Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges

Feng Xie, Yong Peng, Wei Zhao, Yang Gao, Xuefeng Han

Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges

Feng Xie, Yong Peng, Wei Zhao, Yang Gao, Xuefeng Han

China Information Technology Security Evaluation Center, Beijing, China
xief@itsec.gov.cn

Abstract. Cyber security for industrial automation and control systems has been a much discussed topic in recent years. Security evaluation of industrial control devices has been gaining rising attention. In this paper, the security evaluation standards for industrial control devices are analyzed, and the corresponding several certifications are compared. Meanwhile, this paper proposes several key testing technologies that can be used in evaluation of devices, and analyzes primary difference compared with traditional IT devices. Finally, this paper discussed the challenges facing us in evaluation of industrial control devices.

Keywords: cyber security; industrial control device; standards; certifications; testing technologies

1 Introduction

Industrial control systems have been widely used in petrochemical factories, power generation systems, manufacturing facilities, and many other critical infrastructures. Traditional industrial control systems typically consist of instrumentation, fuses, system simulation screen and control cables. With more information technology, modern industrial control systems are composed of the industrial control devices, historical data servers, engineer stations as well as HMIs. Industrial control devices (ICDs) usually locate in industrial fields and implement the core control functions. They are often directly connected to sensors and actuators, reading data from sensors, executing a predefined control algorithm, and sending an output to a final element (e.g. control valves or damper drives). Typical industrial control devices include distributed control system controllers (DCS controllers), programmable logic controllers (PLCs), intelligent electronic devices (IEDs) and remote terminal units (RTUs).

In the early development of industrial automation, industrial control system is a closed and proprietary environment, almost free from the threat of cyber attacks. Thus the design of industrial control device is focused on reliable and real-time requirements, which is solved by fault detection, redundancy, fault-tolerant control and other mechanisms. However, with more and more information technologies, such as TCP/IP network and embedded operating system, being applied to industrial automation controls, and with more requirements for interconnection between industrial network and business network, a lot of security incidents have occurred in recent years.

Table 1 shows a part of industrial incidents, including the brief incident description, the potential impact and the most likely reason (root cause).

Table 1. A part of industrial security incidents occurred in recent years.

Year	Incident Description	Root Cause	Impact
2000	An engineer attacked a sewage treatment system in Australia by radio, resulting in large amounts of sewage directly into the river and causing serious environmental disaster. [1,2]	Unauthorized access	An environmental disaster occurred.
2003	A computer virus named Sobig attacked train signaling, dispatching and other systems at CSX Corporation in Florida, U.S.[3]	Malware	Trains were delayed.
2008	A nuclear power plant in Georgia was shut down for 48 hours unexpectedly due to software updates.[4]	Software update	The nuclear power plant was closed unexpectedly.
2010	Stuxnet virus infected Iran's nuclear power plant, tampered programmable logical controller (PLC), and eventually led to centrifuges damaged. [5,6]	Malware	A lot of centrifuges were destroyed.
2011	Hackers claimed to have taken control of U.S. water treatment plant in South Houston by remotely cracking passwords of SCADA system.[7]	Password cracked	Hackers seized control of the public water facility.
2011	Conficker worm infected a steel system, resulting in unstable communication between the PLC and the monitoring station, and resulting in most of the surveillance system failure.	Malware	Plant surveillance was blocked, affecting industrial production.

From these accidents it can be seen that common cyber attacks, e.g. malware, password cracking, unauthorized access and denial of service attacks, have an ability of affecting industrial control systems. In particular, considering that control systems are often used in plant automation control, the impact would lead to industrial operation damage, or even failure, which inevitably would lead to affecting health, safety, and environment.

Nowadays the industrial control devices become more intelligent and networked, which means that they are more vulnerable to cyber attacks. For example, Stuxnet virus, as shown in Table 1, tampered the control program in PLC at the Iran nuclear facility, resulting in PLC sending the wrong instructions to controlled equipments and furthermore destroying about one-tenth of the centrifuges [5, 6]. Therefore, it becomes very important to improve the security of industrial control devices itself.

In this paper, the security evaluation of industrial control devices is reviewed, including the state-of-the-art cyber security standards for evaluating industrial control devices, the existed products certification, as well as some key testing technologies that could be used in evaluation. Further, the issues and challenges of security evaluation are discussed.

The rest of paper is organized as follows: Section II discusses the state-of-the-art security standards for industrial control devices. Section III compares several security

certifications used in industrial control devices. Section IV proposes some technologies that can be applied to assess and test industrial control devices. Section V summarizes the current issues and challenges. Finally section VI concludes the paper.

2 Security Evaluation Standards

In recent years, many security standards for industrial control systems have been proposed. For example, NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) standards provide a cyber security framework for identification and protection of critical cyber assets to support reliable operation of the bulk electric system [8]. Meanwhile, the IEC 62351 standard defines end-to-end security methods for SCADA protocols and security in diverse protocol layers in layered communications architecture [9]. However, as far as security evaluation of industrial control devices, the condition is far from satisfactory. Whether comprehensiveness or feasibility, industrial control devices security evaluation is not only far behind IT devices security evaluation, but also far behind functional safety evaluation. These standards include ISA99 [10], ISO/IEC 62443 [11], WIB 2.0 [12] and so on.

2.1 ISO/IEC 62443

ISO/IEC 62443 is not a single standard, but a standard series. It derives from ISA 99, and has undergone several major changes in recent years. Now it becomes a very comprehensive standard suitable for industrial control products, vendors, system integrators and end users. There are 12 sub-standards in ISO/IEC 62443 and can be divided into four categories, as shown in table 2. However, only the fourth part is aiming to industrial control components or products including ICDs. It involves two security requirements of industrial control components: development requirements and technical security requirements. The former describes the security development process for products, covering 12 stages from security architecture design, threatening modeling, software detailed design, to security integration testing. The latter provides the information security function of industrial automation and control components. Figure 1 shows the framework of ISO/IEC 62443, in which each black point denotes that corresponding standards are applicable. For example, the part 2-4 is applicable for automation supplier and system integrator, and the part 4-1 as well as 4-2 are only applicable for device.

Table 2. Four categories in ISO/IEC 62443.

Category	**Description**
General	Composed of industrial control system security terminology, concepts, models, etc. They are applicable to entire standard series.
Policies & Procedures	Composed of requirements to the security organization and processes of the plant owner and suppliers. They can be seen as security operation and management of an organization.

System	Composed of requirements to a secure industrial control system. They can be adapted as construction guide.
Component	Composed of requirements to secure industrial control components including security development and security functions of ICDs.

Due to the security development of industrial control devices are essentially like software security development, part 4-1 appears relatively mature. In contrast, industrial control devices are distinct with traditional IT products in hardware, software and architecture, therefore existed IT product security requirements cannot be directly applied to industrial products, which leads to part 4-2 is still incomplete.

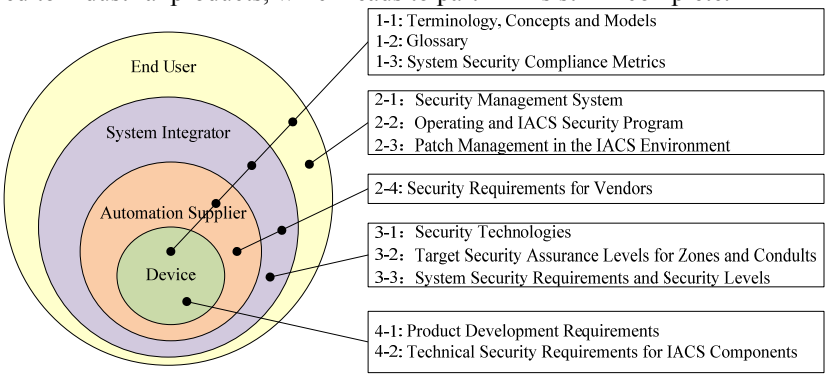

Fig. 1. The framework of ISO/IEC 62443 standard. It involves 12 sub-standards, covering the device, the automation supplier (vendor), the system integrator and end use. Each black point indicates that the sub-standard is applicable.

2.2 WIB 2.0

WIB 2.0 is published by international instrument user's associations (WIB) [12]. Noticed that it is not fit for a product or a device, but rather for a product vendor or system integrator. It defines security requirements on the organizational policies, procedures as well as responsibilities, which should be fulfilled by vendors or integrators in process control domain. Now it is still in draft and is adopted as a part of ISO/IEC 62443 (i.e., ISO/IEC 62443-2-4).

The purpose of this standard is to ensure industrial control devices security through a maturation process covering whole life cycle from design and development to maintenance of industrial control systems, which is clearly based on the capability maturity model (CMM). A total of 35 process areas (PAs) can be categorized as four classes: organizational, system capability, system acceptance testing and commissioning, as well as maintenance and support. Each PA is composed of many basic processes. These requirements basically seem to ensure that product capabilities defined in the product process area are properly used.

In order to identify security degree, different levels are divided based on the maturity of the process. Higher certification level indicates a more mature organization with advanced policies and procedures in place, which should be able to produce better security. Figure 2 shows the framework of WIB 2.0.

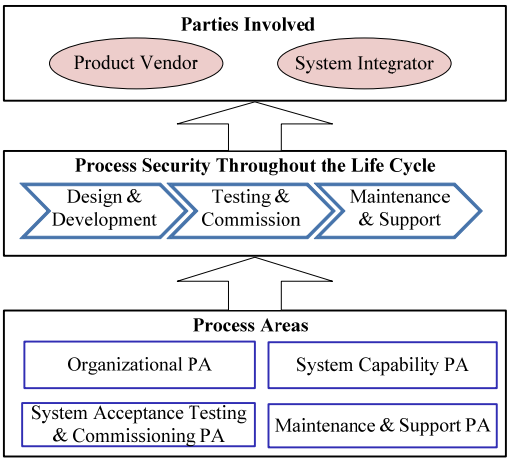

Fig. 2. The framework of WIB 2.0. It comprises of four process areas, covering the whole security life cycle, and is suitable for product vendors as well as system integrators.

3 Security Certification for Industrial Control Devices

Securing industrial control devices are very important for industrial automation. Are there vulnerabilities in these devices? Are the devices secure and robust enough for cyber attacks? Whether do they have some security features and meet requirements of industrial environments such as real-time and reliability? They all are urgent questions to industrial users, vendors and sector administrators. Security certification is a good way to identify a device security level. At present security certifications for industrial control devices include EDSA, APC, ACC, MUSIC, etc.

3.1 Embedded Device Secure Assurance (EDSA）

In order to promote industrial device evaluation and certification, ISA (International Society of Automation) developed a program, ISASecure, for industrial devices and systems [14], in which EDSA is the first step suitable for embedded devices. EDSA consists of three kinds of tests as follows:

- Communication robustness test (CRT). It tests a device's communication ability to resist large traffic and malformed packets. By CRT we can know the extent to which network protocol implementations on an embedded device defend themselves and other device functions against unusual or intentional malicious traffic received from network. Inappropriate message response or failure of device always implies there is something wrong in device due to the incorrect communication.
- Function security assessment (FSA). It tests whether or not security features of a device are correctly implemented. In EDSA all security functionality are divided into seven categories: access control, usage control, data integrity, data

confidentiality, data flow restrictions, incident response, and network resource availability. It is noticed that these security features mainly come from ISO/IEC 62443 and NIST 800-53.

– Software development security assessment (SDSA). It derives from software security development process and is compliance with the ISO/IEC 62443 4-1. SDSA can detect and avoid the systematic design faults. The vendor's development and maintenance processes are audited, respectively.

To distinguish security capability, the devices are divided into three security levels in EDSA: low, middle, and high (Figure 3). The higher the level is, the more the content needed to assess, and the more secure the product. In figure 3, the number represents the number of test cases. For example, in level 1 SDSA involves 130 test cases, and in level 2 the number becomes 149. But CRT remains the same regardless of certification level.

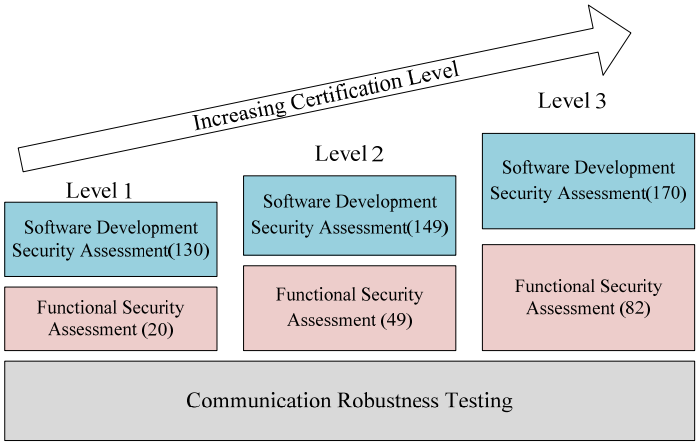

Fig. 3. The framework of EDSA. It consists of three kinds of tests: CRT, SDSA and FSA. Three security levels are determined in EDSA, and different security certification level involves different test cases.

3.2 Achilles Communications Certification (ACC)

ACC is a communication robustness certification for industrial devices [15]. It is provided by Wurldtect Corporation. In nature, ACC is focused on the assessment whether the communication process of a device is robust by testing network protocols covering the link layer, the network layer and the transport layer.

Because focused on protocol stack, ACC is not only fit for embedded control devices (e.g., PLC/DCS/RTU), but also for PC host devices (e.g., engineer station, history server and domain controllers), control applications (e.g., HMI software and control software), and network devices (e.g., routers and switches).

In order to identify security degree, two levels are provided in ACC: level 1 and level 2. Compared with level 1, level 2 has more testing cases.

Also three kinds of test cases are carried out in ACC (Table 3): traffic storms, protocol fuzz-testing (or negative testing), and known vulnerability testing.

Table 3. Three kinds of test cases categories in ACC.

Category	Meaning
Traffic storms	Traffic storms simulate denial-of-service attack, in an attempt to exhaust resources, such as network, bandwidth, CPU time, or memory.
Protocol fuzz-testing	It iterates through the protocol to identify various implementation weaknesses/vulnerabilities, e.g. coding errors (buffer overflow, and format string bugs).
Known vulnerability	Identify existing weaknesses and security holes by appropriate tools and techniques.

Figure 4 shows the tested protocols, tested objects and key testing technologies in ACC.

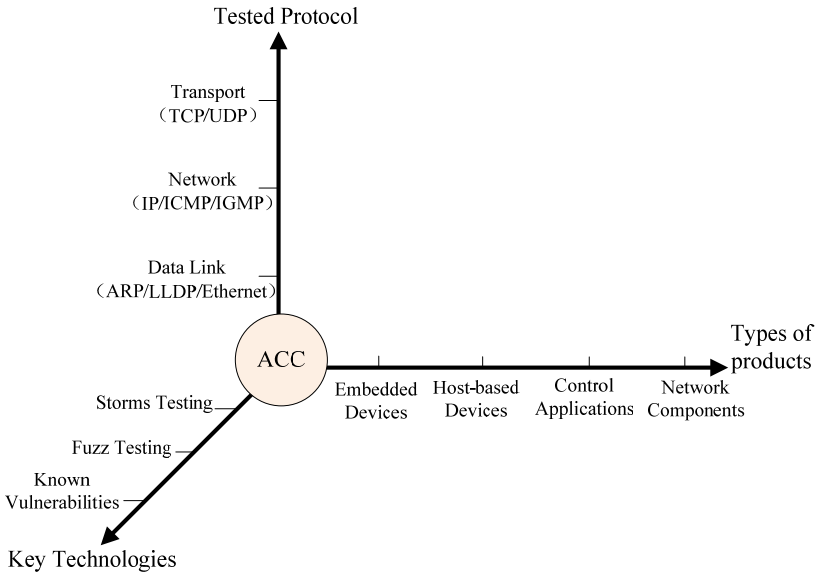

Fig. 4. Achilles communication certification (ACC). It mainly makes use of three key testing technologies: storm testing, fuzz testing and known vulnerabilities detection, and focuses on TCP/IP protocols. At present, four types of products can be certified by ACC.

3.3 Achilles Practices Certification（APC）

APC is also provided by Wurldtect Corporation [15]. Different from ACC, APC is more fit for practices of vendors. This certification is based on WIB 2.0. It is noticed that APC does not address a product itself, but rather a product vendor and/or system

integrator. It defines requirements on the organizational policies and procedures as well as organizational responsibilities.

3.4 MUSIC Certification

MUSIC is an industrial device certification offered by Mu Dynamics, Inc. It requires the use of an evaluation platform for the testing for network protocols covering link layer, network layer, transport layer and application layer. Although it operates in a similar manner to that of the ACC program, the acceptance of MUSIC lags behind that of ACC.

3.5 Comparison Among Several Certifications

Table 4 shows the comparison results among four certifications of industrial control devices, from which we can draw the following conclusions.

(a) Communication security is very important for a device and therefore is widely used in certification, even sometimes as the only requirement.
(b) EDSA is the only certification assessing security function of products.
(c) Process assurance is an effective way securing products, and is involved in many certifications. For example, EDSA involves security development process assessment, and APC is itself fit for process vendors.

Table 4. Comparision amoung several certifications.

Certification	Organization	TOE (Target of Evaluation	Description
EDSA	ISA	Device	Test the product's stack robustness, security functionality and security development practice being an acceptable level.
ACC	Wurldtect	Device	Test the product's stack robustness being an acceptable level.
APC	Wurldtect	Vendor	Test organizational preparedness being an acceptable level.
MUSIC	Mu Dynamics	Device	Test the product's stack robustness being an acceptable level.

4 Key Testing Technologies

The following technologies can be used in the security evaluation for industrial control devices.

4.1 Data Storm Testing

Usually industrial control systems require high real-time. Any short latency maybe has an immeasurable impact on industrial operations, therefore these devices should have a good performance. Data storms test is an important evaluation technique aiming at processing capability of a device by sending packets with different rates. Usually data storms consist of TCP SYN storm, TCP LAND attack, ICMP storm, UDP unicast/multicast/broadcast storm, ARP request storm, and so on.

4.2 Protocol Fuzz-Testing

Fuzz-testing is a popular security evaluation technique in which hostile inputs are crafted and passed to the target in order to reveal bugs. An industrial control device often communicates with HMI or field device based on different communication protocols. The vulnerability which can be exploited by hacker maybe exists for design and implement of protocols. Therefore identifying protocol vulnerabilities via fuzz-testing plays an important role in EDSA, ACC as well as MUSIC. The typical process is to inject a lot of erroneous or variation data to the target device and to monitor whether or not it runs normally. An abnormal behavior implies that a bug in protocol is triggered. Many researchers discovered vulnerabilities by this technique. To improve the efficiency, many fuzz-testing tools such as Spike [18], Sulley [19] and Peach [20] are developed. However when applied directly to industrial control devices, they encountered many problems as follows.

Problem 1. These tools are developed for conventional TCP/IP protocols which are open. However, most of industrial protocols are proprietary and not known by outsiders. As a result researchers have to crack the packet structure and session process before fuzz-testing for a proprietary protocol, which distinguishably increases the difficulty.

Problem 2. As far as exception monitoring is concerned, it becomes more difficult in industrial environment. Traditionally, network survival detection can be used to monitor exceptions when fuzz-testing is carrying out. In this approach, after each set of testing cases to send, a specific probing packet is sent to the target in order to detect whether or not the network is survival. Usually probing packet is ICMP or ARP packet. By the intermittent request-response, we can know whether or not the test cases trigger the exception and further crash the device. When fuzz-testing is used for industrial control devices, a new issue occurs. In fact an industrial control device can be seen as a device connecting the information space and physical space [13, 17]. It usually consists of two kinds of interface connected to other devices. One is network interface such as Ethernet and wireless network, by which ICDs can be connected with other host devices (e.g., HMI and engineering station) and network devices (e.g., switch and router), and can transmit all kinds of data such as monitoring status information and control instruction. The other is input/output signal interface such as analog I/O and digital I/O, by which ICDs can communicate with different field devices such as sensors and actors. Therefore, when testing an industrial control device, not only is the network exception detection needed, but also the output signal exception

detection is needed. The former is used to monitor whether or not the network behavior is abnormal. Abnormal behaviors typically include the slowing network packet speed, the increasing latency, or even loss of response. These anomalies usually indicate that network protocol stack of control device are damaged by test cases. The latter is used to monitor whether the output signal is expected. Anomaly signal indicates that the test cases have an impact on control program running on the device. In order to do it, the expected output signal should be known before testing starts.

Problem 3. It is very difficult to debug the exceptions or errors on industrial control devices. Noticed that most industrial control devices are embedded devices with different platform from computers. As a result, many traditional debuggers (e.g. Ollydbg and Windbg) based on computers cannot be used on industrial control device, which makes it difficult to debug the exceptions to acquire root cause.

4.3 Penetration Testing

Penetration testing is directed toward finding vulnerabilities that enable a user to violate the security policy in the target (i.e. the device under test). It is based upon an analysis of the target that specifically seeks to identify vulnerabilities in the design and implementation, and can be simply considered as vulnerability assessment. Penetration testing becomes an important approach for security evaluation of devices as well as systems. For example, it is already widely used in common evaluation criteria for IT security (i.e. ISO/IEC 15408 [16]). Similarly, it also can be used to test industrial control devices.

Penetration testing involves a lot of attack techniques to identify, analyze and exploit vulnerabilities. The following techniques often can be used in penetration testing.

- Scanning. Scanning can be defined as “a method for discovering exploitable communication channels”. Via scanning, we can know the open ports as well as existed services in a device. Unnecessary ports should be shut down to reduce attack surface.
- Known vulnerability exploit. It is well-known that many control devices nowadays often use COTS operating systems such as VxWorks and embedded Linux. The known vulnerabilities in the operating system are often acquired easily from Internet (such as CVE database [21]). It is a good approach to attack a control device by means of exploiting the known vulnerability in the operating system of the device.
- Firmware analysis. The firmware of a device is the set of all code running on the hardware's processor (machine code and virtual machine code). Undoubtedly, industrial control devices belong to firmware-driven devices. If the firmware of devices is not encrypted or protected well, it is can be reverse engineered by security researchers. Hereby, finding security issues become possible. In some cases, even hard-code usernames and passwords as well as undocumented access approaches such as back doors can be identified.

5 Current Challenges

At present, several key challenges in security evaluation for industrial control devices are as follows:

Firstly, although security has become an abstracting topic in recent years, it is not be widely accepted by industrial vendors and users. Security evaluation for industrial control equipments has drawn little attention. In contrast, the functional safety of devices has been emphasized in industrial automation sector for a long time. At present, security is not embedded in the whole life cycle of industrial products covering design, development, delivery and maintenance.

Secondly, most of industrial security standards are still in discussion and draft, which brings great challenges to industrial equipment assessment. Meanwhile, these standards are concentrated on basic concepts, frameworks and models, while detailed technical requirements still keep a blank. For example, although the fourth part of ISO/IEC 62443 can be regarded as technical requirements of industrial control products, most requirements in ISO/IEC 62443 4-2 are missing, which makes it difficult to evaluate the compliance with standards. Due to the reasons above, the current industrial equipment evaluation still mainly focused on communication robustness tests.

Thirdly, although many perfect testing techniques/tools are developed and used in IT security evaluation, they are often not suitable for industrial devices testing. For example, many protocol analyzers based on conventional TCP/IP protocols hardly know the industrial protocols, therefore they cannot identify the vulnerabilities inherent in industrial devices. Because industrial protocols are often proprietary and abundant, it is a horrible work to develop new analysis devices. Similarly, many existing tools cannot be directly used in the vulnerability analysis of control devices due to the huge difference between control devices and person computers in hardware and operating system, while vulnerability testing is very critical for security evaluation.

Fourthly, because the industrial control devices are often used for real-time control of physical process or industrial production, the security evaluation cannot be performed in plants to avoid the impact on the physical environment, which indicates the needs for simulated testing environment. This is a considerable investment!

Finally, automation security is related with many fields such as industrial automation, sectors (i.e. applications) and cyber security, therefore the knowledge and skills of testers become very important. They not only need to be familiar with different industrial applications and control devices with different architecture, but also need to master a number of security testing technologies to identify security vulnerabilities in control equipments. Unfortunately, the amount of staff with such knowledge is too little.

6 Conclusions

In this paper, the security evaluation standards, certifications, key testing technologies as well as challenges of industrial control devices are reviewed. Compared with functional safety assessment, the security evaluation for industrial control devices lags far

behind. Most of security standards are still in draft, and the certification has not widely accepted by industrial vendors and users. Many traditional security testing techniques encounter unique problems when they are used to evaluate industrial control device. All these difficulties give us tremendous challenges.

7 References

1. Marshall Abrams, Joe Weiss. Malicious control system cyber security attack case study-maroochy water services, Australia.
2. Bill Miller, Dale Rowe. A survey of SCADA and critical infrastructure incidents. In Proc. Of the 1st annual conference on research in information technology, 2012.
3. Nicholson. SCADA security in the light of cyber-warfare. Computers & Security, 2012.
4. http://www.waterfall-security.com/cyber-incident-blamed-for-nuclear-power-plant-shutdown-june-08/
5. Luders S. Stuxnet and the impact on accelerator control systems. In Proc. Of the 13th Conference on Accelerator and Large Experimental Physics Control Systems. Geneva, Switzerland: JACoW, 2011: 1285-1288.
6. Farwell, Rohozinski. Stuxnet and the futher of cyber war. Survival: global politics and strategy, 2011.
7. http://www.dailymail.co.uk/sciencetech/article-2064283/Hackers-control-U-S-public-water-treatment-facilities.html
8. North American Electric Reliability Council (NERC), Critical Infrastructure Protection Committee, NERC Standard CIP-002 through -009, Cyber Security, 2006.
9. IEC 62351 Power systems management and associated information exchange data and communication security, 2007.
10. ANSI/ISA 99. Security for industrial automation and control systems. Research Triangle Park, USA: ISA, 2007.
11. ISO/IEC 62443. Security for industrial automation and control systems. Switzerland: International Electrotechnical Commission, 2010.
12. M 2784 X10. Process control domain-security requirements for vendors.
13. Rajkumar R., Lee Insup, Sha Lui, et al. Cyber-physical systems: the next computing revolution. In Proc. Of 47th Conference on Design Automation Conference. Piscataway, NJ: IEEE Press, 2010: 731-736.
14. ISA Security compliance institute. ISASecure Embedded Device Security Assurance Certification, http://www.isa.org/filestore/asci/isci/ISCI%20ISASecure%20ECSA%20Certification%20brochure.pdf
15. Wurldtech Security Inc. Achilles practices certification. http://www.wurldtech.com/product_services/certify_educate/achilles_practices_certification
16. ISO/IEC 15408. Evaluation criteria for IT security. Switzerland. ISO, 2005.
17. WANG Zhongjie, XIE lulu. Cyber-physical systems: a survey. ACTA AUTOMATICA SINICA. 2011, 37(10): 1157-1166.
18. D. Aitel. An introduction to SPIKE, The fuzzer creation kit. BlackHat Conference.
19. Sulley: fuzzing framework. http://www.fuzzing.org/wp-content/SulleyManual.pdf
20. http://peachfuzzer.com/
21. http://cve.mitre.org/