CS573 - Assignment 2 **Fatih Izgi** (10457950)

A CYBER SECURITY RISK ASSESSMENT
FOR THE DESIGN OF I&C SYSTEMS IN NUCLEAR POWER PLANTS

In this paper, the characteristics of nuclear power plant instrumentation and control systems are described, and the considerations needed when conducting cyber security risk assessments in accordance with the lifecycle process of instrumentation and control systems are discussed.

The activities and considerations are presented in the following 6 steps:

1) System Identification and Cyber Security Modeling

In this step, the target system for which a cyber security risk assessment is performed should be analyzed to acquire basic information about the system.

- One-to-one direct data communication, analog input/output, and digital input/output can be excluded or simplified;
- The direction and mechanism of the data transfer should be identified
- Security controls that are already included in the design, such as firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), the application of encryption, or data flow control status, should be identified;
- The possible paths from outside or through portable devices used for maintenance should be investigated.

> Since the system can be integrated with different structures and installed in the site, the location of the system in the site's virtual environment, its reference to the other structures, and interfaces with different virtual belongings of the plant should additionally be taken into consideration throughout the evaluation and modeling of this step.

2) Asset and Impact Analysis

To be able to apply in-depth defense strategy in the I&C systems, security levels should be defined, and an appropriate security level should be assigned to each CDA by using firewalls, the creation of demilitarized zones, intrusion detection capabilities, and other managerial security programs.

Each security level has the following characteristics:

Security level 4: This level contains CDAs associated with safety and those important to plant trips. The CDAs at this level should be protected from the malfunctions of devices at the lower levels. Only a one-way data flow is allowed from Level 4 to Level 3

Security level 3: This level contains the assets or systems that do not impact safety directly, but may cause the plant trips or are connected to other systems at security level 4 through a network. The assets or systems at this level should not receive any data from the devices at security level 2. Security controls or mitigation measures regarding vulnerabilities should be applied.

Security level 2: This level contains independent assets or systems that do not impact plant safety or trips and are not connected to any network. Security controls or mitigation measures regarding vulnerabilities may be applied in consideration of the impact of cyber threats to an asset or system itself.

> In the threat evaluation of IT systems, virtual assets are analyzed in attention of the effect and chance of loss in confidentiality, integrity, and availability predicted with the aid of using cyber threats. I&C systems (both Safety and Non-Safety Systems) should be covered from cyber attacks. Nuclear power plants have security levels which allow one-way data flow from Level 4 to Level 3 and from Level 3 to Level 2 to protect the system from external threats.

3) Threat Analysis

The following attack scenario is assumed as possible and harmful to NPP I&C systems:

Stage 1: Reconnaissance / Footprinting: Attackers study methods to collect information necessary for accessing NPP digital I&C systems

Stage 2: Scanning: If the malware successfully infects, attackers continue to collect information, arrange attack paths to send the information to their ghost sites, and update the malware as needed, until they obtain the information on the target system.

Stage 3: Gaining Access: Once malware has infected a system, it can be spread to a connected target system through internal networks

Stage 4: Maintaining Access: After the scanning stage, attackers maintain a passive access route to gather information continuously for making an easy-to-attack environment.

Stage 5: Attack: By using emails again, attackers try to infect the I&C systems with the malware that includes codes for carrying out an attack

Stage 6: Covering Tracks: Attackers rewrite and recover the files that they backed up previously, and revive system logging functions to cover the attack tracks. By doing this, they can prohibit any changes to the systems from being recorded during the attack

> NPP I&C structures differ from well-known IT structures as they normally use closed data and communication networks. However, NPP I&C structures can be infected through malware designed with codes permitting cyber attacks through transportable devices consisting of laptops and USB flash drives as in the Stuxnet case, which targeted supervisory control and data acquisition systems and is believed to be responsible for causing substantial damage to the nuclear power plant of Iran.

4) Vulnerability Analysis

Considering the previous threat analysis with the attack scenario, security design features that are absent in the current design, but should exist to comply with the definition of assigned security levels, should also be treated as vulnerabilities. In the CD/ES phase, vulnerability data collection and evaluation should be based on the hardware and software design specifications, which need more specific vulnerability information for cyber security risk assessments.

> The data accrued in this step should be evaluated to decide if the distinctive vulnerability statistics corresponds to the characteristics of I&C systems. In the SD phase, vulnerability data and assessment should be based on the network and system design, and also the system architecture.

5) Security Control Design

In terms of their importance, vulnerabilities can be analyzed to decide whether additional security design features are required that should be incorporated into the system or can be mitigated by other techniques, such as security controls for organizational and management. In both the SD and CD/ES phases, a security control should not be applied if the control adversely impacts plant safety and security functions, or performance. If an adverse effect is expected, alternate controls should be considered. The subject of this risk management is the development environment, which includes workstations, servers, network devices, development tools, and code repositories.

> During device hardware and software deployment, the configuration of the development environment can be modified. Therefore by managing this changing environment, it is necessary to maintain the system under development in a secure state.

6) Penetration Test

A penetration test can be performed after integration of the system in the CD/ES phase as a part of the functional performance tests of the system. As studied in the threat analysis, possible attack scenarios can be used for the test. There can be a potential for a disruption of the system when simulated attacks are conducted.

> Penetration Test is a simulated cyber attack against the system to test it for exploitable vulnerabilities. It is advised that this procedure be carried out on a test platform or on additional items to maintain the safety.

Conclusion

The characteristics of NPP I&C systems are described, and the considerations needed when conducting cyber security activities during the SD and CD/ES phases within the lifecycle process of the I&C systems are discussed. It is claimed that 1) maintaining a secure development environment and 2) developing the proper security features of the I&C systems are two important goals in cyber security designs or assessments.

> The applications of computers and network technologies in nuclear power plants have expanded recently and these applications to the instrumentation and control systems of nuclear power plants brings cyber security concerns similar to other critical infrastructures. While the instrumentation and control systems of nuclear power plants are similar to industrial control systems, the former have specifications that differ from the latter in terms of architecture and function, in order to satisfy nuclear safety requirements, which need different methods for the application of cyber security risk assessment.

1287 words

Source: http://koreascience.or.kr/article/JAKO201206735655088.page

JAE-GU SONG, JUNG-WOON LEE* , CHEOL-KWON LEE, KEE-CHOON KWON, and DONG-YOUNG LEE
Korea Atomic Energy Research Institute
989-111 Daedeok-daero, Yuseong-gu, Daejeon 305-353, Republic of Korea
*Corresponding author. E-mail : leejw@kaeri.re.kr

Received November 21, 2011
Accepted for Publication March 13, 2012