Research Article

Cyberphysical Security for Industrial Control Systems Based on Wireless Sensor Networks

Tianbo Lu, Xiaobo Guo, Yang Li, Yong Peng, Xiaoyan Zhang, Feng Xie, and Yang Gao

1 School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
2 Information Technology Research Base of Civil Aviation Administration of China, Civil Aviation University of China, Tianjin 300300, China
3 Technical Evaluation Laboratory, China Information Technology Security Evaluation Center, Beijing 100085, China

Correspondence should be addressed to Tianbo Lu; lutb@bupt.edu.cn and Xiaobo Guo; gxbbest@126.com

Received 28 February 2014; Accepted 9 May 2014; Published 26 June 2014

Academic Editor: Tai-hoon Kim

Copyright © 2014 Tianbo Lu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In recent years, the security of cyberphysical system (CPS) has been focused on increasingly. The most common example of CPS is industrial control system (ICS), which is prevalent in almost every critical infrastructure, such as electricity, oil and gas, water, chemical processing, and healthcare. So ICS security has become a top priority in the security field. Based on a general description of the wireless sensor network (WSN), which is an important element of CPS, this paper first gives a comprehensive and deep understanding of CPS. Secondly, it provides a comprehensive description of the current situation of ICS security in the U.S. and the corresponding approaches the U.S. government and some industries have taken, including management, technology, standards and regulations, and researches of national laboratories. Thirdly, the paper shows the research on ICS in Europe, focusing on the most important report issued by ENISA. Then, compared with developed countries, it presents the grim situation of ICS security and describes the efforts of ICS security management in China.

1. Introduction

A cyberphysical system (CPS) is a system of systems, in which the cyber technologies and the physical processes are highly integrated, in order to add new capabilities into physical system. It is an emerging area in the 21st century, as most of the world’s leading economies are seeking competitiveness in this field. U.S. President’s Council of Advisors on Science and Technology (PCAST) in a report [1] found that cyberphysical systems “are now a national priority for Federal R&D. Improved methods are needed for the efficient development of these systems. These methods must assure high levels of reliability, safety, security, and usability.”

The implementation of CPS is largely dependent on the wireless sensor networks (WSNs), as it can help collect huge amount of data from the physical world and transmit in-time control command from the cyberworld. It is because of the use of WSNs that CPS can make correct perception of the physical world and real-time reaction to its changes. A typical WSN is usually deployed in the interior or in the neighboring of the being-detected objects. The node of WSN consists of a sensing unit (including a sensor and an analog to digital converter), a processing unit, a transceiver unit, and a power unit [2]. Many single nodes can build a multiple-hop network in a self-organized way, through an initial wireless communication and consultation. As shown in Figure 1, each WSN is equipped with a gateway connected to a transmission network, which is a made up of a series of wireless network nodes. Through this pathway, the sensed data can be sent from the sensing area to the sink, which has the function of remote access and data processing. Then, the sink will carry on bulk data transfer to the database or control center, with the use of local gateway which is connected to various networks [3].

CPS attaches more importance to timely perception, deep interaction, smart processing, and real-time reaction, compared with traditional wireless sensor networks. As shown in
Figure 2, CPS Unit, in which there can be many CPS nodes connected wirelessly, is an individual divided by different tasks and different CPS Units could exchange information with each other to acquire a more clear cognition. Each CPS Unit timely perceives changes in the environment through the sensor function, makes an analysis on the data through the processing function, then exchanges information with the other CPS Units through the communication function, and finally realizes the information fusion to acquire a correct and comprehensive understanding of the environment. In some relatively simple conditions, the CPS Units could make decisions by themselves according to the information between different units and could make the execution command locally. In other conditions, the CPS Units need to transmit the fused information to the remote smart control center to acquire a more comprehensive and complex process and a real-time decision according to the cognition and rules mastered by the system, and after this the execution command will be transmitted to all the related CPS Units to respond to the changes in the physical world. The whole procedure, full of feedback, is real-time and the process of perception, communication, computing, and execution is in a closed circuit. In this way, a virtuous circle of timely feedback and decision-making can be obtained.

According to the above, WSN is the medium of the interaction between cyberworld and physical world, which achieves real-time information collection and input from the physical world to the cyberworld and real-time decision output from the cyberlayer to the physical layer. Comparing with WSN, we can draw a deep understanding of CPS from the following aspects:

(i) Physical Components. There is a big limitation to the energy, storage space, and computing capacity of the WSN nodes, so only simple operations could be carried out in the nodes and most analysis tasks are finished in the control center. However, in CPS, many decisions could be made in physical layer by the CPS Units as the interaction between the CPS Units and the CPS nodes in each unit and their relatively strong computing and communication capabilities.

(ii) Resource Allocation. As sensors are usually deployed in unmanned area or in harsh environment, the continuous use of resources becomes a big problem for both WSN and CPS. WSN aims to save the energy by only providing some limited functions; actually, it is to acquire a longer use time at the cost of reducing the intelligence and it just gives little attention to resource allocation [4]. However, CPS aims at how to finish the tasks with limited resources via a reasonable resource allocation. All resources could be dynamically reorganized and reconfigured according to different demands of different tasks; for example, different sensor groups may be in work status or sleep mode according to different tasks.
(iii) Network Convergence. The physical devices connected to WSN have to be within many rules to ensure a certain degree of connectivity and aggregation of the collected data [5]. However, CPS could be connected to many different WSNs and different devices, compatible with different standards and protocols, and able to dispose of collected data with different connectivity and aggregation.

(iv) Time Delay. In the traditional WSN, because of limited computing capacity and little interaction between nodes, the collected data which is transmitted to the control center is always in its relatively original status. The control center needs to make a comprehensive analysis on all the original data, so it always takes an obvious time delay before the device obtains the decision of what to do next [6]. As for CPS, each connected CPS Unit has a relatively strong computing and communication capacity, which allows it to share some tasks with the control center. In this way, a correct understanding of the environment and a quick feedback can be achieved. In a word, the whole CPS was involved in the calculation and procession of data, reducing the delay and ensuring a real-time reaction to the changes in the physical world.

In a word, CPS is an intelligent large-scale integration control system, which achieves a seamless fusion of the cyberworld and the physical world, with the adaptability to respond to the uncertain changes in the environment. Though the theory of WSN greatly contributes to the implementation of CPS, it brings data security challenges at the same time, such as availability, authorization, authentication, confidentiality, integrity, nonrepudiation, freshness, forward secrecy, backward secrecy, and location awareness [7], because of the widespread invisible wireless communication, unrestricted

![Diagram of a CPS framework based on WSN.](image)
large-scale deployment, and the increasingly powerful computing and storage capacities [8]. From the perspective of information security, bad information detecting [9] in wireless network can be a new research field, and the theory of protecting user privacy in phone protector [10] may be available for reference. As CPS is a "system of systems" and its popularity is increasing rapidly, interconnections of CPS are growing in size, complexity, and vulnerability. Uncontrolled CPS risk will definitely not only bring significant damages to our economy but also cause great threat to the life of human beings. The most common example of CPS is the industrial control system (ICS), which is prevalent in almost every critical infrastructure, including electricity, oil and gas, water, chemical processing, and healthcare [11].

Studying the strategies and programs taken worldwide will help sort out the best practices of ICS security. As the ICS is touching the nerves of almost every critical economy entity around the world, many counties have taken efforts to cope with the risks. However, each country has its own distinct basic condition or state and their approaches towards ICS security will never be completely the same. The world's leading economies, such as the United States, Europe, and China, walk in the forefront of the world ICS security. This paper explicitly studies the research trend in the fields of management, technology, and standards and makes a comprehensive analysis on the status quo of ICS security researches in those countries.

This paper is organized as follows: Section 1 gives an overview of cyberphysical system, based on a general description on WSN and a brief introduction to ICS. Section 2 presents the details of ICS and lists some serious ICS security incidents to show that it is easier to launch attacks in ICS and the impacts of the attacks are widened. Section 3 describes the relatively complete information security management system and technical system of ICS in the United States from four dimensions, that is, ICS management system, technology and research, emergency readiness, and standards and regulations. Section 4 shows some important measures of European countries to improve the security, safety, and resilience of European ICS systems. Section 5 presents that the ICS in China is facing a more severe situation, compared with developed countries, and that the government and correlated industries have attached great attempt to improve the security of ICS.

2. Industrial Control System

ICS are typically used in industries such as electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). These control systems are often highly interconnected and mutually dependent systems and they are always critical to those industries. The most common types of ICS include SCADA (supervisory control and data acquisition), DCS (data communication system), and PLC (programmable logic controller).

(i) SCADA is generally used to control dispersed assets using centralized data acquisition and supervisory control [12].
(ii) DCS is generally used to control production systems within a local area such as a factory using supervisory and regulatory control [13].
(iii) PLC is generally used for discrete control for specific applications and provides regulatory control [14].

ICS used to be isolated systems as they are only applied to specific industries or specific areas [15]. So, the software and hardware of ICS, including those protocols about them, are customized for each application. However, the widely spread Internet Protocol provides a possibility to integrate the already existing systems to form a more interconnected one in order to add new capabilities, such as remote access and business corporation into the traditional systems. It is a trend to use standard communication protocols, operating systems, and computing devices designed for compatibility [16]. ICS is becoming more and more interconnected and accessible through public network, which has introduced a greater risk.

In the past, the SCADA in ICS were independent systems with no connections to other systems, while, at present, ICS is widely distributed and networked since the systems are dependent on open protocols of the internet, which makes it vulnerable to a lot of external remote threats [17]. As new IT related capabilities are added, ICS is no longer isolated from the outside world, compared with the predecessor systems, posing a greater risk to its security. According to a 2010 report [18], named “Security Incidents Rise in Industrial Control Systems,” only 10 percent of industrial control systems are actually connected to the Internet, while there are a growing number of cybersecurity incidents from 2005 to 2010 in the ICS of water, wastewater, and utility power plants. Therefore, there is an urgent need of ICS security measures which not only have to cope with the already known IT related vulnerabilities but also should be designed for specific ICS needs. Coupled cybersecurity threats appear in many complex forms, including physical damage, data tampering, sensor spoofing, code injection, cyberintrusion, theft, and vandalism. To date, very little work has been done to ensure the cyberphysical security of such systems deployed in unstructured, potentially adversarial environments.

In recent years, security incidents of ICS have emerged constantly in many areas. Table 1 shows some main ICS security accidents. With the popularity of the ICS and the development of intelligent and networked trend of ICS, the harm is increasingly worsening. We can see from the list that the number of incidents is increasing these years. As the ICS is becoming larger and more interconnected, it is easier to launch attacks and the impacts of the attacks are widened. As the ICS is touching the nerves of almost every critical economy entity around the world, many counties have taken efforts to cope with the risks.

3. ICS Security in the United States

From a global perspective, the United States is in the forefront of the world in the field of safety and security of ICS. As the
### Table 1: ICS incidents.

| Date  | Location         | Details                                                                                                                                                                                                 |
|-------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2013  | South Korea and Japan | Icefog is a small yet energetic APT group, who maintain a foothold in corporate and governmental networks to smuggle out sensitive information. |
| 2012  | Global incident  | Elderwood attack, spear phishing emails, watering hole, and zero-day exploits are always used.                                                                                                       |
| 2012  | Middle East      | Flame is being used for targeted cyberespionage in Middle Eastern countries.                                                                                                                           |
| 2011  | Global incident  | Duqu virus was found, a complex attack tool specifically for critical infrastructure.                                                                                                               |
| 2011  | U.S.             | Hackers attacked the control systems of water supply facilities in Illinois.                                                                                                                             |
| 2011  | Japan            | Hackers invaded the control and management system of Shinkansen in Japan.                                                                                                                               |
| 2010  | Global incident  | Stuxnet virus was found. Iran is the most serious that the generation of its nuclear power plant was delayed.                                                                                               |
| 2008  | Poland           | Juvenile attacked the suburban railway system in Lodz, Poland                                                                                                                                             |
| 2007  | Canada           | Attacker invaded one Canada's Water SCADA control system and destroyed the control computer system.                                                                                                      |
| 2006  | U.S.             | Hackers invaded the systems of the sewage treatment plant in Harrisburg, Pennsylvania.                                                                                                               |
| 2005  | U.S.             | Zotob worm was found in the automobile corporate network and control network.                                                                                                                            |
| 2003  | U.S.             | Teenager invaded the computer system of Houston Ferry.                                                                                                                                                   |
| 2003  | U.S.             | Worm was found in the control network of Davis-Besse nuclear power plant.                                                                                                                              |
| 2001  | U.S.             | Hacker invaded the control system of electricity transmission system in California.                                                                                                                      |
| 2000  | Russia           | Hacker had controlled the largest natural gas pipeline network in the world on the part of Gazprom.                                                                                                |
| 1997  | U.S.             | Teenage boy invaded (New York) NYNES system.                                                                                                                                                           |
| 1994  | U.S.             | Hacker invaded the Salt River Project in Arizona.                                                                                                                                                       |
| 1992  | U.S.             | Former employee of Chevron closed the emergency alarm systems located in 22 states.                                                                                                                       |

As early as 2002, the U.S. government attached great importance to ICS security. And, in the last decade, a lot of work has been done in ICS security management. Now, a complete information security management system and technical system of ICS have been established. In terms of the information security research of ICS, the U.S. focuses on petrochemical, power, and energy industry; and, in terms of management system, technical systems, and standards and regulations, the U.S. Department of Homeland Security (DHS), Department of Energy (DOE), and National Laboratory jointly promote industrial control system information security in the United States.

#### 3.1 ICS Management System

The U.S. developed special programs in the field of ICS information security, mainly led, respectively, by the Department of Homeland Security and Department of Energy. There has been significant development in SCADA systems in the electric sector, and noteworthy progress has been made in identifying and mitigating vulnerabilities under the sponsorship of the Department of Energy.

In 2004, the Department of Energy and the Department of Homeland Security established two multiyear programs to protect the nation's infrastructures against attacks from hackers, virus writers, disgruntled employees, terrorist organizations, and nation states. National Supervisory Control and Data Acquisition (SCADA) Test Bed was funded by the Department of Energy (Office of Electricity Delivery and Energy Reliability, DOE-OE) to provide real test environment to systematically analyze, test, and improve cybersecurity features for a variety of ICS and help the industry and government assess vulnerability of the ICS and test the security of the hardware and software in ICS [19]. Control Systems Security Center was funded by the Department of Homeland Security (National Cyber Security Division, NCSD) to identify and develop solutions to protect vital infrastructures from a cyberattack. The center provides a centralized location for vulnerability assessment, tool development, research, and incident response to eliminate all the ICS security risks in critical infrastructure and key resources sectors. Both programs are key efforts in response to President Bush's National Strategy to Secure Cyberspace [20] and employ experts in control systems operation, design, cybersecurity, and risk analysis. State-of-the-art research and testing facilities enable the running of mock exercises and calculated scenarios on full-scale control systems. The testing results provide the owners and manufactures of the facilities with necessary data to improve cybersecurity standards within their control systems. At the same time, the Department of Homeland Security and the Department of Energy developed the ICS security roadmap. Since 2005, they began to cooperate with Energy Infrastructure Protection Division of Natural Resources Canada and completed Roadmap to Secure Control Systems in the Energy Sector (2006) [21]. This roadmap provides a common vision and strategic framework for the government, research institutions, and universities to develop, deploy, and maintain control system to survive...
under the intended cyberattacks and without losing critical capabilities.

Later, in 2011, they update the roadmap with Roadmap to Achieve Energy Delivery Systems Cybersecurity (2011) [22] in “Changing landscape,” “building on success and addressing gaps,” “advancing threat capabilities,” and “emphasizing a culture of security.” Table 2 gives an insight of the roadmap and Table 3 attaches the projects or efforts made by the industries and government. Among the leading organizations, six national laboratories in the United States launched a systematic and comprehensive study on ICS, covering the ICS security standards, protocol development, research on industrial control security threat and vulnerability, research and development of security control technology, and so forth. They provide strong support for the U.S. security management of ICS.

(i) Idaho National Laboratory (INL). INL was established in 1949, located in Idaho, and under the U.S. Department of Energy. The lab has provided 60 years of national security service for customers including DOD (the Department of Defense of the United States), DHS, DOE, and industry. The lab’s 890-square-mile site includes a utility-scale power grid, explosives range, wireless test bed, nuclear reactors, hot cells, and fuel treatment facilities. INL offers malware laboratory, focusing on analysis of the Stuxnet virus. INL has high-class capacity in vulnerability identification and vulnerability mitigation of ICS and has been internationally recognized. Backed by the U.S. Department of Energy and the Department of Homeland Security, the Idaho National Laboratory began to establish the Critical Infrastructure Test Range (CITR) in 2003 and officially put it into operation in 2005, which includes the National SCADA Test bed and the Electric Grid Test bed. This laid a good foundation for the smooth development of ICS security.

INL’s SCADA Security Center in the auspices of the Department of Energy presided over the National SCADA Test Bed (NSTB) Program, which was started in 2003. NSTB has now completed the assessment of control systems and components and network vulnerability for 37 organizations, including assessment of control system components for 14 organizations and assessment of control system for 15 organizations, as well as on-site assessment of infrastructure system for 8 organizations.

INL assists the Department of Homeland Security to develop self-assessment tools for the control system network security and train on the control system network security. INL has issued a series of industrial control security related research reports, including “The Control System Network Security Assessment Methods” (2005) [23], “The Control System Network Security: Defense Strategy in Depth” (2007) [24], and “Common Network Security Vulnerabilities in the Assessment of Control Systems” (2008) [25]. Its current research focuses on tool suite for sensing situation of control system.

(ii) Sandia National Laboratories (SNL). SNL was established in 1949 under the U.S. Department of Energy, with the specific research direction on infrastructure, specifically the SCADA system security research and global critical energy infrastructure protection.

In the course of fulfilling its national security mission over more than 50 years, Sandia has developed deep expertise in protecting critical infrastructure. Sandia National Laboratories and Los Alamos National Laboratory (LANL) are the prime contractors for National Infrastructure Simulation and Analysis Center (NISAC) and they integrate the two laboratories’ expertise in the modeling and simulation of complex systems for evaluating national preparedness and security issues. NISAC is a modeling, simulation, and analysis program that prepares and shares analyses on critical infrastructure and key resources including their interdependencies, vulnerabilities, consequences of disruption, and other complexities. NISAC is under the direction of the Department of Homeland Security.

The SNL set up the SCADA laboratories and research center to research the security of the SCADA system. SCADA focuses on analysis of vulnerabilities in the SCADA system and components to support highly assured SCADA system. The SCADA security research center consists of several test facilities, which can implement mold design, simulation, and verification of critical infrastructure. The research center focuses on security of the current control system and the development of next generation control system. The study of SCADA security research center includes SCADA assessment and SCADA engineering solutions.

The SNL has many research results in ICS security, encompassing the assessment, framework, indicators, and protocols of ICS security. And it has published “Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment” [26], “Security Framework for Control System Data Classification and Protection” [27], “Security Metrics for Process Control Systems” [28], and “Secure ICCP Integration Considerations and Recommendations” [29].

SNL currently focuses on the development of trust anchor (an independent testing and control equipment) and has carried out the program on protecting life cycle of the process control system from attack with the use of the trust anchor. SNL provides a diverse range of services from supplying basic necessities, such as power and water, to ensuring the information foundation for our economy. The systems, facilities, and functions that make up our nation’s critical infrastructure are essential to our vitality, security, and quality of life and ensuring the smooth operation of the sophisticated and highly interdependent components of critical infrastructures is a crucial but complex challenge, especially in face of today’s troubling threats.

(iii) Oak Ridge National Laboratory (ORNL). ORNL is a large national laboratory under the U.S. Department of Energy, established in 1943, and has been comanaged by the University of Tennessee and Battelle Memorial Institute since April 2000.

ORNL’s scientific programs focus on materials, neutron science, energy, high-performance computing, systems biology, and national security. ORNL is currently undergoing the testing research on network security of SCADA system through portable acceptance tester and protocol. Meanwhile,
| Strategies | Near-term Milestones | Mid-term Milestones | (3) Develop and implement new protective measures to reduce risk (2.1) Common terms and measures specific to each energy subsector available for base lining security posture in operational settings [1] [3] [14] [16] [17] [18] [19] [20] (1.1) Executive engagement and support of cyberresilience efforts [1] [2] (1.2) Industry-driven safe code development and software assurance awareness workforce training campaign launched [3] (1.3) Vendor systems and components using sophisticated secure coding and software assurance practices widely available [4] [5] [6] [7] [8] (1.4) Field-proven best practices for energy delivery systems security widely employed [2] [9] [10] [11] [12] [13] [14] (1.5) Compelling business case developed for investment in energy delivery systems security [1] [3] (2.2) Most of asset owners assess their security posture, with the use of specific metrics of energy subsectors [14] [17] [19] (2.1) Common terms and measures specific to each energy subsector available for base lining security posture in operational settings [1] [3] [14] [16] [17] [18] [19] [20] (2.2) Most of asset owners assess their security posture, with the use of specific metrics of energy subsectors [14] [17] [19] (2.3) Scalable access control for all energy delivery system devices available [5] [30] [35] [38] [42] [39] [43] [44] (3.3) Next generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented [24] [25] [30] [31] [35] [39] [40] [42] [43] [45] [46] [47] [48] [49] [50] [51] [52] [56] [58] [59] (3.2) Scalable access control for all energy delivery system devices available [5] [30] [35] [38] [42] [39] [43] [44] (3.2) Scalable access control for all energy delivery system devices available [5] [30] [35] [38] [42] [39] [43] [44] (3.3) Next generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented [24] [25] [30] [31] [35] [39] [40] [42] [43] [45] [46] [47] [48] [49] [50] [51] [52] [56] [58] [59] (4.1) Tools to identify cyberthreats across all levels of energy delivery system networks commercially available [36] [35] [24] [40] [21] [57] [50] [32] [55] [58] [59] [37] [32] [23] [28] (4.3) Incident reporting guidelines accepted and implemented by each energy subsector [14] (4.2) Tools to support and implement cyberattack response decision making for the human operator commercially available [38] [26] [24] [25] [27] [40] [21] [42] [59] [41] [53] [34] [22] [23] [28] (4.4) Real-time forensics capabilities commercially available [32] [58] [22] (4.5) Cyberevent detection tools that evolve with the dynamic threat landscape commercially available [9] [58] [60] [41] (5.1) Cyberthreats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders [10] [6] (5.2) Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems (5.3) Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners [2] [11] [15] [39] (5.4) Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining (5.5) Sustainability of energy delivery systems security widely employed [12] [13] [14] |
| Strategies            | (1) Build a culture of security | (2) Assess and monitor risk | (3) Develop and implement new protective measures to reduce risk | (4) Manage incidents | (5) Sustain security improvements |
|-----------------------|---------------------------------|----------------------------|---------------------------------------------------------------|----------------------|----------------------------------|
| **Long-term Milestones** | (1.6) Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry [15] | (2.3) Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyberphysical domains commercially available [1] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] | (3.4) Self-configuring energy delivery system network architectures widely available [21] [38] [42] [53] [54] | (4.6) Lessons learned from cyberincidents shared and implemented throughout the energy sector [3] | (5.5) Private sector investment surpasses federal investment in developing cyber security solutions for energy delivery systems |
| | | | (3.5) Capabilities that enable security solutions to continue operation during a cyberattack available as upgrades and built-in to new security solutions [9] [38] [26] [42] [27] [30] [57] | | (4.7) Capabilities for automated response to cyberincidents, including best practices for implementing these capabilities available [9] [38] [57] [55] [29] |
| | | | (3.6) Next generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented [11] [51] [54] [39] | | (5.6) Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector |
Table 3: The projects and efforts in the roadmap.

| Project number | Project description                                                      | Lead organization                                                                 |
|----------------|-------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| [1]            | Electricity Subsector Cybersecurity Risk Management Process              | U.S. Department of Energy Office of Electricity Delivery and Energy Reliability    |
| [2]            | Securing the Smart Grid: Best Practices in Security, Integrity, and Resilience | U.S. Resilience Project                                                            |
| [3]            | Secure Coding for Energy Delivery Systems                                | Pacific Northwest National Laboratory                                             |
| [4]            | Automated Vulnerability Detection for Compiled Smart Grid Software      | Oak Ridge National Laboratory                                                     |
| [5]            | High-Level Language Microcontroller Implementation                      | Idaho National Laboratory                                                         |
| [6]            | Programmable Logic Controller (PLC) Component Analysis                  | Sandia National Laboratories                                                      |
| [7]            | Source Code Analysis and Conformance Testing                            | Software Engineering Institute                                                    |
| [8]            | Formal Methods for Programmable Logic Controller (PLC) Logic Verification | Sandia National Laboratories                                                      |
| [9]            | Field Device Management                                                 | Pacific Northwest National Laboratory                                             |
| [10]           | Advanced Metering Infrastructure (AMI) ZigBee Home Area Gateway Assessment | Sandia National Laboratories                                                      |
| [11]           | Trustworthy Wireless for Critical Infrastructure Sites                  | Trustworthy Cyber Infrastructure for the Power Grid                               |
| [12]           | Advanced Security Acceleration Project for Smart Grid (ASAP SG)         | Oak Ridge National Laboratory                                                     |
| [13]           | 2011 NERC Grid Security Exercises (GridEx)                              | North American Electric Reliability Corporation                                   |
| [14]           | Usable Management Tools for the Smarter Grid's Data Avalanche           | Trustworthy Cyber Infrastructure for the Power Grid                               |
| [15]           | SCADA Security Training Workshops                                       | Idaho National Laboratory                                                         |
| [16]           | Electric Vehicle Battery Charger Vulnerability Analysis                | Idaho National Laboratory                                                         |
| [17]           | Cyber-Physical Survivability Metrics-Quantifying the Survivability Properties of Intelligent Energy Delivery Systems | Software Engineering Institute                                                    |
| [18]           | Dynamic Analysis of Mobile Device Applications                          | Idaho National Laboratory                                                         |
| [19]           | PMU Data Quality                                                        | Trustworthy Cyber Infrastructure for the Power Grid                               |
| [20]           | Test Bed Control System Assessments                                     | Idaho National Laboratory                                                         |
| [21]           | Application of Cyber Security Techniques in the Protection of Efficient Cyber-Physical Energy Generation Systems | Lawrence Berkeley National Laboratory                                             |
| [22]           | Assessment and Forensics for Large-Scale Smart Grid Networks            | Trustworthy Cyber Infrastructure for the Power Grid                               |
| [23]           | Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector | Pacific Northwest National Laboratory                                             |
| [24]           | Control System Situational Awareness Technology                         | Idaho National Laboratory                                                         |
| [25]           | Control System Situational Awareness Technology: Data Fusion            | Idaho National Laboratory                                                         |
| [26]           | Control System Situational Awareness Technology: Intelligent Cyber Sensor | Idaho National Laboratory                                                         |
| [27]           | Control System Situational Awareness Technology: Sophia Tool            | Idaho National Laboratory                                                         |
| [28]           | Development and Demonstration of a Security Core Component              | Siemens Energy                                                                    |
| [29]           | Game-Theoretic Intrusion Response and Recovery Engine                   | Trustworthy Cyber Infrastructure for the Power Grid                               |
| [30]           | Grid Security with Quantum Architectures and Resources (Grid SQuARe)   | Oak Ridge National Laboratory                                                     |
| [31]           | GridStat Middleware Communication Framework: Application Requirements   | Trustworthy Cyber Infrastructure for the Power Grid                               |
| [32]           | Host Event Based Network Monitoring                                     | Idaho National Laboratory                                                         |
| [33]           | Implications of Design Basis Threat (DBT) on Critical Infrastructure Protection and Homeland Security | Pacific Northwest National Laboratory                                             |
| [34]           | Lossless Compression of Synchronized Measurement Unit Archives          | Trustworthy Cyber Infrastructure for the Power Grid                               |
| [35]           | Padlock Project                                                         | Schweitzer Engineering Laboratories                                               |
| [36]           | Programmable Logic Controller (PLC) Integrity Checking                 | Sandia National Laboratories                                                      |
| [37]           | Specification-based Intrusion Detection System for Smart Meters        | Trustworthy Cyber Infrastructure for the Power Grid                               |
| [38]           | State Aware Database Systems                                            | Trustworthy Cyber Infrastructure for the Power Grid                               |
| Project number | Project description                                                                 | Lead organization                                      |
|----------------|-------------------------------------------------------------------------------------|-------------------------------------------------------|
| [39]           | Testbed Initiatives                                                                  | Trustworthy Cyber Infrastructure for the Power Grid    |
| [40]           | Trust Anchors                                                                        | Sandia National Laboratories                           |
| [41]           | Trustworthiness Enhancement Tools for SCADA Software and Platforms                   | Trustworthy Cyber Infrastructure for the Power Grid    |
| [42]           | GridStat Middleware Communication Framework: Management Security and Trust            | Trustworthy Cyber Infrastructure for the Power Grid    |
| [43]           | Password Changing Protocol                                                            | Trustworthy Cyber Infrastructure for the Power Grid    |
| [44]           | RBAC Driven Least Privilege Architecture for Control Systems                          | Honeywell International                                |
| [45]           | IEC 61850 Cybersecurity Acceleration R & D                                          | Pacific Northwest National Laboratory                  |
| [46]           | Secure SCADA Communications Protocol (SSCP) Commercialization                        | Pacific Northwest National Laboratory                  |
| [47]           | SIEGate                                                                              | Grid Protection Alliance                               |
| [48]           | Tools and Methods for Hardening Communication Security of Energy Delivery Systems     | Applied Communication Sciences                         |
| [49]           | Quantum Cryptography Applied to Electric Grid Security                                | Los Alamos National Laboratory                         |
| [50]           | SCADA Protocol Anomaly Detection Using Compression Techniques                          | Idaho National Laboratory                              |
| [51]           | Smart Grid Cryptographic Key Management                                              | Syris Electronics, LLC                                  |
| [52]           | Trustworthy Framework for Mobile Smart Meters                                        | Oak Ridge National Laboratory                          |
| [53]           | Coordinated Island Operation and Resynchronization                                    | Trustworthy Cyber Infrastructure for the Power Grid    |
| [54]           | Next-Generation Secure, Scalable Communication Network for the Smart Grid             | Oak Ridge National Laboratory                          |
| [55]           | Designing SCADA Systems for the Self-Verifiability of Their Security and Survivability | Software Engineering Institute                         |
| [56]           | exe-Guard Project                                                                    | Schweitzer Engineering Laboratories                    |
| [57]           | Time-based Intrusion Detection                                                        | Software Engineering Institute                         |
| [58]           | Watchdog Project                                                                     | Schweitzer Engineering Laboratories                    |
| [59]           | Security and Robustness Evaluation and Enhancement of Power System Applications       | Trustworthy Cyber Infrastructure for the Power Grid    |
| [60]           | Hardware-based IDS for AMI Devices                                                    | Trustworthy Cyber Infrastructure for the Power Grid    |

it is developing the next generation of security and scalable communications network of smart grid.

(iv) Argonne National Laboratory (ANL). ANL is under the U.S. Department of Energy. It is one of the U.S. government’s oldest research institutions, established in 1946, with five main research areas covering basic science, scientific facilities, energy resource planning, environmental management, and national security.

ANL’s research on ICS security focuses on the field of SCADA systems, mainly on the SCADA system of natural gas pipeline transportation. ANL has carried out the investigation and assessment of the SCADA system, and the development of a variety of tools, techniques, and methods for assessing and improving the SCADA system.

(v) Pacific Northwest National Laboratory (PNNL). PNNL was established in 1965 in Washington. It is committed to solve the most intractable problems of energy, environment, and national security. PNNL is one among ten U.S. Department of Energy national laboratories.

PNNL has proposed the concept of SSCP (secure SCADA communication protocols) and its ongoing research includes building secure communication architecture for energy industry, developing the field device management software and the encryption trust management software, and improving the protocol analyzer.

(vi) Los Alamos National Laboratory (LANL). Established in 1943, LANL is also a part of the U.S. Department of Energy. It is famous for developing the world’s first atomic bomb. The key research areas of LANL include national security, space exploration, renewable energy, medicine, nanotechnology, and supercomputers.

LANL is currently focusing on the signature science. In order to advance the signature science, the cyberphysical security challenges associated with the forward deployment of measurements systems, such as wireless sensor networks, or robotic swarms carrying measurement payloads, must be addressed. LANL is carrying out researches on communication, and it is committed to the development of a detailed cost-benefit modeling tool for the SCADA communication framework of the next generation to help operators select
an appropriate communication technology for each network node or level.

3.2. Technology and Research. In the research mechanism, specific technologies, and measures, the U.S. has made a great effort. In mechanism, the U.S. established a technical system which was coordinated and managed by national departments and supported in technology by national professional teams. In the specific technologies and measures, the U.S. sets up assessment methods with the combination of on-site evaluation and laboratory evaluation relying on simulation platform. Simulation platform-based authentication service and self-controlled evaluation service have become an inevitable trend of the ICS security.

Since 2006, the U.S. National Science Foundation (NSF) has awarded large amounts of funds to research projects for CPS. Many universities and institutes join these research projects. Table 4 is a brief outline of the projects NSF has funded for the universities.

Power Infrastructure Cybersecurity Laboratory of Iowa State University focuses on cyberphysical systems framework for risk modeling and mitigation of cyberattacks on the power grid that accounts for dynamics of the physical systems, as well as the operational aspects of the cyber-based control network. PowerCyber, PENET Tool, and TraceDos have been developed to serve the research on power grid security.

Penn Research in Embedded Computing and Integrated Systems Engineering (PRECISE) Center serves as the convergence of related research efforts by affiliated faculty spanning the CPS domain. Currently, PRECISE researchers are actively collaborating with CPS application-area experts to develop next generation medical systems, automotive systems, green energy buildings, wireless industrial automation, and avionics.

In University of California-Berkeley, there are mainly three research institutions developing CPS related knowledge. Center for Hybrid and Embedded Software Systems (CHESS) is aimed at developing model-based and tool-supported design methodologies for real-time fault tolerant software on heterogeneous distributed platforms. Partners for Advanced Transportation Technology (PATH) is to develop solutions to the problems of California’s surface transportation systems through cutting edge research. Cyber-Physical Cloud Computing Lab (CPCC) is to explore the interaction of ubiquitous computing, cloud computing, robotics, and oceanic science. Moreover, Industrial Cyber-Physical Systems Center (iCyPhy) is to identify and develop new engineering techniques that will make it easier to successfully build products and services that combine complex software, hardware, and mechanical components. Last but not least, TerraSwarm Research Center is addressing the huge potential of pervasive integration of smart, networked sensors and actuators into our connected world.

The IMPACT mobile computing lab at Arizona State University focuses on developing protocols and middleware for pervasive and mobile computing applications. Currently, it is developing a sensor network-based medical monitoring infrastructure called Ayushman, which is to provide a dependable, secure, real-time automated health monitoring and to serve as a realistic environment (test bed) for testing communication protocols and systems for medical applications.

Carnegie Mellon CyLab is a world leader in both technological research and the education of professionals in information assurance, security technology, business, and policy, as well as security awareness among cybercitizens of all ages. One of its main research areas is security of cyberphysical systems and there are about 40 projects up to now. Its objective is to build a new generation of technologies that will lead to measurable, available, secure, trustworthy, and sustainable computing and communications systems, as well as associated management and policy tools that enable successful exploitation of the new technologies.

The Cyber-Physical Systems Laboratory (CPSL) at Washington University in St. Louis performs cutting-edge research on real-time systems, wireless sensor networks, embedded systems, and cyberphysical systems that cross-cut computing, networking, and other engineering disciplines. It has been awarded NSF 1329861 to do research on “Safety-Feature Modeling and Adaptive Resource Management for Mixed-Criticality Cyber-Physical Systems.”

The Cyber-Physical Systems Laboratory (CyPhyLab) of the University of California at Los Angeles is currently conducting research on the modeling, analysis, and control of real-time, embedded, networked, and distributed systems. It has been awarded NSF 1239085 “Correct-by-Design Control Software Synthesis for Highly Dynamic Systems” and NSF 1035916 “Foundations of secure Cyber-Physical Systems.”

Cyber Physical Systems Integration Lab of the University of Illinois at Urbana-Champaign focuses on reduced complexity architectural design to compose large-scale, safe, and secure cyberphysical systems, such as avionics and medical systems. It is undertaking the safe “MD PnP” (Medical Device Plug and Play) research program to identify the broad requirements for the integration of medical devices in high-acuity settings. Another famous lab of this school is Cyber-Physical-Human (CPH) Systems Lab, which aims at development of robust, fault-tolerant architectures that would ensure predictable operation of the system with the given hardware constraints, despite the uncertainties in physical processes and cyber- and human faults.

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG), whose researches are mainly from the University of Illinois at Urbana-Champaign, Dartmouth College, the University of California at Davis, and Washington State University, focuses on securing the low-level devices, communications, and data systems that make up the power grid, to ensure trustworthy operation during normal conditions, cyberattacks, and/or power emergencies.

Besides these, Bruce McMillin from Missouri University of Science and Technology, Matthew Migh and Chris Myers form Utah University, Inseok Hwang from Purdue University, Yuhong Zhang from Texas Southern University, Francesco Bullo from the University of California at Santa Barbara, and Sriram Sankaranarayanan from the University of Colorado Boulder have also made contributions to the development of CPS security research.
Table 4: NSF funded projects and corresponding universities (most of these projects are collaborated reaches and this table may not list all the universities in each project).

| Project                                                                                                                                  | University                                      | Award          | Duration                        | Description                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|----------------|---------------------------------|-------------------------------------------------------------------------------------------------|
| Foundations of Secure Cyber-Physical Systems (NSF: 1136174)                                                                             | University of California UCLA team              | $1,799,925.00  | Sep. 1, 2011–Aug. 31, 2015      | Find movement patterns and distinguish activities in CPS and then validate them in the cyber part. |
| The Cyber-Physical Challenges of Transient Stability and Security in Power Grids (USF: 1135895)                                         | Carnegie Mellon University                      | $375,000.00    | Sep. 1, 2011–Aug. 31, 2014      | Develop new principles of cyberphysical engineering by focusing on the instabilities of electric power. |
| Enabling and Advancing Human and Probabilistic Context Awareness for Smart Facilities and Elder Care (NSF: 1035565)                          | University of Utah and University of South Florida | 1 million total, 750 k at the University of Utah | Sep. 15, 2010–Aug. 31, 2013       | Enable cyberphysical systems to be context-aware of people in the environment and to use data from real-world probabilistic sensors. |
| Assuring the Safety, Security and Reliability of Medical Device Cyber Physical Systems (USF: 1035715) [31]                                   | University of Pennsylvania Health System, University of Minnesota, and University of Waterloo Massachusetts General Hospital | $757,498.00    | Oct. 1, 2010–Sep. 30, 2015      | Find a new development paradigm for the design and implement of safe, secure, and reliable MCPS. |
| Towards robust cyber-physical systems (NSF: 1035916)                                                                                   | University of California UCLA team              | $530,000.00    | Sep. 15, 2010–Aug. 31, 2013      | Develop theoretical foundations of robust CPS. Define a notion of robustness and develop the corresponding research methods and tools. |
| Dependability Techniques for Instrumented Cyber-Physical Spaces                                                                        | University of California-Irvine                 | $499,996.00    | Oct. 1, 2010–Sep. 30, 2013       | Develop a semantic foundation, cross-layer system architecture, and adaption services to improve dependability in instrumented cyberphysical spaces. |
| Monitoring Techniques for Safety Critical Cyber-Physical Systems (USF: 1035914) [32]                                                 | University of Illinois                          | $360,000.00    | Oct. 1, 2010–Sep. 30, 2013       | Optimize the monitor for CPS security in timely response, cost, pattern, and efficiency. |
| A Study of Security Countermeasure for Cyber-Physical Systems (USF: 1039127) [33]                                                      | Temple University, Philadelphia, PA Texas Southern University, Houston, TX | $119,886.00    | Sep. 15, 2010–Aug. 31, 2013      | Incorporate real-time traffic techniques into security service, enhancing both system security and real-time capabilities in an adverse environment. |
| Foundations of Cyber-Physical Networks (USF: 0931972)                                                                                   | University of Virginia Main Campus              | $275,000.00    | Sep. 1, 2009–Aug. 31, 2012       | Investigate the foundations, methodologies, algorithms, and implementations of cyberphysical networks in the context of medical applications. |
| Establishing Integrity in Dynamic Networks of Cyber Physical Devices (USF: 0931914) [34]                                               | Pennsylvania State University                   | $185,000.00    | Sep. 1, 2009–Aug. 31, 2013       | Develop energy-efficient integrity establishment techniques for dynamic networks of cyberphysical devices. |

In addition, there is Cyber-Physical Systems Virtual Organization (http://cps-vo.org), supported by NSF, to foster collaboration among CPS professionals in academia, government, and industry of the United States. It can be regarded as a broad community of interest for people who work on a wide range of CPS related disciplines with different approaches, methods, tools, and experimental platforms. They are driven by a shared goal: to advance human’s knowledge in the science and engineering of CPS.

Although the researchers have made some progress in modeling, energy and security control, software design approaches, and so forth, the researches on CPS are just in an embryonic stage.

3.3. Emergency Readiness. “Computer Emergency Readiness Team” was referred to the first team of CERT Coordination Center (CERT/CC), established at Carnegie Mellon University in 1988, which works jointly with DHS and contributes...
expertise to protecting the nation’s information infrastructure by coordinating defense against and response to cyberattacks. Now, the CERT is licensed to other teams around the world. Worldwide, there are more than 250 organizations that use the name “CERT” for cybersecurity response; US-CERT (United States Computer Emergency Readiness Team) is independent of these but may coordinate with them to security incidents [30].

The Industrial Control Systems Cyber Emergency Response Team of the Department of Homeland Security (ICS-CERT) collaborates with the US-CERT, focusing on ICS security, and has carried out related work, including the response to control system incidents, execution vulnerability and malicious code analysis, on-site support for incident response and forensics analysis, situational awareness in the form of actionable intelligence, and reliable disclosure of coordination vulnerability.

For control system security, US-CERT publishes documents to assist in determining vulnerabilities and improving control system security including vendor specific vulnerabilities and solutions. The “ICS-CERT Monthly Monitor” published by ICS-CERT not only includes news, reports, and announcements in ICS field but also timely reports the new vulnerabilities in ICS.

3.4. Standards and Regulations. The United States has formed a set of national regulations and standards and industry standard specification.

As shown in Table 5, it has established a series of management systems on the national level, developed a number of large special programs, developed a technical and research system which is coordinated and managed by national departments, set up assessment methods with the combination of on-site evaluation and laboratory evaluation relying on simulation platform, and passed a set of standards and regulations from national standards to regulations supporting key sectors of energy, nuclear facilities, chemical industry, and the people's livelihood.

4. ICS Security in Europe

4.1. ARTEMIS Program. The ARTEMIS Program in EU invests seven billion dollars in mid-2007 in R&D to achieve “world leadership in intelligent electronic systems” by 2016.

In 2011, The European Network and Information Security Agency (ENISA) conducted a study on the ICS Security, identified threats, risks, and challenges, and took stock of national, European, and international initiatives. Moreover, based on the active collaboration of experts belonging to ICS related sectors, the study released a report named “Protecting Industrial Control Systems” [47]. This report, with a main report and six annexes, is currently the most important and comprehensive result of ICS security research in Europe.

The main report proposes good practices and recommendations which aim at helping to improve the security, safety, and resilience of European ICS systems. The 6 annexes of the report can be regarded as a reference manual to the relative persons who are undertaking the research on ICS security. Annex I presents the main results of a desktop research phase. It provides a comprehensive overview of the current panorama of ICS security. Annex II provides a detailed analysis on the data gathered from the interviews and survey which ICS security experts participate in. Annex III is a compilation of current security guidelines and standards for ICS. Annex IV includes a complete list of initiatives related to ICS security. Annex V provides a detailed description of the key findings. Annex VI includes the minutes of the workshop.

The final report proposes 7 recommendations to the public and private sector involved in the area of industrial control systems. Recommendation (1) is creation of pan-European and national ICS security strategies. Recommendation (2) is creation of a good practices guide for ICS security. Recommendation (3) is creation of ICS security plan templates. Recommendation (4) is to foster awareness and training. Recommendation (5) is creation of a common test bed, or alternatively, an ICS security certification framework. Recommendation (6) is creation of national ICS-computer emergency response capabilities. Recommendation (7) is to foster research in ICS security leveraging existing research programs. These recommendations intend to provide useful and practical advice aimed at improving current initiatives, enhancing cooperation, developing new measures and good practices, and reducing barriers to information sharing.

4.2. CyPhERS Program. The CyPhERS (Cyber-Physical European Roadmap and Strategy, http://clyphers.eu) project aims at combining and expanding Europe's competence in embedded and mobile computing and in control of networked embedded systems. The main objective of the project is to develop a European strategic research and innovation agenda for cyberphysical systems (CPS) to ensure Europe’s competitiveness in this emerging field.

4.3. CPSoS. CPSoS (Towards a European Roadmap on Research and Innovation in Engineering and Management of Cyber-physical Systems of Systems, http://www.cpsos.eu) is a 30-month Support Action supported by the European Commission under the FP7 programme. It aims to build constituencies for a European R&I agenda on SoS. CPSoS provides a forum and an exchange platform for systems of systems related communities and ongoing projects, focusing on the challenges posed by the engineering and the operation of technical systems in which computing and communication systems interact with large complex physical systems. The final outcomes of the project will be identification of industrial and societal needs and the state-of-the-art tools and theories for cyberphysical SoS and so on.

5. ICS Security in China

In China, the ICS has emerged in various fields, like industry, energy, transportation, water, and municipal sectors. In recent years, with the deep integration of information technology and industry and the rapid development of Internet of Things, the intelligent and networked control system becomes the development trend of industrial automation in
| Organization                                      | File name                                                                 | Type  | Data        |
|--------------------------------------------------|---------------------------------------------------------------------------|-------|-------------|
| American National Standards Institute of Technology (NIST) | “System Protection Profile-Industrial Control Systems” (NISTIR 7176) [35] | Guide | Oct. 2004   |
|                                                  | “Field Device Protection Profile for SCADA Systems in Medium Robustness Environments” [36] | Guide | Jun. 2006   |
|                                                  | “Recommended Security Controls for Federal Information Systems and Organizations” (NIST SP 800-53) [37] | Guide | Aug. 2009   |
|                                                  | “Guidelines for Smart Grid Cyber Security” (NISTIR 7628) [38]               | Guide | Sep. 2010   |
|                                                  | “Guide to Industrial Control Systems (ICS) Security” (NIST SP 800-82) [39]  | Guide | Jun. 2011   |
| U.S. Department of Energy                        | “21 Steps to Improve Cyber Security of SCADA Networks” [40]                 | Guide | Jan. 2007   |
|                                                  | “Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities” [41] | Guide | Aug. 2002   |
| U.S. Department of Homeland Security             | “A Catalog of Control Systems Security: Recommendations for Standards Developers” [42] | Guide | Sep. 2009   |
| North American Electric Reliability Council (NERC) | “Cyber Security Standards for the Bulk Power System” (NERC CIP 002-009)       | Standard | Mar. 2006 |
| U.S. Nuclear Regulatory Commission               | “Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities” (RG5.71) [43] | Guide | Jan. 2010   |
| Chemical Industry                                | “Chemical Facility Anti-Terrorism Standards” (RBPS6/7/8 (cyber)/14/15)        | Standard | Jun. 2007 |
| American Gas Association (AGA)                   | “Cryptographic Protection of SCADA Communications” (AGA report number12) [44] | Standard | Mar. 2006 |
| American Petroleum Institute (API)               | “Pipeline SCADA Security” (API 1164) [45]                                    | Guide | Jun. 2009   |
|                                                  | “Security Guidelines for the Petroleum Industry” [46]                         | Guide | Apr. 2005   |

China. More and more computer and network technologies, such as Internet of Things, cloud computing, and mobile computing, are applied to the ICS. Though enhancing the industrial production capacity, new technology increases risks of ICS security.

Compared with developed countries, the ICS in China is facing a more severe situation: firstly, there are uncontrollable risks because of the low proportion of domestic ICS products. The proportion of domestic ICS products is very low, especially the PLC products. The domestic PLC market is mostly occupied by large international companies as Siemens, Mitsubishi, and Omron. Overreliance on foreign products leads to uncontrollable risk so that it is difficult for domestic enterprises to carry out the work of testing, assessment, prevention, and management of the ICS security. Secondly, domestic products are more focusing on efficiency and lack of the necessary security mechanisms. Thirdly, the enterprises pay insufficient attention to the ICS security, so it is difficult to respond effectively to security threats. Fourthly, domestic ICS risk assessment is relatively backward compared with developed countries.

One main problem is that ICS test platform has not yet been built. For some reasons, the test environment for ICS security testing is not yet established, and the implementation of risk assessment will be restricted. Due to lack of technical capacity, the procurement of special tools for ICS
is mainly from developed countries. Moreover, whether from the national level or at the industry level, China has not yet developed the ICS security standards. ICS risk assessment is an interdisciplinary field. Employees need to have not only the traditional information security skills but also the automation control and the industry knowledge, and the professionals of ICS risk assessment are scarcer.

Faced with the grim situation of ICS security, China needs to comprehensively strengthen the ICS security management. Both the government and correlated industries have attached great importance to the security of ICS, especially since the strike of "Stuxnet" in 2010. Besides the concern on ICS security, the government takes lead on mitigating the risk of ICS. It takes measures on several aspects from management to technical support. The efforts of China ICS security management rest on three aspects as the following.

5.1. Policy Guidance. In September 2011, the Ministry of Industry and Information Technology (MIIT) published “The Notice on Strengthening the Information Security Management of Industrial Control Systems” ([2011] 451), in order to raise wide awareness of the importance and urgency of ICS security and call for strengthening the security of basic control facilities and the SCADA system in major industrial areas.

Three months later, in December 2011, the Ministry of Industry and Information Technology published “The Notice on the Survey of Critical Industry ICS Risk” ([2011] 1003), requiring that every region should make a basic survey on all the critical industries including steel, chemistry, oil, electricity, gas, water, heat, and all kinds of transportation on their ICS security. This is taken as a reaction to the Notice 451.

In the middle of 2012, the State Council published “Several Opinions of State Council on Vigorously Promoting the Informationization and Secure the Information Security” ([2012] 23), demanding that local governments and related departments secure the ICS and launch periodically security inspection and risk assessment, especially those critical ICS related to the public safety. It also demands that critical products in critical areas should be inspected and timely reporting mechanism for the risks and vulnerabilities should be established. Also, in 2012, State Council published “The Circular of Carrying out Inspection Action in Network and Information Security in Important Fields” ([2012] 30) demanding strict inspection on critical IT system and ICS, including oil, water, and transportations.

Moreover, besides these kinds of regular inspections or self-inspection, the government has also published circular demand to organize a spot-check team to help check the risks and vulnerabilities of ICS, assess the risks, and provide advices on ICS security.

5.2. Industrial Efforts. Among several critical industries, the electricity power grid has the earliest insight on ICS security. Early on June 2002, former State Economic and Trade Commission has published “The Data Network Security Stipulation on Power Grid Surveillance and Dispatch” ([2002] 30), in order to prevent attacks on power grid system and ensure the power grid security. Later, State Electricity Regulatory Commission published several secondary system safety protection regulations and schemes at national level, provincial level, town level, and power plant level.

As for oil industry, Petro China and China Petrochemical Industry have been far aware of the importance of ICS security and have made much effort on industry regulation, inspections, and safeguard. In October 2011, Petro China and China Information Security Evaluation Center held an evaluation on the schemes of Petro China ICS security. A month later, Petro China officially launched the investigation and inspection on its own ICS security, in order to figure out the status quo of its ICS security and sort out the most urgent issues to raise the foundation for coming works.

5.3. Technical Research Support. In 2011, National Development and Reform Commission organized and implemented the national information security program. The National Development and Reform Commission also began to support industrial projects on ICS security services. On the precondition of enhancing the awareness of risks, China will speed up the development of ICS test bed and the information security standards. On the other hand, China will encourage innovation and advocate professional training in technology, to further enhance the security capabilities of domestic ICS. In fact, many universities and research institutions in China have begun to study the technical foundations for the ICS security.

6. Conclusion
ICS is the central nervous system of national critical infrastructures (such as power plants, power grids, oil refineries, oil and gas pipelines, chemical plants, urban transport, railways, shipbuilding, and defense). If ICS collapse, the consequences could be disastrous. ICS security has become a top priority in the security field. The United States realizes the risks of ICS in the early phase of deployment and the U.S. government has appointed the DOD and DOE to deal with measures and strategies towards mitigating the risks of ICS, which developed NSTB and a center to assess and mitigate the risks. As for the technical countermeasures, quite a lot of universities and industry labs, along with national labs, have engaged in developing the models, theories, methods, and tools for ICS security, with the fund from NSF and other organizations. Meanwhile, EU has invested billions of dollars in the R&D of ICS and conducted the study of the best practices of mitigating the risk of ICS, from the information sharing and staff training to stressing on the technical researches. China government has also noticed the ICS risk and has claimed the demand for checking ICS risks and it also supports industrial projects on ICS security services.

In this paper, we have reviewed the possible threats posed to the ICS and made a survey about related researches on the security countermeasures. Although many countries and areas have attached importance to the ICS security and taken steps to mitigate the risks, there are still many things to do.
Conflict of Interests

The authors declare that they have no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the following programs: the National Natural Science Foundation of China under Grant no. 6170273; Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (no. CAAC-ITRB-201201); 2010 Information Security Program of China National Development and Reform Commission with the title “Testing Usability and Security of Network Service Software.”

References

[1] President’s Council of Advisors on Science and Technology, Leadership Under Challenge: Information Technology R&D in a Competitive World, President’s Council of Advisors on Science and Technology, Washington, DC, USA, 2007.

[2] C.-Y. Lin, S. Zeadally, T.-S. Chen, and C.-Y. Chang, “Enabling cyber physical systems with wireless sensor networking technologies,” International Journal of Distributed Sensor Networks, vol. 2012, Article ID 489794, 21 pages, 2012.

[3] C. Own, “For the pet care appliance of location aware infrastructure on cyber physical system,” International Journal of Distributed Sensor Networks, vol. 2012, Article ID 421259, 8 pages, 2012.

[4] L. Cheng, C. Wu, Y. Zhang, H. Wu, M. Li, and C. Maple, “A survey of localization in wireless sensor network,” International Journal of Distributed Sensor Networks, vol. 2012, Article ID 962523, 12 pages, 2012.

[5] J. Jones and M. Atiquzzaman, “Transport protocols for wireless sensor networks: state-of-the-art and future directions,” International Journal of Distributed Sensor Networks, vol. 3, no. 1, pp. 119–133, 2007.

[6] Z. An, “Medium access control protocol with dynamic duty cycle in wireless sensor network,” International Journal of Future Computer and Communication, vol. 1, no. 1, 2012.

[7] R. Vaid and V. Katiyar, “Pairing based Encoding Schemes (PBES) for secure wireless sensor networks,” International Journal of Computer Applications, vol. 70, no. 17, pp. 43–49, 2013.

[8] M. K. Khan, Y. Xiang, S.-J. Horng, and H.-H. Chen, “Trust, security, and privacy in next-generation wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID 956736, 2 pages, 2013.

[9] W. Zhang, Y. Zhang, and T.-H. Kim, “Detecting bad information in mobile wireless networks based on the wireless application protocol,” Computing, 2014.

[10] W. Zhang, H. He, Q. Zhang, and T.-H. Kim, “Phoneprotector: protecting user privacy on the android-based mobile platform,” International Journal of Distributed Sensor Networks, vol. 2014, Article ID 282417, 10 pages, 2014.

[11] R. J. Robles, M. Choi, E. Cho, S. Kim, G. Park, and J. Lee, “Common threats and vulnerabilities of critical infrastructures,” International Journal of Control and Automation, vol. 1, no. 1, pp. 17–22, 2008.

[12] T.-H. Kim, “Integration of Wireless SCADA through the Internet,” International Journal of Computers and Communications, vol. 4, no. 4, pp. 75–82, 2010.

[13] S. A. M. Anand, S. Sarkar, and S. Rajendra, “Application of distributed control system in automation of process industries,” International Journal of Emerging Technology and Advanced Engineering, vol. 2, no. 6, 2012.

[14] A. R. Kiran, B. V. Sundeeup, S. Ch. Vardhan, and N. Mathews, “The principle of programmable logic controller and its role in automation,” International Journal of Engineering Trends and Technology, vol. 4, no. 3, pp. 500–502, 2013.

[15] S. Katzke and K. Stouffer, “Applying NIST SP 800-53 to industrial control systems,” in Proceedings of the ISO EXPO, 2006.

[16] K. Stouffer, J. Falco, and K. Scarfone, NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, Gaithersburg, Md, USA, 2011.

[17] H. J. Kim, “Security and vulnerability of SCADA systems over ip-based wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2012, Article ID 268478, 10 pages, 2012.

[18] K. J. Higgins, Security incidents Rise in industrial Control Systems, Dark Reading, 2010.

[19] Idaho National Laboratory, “Wireless procurement language in support of advanced metering infrastructure security,” Tech. Rep. INL/EXT-09-15658, U.S. Department of Energy, Idaho National Laboratory, Idaho Falls, Idaho, USA, 2009.

[20] The White House, The National Strategy to Secure Cyberspace, The White House, Washington, DC, USA, 2003.

[21] J. Eisenhauer, P. Donnelly, M. Ellis, and M. O’Brien, Roadmap to Secure Control Systems in the Energy Sector, Energetics Incorporated Columbia, Maryland, Md, USA, 2006.

[22] Energy Sector Control Systems Working Group, “Roadmap to Achieve Energy Delivery Systems Cybersecurity,” 2011.

[23] M. R. Permann and K. Rohde, “Cyber assessment methods for control system security,” in Proceedingsof the 15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference, pp. 615–620, June 2005.

[24] M. Fabro and T. Nelson, “Control Systems Cyber Security: Defense-in-Depth Strategies,” Tech. Rep. INL/CON-07-12804-8-87, Idaho National Laboratory, Idaho Falls, Idaho, USA, 2007.

[25] Idaho National Laboratory, “Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL,” National SCADA Test Bed Program INL/EXT-08-13979, Idaho National Laboratory, Idaho Falls, Idaho, USA, 2008.

[26] R. C. Parks, “Guide to critical infrastructure protection cyber vulnerability assessment,” SANDIA Report SAND2007-7328, 2007.

[27] B. T. Richardson and J. Michalski, “Security framework for control system data classification and protection,” Tech. Rep. SAND2007-3888P, Sandia National Laboratories, Albuquerque, NM, USA, 2007.

[28] A. McIntyre, B. Becker, and R. Halbgewachs, Security Metrics for Process Control Systems, U.S. Department of Energy, Sandia National Laboratories, Albuquerque, NM, USA, 2007.

[29] J. T. Michalski, A. Lanzone, J. Trent, and S. Smith, Secure ICCP Integration Considerations and Recommendations,” Tech. Rep. SAND2007-3345, Sandia National Laboratories, Albuquerque, NM, USA, 2007.

[30] Department of Homeland Security Office of Inspector General, “U.S. computer emergency readiness team makes progress in
securing cyberspace, but challenges remain,” Tech. Rep. OIG-10-94, Department of Homeland Security Office of Inspector General, Washington, DC, USA, 2010.

[31] I. Lee, “CPS: large: assuring the safety, security and reliability of medical device cyber physical systems (NSF CNS-1035715),” in Proceedings of the CPS Principal Investigators’ Meeting, University of Pennsylvania, National Harbor, Md, USA, 2011.

[32] A. P. Sistla, M. Zefran, Y. Feng, A. Yavoovsky, and Y. Ben, “Monitoring Techniques for Safety Critical Cyber-Physical Systems,” 2013.

[33] W. Zhao and Y. Zhang, “A study of security countermeasure for cyber-physical systems,” NSF Award Number 1059116, 2011.

[34] V. Ganapathy, U. Kremer, and T. Jaeger, “Establishing Integrity in Dynamic Networks of Cyber Physical Devices,” 2013.

[35] US Department of Commerce and National Institute of Standards and Technology, “System Protection Profile-Industrial Control Systems Version 1.0,” NISTIR 7176, 2004.

[36] National Institute of Standards And Technology, Field Device Protection Profile for SCADA Systems in Medium Robustness Environments. Version 0.75, Process Control Security Requirements Forum (PCSDF), Digital Bond, Sunrise, Fla, USA, 2006.

[37] National Institute of Standards and Technology and US Department of Commerce, “Recommended Security Controls for Federal Information Systems and Organizations,” 2009.

[38] The Smart Grid Interoperability Panel Cyber Security Working Group, “Introduction to NISTIR, 7628 Guidelines for Smart Grid Cyber Security,” NIST Special Publication 800-53 Revision 3, 2010.

[39] K. Stouffer, J. Falco, and K. Scarfone, “Guide to Industrial Control Systems (ICS) Security,” Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Md, USA, 2011.

[40] US Department of Energy, 21 Steps to Improve Cyber Security of SCADA Networks, U.S. Department of Energy, Washington, DC, USA, 2007.

[41] US Department of Energy Office of Energy Assurance, Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities, U.S. Department of Energy Office of Energy Assurance, Washington, DC, USA, 2002.

[42] Homeland Security, Catalog of Control Systems Security: Recommendations for Standards Developers, Control Systems Security Program, National Cyber Security Division, Washington, DC, USA, 2011.

[43] US Nuclear Regulatory Commission, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, Washington, DC, USA, 2010.

[44] American Gas Association, Cryptographic Protection of SCADA Communications, American Gas Association, Washington, DC, USA, 2006.

[45] Pipeline SCADA Security, API Standard II64, Product No. DII642, 2nd edition, 2009.

[46] American Petroleum Institute, Security Guidelines for the Petroleum Industry, American Petroleum Institute, Washington, DC, USA, 2005.

[47] European Network and Information Security Agency, Protecting Industrial Control Systems: Recommendations for Europe and Member States, European Network and Information Security Agency, Athens, Greece, 2011.
