NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Roadmap for Measurement of Security Technology Impacts for Industrial Control Systems

Prepared by Energetics Incorporated for the
National Institute of Standards and Technology

Cover Photo credits:

http://patapsco.nist.gov/imagegallery/details.cfm?imageid=765

http://patapsco.nist.gov/imagegallery/details.cfm?imageid=1231

Shutterstock 86500699

iStock 24012273

Roadmap for Measurement of Security Technology Impacts for Industrial Control Systems

Prepared for the National Institute of Standards and Technology
by Energetics Incorporated

September 2014

PREFACE

This *Roadmap for Measurement of Security Technology Impacts for Industrial Control Systems* was prepared based on the results of a workshop hosted by the National Institute of Standards and Technology (NIST) Intelligent Systems Division (ISD) within the Engineering Laboratory. Workshop planning and execution, and preparation of this report, were conducted under the direction of Keith Stouffer, Project Manager, Cybersecurity for Smart Manufacturing Systems, for ISD. The information contained herein is based on the facilitated workshop discussion and follow-up comments by a diversity of stakeholders working in the field of industrial controls and related security systems. It represents the expert perspectives of workshop participants, but does not purport to represent the views of the entire community working in this area.

ACKNOWLEDGMENTS

This report summarizes the results of the *Measurement of Security Technology Impacts for Industrial Control Systems Workshop* held December 4-5, 2013, in Gaithersburg, Maryland. The workshop was convened by the National Institute of Standards and Technology (NIST). The presentations and discussions that took place at the workshop provide the foundation for this report. Special thanks are extended to the plenary speakers (listed below), the many expert participants (a complete list is provided in Appendix A), and white paper contributors (white papers are provided in Appendix B.)

Speakers and Panelists

Harold Booth, National Vulnerability Database, NIST
Mark Bristow, Chief, Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT)
Alvaro Cardenas, Assistant Professor of Computer Science, Erik Jonsson School of Engineering and Computer Science University of Texas at Dallas
Manimaran Govindarasu, Professor, Department of Electrical and Computer Engineering, Iowa State University
Carol Hawk, Cybersecurity for Energy Delivery Systems Program Manager, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy
Janos Sztipanovits, Professor of Electrical Engineering and Professor of Computer Engineering and Director of the Institute for Software Integrated Systems, Vanderbilt University
Dawn Tilbury, Professor, Mechanical Engineering and Professor, Electrical Engineering and Computer Science, University of Michigan
Alfonso Valdes, Managing Director, Smart Grid Technologies, University of Illinois at Urbana-Champaign
Steven Venema, Associate Technical Fellow, Cyber Security & Network Technology Engineering, Operations & Technology, The Boeing Company

White Paper Contributors

Measurement of Security Technology Performance Impacts for Industrial Control Systems:
Devu Manikantan Shila, United Technologies Research Center

Metadata Isolation and Intrusion Protection:
W. J. Miller, President, MaCT

Extending the Semantic Web to Peer-to-Peer-Like Sensor Networks Based on XMPP:
Peter Waher, Member, XMPP Standards Foundation, and ISO/IEC/IEEE P21451-1-4

Special thanks are due to the Energetics Incorporated team who provided support for workshop planning, facilitation, and preparation of the summary report. The workshop report and supporting documents can be found on the workshop website at http://www.nist.gov/el/isd/cs/roadmapwksp.cfm

Further information about this report can be obtained by contacting Keith Stouffer at keith.stouffer@nist.gov.

TABLE OF CONTENTS

1 INTRODUCTION

The vulnerability of critical infrastructure to disruption has been of increasing concern after the Stuxnet attack of 2011.[1] That event raised the possibility of cyber-attacks across the internet against the Industrial Control Systems (ICS) that operate essential power, transport, manufacturing, and other infrastructures. The risk environment is dynamic and continues to evolve rapidly, with increasing amounts of online information available and vulnerable to those with malicious intent.

The escalating volatile threat environment has brought greater attention to the need to prevent advanced attacks on industrial systems. Methods and metrics for measuring the performance impact of security technologies are needed to understand and address current limitations and enable adoption in ICS. Accomplishing this may require research and development (R&D) as well as demonstration and validation of methods in testbed environments.

Common security technologies, such as encryption and device authentication, and associated research, focus primarily on desktop and enterprise IT systems. These security technologies have not been widely applied in ICS because they have not been designed to meet the specific timing, availability, and scale requirements of ICS. These limitations are exacerbated by a threat environment that has changed dramatically with the appearance of advanced persistent attacks specifically targeting industrial systems, such as Stuxnet. Methods and metrics for measuring the performance impact of security technologies will help address these limitations and promote innovation, development, and adoption of security technologies to reduce cyber risks in ICS.

> "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cyber security. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront".
>
> *From the Executive Order, Improving Critical Infrastructure Cybersecurity, Barack Obama, February 12, 2013*

ICS security controls fall into three general categories: management controls, operational controls, and technical controls. Management control strategies include security assessment and authorization, planning, risk assessment, system and services acquisition, and programs management. Operational controls take the form of personnel security, physical and environmental protection, contingency planning, configuration management, maintenance, system and information integrity, media protection, incident response, and awareness and training. Security technology can be grouped into four broad categories: identification and authentication, access controls, audit and accountability, and system and communications protection. All aspects of security are vital to the reliability and protection of ICS.

1.1 Roadmap Development Process

The mission of the National Institute of Standards and Technology (NIST) is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in areas of national importance. A sound understanding of future technology trends and relevant standards-related issues is a key component in conducting their activities related to ICS security and other advanced manufacturing technologies. NIST programs in the area of smart manufacturing address high-priority technology growth areas for U.S. manufacturers. ICS is of particular importance.

1 David Kushner, "The Real Story of Stuxnet", IEEE Spectrum, posted February 26, 2013, accessed March 15, 2014. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

To aid in identifying the key technology and measurement challenges related to ICS security performance, NIST hosted the *Roadmap Workshop for Measurement of Security Technology Impacts for Industrial Control Systems Workshop* on December 4-5, 2013, at their Gaithersburg, MD, campus. The workshop brought together experts in manufacturing and industrial controls from across the various stakeholder groups to identify measurement science challenges and prioritize needs in this manufacturing technology area. White papers were created and submitted by workshop participants prior to the workshop to provide additional background and a starting point for discussions; these are provided in Appendix B.

Participants considered a variety of breakout topic areas, as shown below. Figure 1-1 illustrates the key questions considered during the workshop.

- Security technology performance impacts for ICS
- Security architecture performance impacts for ICS
- Modeling and simulation of security impacts for ICS performance
- Security Content Automation Protocol (SCAP) for ICS
- Security R&D needs beyond SCAP
- Testbed coordination and collaboration: opportunities for new testbeds

Figure 1-1. Questions Considered for the Roadmap Process

- What **security technology and architecture-related performance issues** are of most concern (e.g. latency, jitter, and throughput)? What security technologies create the most challenges and/or impacts? At what points in the system do they create impacts? What are the major measurement science challenges and gaps in assessing security technology and architecture performance impacts?
- What **models and tools** currently exist for simulation of security impacts on ICS performance, and what are their capabilities for security? What tools are currently under development for modeling of security impacts of ICS? Can existing models be adapted to testing/modeling of security impacts? What are the major measurement science challenges and gaps in modeling and simulation of security impacts on ICS performance?
- What are some of the limitations seen or anticipated with implementing **SCAP** for ICS? What challenges and gaps do we face with use of automated security validation protocols like SCAP? How is SCAP being implemented today in ICS?
- What **testbeds** exist today for use in testing security performance issues in ICS (architecture or technology)? What performance parameters or protocols are they testing or evaluating?
- What **additional R&D, measurement tools, or other methods** are needed to overcome the challenges and gaps for automated vulnerability and security testing? What additional IT security capabilities would you like to see extended to ICS? What industrial automation scenarios should NIST test (e.g., manufacturing and process)?

The results of workshop discussions are summarized in the following chapters, which are organized by topic.

Each breakout group used a simple voting scheme to indicate which challenges would potentially have the most impact if addressed, and those most urgent to address, to ensure resolution of the main challenges and problems. After prioritizing the challenges as high, medium, or low, several of the higher priority challenges were examined more closely to create a roadmap for R&D, standards development, testbeds, and other future efforts to enhance the performance impacts of security on ICS. The results of these in-depth deliberations can be found in the *Roadmap for Priority R&D* section of each chapter. A variety of acronyms are noted throughout the report and listed with explanations in Appendix C.

Note that the ideas presented here are a reflection of the participant expertise and not necessarily the entire ICS community or NIST. As such, they should be viewed as a snapshot of the important perspectives, and not all-inclusive.

This report provides useful information to both public and private decision-makers interested in resolving the issues of security and ICS performance and assuring more widespread use of security for these systems.

It is hoped that the national research agenda for security and ICS will incorporate the consensus-based needs and priorities established during this workshop and presented in this report. The information contained here will also provide insights for NIST as they design future testbeds and other R&D programs related to security and ICS.

2 SECURITY TECHNOLOGY PERFORMANCE IMPACTS FOR ICS

2.1 Overview

This topic focuses on the performance impacts on ICS resulting from implementation of security technologies. This includes identification of principal security-related ICS performance concerns as well as how to best prioritize security requirements within each component of the ICS network. Measurement science barriers and gaps are an important aspect, particularly as related to monitoring ICS security status, reaction to a cyber-attack, and potential impacts on ICS performance.

2.2 Security Technology-Related Impacts on ICS Performance

A number of issues can arise from the use of security technology in ICS; those identified in the workshop are outlined in Table 2-1. Issues are wide-ranging, from interoperability of systems to technology-specific problems and the ability to prioritize security needs.

TABLE 2-1: SECURITY TECHNOLOGY ISSUES

Security Strategy, Cost and Workforce Issues	Problematic Security Technologies and Related Issues Impacting ICS Performance	Security Prioritization

• High cost of total life cycle implementation and management of security technology, especially technology upgrades
• Undefined security technology management strategy, incorporating in–depth security technology understanding and roadmaps
• Undefined security technology implementation strategy including appropriate operations for IT management and user access
• Defining roles of system versus security operators, and avoiding excessive number of different alarms
• Ever growing number and diversity of potential cyber threats
• Difficulty in training the IT workforce to implement security technology
• Difficulty in training the ICS workforce to be security conscious
	• Poor interoperability of different security and ICS equipment
	• Inadequate continuous monitoring of the ICS network infrastructure integrity, including discovery, situation awareness, and profile of every asset on the network
	• Insecure communication within the ICS network infrastructure
	• Difficulty in automatically detecting vulnerabilities and misconfigurations
	• Effectively differentiating between process and security alarms
	• Inadequate automatic isolation and repair of an incident
	• Problematic integration of state-of-the-art security technology and practice (e.g., encryption for data messages) to legacy ICS equipment
	• Negative effects of security technology implementation on real-time ICS performance and control (e.g., timing and latency, SCADA management, and network interconnect)
		• Ability to mitigate security vulnerability from all aspects, specifically
		  ○ Electronics and software in existing ICS equipment
		  ○ New electrical and software components incorporated into the ICS as part of an update
		  ○ Electrical component and software in current supply chain

2.2.1 Security Strategy, Cost, and Workforce Issues

System cost, workforce training, and management and implementation strategy are some of the main technology-agnostic concerns related to the impacts of security systems on ICS performance.

The long-term, total cost of ownership (TCO) in security technology implementation is a major cost issue. Specifically, the operational and maintenance cost of security technology can escalate as regular

updates and refreshes are needed. Furthermore, multiple sources of security technology (e.g., commercial, government) can increase the complexity and therefore the cost of interoperability, operations, and maintenance. This concern is further elevated considering that a comprehensive security solution is usually an integration of multiple security technologies rather than a single technology.

Training the appropriate workforce is another cost-related concern. A trained information technology (IT) workforce is needed to operate and maintain the security technology in the industrial environment. The existing and future ICS workforce will need to be trained to be security conscious as they operate these systems integrated with security platforms.

ICS consoles will display process alarms, but the security technology will display security alarms. The roles of system operator versus security operator need to be defined, and implementation must not overwhelm the system operator with alarms. This is a technology impact as well as a workforce issue.

The effectiveness of the implementation and the management strategy for security technology will also affect the performance impacts on ICS. While minimizing overhead costs, the strategy must assure that the security technology provides the proper cyber protection to the ICS without compromising system performance.

2.2.2 Problematic Security Technologies and Related Issues Impacting ICS Performance

The interplay between ICS performance (e.g., timing, latency) and the implementation and integration of security technology is a major performance issue. Negative impacts (e.g., jitter, timing lags) on process, production, and quality control systems can have significant and costly outcomes.

A spectrum of technologies often work together to protect an ICS network from a cyber-attack. Key technologies are those related to continuous monitoring of the ICS network infrastructure integrity, including discovery, situation awareness, and profile of every asset on the entire network. Continuous monitoring technologies enable automatic detection of vulnerabilities and misconfigurations, which trigger automatic isolation and repair of an incident. Encryption and securing all components individually provides further fortification of the entire ICS network. Secure communication must be the common practice throughout the ICS network, as well as in external networks communicating with it. Performance issues can arise when any of these points are compromised.

Monitoring detects vulnerabilities and misconfigurations, but also detects incidents in real time. Vulnerability monitoring can be done as part of the maintenance cycle, and ideally not on a running production system. For some time-critical operations (e.g., protection in electrical systems), encryption introduces unacceptable time impact—even with current equipment.

Equally important are appropriate methods to protect legacy ICS equipment from cyber-attack. Incompatibility between legacy ICS equipment and current security technology can cause problems. Additionally, security vulnerabilities are inherent in legacy ICS equipment since they were designed with minimal or no cybersecurity requirements in mind.

2.2.3 Security Prioritization

In current practice, ambiguities exist as to how and where to prioritize security technology implementation. Overall perspectives are that security needs to be a priority throughout the ICS network and that no singular location should be the focus of security technology implementation. Instead, the approach must be comprehensive, including incorporating electronics and software components in legacy equipment, ICS updates, and the current supply chain. A cyber-attack can originate from multiple sources, requiring a comprehensive strategy to protect ICS.

In addition to a comprehensive strategy for prioritization, common terminology and encryption methodologies are needed for security communication among all components of ICS.

2.3 Security Technology Challenges and Gaps

TABLE 2-2: MAJOR CHALLENGES AND GAPS IN SECURITY TECHNOLOGY FOR ICS

- Inability to continuously monitor and catalog ICS network infrastructure, including discovery and profiling of every asset on the entire network for situation awareness
- Inability to continuously monitor and catalog new cybersecurity threats
- Undefined common terminology and key performance metrics
- Inadequate risk benefit analysis / business case for implementing security technology on ICS
- Vulnerability inherent in ICS software
- Lack of risk management approach to ICS cybersecurity
- Protecting national security and proprietary data
- Confirming data integrity
- Inadequate modeling and simulation of cyber-attacks, including impact on ICS processes
- Immature measurement capabilities for monitoring ICS security
- Insufficient security analytics to transform security data to system integrity and provide performance information
- Undeveloped user dashboard with visibility to system health and actionable information

The major challenges and gaps identified at the workshop are presented in Table 2-2. The inability to continuously measure all equipment and software within the ICS network is a significant problem. With continuous measurement, "normal" baseline situational awareness can be established so that unusual behaviors caused by a cyber-attack can be detected. Similarly, building the capacity to continuously monitor and catalog new cybersecurity threats would facilitate rapid cyber-attack detection across the ICS sector, as well as enhance attack prediction capabilities. Modeling and simulation of cyber-attacks and their impact on ICS processes must be improved to provide baseline understanding of the ICS. This increased understanding will drive development of new measurement capabilities to monitor ICS hardware and software integrity.

In some cases, monitoring of ICS security suggests that metrics exist, so that "acceptable" and "not acceptable" states can be quantified. This is not true in all cases. For example, an Intrusion Detection System (IDS) does not imply that a detection metric exists for all attacks. A common set of performance metrics will be essential to defining the security of an ICS in a consistent way. Similarly, producing a common language for the disparate terminology for security technology across industries and suppliers is a challenge but essential.

Given the potential combined complexity of the cyber threats and security technology implementation, a well-defined cost and benefit analysis methodology would aid in articulating the business case for adoption of ICS security technology. Often, justification is needed for the added cost of secure software development techniques to minimize security risk from vulnerable software, and to address the challenges of integrating state-of-the-art security technology into existing ICS.

Improved algorithms and analytics will be needed to translate security data into system integrity and performance information. Clear visualization of these analytics though a user-friendly display is necessary to communicate situation awareness and actionable information during a cyber-attack.

2.4 Roadmap for Priority R&D

Two areas are identified as a high priority for R&D to improve understanding and measurement of the impacts of security technologies on ICS. These are outlined below and discussed in more depth in Figures 2-1 and 2-2.

- **Figure 2-1: Big Data Analytics for ICS** – Large amounts of data can be collected from ICS, and there is a strong need to connect this data with security aspects to understand the potential impacts on controls performance. To support data analytics, this activity would develop common, consistent methods that can be used across the board for analysis of massive data sets streaming in real time from control systems. This includes measurement and data collection approaches, a data sharing framework, data storage and access, and ICS security analytics.

- **Figure 2-2: Technologies for Human Proofing** – Human factors play a large role in the proper use and performance of security systems. This activity will develop solutions and policies to detect, correct, and prevent policy violations. Research for usable security is also needed. Awareness and compliance are a good approach, but if security makes the job too difficult (e.g., strong, frequently changed passwords) users may look for workarounds. Creating effective solutions will help maximize user or operator awareness of security issues and foster greater compliance with security policies and procedures.

FIGURE 2-1: BIG DATA ANALYTICS FOR CONTROL SYSTEMS

Barriers: Lack of total situation awareness across the ICS; user dashboards do not provide adequate system health visibility and actionable information; nonexistent common data sharing framework.

Approach Summary: Develop measurement and data collection approach; develop common data sharing frameworks, data storage and access; develop ICS security analytics, including multi-source data analysis and display; develop an ICS testbed for demonstration of analytics.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Define standard ontologies and performance metrics • Improve instrumentation and data collection • Delineate domain specific data analytics • Develop ICS security analytics architecture	• Ontologies and related standards published • Concepts demonstrated via models and simulations • ICS security analytics design drafted	• Improve total situation awareness • Develop detailed risk analysis and management procedures • Integrate ICS security status and performance views • Identify the appropriate security technology architecture to achieve cyber resilience
3-5 years	• Develop ICS analytics testbeds using approach security technology architecture • Refine security technology / data analytics evaluation methodologies • Develop prototype ICS security analytics architecture	• Testbeds instrumented • Evaluation methodologies validated • ICS security analytics architecture demonstrated with industry partners • Standard ontologies and performance metrics validated	
5+ years	• Field test and demonstrate ICS security analytics architecture	• ICS security analytics accepted by industry	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users** Produce data; define use cases; perform limited testing / demonstration
- **Industry/ Control System Providers:** Develop ICS and measurement instrumentation
- **IT Community:** Create data collection infrastructure and tools
- **Academia:** Resolve algorithms; develop testbeds
- **SDOs/Standards Committees:** Publish standards and metadata
- **Government:** Develop policies; provide funding; resolve algorithms; develop testbeds; form public and private partnerships

RELATIVE IMPACTS

LOW —HIGH POTENTIAL

- ♦♦♦ **Improves system performance:** Measures and improves analytics
- ♦♦♦ **Reduces costs of security:** Facilitates data collection for decisions from accumulated experience
- ♦♦♦ **Improves security / resilience:** Detects issues and reconfigures system appropriately
- ♦♦♦ **Enhances industry competitiveness:** Total situation awareness increases competitiveness
- ♦♦♦ **Reduces time/ complexity of security validation:** Automated forensic methods reduce time required and complexity

FIGURE 2-2: TECHNOLOGIES FOR HUMAN PROOFING

Barrier: Maximizing user awareness and ensuring compliance with secure policies and procedures.

Approach Summary: Develop solutions and policies to detect, correct, and prevent policy violations; conduct research to establish usable security methods.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Conduct risk assessment of policy violations and their associated consequences • Develop risk mitigating / containment approaches and policies • Coordinate with security architecture design	• Risk management framework developed • Prioritized list of policy violations to circumvent created	• Maintain system uptime and product quality
3-5 years	• Simulate impact of ICS performance resulting from policy violation • Identify method to isolate security breaches • Research usable security methods • Develop predictive analytics to mitigate potential future policies violations • Test and validate with current security architecture	• Technology solutions that detect, correct, and prevent policy violations are developed • Usable security solutions that avoid user workarounds are developed	
5+ years	• Perform limited field demonstration of predictive analytics to mitigate potential future policies violation	• Future accidental and malicious policy violations are prevented	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Produce data; define use cases; perform limited testing / demonstration
- **Industry/ Control System Providers:** Provide ICS equipment
- **IT Community:** Develop security architecture, policies, and technology
- **Academia:** Develop security tools and technology
- **SDOs/Standards Committees:** Publish standards; perform testing
- **Government:** Regulate security architecture, policies, and technology; manage projects; collect data

RELATIVE IMPACTS

LOW —HIGH POTENTIAL

- ♦♦♦ **Improves system performance:** Improves overall consistency of security
- ♦♦♦ **Reduces costs of security:** Establishes risk mitigation framework
- ♦♦♦ **Improves security / resilience:** Establishes preventative measures for policy violations
- ♦ **Enhances industry competitiveness:** Minimizes ICS security risk
- ♦♦♦ **Reduces time/ complexity of security validation:** Prevents workarounds with more usable solutions

3 SECURITY ARCHITECTURE AND ICS PERFORMANCE

3.1 Overview

Security architectures are critically important to the performance of ICS. Poor security architecture can make it difficult or impossible to properly secure a distributed control or SCADA system and maintain performance. Architectures must work with the control system local area networks (LANs), wide area networks (WANs), servers, workstations and field devices, and integrate with existing infrastructure, systems, and policies. Architecture components can encompass network interfaces (ICS, enterprise and other non-ICS networks), underlying network components, tools for redundancy and recovery, network and security management, and a host of other elements.

3.2 Security Architecture-Related Impacts on ICS Performance

Security architecture and design can give rise to a number of issues that ultimately affect the performance of ICS. Security architecture-related performance problems can occur at the interface of ICS networks with outside networks as the result of inadequate real-time communications between control zones. The main issues identified by workshop participants are shown in Table 3-1.

TABLE 3-1: SECURITY ARCHITECTURE ISSUES

Most Concerning Security Architecture-Related Performance Issues	Security Architectures Producing Greatest Impacts on ICS Performance

• Interface of ICS network with corporate network/outside network
• Enforcement of a minimal privilege principle to isolate identified information flows and provide security properties (e.g., integrity protection) for devices and/or systems, i.e., an entity (user, device, software module, etc.) should have no more privilege than is required to accomplish a legitimately assigned task
• Increased complexity of controllers (e.g., distribution, encryption, certifications, autonomous response)
• Necessity of providing protection for device and providing enumeration of device statistics
• Ensuring that the system architecture continues to implement best practices in a dynamic environment
• Real-time communications between control zones
• Determining security impact on control system performance
• Reliability of networks
• Common user authentication across multiple control systems in the same plant
• System designed to track infections and report similar issues or vulnerabilities in real-time
	• Secure remote maintenance of systems (e.g., firmware updates) when possible
	• Encryption of ICS protocols
	• Legacy systems and architectures
	• PLC subnet real-time control circuits
	• Monitoring SCADA/PLC for ICS
	  ○ External to unit
	  ○ Built-into unit
	• Architectures that have not included business risk, cybersecurity risk, and threat vector analysis into a mission impact analysis
	• Architectures producing performance issues such as delay, jitter, throughput, packet loss, or bit error rate
	• Adding security functions/protocols into a class of endpoint devices not traditionally designed to handle crypto/decrypto, real-time analysis, logging of activity over extended periods, etc.
	• Convergence of critical ICS traffic into multipurpose/untrusted networks which have minimal performance guarantees
	• Critical command verification and authorization checks
	• Complexity, reliability, and observability of the system arising from integration
	• Domain-specific issues, such as architectures in manufacturing focused mainly on throughput, or those in defense focused mainly on data and product integrity
	• Architecture without sufficient rights management (where needed) and policy enforcement
	• Architecture causing host-based security performance impacts
	• Security architectures that place bulk of responsibility on the controlling device
	• Architecture for co-existence of wireless protocols

Security architectures that do not account for business risk, cybersecurity risk, and threat vector analysis in the mission impact analysis can produce considerable impacts on performance. The result can be an architecture that potentially addresses the wrong problem.

Potential performance issues also arise from the convergence of critical ICS traffic into multi-purpose, untrusted networks, as well as from adding security functions and protocols into a class of endpoint devices not traditionally designed to handle encryption and decryption, real-time analysis, and logging of activity over extended periods. Performance issues could include delays, packet loss, and bit error rates. Architecture design must also be domain-specific. For example, defense customers may be most concerned with data integrity, while manufacturers pay more attention to throughput.

3.3 Security Architecture-Related Challenges and Gaps

3.3.1 Security Architecture Challenges and Gaps

Table 3-2 illustrates the list of challenges and gaps identified for security architecture as it applies to ICS. Challenges are categorized into the major areas of accuracy, security definitions, metrics, economics, performance, authentication, and tools and models.

The need for metrics is a major gap in assessing security architecture performance impacts. Specifically, there is a need for metrics for evaluating the security performance of degraded systems and static as well as dynamic security (when appropriate). These metrics should enable prediction of security indices.

The economics of ICS security is an important challenge. Formulas, with quantified constants and variables, should be explored to aid in calculating the return on investment (ROI) of ICS security investments and better demonstrate their value.

ICS security is not uniformly defined and it is especially challenging to quantify it. Addressing this challenge would require: (1) surveying existing ICS cybersecurity definitions and quantification techniques; (2) developing equations or models that incorporate performance; (3) surveying end user/practitioner cybersecurity experiments with numeric models for quantification; (4) publishing an ICS cybersecurity definition and recommendations for ICS cybersecurity quantification; and (5) adopting methods for ICS cybersecurity quantification that are well understood, consistent, and relevant to end users.

Understanding how ICS component characteristics compare feature for feature, when combined with other devices in an ICS network, is another key challenge. One approach to address this involves mapping devices to security functions as they apply to defense in depth architecture. The desired goal is the ability to apply tailored ICS security controls using certified devices with predictable results.

TABLE 3-2: SIGNIFICANT CHALLENGES AND GAPS IN SECURITY ARCHITECTURE

Accuracy

- Inaccurate modeling and simulation derived from an architecture
- Ability to pull metrics from a model/system
- Complications using SysML in ICS system modeling
- Misunderstood human/operator inputs
  - Action/reaction
  - Intention
  - Impact/outputs
- Difficulty measuring architecture and network anomalies

Defining Security

- Inability to quantify "security" (associated with ICS security definition)
- Poorly understood relationships between security components with respect to security performance, which is not clearly defined
- Unclear definition of a secure system and metrics of success
- Inability to quantify uncertainty in measurement science
- Defining domains/requirements of secured systems/components

Metrics

- Inability to measure security performance of degraded systems
- Inadequate static and dynamic security metrics
- Common classifier measures (i.e., intrusion detection evaluation) that do not map to end user issues
- Undeveloped quantification methods for end user performance
- Lack of techniques to down-select to optimal security methods
  - Metrics
  - Tools
  - Analytical models for comparison of techniques for various hardware architectures
- No useful scale for security performance
- Inadequate threat capability and intent metrics
- Difficulty measuring statistics for combined systems as opposed to individual devices
- Delay in latency/timing across the ICS WAN after security controls are applied

Performance

- Difficulty ensuring resiliency
- Longevity of security architecture (e.g., remaining secure for 20+ years in the face of increasing and unknown threats while providing sufficient performance)
- Assessment of impacts and cascading effects
- Difficulty measuring how security is affected in a degraded system

Authentication

- Human factors and authenticating sessions
- Data authenticity, from field devices to HMI

Economics

- Difficulty measuring return on investment of security
- High cost of enumeration, not just data communication

Tools, Models, Processes

- Inability to compare feature for feature in-depth defense versus one-layer defense
- Undefined security measurement methodology
- Non-standardized security measurement and testing methods for wireless networks
- Inaccurate security-related metrics time stamp
- Ability to know if ICS system partitions exist and if template architectures can be defined
- Non-standardized stack-trace functionality in end devices to allow benchmarking impacts of added security features/protocols (the embedded operating system problem)

3.3.2 Gaps in Testing of Security Protocols

A number of protocols should be tested to enable better design and adoption of security architectures integrated with ICS. Those identified as important in various key categories (Internet, wireless, authentication, tele-controls) are listed in Table 3-3. These are intended to be representative, not all-inclusive.

TABLE 3-3. ARCHITECTURE ELEMENTS REQUIRING TESTING OF SECURITY PROTOCOLS

Internet Protocols	Wireless Communications
• Ethernet/IP • Protocols used between zones across 'conduits' (e.g., OPC, Modbus/TCP) • EtherCAT for robotics • TLS/SSL • IPSEC with IKE • L2TP • SCEP/OCSP • Radius/LDAP/TACACS • Protocols prescribed by IEC 62351 and associated configurations • SNMP • BACnet security • VPN • IPUG from an ICS perspective • MT Connect	• WiFi • WirelessHART • Zigbee • 6LoWPAN • Bluetooth • ISA 100.11a • Secure use of mobile technologies when interfacing with ICS network devices • BYOD • Comparison of integrity providing protocols based on shared keys (SHA) which are generally more efficient versus public key (SSH) which have easier key deployment • Incorporation of spread spectrum into new system designs
	Authentication and Tele-Controls
	• DNP3 with SAv5, Modbus, IEC 60870-5, IEC 61850 GOOSE/MMS, ICCP

3.4 Roadmap for Priority R&D

Five areas are identified as a high priority for R&D to improve understanding and measurement of the impacts of security architectures on ICS performance. These are outlined below and discussed in more depth in Figures 3-1 to 3-5.

- **Figure 3-1: Static and Dynamic Security Metrics** – There is a need to capture the static as well as the dynamic nature of system architecture, or time dependencies. This activity will focus on identifying frameworks for capturing and predicting system security indices and system dynamics and uncertainties. The objective is to develop underlying foundations for metrics for security architecture impacts on performance.

- **Figure 3-2: Measurement of Security Performance of Degraded Systems** – It is currently difficult to measure the security performance of degraded systems as compared to nominally operating systems. To address this challenge, an approach is proposed for measuring and comparing the security performance of systems in a nominal mode with all, or a subset of the modes that have been degraded. This will enhance the ability of real and modeled systems to detect/respond to attacks in real time.

- **Figure 3-3: Feature for Feature Component Comparison** – Currently, there is limited ability for feature for feature comparison of ICS component characteristics when the devices

are combined in an ICS network. The suggest approach is to develop the ability to map devices to security functions as they apply to defense in depth architecture (e.g., ISA99). Achieving this will make it possible to apply tailored ICS security controls using certified devices, with more predictable results, including impacts on performance.

- **Figure 3-4: Quantification of Security** – ICS security is inconsistently defined and quantified in today's industrial environment for a number of reasons. To some extent this is because the level of security now required is much greater than it was when some of these systems were designed, developed, and installed. Since security quantification is a relatively new requirement, the relevant methods are still highly uncertain. A suggested approach to address this is to develop security quantification methods through surveying, modeling, experimenting, publication of results, and ultimately practical demonstration and adoption in industrial environments.

- **Figure 3-5: Return on Investment for ICS Security Systems** – The formulas (with quantified constants and variables) for parameters expressing ROI in use today that can be applied to security systems for ICS are inadequate. Conceptual models to quantify—or "operationalize"—key terms in the ROI formula are currently undefined. To address this challenge, one approach is to assume an accepted definition of security with respect to ICS, decompose major terms into quantifiable/measurable parameters, create test cases, and then refine them for real-world applications.

FIGURE 3-1: STATIC AND DYNAMIC SECURITY METRICS

Barriers: Inadequate metrics to capture static and dynamic (i.e., time dependent) security performance relative to the nature of the system architecture; undefined boundaries to accurately capture dynamic nature of system and predict security indices.

Approach Summary: Identify the right mathematical framework for capturing these indices; capture system dynamics, uncertainties, and qualifications.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Investigate the attributable performances of the system (system of systems) • Identify the relationship between attributes and security techniques • Investigate/quantify system dynamics (e.g., uncertainties such as rare events)	• Relationship of significant attributes to security techniques defined • Time dependent nature of system security captured • Class of models to capture system dynamics, uncertainties, and security are developed	• Guidance to design secure and resilient systems that will work well / remain relevant for a specified number of years
3-5 years	• Develop a mathematical model that will aid in capturing static and dynamic nature of security metrics	• Reliable mathematical framework available	
5+ years	• Refine metrics as systems develop	• Updated metrics prepared	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Develop/test metrics
- **Industry/ Control System Providers:** Test metrics
- **IT Community:** Contribute to guidance as appropriate
- **Academia:** Develop models and metrics
- **SDOs/Standards Committees:** Develop and test metrics and frameworks
- **Government:** Contribute to testing and frameworks (DOC, Army, DOD)

RELATIVE IMPACTS

LOW —HIGH POTENTIAL

- ♦♦♦ **Improves system performance:** Capture all dynamics and security issues
- ♦♦♦ **Reduces costs of security:** Design of secure system guidance that is relevant for years reduces development costs
- ♦♦♦ **Improves security / resilience:** Supports better security performance
- ♦♦♦ **Enhances industry competitiveness:** Indirect competitiveness increase
- ♦♦♦ **Reduces time/ complexity of security validation:** N/A

FIGURE 3-2: MEASUREMENT OF SECURITY PERFORMANCE OF DEGRADED SYSTEMS

Barrier: Inability to measure security performance of degraded systems as compared to nominally operating systems.

Approach Summary: Measure and compare security performance of systems in nominal mode with all or a subset of the modes degraded.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Develop security metrics • Identify degraded states to be tested for every system/component	• Well-defined metrics and tests are available • Methodology for identifying degraded states (e.g., cause and effect diagrams, etc.) in use	• Ability of real and modeled system to detect/respond to attacks in real time • Ability to compare component upgrades and replacements
3-5 years	• Build models for previously identified nominal states and degraded states • Integrate capability for each layer or component	• Model framework to test security performance developed	
5+ years	• Develop inter-component communication • Develop system-level ability to monitor states and measure security	• Ability to detect degraded state (attack or failure) in real time made possible	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Identify and supply use cases
- **Industry/ Control System Providers:** Implement framework; define component security parameters
- **IT Community:** Supply knowledge/tools
- **Academia:** Develop and test definitions of degraded component states
- **SDOs/Standards Committees:** Identify testable security metrics; create framework
- **Government:** Engage stakeholders; drive impetus for solutions; supply testbeds and research funding

RELATIVE IMPACTS

LOW —HIGH POTENTIAL

- ♦♦♦ **Improves system performance:** Increased system uptime and reliability
- ♦ **Reduces costs of security:** Reduces cost impacts of adding security
- ♦♦♦ **Improves security / resilience:** Supports system performance design
- ♦♦ **Enhances industry competitiveness:** Provides metrics for comparison

FIGURE 3-3: FEATURE-FOR-FEATURE COMPONENT COMPARISON

Barrier: Lack of capability for feature-for-feature comparison of ICS component characteristics when the devices are combined in an ICS network.

Approach Summary: Map devices to security functions as they apply to defense of in-depth architecture (e.g., ISA99).

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Define a catalogue of security functions applicable to ICS • Develop criteria for determining effectiveness for each security function • Develop formula that relates effectiveness to security impact	• Catalogue with definitions for vendors to develop security devices is available	• Ability to apply tailored ICS security controls, using certified devices, with predictable results
3-5 years	• Test and certify devices that allow selection of security controls • For each device, map latency for each security feature to its effectiveness	• Devices to deploy in the field that can be properly integrated with optimal security/latency tradeoffs are certified	
5+ years	• Update devices to meet latest security threats	• New devices that keep pace with new security issues as they are discovered are available	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Identify security most desirable functions
- **Industry/ Control System Providers:** Implement, test, and certify devices with functions
- **IT Community:** Support research, development, and testing of multi-function security devices
- **Academia:** Convert R&D into multi-function security devices/methods
- **SDOs/Standards Committees:** Implement security functions/devices that work into standards
- **Government:** Support standards development

RELATIVE IMPACTS

LOW —HIGH POTENTIAL

- ♦ **Improves system performance:** Provides combined system perspective
- ♦♦ **Reduces costs of security:** Possible reduction —multi-function security devices may be less costly than specific devices
- ♦♦♦ **Improves security / resilience:** Multi-function security devices are designed to improve security
- ♦♦ **Enhances industry competitiveness:** Multi-function security devices may improve competitiveness through standardization
- ♦♦ **Reduces time/ complexity of security validation:** Checking multi-function security device settings validates security level

FIGURE 3-4: QUANTIFICATION OF SECURITY

Barrier: Inconsistent definition of ICS cyber-security; uncertain security quantification methods.

Approach Summary: Develop security quantification through surveying, modeling, experimenting, publishing, and adoption phases.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Survey existing definitions of ICS security • Create definition ontology • Survey ICS security quantification techniques	• ICS cybersecurity definition published • Section for 800-82/NISTIR 7628 drafted	• Means of ICS cybersecurity quantification that is well understood, consistent, and relevant to end users. • Incorporation of ICS-CERT data • Apply means to CERT evaluations
3-5 years	• Survey end user/practitioner cybersecurity issues • Perform experiments with numeric models for quantification • Develop equations and models that incorporate performance metrics and output with well understood, consistent values relevant to end users	• Recommendations for ICS cybersecurity quantification published • Mapping to reference architectures published	
5+ years	• Solicit feedback and revise definitions	• NIST publications receive feedback and are revised	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Serve as the voice of the customer
- **Industry/ Control System Providers:** Serve as the voice of the customer; collaborate in experiments
- **IT Community:** Serve as historical subject matter experts, and provide lessons learned
- **Academia:** Develop models; provide resource support
- **SDOs/Standards Committees:** Map research results to standards
- **Government:** Champion efforts and adoption; incorporate government information into development activities

RELATIVE IMPACTS

LOW —HIGH POTENTIAL

- ♦♦♦ **Improves system performance:** Facilitates system tuning and performance
- ♦♦♦ **Reduces costs of security:** Optimizes cost relative to perceived risk
- ♦♦♦ **Improves security / resilience:** Better decisions lead to a more relevant system
- ♦♦ **Enhances industry competitiveness:** N/A
- ♦♦♦ **Reduces time/ complexity of security validation:** Provides more consistent measurements

FIGURE 3-5: RETURN ON INVESTMENT for ICS Security Systems

Barrier: Inadequate formulas (with quantified constants and variables) for parameters expressing ROI; undefined conceptual models to quantify, or 'operationalize' key terms in the ROI formula.

Approach Summary: Assuming an accepted definition of security with respect to ICS; decompose major terms until quantifiable/measurable parameters and relationships are delineated; then search for unknown issues.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Research existing ROI and risk management literature • Conduct consensus-building workshops • Create and test prototype models/simulations	• Useful approaches and clarity on gaps for model development are developed • Accepted formula for testing in place	• Implemented ROI model • Industry accepted validation scheme for ID, liability, lost opportunities
3-5 years	• Refine models	• Formal methods for ROI established	
5+ years	• Refine models	• Methods are adjusted as technology emerges	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Provide data
- **Industry/ Control System Providers:** Provide data
- **IT Community:** Understand and impart lessons learned as a testbed provider; provide technology risk information and expertise
- **Academia:** Perform literature search of taxonomy
- **SDOs/Standards Committees:** Perform taxonomy model testing
- **Government:** Address statutory and liability issues

RELATIVE IMPACTS

LOW —HIGH POTENTIAL

♦♦♦ **Improves system performance:** Supports cost-effective security system adoption

♦♦♦ **Other:** Enables business case for ICS security system and process investment and refinement

4 MODELING AND SIMULATION OF SECURITY AND ICS

4.1 Overview

This topic addresses the opportunities, issues, and concerns related to modeling and simulation of security technology, as well as the subsequent impacts on understanding secured ICS performance. This includes how existing and emerging models and tools could be used to enhance ICS security testing. There are also security performance challenges where new models and simulation paradigms may be required to accurately predict security impacts on ICS.

4.2 Models and Modeling Capabilities for ICS and Security Impacts

Current developers of models and tools, existing modeling and simulation capabilities, and tools under development are illustrated in Table 4-1 and further examined below. The information provided in Table 4-1 is a snapshot of what is available or emerging based on the viewpoints of the contributors to this report; it is not intended to be all-inclusive.

TABLE 4-1: EXAMPLES OF MODELING AND SIMULATION DEVELOPERS AND CAPABILITIES

Model/Tool Developers	Existing Modeling/Simulation Capabilities for ICS Security Testing	Tools under Development for Testing/Modeling of Security Impacts
• DOD SPIDERS JCTD with DOE and DHS • National Security Agency (NSA) • U.S. Navy • Federal Laboratories (e.g., NASA Ames Laboratory, Sandia National Laboratory, NIST) • Other organizations (SANS Institute, TCIPG)	• SimuLink by Mathworks • Specialized real time digital power system simulators (e.g., by RTDS Technologies) • PetriNet based network simulation software • Passive Vulnerability Scanner (Tenable) • Snort for SCADA (Sourcefire) • SCADA+ Pack (GLEG)	Security Software • Kali Linux (Offensive Security) • SOPHIA (NexDefense, in Beta Test) Network Simulation Software • OPNET Modeler Suite (OPNET) • OMNeT++ (Open Source) • NS-3 (Open Source)

4.2.1 Current Model and Tool Developers

Both models and simulations can be used to analyze and predict how security technology affects ICS performance and to develop and test solutions that improve ICS performance. A number of illustrative examples of this are ongoing.

The Department of Defense (DOD) Joint Capabilities Technology Demonstration (JCTD) program—known as Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)—developed a set of models and tools for smart grid cybersecurity. While not directly applicable to ICS, this provides provide a strong foundation of hardware and security models and simulation. In addition, other organizations such as the Navy and NSA have developed similar models and tools. Key federal laboratories, as Idaho National Laboratory and NIST, also have developed smart grid security tools, as have organizations such as the SANS Institute and the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG), university collaboration.

Note that tools such as those emerging from SPIDERS have been developed to address the security concerns of the SCADA system as related to the power grid. Although SCADA is a specific instance of an ICS, some development work will be needed to adapt these capabilities to ICS as used in

manufacturing. In addition, some models and tools, like the ones from NSA, may not be available to the public.

4.2.2 Existing Modeling/Simulation to Enhance ICS Security Testing

Currently there are a variety of available modeling and simulation capabilities that are applicable for ICS security testing. These include, for example: SimuLink by Mathworks; specialized real-time digital power system simulators, such as the ones developed by RTDS Technologies; and simulation software written in PetriNet. All these capabilities can support real-time hardware-in-the-loop testing and capture of performance and security related data. However, some effort will be needed to adapt these capabilities to specific ICS security testing requirements. The Passive Vulnerability Scanner has also deployed extensively (Tenable). Tools primarily employed for SCADA include Snort software (now developed by Sourcefire) and SCADA+ Pack (developed by GLEG).

4.2.3 Tools Currently under Development for Testing/Modeling of Security Impacts

Two categories of emerging software could be used for ICS security risk assessment and contingency analysis: security software and network simulation software.

There are three kinds of security software, as differentiated by its developer: open source (sometime with government resources), government-supported, and privately funded. Kali Linux is security testing forensic software that has been developed by a consortium of developers, following the model of the original Linux development. It is now hosted by Offensive Security. Sophia is security software designed to passively monitor networks and detect intruders and anomalies. Sophia was developed by the Department of Energy (DOE) Idaho National Laboratory (INL) with funding from Office of Electricity Delivery and Energy Reliability (OE) and from the Department of Homeland Security (DHS). It is being commercialized by NexDefense and is in Beta II test, and about ready to go live. There are also tools developed by the SANS Institute, known for their cybersecurity training and related software.

For network simulation software, two privately developed network simulation and evaluation software tools are the OPNET Modeler Suite developed by Riverbed Technology and the software and tools developed by SANS Institute. Two open source software packages are NS-3, designed to simulate discrete-event networks, and OMNeT++, an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators. Nessus Passive Vulnerability Scanner has also been deployed extensively

The aforementioned set of security and network modeling software tools are considered sufficiently mature and can be readily applied to current ICS security concerns.

4.3 Challenges and Gaps for Modeling and Simulation for ICS Security

Challenges and gaps for modeling and simulation have been identified in three areas: metrics, models, and methods. Table 4-1 provides a list of challenges and gaps in these areas.

Metrics

Metrics are essential for measuring security aspects of ICS and associated networks. Metrics facilitate the evaluation of vital security functions and help quantify the security, trust, reliability, and usability of an ICS network. Metrics are of several types:

- Checklist or compliance metrics (e.g., Federal Energy Management Act [FISMA] compliance, or NERC CIP)
- Vulnerabilities found in vulnerability scanning (e.g., using a pen tester)

- Time to apply security patches from an operating system (OS) or application provider: in an enterprise setting, "as quickly as possible" is desirable, but for reasons of patch vetting and need for continuous operation, this can be problematic in ICS
- Frequency of monitoring
- Time/effort/resources for a skilled pen tester to penetrate a system
- Running anti-virus, whitelist, and host firewalls; these can be a case of compliance metrics; anti-virus is increasingly perceived as not useful
- Alerts from security monitoring, per unit time, and how many of these turn out to be security-relevant

None of the above translates to a universally accepted "security metric" or criterion to demonstrate that one system is more secure than another. A metric for frequency of monitoring each asset and software checkpoint on the ICS network is one approach for some measure of confidence on each component of the ICS network (i.e., higher monitoring frequency, greater trust of the ICS network). Similarly, metrics need to be developed for the protocols (e.g., SCAP) that are used for communication within an ICS network.

An integrated metric that captures both system security and system performance could help ICS operators evaluate ICS security and performance interactions. The definition of ICS performance should be considered carefully. Since ICS include components such as SCADA systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC), the location of performance measurements and the directly measureable metrics must be carefully selected. A standard, baseline system should be developed to serve as a benchmark from which to evaluate the validity of each selected metric. This baseline system can also be used to build ICS security risk models.

Models

Just as a standard baseline system is needed to close the metrics gap, a baseline model is needed to support a host of development and testing efforts, ranging from validating new security software performance to baseline new performance metrics. One key gap is the lack of a high fidelity ICS test and development model that simulates the main functions and real time dynamics of the ICS, taking into account potential security vulnerabilities in the ICS. Since an ICS may be an integration of multiple ICSs, the model will also need to accommodate any heterogeneity within an ICS. Operation center characteristics should also be included, which will enable analysis and evaluation of the data analytics and display of security data. Developers can use the model to test new security technology and software, new security protocols, and new control paradigms. In addition, this model enables an understanding of how security technology affects ICS performance. Key metrics for both security and performance can be captured and baselined via this model.

TABLE 4-2: SIGNIFICANT CHALLENGES AND GAPS IN SECURITY MODELING

Metrics

- Lack of metrics for security, trust, reliability, usability, and ICS performance
- Undefined standard baseline system

Methods

- Lack of security assessment methods that adapt to the changing malware threat
- Inadequate smart diagnosis of anomalies
- Lack of non-invasive assessment/ inspection tools

Models

- Nonexistent high fidelity ICS model of a test and development environment, including operations center
- Nonexistent high fidelity threat model that accommodates malicious and accidental security breaches
- Undeveloped tools and models to assess financial impact of security and breach in ICS
- Lack of supporting information that aides in model development (e.g., industrial processes, malware)

A high-fidelity threat model is also necessary to simulate the security threats that an ICS may experience. This threat model must simulate an adversary's approach and its attributes. In addition, the combination of threat model with the ICS model must simulate a security breach life cycle, both malicious and accidental, ranging from the infection entering the ICS network via an attack surface to the appropriate ICS behaviors attributable to the attack. The model combination not only enables assessment of a security breach impact on ICS performance and usability, but also assessment of any safety concerns. Fail-stop and fail-operation on an ICS from attacks must be simulated in the model. Modeling of the accidental breach could be challenging since this type of breach is usually caused by a human error or oversight.

The financial impact of a security breach on ICS can be sizeable. Therefore, tools and models need to be developed to assess the financial impact of a security breach in an ICS. To make a model successful, access is needed to detailed information on industry processes (of which ICS is designed to support), measured ICS performance data, and details and data on the threat. Without these three key pieces of information, the models built for ICS security will not have the appropriate fidelity.

Methods

New methods need to be developed to measure the ICS security status and related performance metrics. Recognizing that the threat is not only diverse but also evolving, a key gap in measurement methodology is an approach to conduct ICS security assessments that adapt with the threat. Furthermore, a smart diagnosis of anomalies that not only identifies the threat but also enables containment procedures is needed. Existing security software has the diagnosis and containment capabilities. However, for an ICS application, where the network is large and diverse, the security software must be implemented in concert with the ICS security assessment methods. Whatever measurement methodology is chosen, it must be non-invasive and invisible to the day-to-day operation of the equipment and network supported by the ICS.

4.4 Roadmap for Priority R&D

A number of priority R&D areas were identified as important to modeling and simulation for security of ICS. The results are summarized below and detailed in the following figures.

- **Figure 4-1: Adaptability of ICS Security Solutions** – With the increasing and evolutionary nature of cybersecurity threats, it is becoming more complex to protect a

dynamic ICS system. Many existing ICS were built without organic cybersecurity protection in mind. An adaptable and dynamic security solution for ICS is suggested that would help elevate ICS security capabilities to successfully handle today's threat environment.

- **Figure 4-2: Model the Adversary** – Quantitative and qualitative cyber threat models are limited today, including those that can simulate attack methods, motivation, and capabilities. A suggested approach is to develop a set of models that represent the diversity and complexity of the cyber-attack in ICS.

- **Figure 4-3: Models of Human Performance/Decision on Impact** – Pragmatic behavior models and tools are currently lacking to understand, assess, and predict human-machine interactions in the ICS security and performance environment. Operational tools are also needed to balance security and usability tradeoffs. To attack this behavioral challenge, one approach is interdisciplinary research that brings synergistic domain expertise together from ICS, behavior science, computer science, and industry stakeholders. This effort would build, test, and validate models and tools with behavioral components.

FIGURE 4-1: ADAPTABILITY OF ICS SECURITY SOLUTIONS

Barrier: Evolving cybersecurity threats and the protection of a dynamic ICS system against such threat; outdated ICS built without organic cybersecurity protection in mind.

Approach Summary: Develop an adaptable and dynamic security solution for ICS.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Develop smart diagnostics tools that are reconfigurable, forensic, and adaptable to new ICS configurations and security threats • Identify and develop ICS security modeling approaches and techniques • Define metrics to measure the complexity of the security vulnerability	• Ability to demonstrate detection of beaches in static and dynamic systems • Demonstration of improved diagnostic time, cost, and accuracy • Assess financial impact of adaptable versus non-adaptable security solutions	• Maintenance of ICS security as both the ICS and security environments evolve • Adaptation of security solutions from manual to automatic to self-learning
3-5 years	• Develop forensic diagnostics that are adaptable to new security systems • Develop robust control paradigms to ensure security adaptability	• Demonstrate adaptability for each new secure control paradigm • Demonstrate robustness of control paradigms in real systems	
5+ years	• Develop self-adaptive ICS security systems • Develop a shared enterprise repository of ICS security tools • Explore application of artificial intelligence merging with emerging control system paradigms	• Define taxonomy, specification, and BPM for repository participation • Established repository of ICS security tools	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Provide requirements, data, use cases, and test platforms
- **Industry/ Control System Providers:** Provide requirements, test environments, and prototypes
- **IT Community:** Share cyber-security use cases
- **Academia:** Develop models and methods; perform simulations; develop prototypes
- **SDOs/Standards Committees:** Maintain metrics and definition libraries for ICS security/performance quantification
- **Government:** Support longer term goals; fund testing including testbeds

RELATIVE IMPACTS
LOW —HIGH POTENTIAL

- ♦♦ **Improves system performance:** Balances performance and security continuously
- ♦♦♦ **Reduces costs of security:** Adapt solutions, avoiding re-design
- ♦♦♦ **Improves security / resilience:** Main goal of adaptability (i.e., continuous optimization)
- ♦ **Enhances industry competitiveness:** Depends on the amount of sharable information
- ♦♦ **Reduces time/ complexity of security validation:** Adaptable systems reduce complexity
- ♦♦♦ **Speed of Diagnosing and Recovery:** Reduces downtime; reduce potential for recurrence

FIGURE 4-2: MODEL THE ADVERSARY

Barrier: Lack of quantitative/qualitative cyber threat models including methods, motivation, and capabilities.

Approach Summary: Develop a set of models that represent the diversity and complexity of the cyber-attack.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Survey existing security breaches and classify into different attack models • Develop a taxonomy of ICS attack/breach • Develop a game theoretic approach/model to represent one attack model	• Published report with lessons learned and taxonomy • Designed initial adversary model	• Adaptive, on-line model building of adversary behavior • Automatic and instantaneous deployment of security to prevent adversary success • Ability to isolate and minimize impact of attack
3-5 years	• Validate model on new emerging attacks • Enhance model to capture emerging behavior • Incorporate stochastic and/or behavioral models • Test adversary model against existing/proposed security protocols	• Enhanced adversary model • Tested and validated results	
5+ years	• Develop adaptive, on-line model-buildings and instantaneous protection deployment to prevent security breaches	• Defined method for on-line adversary model development	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Share existing breaches and lessons learned; collaborate on testing and validation
- **Industry/ Control System Providers:** Share existing breaches and lessons learned; collaborate on testing and validation
- **IT Community:** Share existing work on adversary modeling; collaborate on model development.
- **Academia:** Perform research and testing
- **SDOs/Standards Committees:** Integrate adversary models into security standards
- **Government:** Support esearch and testing; facilitate collaboration

RELATIVE IMPACTS

LOW —HIGH POTENTIAL

- ♦♦♦ **Reduces costs of security:** Know what you are defending against
- ♦♦♦ **Improves security / resilience:** Know what you are defending against
- ♦♦ **Enhances industry competitiveness:** Greater security of manufacturing and other systems to produce as expected; lower costs
- ♦♦ **Reduces time/ complexity of security validation:** Defined methods reduce time and difficulty of validation

FIGURE 4-3: MODELS OF HUMAN PERFORMANCE/DECISION ON IMPACT

Barrier: Lack of pragmatic behavior models and tools to understand, assess, and predict human-machine interactions in ICS security and performance; lack of available operational tools to balance security and usability tradeoffs.

Approach Summary: Conduct interdisciplinary research bringing synergistic domain expertise from ICS, behavior science, computer science, and industry stakeholders; build models and tools; pilot test models in real environments; assess/validate models' effectiveness; continuously improve models.

Time-Line	ROADMAP ACTION PLAN	MILESTONES AND RESULTS	OVERARCHING TARGETS
1-2 years	• Identify challenges, best practices, and barriers to improvement in ICS security through focus groups, workshops, and industry surveys • Seed research activities/funding on models and tool developments	• Published modes, tools needs, and best practices • Proposed framework • Prototyped tools and preliminary field studies	• Accurate ability to model, assess, and predict human behavior, including accidental, intentional, and malicious behavior • Increased resiliency and greater control to deal with extreme cyber and physical events
3-5 years	• Select best models, methodology, and tools • Develop benchmarks • Develop formal process for research, development, deployment, and continuous improvements	• Developed standard for human-machine interface for ICS security and performance review and publish the standards • Published implementation guidelines • Published the process for standard development and revision	
5+ years	• Establish standards review process • Adapt models, tools, and process to reflect current and emerging system states	• Published periodic updates to standards • Published periodic implementation guidelines • Published periodic update to the process	

STAKEHOLDERS & POTENTIAL ROLES

- **Industry/ Control System Users:** Provide input to surveys; share best practices
- **Industry/ Control System Providers:** Provide input to surveys; share best practices
- **IT Community:** Develop models and technologies
- **Academia:** Perform research; develop theoretical models and framework
- **SDOs/Standards Committees:** Develop and maintain standards; perform standards review and revisions
- **Government:** Enforce regulations enforcement; endorse stakeholder coordination

RELATIVE IMPACTS
LOW —HIGH POTENTIAL

- ♦♦♦ **Improves system performance:** Improves models, validation, and deployment
- ♦♦ **Reduces costs of security:** Reduces technical constraints
- ♦♦♦ **Improves security / resilience:** Handles accidental, intentional, and malicious events
- ♦♦ **Enhances industry competitiveness:** Increases resiliency of infrastructure
- ♦♦ **Reduces time/ complexity of security validation:** Reduces complexity of validation
- ♦♦♦ **Other:** Improves security versus usability

5 SECURITY CONTENT AUTOMATION PROTOCOL AND OTHER ICS SECURITY NEEDS

5.1 Overview

The Security Content Automation Protocol (SCAP) describes how to use specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation. SCAP content resides currently in the government-supported National Vulnerability Database (NVD). SCAP combines the requirements of multiple open standards that are used to enumerate security-related software flaws and configuration issues. SCAP provides methods to measure systems to find vulnerabilities and offers ways to score results and evaluate possible impacts.

The communication of software flaws and security configurations is essential to ICS and non-ICS systems. To facilitate this communication, NIST is guiding a community effort to develop a series of specifications to standardize the format and nomenclature by which security software communicates.[2] These specifications with respect to their effects on ICS were explored at length in the workshop, with a focus on the challenges and gaps.

5.2 Major Challenges and Gaps for Using SCAP in ICS

Several challenges and gaps were identified with respect to the use of SCAP. These challenges and gaps are listed in Table 5-1 and discussed below.

The first set of challenges relates to education and outreach. A greater general awareness of SCAP and the security protection it brings to ICS (as well as the potential benefits) must be fostered. Furthermore, a workforce trained in SCAP must be developed to support and maintain widespread implementation.

TABLE 5-1: SIGNIFICANT CHALLENGES AND GAPS RELATED TO SCAP

Awareness
- Increasing general awareness of SCAP for ICS; minimal workforce training on SCAP for ICS

SCAP Implementation
- Difficulty of retrofitting legacy ICS with SCAP
- Identifying / addressing the ICS performance issues associated with SCAP implementation
- Technical (e.g., interface) and logistical (e.g., scalability) challenges of implementing SCAP into existing ICS
- Validation of the security protection enabled by using SCAP with other security technologies
- Inability to validate SCAP mitigating security risk within embedded systems in existing ICS
- Difficulty validating integrity of communication / data flow from networks that do not employ SCAP
- Expanding SCAP to accommodate a vertically integrated system

Strategy and Business Planning
- Nonexistent plan, strategy, or roadmap to implement SCAP to existing ICS
- Risk / benefit analysis of implementing SCAP into existing ICS

[2] http://scap.nist.gov/publications/index.html

The technical challenges of using SCAP include retrofitting existing legacy ICS with SCAP, as well as the potential ICS performance issues associated with SCAP implementation. Better understanding is needed of potential performance impacts and the issues that may arise with integration of SCAP into existing systems.

The business case and risk / benefit analysis for SCAP in ICS are not well developed. Justifiable business models will be needed to substantiate the introduction and wider implementation of SCAP for ICS. A defined roadmap for SCAP implementation could support business planning, SCAP demonstrations, and outline pathways for addressing potential performance challenges. Validation and proof of the cyber protection enabled by SCAP is needed to determine levels of assurance in the complex industrial environment.

5.3 R&D, Testbed, and IT Needs for SCAP and ICS Security

Beyond the priorities outlined in previous chapters, additional challenges exist that will require research and development (R&D), testbed verification, and/or new IT security capabilities, including those related to SCAP. These additional needs are listed in Table 5-1.

TABLE 5-1: FUTURE R&D, TESTBED, AND IT SECURITY CAPABILITY NEEDS

R&D	Testbeds	IT Security Capability
• Develop a turnkey ICS security solution • Define ICS security requirements and performance metrics • Perform risk / benefit analysis of SCAP compliance criteria in future performance / certification programs • Develop SCAP for extension to supply chain	• Validate SCAP in a testbed environment, for ICS plus at system level • Validate automated asset and vulnerability discovery • Verify data sharing framework and options • Invest strategically to accommodate future testing needs • Define testing standards to accommodate current and future needs	• Implement security technology and protocol across a large network • Develop tools and software for automatic asset management • Automate asset management – asset discovery tool/system

Future R&D

Future ICS security protection depends on R&D progress. One key R&D focus is a turnkey solution to implement security technology on ICS that accommodates SCAP compliant electronics as well as legacy ones. Turnkey solutions will certainly reduce the cost barriers involved in securing ICS. Further cost reduction, especially on the upfront investment, will be achieved when this turnkey solution can be applied across multiple industries.

Analysis-oriented R&D needs for ICS security protection include the risk and benefit of incorporating SCAP compliance criteria in future performance / certification programs and extending SCAP to the supply chain networks.

Testbeds

Validation of SCAP in a testbed environment is essential. Now, SCAP testing is performed at the system level and not the component level. Testbeds must validate the ability to continuously monitor the ICS network infrastructure integrity, including discovery and profile of every asset on the entire network for situation awareness. The testbed must also verify data sharing options. A data-sharing network among different components of ICS, or different ICSs, must be defined. The issues of big data

(increasing volumes and types of data) will need to be considered. Both test criteria and testbeds must also be designed to handle current needs and accommodate future needs.

Additional IT Security Capabilities Needed for ICS

Various additional IT security capabilities needed for ICS were identified. The scalability of security technology deployment across ICS is particularly concerning. For example, deploying public key infrastructure (PKI) certificates across an ICS network and mutual authentication among entities is challenging.

Future software and tools will be required to continuously monitor ICS security health and status, performing functions such as identification of vulnerability, discovery of new software, and detection of removal or addition of assets.

6 TESTBED COORDINATION

6.1 Overview

Many testbeds have already been created by government, academia, and industry to facilitate the evaluation of various aspects of security technology, systems, and architecture. These testbeds provide invaluable resources to the communities they serve. However, additional testbeds are needed to support security development efforts not served by these existing testbeds.

6.2 Existing Testbeds and Capabilities

The existing testbeds explored include:

- Cyber-Defense Technology Experimental Research (DETER)
- National SCADA Testbed
- Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)

The DETER testbed is an open source cybersecurity experimentation and testing facility. It is an emulator capable of testing security technologies through virtualizations and attack emulations. It does not evaluate ICS systems, but it evaluates IT systems. It is used by DHS-funded researchers and the cybersecurity research community including government, industry, and academia. The DETER-Enabled Federation of Testbeds (DEFT) initiative uses the DETER framework to federate cyber and cyber-physical assets in various existing test environments, and is at present more directly amenable to ICS security experiments.

The National SCADA Testbed is available to the DOD, DHS, and DOE. It mainly enables testing of security technologies, but also allows for testing of architectures and the use of tools and simulations. It encompasses testing of products, wireless technology, protocols, and real hardware systems.

The DOD's SPIDERS testbed provides testing of security technologies and architectures and model and simulation tools. The testbed is applicable for power grid installations with multiple renewable energy systems.

Details of several testbeds that were discussed by workshop participants are presented in Table 6-1. Neither Table 6-1 nor Figure 6-1 is intended to be complete, or endorse or discredit any of the testbeds included or not included here.

TABLE 6-1: IDENTIFICATION OF EXISTING TESTBEDS AND CAPABILITIES

Name of Testbed	Items Tested	Capabilities of Testbeds	Collaborators/ Testbed Users

• **DETER (DHS)**	• Testing security technologies (i.e., an emulator)	• Emulates IT systems – not ICS
		  ○ Attack emulations
		  ○ Virtualization
		  ○ Not for wireless
			• Open source

• **National SCADA Testbed**	• Security technologies mainly, but it's a hybrid	• Wireless • Product testing • Protocols • Real systems (hardware)	• DOE, DOD, DHS

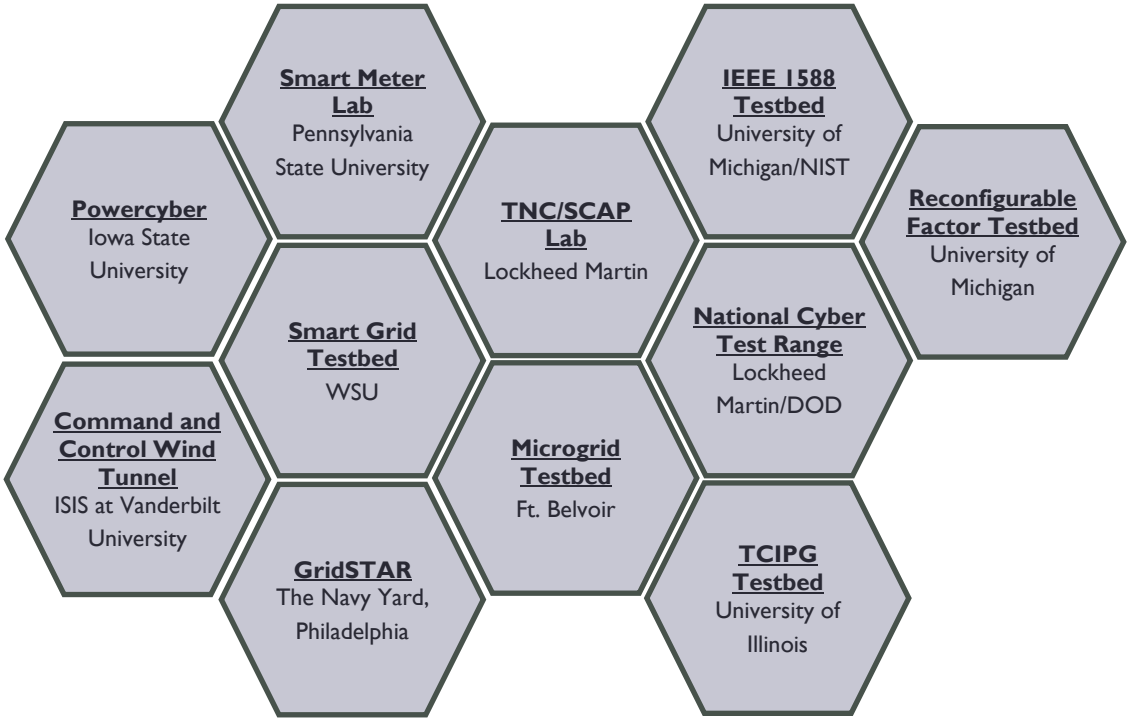
• **SPIDERS (DOD)**
  ○ **Full scale**
  ○ **Validate CSET 5.1**
  ○ **Define enclave bound**
	• Security technologies and architectures, use of models and simulation tools
	• Final phase: SCADA systems security
		• Power grid installation with multiple renewable energy systems	• Mainly:
			  ○ DOE
			  ○ DOD
			  ○ Utilities
			  ○ DHS

TABLE 6-1: IDENTIFICATION OF EXISTING TESTBEDS AND CAPABILITIES (CONTINUED)

Name of Testbed	Items Tested	Capabilities of Testbeds	Collaborators/ Testbed Users
• **DOE Smart Grid Platform Testbed**	• Testing smart grid techniques (not setup to test security) • Modeling and simulation	• Modeling of real manufacturing systems ○ Higher-level monitoring/ control	• Manufacturers • Vendors • NIST/DOE • JPL
• **Center for Advanced Engineering and Research (CAER) Testbed at UVA**	• Testing security and • Using models/simulation	• Human factor testing • Cyber incident simulation • Planning to have hardware in the loop	• Academia • EPRI • Manufacturers • States

• **Mississippi State University ICS Testbed**	• Technologies testing	• Testing of OTC technologies
		  ○ PLCs
		  ○ HVAC
		  ○ Industrial Ethernet
			• DHS
			• Vendors

FIGURE 6-1: OTHER TESTBEDS



6.3 Opportunities for New Testbeds

Several areas were identified to support the development of a new testbed, the improvement of an existing testbed, or the testing of industrial scenarios. One opportunity is the development of a real-time extension of existing testbeds, which would utilize tools to simulate ICS processes in real time and provide interfaces for hardware networks. DETER, for example, could be expanded to include ICS systems (rather than IT systems) and wireless technologies. Heterogeneous testbeds could also benefit from improving the composition framework, which could include openly accessible federated testbeds, multi-domain testbeds, hybrid testbeds (real, emulated, simulated, and scalable), and composable testbeds. Another opportunity is the insertion of ICS technologies in real world use, such as through DOE's Smart Grid Testbed.

Industrial Automation Scenarios Testing

There is an opportunity for physical/virtual integration, such as a virtual manufacturing environment with hardware in-the-loop and security instruments. Another opportunity of real-time test scenarios could include the interaction of cyber control and physical processes in the use of collaborative robotics for manufacturing and assemblies requiring real-time controls, and in synchronized motor controls across subnets. Other industrial automation scenarios include dynamic testing for intrusion detection to ensure that network components have not been compromised or altered, and simulations of optimal level of security for time sensitive functions.

Security Capabilities/ Technologies to Test for ICS Performance Impacts

The overarching need is to co-optimize security and performance. Efforts include resiliency for control systems under attack, SCAP for ICS, external system communications and interfaces, network monitoring versus component monitoring, and datasets to make meaningful test experiments. Others might include new control paradigms that are more secure, and key management practices for ICS.

TABLE 6-2: OPPORTUNITIES TO IMPROVE/EXPAND EXISTING TESTBEDS

Composition Framework for Heterogeneous Testbeds	Real Time Extension of Existing Testbeds	Other Opportunities for Existing Testbeds

• Composable Testbed
  ○ Simulator Integration
  ○ Model Integration
  ○ Model Libs
  ○ Hardware (HW) in the loop
• Hybrid Testbed:
  ○ Real
  ○ Simulated
  ○ Emulated
  ○ Fidelity
  ○ Scalability
  ○ Federated
• Linked testbeds and collaborative meta-testbed (multi-domain)
• Openly-accessible federated testbeds
	• DETER plus additional capabilities:
	  ○ ICS
	  ○ Real-time
	  ○ Wireless
	• Expand: Testbed to real-time NCS, e.g., EtherCat with security layers and breach test cases
	• Tools to simulate ICS processes in real time and also provide interfaces for hardware networks
		• Building control systems
		  ○ Fire, security, energy, transport, etc. "Smart Building"
		• Define metrics and methods for testing
		• DOE Smart Grid testbed
		  ○ Insertion opportunity for ICS technology in real world use
		• Wireless protocol testing
		• Security performance impact metrics testing

TABLE 6-3: INDUSTRIAL AUTOMATION SCENARIOS FOR TESTBED VALIDATION

Physical/Virtual Integration	Real-Time Test Scenarios	Other Industrial Automation Scenarios

• Physical to virtual replication
• Test patches, whitelist pen test
• Virtual factory
  ○ With hardware in-the-loop
  ○ With security instruments
	• Synchronized motor control across subnets/PLC's
	• Collaborative robotics for manufacturing/assembly requiring real-time control
	• Multi-levels of manufacturing control
	  ○ Device, cell, system, etc.
	• Interaction between cyber-control and physical processes
	• Timing properties with security
	• Heterogeneous system of systems and interactions
		• Dynamic test for intrusion detection to ensure that network components have not been compromised/altered
		• Integrate and coordinate between safety and security
		• Chip manufacturing
		• Board build-ups
		• Process-based (chemical industry); Discrete (automotive manufacturing)
		• For time sensitive functions simulate optimal level of security

TABLE 6-4: SECURITY CAPABILITIES/TECHNOLOGIES TO TEST FOR PERFORMANCE IMPACTS IN ICS

Co-Optimization of Security and Performance

• Real-time focus
• Resiliency for control systems under attack
• Intrusion detection systems (performance and impact)
• Soft-PLCs with host-based security
• "Fieldbus" i.e., non-IP protocols for older control systems
• SCAP for ICS
• External system communications and interfaces
• Need datasets to make meaningful test experiments
• Network monitoring vs. component monitoring - Internal vs. external
• System-level experiments
  ○ Impact studies
  ○ Attack-defense evaluations
  ○ Validating countermeasures
• Security based on kinematics/dynamics of the process
• Immutable roots of trust
• Risk analysis and management
• New control paradigms that are more secure
• Key management practices for ICS

APPENDIX A: PARTICIPANTS

Marshall Abrams
The MITRE Corporation

Carlos Aguayo Gonzalez
Power Fingerprinting, Inc.

DJ Anand
NIST

Demos Andreou
Eaton's Cooper Power Systems

John Baras
University of Maryland

Getachew Befekadu
University of Notre Dame

Holly Beum
Interface Technologies

Harold Booth
NIST

Mark Bristow
DHS (ICS-CERT)

Thurston Brooks
Power Fingerprinting, Inc.

Lewis Campbell
PNM Resources

Rick Candell
NIST

Alvaro Cardenas
UT Dallas

Lisa Carnahan
NIST

Steven Chen
Power Fingerprinting.com

Michael Chipley
The PMC Group LLC

Stephen Dill
Lockheed Martin

Michael Dransfield
NSA

Earl Eiland
TÜV SÜD America

Douglas Eskins
U.S. Nuclear Regulatory Commission

James Formea
Cooper Power Systems

Manimaran Govindarasu
Iowa State University

Robert Graybill
Nimbis Services Inc.

Chris Greer
NIST

Adam Hahn
MITRE

Jihyun Harper
DoD USAF

Carol Hawk
U.S. Department of Energy

John Horst
NIST

Robert Huba
Emerson Process Management

Larry John
Analytic Services Inc.

Tadashi Kamiwaki
Control System Security Center

John Kenworthy
Red Tiger Security

Himanshu Khurana
Honeywell

Xenofon Koutsoukos
Vanderbilt University/ISIS

Abhai Kumar
ANSER

Margaret Leary
Avaya Government Solutions

Kang Lee
NIST

Suzanne Lightman
NIST

Joshua Lubell
NIST

Jose Maldonado-Lizardi
NSA

Devu Manikantan Shila
United Technology Research Center

Jeremy Marvel
NIST

Mark McClellan
US Air Force

Larry McFadden
NSA

Jim McGlone
Ultra Electronics, 3eTI

James Moyne
University of Michigan

Dave Norton
Federal Energy Regulatory Commission

Roger Pan
Emerson Process Management

Vicky Pillitteri
NIST

Charley Robinson
ISA

Thomas Ruchti
Eaton

Rick Sarver
PNM Resources

Eugene Song
NIST

Dean Stewart
Interface Technologies

Keith Stouffer
NIST

Janos Sztipanovits
Vanderbilt University

Dawn Tilbury
University of Michigan

Al Valdes
University of Illinois

Steven Venema
Boeing

Dave Wollman
NIST

APPENDIX B: WHITE PAPERS

Measurement of Security Technology Performance Impacts for Industrial Control Systems:

Devu Manikantan Shila, United Technologies Research Center

Metadata Isolation and Intrusion Protection:

W. J. Miller, President, MaCT

Extending the Semantic Web to Peer-to-Peer-Like Sensor Networks Based on XMPP:

Peter Waher, Member, XMPP Standards Foundation, and ISO/IEC/IEEE P21451-1-4

Measurement of Security Technology Performance Impacts for Industrial Control Systems

Devu Manikantan Shila
United Technologies Research Center

Some of the key measurement science barriers or challenges that prevent the implementation of security technologies in industrial control systems are:

- Control systems typically have ***stringent constraints*** on size, weight, latency, processing power, and cost. Implementation of existing computationally intensive but highly secure encryption or authentication protocols can lead to decreased life-cycle and increased size, weight and cost. Therefore, light weight implementations of existing secure protocols or design of novel protocols and standards that can perform well within these constraints are needed to ensure confidentiality and integrity in these systems.
- Limited or no techniques to ***down select optimal security technology*** for a given system with design, cost, weight and power constraints. Novel tools, metrics or models that will facilitate the comparison of different security technologies for various hardware architectures are required.
- Trusted platform modules typically used to protect the secrets are costly to implement in a resource-constrained control system environment. An adversary may have ***easy physical access to control system end devices*** e.g., smart meters and hence new methodologies are needed to ensure and test security of firmware, cryptographic materials stored in end systems such as certificates, keys, passwords etc.
- Complexity in ***implementing security technologies in legacy control systems*** which may require upgrading the hardware or software of the devices to secure version of the protocols. It is not economically or technically feasible to put new systems and throw away existing ones.
- Complexity in **fixing security bugs or patches** due to real-time application needs and constraints. Additionally, current techniques such as IPSec, SSL are very costly to implement in control systems and therefore, remote maintenance via direct connection to these devices is hard to perform.
- Limited or no tools for ***assessing the vulnerability of control systems*** at the hardware, control, software and network level and hence, security personnel often face difficulty in choosing appropriate countermeasures for these systems.
- Hard to ***ensure non-repudiation*** (auditing real-time events) due to limited storage space.

The following are some of the most important areas we think where R&D is needed in measurement and standards that enable the use of secure techniques for control systems, without impacting the performance.

- Analytical models, tools and metrics for quantifying the performance of cryptography protocols for various platforms with different requirements (e.g., processor speed, memory, code space)
- Virtual hardware solutions that can be used to emulate the performance of secure technologies. These techniques will enable a designer to choose appropriate technology for the targeted platform.
- Light weight implementations of existing secure algorithms or design of novel cryptography protocols and standards
- Cost-effective and scalable methodologies for retrofitting security in legacy control systems
- Secure remote firmware updates
- Automated tools for risk management including identifying the threats, quantifying the risks and prioritizing the risks.

METADATA ISOLATION AND INTRUSION PROTECTION

William J. Miller
Chairman
ISO/IEC/IEEE P21451-1-4

Meta Data Isolation (MDI), offers a process for transition ("transversion") of a legacy protocol, used in semantic messaging, using eXtensible Messaging and Presence Protocol (XMPP), which is based on XML (eXtensible Markup Language). This capability is being defined in ISO/IEC/IEEE P21451-1-4 XMPP Interface Standard also known as "Sensei/IoT" which the first joint standard effort among ISO, IEC, and IEEE, specifically for Sensors Networks, Machine-2-Machine (M2M), and the Internet of Things (IoT) as a Semantic Web 3.0 Sensor Standard.

MDI offers the inherit characteristic when used to provide transversion of legacy protocols such as MODBUS to XMPP. MDI uses port translation during transition of Port 80 data traffic to XMPP. The traffic is firewall friendly and avoids invoking an action on a control system that could adversely affect the process. All endpoints can utilize MDI to restrict access to certain registers or provide alert and status messages depending up the end device.

MDI provides an effective means of virtual isolation of data traffic and provides other new capabilities. The MDI provides a transparent inline means of applying policy and exposing data, status, and alerts that can be shared with mobile devices. The data residing in XML can now imported directly into a web page or applications such as spreadsheets and databases.

P21451-1-4 defines the requests/responses for a common transport and provides bi-directional transversion so the XMPP can be restored to the legacy protocol since the endpoint device looks the same as any other field device, it can be connected to any SCADA system. MDI provides a point-to-point or point-to-multipoint connections within a facility. It can utilize centralized or distributed architecture to provide application layer routing including registration and authorization of devices.

MDI provides a means of identification of the participating devices and assuring that they are interoperable. Today, we operate plants with inferred trust and security, if utilized, provided by the physical layer. The MDI provides TLS encryption while in transport and EXI (Efficient XML Interchange) metadata identification digital signed information between the endpoints. It is envisioned as the standard evolves that these devices would be added as a security safeguard or embedded into end devices.

MDI provides useful capabilities for Common Network Management and Security Event Reporting. This type of capability has not been provided for control systems. Security events are reactionary and as such are after the fact. The current approach of using anti-virus, IDS, and IPS has been used on computers systems but is generally impractical for field computing systems. It is now more difficult since even those systems are isolated within a facility. In addition, they are generally restricted from having access to the Internet.

MDI provides capabilities needed to protect critical systems, which generally have no protection at all. It provides a means of isolation of protocols, inspection of packets, and prevention of improper or unauthorized actions utilizing a Meta data approach based upon a standard.

Extending the Semantic Web to Peer-to-Peer-Like Sensor Networks Based on XMPP

Peter Waher,
Member, XMPP Standards Foundation, and
ISO/IEC/IEEE P21451-1-4

***Abstract* — This paper provides a novel approach in bridging the traditional semantic web based on the HTTP protocol and peer-to-peer-like sensor networks based on the XMPP protocol, thus extending the reach of semantic technologies to private spheres otherwise not accessible due to firewalls and other security measures, but still maintaining a high level of security and end-user data privacy and access control.**

***Index Terms* — Internet of Things, Peer-to-peer networks, Semantic web, data privacy, access control, plug computing, grid computing.**

I. INTRODUCTION

HE USE of Semantic Web technologies [1] within the TInternet of Things is a very promising area of research and development. It allows for the unification of a huge amount of proprietary APIs into one set of standardized APIs for accessing and linking data not only between Things in the network, but also between services and consumers, regardless of who has published the data and where it is stored. It replaces the more difficult problem of implementing and supporting a huge array of proprietary communication APIs and protocols with the simpler problem of mapping or understanding the information provided by different Things.

The tradition of basing the Semantic Web on the HTTP protocol [2] has several implied limitations, especially when Things move closer to the private spheres of end-users, such as within people's homes, inside office buildings, etc. As long as all Things are publicly available on the Internet, HTTP works fine. But as soon as the content starts moving into areas where access is limited by firewalls, HTTP as a transport method starts failing, since connections most often can only be established from the inside out. If the SPARQL [3] end-point resides outside of the firewall, it cannot reach Things residing inside the firewall using normal HTTP.

The same problem exists within the Internet of Things in general and not only to semantic web applications. All request/response-based communication protocols inherently have this problem. To solve this problem of communication between Things behind firewalls within the Internet of Things community, various solutions have been proposed:

A) Publish/Subscribe architecture patterns
B) Cloud storage of data
C) Peer-to-Peer communication
D) Hybrid approaches

A. Publish/Subscribe architecture pattern

The publish/subscribe architecture pattern [4] basically consists of three types of actors: Publishers, message brokers and subscribers. Publishers generate content and publish it to a message broker. The message broker immediately distributes the content, or information about the content, to subscribers having subscribed to the particular content.

Using this pattern, publishers and subscribers connect to the message broker and can therefore reside behind firewalls. The message broker however, needs to be reachable by all actors in the network.

As described above, all publishers and subscribers connect to the broker, bypassing any firewall restrictions on traffic in the opposite direction. Subscribers are also required to maintain the connection with the broker in order to be able to receive the corresponding information. In Fig. 1 the flow of information is from left to right. However, publishers can also be subscribers.

The publish/subscribe architecture is very efficient in distributing messages in large networks. However, it only supports one type of communication pattern: Things publishing information, consumed by others. It is difficult to create an environment permitting two-way communication and impossible for the publishers to control who gets access to what, which makes it impractical and useless in semantic web applications.

There are various protocols that readily provide publish/subscribe architecture sup-port, like XMPP [5] with its publish-subscribe extension [6]. There are also protocols or platforms that are designed primarily with publish/subscribe in mind, like MQTT [7]. Web platforms such as Twitter [8] also work according to the publish/subscribe pattern.

Paper submitted 28th October 2013. Financial support for this study was provided by KTC [50], Manodo [51] and Weevio [52].

P. Waher works for Clayster Laboratorios Chile S.A., Calle Blanco 1623, Valparaíso, Chile (e-mail: peter.waher@clayster.com).

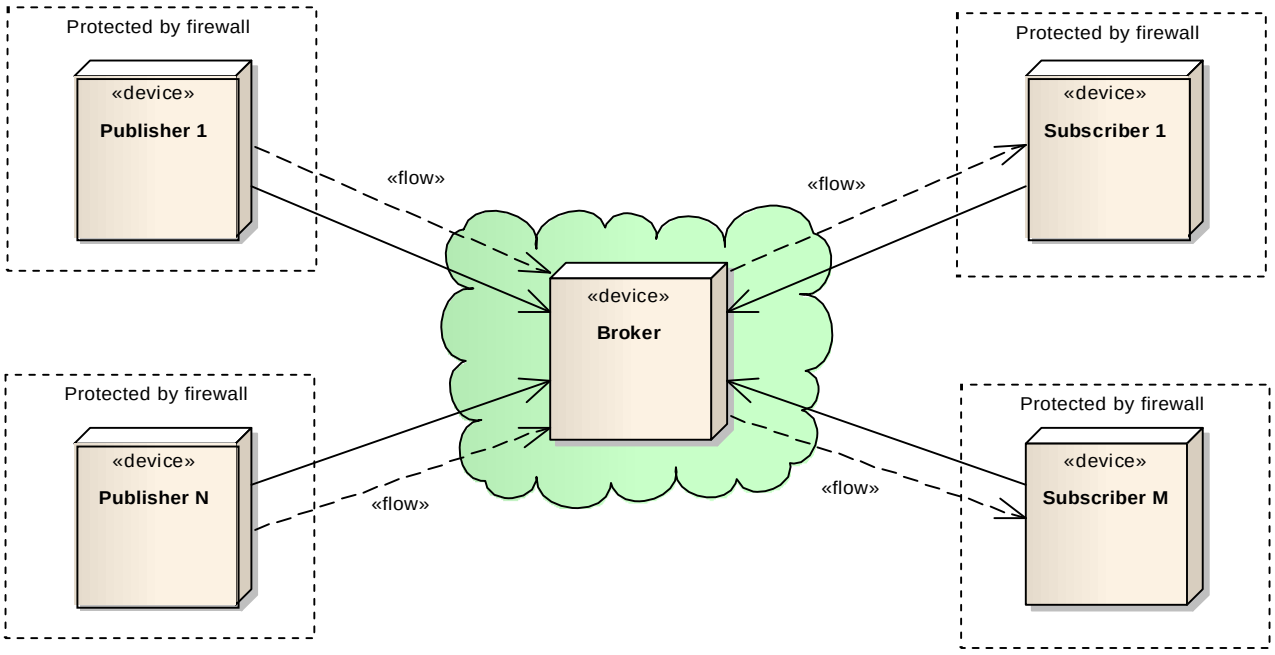


Fig. 1. Publish/Subscribe pattern

Cloud storage of data

Cloud storage of data uses a similar approach as publish/subscribe, except that there is no actual subscription of data involved that provides data in real-time. Publishers publish data to a server, which in turn always store it for future access. Consumers of the data are required to poll data from the server regularly or on demand. However, solutions exist which implement custom triggers that notify clients of events. These in turn can be used to closely mimic the publish/subscribe pattern of immediate content delivery to the final recipients.

Data published on servers is typically available through some sort of API. Common APIs can be RESTful web services [9] returning XML, using either proprietary formats or standardized formats such as RSS [10] or ATOM [11]. JSON is also popular since it allows for easy implementation in script languages.

Examples of platforms that use this technique for Internet of Things applications include Xively [12], Open.sen.se [13], SicsthSense [14] etc.

Even though this architectural pattern partly lends itself to the incorporation of the Internet of Things into the semantic web, it does so only with difficulty and with great limitations imposed on it:

First, only historic data published on the server will be available on the semantic web. There can be no direct interaction with the Things that published the information without introducing significant latency. Secondly, the publishers have no control of who can see what data. Thirdly, the publishers lose control and ownership of the data, making changes or removal difficult. Fourthly, the risk of exposing private data to unknown corporate or government interests is great if the data is stored centrally, minimizing the desire of end-users to use the approach when it comes to private information. Companies that want to exploit the information and sell data mining and big data services will of course see no problem with this approach.

B. Peer-to-peer communication

Peer-to-peer communication techniques originally developed for file sharing, instant messaging or gaming applications have become a promising field of research for Internet of Things also, in particular since these techniques provide a mechanism for devices to talk to each other, even though they reside behind different firewalls.

There are many different peer-to-peer protocols available that solve the problem on how to bypass firewall in different ways. Following is a non-exhaustive list of popular ways to achieve peer-to-peer functionality in networks:

Internet Group Management Protocol IGMP [15] is a way to send IP multicast messages. In networks where firewalls permit IGMP communication, peers can sub-scribe to IP multicast addresses and routers will forward communication to all sub-scribed peers. A party in a conversation can both send and receive information. The architecture is similar to that of the publish/subscribe pattern, with the exception that routing is done on a network layer in

routers and not in the application layer of a message broker. Also, IGMP doesn't allow for a fine grained subscription model, where you can subscribe to specific topics. Anything sent on a multi-cast channel will be received by all subscribers of that channel, unless packets are lost. Secure packet delivery is not available. Another big disadvantage is that everyone subscribed to the multicast address will receive all messages. Two implications of this are that the CPU load increases as the number of senders grows and that it is difficult to send private messages.

IGMP is popular in streaming services, especially in IP-TV networks, as it allows for efficient distribution of information where loss of packets doesn't affect the quality of the service. In order to create point-to-point communication using IGMP it is required to add a secondary addressing mechanism to make sure the recipients know what packets are meant for them and what packets are meant for others. For this reason IGMP only serves to solve certain aspects of IoT-based communication, mostly concerned with discovery of devices. Examples that use this technique for device discovery include SSDP [16] on which UPnP [17] and DLNA [18] are based. Multicast DNS [19] is another discovery method using IGMP. Multicast DNS is used by Bonjour [20] and XMPP server-less messaging [21].

To circumvent the problems of multicasting and create a peer-to-peer protocol based on single-casting, i.e. point-to-point communication, other mechanisms have to be incorporated to bypass any firewalls. One such collection of methods goes by the collective name NAT traversal [22]. It includes a series of different techniques, none guaranteed to work in all settings since NAT traversal is not standardized. Basically, it includes methods where the firewalls are programmed to forward messages received on their public IP addresses, with given port numbers, to corresponding private IP addresses and corresponding port numbers behind the firewall. This is sometimes referred to as "punching holes in the firewall". It may also include the incorporation of publically available servers that route messages, just like message brokers do.

Unbeknown to many, NAT traversal may actually create a big security problem for its users, since it partly removes the original function of the firewall: Preventing unauthorized or unauthenticated users access private resources on the network. Although popular protocols like UPnP allow devices to automatically "punch holes" in the firewall, doing so allows friendly external actors (but also unfriendly) to access devices on the network, thereby creating security holes that are easy to exploit [23].

Peer-to-peer networks are normally divided into two different types of networks: Unstructured and Structured peer-to-peer networks. Unstructured networks have no explicit network topology, and peers connect to each other "randomly" or though friendship requests. One problem such networks have is that it is difficult to find useful resources. Normally, peers can only ask known peers if they have access to a given resource. These peers can forward the question to their peers, and so on, until the resource is found. This normally works well for well-known resources. But for scarce resources, such questions impose a great load on the network.

To solve this problem, many solutions have been developed which define an explicit network topology that includes centralized resources to manage content, searching, access privileges, etc. These solutions range from content directories, to access privileges, friendships, scheduling, task lists, etc. Even though they require the use of centralized publically available servers, they are considered peer-to-peer networks, albeit structured peer-to-peer networks, as the actual peer-to-peer communication is later done directly between peers.

C. Hybrid approaches

Had it not been for the security issues described in the previous section, peer-to-peer network architecture might have been a perfect candidate for the Internet of Things due to its flexibility when it comes to point-to-point communication between peers in the network. The publish/subscribe pattern described earlier does not have this vulnerability: As devices behind firewalls all connect to a message broker that redistributes messages to interested parties, and no holes are punched in the firewall, it's impossible for external parties to connect directly to the device. This motivates the use of hybrid approaches, using federated message brokers, but having an architecture permitting point-to-point communication instead of one-to-many types of communication.

As devices connect to a message broker, external entities cannot connect to the devices, unless the message broker authenticates the device and authorizes its relationship with the original device. Even though this adds a component to the network, it is not much different from other publically available components available in structured peer-to-peer networks, as described earlier. It is even similar to the case where NAT-traversal requires the use of a public proxy server to forward messages between peers. For this reason, we will call this hybrid approach peer-to-peer-like communication. It works as a peer-to-peer protocol on the application layer, but not on the network layer.

Apart from fulfilling these requirements we also want the protocol to be open, standardized, efficient and easy to extend without the possibility of confusion. XMPP meets all these requirements [24]. XMPP was originally defined for use in instant messaging applications, which can be seen in the acronym "eXtensible Messaging and Presence Protocol". It is based on XML and the use of namespaces makes XMPP extensible and easy to extend without creating conflicts. It is also standardized by IETF. Extensions to the protocol are published and maintained by the XMPP Standards Foundation

[25]. The list of extensions available to XMPP [26] continues to grow and demonstrates how the protocol has evolved from its original domain to become a versatile protocol for the Internet in general and the Internet of Things in particular. As is shown in this paper, XMPP also provides architectural support for a logical extension of the Semantic Web into the Internet of Things. A recent extension also provides a mechanism for efficiently compressing XMPP messages, permitting the use of XMPP in wireless sensor networks with limited maximum package sizes [27].

XMPP also adds a security mechanism whereby clients are authenticated, and the broker (the XMPP Server) ensures each client sending a message to another is authorized to do so. This adds a layer of added security to the network. A recent extension of the protocol permits even better control of who can talk to whom, what they can talk about, what services are available to whom, and permitting provisioning of devices and services in Internet of Things networks [28]. If end-to-end encryption is desired, to make sure the message broker cannot eavesdrop on the conversation, work is being done within IETF to solve this issue as well [29]. Extensions also exist for communication of sensor data [30], controlling devices [31] and bridging legacy or proprietary protocols and interfacing subsystems [32].

Furthermore, XMPP can be used both in server or server-less mode using a small memory footprint, as is demonstrated by Ronny Klauck and Michael Kirsche in their work related to Chatty Things [33] [34]. Interesting Internet of Things-related projects and groups include a working group within IEEE/IEC/ISO [35], KTC [36] [37] and SUST [38] [39]. Work is also underway to define common interoperable interfaces for Internet of Things, based on available extensions [40]. A repository for XMPP-related research papers is also available at Mendeley [41]. The XMPP wiki also has a section dedicated to the Internet of Things [42].

II. BRIDGING THE SEMANTIC WEB AND XMPP NETWORKS

As was described in the previous section, the peer-to-peer-like network architecture provided by XMPP and available extensions permits the creation of secure and interoperable networks for the Internet of Things, including an architecture for provisioning with fine-grained control of who can talk to whom, who has access to what information, who can control what, and what services should be available to whom. This section will describe how this architecture can be used by semantic web applications as well.

Traditional semantic web applications are forced to use normal HTTP over TCP or TLS connections. Security is limited to HTTP-based authentication which is very coarse and difficult to implement and manage on small devices. Leaving the implementation of web security to device manufacturers furthermore increases the risk of it being completely ignored. Reutilizing the existing security framework provided by XMPP networks, where such security features as user authentication and authorization is automatically provided by the message broker, automatically provides the network with a better security model than what can be provided by normal HTTP over TCP or TLS.

The HTTP over XMPP transport extension [43] provides a mechanism to transport ordinary HTTP requests and responses over an XMPP network. Apart from supporting different HTTP versions, all HTTP methods and HTTP header semantics, it allows for various efficient encodings and transport schemes for efficient transfer of different types of data, including text, XML (allowing efficient compression if EXI is used), binary base64-encoding, chunked encoding for dynamic content, file transfer [44] for transfer of existing files, In-band byte streams [45] and Jingle [46] for different types of streaming.

It also proposes a new URI scheme: httpx for easy integration into systems and browsers using URLs to identify resources. As the Semantic Web and Linked Data are based on IRIs (IRI being a generalization of URI), the extension of the Semantic Web onto peer-to-peer-like XMPP networks is seamless.

The Clayster platform [47] has been used to build various semantic web applications in different constellations. The Clayster platform can be hosted on both Windows servers in clustered environments, or on Linux platforms using Mono [48]. The platform provides a web 3.0[1] runtime environment including a SPARQL 1.1 endpoint, web server, integrated XMPP support, pluggable Internet of Things architecture including multi-protocol support, pluggable object database and a powerful engine for 10-foot user interface [49] applications optimized for mobile phones, televisions and touch pads.

Fig. 2 shows a constellation where an application is asking a central web server running Clayster to create a report using a single federated SPARQL query. In the illustration, solid lines represent actual socket connections, and the direction of the arrow shows the direction of the connection. Dashed lines represent peer-to-peer-like communication made over the underlying XMPP network and the direction of the arrow represents the direction of the request/response-based communication. The SPARQL engine joins data together from publically available RDF(a) data sources using normal HTTP or HTTPS, but also from privately hosted RDF data sources and from the results of federated queries to private SPARQL endpoints behind firewalls. In these cases, the httpx URI scheme [43] is used. Both the private RDF source

[1] Web use the term web 3.0 as a synonym of a distributed semantic web fused with Internet of Things. The fundament of web 3.0 [52] is Linked Data.

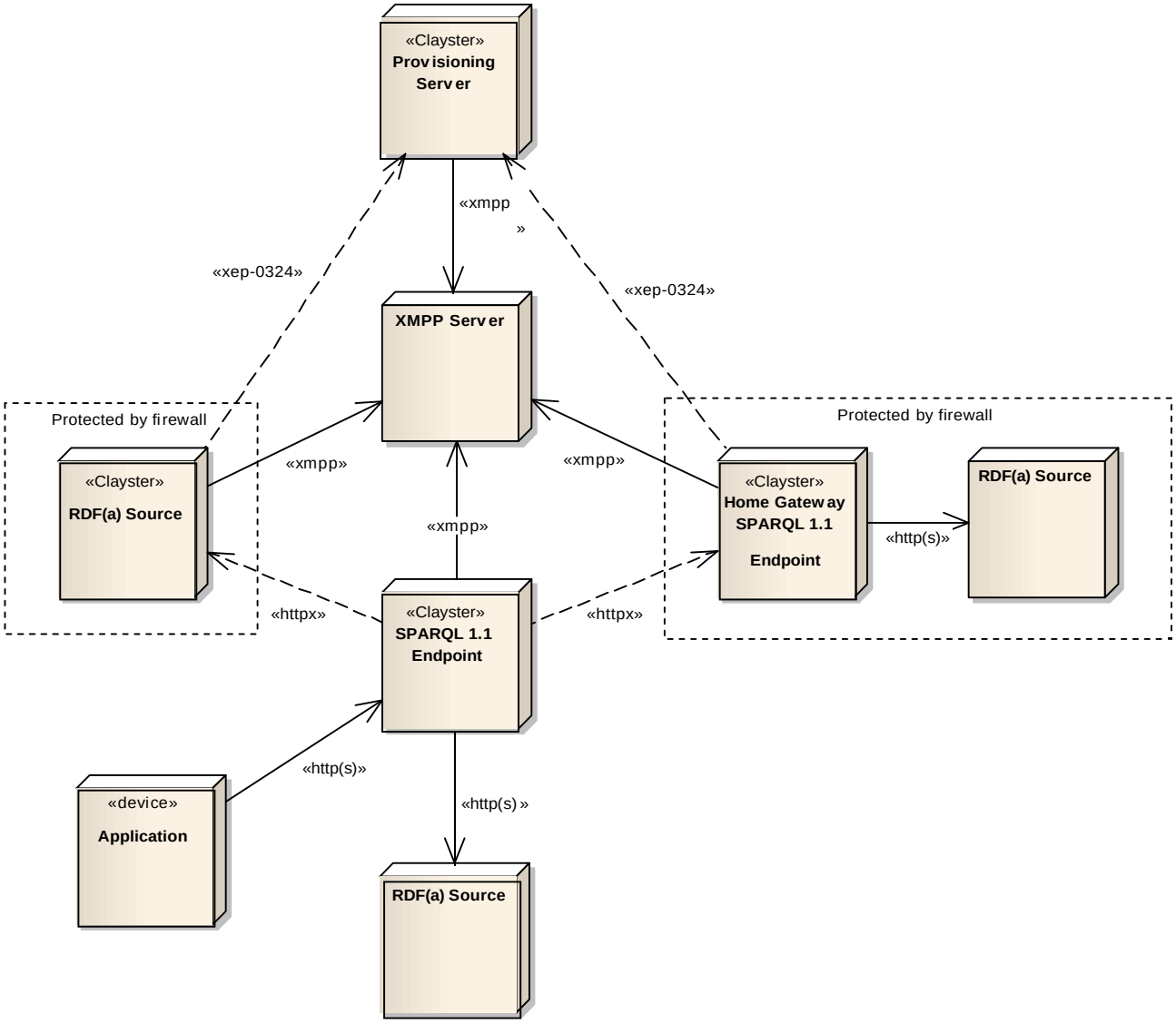


Fig. 2. Federated query accessing private information

and the private SPARQL Endpoint are hosted on separate Clayster platforms. The XMPP server acts as a guarantor that the main SPARQL endpoint can access the private data. Since XMPP is used, no holes are punched in the firewalls, and the private data remains private and is only accessible by parties with access according to the provisioning server (also hosted on the Clayster platform). The provisioning server can also provide fine-grained control of what data and from what devices the end user has the right to see.

Fig. 3 shows another constellation using the same protocols achieving a completely different application. This time, it is a web application hosted on a plug computer running the Clayster platform on Mono. Instead of hosting private information like private photos, videos, cameras at home, etc., on a web server in the cloud, the content is hosted privately on a cheap and power efficient plug computer. It is accessible as a normal web application within the boundaries of the local network protected by the firewall. But by using the httpx URI scheme the web application is available from everywhere the federated XMPP server is reachable, and only to authenticated and authorized parties. Which parties are determined by the XMPP Server and complemented by the provisioning server. The web application can also access private content in other domains by returning URL's to the content, using the httpx URI scheme itself. Examples might be a web camera in a child's room or a security camera in the home of a vacationing neighbor. The provisioning server gives added control of what can be shared with what parties. In the example above, the mobile phone would have access to all local content, sensor

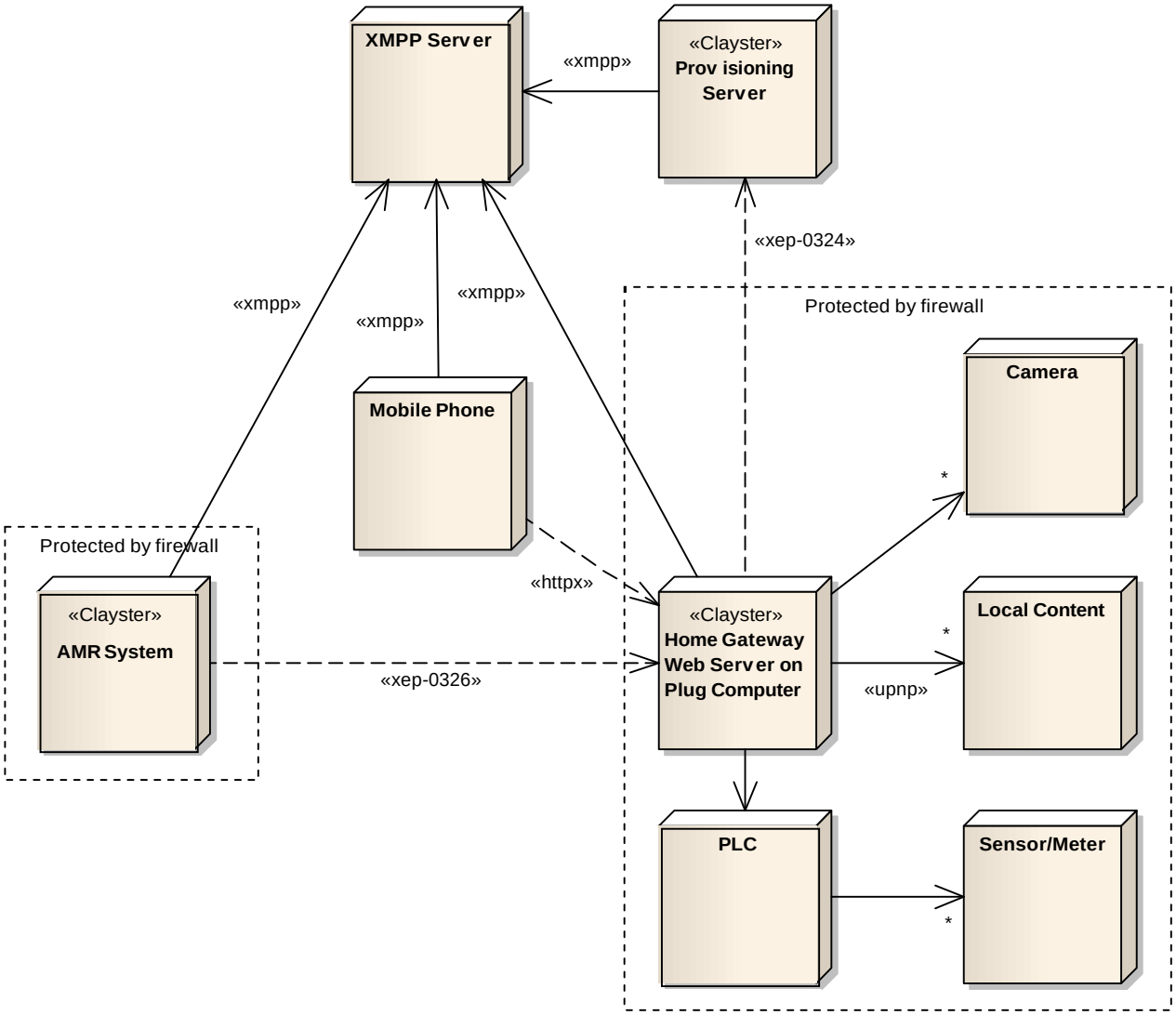


Fig. 3. Mobile phone accessing private web application

values and cameras, while an Automated Reading System would only have access to the Accumulated Energy value of given Electricity Meter, and no other sensor values.

III. CONCLUSION

Semantic web technologies provide for a very powerful set of tools to be used within the Internet of Things. Not only do semantic technologies provide a powerful abstraction of data, the technologies also resolve the problem of maintaining numerous proprietary APIs for communication with devices and/or systems from different manufacturers. Semantic web technologies also provide a standardized way to perform actions on a grid of devices as a whole, through the use of federated queries.

One of the challenges for semantic web technologies is how to solve access rights to private information, which is of paramount importance to the Internet of Things. This cannot be sufficiently solved by using the traditional HTTP model. HTTP authentication simply does not provide sufficient protection, granularity and manageability across large networks of devices with limited user interfaces. And, the use of pre-existing architectural patterns adapts poorly to the semantic web or implies huge restrictions on the Internet of Things as a concept.

The introduction of HTTP over XMPP offers a radical, yet practical solution. It permits access to HTTP resources behind firewalls without the use of unsafe firewall hole punching techniques and without publishing private and sensitive information in the cloud. It furthermore allows the end-user a simple way to control who gets access to the material. The use of provisioning servers based on published extensions of XMPP permits fine-

grained control of what data can be accessed by whom and which services they are allowed to use.

ACKNOWLEDGMENT

Financial support for this study was provided by KTC [50], Manodo [51] and Weevio [52]. The author wishes to thank Dr. Yusuke DOI, Dr. Karin Forsell, Ellis Eric Lee and Jeff Freund for their suggestions and comments on this document.

REFERENCES

[1] W3C, "Semantic Web," [Online]. Available: http://www.w3.org/standards/semanticweb/.

[2] R. Fielding, U. Irvine, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee, "RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1," June 1999. [Online]. Available: http://tools.ietf.org/html/rfc2616.

[3] W3C, "SPARQL Current Status," [Online]. Available: http://www.w3.org/standards/techs/sparql.

[4] Publish-subscribe pattern, "Wikipedia," [Online]. Available: http://en.wikipedia.org/wiki/Publish%E2%80%93subscribe_pattern. [Accessed 22 July 2013].

[5] XSF, "XMPP Standards Foundation," [Online]. Available: http://xmpp.org/.

[6] P. Millard, P. Saint-Andre and R. Meijer, "XEP-0060: Publish-Subscribe," 2002-2010. [Online]. Available: http://xmpp.org/extensions/xep-0060.html.

[7] "MQ Telemetry Transport," [Online]. Available: http://mqtt.org/.

[8] Twitter, "Developers," [Online]. Available: https://dev.twitter.com/.

[9] Wikipedia, "Representational state transfer," [Online]. Available: http://en.wikipedia.org/wiki/Representational_state_transfer. [Accessed 22 July 2013].

[10] Harvard Law, "RSS 2.0 Specification," 2003. [Online]. Available: http://cyber.law.harvard.edu/rss/rss.html. [Accessed 22 July 2013].

[11] M. Nottingham and R. Sayre, "RFC 4287: The Atom Syndication Format," December 2005. [Online]. Available: http://tools.ietf.org/html/rfc4287.

[12] Xively, "Xively cloud platform," [Online]. Available: https://xively.com/.

[13] Open.Sen.Se, "Open.Sen.Se cloud platform," [Online]. Available: http://open.sen.se/.

[14] ICS, "SicsthSense cloud platform," [Online]. Available: http://sense.sics.se/API.

[15] Wikipedia, "Internet Group management Protocol," [Online]. Available: https://en.wikipedia.org/wiki/Internet_Group_Management_Protocol. [Accessed 22 July 2013].

[16] Wikipedia, ""Simple Service Discovery Protocol," [Online]. Available: http://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol. [Accessed 22 July 2013].

[17] Universal Plug and Play Forum, "UPnP," [Online]. Available: http://www.upnp.org/.

[18] Digital Living Network Alliance, "DLNA," [Online]. Available: http://www.dlna.org/.

[19] Wikipedia, "Multicast DNS," [Online]. Available: http://en.wikipedia.org/wiki/Multicast_DNS. [Accessed 22 July 2013].

[20] Wikipedia, "Bonjour," [Online]. Available: http://en.wikipedia.org/wiki/Bonjour_(software). [Accessed 22 July 2013].

[21] P. Saint-Andre, "XEP-0174: Serverless Messaging," 2008. [Online]. Available: http://xmpp.org/extensions/ xep-0174.html.

[22] Wikipedia, "NAT traversal," [Online]. Available: http://en.wikipedia.org/wiki/NAT_traversal. [Accessed 22 July 2013].

[23] H. Moore, "Security Flaws in Universal Plug and Play: Unplug, Don't Play.," January 2013. [Online]. Available: https://community.rapid7.com/docs/DOC-2150. [Accessed 22 July 2013].

[24] "XMPP Technologies Overview," [Online]. Available: http://xmpp.org/about-xmpp/technology-overview/.

[25] "About XMPP Standards Foundation," [Online]. Available: http://xmpp.org/about-xmpp/xsf/.

[26] "XMPP Extensions," [Online]. Available: http://xmpp.org/xmpp-protocols/xmpp-extensions/.

[27] P. Waher and Y. DOI, "XEP-0322: Efficient XML Interchange (EXI) Format," 2013. [Online]. Available: http://xmpp.org/extensions/xep-0322.html.

[28] P. Waher, "XEP-0324: Internet of Things - Provisioning," 2013. [Online]. Available: http://xmpp.org/extensions/xep-0324.html.

[29] M. Miller, "End-to-End Object Encryption and Signatures for the Extensible Messaging and Presence Protocol (XMPP)," 2013. [Online]. Available: http://tools.ietf.org/html/draft-miller-xmpp-e2e-06. [Accessed 22 July 2013].

[30] P. Waher, "XEP-0323: Internet of Things – Sensor Data," 2013. [Online]. Available: http://xmpp.org/ extensions/xep-0323.html.

[31] P. Waher, "Internet of Things - Control," 2013. [Online]. Available: http://xmpp.org/extensions/xep-0325.html.

[32] P. Waher, "Internet of Things - Concentrators," 2013. [Online]. Available: http://xmpp.org/extensions/xep-0326.html.

[33] R. Klauck and M. Kirsche, "Chatty Things – Making the Internet of Things Readily Usable for the Masses with

XMPP," 2012. [Online]. Available: https://www-rnks.informatik.tu-cottbus.de/content/unrestricted/staff/mk/Publications/CollaborateCom_2012-Klauck_Kirsche.pdf.

[34] M. Krische and R. Klauck, "Unify to Bridge Gaps: Bringing XMPP into the Internet of Things," 2012. [Online]. Available: https://www-rnks.informatik.tu-cottbus.de/content/unrestricted/staff/mk/Publications/PerCom_2012-WiP-Kirsche_Klauck.pdf.

[35] "ISO/IEC/IEEE P21451-1-4 Standard for a Smart Transducer Interface for Sensors, Actuators, and Devices based on the eXtensible Messaging and Presence Protocol (XMPP) for Networked Device Communication," [Online]. Available: http://wiki.xmpp.org/web/Tech_pages/IoT_Sensei. [Accessed 22 July 2013].

[36] KTC, ”KTC tar klivet in i den digitala tidsåldern för fastighetsautomation,” 2013. [Online]. Available: http://www.ktc.se/2013/06/ktc-tar-klivet-in-i-den- digitala-tidsaldern-for-fastighetsautomation/. [Använd 22 July 2013].

[37] KTC, ”KTC förbinder sig till att skydda sina kunders och deras kunders data,” 2013. [Online]. Available: http://www.ktc.se/2013/07/ktc-forbinder-sig-till-att- skydda-sina-kunders-och-deras-kunders-data/. [Använd 22 July 2013].

[38] SUST, "Intelligent Energy Services," [Online]. Available: http://iea.sust.se/. [Accessed 22 July 2013].

[39] SUST, ”Kommunikationsstandarder för energieffektivisering i Almedalen,” 2013. [Online]. Available: http://www.ktc.se/2013/06/kommunikationsstandarder-for-energieffektivisering-i-almedalen/. [Använd 22 July 2013].

[40] P. Waher, "Proto-XEP: Internet of Things – Interoperability," 2013. [Online]. Available: http://htmlpreview.github.io/?https://github.com/joachimlindborg/XMPP-IoT/blob/master/xep-0000-IoT-Interoperability.html. [Accessed 22 July 2013].

[41] "XMPP research paper repository at Mendeley," [Online]. Available: http://www.mendeley.com/groups/3516891/xmpp/.

[42] wiki.xmpp.org, "Tech pages/IoT systems," [Online]. Available: http://wiki.xmpp.org/web/Tech_pages/IoT_systems. [Accessed 22 July 2013].

[43] P. Waher, "XEP-0332: HTTP over XMPP transport," 2013. [Online]. Available: http://xmpp.org/extensions/ xep-0332.html.

[44] T. Muldowney, M. Miller, R. Eatmon and P. Saint- Andre, "XEP-0096: SI FileTransfer," 2004. [Online]. Available: http://xmpp.org/extensions/xep-0096.html.

[45] J. Karneges and P. Saint-Andre, "XEP-0047: In-Band Bytestreams," 2012. [Online]. Available: http://xmpp.org/extensions/xep-0047.html.

[46] S. Ludwig, J. Beda, P. Saint-Andre, R. McQueen, S. Egan and J. Hildebrand, "XEP-0166: Jingle," 2009. [Online]. Available: http://xmpp.org/extensions/xep- 0166.html.

[47] "Clayster platform," [Online]. Available: http://clayster.com/.

[48] "The mono project," [Online]. Available: http://www.mono-project.com/.

[49] Wikipedia, "10-foot user interface," [Online]. Available: http://en.wikipedia.org/wiki/10-foot_user_interface. [Accessed 22 July 2013]. [50] ”KTC,” [Online]. Available: http://www.ktc.se/.

[51] "Manodo," [Online]. Available: http://www.manodo.se/.

[52] "Weevio AMR," [Online]. Available: http://weevio.com/.

[53] Wikipedia, "Semantic Web & Web 3.0," [Online]. Available: http://en.wikipedia.org/wiki/Semantic_Web# Web_3.0. [Accessed 22 July 2013].

Peter Waher was born in Stockholm, Sweden, in 1971. He studied mathematics at Stockholm University between 1990 and 1993, specializing in abstract algebra and computer algebra.

From 1988 to 1994 he worked in the computer games industry developing games and graphics engines for various platforms. Since 1994 he has been working with machine-to-machine communications, sensor networks and Internet of Things. He is a co-founder of Clayster, a company developing technology and IoT & Smart City application platform that it licenses to its partners. He currently works in Valparaíso, Chile, where he promotes IoT and www 3.0 in South America. As a member of XMPP standards foundation he is the author of seven published XMPP extensions, and holds two patents.

Mr. Waher is member of ISO/IEC/IEEE P21451 “Standard for Smart Transducer Interface for Sensors and Actuators” (“Sensei/IoT”) where he works in the P21451-1-4 subgroup “eXtensible Messaging and Presence Protocol (XMPP) for Networked Device Communication” creating standards for communication over XMPP. Mr. Waher is also the recipient of the Living Labs Global Showcase award 2010 for his involvement in the development of the service “Energy Saving through Smart Applications”.

APPENDIX C: ACRONYMS/ABBREVIATIONS

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
BPM	Business Process Model
BYOD	Bring Your Own Device
CAER	Center for Advanced Engineering and Research
DCS	Distributed Control Systems
DEFT	DETER-Enabled Federation of Testbeds
DETER	Cyber-Defense Technology Experimental Research
DHS	Department of Homeland Security
DNP3/SAv5	Distributed Network Protocol with Secure Authentication Version 5
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
EPRI	Electric Power Research Institute
FISMA	Federal Information Security Management Act
HART	Highway Addressable Remote Transducer Protocol
HMI	Human-Machine Interface
HVAC	heating, ventilating, and air conditioning
HW	Hardware
ICCP	Inter Control Center Communication Protocol
ICS	Industrial Control Systems
ICS-CERT	ICS Cyber Emergency Response Team
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange, protocol used to set up a security association
INL	Idaho National Laboratory
IP	Internet Protocol
IPSEC	Internet Protocol Security, a protocol suite for securing IP communications
IPUG	Information Providers Users Group
ISA	International Society of Automation
IT	Information Technology
JCTD	DOD Joint Capabilities Technology Demonstration
JPL	Jet Propulsion Laboratory
L2TP	Layer Two (2) Tunneling Protocol (supports virtual networks)

LAN	local area network
LDAP	Lightweight Directory Access Protocol
MMS	Multi-media Messaging Service
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OE	Office of Electricity Delivery and Energy Reliability (DOE)
OPC	Object Linking and Embedding (OLE) for Process Control
OS	Operating System
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
R&D	Research and Development
ROI	Return on Investment
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Control Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SPIDERS	Smart Power Infrastructure Demonstration for Energy Reliability and Security
SSH	Secure Shell
SysML	Systems Modeling Language
TACACS	Terminal Access Controller Access-Control System
TCIPG	Trustworthy Cyber Infrastructure for the Power Grid
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide-Area Network