PBNC 2012

CHALLENGES OF CYBER SECURITY FOR NUCLEAR POWER PLANTS

Kwangjo Kim

KAIST, Daejeon, Korea
Khalifa University of Science, Technology and Research, Abu Dhabi, UAE

kkj@kaist.ac.kr, kwangjo.kim@kustar.ac.ae

Abstract

Nuclear Power Plants (NPPs) become one of the most important infrastructures in providing efficient and non-interrupted electricity in a country using radioactive elements due to global warming and shortage of fossil resources. To provide the higher reliability and better performance with additional diagnostic capabilities in operating NPPs, digital Instrumentation and Control (I&C) systems have been introduced to replace the analog I&C system. However, the digitalized I&C systems bring us new vulnerabilities and threats over the cyber space. In this paper, we discus that the trends of cyber security for legacy IT system and its countermeasure have been developed for last three decades from the security point of view. We found that the nuclear industry has an inherently conservative approach to safety and substantial effort is required to provide the necessary evidence and analysis to assure that digital I&C systems can be used in safety-critical and safety-related applications.
NPP I&C systems are generally isolated from external communication systems. This cannot provide 100% cyber attack–free operation for NPP lessoned from an attack using stuxnet. Experience gained from cyber security in other sensitive fields, such as the military, national security, banking, and air-traffic control, *etc.* is valuable both for improving cyber security at NPPs with digital I&C systems and for demonstrating that cyber defenses can consistently stay ahead of cyber attacks. But as with safety and other areas of security, cyber security is an area where no-one can rest on his laurels. Continued success requires continuous vigilance and continuous improvement.

1. Introduction

Nuclear Power Plants (NPPs) become one of the most important infrastructures in providing efficient and non-interrupted electricity in a country using radioactive elements due to global warming and shortage of fossil resources. To provide the higher reliability and better performance with additional diagnostic capabilities in operating NPPs, digital Instrumentation and Control (I&C) systems have been introduced to replace the analog I&C system. However, the digitalized I&C systems bring us new vulnerabilities and threats over the cyber space.

To make an efficient countermeasure against cyber attack for NPPs, we need to know how attacking methods have been developed for legacy IT infrastructure for last decades. This will be best practices to nuclear industry who is very conservative and uses commercial-off-the-shelf only.

In this paper, we will discuss how the security for IT infrastructure has been developed in Section 2 and what countermeasure against cyber attack in NPP has been prepared and recommended in Section 3. We make a summary of this paper and conclusion in Section 4.

2. Development of Security for IT Infrastructure

2.1 Security of IT Infrastructure

At the beginning of digital communications in the sixties over the physical media before the Internet and mobile communications have been introduced, the passive attack such as eavesdropping done by an adversary is of a great issue to legitimate communication partners. This was an era of communication security (COMSEC) over the physical communication channel. At the same time, host-level computing facilities have been operated as standalone by a limited expertise, but the birth of personal computer (PC) becomes easier to use to everyone and many people got access to them with interactive sessions. The information on the computers became accessible to anyone who are authorized to use the computer. This gave rise to the need for Computer Security (COMPSEC). When computers are networked together for remote access, new security problems occur and old problems behave in different ways. For example, we have communications over local area network (LAN) privately instead of wide area network (WAN) which Information Service Provider(ISP) has offered over the public and shared media. A networked environment of computers created the concept of Network Security (NETSEC). Unfortunately, it too linked functionality with assurance. The merging of COMSEC, COMPSEC and NETSEC together give a girth of coined "Information security (INFOSEC)".[1]

Information security is the process of the protection the valuable or critical information from the unauthorized access, use, disclosure, destruction, modification or disruption by an adversary. The basic goal of INFOSEC is to provide Confidentiality, Integrity and Availability (simply CIA) services. Confidentiality is to send your information safely (*e.g.*, in an encrypted form) to your counterpart over the cyberspace even if an eavesdropping occurs. Integrity is to provide some cryptographic mechanism that your message is delivered correctly without any modification. Availability is to ensure your requested service into the host computer or network server over the cyber space is to be available without interruption. Depending on the type of applications, additional security requirements must be provided.

According to DOD, the cyberspace can be interpreted as a global domain within the information environment which consists of the interdependent networks of information technology(IT) infrastructures includes the Internet, telecommunication networks, computer systems and embedded processors and controllers. On the other hand, UN defines cyber as "the global system of systems of Internetted computers, communication infrastructure, inline conferencing entities, databases, and information utilities generally known as the Net. When we are interested in the security of the Internet only, Internet Security is also of a popular terminology.

After the Internet and personal mobile communication has become into service, new digital services over the cyber space become feasible at any time, at any place and to any person in ubiquitous environments. This gives a birth of Ubiquitous security(UBISEC). There are security issues that are not covered by current INFOSEC, Internet Security and IT security best practices because there are gaps between these domains. Cyberspace security or cyber security is about the security of the cyberspace providing guidance to address issues arising from the gaps between the different security domains in the cyberspace environments while at the same time providing an infrastructure for collaboration.

2.2 What Hacking tools Evolved

We being with the concept of Malware (malicious software) which includes the broad range of software designed to infiltrate or damage computing systems without user knowledge or consent. The most well-known forms of malware include the following:

- Virus: self-replicating malware requiring a host file that depends on human action to spread it.
- Worm: self-contained malware, needing no host file that spreads automatically through networks.
- Trojan Horse: an apparently useful and innocent application containing a hidden malicious program
- Rootkit: a software that enables continued privileged access to a computer which actively hiding its presence from administrators by subverting standard OS functionality or other applications.

The popular attacks over the cyber space can be classified as below:

- Zero-day attack takes advantages of computer vulnerabilities that do not currently have a solution. It named "zero day" because the attack occurs before the first day the vulnerability is known.
- Distributed Denial of Service (DDoS) attacks form a significant security threat marking networked systems unavailable by flooding with useless traffic using large number of "zombies". When this attack happens in network-configured form, sometime we say this network to be "botnet".
- Stuxnet: a large, complex piece of known malware (zero-day exploits, Windows rootkit, AV evasion, *etc*.) with many different components and functionalities which was primarily written to target an industrial control system (ICS) or set of similar systems. Its goal is to reprogram ICS by modifying code on programmable logic controllers (PCLs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment.
- Advanced Persistent Threat(APT): usually refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage, but applies equally to other threats such as that of traditional espionage or attack. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

In spite that the capability of an adversary have been improved in a combined form of previous attacks rapidly, the capability of its defence is always behind that of the attackers. We

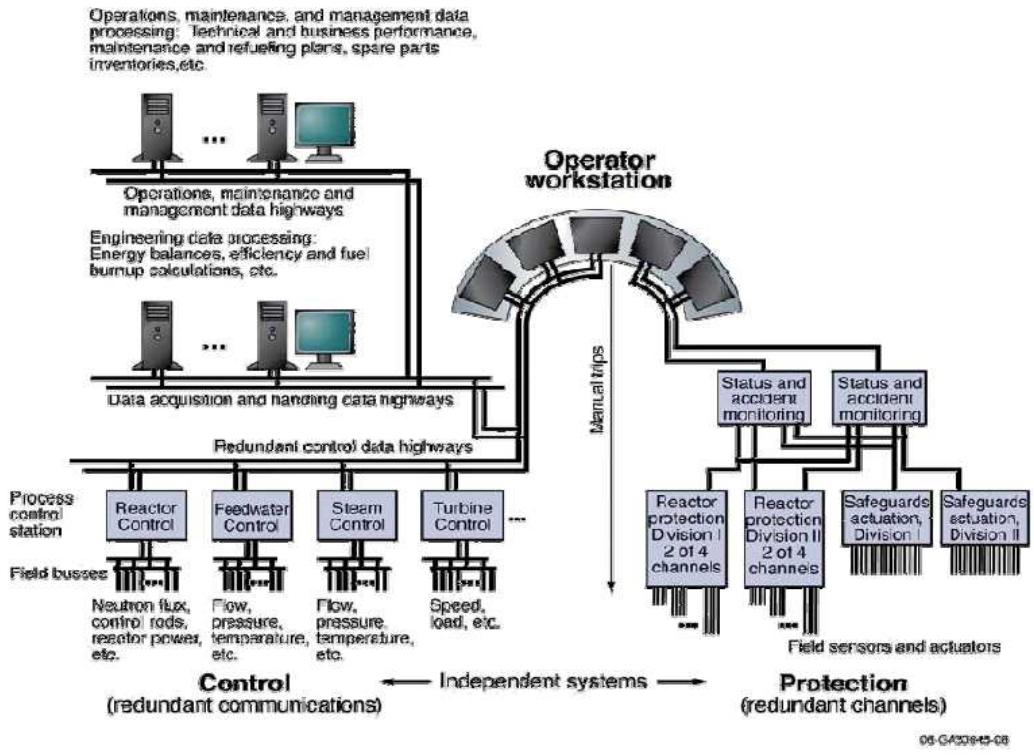
need to reduce the window of vulnerability as small as possible and to be proactive against new attacks.

3. Cyber Security for NPPs

According to [2], progress in electronics and IT has created incentives to replace traditional analog instrumentation and control (I&C) system in NPP with digital I&C system. *i.e.,* systems based on computers and microprocessors. NPPs rely on I&C system for protection, control, supervision and monitoring. Digital systems offer higher reliability, better plant performance and additional diagnostic capabilities. Analog system will gradually become obsolete in the general IT shift to digital technology. Digital I&C systems nervous system of NPPs which monitor all aspects of plant's health and help respond with the care and adjustments needed. A typical I&C system consists of approximately 10,000 sensors and detectors and 5,000 Km of I&C cables. About 40% nearly 30 countries of 439 operating reactors in the world modernized to include digital I&C system. In Korea, three 1000 MW PWRs are under construction (Shin-Kori-1 and -2 and Shin-Wolsong-1). All with full digital I&C safety and control systems and hybrid human-system interface(HSI) in the control rooms. Also new NPP APR1400, UAE includes digital I&C system.

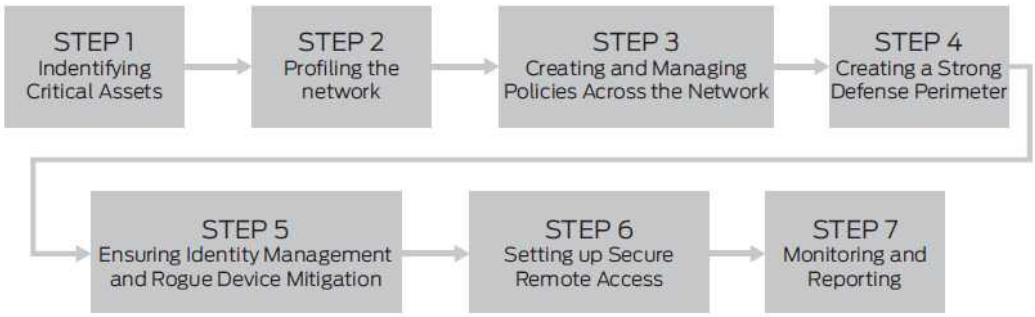
For industry adoption and regulatory approval, digital I&C systems have more connections among its many components and is simply more complex than its analog predecessor and more dependent on software. This overall dependence raises the importance of cyber security.

(Fig. 1) shows a simplified illustration of a US case where the I&C systems for controlling the plant, on the left side of the figure, are digital (computers, digital data networks, automatic calculations, and microprocessor-based sensors), and the I&C systems for safety, labelled "protection" on the right side of the figure are analog.



(Figure 1) Typical I&C architecture with Analog and Digital
(Source: US National Research Council)

This transition has presented new potential security threat – referred to as cyber security- that includes such threats we have discussed in the last section. This will be new challenges for the industry and regulators.The security of NPPs' control system networks is critical to achieving mission objectives. To effectively protect the security of their plants, control system network administrators and network security specialists must have insight into the multiple types and levels of evolving threats to secure their network perimeter, critical resources and remote access. A systematic and step-by-step plan[3] for plant control system cyber security has been suggested in (Fig. 2).



(Figure 2) Seven-step plan for plant control system cyber security

This is a kind of approach for NPPs' cyber security. Depending on their strategy, policy and culture in an operating country, there will be customized approach according to their own culture.

The scope of cyber security was defined by the international communication standardization, ITU-SC17 as below:

(1) What is cyber security
Risk Analysis
Protective Measure
Detection Measure & Remedial Measure
Freedom from harm or danger
Minimizing threats to the cyber environment
Intentional or Unintentional Threats

(2) Who or What is affected
Persons
Objects
Resources and assets
Extrinsic actions and consequences
Infrastructure including SCADA

(3) What measure enable protection
Encryption /VPN
Resilient Infrastructure
Network/application integrity
Real-time data availability
Data retention and auditing
Identity Management
Routing & Resource constraints

(4) What measure enable threat detection
Forensic analysis
(5) What measures enable thwarting and other remedies
Blacklist/Whitelist
Investigatory measures
(6) What legal remedies exist
Contractual service agreement and federations
Intergovernmental agreement and cooperation
Regulatory/Administrative law
Criminal Law

NRC and NIST [4-12] have published many guidelines and rules for NPP cyber security whose key concepts are as below:

- The licensee shall provide high assurance (HA) that digital computer and communication systems and networks are adequately protected against cyber attacks.
- The ranges from simple attacks to those defined in the design basis threat (Title 10 of the Code of Federal Regulations (10 CFR) Part 73, Section 73.1).
- Covers safety, security, and emergency preparedness systems (including other systems that can impact their performance).
- Assets shall be protected from attacks that could adversely impact the CIA and operation of systems, networks, and associated equipment.
- This shall include employing state-of-the-art defence-in-depth protective strategies to detect, protect, response to, and mitigate cyber attacks.
  - Use multiple-layered security control.
  - Have appropriate detection, mitigation, response, and recover capabilities in place if your security control fails.
- Implement appropriate security controls to protect assets. This includes management, operational and technical security controls.
- Ensure the functionality of critical systems is maintained.
- Systematically evaluate cyber security risks for all critical systems.
- Consider cyber security implications before making any system modifications.
- Provide appropriate and position-specific cyber security training.
- Licenses shall submit a *formal cyber security plan* to the NRC and shall implement a *formal cyber security program* that is part of their physical security program.

In addition, the NRC is preparing more regulatory guidelines.

4. Discussions and Conclusions

This paper is the general overview how cyber security for NPP must be prepared from the lessons we have experienced to develop the cyber security for IT infrastructure.

Digital equipment with improved performance has had an important influence on I&C systems design in NPP. However, in NPPs digital technology has been adopted more slowly, especially for safety I&C systems compared to IT infrastructure. For good reason, the nuclear industry has an inherently conservative approach to safety, and substantial effort is required to provide the necessary evidence and analysis to assure that digital I&C systems can be used in safety-critical and safety-related applications.

NPP I&C systems are generally isolated from external communication systems. This cannot provide 100% cyber attack–free operation for NPP lessoned from an attack using stuxnet. Experience gained from cyber security in other sensitive fields, such as the military, national security, banking, and air-traffic control, *etc.* is valuable both for improving cyber security at NPPs with digital I&C systems and for demonstrating that cyber defences can consistently stay ahead of cyber attacks. But as with safety and other areas of security, *cyber security is an area where no-one can rest on his laurels*. *Continued success requires continuous vigilance and continuous improvement*.

Finally don't overlook to conclude the cyber security is to be an easy job. The ways of new hackings are evolving very rapidly. We need to be proactive before an attack happens.

References

1. Eric Maiwald, "Fundamentals of Network Security", McGraw Hill Technology Education, 2004.
2. Instrumentation and Control (I&C) Systems in Nuclear Power Plant: A Time of Transition, Obtained from the Internet, 2012.
3. Nuclear Power Plant Control System Cyber Vulnerabilities and Recommendations Toward Securing Them, Jupiter Networks, 2009.
4. Cliff Glantz, *et. al.*, "The Nuclear Regulatory Commission's Forthcoming Cyber Security Rule : Application to Emergency Preparedness Systems at Nuclear Facilities", Obtained from the Internet, 2012.
5. NRC Order EA-02-026, "Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants", U.S. Nuclear Regulatory Commission, Washington DC, February 2002.
6. NRC Order EA-03-086, "Design Basis Threat for Radiological Sabotage", U.S. Nuclear Regulatory Commission, Washington DC, April 2003.
7. NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants", October 2004.
8. R.P. Zimmerman, Letter to M.T. Coyle, NEI, Subject: "NRC Acceptance of NEI 04-04, Cyber Security Program for Power Reactors, Rev. 1", December 23, 2005.
9. NEI 04-04, Rev. 1, "Cyber Security Program for Power Reactors", Nuclear Energy Institute, November 18, 2005.
10. NIST SP 800-53, Rev. 3, "Recommended Security Controls for Federal Information Systems", National Institute of Standards and Technology, Gaithersburg, MD, August 2009.
11. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants", U.S. Nuclear Regulatory Commission.
12. NIST SP 800-82, "Guide to Industrial Control Systems Security", National Institute of Standards and Technology, Gaithersburg, MD, September 29, 2008.