

SANDIA REPORT

SAND2017-1785

Unlimited Release

Printed 27 January 2017

Cyber Security Gap Analysis for Critical Energy Systems (CSGACES)

U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability

Program Manager: Dan Ton (U.S. Department of Energy)

Project Lead: Jason E. Stamp, Ph.D. (Sandia National Laboratories)

Authors:

Jason E. Stamp, Ph.D.¹

Jimmy E. Quiroz¹

Abraham Ellis¹

B. Bhagyavati²

Joseph A. Cooley²

Kristin Dahl²

Erik R. Limpaecher²

¹ Sandia National Laboratories

² Massachusetts Institute of Technology Lincoln Laboratory

Prepared by

Sandia National Laboratories

Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Approved for public release; further dissemination unlimited.



Sandia National Laboratories

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

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

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

Available to DOE and DOE contractors from:

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

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: <http://www.osti.gov/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.fedworld.gov
Online ordering: <http://www.ntis.gov/search>



Cyber Security Gap Analysis for Critical Energy Systems (CSGACES)

U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability

Program Manager: Dan Ton (U.S. Department of Energy)

Project Lead: Jason E. Stamp, Ph.D. (Sandia National Laboratories)

Authors:

Jason E. Stamp, Ph.D. ¹

Jimmy Quiroz ¹

Jimmy Quiroz ¹

B. Bhagyavati ²

Joseph A. Cooley ²

Kristin Dahl ²

Erik R. Limpaecher ²

¹ Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1188

² Massachusetts Institute of Technology Lincoln Laboratory
244 Wood Street
Lexington, MA 02421-6426

Abstract

This study describes a cyber security research & development (R&D) gap analysis and research plan to address cyber security for industrial control system (ICS) supporting critical energy systems (CES). The Sandia National Laboratories (SNL) team addressed a long-term perspective for the R&D planning and gap analysis. Investment will posture CES for sustained and resilient energy operations well into the future.

Acknowledgements

The authors would like to acknowledge the funding and technical support from the Department of Energy Office of Electricity Delivery & Energy Reliability for the development of this report. The authors are very appreciative of the key contributions by other SNL personnel in supporting the analysis, particularly from Jennifer Depoy, Abraham Ellis, Derek Hart, Jordan Henry, John Mulder, and Jennifer Trasti.

The authors would also like to thank the following government and non-government organizations for their invaluable input to this study:

Government

Massachusetts Institute of Technology Lincoln Laboratory
Construction Engineering Research Laboratory (CERL)
Idaho National Laboratory
Marine Corps Air Ground Combat Center, Twentynine Palms, California
National Renewable Energy Laboratory
National Institute of Standards and Technology
Pacific Northwest National Laboratory
U.S. Army Corps of Engineers
U.S. Army Cyber Command
U.S. Navy Installations Command

Non-Government

Customized Energy Solutions
Electric Power Research Institute
Enchanted Rock
ICETEC
Integrated Energy Solutions
NEC Energy Solutions
OpenADR Alliance
PJM
POWER Engineers
Schweitzer Engineering Laboratory
Southwest Research Institute
Typhoon HIL, Inc.

Executive Summary

This study describes a long-term cyber security R&D plan to address ICS cyber security for CES. Long-term goals for ICS were assumed to be those that would require significant action and R&D to achieve, as opposed to being addressable by applying existing technology and best practices. Long-term R&D would roughly fall into the window of 5-10 years out. Investing in the identified R&D will posture CES for sustained resilient energy operations well into the future.

The gaps were identified using a conventional gap analysis process. The current state of cyber security R&D was surveyed and summarized. Then, the desired future state of ICS cyber security was characterized, in terms of required capabilities for a secure and resilient ICS. Afterward, gaps were identified by comparing the current state of cyber security to the desired end-state. Finally, the gaps were prioritized and paired (where important) with the appropriate communities (industry, vendors, academia, etc.) suitable to address them.

The baseline survey of the existing R&D focused on efforts in government, academia, federally funded research and development centers (FFRDCs), and industry (including vendors). One primary source was existing DOE, Department of Homeland Security (DHS), and Department of Defense (DoD) programs, including Cybersecurity for Energy Delivery Systems (CEDS) and Defense Advanced Research Projects Agency (DARPA). Crucial documents from the National Institute of Standards and Technology (NIST) were also surveyed. On the academic side, the group included work from the Institute for Information Security & Privacy (IISP) and Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) research consortiums. Numerous other smaller efforts were cataloged as well. Overall, the results show significant attention on the cyber security issues faced by ICS, but with a definite tendency toward near-term solutions, and less defined long-term goals, particularly in terms of needed R&D.

The surveyed concepts and goals were used to develop the desired state for long-term ICS cyber security. These were complemented by concepts and frameworks previously used for ICS cyber security. The overall result was the development of a matrix of needed technical capabilities for secure and resilient ICS in the long term. Eighteen cyber security concepts (referred to as “topics” for gap analysis) were identified and sorted according to their positions in the security lifecycle (secure design, reinforced implementation, operation and deployment, or cross-cutting capabilities) and security category (protect, detect, react, or recover). For each topic, a description was provided, as well as other discussion, including a comparison to existing work.

The comparisons formed the basis for the gap analysis. Some security topics, although an essential part of a desired secure ICS state in the future, have significant R&D resources already working to realize the goal. Others, however, are only partially addressed. Besides the severity of the R&D gap, an important consideration is that *perfect security is unattainable; therefore, strong security engineering must be complemented with additional security monitoring.*

The final rankings for long-term R&D, including specific opportunities and challenges, along with suggestions about which group or groups should be targeted for funding opportunities, are in Chapter 4 of the report. Some of the key results include:

1. Trusted monitors, which act as out-of-band security sentinels, and security analytics, which fuse weak indicators to detect security anomalies, have very high priority for R&D. As mentioned previously, no system can be completely trusted (or, given the potential ramifications, even *reasonably* trusted); therefore, monitoring is essential.
2. Virtualization is a key capability for many aspects of ICS cyber security; potential applications include training environments, pre-deployment change testing, red/blue engagement, evaluating tactics-techniques-procedures (TTPs), and others. Virtualization capability would be greatly enhanced with better support for ICS field devices (like relays, programmable logic controllers, etc.) and automated model generation from design or operational system information.
3. Field devices have unique cyber security issues, and are critical to cyber risk given their application: straddling the cyber/physical domains. Addressing these issues in an organized fashion (including their virtualization) is a priority R&D gap. This is also an example where industry (particularly vendors) must complement other R&D organizations.

Contents

Executive Summary	5
1 Introduction	11
1.1 Energy ICS Design Challenges	12
1.2 Long-term R&D Gap Analysis	16
1.3 Report Roadmap	16
2 ICS Cyber Security Research and Existing Capabilities	17
2.1 NIST Guide to Industrial Control Systems Security	20
2.2 Cyber Security for Energy Delivery Systems (CEDS)	23
2.3 Academia	24
2.4 DoD and Others	26
3 Future Vision: Long-Term	27
3.1 Planned Approach	28
3.2 ICS Cyber Framework	28
3.3 Categorizing Cyber Security	32
3.4 Summarized Long-Term State for ICS Cyber Security	34
3.5 Long-Term ICS Cyber Topics	37
3.6 Long-term R&D Summary	56
4 Conclusions	57
References	61

Appendices

A	Revision History	67
B	Contact Information	69

List of Figures

1.1	Five-level ICS architecture	13
1.2	SDLC, cyber security, and effectiveness	15
1.3	Gap analysis process for long-term ICS cyber R&D	16
2.1	Reference architecture test network (flat configuration)	18
2.2	Reference architecture test network (enclaved configuration)	19

List of Tables

3.1	Concise long-term ICS cyber security R&D topics	34
3.2	Categorized long-term ICS cyber security R&D topics	36
3.3	Topic description, categorization, and analysis: Moving Target Defense	38
3.4	Topic description, categorization, and analysis: Protected Computing	39
3.5	Topic description, categorization, and analysis: Resilient Systems	40
3.6	Topic description, categorization, and analysis: Obfuscation	41
3.7	Topic description, categorization, and analysis: Defense-in-depth	42
3.8	Topic description, categorization, and analysis: Boundaries/Authentication	43
3.9	Topic description, categorization, and analysis: Security Analytics	44
3.10	Topic description, categorization, and analysis: Trusted Monitors	45
3.11	Topic description, categorization, and analysis: Minimize System Impact	46
3.12	Topic description, categorization, and analysis: Trusted Gold Masters	47
3.13	Topic description, categorization, and analysis: System Adaptation	48
3.14	Topic description, categorization, and analysis: System Assessment/Audit	49
3.15	Topic description, categorization, and analysis: Temporary Capability	50
3.16	Topic description, categorization, and analysis: Secure Recovery	51
3.17	Topic description, categorization, and analysis: Field Device Security	52
3.18	Topic description, categorization, and analysis: Virtualization	53
3.19	Topic description, categorization, and analysis: Threat Analysis	54
3.20	Topic description, categorization, and analysis: Policy/Personnel	55
4.1	Long-term ICS cyber security R&D gaps	58
4.2	Priority long-term ICS R&D gaps related to DOE	59

Chapter 1

Introduction

The purpose of this report is to communicate the findings of a gap analysis performed by SNL. This study is intended to serve as a gap analysis for efforts in the area of ICS cyber security for CES. The focus of the study was electrical power systems, but many of the technical aspects are applicable to other ICS-supported systems, such as fuels, manufacturing, and water treatment. The final results and recommendations are ranked to prioritize investment; further, there is additional discussion as to the best R&D community for addressing the gaps (including academia, national laboratories, industry, or combinations).

The long-term analysis was led by SNL based on past experience of R&D for ICS cyber security. The project team reached out to and interviewed numerous stakeholders from both government and non-government sectors (as listed in the “Acknowledgments” section). Their input and suggestions were invaluable in the development of the results in this report.

The long-term R&D gaps were developed in the context of a set of required technical capabilities for a secure and resilient ICS. The gaps span the security lifecycle and also the common security categories: protect, detect, react, and respond. While a vision of what CES will look like many years from now is not explicitly described, the challenges associated with the identified gaps are anticipated to be applicable to future energy systems. Long-term goals were assumed to be those that would require significant action and R&D to achieve, as opposed to being attainable with existing technology and best practices, and would roughly fall into the window of 5-10 years out. Investing in these will posture CES for sustained resilient energy operations well into the future.

While this report focuses on the long-term R&D gaps, we acknowledge that cyber security of CES could benefit from actions that do not require fundamentally new technology or R&D investment. The following recommendations were identified:

- **Make existing cyber security guidelines easier to apply:** Cyber security guidelines such as North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) [26] or NIST Risk Management Framework (RMF) are descriptive in nature and require deep expertise in order to apply them in practice. Guidance typically spans the lifecycle of the ICS systems, from architecture and design through operations and maintenance. It also frequently spans the dimensions of personnel, policy, processes, and technology. There is no single answer when designing, building, operating, and maintaining a safe and secure ICS. Going forward, it would be very helpful to develop prescriptive guidance built upon software

samples, system configurations, and best-practices that reduce descriptive guidance closer to practice. Such an approach would take the engineering time and cost, guesswork, and error out of interpreting and properly implementing and maintaining guidance.

- **Improve cyber security hygiene:** Poor inventory control, outdated system patch levels of software and firmware (i.e., poor configuration management), and undocumented operational network connectivity are all common occurrences within ICS environments. This lack of basic hygiene leaves control systems particularly vulnerable to compromise because they also frequently lack strong digital identities, authentication, authorization, and other basic security functionality common to secured systems. ICS frequently lack access controls such that any device on the network has full read-write access to all other devices on the same ICS network, particularly at the field device level and below. Business case studies should be undertaken to discover the fundamental contributors to the lack of basic hygiene. Problems likely span the system development lifecycle and include personnel training; incomplete and/or inadequate processes; complex, poorly understood, and descriptive rather than prescriptive policies; and poorly defined investment models for operations, administration, and maintenance of safe and cyber-secure ICS systems.
- **Clarify cyber-related authority and responsibility:** The U.S. government needs to define cyber security authority and responsibility for major critical infrastructure. Between government organizations at various levels and varieties, and the private sector, it must be well-defined who responds to cyber events that have a large-scale impact on the nation and its security. Beyond that, working relationships need to be formed between appropriate entities, detailed dependencies defined, and routine table-top and real-world exercises carried out in order to maintain a proper readiness level.

To implement these recommendations in a specific class of applications, it is generally useful to define a common architecture that accommodates the range of applicable use cases. The NIST RMF and derivatives such as the Purdue Enterprise Reference Architecture (PERA) are good candidates for this purpose. These recommendations are increasingly relevant considering that more CES operate in regimes that require more automation and cyber-interaction, such as participation in energy and ancillary services markets.

1.1 Energy ICS Design Challenges

DHS has identified sixteen critical infrastructure sectors comprised of “assets, systems, and networks, whether physical or virtual, [that] are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof” [1]. Examples include transportation, critical manufacturing, and energy. A majority of these sectors are controlled and monitored with ICS, which are physical systems controlled by cyber processes, or “cyber-physical” systems. *Cyber events in these systems can have physical consequences.*

ICS are comprised of embedded controllers, sensors, actuators, and related technologies commonly referred to as operational technology (OT). Compared to the traditional information technology (IT) systems found in enterprise networking environments, OT may be specialized in order to implement physical processes with strict measurement, movement, and time-sensitive requirements. A widely-used conceptual architecture for OT systems is the five-level PERA as depicted in Figure 1.1.¹

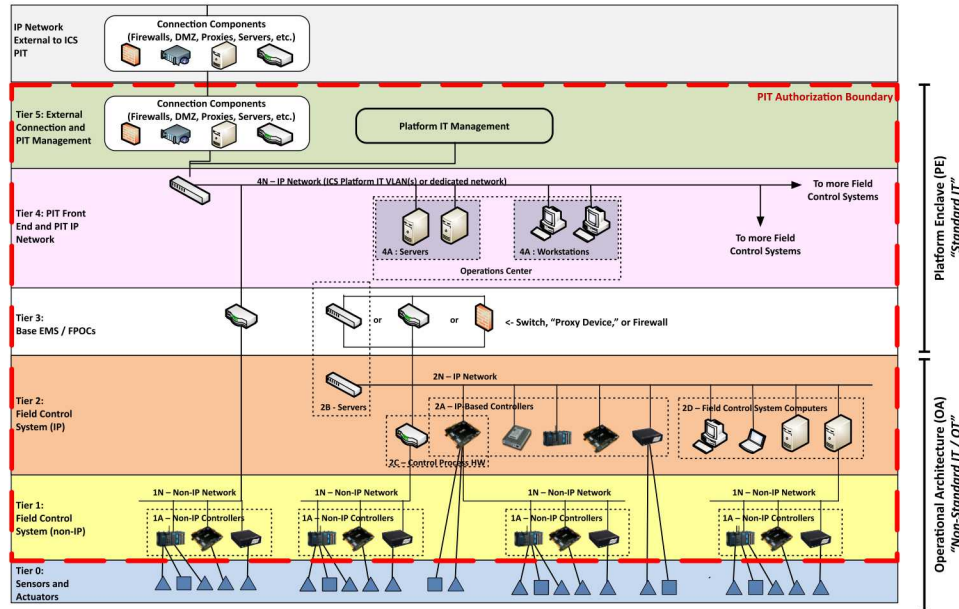


Figure 1.1: Five-Level ICS Control Architecture. OT is organized into a five-tier architecture known as the PERA reference model [3], with sensors and actuators at the bottom and PIT management at the top. Tiers 3–5 (roughly) are comprised of IT systems and Tiers 0–2 (roughly) are OT systems. Field control systems in Tiers 1 and 2 control physical processes in Tier 0. UMCS in Tier 4 centralize control and monitoring among field sites. Successive tiers are segmented from one another based on network technology, firewalls, and translation boxes. In practice, tiers frequently do not exhibit proper network segmentation—field control and sensors and actuators may be accessible from higher tiers and even the Internet. Tiers 0–2 typically lack DiD cyber security mechanisms such as network and protocol authentication, authorization, and underlying cryptographic identities. Instead, devices frequently implement weak or default, well-known passwords. In such cases, an entity with network access also obtains physical process control.

Historically, OT devices and their operating environments were designed to implicitly “trust” peers rather than enforce network and system access policies. In addition, many OT platforms lack authenticated, authorized, and integrity-protected command and control (C2). An “air-gap” between OT networks and traditional IT networks was presumed to provide sufficient security. However, this has led to an emerging challenge in that previously-isolated OT networks are now being interconnected to traditional enterprise IT networks (including the Internet). The motivating factor is that this provides a means to centralize and simplify real-time command, control, and

¹See Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems (UFC 4-010-06) for further discussion regarding the PERA reference model as it relates to secure design [2].

visibility of physical processes. It is not uncommon for CES systems to remain interconnected in undocumented, unmanaged ways with vendors and other networks.

This “network bridging” with external networks can also occur during operations, administration, and maintenance (OA&M) of OT components. OA&M often includes the temporary introduction of a portable computer into an ICS environment, effectively bridging source and destination networks of the portable and subsequently subverting any “air-gap” property the ICS network may have held.

Altogether, implicit trust and broad network accessibility leaves ICS environments vulnerable to exploitation. This presents a serious threat when combined with the broad scope of our nation’s dependence on such systems. The problem is particularly acute for the CES systems addressed by this study, which can include systems deployed at military installations. Malfunction or exploitation of the bulk electric system (BES) and CES systems would cause outages at critical installations.

1.1.1 Threats

Modern threats have demonstrated the ability to capitalize on this situation across the world. Targeted, sophisticated attacks have been conducted to commit espionage and destroy equipment in operational ICS environments. Consider the following examples:

- In 2010, the STUXNET virus bridged “air-gapped” systems and reported false system statuses to the operators at the *Natanz* nuclear facility in Iran. In fact, the malware was providing unexpected and destructive commands to the uranium centrifuges [4];
- In 2013, DragonFly [5, 6] began targeting pharmaceutical companies by compromising supply chain businesses, but was not announced publicly until 2014 [7]; and
- In 2015, malware was reportedly used to disrupt power grid facilities in the Ukraine [8].

This short list is representative of a much larger problem and suggests that simply maintaining the cyber security status quo for CES will inevitably lead to similar (or worse) headlines.

This work assumes that CES face the full spectrum of threats defined by the Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat [9]. The advanced persistent threat (APT) is of particular concern. These are resource-rich entities with people, time, and money to carry out sophisticated attacks over long periods. Supply-chains, logistics chains, and any other vectors into CES are susceptible. Sound defenses across the ICS lifecycle are necessary to slow progress of APT. No defense will defend perfectly against them.

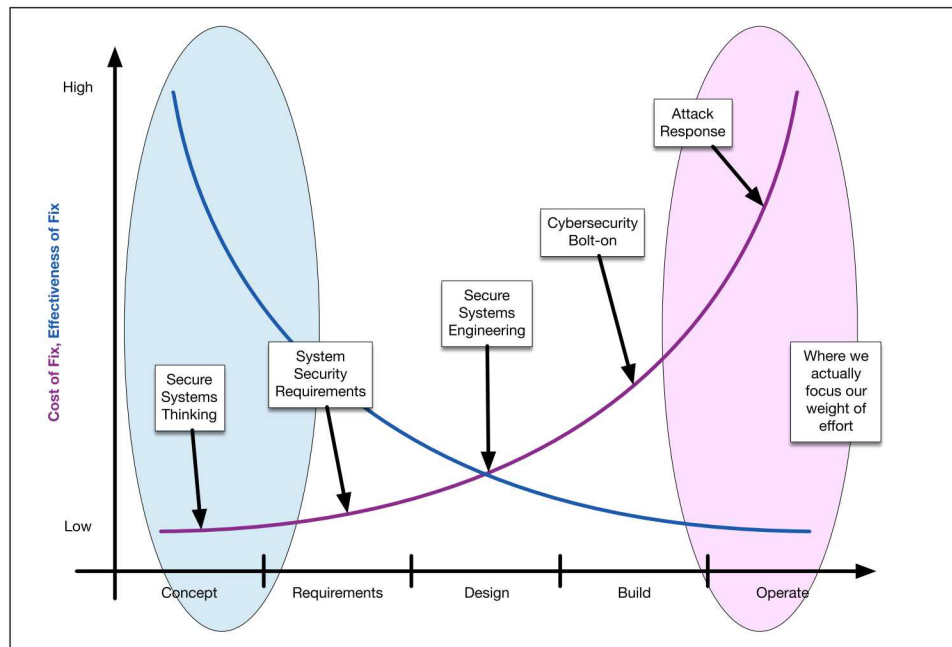


Figure 1.2: SDLC, cyber security, and effectiveness. To have a significant impact, cyber security should be considered early and often in the SDLC. Large, fundamental changes can be made early in the conceptual and design phases of a system that have a significant impact on its overall cyber security posture. On the other hand, only minor changes, such as bug fixes and feature additions, can be cost-effectively applied later in the SDLC. Wide-sweeping design or architectural modifications that fundamentally change the cyber security posture of the system are cost prohibitive later in the SDLC and rarely made.

1.1.2 Effective Cyber Security Engineering

Proper ICS cyber security engineering is required to combat these problems and assure safe and secure operational CES and ICS environments in general. However, engineering said environments is a challenge. It requires a deep understanding of cyber security principles, standards, best practices, and operational nuances of ICS applied across the lifecycle of the environment. Unfortunately, this expertise is often lacking. Near- and long-term R&D is required to improve this overall situation.

To be effective against cyber security problems and cost-effective overall, cyber security must be considered early and often in the ICS SDLC and maintained throughout; it is not a one-and-done activity. Figure 1.2 depicts the nature of this important concept.

It also requires an effective DiD strategy. According to the National Security Agency (NSA), DiD “recommends a balance between the protection capability and cost, performance, and operational considerations”[10]. DiD is characterized by multiple layers of security placed throughout a system and its encompassing environment in order to prevent the failure of any single mechanism from compromising the safety and security of the entire system [11]. Cyber security mechanisms span the entire SDLC. In addition to NSA, the DiD strategy is promoted by NIST RMF, DHS [12], and others [13].

1.2 Long-term R&D Gap Analysis

To accomplish the long-term gap analysis, SNL followed the approach depicted in Figure 1.3. (The “Section” information under each of the three columns corresponds to the location within this report where the respective documentation is located.) This mirrors conventional gap analysis, in that both an existing and a desired state are developed, then compared to identify gaps, and finishing with ranking the gaps. This was only slightly more difficult for the needed R&D analysis; here, the existing state is a survey of existing R&D programs and modern ICS technology capabilities, while the desired state is the idealized secure and resilient ICS in the future. The gaps therefore are the differences in the expected capabilities for secure ICS compared to the characteristics of the desired state. The gap ranking and recommendations depend on an estimation of the best cost-benefit in terms of cyber resilience and risk reduction versus needed investment and uncertainty about the success for the needed R&D.

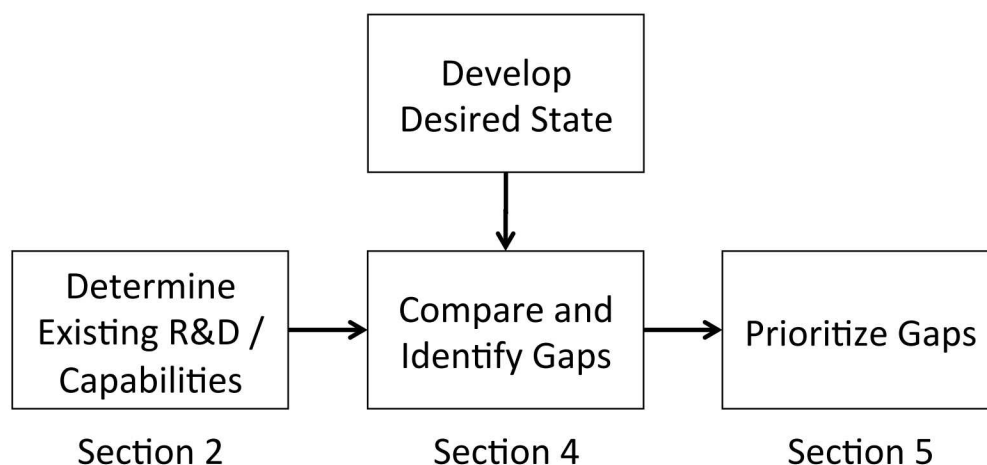


Figure 1.3: Gap analysis process for long-term ICS cyber R&D

1.3 Report Roadmap

The remainder of this document is divided into four chapters. The content of each chapter is itemized below:

- **Chapter 2** discusses the current major R&D thrusts affecting the long-term.
- **Chapter 3** describes the desired long-term ICS cyber security R&D state (subdivided into topic areas) and identifies the gaps associated with each topic.
- **Chapter 4** concludes the report and provides recommendations about gap prioritization.

Chapter 2

ICS Cyber Security Research and Existing Capabilities

In support of the gap analysis process illustrated in Figure 1.3, a literature search was performed in an attempt to narrow down the extensive universe of existing R&D programs and capabilities to some important sources recommended as a baseline for the long-term R&D gap analysis. While it would be unrealistic to capture and include all existing research, the following materials are proposed as some of the most relevant agencies/industries and key documents. Many of these agencies and documents can serve as a launching pad to more literature referenced within them, so the idea is to capture a good set of root documents from which to summarize the current state.

2.0.1 SPIDERS

The Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Joint Capability Technology Demonstration (JCTD) project addressed the need of secure and reliable electric power at military installations by building microgrids at three military installations. This was a combined effort funded by both DoD and DOE, and included support from numerous agencies and laboratories. The microgrids included:

- Joint Base Pearl Harbor-Hickam (JBPHH) in Hawaii (operational in 2012)
- Fort Carson in Colorado (operational in 2014)
- Camp H. M. Smith in Hawaii (operational in 2016)

Each microgrid depended on networked control systems to manage generation, loads, and the installation's electrical grid. As the goal was to *improve* energy reliability, the project made it a priority to ensure that the new control systems did not *decrease* reliability through cyber vulnerability.

In parallel with the actual ICS installation, the SPIDERS team developed the Cyber Security Reference Architecture (CSRA) to improve the cyber security beyond the strict minimum needed for approval [14]. The CSRA applies defense-in-depth techniques described in various references. A key concept for the approach is that ICS have narrowly-defined operating conditions; therefore,

network segmentation that allows by exception and denies by default is easily applied. This has a further advantage in simplifying monitoring for alarms.

The CSRA utilizes the following process, each of which is described at length in the document:

- Enumerate the actors in the ICS system
- Develop requirements for each required data exchange between ICS actors
- Sort the actors into enclaves, based on location, network connectivity, and other reasonable factors
- For required communications between different enclaves, develop a functional domain, which allows only the required data exchange
- Develop an overlay of cyber security controls to enforce the enclaves and functional domains

The defense-in-depth concepts in the CSRA may not be revelatory, but they are straightforward, and this is an advantage for cyber security engineering. Consider the example ICS system shown in Figure 2.1. The example system includes several common elements: human-machine interface (HMI), energy management system (EMS), front end processor (FEP), and several remote terminal units (RTUs). Following the CSRA process, the actors and data exchanges were identified. Afterward, the actors were sorted into enclaves: first, by location, and then by function. The resulting enclaves are shown in Figure 2.2. Functional domains were identified to support the needed data exchange. Finally, firewalls (in this case, three) and ACL – here, on the router between the FEP and RTU enclaves – were used to enforce the enclaves and functional domains.

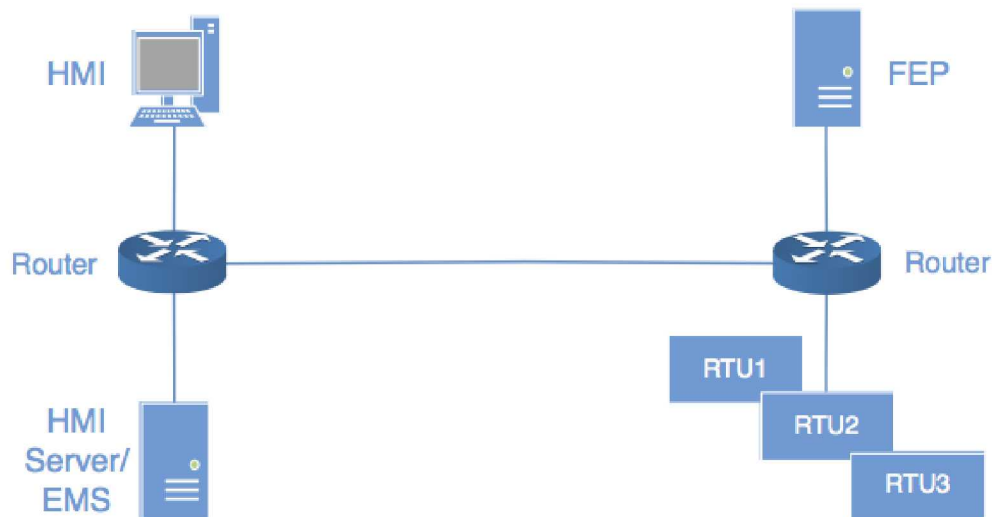


Figure 2.1: Reference architecture test network (flat configuration).

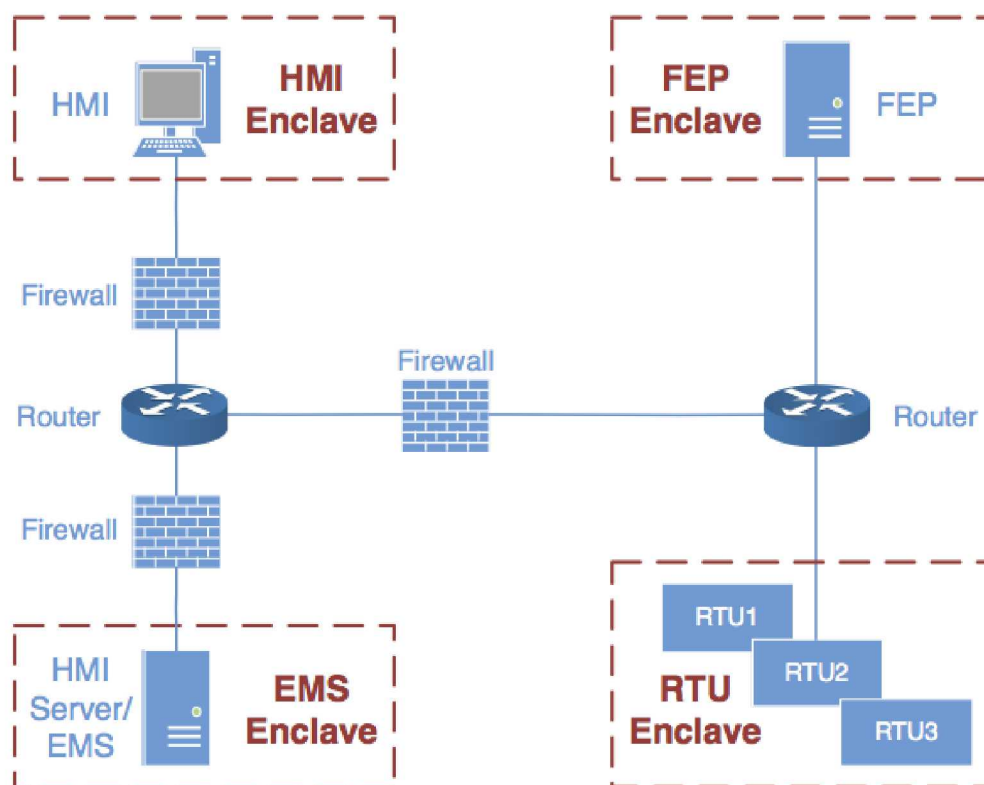


Figure 2.2: Reference architecture test network (enclaved configuration).

The work done to develop enclaves and functional domains can be leveraged to create a Red Team scoring system for the microgrid control network. Each data exchange – control, data, or otherwise – includes requirements for the security attributes confidentiality, integrity, and availability. In the CSRA document, assigning “high,” “medium,” and “low” is recommended; these are used to drive the architecture and cyber security controls. The scoring system derives naturally from mapping the low-medium-high to the numerical values 1, 2, and 3 respectively (although any could be used, the simplest approach is simple incrementing values).

Red Team tests are scored by carefully monitoring the data flows within functional domains during the engagement. If any flow was impacted according to confidentiality, integrity, or availability, then the affected security attribute was scored as a zero; otherwise, if unaffected it was scored according to its value from the data exchange worksheet. At the end, if any security attribute was impacted, then test score was less than perfect. During CSRA testing during SPIDERS, both read and write flows were impacted, sometimes differently. As expected, different scored resulted from different Red Team starting conditions and ICS defensive arrangements. The CSRA approach, and the resulting scoring, provides a quantitative way to compare defensive strategies.

2.1 NIST Guide to Industrial Control Systems Security

The “Guide to Industrial Control Systems Security (800-82rev2)” is a NIST publication [15] released in May 2015. The document provides guidance on how to secure ICS, including supervisory control and data acquisition (SCADA), distributed control system (DCS), and other control system configurations such as programmable logic controllers (PLCs), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. The following are some of the main general threat and vulnerability points of the guide:

- ~90% of the nation’s critical infrastructures are privately owned and operated.
- Internet Protocol (IP) devices can increase cyber security vulnerabilities and incidents, largely because protection and engineering is rarely implemented.
- Increased use of wireless networking can increase risk from close physical proximity without needing direct physical access to equipment.
- Threats can come from many sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters.

According to NIST 800-82, the incidents that an ICS may face can be categorized into six major groups, as follows:

- Blocked or delayed flow of information through ICS networks, potentially disrupting ICS operation.
- Unauthorized changes to instructions, commands, or alarm thresholds, potentially damaging, disabling, or shutting down equipment, creating environmental impacts, and/or endangering human life.
- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects.
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the operation of safety systems, which could endanger human life.

Considering the variety of threats, NIST 800-82 provides guidance on achieving the following general ICS implementation security objectives:

- Restricting logical access to the ICS network and network activity:
 - Unidirectional gateways
 - Demilitarized zone (DMZ) network architecture with firewalls preventing network traffic from passing directly between the corporate and ICS networks
 - Separate authentication mechanisms and credentials for users of the corporate and ICS networks
 - Using a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer
- Restricting physical access to the ICS network and devices with a combination of physical access controls, such as locks, card readers, and/or guards.
- Protecting individual ICS components from exploitation:
 - Deploying security patches in as expeditious a manner as possible, after testing them under field conditions
 - Disabling all unused ports and services and assuring that they remain disabled
 - Restricting ICS user privileges to only those that are required for each person's role
 - Tracking and monitoring audit trails
 - Using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware
- Restricting unauthorized modification of data, including data that is in transit (at least across the network boundaries) and at rest.
- Detecting security events and incidents, including the capability to detect failed ICS components, unavailable services, and exhausted resources that are important to provide proper and safe functioning of the ICS.
- Maintaining functionality during adverse conditions:
 - Designing the ICS so that each critical component has a redundant counterpart
 - Components should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event
 - Graceful degradation such as moving from “normal operation” with full automation to “emergency operation” with operators more involved and less automation to “manual operation” with no automation
- Restoring the system after an incident.

A typical ICS defense-in-depth strategy is then proposed in the document, to include the following:

- Developing security policies, procedures, training and educational material that applies specifically to the ICS.
- Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, increasing heightened security as the threat level increases.
- Addressing security throughout the lifecycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning.
- Implementing a network topology for the ICS with multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Providing logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways).
- Employing a DMZ network architecture (i.e., preventing direct traffic between the corporate and ICS networks).
- Ensuring the critical components are redundant and are on redundant networks.
- Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
- Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Restricting physical access to the ICS network and devices.
- Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).
- Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).
- Using modern technology, such as smart cards for Personal Identity Verification (PIV).
- Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.
- Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate.
- Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS.
- Tracking and monitoring audit trails on critical areas of the ICS.
- Employing reliable and secure network protocols and services where feasible.

2.2 Cyber Security for Energy Delivery Systems (CEDS)

The DOE OE CEDS program was designed to assist the energy sector (electric, oil, and gas) with cyber security solutions for energy delivery systems [I6]. CEDS co-funds projects with industry partners to make advances in cyber security capabilities for energy delivery systems. The CEDS program focuses on the threats posed to control systems within energy delivery systems, such as SCADA and DCS.

The CEDS program activities are categorized into five project areas, guided by the *Roadmap to Achieve Energy Delivery Systems Cybersecurity* [I7]:

- **Build a Culture of Security:** Through extensive training, education, and communication, cyber security “best practices” are encouraged to be reflexive and expected among all stakeholders.
- **Assess and Monitor Risk:** Develop tools to assist stakeholders in assessing their security posture to enable them to accelerate their ability to mitigate potential risks.
- **Develop and Implement New Protective Measures to Reduce Risk:** Through rigorous research, development, and testing, system vulnerabilities are revealed and mitigation options are identified which has led to hardened control systems.
- **Manage Incidents:** Facilitate tools for stakeholders to improve cyber intrusion detection, remediation, recovery, and restoration capabilities.
- **Sustain Security Improvements:** Through active partnerships, stakeholders are engaged and collaborative efforts and critical security information sharing is occurring.

The Energy Sector Control Systems Working Group (ESCSWG) updated the *Roadmap to Achieve Energy Delivery Systems Cybersecurity* to build upon the successes of the energy sector and address gaps created by the changing energy sector landscape and advancing threat capabilities, and to emphasize a culture of security. Released in 2011, the updated *Roadmap to Achieve Energy Delivery Systems Cybersecurity* identifies the critical needs and priorities of the energy sector and provides a path for improving security, reliability, and functionality of energy delivery systems.

CEDS supports industry-led, cost-shared projects that improve cyber intrusion detection, remediation, recovery, and restoration capabilities of both the energy delivery systems as well as the cyber-physical interfaces. This is done in collaboration with National SCADA Test Bed (NSTB) labs and other private-sector partnerships to develop and commercialize tools and technologies that can make real and immediate impacts on energy sector cyber security. Also, through partnerships with academia, CEDS supports the development of new research, providing a platform to bring power systems engineering and computer science together, to meet the current and future needs of providing cyber security for energy delivery systems, e.g. TCIPG [I8].

2.3 Academia

One of the goals when exploring the baseline was to consider important academic sources involved in ICS cyber security, specifically those rooted in the University of Illinois at Urbana-Champaign's TCIPG and Georgia Institute of Technology Research Institute's IISP. The IISP at Georgia Tech is as an international leader in researching, developing, and disseminating technical solutions and policy about cyber security and privacy. The mission of IISP is to identify and address the grand challenges in cyber security and privacy. Also, to engage the government, industry and general public on cyber security and privacy issues, and transfer results into deployable technologies.

The IISP focuses on six initial research topics [19]:

- **Attribution:** malicious code is one of the most common pieces of forensic evidence available to the security research community. However, a standalone binary by itself is not very useful in developing attribution statements. This is due to the lack of context in standalone binary: it does not indicate an author, controller, infected victims or the aim of the operation. A standalone binary does not even confirm in which operation it was used. IISP is working on large-scale collections of malware samples to identify relationships between binaries. With a sufficient sample size, machine-learning techniques can be applied.
- **Consumer-facing Privacy:** the PrivacyGuard project is a first step toward establishing a practical way of ensuring end-to-end privacy for big data computations. To achieve this, IISP is working to develop protocols that split the responsibility for data privacy protection into three areas: data entry, execution, and output.
- **Cyber-Physical Systems:** physical systems are increasingly monitored, protected, and controlled by cyber systems; such as electric power generation, gas/petroleum production, air and land transportation, or medical systems. Control and protection decisions are now made in cyberspace and executed via a cyber/physical interface where intruders can steal sensitive information, cause disruptions, and irreparable harm. Detection of attacks now requires that domain-specific models and simulators, which can provide physical-system awareness, be included early in the design process.
- **Privacy Policy:** there are challenging privacy issues concerning who should be authorized to collect, use, and share personal information. There are both privacy and security issues since many computer systems have flaws that can be exploited for malicious purposes. Current research topics include:
 - Encryption and government access to the content of communications in transit and at rest, as discussed in this 2015 Senate testimony
 - Rules for transfer of personal information between the European Union and the United States, in light of the 2015 court decision striking down the “Safe Harbor” agreement for data transfers
 - Updating the mutual legal assistance process (the major legal mechanism for sharing electronic evidence between nations)

- Private-sector use of information, including in connection with Internet Service Providers (privacy rules concerning them come under debate at the Federal Communications Commission)
 - Smart cities and smart campus initiatives, to ensure privacy and security for the “internet of things”
- Risk: cyber attacks can lead to significant financial and reputation loss, severely inconvenience customers and employees, lead to loss of privacy, cripple the operations of an organization and the economy, and even cause physical harm. Organizations must manage the risk their organizations face from cyber attacks and data breaches. The research focus of the risk management area is on the middle layer that deploys the technical solutions available to meet the risk objectives of senior management, with special emphasis on policies, procedures and end-user training that creates a safer computing environment. In addition, the research focus is also on public policy issues that provide the right incentives to various stakeholders within the ecosystem to minimize risk for participants.
 - Trust: the reliance on machine-to-machine (M2M) systems to make decisions has profound implications. Trust is the belief in the competence of a machine or sensor to act dependably, securely and reliably within a specified context. In machine-to-machine systems, trust is commonly accomplished using cryptography, digital signatures, and electronic certificates. This approach establishes and evaluates a trust chain between devices, but it does not reveal enough about the quality of information being exchanged among machines. Trust is a broader notion than information security; it includes subjective criteria and experience [20].

The TCIPG project at the University of Illinois at Urbana-Champaign (UIUC), funded by the DOE OE and DHS Science and Technology Directorate as a part of CEDS, is a project based on the partnership of four academic institutions: UIUC, Arizona State University, Dartmouth College, and Washington State University. The project is intended to meet the challenge of protecting the power grid by significantly improving the way the power grid infrastructure is designed, making it more secure, resilient, and safe. The TCIPG research has produced important results and innovative technologies in the following areas [18]:

- Detecting and responding to cyber-attacks and adverse events, including incident management of these events
- Securing of the wide-area measurement system on which the smart grid relies
- Maintaining power quality and integrating renewables at multiple scales in a dynamic environment
- Advanced testbeds for experiments and simulation using actual power system hardware “in the loop”

2.4 DoD and Others

DARPA heads the rapid attack detection, isolation, and characterization systems (RADICS) program. The goal of the RADICS program is to develop innovative technologies for detecting and responding to cyber-attacks on US critical infrastructure, especially those parts essential to DoD mission effectiveness. DARPA is interested, specifically, in early warning of impending attacks, situation awareness, network isolation and threat characterization in response to a widespread and persistent cyber-attack on the power grid and its dependent systems. Potentially relevant technologies include anomaly detection, planning and automated reasoning, mapping of conventional and industrial control systems networks, ad hoc network formation, analysis of industrial control systems protocols, and rapid forensic characterization of cyber threats in industrial control system devices [21]. There is an extensive amount of research material available via DARPA's RADICS website containing a vast amount of information regarding the current state of ICS cyber security.

For an example of a more specific ICS cyber security application in use today, SNL's WeaselBoard PLC backplane analysis system is included. The "WeaselBoard: Zero-Day Exploit Detection for Programmable Logic Controllers" is a SNL publication [22] released in October 2013. The document describes how the WeaselBoard PLC backplane analysis system can provide means to detect attacks on PLCs at the hardware or firmware level by detecting changes in the PLC and the process. The WeaselBoard connects directly to the PLC backplane to capture backplane communications between modules. Inter-module traffic is then forwarded to an external analysis system that detects changes to process control settings, sensor values, module configuration information, firmware updates, and process control program (logic) updates.

As previously mentioned, it would be unrealistic to list all existing technologies in this baseline section, but the preceding were some of the key examples. Beside the vast exploration available within each of the entities already discussed in Chapter 2, the following documents and groups also offered extensive background pertinent to the long-term R&D gap analysis:

- NIST Cybersecurity Framework [23]
- International Society of Automation (ISA) [24]
- DoD Cyber Strategy [25]
- NERC CIP [26]
- DOE OE Cybersecurity [27]
- Institute of Electrical and Electronics Engineers (IEEE) Cybersecurity Initiative [28]
- DHS Cyber Security [29]
- Other FFRDC programs, e.g. at SNL, Oak Ridge National Laboratory (ORNL), Massachusetts Institute of Technology Lincoln Laboratory (MIT LL), Pacific Northwest National Laboratory (PNNL), etc.

Chapter 3

Future Vision: Long-Term

The first major task for the desired long-term R&D gap analysis is to describe the existing state; this was summarized in Chapter 2. The second task is to characterize the desired end state for the concept or situation being analyzed: here, security for ICS systems. Again, the particular focus is on energy systems support for critical missions at government or other important sites. The third task is to compare the two (existing and desired) to identify the gaps. This is the focus of this chapter. The subsequent section (Chapter 4) will prioritize gaps to provide additional recommendations.

For an ICS, in the long term the desired end state should represent a safe, secure, and resilient control system that supports telemetry of time sensitive data (in order to support physical process control) and provides sufficient power when needed. Some key security and resiliency features may include:

- Allows different categories of process functional requirements (availability, integrity, and confidentiality as needed)
- Is resistant to adversarial penetration
- Is able to interface securely with data sharing partners
- Supports updating and adaptation without service interruption
- Monitoring for quick and accurate diagnosis of cyber conditions
- Degrades gracefully for some reasonable expected adversarial penetration
- Supports attribution necessary for law enforcement and national response requirements
- Can be recovered to pre-incident conditions without excessive burden

Gap analyses for R&D are slightly more complex than gap analyses for business processes. Here, determining the current state of R&D is straightforward enough (although complex). The desired state is less obvious, as an ICS has peculiar concerns. Conventionally, the “buckets” for desired end state and gaps are called *topics*. These subdivisions are less science than art, although clearly they should be selected to support the discussion. The slices can also be informed by divisions within R&D programs, and might mirror surveys of IT R&D. The topics can also be derived from existing perspectives on cyber security.

3.1 Planned Approach

The approach for the development of topics for long-term ICS cyber security R&D will proceed according to the following steps:

1. Introduce an underlying framework for ICS cyber gap analysis, currently used at SNL (Section 3.2)
2. Develop an organization for the security topics leveraging common NIST and DoD frameworks for security lifecycle and mitigations (Section 3.3)
3. Present summary tables containing long-term security topics (Section 3.4)
4. Discuss each topic in-depth, including gap identification (Section 3.5)

3.2 ICS Cyber Framework

Consider the potential goals for cyber attacks against ICS, which can generally fall into five categories. An adversary will seek one or more goals to achieve a desired effect in the underlying physical architecture (electric supply, machinery control, weapons systems, oil/gas pipelines, manufacturing, building automation, etc.). These are the outcomes that must be prevented or attenuated by ICS cyber security measures, as represented by the desired long-term end state.

- **Goal G1 – Change behavior:**

Changing the control settings or logic can lead to behavior that is advantageous to an adversary. In extreme cases, this could cause or contribute to equipment damage, dangerous hazards, or systems degradation/failure.

- **Goal G2 – Misrepresent state:**

ICS devices form the boundary between operators and the physical process. Vulnerabilities might facilitate the device misrepresenting the process state (or its own), either directly (the device itself is misrepresenting) or indirectly (the device can be easily impersonated).

- **Goal G3 – Obtain or change data:**

Any ICS device may be more or less amenable to reporting potentially sensitive data about itself or the underlying process to unauthorized actors, or toggling control based on correctly-formatted protocol directions.

- **Goal G4 – Deny operation:**

An ICS is almost always expected to have very high uptime, particularly to manage potentially dangerous physical processes. Therefore, a short-term loss of functionality – even

partial – could be important. Straightforward vulnerabilities can permanently disable some devices. Note that the denied operations are being analyzed from the perspective of the field device itself; therefore, denial of communications external to the device would be an example of a procedure that would be out-of-scope.

- **Goal G5 – Use as intermediate attack platform:**

An adversary can theoretically use any computing device as a network or systems beach-head for further malevolent activities. This will usually take the form of a high-privilege interactive session for the adversary, with the download and hosting of additional software tools desirable. Very often, the architecture of embedded devices makes this goal unlikely for them, but it remains reasonable for many scenarios, especially for platforms that leverage more conventional hardware/software.

An adversary has several generalized operations that can support the realization of these goals. Procedures can be thought of as the net results of overall scenarios that involve manipulation of the targeted equipment and systems in ways outside their intended applications. Topics for long-term R&D must improve the resistance of a targeted ICS against one or more procedures.

In a general sense, an ICS has both an *operational* character and a set of capabilities for *administration*, particularly the configuration of the control and monitoring envelope. ICS cyber security measures will reduce the likelihood that adversaries can successfully execute procedures, even if they are able to gain to initial opportunity to do so. The list of adversary procedures, shown below, can affect either or both of the operational character or administrative configuration for equipment within a system:

- **Procedure P1: Achieve device management access**

Typical configuration parameters include management-specific information, like networking addresses, accounts (to the extent that the device supports them), logging frequency and parameters, etc. Other configuration data affects the equipment's control and measurement of physical data, like control setpoints, measurement intervals and scaling, ladder logic, etc. Modifying the device's behavior could allow an adversary to achieve any goal (although G5 might be difficult if malware or tools are not available for the targeted equipment's architecture). The device hardware may also be changed to suit an adversary. P1-type scenarios could easily lend themselves to minimal probability of detection or attribution and because ICS devices have long operational deployments, adversary-driven changes in configuration could have a long-term presence.

- **Procedure P2: Gain privileged operational relationship**

Depending on the situation and access, an adversary could gain valuable data and potentially affect processes by manipulating network data. This might involve accessing existing peer devices, adding customized hardware to the network, or simply injecting traffic. The ability to view device traffic on a network could allow for unauthorized access to data being sent to or from an ICS device (depending on the protocols and safeguards used), which is a type of

privileged relationship. Depending on the particulars of the resulting data relationship, any of G1 – G4 are potential outcomes.

- **Procedure P3: Impersonate the device**

The scenario described in P2 above also extends to the possibility of an attacker providing or consuming data in place of a targeted piece of equipment. The authentic data messaging for the targeted device could be blocked, changed, or ignored depending on the adversary's needs. This procedure would allow an adversary to misrepresent state (G2).

- **Procedure P4: Affect device operation via atypical stimuli**

This type of procedure covers tactics not previously mentioned and that do not depend on the intended administration or operations of the device. Examples would include denial of service (DOS) attacks, susceptibility to radio frequency (RF) that affects operation or management, flaws in protocol or server implementations that could crash devices, adding unauthorized hardware to systems, etc. Successful P4 tends to achieving goals G1 (change behavior, in the sense that severe issues could change how the device operates) or G4 (deny operation, if all or part of the targeted ICS crashes).

Finally, access allows the potential execution of steps in one or more selected procedures. Access represents a fundamental requirement for any planned procedure and, if unavailable, would negate the feasibility of even attempting some procedures. However, access can be gained in many different ways over diverse timeframes, including the key opportunities below:

- **Access A1 – Physical**

An adversary could leverage physical access to introduce additional equipment, either in the local network, on a configuration interface, within the device itself, or added to a modular chassis (like many PLCs have). These can provide varying opportunities for procedures with low potential for detection (depending on the configuration control and monitoring scheme). Physical access can also easily affect device configuration if firmware is stored on removable media. Local physical access might also enable targeting of secondary communications ports used for device configuration (like a console port on a PLC). If there is a dedicated configuration interface, then this represents a potentially attractive opportunity for an adversary if it can be physically accessed, because it typically has the highest privilege levels available. If there are authentication challenges, these can be often defeated by jumpers or other physical interfaces on the equipment. Another particularly insidious type of access would be to achieve net physical access using social engineering vectors (like the classic case of the USB drive in the parking lot). Similarly, an adversary could game operators to manipulate ICS equipment to affect a number of procedures and achieve goals. Many physical access avenues could be very persistent and stealthy.

- **Access A2 – Network**

ICS devices are very often networked via their operational interfaces to participate in control with peer or remote systems. Networks can be based on legacy serial technology or

modern systems like Ethernet and Transmission Control Protocol/Internet Protocol (TCP/IP) (although tending toward the latter in the future, and possibly including more wireless channels).

- **Access A3 – Secondary communication**

Permanent or periodic remote access can be intended for the equipment-owning entity to gather data or manage configuration, or could be used via trusted partners like outsourced technical management or vendors (many of which often require highly privileged access to their equipment). This is separate from continuous network access (A2), in that if both A2 and A3 are present, A3 offers distinct opportunities for adversaries (including, potentially, network access or A2).

- **Access A4 – Peer device**

An adversary might access functionality on a targeted device by successfully gaining privileges on a peer device, and then exploit the existing trusted data relationships that support the operations of the ICS system. This would be a straightforward way to execute scenarios that depend on P2 (Gain Privileged Operational Relationship).

- **Access A5 – Engineering workstation**

As noted in the “Procedures” discussion, unauthorized device management is a key problem for ICS. One extremely attractive access opportunity would therefore be via the platform that is normally used to manage and configure the targeted equipment (typically called the engineering workstation – one or more computing platforms used for authorized configuration control of embedded systems). Either the management software itself or other hardware/software elements of the platform could be targeted.

- **Access A6 – Supply chain**

Another interesting avenue for access is to consider the possibility that an adversary has affected an ICS device’s hardware or software as it was being developed or sourced. Trojan code or modified silicon may require very high investments to achieve, but for certain classes of adversaries the possibilities are reasonable. Another avenue for access in this category involves an adversary affecting the supply chain for product updates, particularly for software/firmware. Although ICS devices are rarely updated or patched by current practice, there appears to be more acceptance coming for field updates to ICS. Under those conditions, Trojan code may be introduced into systems for later use.

Many accesses map to more than one opportunity to execute a procedure (and subsequently achieve an attack goal). Often, network access has an incredible force multiplier in poorly-secured networks (i.e. an adversary can execute procedures against many devices with scarcely more resources than would be required to attack a single component); as a result, denying or limiting network ingress is critical. Physical access is similarly troubling, as many ICS depend on equipment that are in poorly-visited engineering spaces, and the scope of attack possibilities given physical access is astronomical.

In summary, this framework represents an analytical perspective that grounds the long-term gap analysis. The desired state for cyber security will include measures that will:

- Reduce the likelihood of an adversary achieving goals even if they are able to successfully execute procedures
- Reduce the likelihood of an adversary executing procedures even if they are able to achieve access
- Reduce the likelihood of an adversary achieving access

At the extreme, a secure ICS will be resilient and degrade gracefully even if an adversary is successful in achieving goals.

3.3 Categorizing Cyber Security

This section will discuss a categorization scheme for long-term capabilities that will support the desired ICS cyber security state. To manage risk and improve security, system designers proactively employ mitigation measures throughout the lifecycle of the system. As described in [I5], the lifecycle of a secure information system (which includes ICS) has several stages:

- Architecture & design
- Procurement & installation
- Maintenance
- Decommissioning

For the long-term time horizon, the issue of decommissioning will be set aside, as problems in this area relate more to insufficient attention and care than any fundamental deficiencies. There are significant cyber issues in the remaining three stages. For clarity, these will be rewritten slightly to emphasize resilience:

- **Secure Design**

The goal of secure design is to execute on the old maxim to “include security early in the development.” Topics in this category will cover security and resilience issues that must be in mind for an ICS at the earliest stages of development, as they cannot be added later. An example would be resilient control algorithms, which would allow graceful degradation even if one or more goals are achieved by an adversary. (In contrast, too often contemporary controls are brittle to intentionally manipulated data.)

- **Reinforced Implementation**

This also represents including security early in the development, but in the lifecycle period where the design is being translated into equipment and systems. There are many, many opportunities to add security measures and technology that do not require fundamental design changes, but will provide enormous benefit. One simple example here is network defense-in-depth: limiting successful network access by an adversary by creating data enclaves [14]. Another key opportunity is automated device monitoring, by adding separate, better-trusted components to spy on key ICS buses, possibly within modular chassis [22].

- **Deployment and Operation**

Once an ICS is deployed, then the security challenges change. As suggested by the NIST lifecycle term “maintenance,” there is a requirement to maintain the ICS’s cyber security under changing threat and vulnerability conditions. Operation is also when the issue of addressing attacks and restoring afterward are encountered.

There are different *types* of opportunities for cyber security and resiliency within the described lifecycle categories. Security improvement, or vulnerability mitigation, reduces adversary opportunities described within the framework (Section 3.2). Potential examples include detecting adversary indicators via cyber controls or guarding against physical effects using physical controls (like pressure relief valves or fuses).

Within the NIST security “Framework Core,” there are five stages for security [30]:

- **Identify:** Organizational understanding and management of cyber security
- **Protect:** Stop or delay adversary manipulation of systems
- **Detect:** Direct evidence or correlated indicators that reveal adversary presence and activity
- **Respond:** Managing ongoing adversary activity while maintaining operations to the best reasonable extent
- **Recover:** Restoring the normal ICS state and minimizing continuing adversary presence

Often, DoD guidance focuses on the latter four [31], and this is the approach that will be followed here.

To summarize this section, the long-term ICS cyber security R&D topics will be organized per the categories for lifecycle (secure design, reinforced implementation, and deployment and operation) and stage (protect, detect, react, and recover). This will result in a grid format within a table.

3.4 Summarized Long-Term State for ICS Cyber Security

The desired end-state for long-term ICS cyber security R&D topics is shown in Tables 3.1 and 3.2. The information in the tables is organized per the scheme introduced in the prior section (3.3). Table 3.1 numbers the R&D topics from 1 to 18; these numeric indices will be referenced later.

Table 3.2 contains far more descriptive information than Table 3.1, but is clearly more dense visually. The 18 numbered R&D topics from Table 3.1 are repeated as the framed phrases in Table 3.2; some short bullets under each provide a quick introduction to the concepts within the topic. The topics themselves are derived from:

- Experience by DOE labs in the area, particularly as referenced to frameworks (Sections 3.2 and 3.3)
- Stakeholder input, both from prior experience as well as discussions specific to this effort
- Concepts gleaned from the relevant background research (Chapter 2)

Table 3.1: Concise long-term ICS cyber security R&D topics

Category	Protect	Detect	React	Restore
Secure Design	1. Moving Target Defense 2. Protected Computing		3. Resilient Systems	
Reinforced Implementation	4. Obfuscation 5. Defense-in- depth 6. Boundaries/ Authentication	7. Security Analytics 8. Trusted Monitors	9. Minimize System Impact	10. Trusted Gold Masters
Deployment & Operation	11. System Adaptation	12. System Assessment/Audit	13. Temporary Capability	14. Secure Recovery
Cross-cutting Capabilities	15. Field Device Security	16. Virtualization	17. Threat Analysis	18. Policy/ Personnel

Taken as a whole, Table 3.2 provides a concise overview of the desired end-state, which will be crucial to the subsequent gap analysis. Each topic is described in detail in the subsequent section.

The general theme of the table is that security – trusting the ICS to correctly and safely manage a physical process – can be improved by resiliency. Many topics promote acceptable operation even after an adversary gains some level of access, in the sense of limiting further access, or curtailing opportunities to execute attack procedures even with sufficient access. Ultimately, a key principle is that *perfect security is unattainable; therefore, strong security engineering must be complemented with additional security monitoring*. Ideally, the monitoring measures should be built as simply as possible, in order to be able to better characterize their own security (and avoid having the monitoring system adding vulnerability). Overall, the combined system should improve trustworthiness, compared to the the primary ICS by itself.

Finally, note that there are four major rows within the table. Three correspond to the given security lifecycle subdivisions. The fourth is an artifact of the issue often encountered when attempting to sort concepts into neat bins: there are always some outliers that either do not fit well into the given taxonomy, or they fit in multiple places. Therefore, the last row, “Cross-cutting Capabilities” is a catchall. The four topics here are not specified in terms of lifecycle or stages.

Table 3.2: Categorized long-term ICS cyber security R&D topics

Category	Protect	Detect	React	Restore
Secure Design - Intrinsic capabilities - Resilience and security	Moving Target Defense - Variability in configuration - Rotating security parameters Protected Computing - Leverage trusted execution/TPM - Minimum privilege/sandboxing		Resilient Systems - Algorithms minimize impacts - Graceful degradation	
Reinforced Implementation - Enhance security during system & component development - Resiliency support	Obfuscation - Misleading additional ICS traffic - High-detail honeynets - Conformal coatings Defense-in-depth - Network enclaves/zones - Anti-tamper protection - Apply cryptographic protections Boundaries/Authentication - Connect different trust zones - Multi-factor authentication support	Security Analytics - Alarms for strong/weak indicators - Requires ICS network sensors - Assimilate all data (platforms, networks, threat indicators, etc.) - Apply varying trust for data - Monitor configuration by measuring response to minor perturbations Trusted Monitors - Deep inspection for components - Support physical data resampling to detect deception	Minimize System Impact - Separate safety engineering from networked control - Minimum-set digital supervision or voting to block dangerous actions - Analog limiter backup protection	Trusted Gold Masters - Protected, secure change control - Regular evaluation for Trojan code
Deployment & Operation - Instantiated systems - Maintenance/testing	System Adaptation - Risk-informed reactions - Changes in operational posture, patches, and upgrades	System Assessment/Audit - Verify logic systematically (components or entire system) - Automated audit - Quantitative metrics	Temporary Capability - Maintain acceptable performance, enable forensics/evidence collection - Virtualized failover systems - Portable temporary equipment	Secure Recovery - Golden master change control - Rapid acceptance/reauthorization for replacement equipment
Cross-cutting Capabilities - Covers testing and assessment - Strong focus on virtualization	Field Device Security - Virtualization for firmware analysis and simulation support - Independent verification & validation of security	Virtualization - Evaluate changes & TTPs - Persistent training environment - Near-real-time model generation & updates	Threat Analysis - Automated threat discovery and fusion with indicators - Actionable indicators without jeopardizing sources or methods	Policy/Personnel - Assess conflicting and unfavorable requirements - Develop security TTPs - Data security definitions - Training

3.5 Long-Term ICS Cyber Topics

In this section, each of the major topics (the numbered items in Table 3.1 or equivalently the boxes in Table 3.2) are described and characterized. These discussions are captured in tables, one per topic. Each table contains the following:

- **Discussion:** A concise overview of the topic, including illustrative examples where appropriate
- **Categorization:** Here, the lifecycle (secure design, reinforced implementation, deployment and operation – or cross-cutting) and security stage (protect, detect, react, recover) are noted, and the rationale for their assignment is explained
- **Framework Mapping:** Often, the topic can be mapped to reducing adversary opportunity to achieve access or procedures, and these are discussed where relevant
- **Current Capabilities and R&D:** The topic is mapped to the documentation in Chapter 2 describing the long-term ICS R&D state; similar or complementary work is summarized
- **R&D Gaps:** The topic description along with the current work will illuminate gaps; the major ones will be amplified and ranked in a subsequent discussion

Table 3.3: Topic description, categorization, and analysis: Moving Target Defense

Desired State (Long-term) R&D Topic 1: Moving Target Defense	
Description	
Moving-target defense involves developing systems that change configuration or operational character while still supporting the necessary control for the underlying physical process. This can range from simply rotating network addresses or cryptographic material to subtly changing control timing (in ways that do not materially affect the system operation, but which reduce predictability for potential adversary procedures). Configuration interfaces could present settings dialogs using different phrasing to defeat some automated attacks.	
Categorization	
Lifecycle:	Secure Design
Stage:	Protect
This opportunity is best addressed at the design stage, as there can easily be ramifications for the algorithmic character of the necessary controls, which would make this challenging as an implementation issue. The topic is labeled “Protect” as it most directly impacts an adversary’s opportunity to attack.	
Framework Mapping	
Relevant access:	A2, A3, A4
Applicable procedures:	All
Moving target defense, even in its most basic form, certainly makes pre-action network (A2) reconnaissance more difficult and time-consuming. Similar communications-based access (A3, A4) could likewise be impacted. Limiting live system information clearly reduces opportunities for many successful attack procedures. Moving target defense may also change key parameters needed for precise targeting for adversary attack (for instance, a vulnerable service may rapidly change its network socket).	
Current Capabilities and R&D	
This topic is of very high interest within the IT community, but is only beginning to be considered for ICS, based on a handful of relevant research papers that were identified (examples include [32, 33, 34]). On the IT side, there are mature R&D efforts at MIT-LL (Moving Target Techniques – Leveraging Uncertainty for Cyber Defense; a review of five dominant categories of cyber moving target techniques assesses their benefits and weaknesses), DHS-CSD (controlling change across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity and increase the costs of their probing and attack efforts [29]), Carnegie Mellon University (Moving Target Reference Implementation; iteratively build moving target middleware for parallel deployment into different lab environments), and Morphisec (Moving Target Defense; morphs the runtime environment so authorized code runs safely while attacks miss their mark [35]).	
R&D Gaps	
There is a significant and attractive R&D gap here, based on the nascent work in the ICS area, lack of focused funding for the concept, and the extensive IT foundational concepts.	

Table 3.4: Topic description, categorization, and analysis: Protected Computing

Desired State (Long-term) R&D Topic 2: Protected Computing	
Description	
The software architecture within platforms supporting ICS should be optimized for an adverse cyber security environment, given their intrinsic attractiveness to many classes of advanced adversaries. Many architectures support opportunities like trusted execution and even trusted platform module (TPM). At a minimum, processes can be developed with minimum privilege or confined to sandboxes to limit cyber impacts. R&D can lower the cost and improve the reliability for vendors to apply these services.	
Categorization	
Lifecycle:	Secure Design
Stage:	Protect
The architectures and tradeoffs involved in leveraging protected computing technologies necessitate their consideration early in the ICS development. Also, this is a protection issue, limiting adversary attack opportunities.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	P1, P4
Protected computing is less about the access needed for attack, and more about attenuating the likelihood of successful procedures.	
Current Capabilities and R&D	
This topic is applicable to either control center platforms (x86 type) or ICS-specific field devices. In both cases, there appears to be only a small extant body of work. One example is from the VTT Technical Research Centre of Finland. Their “Remote Attestation for Embedded Systems” project allows a remote verifier, e.g. a service provider, to verify integrity of the connecting system before providing a service. The current standard practice is based on integrity measurements stored into a TPM. Implementing similar functionality using an Advanced RISC Machine (ARM) processor emulator, including the ARM Trusted Execution Environment (TEE) providing isolated trusted component functionality, is discussed [36].	
R&D Gaps	
This is a significant gap, and one very suitable for ICS R&D investment given its criticality and abundance of non-x86 architectures. This will be best approached by a research consortium including the vendor community.	

Table 3.5: Topic description, categorization, and analysis: Resilient Systems

Desired State (Long-term) R&D Topic 3: Resilient Systems	
Description	
Given that security is imperfect, it is an entirely reasonable assumption that adversarial penetration and activity will impact a fielded ICS given sufficient time and resources. A secure and resilient control system should take that into account and incorporate measures to ensure that degradation is (1) minimized where feasible and (2) graceful when necessary. ICS resources are prioritized to support critical functions during active attack. A resilient control system should maintain state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. False and misleading data would be identified and be less trusted for control (either automatic or supervisory).	
Categorization	
Lifecycle:	Secure Design
Stage:	React
This is a design stage opportunity as it directly impacts algorithmic character for controls. The outcome of resilient systems optimizes reaction during the timeframe of a cyber attack. A resilient control system approach maintains adequate adaptive capacity to ensure minimum normalcy (performance) is maintained to withstand a disturbance.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
R&D focus on resilient systems engineering blunts the impact of all adversary actions. Resilient control systems have adaptive capacity to adapt to adversarial attack, including a time element (agility). A resilient design transforms to protect itself from adversarial action, maintains state awareness to detect if degradation may be occurring and reacts to prevent further impact and expedite recovery.	
Current Capabilities and R&D	
Current ICS can be brittle, with little or no planning to deal with cyber attack (like intentionally false data planted by an adversary). This could lead to complete or near-complete ICS failures and unacceptable impacts. Some R&D approaches, like [37], approach this obliquely through data management. The “human-in-the-loop” aspect of cyber resilience should also be considered. An automated process must trust the data that it is given to make a decision, constrained by its logic. A human has the ability to check out of band validators such as physical measures.	
R&D Gaps	
Targeted investment would be beneficial in the improvement for technology readiness level (TRL) of cyber-physical degradation assessment/trust/mitigation architectures, data fusion and context-aware, cyber-physical visualization for prioritized human response, cross-architecture, extensible and scalable anomaly detection methods, etc.; all of which provide benefit in different aspects of ICS design. All control algorithm development (whether for smart grid, microgrids, transmission, protection, etc.) should include requirements that consider the possibility of adversarial penetration and manipulated data/system settings.	

Table 3.6: Topic description, categorization, and analysis: Obfuscation

Desired State (Long-term) R&D Topic 4: Obfuscation	
Description	
Obfuscation protects ICS security by increasing the noise floor that must be penetrated by a cyber adversary. Both reconnaissance and targeting could be affected. Communications traffic as well as physical hardware can be hidden or camouflaged. Honeypots and honeynets are already used, but these can be made to adapt to current conditions so they are harder to distinguish. Any platform with hot spares could be converted on the fly to honeypot status if adversary action is detected (this is more approachable for a virtualized platform). Conformal coatings make it more difficult (although certainly not impossible) for an adversary to discover chip architectures and unused, attackable ports.	
Categorization	
Lifecycle:	Reinforced Implementation
Stage:	Protect
Obfuscating measures are intended to protect from attack, and can be added after primary design is complete.	
Framework Mapping	
Relevant access:	A1, A2, A3, A4
Applicable procedures:	P2
Obfuscating measures are most applicable to communications access (A2, A3, A4) and also physical (A1). A key protection is denying data to an adversary (P2).	
Current Capabilities and R&D	
There is little existing work for ICS, but much for IT. Some highlights include:	
• Arxan Advanced Obfuscation: patented techniques to transform program code so it is extremely difficult to understand and analyze. These techniques are highly effective in concealing the purpose and/or the logic of the software program to prevent application tampering, deter reverse engineering, and safeguard intellectual property [38]. • Vencore Labs Inc., Advanced Cryptographic Obfuscation Techniques: work in progress under a \$3.7 million contract from the DARPA SafeWare Program. Research will focus on enabling highly secure, highly efficient techniques that meet real-world applications and are relevant to defending programs against reverse engineering attacks [39].	
R&D Gaps	
The deterministic nature of ICS relative to IT makes the usefulness of obfuscation unsure. The R&D gap is to identify what techniques are most useful, and if any are effective enough to be justified.	

Table 3.7: Topic description, categorization, and analysis: Defense-in-depth

Desired State (Long-term) R&D Topic 5: Defense-in-depth	
Description	
The security of an ICS can leverage network segmentation to reinforce defense-in-depth practices. A system may be subdivided into enclaves defined by system functions, physical locations, and security concerns. Communication between enclaves is then allowed by exception via contracts referred to as functional domains. Although these concepts are reasonably well established, there is further need to develop standardized approaches to the practice, based on measured efficacy and cost-effectiveness of risk reduction. Furthermore, network defense-in-depth will be challenging when applied concurrently with other security technologies (e.g. traffic obfuscation and moving target defense). Layered cryptography protections for communications and data-at-rest are similarly extant, but needing significant additional research for effective application to ICS, particularly field devices. Finally, anti-tamper protection is a key opportunity for field devices as well, and particularly apropos given their common locations away from manned spaces.	
Categorization	
Lifecycle:	Reinforced Implementation
Stage:	Protect
Defense-in-depth is a key opportunity to enhance protection against adversaries that can be added to ICS designs as reinforcement.	
Framework Mapping	
Relevant access:	A1, A2, A3, A4
Applicable procedures:	All
Defense-in-depth protects operational systems from communications and physical attacks, and attenuates opportunities for all categories of adversary procedures.	
Current Capabilities and R&D	
There has already been a significant amount of investigation into ICS defense-in-depth, particularly as it relates to network enclaves [14] and applications of cryptography [40, 41]. Other highlights: • Per [15], network segmentation involves partitioning the network into smaller networks, where the partitioning is based on factors such as management authority, uniform policy and level of trust, functional criticality, and amount of communications traffic that crosses the domain boundary. Network segmentation and segregation is one of the most effective architectural concepts that an organization can implement to protect its ICS. • Cisco, Cybersecurity for Defense: Network Segmentation: Cisco's Identity Services Engine (ISE), along with Cisco TrustSec and StealthWatch, build network segmentation directly into the network. The technology uses policy-driven segmentation based on identity to simplify the provisioning of network access, accelerate security operations, and provide consistent enforcement anywhere in the network.	
R&D Gaps	
Although defense-in-depth is important to future ICS cyber security, there is little R&D gap evident here.	

Table 3.8: Topic description, categorization, and analysis: Boundaries/Authentication

Desired State (Long-term) R&D Topic 6: Boundaries/Authentication	
Description	
ICS often requires connections between different zones of trust, e.g. vendor/integrator maintenance, coordination of smart grid revenue activities, etc. The R&D opportunity here is to develop technologies and architectures that suit these connections, but are also adaptable to other advanced security countermeasures, like moving target defense. Furthermore, ICS configuration parameters are key opportunities for attack (as discussed in P1 and A5), and so authentication access may be greatly strengthened in the long-term, perhaps leveraging multi-factor technology or one-time-use tokens (delivered out-of-band).	
Categorization	
Lifecycle:	Reinforced Implementation
Stage:	Protect
Cyber boundaries are an important protection mechanism (as well as authentication, which is also a barrier to adversaries) that can be applied after the design stage and before deployment.	
Framework Mapping	
Relevant access:	A1, A2, A3, A4, A5
Applicable procedures:	All
Boundaries and authentication protect operational systems from adversaries, who may seek access to attack via communications (A2, A3, A4), the device itself (A1), or the authorized configuration platform (A5). Preventing this access attenuates the likelihood of success for all classes of attack procedures.	
Current Capabilities and R&D	
There are many. Highlights from major sources include:	
• Per [15], using unidirectional gateways, a demilitarized zone (DMZ) network architecture with firewalls prevents network traffic from passing directly between the corporate and ICS networks. The same reference also recommends using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts), and using a network topology with multiple layers, with the most critical communications occurring in the most secure and reliable layer. • The SANS Institute, Secure Architecture for Industrial Control Systems: increased security can be achieved by using two-factor authentication mechanisms for all access, preventing credential reuse, and thwarting password guessing attacks [42].	
R&D Gaps	
Although boundaries and authentication are important to future ICS cyber security, there not a large R&D gap.	

Table 3.9: Topic description, categorization, and analysis: Security Analytics

Desired State (Long-term) R&D Topic 7: Security Analytics	
Description	
Per a previous discussion, detection of adversary activity is an important safeguard given that cyber risk cannot be completely eliminated. An ICS has critical advantages over conventional IT, in that its range of allowed operation is relatively narrow. Therefore, cyber security monitoring that incorporates advanced analytics is a crucial R&D need that will enhance security alarms for both strong and weak indicators. This will necessarily require ICS protocol-aware sensors, that can perform deep inspection into network streams to correlate evidence of adversary activity over both the cyber and physical domains. For maximum efficacy, all possible sources of data should be included, such as platform logging, network monitoring, threat indicators, etc. One critical feature is that the analytics engine should apply varying trust for data; more vulnerable ICS devices and 3rd-party data feeds may not be valued as highly as purpose-built highly-secure point monitoring solutions. Finally, the analytics may detect evidence of adversary activity by adaptively measuring system response to perturbations, where deviations might indicate altered configurations. Ultimately, the security analytics could itself inject useful minor perturbations into the functioning cyber-physical system.	
Categorization	
Lifecycle:	Reinforced Implementation
Stage:	Detect
Security analytics is a critical detection measure, which is part of an effective reinforced implementation for an ICS.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
Monitoring through analytics can cover all access opportunities, and it is the first countermeasure in Table 3.2 that significantly affects lifecycle attacks (A6). It will help distinguish evidence of adversary procedures, to streamline and optimize reaction/recovery.	
Current Capabilities and R&D	
Representative examples include:	
• LOGIIC: this was a DHS funded project for ICS security analytics from 2006 [43]. The primary R&D focus was on the necessary sensors and correlation engine. • Oak Ridge Cyber Analytics (ORCA): applying machine-learning to network traffic to reliably discriminate known and unknown network-based attacks (zero-day network intrusion detection); mapping the distribution of textual data on a network; detecting malicious behaviors in critical infrastructure systems; alert correlation and visualization; host-based exfiltration detection [44]. • ICS-CERT Advanced Analytics Laboratory (AAL): reverse engineering malware and analyzing the available log files for attribution, forensics, and defense [45].	
R&D Gaps	
The R&D gap here is difficult to judge, as there is considerable work stretching back a decade. However, detection is a critical security service, and security analytics are progressing rapidly for IT. Therefore, targeted investment may lead to significant improvement for ICS cyber security.	

Table 3.10: Topic description, categorization, and analysis: Trusted Monitors

Desired State (Long-term) R&D Topic 8: Trusted Monitors	
Description	
Trusted monitors are a crucial foundation for security analytics, but are also an important topic for even simple monitoring schemes. The concept of a trusted monitor is to add narrowly-defined incremental equipment to a system that will monitor for appropriate operation with an out-of-band approach. A trusted monitor can check critical system buses within platforms, or communications between them, for evidence of anomalous behavior which may indicate cyber attack (or other problems). To be most effective, the monitor should be simple, and leverage trusted development/implementation capabilities, in order to maximize the potential to trust the resulting security data that it generates. The expected regularity of ICS behavior is an opportunity to improve accuracy for anomaly detection. An part of a security analytics package, a trusted monitor may even perform minimal resampling for physical data to enable the analytics to detect conflicting measurements (ranging from different values for a single sampled quantity, or data for different analog quantities that are likely untrue given the physical character of the underlying system). Eventually, components will supply ready interfaces to key monitoring points, and there will be verification procedures to ensure that these present unaltered data.	
Categorization	
Lifecycle:	Reinforced Implementation
Stage:	Detect
According to the description, trusted monitors are generally considered reinforced implementation technology suitable for detection.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
Like security analytics, a trusted monitor addresses all access opportunities (including lifecycle) and procedures.	
Current Capabilities and R&D	
The concept of a reference monitor was articulated in 1972 [46] and recently instantiated for ICS under the WeaselBoard program [22] supported by SNL and the U.S. Navy. The WeaselBoard provides inspection for cyber terrain within modular ICS devices. Another effort by PFP (funded by DARPA, DOD, and DHS) monitors a device's power draw for evidence of anomalous behavior [47].	
R&D Gaps	
This is a crucial area for cyber monitoring. The opportunity space for diverse vendor equipment is very wide, and trusted monitors can potentially be built to a modular specification to ease integration into existing product lines. This gap requires participation from both R&D and industry.	

Table 3.11: Topic description, categorization, and analysis: Minimize System Impact

Desired State (Long-term) R&D Topic 9: Minimize System Impact	
Description	
To reduce the likelihood of severe impacts to underlying physical processes, R&D that cover and address the cyber/physical boundary will help. Safety systems are generally very close to the boundary, and the trend of integrating safety with other control should be examined in light of the potential risks. Furthermore, in the spirit of avoiding completely trusting ICS, careful analog or completely minimized digital controls between the ICS endpoints and the sensors and actuators for physical process under control can reduce risk. These can take to form of analog limiters or simple analog logic controls; for example, if an ICS field device can theoretically output 20V, but anything over 10V is too much for a component, then the voltage can be clamped. As another example, if safety depends on the combined temperatures of two components not exceeding a set value, they can be summed and compared using analog components. More complex safety engineering may be accomplished using very simple digital supervision (where the simplicity minimizes the potential attack surface, and maximizes opportunities for security validation). Multi-component voting schemes may also address these concerns. In every case, the goal is not to re-engineer safety controls, but to add reasonable investments in highly trusted systems that can help avoid complete catastrophe.	
Categorization	
Lifecycle:	Reinforced Implementation
Stage:	React
Measures to minimize physical impact are a part of cyber security reaction for ICS. These concepts affect design, in that they suggest a boundary between some types of controls, but this is primarily a measure to contain impacts of an untrusted ICS, so it is grouped into implementation.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
All elements for react/recovery are applicable to post-attack conditions for any access or procedure.	
Current Capabilities and R&D	
• Per Ralph Langner, every digital system has a vulnerability, and it is nearly impossible to rule out the possibility that potentially harmful vulnerabilities will not be discovered during the design and testing phase of a digital ICS product [48]. The vast majority of dangerous, remotely exploitable vulnerabilities in ICS products are not found until those systems are already deployed in the field. Analog systems may serve as a way to segment or backstop critical digital systems, creating a market for the types of technologies that critical infrastructure owners need. • Curtiss-Wright Nuclear - analog equipment provides great benefits for safety-related applications, including cyber security since an analog system is not vulnerable to cyber attack (there is no software to attack) [49].	
R&D Gaps	
There is a reasonable R&D gap here; the concept is not unheard of, but there is little information about the technical feasibility. In some cases, this is a retrofitting of minimal analog controls back into systems that had divested themselves from analog. Also, the cost/benefit is largely unknown.	

Table 3.12: Topic description, categorization, and analysis: Trusted Gold Masters

Desired State (Long-term) R&D Topic 10: Trusted Gold Masters	
Description	
The concept of restoring a system to a “golden master” version is not new; however, the application to the ICS space is immature and must overcome the unique technical challenges there. One primary issue is the difficulty of evaluating code for ICS-specific devices like protection relays and PLC. Code evaluation for normal IT is an ongoing problem, and the proliferation of computing architectures makes detection of Trojan code for ICS extremely challenging. Furthermore, system development practices are weak in the areas of secure change control for exotic ICS architectures.	
Categorization	
Lifecycle:	Reinforced Implementation
Stage:	Restore
The need to trust recovery materials is essential for restoration, and this is a security-reinforcing issue to be addressed during implementation.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
All elements for react and recovery are applicable to post-attack conditions for any access or procedure.	
Current Capabilities and R&D	
The work in this area is not extensive; and this is particularly true for ICS and APT. A key issue is understanding the software on the device, and this is complicated by the proliferation of platforms for ICS field devices. Another problem is the inability to easily refresh and reconstitute a system in a secure manner with a limited impact to continuous system operation. The application whitelisting approach in [50] may help establish trusted executables. Red Balloon is also developing a better understanding of field device firmware [51].	
R&D Gaps	
Protecting the development process (both at the vendor and for the integrator) and being able to understand the results well enough to have confidence in the “golden master” is crucial, but under-explored in ICS. This is a significant gap that will likely require collaboration across many groups of stakeholders, including government, industry, FFRDCs, and academia.	

Table 3.13: Topic description, categorization, and analysis: System Adaptation

Desired State (Long-term) R&D Topic 11: System Adaptation	
Description	
Risk analysis is a key driver for IT security management and should also affect ICS. However, configuration changes are currently orders of magnitude more difficult in ICS, making even simple patching exercises more complicated. More advanced countermeasures than patching might recommend an ICS to change its configuration while operating (like if threat information suggested an attack was imminent). R&D support is necessary in the development of needed processes and technical capabilities to evaluate potential system changes in a timely manner before deployment. Alternative ICS, possibly virtualized, will be needed as proving grounds. Further development will describe the required operational workarounds if potentially reduced ICS functionality is possible (like in the case of patching) or needed (as in the case of timely threat reactions).	
Categorization	
Lifecycle:	Deployment & Operation
Stage:	Protect
This topic describes protection improvement for operational, post-deployment systems.	
Framework Mapping	
Relevant access:	A1, A2, A3, A4, A6
Applicable procedures:	All
The conditions driving the reaction may be associated with physical, communication, or even supply chain (A6) issues (like if a patch is needed to remove Trojan code). The system adaptations may decrease an adversary's likelihood of success for any procedure, depending on the details.	
Current Capabilities and R&D	
Patching challenges, to keep up with vulnerabilities, are a known issue for ICS; this is receiving attention within the relevant communities.	
R&D Gaps	
Virtualization may have a bigger role in ICS patch/update management than is currently being used. ICS/operations adapting to threat is an opportunity. For CES, often the fallback is full manual control; the R&D would evaluate opportunities to add finer steps, which may be quite important depending on staffing levels.	

Table 3.14: Topic description, categorization, and analysis: System Assessment/Audit

Desired State (Long-term) R&D Topic 12: System Assessment/Audit	
Description	
As described under “Reinforced Implementation,” there are opportunities for R&D to develop monitoring technologies for attack detection. Auditing and assessment are important complementary efforts. There are important R&D opportunities that are unique to ICS and relevant in the long-term. Understanding the character for the controls and subsystems in a complex cyber-physical system is daunting, but will be a foundation to understanding the potential opportunities that an adversary may take to achieve their goals. Eventually, this characterization may be developed automatically (and incrementally) by observation and parsing more smaller system configuration elements. The possibilities for undesirable system operation and associated risks will need quantitative metrics, as will any analysis approaches that subdivide the scope by device, subsystem, threat, access, procedure, etc.	
Categorization	
Lifecycle:	Deployment & Operation
Stage:	Detect
This is a key reaction measure supporting the operational system.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
Improved assessment may be targeted toward any or all access or procedure.	
Current Capabilities and R&D	
cyber security assessment has transitioned from government support to a significant segment of industry, and various regulations mandate assessments/audits for ICS. Online configuration audit tools exist for IT and may be applied (after customization) to ICS.	
R&D Gaps	
The R&D gap here is to better understand the operational character of the system, as relates to cyber risk, in the context of a cyber-physical analysis. Large-scale understanding for the response of sufficiently complex hybrid systems to assess cyber risk is a significant research challenge which can be pursued by academia, FFRDCs, and other laboratories.	

Table 3.15: Topic description, categorization, and analysis: Temporary Capability

Desired State (Long-term) R&D Topic 13: Temporary Capability	
Description	
A systematic approach to implementing temporary capabilities is seemingly lacking for ICS. Therefore, effective R&D in this area would develop cross-industry solutions that allow for manual or minimal automatic controls to maintain acceptable performance for a limited but reasonable time, assuming more automated controls are temporarily untrusted or unavailable post-attack. The failover would also allow for necessary forensics and evidence collection. Ideally, the shift from full to reduced capability should be adaptive and transparent (system might use the last known good state for the primary system to streamline the transition). Virtualized, rapidly deployable failover systems may be an attractive option. In cases where temporary ICS hardware is necessary, the capability should be broad and modular (e.g. a minimally-functional set of relays for substation protection if existing electronic ones are unavailable for evidence collection).	
Categorization	
Lifecycle:	Deployment & Operation
Stage:	React
This a key reaction measure supporting the operational system.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
All elements for react and recovery are applicable to post-attack conditions for any access or procedure.	
Current Capabilities and R&D	
Per [15], graceful degradation can be described as moving from “normal operation” with full automation to “emergency operation” with operators more involved and less automation, to “manual operation” with no automation. Per [52], industry should deploy redundant systems in a security operations center to provide failover capability; maintain protected copies of critical resources; design for spare capacity and secure failover; and test failover systems to ensure proper operation.	
R&D Gaps	
Although this is fairly well specified for many industries, the actual ability to exercise temporary capability is necessarily unclear given the relative lack of full-scale drills or adverse events. As a gap, while improving temporary capability is a benefit, the technical challenges are limited. One opportunity is to leverage virtualization extensively for drills (Table 3.18), and another is to improve forensics/evidence collection capabilities to minimize their duration.	

Table 3.16: Topic description, categorization, and analysis: Secure Recovery

Desired State (Long-term) R&D Topic 14: Secure Recovery	
Description	
Restoration after cyber attack is not well explored, given the few opportunities that have been experienced. Eventually, the needed restoration will involve repairing or replacing ICS hardware, and subsequent restoration of the ICS software via golden masters. Therefore, a key challenge is safeguarding the golden masters, especially given the possibilities of tweaking or tuning the deployed system to improve performance or manage issues. The masters should remain synced to some extent with these changes, but allowing change to the golden masters opens avenues of attack, in addition to whatever attack surface they assume merely by existing. Very secure change control and monitoring is warranted, in ways that suit ICS engineers' requirement to incrementally improve the system. Another challenge is that acceptance and authorization for replacement equipment is an intensive process (not unreasonably, especially for safety equipment in a cyber-physical system). ICS operators need to be ready for rapid restoration of many devices at once, given the potential extent of a cyber attack. As an example, consider the possibility for all of the electronic relays in a critical substation to be wiped out; streamlining and accelerating the required testing would reduce the restoration interval.	
Categorization	
Lifecycle:	Deployment & Operation
Stage:	Restore
R&D in this topic area will support restoration post-deployment.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
Restoration counters the effects of all attacks.	
Current Capabilities and R&D	
In terms of current R&D, restoration is a recognized issue, although the potential extent may not be well-known. Clearly, the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is at the forefront, identifying vendor support engineers to provide technical support to the asset owner on the equipment and systems involved in an incident. Further, actions identified in a response plan must include a comprehensive response covering containment of the problem, restoration of operations to a functional state, and prevention of a reoccurrence. Finally, the group recommends establishing and running acceptance tests and procedures, automated and/or manual, to ensure that systems have been restored to the pre-incident state. [53] Ongoing security management change control for golden masters appears to be based on best practices [54], which may not be risk-informed for cyber.	
R&D Gaps	
The technical issues needed for rapid recovery and managing changes securely in ICS golden masters are opportunities for high-impact R&D that could affect restoration practice in a relatively short time frame. In this case, industry participation is critical.	

Table 3.17: Topic description, categorization, and analysis: Field Device Security

Desired State (Long-term) R&D Topic 15: Field Device Security	
Description	
Right now, field devices within ICS are a hodgepodge of modular/single-purpose components, proprietary internal/external communications, software/hardware architectures, and varying security services (some of which are ineffective as a result of poor implementations). Being the key link to physical process sensors and actuators, they are very attractive to adversaries seeking high-confidence impacts. Although some standardization may help improve the situation, it is unclear as to its likelihood for success and even its ultimate efficacy. The R&D topic here is to develop important supporting capabilities that will provide security value across diverse technologies. Virtualization for firmware analysis and simulation support is a high-return issue which is challenged by field device diversity. Firmware analysis itself is also difficult, but is probably necessary to develop needed levels of trust for these devices.	
Categorization	
Lifecycle:	N/A
Stage:	N/A
This is under “Cross-cutting Capabilities,” so the categorizations are not relevant.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
Improving trust and integrating field devices into virtualized environments improve analysis for all adversary opportunities. Firmware analysis in particular improves defense against lifecycle access (A6).	
Current Capabilities and R&D	
Field devices are often deficient in terms of cyber security, but this is improving slowly. The inertia of decades where sole focus was on reliability impedes progress. Vulnerabilities and R&D for these devices are appearing at trade shows [55] and industry (a key resource is Project Basecamp at Digital Bond [56]). There is some limited virtualization for these devices (not including unknown in-house vendor work), confined almost exclusively to x86 architectures.	
R&D Gaps	
The usefulness of virtualization (see Table 3.18) and the critical nature of field devices puts a high priority on virtualization. This will be a significant challenge given the myriad architectures, and may ultimately be adaptive to firmware images, if feasible. A strong partnership among most stakeholders, definitely including vendors, is important.	

Table 3.18: Topic description, categorization, and analysis: Virtualization

Desired State (Long-term) R&D Topic 16: Virtualization	
Description	
Current trends in information systems show that virtualization is a key enabling technology and approach to repeatable, cost-effective analysis. There are also examples of its use in cyber-physical systems, although there require some effort to model the underlying physical process, and specialized test rigs for real-time simulation and some examples of hardware-in-the-loop (HITL). Better virtualization for ICS and associated systems will support development of crucial security TTP, can help evaluate changes prior to introducing them into live systems, and provide persistent training environments (with excellent repeatability, since redeploying virtualized environments will minimize changes from one session to the next). One current hurdle to virtualization for ICS is the time and effort needed to develop the simulation environments; advances in automatically ingesting data will make virtualization more affordable. In the long run, virtualized environments may maintain accuracy by constantly incorporating live ICS data.	
Categorization	
Lifecycle:	N/A
Stage:	N/A
This is under “Cross-cutting Capabilities,” so the categorizations are not relevant.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
Virtualization is a key enabling technology to investigate many adversary opportunities. More advanced attacks, like lifecycle (A6) and management (P1) will require greater modeling accuracy.	
Current Capabilities and R&D	
Many organizations are moving toward live-virtual-constructive (LVC) approaches [57, 58] for cyber security analysis. These support repeatable and controllable experiments, as well as some persistent training environment applications (primarily on the DoD side). There is nascent work for automating the construction of the ICS LVC models.	
R&D Gaps	
Given the reasonable existing interest and capability here, the primary gaps are for automated model development (which will be a significant challenge given the cyber-physical character of an ICS) and the novel use of these environments.	

Table 3.19: Topic description, categorization, and analysis: Threat Analysis

Desired State (Long-term) R&D Topic 17: Threat Analysis	
Description	
Sharing threat information to enable response has always been a challenge. The data itself is sensitive, either because of its sources and methods or because it may reveal proprietary information. Thus, access is a matter of bureaucratically managed privileges, and dissemination carries risk. Threat discovery itself is difficult, which is a root cause for the high values for the data and the means of acquiring it. However, the risk may be warranted for high-impact systems being controlled by ICS. The goal for R&D in this space is to improve detection capabilities through automated discovery and correlation, which may include key indicators being generated by advanced ICS monitoring analytics. And to be realistic, any resulting system would minimize the potential adverse impacts of sharing data.	
Categorization	
Lifecycle:	N/A
Stage:	N/A
This is under “Cross-cutting Capabilities,” so the categorizations are not relevant.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
Threat analysis covers all access and procedures.	
Current Capabilities and R&D	
The possibility of information sharing via communities of interest is the primary approach in use currently, and has been extended to ICS for critical infrastructure. However, its efficacy is questionable, and there are no ready obvious alternatives. Other approaches leverage analytics for threat discovery (as opposed to system/device monitoring, as in topic 7): • IBM i2 Enterprise Insight Analysis: helps analysts and investigators quickly derive hidden connections and patterns buried in enterprise, third party, and public data sets to understand their threatscapes [59]. • Splunk for Cyber Threat Analysis: supports analysis of very large datasets through data indexing and MapReduce functionality; collects data from virtually any available data source without normalization [60].	
R&D Gaps	
This topic is another example of an issue having significant IT-side work that may be ripe for application to the ICS space, particularly for automated threat discovery.	

Table 3.20: Topic description, categorization, and analysis: Policy/Personnel

Desired State (Long-term) R&D Topic 18: Policy/Personnel	
Description	
There are several R&D opportunities here. The proliferation of requirements by law and policy may make ICS development difficult, and it is not unreasonable to imagine that some poorly-considered requirements may tend to increase risk rather than reduce. Furthermore, two or more well-intentioned requirements may conflict, with the overall result being reduced security. Also, the secure ICS systems of the future will depend in part on technology, but also on the TTP and training for personnel to manage and execute on protecting, detecting, reacting, and restoring. Although these are softer requirements than many others previously described, they are still opportunities for improvement that can be addressed by focused R&D.	
Categorization	
Lifecycle:	N/A
Stage:	N/A
This is under “Cross-cutting Capabilities,” so the categorizations are not relevant.	
Framework Mapping	
Relevant access:	All
Applicable procedures:	All
While individual development in requirements, TTPs, and training may address subsets of access or procedures, the overall aim is improving security for all possibilities.	
Current Capabilities and R&D	
The proliferation of bureaucracy in all walks of life is an ongoing challenge. Although it is not unique to ICS, it will become a key issue as cyber security guidance specific to ICS is developed. There is interesting R&D (e.g. [61, 62, 63]) in policy understanding and deconfliction which can be applied to ongoing ICS work. As for training, lessons learned from numerous DoD energy experiences show that complex systems can lead to more mis-operation.	
R&D Gaps	
This is a crucial issue for long-term ICS security and resiliency. However, the problem extends well beyond ICS, and so it is less suitable for ICS R&D investment, except possibly in the area of training which leverages virtualization (Topic 16) and temporary degraded operation (Topic 13, specifically for complex cyber-physical systems).	

3.6 Long-term R&D Summary

This section of the gap analysis document described the desired end state for long-term ICS cyber security in terms of its constituent technical capabilities. The desired state was summarized into 18 topics which fit into the lifecycle (secure design, reinforced implementation, deployment and operation) and security stages (protect, detect, react, recover), as shown in Table 3.1 (short version) and Table 3.2 (complete version). The cyber security framework in Section 3.2 and background summarized in Chapter 2 were used to develop the desired state, in addition to numerous other references, considerable topical experience, and discussions with outside contributors.

The 18 security topics were described in depth, and compared to existing capabilities and research, in Tables 3.3 through 3.20. Each of those tables also included commentary discussing the importance, characteristics, and specific considerations regarding the needed makeup for R&D groups to address the topic. These indicators will be summarized in the conclusions section, which follows immediately.

Chapter 4

Conclusions

The purpose of this report is to communicate the findings of a gap analysis study performed by Sandia National Laboratories. This study was performed on behalf of the Department of Energy and is intended to serve as a gap analysis for efforts in the area of long-term ICS cyber security for CES. The final results and recommendations are prioritized to optimize R&D investment. Table 4.1 presents results in decreasing order of precedence.

SNL derived the long-term R&D results by comparing existing R&D and capabilities to a set of critical technical characteristics (referred to as *topics*) for a hypothetical highly-secure future ICS system. The cyber security topics ultimately numbered eighteen, and were organized by lifecycle (secure design, reinforced implementation, deployment and operation) and security stages (protect, detect, react, recover), to best show how they complement each other.

Each topic included a discussion of the associated R&D gap. The gap was primarily characterized in terms of its extent (how near or far existing work was from what is needed). Where feasible, there was additional commentary on the opportunities (e.g. likelihood for usable results in a reasonable time frame), and whether there was a particular affinity for certain kinds of R&D support (e.g. vendor participation being crucial to success for a topic, or an academic perspective on very hard problems being needed). These results are summarized in 4.1 in decreasing order of precedence.

Topic	Specific Considerations and Recommendations	Topic ID
Trusted Monitors	• Significant gap; potentially very high impact • Concept is critical for effective ICS cyber security • Suitable for laboratory funding, transitioning to industry	8
Field Device Security	• Significant gap; field devices have many unique security issues • Critical to ICS cyber risk • Virtualization will be extremely beneficial	15
Virtualization	• Moderate gap; some existing capabilities • Opportunities for novel applications • Automated model generation would be very beneficial • Suitable for laboratory or broader funding	16
Security Analytics	• Moderate gap, with some existing work • Potentially very high impact, suitable for laboratory funding	7
Trusted Gold Masters	• Significant gap; likely very challenging • Requires broad R&D consortium	10
Moving Target Defense	• Significant gap; can leverage applicable work in IT • Initial efforts are suitable for laboratory funding	1
Protected Computing	• Significant gap, complicated by pervasive non-x86 systems • Resource consortium should include vendors	2
Obfuscation	• Significant gap • Usefulness and best approaches are unsure	4
Secure Recovery	• Moderate gap; industry participation is critical • Modest R&D challenge but potentially high-impact	14
Threat Analysis	• Moderate gap • Opportunity for automated ICS threat discovery	17
System Adaptation	• Moderate gap • Threat-aware ICS reconfiguration is an interesting opportunity	11
System Assessment/Audit	• Moderate gap; much assessment/audit capability exists • Long-term opportunity for complex hybrid system assessment • Challenging work suitable for academia or laboratories	12
Temporary Capability	• Moderate gap • Leverage virtualization to test “degraded operation”	13
Minimize System Impact	• Moderate gap • Cost/benefit is unclear	9
Policy/ Personnel	• Moderate gap, similar challenges to IT • Opportunity for virtualization-supported training	18
Defense-in-depth	• Not a significant gap • Large body of existing work	5
Boundaries/ Authentication	• Not a significant gap • Large body of existing work	6
Resilient Systems	• Significant gap; not well suited to targeted investment • Include cyber security resilience requirements in control R&D	3

Table 4.1: Long-term ICS cyber security R&D gaps, prioritized in order of importance. For additional information, refer to the relevant sections in Chapter 3. The topics are organized in Table 3.2 (also in Chapter 3).

Within Table 4.1, there is a clear group of high priority R&D topics with “significant” gaps which should be prioritized for R&D investment. (One outlier – “Virtualization” – has a gap rated as moderate but is included in the priority group based on the huge upside of successful R&D outcomes, per the discussion in the corresponding section in Chapter 4. Another outlier – “Resilient Systems” – is at the bottom of chart because it is more of control design question rather than a cyber security topic, as the concept was framed earlier.) The prioritized R&D gaps are summarized in Table 4.2, with specific information about their applicability to DOE investments. For each topic in the group, there is also a column for the expected role that DOE laboratories can support during initial R&D.

Topic	Suitable for DOE Investment?	Initial DOE Laboratory Role
Trusted Monitors	Yes	Develop scientific principles and prototypes
Field Device Security	Yes	Work with vendors to identify and address key risks and technical issues
Virtualization	Yes	Leverage advanced technical capabilities for ICS-specific challenges
Security Analytics	Yes	Develop framework, principles, and proof-of-concept capabilities leveraging available technology
Trusted Gold Masters	Yes	Focus on fundamental challenges for trust and verification
Moving Target Defense	Yes	Determine tradeoff space and applicable approaches
Protected Computing	Yes	Work with vendors and academia
Obfuscation	Yes	Study feasibility issues and cost-benefit

Table 4.2: Priority long-term ICS R&D gaps related to DOE laboratories.

References

- [1] Office of Infrastructure Protection, “Critical Infrastructure Sectors,” October 2015. [Online]. Available: <https://www.dhs.gov/critical-infrastructure-sectors>
- [2] Department of Defense (DoD), “Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems (UFC 4-010-06),” September 2016. [Online]. Available: <https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06>
- [3] T. Williams, *The Purdue Enterprise Reference Architecture: A Technical Guide for CIM Planning and Implementation*. Instrument Society of America, 1992. [Online]. Available: <https://books.google.com/books?id=3vPzPQAACAAJ>
- [4] K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York, NY, USA: Crown Publishing Group, 2014.
- [5] J. Langill, “Defending Against the Dragonfly Cybersecurity Attacks,” December 2014. [Online]. Available: <http://info.belden.com/abcd-cyber-security-dragonfly-bc-lp>
- [6] Symantec Security Response, “Dragonfly: Cyberespionage Attacks Against Energy Suppliers v1.21,” July 2014. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
- [7] F-Secure Lab, “Havex Hunts For ICS/SCADA Systems,” June 2014. [Online]. Available: <https://www.f-secure.com/weblog/archives/00002718.html>
- [8] Industrial Control System Computer Emergency Response Team (ICS-CERT), “Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure,” February 2016. [Online]. Available: <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>
- [9] Defense Science Board, “Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,” January 2013.
- [10] “Defense in Depth: A practical strategy for achieving Information Assurance in today’s highly networked environments.” March 2010. [Online]. Available: <https://www.iad.gov/iad/library/ia-guidance/archive/defense-in-depth.cfm>
- [11] “Defense in depth (computing),” 2016. [Online]. Available: [https://en.wikipedia.org/wiki/Defense_in_depth_\(computing\)](https://en.wikipedia.org/wiki/Defense_in_depth_(computing))
- [12] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,” September 2016. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

- [13] Todd McGuiness, “Defense in Depth,” November 2001. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525>
- [14] J. Stamp, C. Veitch, J. Henry *et al.*, “Microgrid Cyber Security Reference Architecture (V2),” Sandia National Laboratories (SNL), Albuquerque, NM, Sandia Report SAND2015-9711, November 2015.
- [15] National Institute of Standards and Technology, “Special Publication (SP) 800-82r2 Guide to Industrial Control Systems (ICS) Security,” May 2015. [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>
- [16] Department of Energy (DOE) Office of Electricity Delivery & Energy Reliability (OE) Cybersecurity for Energy Delivery Systems (CEDs), “Cybersecurity for Energy Delivery Systems,” <http://energy.gov/oe/services/technology-development/cybersecurity-for-energy-delivery-systems> (accessed 28 November 2016).
- [17] Energy Sector Control Systems Working Group, “Roadmap to Achieve Energy Delivery Systems Cybersecurity,” Tech. Rep., September 2011.
- [18] TCIPG, “TCIPG: Trustworthy Cyber Infrastructure for the Power Grid,” <http://tcipg.org/> (accessed 21 November 2016).
- [19] Institute for Information Security & Privacy (IISP), “Georgia Tech Institute for Information Security & Privacy,” <http://www.iisp.gatech.edu/> (accessed 07 November 2016).
- [20] L. Liu, M. Loper *et al.*, “Machine to Machine Trust in the IoT Era,” IISP, Tech. Rep., 2016, <http://www.cc.gatech.edu/~lingliu/papers/2016/M2MTrust-AAMAS-trust2016.pdf>.
- [21] J. Everett, “Rapid Attack Detection, Isolation and Characterization Systems (RADICS),” <http://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems> (accessed 07 November 2016).
- [22] J. Mulder, M. Schwartz, M. Berg *et al.*, “WeaselBoard: Zero-Day Exploit Detection for Programmable Logic Controllers,” SNL, Albuquerque, NM, Sandia Report SAND2013-8274, October 2013.
- [23] NIST, “NIST Cybersecurity Framework,” <https://www.nist.gov/cyberframework> (accessed 07 November 2016).
- [24] ISA, “The International Society of Automation,” <https://www.isa.org/about-isa/> (accessed 07 November 2016).
- [25] DOD-CS, “The Department of Defense Cyber Strategy,” http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy (accessed 07 November 2016).
- [26] NERC-CIP, “North American Electric Reliability Corporation – Critical Infrastructure Protection,” <http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx> (accessed 07 November 2016).

- [27] DOE-OE Cybersecurity, “Department of Energy Office of Electricity Delivery & Energy Reliability – Cybersecurity,” <http://energy.gov/oe/services/cybersecurity> (accessed 07 November 2016).
- [28] Institute of Electrical and Electronics Engineers (IEEE), “IEEE Cybersecurity,” <http://cybersecurity.ieee.org/> (accessed 07 November 2016).
- [29] D. C. S. Division, “DHS Cyber Security Division,” <https://www.dhs.gov/science-and-technology/cyber-security-division> (accessed 07 November 2016).
- [30] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” February 2014.
- [31] Director, Operational Test and Evaluation (DOT&E), “Cybersecurity Test and Evaluation Guidebook,” Department of Defense (DoD), policy reference, July 2015.
- [32] C. C. Davidson, J. Dawson, P. Carsten *et al.*, “Investigating the Applicability of a Moving Target Defense for SCADA Systems,” *ICS-CSR '15 Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*, pp. 107–110, 2015.
- [33] H. Okhravi, A. Comella, E. Robinson *et al.*, “Creating a Cyber Moving Target for Critical Infrastructure Applications Using Platform Diversity,” *International Journal of Critical Infrastructure Protection*, pp. 30–39, 2012.
- [34] V. Heydari and S.-M. Yoo, “Securing Critical Infrastructure by Moving Target Defense,” *11th International Conference on Cyber Warfare and Security*, pp. 382–390, 2016.
- [35] Morphisec Ltd., “Morphisec Moving Target Defense,” <http://www.morphisec.com/how-it-works/> (accessed 16 November 2016).
- [36] M. Kylänpää and A. Rantala, “Remote Attestation for Embedded Systems,” VTT Technical Research Centre of Finland, Tech. Rep., September 2015.
- [37] Y. J. Kim, J. Lee, G. Atkinson *et al.*, “SeDAX: A Scalable, Resilient, and Secure Platform for Smart Grid Communications,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1119–1136, July 2012.
- [38] Arxan, “Arxan Obfuscation,” <https://www.arxan.com/technology/obfuscation/> (accessed 16 November 2016).
- [39] Vencore, Inc., “Vencore to Develop Advanced Cryptographic Obfuscation Techniques for DARPA,” January 2016, <http://www.vencore.com/news/2016/1/15/vencore-to-develop-advanced-cryptographic-obfuscation-techniques-for-darpa>.
- [40] C. L. Beaver, D. Gallup, W. D. NeuMann *et al.*, “Key Management for SCADA,” SNL, Albuquerque, NM, Sandia Report SAND2001-3252, March 2001.
- [41] R. Mahan, J. Burnette, J. Fluckiger *et al.*, “Secure Data Transfer Guidance for Industrial Control and SCADA Systems,” Pacific Northwest National Laboratory (PNNL), Richland, WA, PNNL Report PNNL-20776, September 2011.

- [42] L. Obregon, “Secure Architecture for Industrial Control Systems,” <https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327>, September 2015, online; accessed 16 November 2016.
- [43] Department of Homeland Security (DHS), “U.S. Department of Homeland Security, Science and Technology Directorate,” https://www.dhs.gov/sites/default/files/publications/csd-logiic-brochure_0.pdf (accessed 28 November 2016).
- [44] Oak Ridge National Laboratory (ORNL), “Oak Ridge Cyber Analytics,” http://orca.ornl.gov/Oak_Ridge_Cyber_Analytics.html (accessed 16 November 2016).
- [45] DHS ICS-CERT, “ICS-CERT Monitor,” https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Mar-Apr2016_S508C.pdf, April 2016, online; accessed 16 November 2016.
- [46] J. P. Anderson, “Computer security technology planning study,” The Mitre Corporation, Air Force Electronic Systems Division, Bedford, MA, Technical Report ESD-TR-73-51, 1972.
- [47] Power Fingerprinting Inc, “PFP Cybersecurity,” <http://pfpcyber.com> (accessed 28 November 2016).
- [48] P. Roberts, “Is Analog The Answer To Cyber Terrorism?” <https://securityledger.com/2014/03/is-analog-the-answer-to-our-digital-insecurity-dilemma/> (accessed 28 November 2016).
- [49] Curtiss-Wright Corporation, “Analog Systems,” <http://www.cwnuclear.com/brands/scientech/instruments-and-controls/analog-systems/default.aspx> (accessed 29 November 2016).
- [50] DHS ICS-CERT, “Guidelines for Application Whitelisting in Industrial Control Systems,” https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf, online; accessed 16 November 2016.
- [51] Red Balloon Security, “Project Symbiote: The First Universal Embedded Defense for all embedded devices,” https://aesop.redballoonsecurity.com/RedBalloonSecurity_AESOP.pdf (accessed 29 November 2016).
- [52] The MITRE Corporation, “Backup Strategies - Reconstituting Information is Key to Recovery,” http://www2.mitre.org/public/industry-perspective/slicksheets/backup_strategies.html (accessed 16 November 2016).
- [53] DHS ICS-CERT, “Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability,” DHS, Tech. Rep., 2009, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf.
- [54] P. Crossley, R. Løken, J. Cardenas *et al.*, “Life-time management of relay settings,” *energize*, pp. 42–43, September 2013.

- [55] M. Mimoso, "Threatpost: Schneider Electric Modicon M340 PLC Station P34 Module HMI Vulnerabilities," <http://www.digitalbond.com/tools/basecamp/> (accessed 28 November 2016).
- [56] Digital Bond, "Basecamp," <http://www.digitalbond.com/tools/basecamp/> (accessed 28 November 2016).
- [57] SNL, "SCEPTRE Demonstration on Vimeo," <https://vimeo.com/178492617> (accessed 28 November 2016).
- [58] E. J. M. Colbert and A. Kott, Eds., *Cyber-security of SCADA and Other Industrial Control Systems*. Springer, 2016. [Online]. Available: <https://books.google.com/books?id=4ZTIDAAAQBAJ>
- [59] IBM Corporation, "Cyber Threat Analysis," <http://www.ibm.com/analytics/us/en/safer-plane/cyber-threat-analysis/> (accessed 16 November 2016).
- [60] Splunk Inc., "Splunk for Cyber Threat Analysis - A Big Data Approach to Enterprise Security," https://www.splunk.com/web_assets/pdfs/secure/Splunk_for_Cyber_Threat.pdf, online; accessed 16 November 2016.
- [61] A. K. Massey, J. Eisenstein, A. I. Antón *et al.*, "Automated text mining for requirements analysis of policy documents," *2013 21st IEEE International Requirements Engineering Conference (RE)*, pp. 4–13, July 2013.
- [62] T. D. Breaux and A. Rao, "Formal Analysis of Privacy Requirements Specifications for Multi-Tier Applications," Carnegie Mellon University, Pittsburgh, PA, Tech. Rep., 2013.
- [63] E. Lupu and M. Sloman, "Conflict Analysis for Management Policies," *Proceedings of the Vth International Symposium on Integrated Network Management IM97*, May 1997.

Appendix A

Revision History

Version	Date	Time	Name	Notes
1.0	20161130	1945	All	Initial version
1.1	20170124	1150	JES	Converted to SAND format per DOE requirement
1.1.1	20170222	2041	JES	Added Table 4.2 per DOE request
2.0	20170508	1600	JEQ	Incorporated review feedback for SNL portions and split
2.1	20170523	1130	JEQ	Incorporated additional internal review feedback
3.0	20170526	1430	JEQ	Final

Appendix B

Contact Information

Name	Organization
Jason Stamp, Ph.D. <i>Project Lead</i>	Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0671 jestamp@sandia.gov
Abraham Ellis, Ph.D. <i>Project Manager</i>	Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-1033 aellis@sandia.gov
Dan Ton <i>Program Manager</i>	U.S. Department of Energy 1000 Independence Avenue SW Washington, DC 20585 dan.ton@hq.doe.gov

Report Distribution

- 1 Dan Ton
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585
- 1 MS0671 Jennifer Depoy, 5628
- 1 MS0671 William Waugaman, 5628
- 1 MS0671 Neeta Rattan, 5623
- 1 MS0671 Jason Stamp, 5623
- 1 MS0899 Technical Library (electronic copy)
- 1 MS1033 Abraham Ellis, 6112
- 1 MS1033 Jimmy Quiroz, 6112

