research shows that STUXNET was designed to stay undetected, and to spread confusion and doubt among the nuclear process control engineers[1, 2].
- HEARTBLEED allowed the stealing of information protected by common encryption software used to secure the Internet[3].
- DRAGONFLY/ ENERGETIC BEAR allowed exploiters to intrude into thousands of power plants to extract and upload stolen data, install malware onto systems, run executable files, collect passwords, take screenshots, and catalogue documents[4].
- BLACKENERGY, recently suspected to be linked to wide-scale power outages in the Ukraine[5]. This is a Trojan malware (crimeware) used to gain a foothold on a system and for downloading other malware, such as KillDisk, can render systems unbootable.

[1] To Kill a Centrifuge, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

[2] Symantec Security Response W.32 Stuxnet Dossier Version 1.4, February, 2011 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers

[3] Forbes: "How Heartbleed Happened, The NSA And Proof Heartbleed Can Do Real Damage," April 14, 2014, http://www.forbes.com/sites/jameslyne/2014/04/14/how-heartbleed-happened-the-nsa-and-proof-heartbleed-can-do-real-damage/

[4] Symantec Emerging Threat: Dragonfly / Energetic Bear – APT Group, June 30, 2103, http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group

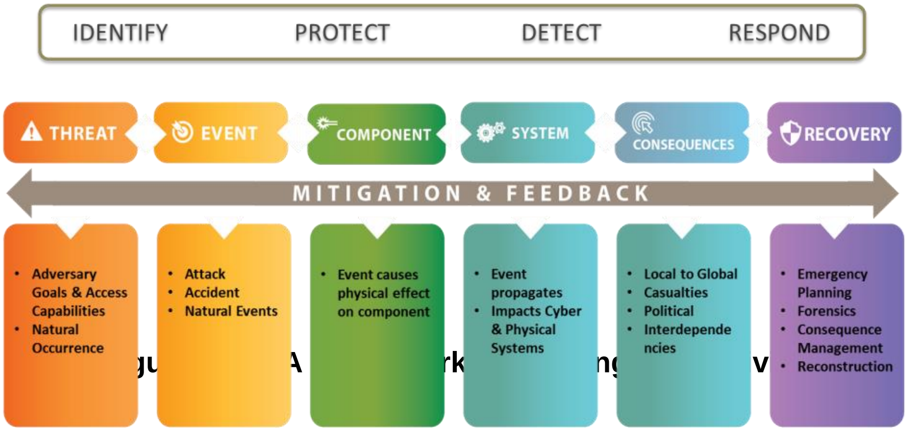
[5] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

- In December 2014, South Korea's Korea Hydro and Nuclear Power (KHNP) publically reported that their information systems had been hacked. KHNP identified that among other things, nuclear power plant design information was stolen.

1.1 Sandia R&D in response to a National Need

Discovering and addressing weaknesses introduced into our energy infrastructure by digital systems is an important mission for Sandia. Sandia has the capabilities needed by our customers to discover cybersecurity weaknesses, avoid them when possible, remove them when practical, and mitigate their impacts when necessary. Consequently, Sandia initiated a mission integration effort that directly leveraged existing cyber simulation tools, cyber emulation and analysis capabilities, and other physical modeling and simulation tools across the lab mission areas to demonstrate the potential impact to the national critical infrastructure of a cyber-initiated event and to accurately model the impact from insertion of the cyber-related anomaly all the way through to the national impact. This analysis capability can be adjusted to evaluate additional concerns by leveraging the extensible and flexible architecture. The work leveraged simulation of cyber-triggering failures in three scenarios – transmission level electric grid, distribution level electric grid, and nuclear power plant. For the nuclear plant, the cyber-attack explored an attack on critical safety systems, specifically the primary plant automatic depressurization system. The analysis extended to beyond-plant consequences of fission product release. The transmission-level electric grid scenario centered on exploiting a known weakness in the Western Electricity Coordinating Council (WECC – effectively the grid covering the western third of the United States in addition to some of Canada and Mexico). For the distribution sector, we examined potential cyberattacks on a photovoltaic manufacturing company's infrastructure for maintenance and upgrades.

From this effort, a 5-stage Integrated Cyber Physical Impact Analysis (ICPIA) framework was developed. ICPIA identified 5 areas where Sandia had unintegrated modeling and simulation capabilities that were necessary to demonstrate threat to impact scenarios.



1.2 ICPIA Overview

Figure 1 shows the different modeling that occurs in each domain. For example, the Event domain includes an attack, accident or natural occurrence that causes an effect on the digital system. This effect then causes a physical impact to the component or system which is modeled in the Component domain. All domains are necessary to appropriately manage cyber risk.

Many capabilities defined in the ICPIA framework are not new and have been used to analyze complex systems from threat to extended consequence for years. However, this effort establishes increased understanding and integration across the key domains. ICPIA provides the foundation to address key objectives, such as:

- **Support New Threat Analysis** - Explore the impact of previously unidentified threats and vulnerabilities
- **Provide test bed for integrating systems** - Install and test Intrusion Detection System (IDS) through network emulation
- **Help design secure architectures** - Evaluating protective measures with detection, deterence, and response
- **Act as a training tool** - Develop and exercise cyber attack and response procedures for Red Teamers and Plant Operators
- **Identify R&D gaps** - Reduce system risks based on analysis
- **Supports integrated risk management** - Achieve an “all hazards” analysis with attack difficulty and impact analysis

2. SCENARIO EXAMPLE – DISTRIBUTED ENERGY

2.1 Overview

The emerging market for large-scale renewable generation will significantly transform today's power grid. Centralized generation and fuel storage will be replaced by large quantities of distributed generation and storage devices. Introduction of these new technologies requires in depth security analysis to ensure protection of information and performance. Sandia partnered with a photovoltaic (PV) manufacturing company to help identify and eliminate potential security concerns with their infrastructure for system maintenance and upgrades. This company is an industry leader in remote controllability of deployed assets and uses this capability to update inverter firmware. The capability raises a concern - *Can the same remote control architecture be used to introduce a malicious upgrade and negatively impact grid stability and consumer confidence*?

Figure 1 is a depiction of the PV components in a typical residential application. The system relies on the home network's internet connectivity to communicate with corporate applications via a web service.

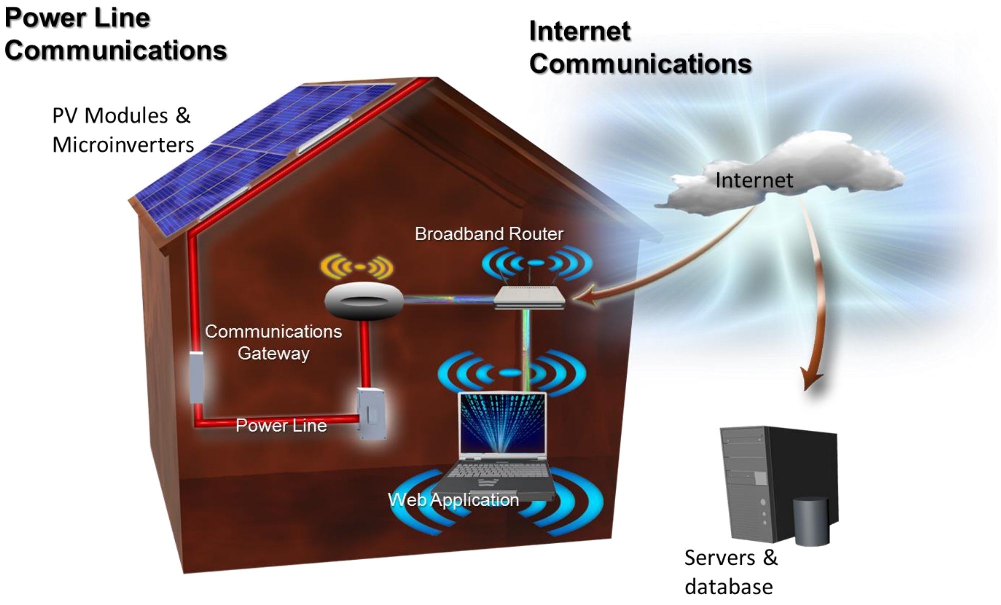


Figure 2 Typical Residential PV System

2.2 Threat Model

A threat model includes an adversary definition, their goals (or system owner consequences of concern) and access. In an adversary-based vulnerability assessment, the threat model sets the boundaries for the attack development. For this effort, the following adversary access locations, critical intermediate nodes and consequences of concern were proposed by the Sandia team:

1. Open Internet
2. Logical access to home network

3. Physical access to router and/or inverter
4. Installer access (credential and application)
5. Enterprise Network without credential
6. Corporate development network with credential
7. Customer Support Web Interface with credential
8. Web service insider
9. Utility
10. Corporate maintenance server with Administrator privileges

Consequences of Concern:

1. Degrade system Confidentiality (loss of data), Integrity (corruption of data) or Availability (further specified to permanent disablement, temporary disablement and remote control), any one of which will result in
2. Reduced consumer confidence and possible slowing of renewable technologies adoption thus
    a. Reduces corporate profitability and market share
    b. Reduces ability to meet the national interest of securing a sustainable energy future

2.3 Cyber Attack/Event

The first step in the assessment was to gather as much data as possible about the system from company and open sources. This information was used to develop attacks and identify additional system information needed to verify critical attack paths. The analysis combined knowledge gained from in depth router device investigation, device communication tests with crafted data packets, and information provided by the parterning company. This effort linked access points to consequences of concern, which led to the following scenarios of interest:

1. Manipulate broadband router performance data reporting (misreporting/stop) to the web service in an attempt to reduce ability for installers to properly bill customers.
2. Manipulate router performance data reporting (misreporting/stop) to reduce manufacturer or installer ability to advertise renewable product. Pollute the publicly accessible web browser view of deployed router through data misreporting, which results in high levels of frustration for stakeholders.
3. Attempt to compromise or virtualize legacy router (older firmware) to malign broader system. Assume older firmware has less security considerations and maintenance but still has strong ties to broader/mixed infrastructure. Manipulate performance data or attempt pivoting/reaching into higher levels of the system (VPN tunnel).
4. Gain access to a commercial or home Local Area Network (LAN) and modify the router to microinverter configuration (drop devices), then add to another router within reach (or falsely register/tie in).

5. Perform a denial of service to the maintenance manager (web-based application) so that installers/do it yourselfers cannot register router. Write a curl based script to either flood the web service or exhaustively assign all possible serial numbers.
6. Determine a way to impersonate corporate support or engineering tech roles to issue malicious actions to router.
7. Initiate a request for retirement of a large set of valid/functional router.
8. Crack the encryption of web service responses to router performance data packets to introduce malicious tasks.
9. Gain access to router in which installer did not change the default password and update to select password for ownership until reset.
10. Obtain installer email addresses and craft periodic emails to report issues with router/ micro-inverter installation and performance.
11. Scan for router existing in a home network. If a router is detected, then attempt to strip the traffic possibly gaining authentication credentials.

These scenarios were further analyzed for attack details, feasibility, and to generate clarifying questions for the company representatives. Four attack categories emerged: 1) Attacks on corporate infrastructure, 2) Attacks on cloud infrastructure, 3) Insider attacks and 4) Attacks originating from a router endpoint. Although each category represents areas of interest, this analysis focused on attacks at the router endpoint.

2.3.1 Attack on the Router Endpoint Description

The inverter and many other embedded devices from a cybersecurity point of view represent a large liability due to wide distribution and ease of accessibility. By placing devices in users' homes, the manufacturer loses a lot of control over the security of those devices. Computers are often considered more vulnerable and even compromised if an attacker can gain physical access. With embedded devices permeating people's homes, an increasing number of devices grant physical access to the general public by design. As those devices are connected to networks to create the 'Internet of Things,' manufacturers face significant security design challenges.

For these devices, the challenge facing manufacturers is how to secure devices in spite of the user. The result is often a security approach that relies on compartmentalization rather than access prevention. This approach means that, even if a person had a device in their home that they could attack, a successful attack would not necessarily allow them to attack other devices. The energy sector must address these security concerns since advanced inverter functions require inverters be linked together for high-level control from the utility or manufacturer.

2.4 Cyber Attack Demonstration

This effort focused on the router as the access point due the significant cyber issues being presented by wide distribution of assets with Internet connection. This effort developed a high-level of system understanding of the device update and support processes, which led to key elements for further investigation:

- The router has credentials to access the VPN; if we log in with those credentials from a computer, it may also allow us to access other routers when they access the VPN for updates or support
- The router has Secure Shell (SSH) enabled, which may allow us access from a local network
- If the corporate server was compromised, an update package with a colliding cryptographic hash could be uploaded and used to compromise a large number of routers
- Access to privileged web service application accounts could allow assignment of malicious tasks, like assigning Trusted Platform Module (TPM) profiles inappropriate to the region in which the router is located or assigning an update from a non-manufacturer location

Error! Reference source not found. presents the subset of attacks specific to an adversary with a router device. Validated paths are shown in red.

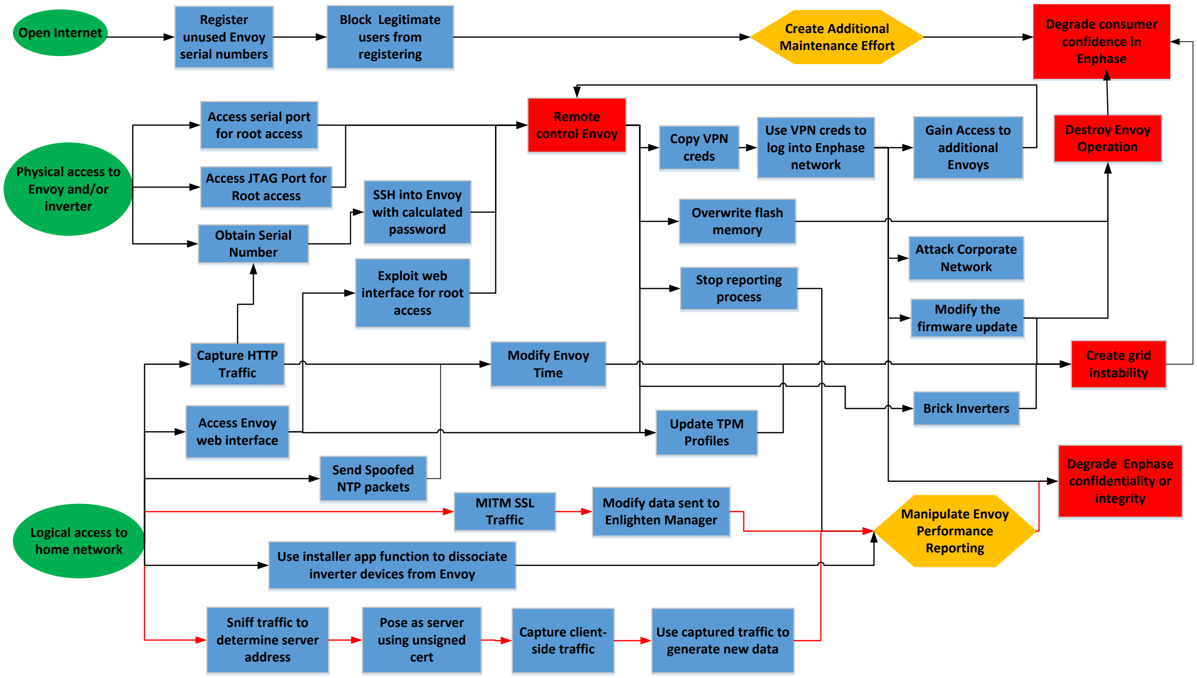

Open Internet
Register unused Envoy serial numbers
Block Legitimate users from registering
Create Additional Maintenance Effort
Degrade consumer confidence in Enphase
Remote control Envoy
Access serial port for root access
Physical access to Envoy and/or inverter
Access JTAG Port for Root access
SSH into Envoy with calculated password
Obtain Serial Number
Exploit web interface for root access
Copy VPN creds
Use VPN creds to log into Enphase network
Gain Access to additional Envoys
Destroy Envoy Operation
Overwrite flash memory
Attack Corporate Network
Stop reporting process
Modify the firmware update
Capture HTTP Traffic
Modify Envoy Time
Create grid instability
Access Envoy web interface
Update TPM Profiles
Brick Inverters
Send Spoofed NTP packets
Degrade Enphase confidentiality or integrity
MITM SSL Traffic
Modify data sent to Enlighten Manager
Manipulate Envoy Performance Reporting
Logical access to home network
Use installer app function to dissociate inverter devices from Envoy
Sniff traffic to determine server address
Pose as server using unsigned cert
Capture client-side traffic
Use captured traffic to generate new data

Figure 3 Attack Graph

2.4.1 Characterization and Analysis

This effort performed system characterization and analysis through traffic interception - observing router traffic using Wireshark[6] and ultimately demonstrating a Man-In-the-Middle (MITM) attack targeting communication between the device and servers. Figure 4 shows a normal HTTPS connection routine.

[6] https://www.wireshark.org

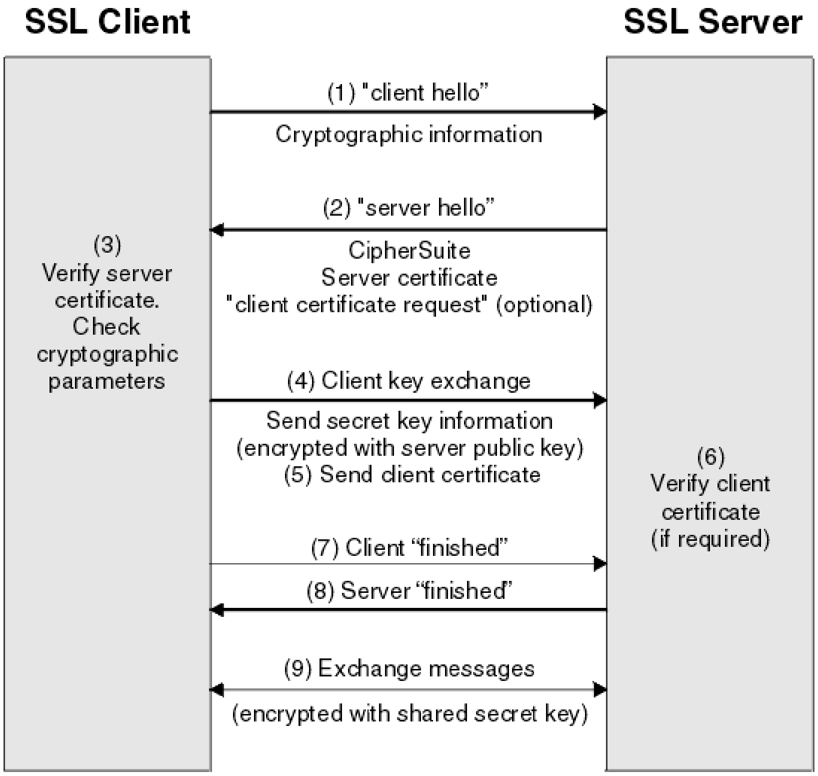

SSL Client
SSL Server
(1) "client hello"
Cryptographic information
(2) "server hello"
CipherSuite
Server certificate
"client certificate request" (optional)
(3) Verify server certificate. Check cryptographic parameters
(4) Client key exchange
Send secret key information (encrypted with server public key)
(5) Send client certificate
(6) Verify client certificate (if required)
(7) Client "finished"
(8) Server "finished"
(9) Exchange messages
(encrypted with shared secret key)

Figure 4 HTTPS Traffic Analysis

In step 3 of Figure 4, a vulnerability was discovered – the lack of a check for the certificate provided by the server to verify the server's identity. To check whether the router was correctly validating certificates, a fake web server was developed to act as the web service application server. The router neither checked that the server name matched the certificate nor if that certificate is valid and trusted: it made a connection with the fake server and sent its reports assuming that it was the web service application. This flaw to intercept traffic between the router gateway and web service application was leveraged to achieve the threat consequences of interest.

2.4.2 Data Analysis

All device communications were monitored by using a Kali Linux machine configured to intercept traffic between the web service application server and the router gateway. With successful interception of decrypted communications, the traffic being sent to and from the web service application server was fully analyzed.. The web service application received configuration and performance reports from a router gateway.

Simple decompression allowed inspection of the data sent by the router Gateway, as well as the structure of the reports sent to the web service application server. Understanding the structure and content of the router gateway reports allowed imitation of actual router traffic in a router spoofing attack. In addition to reports sent by the router gateway, the web service application server sent tasking to the router through the response to router reports. This analysis allowed recreation of configuration update tasks that modified the behavior of the device.

2.4.3 Impact Analysis

The company expressed interested in understanding the physical and economic impacts of a successful cyberattack. To understand the physical impact, this effort collected previous studies surrounding electric grid stability effects with *renewable penetration*. This information fed an additional economic analysis resulting impacts on investor confidence in renewables. The economic analysis concluded wide-scale disruption of inverters leading to system outages will cause some economic losses and reduced investor confidence. However, the overall losses are appear to be mitigated by diversity investment strategies. The existence of multiple types of systems and vendors means that a single disruption will not devistate the entire industry.

2.4.4 Attack Summary

In summary, this analysis identified a flaw in the router's secure communication implementation that allowed for traffic interception and subsequent spoofing. Table 1 summarizes the identified vulnerabilities, effects, and potential mitigations. The vulnerability allowed successful contamination of the web database with incorrect performance data to achieve the consequence of concern.

Table 1. Summary of Vulnerabilities and Potential Mitigations

Vulnerability	Effect	Mitigation
Router doesn't check server name or certificate validity	Traffic sent between router and web service application can be intercepted Server replies can be spoofed to issue commands to router	Require router to check server certificates
JTAG (Joint Test Action Group) port and serial allow access to the device	Firmware can be dumped, may be able to remove credentials from the device, may be able to access and reverse engineer SSH password algorithm	Remove JTAG and serial ports on production boards
Web service application server has no way to validate client	Traffic from the router (client) can be spoofed	Transport Layer Security (TLS) allows for certificate-based client authentication, so devices could be issued a certificate at the factory. The current setup could be used as long as the client and server authenticated certificates.

Web service application server is backward compatible	Upgrading security measures (like checking certificates) doesn’t matter if users can still connect with old devices (and spoofed old devices)	Limit or remove backward compatibility
MD5 encryption is used to hash updates	With access to the server (or if the router were directed to a new URL for updates), an adversary could upload a new firmware image with the same MD5 and malicious content	Use SHA-256, SHA-512, or SHA-3 encryption

.

3. RECENT ACTIVITIES

Sandia continues to invest in this mission integration effort in FY16. Because this effort is so far reaching, we continue to socialize it broadly. This included a formal internal review to evaluate plans and recommend further actions, a presentation to our External Advisory Board, an open-house. In support of broad communication the team has a formal lead center, SNL management champion, a formal graphic (which appears on the title page of this document), an internal webpage and summary presentations of all the subtasks.

We continue to expand the scope to both incorporate additional modeling and simulation capabilities and engage new technologies. FY16 has subtasks for connected vehicles and fuel transport (e.g. Natural Gas pipelines). For a proposed technology area, typical activities include conducting background literature search on previous cybersecurity work in the area, developing a representative system including a potential attack surface and cataloguing relevant modeling and simulation capabilities.

4. FUTURE NEEDS / PLANS

The mission integration project demonstrated that Sandia has the capability to conduct end-to-end analysis of cyber-physical scenarios; however, current tools only analyze a limited set of scenarios at a time and analysts must manually connect the modeling and simulation from different domains. Our sponsors need an analysis capability that can be used to explore a large number of cyber-physical scenarios that may include many threats, events, system designs and configurations, mitigating strategies and responses, potential investments, policy changes, and sensitivities. This will require a multi-objective constrained optimization capability that spans the domains of the ICPIA framework. Additionally, the results of the analysis will ideally be compatible with an "all hazards" perspective on risk, to enable comprehensive decision making.

Recognizing these needs, the team has proposed additional research to improve the ICPIA capability. Specific improvements would address big challenges to securing complex systems:

1) Automating for efficiency (not acceptable to provide point by point analysis)

2) Dealing with change - securing infrastructure is a wicked problem because of new technologies, reliance models, architectures, threats, etc. So when change occurs the model should adapt and propagate the change…

3) Facilitating all-hazard analysis, by using a systems-engineering approach and compile:

   i. Representative inputs such as physical and cyberattack and natural-cause incidents,

   ii. Capabilities (within and outside of Sandia) for modeling and simulation using the 5 ICPIA domains,

4) A complete set of risk management information to effectively manage critical infrastructure – consequences, risks, ROI for potential investments such as security, resiliency, etc.

DISTRIBUTION

1	Energy Policy Institute’s (EPI's) 6th Annual Energy Policy Research Conference scheduled for 8 & 9 September 2016 in Santa Fe, NM		
1	MS1379	Lon Dawson	6221
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories