Progress in Nuclear Energy 88 (2016) 88–94

Contents lists available at ScienceDirect

Progress in Nuclear Energy

journal homepage: www.elsevier.com/locate/pnucene

Implementation of cyber security for safety systems of nuclear facilities

JaeKwan Park*, YongSuk Suh, Cheol Park

Korea Atomic Energy Research Institute, Daedeok-Daero 989-111, Yuseong-gu, Daejeon, South Korea

ARTICLE INFO

Article history:
Received 3 September 2015
Received in revised form
15 December 2015
Accepted 22 December 2015
Available online 2 January 2016

Keywords:
Cyber security
Computer security
Cyber security plan
Cyber security implementation
Software verification and validation

ABSTRACT

Digital computers have been chosen as a safety system in newly constructed nuclear facilities. Owing to digitalization, cyber threats to nuclear facilities have increased and the integrity of the digital safety systems has been threatened. To cope with such threats, the nuclear regulatory agency has published guidelines for digital safety systems. This paper suggests an implementation method of cyber security for the safety system in the development phase. It introduces specific security activities based on a practice in a nuclear facility construction project. It also explains experiences resolving security vulnerabilities of the system and gives lessons learned about considerations in a real construction.

1. Introduction

During the last decade, digital systems have replaced legacy analogue systems extensively in nuclear facilities because the analogue products are no longer produced by the manufacturers. Another reason for such modernization is that nuclear ordering organizations prefer computer systems with a strong performance, high reliability, and convenient maintainability. However, software-based systems are faced with cyber security problems that may compromise their safety functions. In addition, security considerations have often been ignored in the system development process.

Recently, it has been reported that several nuclear facilities have been attacked and malfunctioned by outside intruders (Kesler, 2011). The slammer worm attacked a vulnerability of systems and made malfunctioning of the safety parameter display systems at the Davis–Besse plant in 2003. A shutdown of the Browns Ferry plant was also caused by a cyber-attack in 2006. In 2010, manipulation of the control systems by cyber-attacks was realized in a 'Stuxnet' accident. The Stuxnet was designed to attack programmable logic controllers (PLCs). It exploited the vulnerabilities of Microsoft Windows to manipulate the Siemens control system in an Iranian nuclear plant. As a result, it compromised the PLCs and ruined almost one-fifth of the centrifuges. Nowadays, cyber-attacks have been detected and reported in many plants in the world.

To cope with cyber-attacks, various studies have been carried out in the IT and nuclear industries. Zakaria I. Saleh et al. (2011) suggested a security risk assessment framework in the IT industry. The framework includes processes for a security risk and vulnerability assessment. As efforts in the nuclear industries, Nai Fovino et al. (2011) presented the outcome of information and communication technology (ICT) security assessment targeting an operational power plant. The results show that the vulnerability of a plant to malicious attacks is severe. Lee et al. (2009) introduced a practice for a cyber security risk assessment in power plants. The assessment consists of a target system analysis, asset analysis, threat analysis, vulnerability analysis, risk analysis, and intrusion tests to identify the risks. Park et al. (2013) proposed an approach to establish a cyber security program in a research reactor facility. It explains the graded application of security controls in a small facility.

As emphasized in previous studies, the safety systems should be strengthened against unauthorized accesses. To address these issues, national laboratories, utilities, and regulatory bodies have tried for a long time to find the best way to cope with not only attacks by intruders from outside but sabotage from inside. Since 2006, regulatory guidelines and industrial standards for cyber

* Corresponding author.
E-mail addresses: jkpark183@kaeri.re.kr (J. Park), yssuh@kaeri.re.kr (Y. Suh), cpark@kaeri.re.kr (C. Park).

http://dx.doi.org/10.1016/j.pnucene.2015.12.009
0149-1970/© 2016 Elsevier Ltd. All rights reserved.

security have been published. Therefore, these guidelines should be strongly considered in the development process of digital systems. However, there have been few studies on software development frameworks concerning the emerging cyber security issues. Most digital safety systems have been developed under the software development process guided by the industrial standard (i.e., IEEE 7-4.3.2-2003) without cyber security considerations.

This paper suggests a security-enhancing verification and validation (V&V) method incorporating the cyber security considerations into the software development process for the digital safety system. It recommends that security vulnerability analysis, security design V&V, and security evaluation be performed together with a legacy V&V. To give a detail explanation, an example of a safety system development in a realized construction project is shown and the specific results through the security V&V activities are explained.

To describe the research results, this paper consists of the following sections. Section 2 explains the relevant nuclear regulations and regulatory guidelines of cyber security. Section 3 introduces a cyber security implementation plan for a safety system. In Section 4, an example of the cyber security implementation at a nuclear facility construction project is presented. Finally, a conclusion is given in Section 5.

2. Cyber security requirements in nuclear power plants

10 CFR (Title 10, of the Code of Federal Regulations) and regulatory guidelines published by the United States nuclear regulatory commission (USNRC) are internationally referenced for the design and construction of nuclear plant facilities. The NRC has provided two specific guides: USNRC (2006) and USNRC (2010) for cyber security. USNRC (2006) describes what the staff of the NRC deems acceptable for complying with the regulations for promoting high functional reliability, design quality, and cyber security for the use of digital computers in the safety systems of nuclear power plants. It requires the system features and development activities for cyber security to be implemented and performed through the system development lifecycle. In addition, USNRC (2010) describes a systematic framework and technical methods for the operation and maintenance of nuclear plants to protect digital assets from cyber-attacks. It requires that a defense-in-depth strategy, security controls, and the continuous monitoring be provided during the plant operation. The international standard (IEEE, 2010) also mentions that the digital safety system/equipment development process shall address potential security vulnerabilities in the proper phase of the digital safety system lifecycle, and system security features should be addressed appropriately in the lifecycle phases. In July 2011, the NRC published (USNRC, 2011) to provide consistency with RG. 5.71. The point of view of the guide was changed into a secure development and operational environment. In addition, the requirements for the plant operation phases from installation to retirement were eliminated because the RG. 5.71 provides guidance for the phases. Fig. 1 shows the codes and standards related to the cyber security.

In summary, the requirements of RG 1.152 should be met in the safety system level and the requirements of RG 5.71 should be considered in the plant facility level. Digital safety systems referring to NRC's regulating positions are enforced in conformance with RG 1.152. This paper refers to these requirements as the research basis.

3. Implementation plan of cyber security for safety system

Safety-grade digital computers are used for the reliable protective functions of nuclear facilities. This section introduces a planning for cyber security of the safety systems. Shortly, the cyber security considerations have been incorporated into the safety system development process.

3.1. Relationship between V&V activities and cyber security activities

A well-known industrial standard, IEEE, 2004, endorsed by the nuclear regulatory body gives specific activities for software verification and validation (V&V) of digital safety systems. The security analysis mentioned in the standard has been interpreted as the concept of physical security only. Considering recent regulatory positions, it is acceptable that the security analysis should be conducted for the cyber security of digital systems. Thus, this study decomposes the standard requirements into three major parts, software V&V, safety analysis, and cyber security analysis. The analysis results for each part through the development phases are published independently. Fig. 2 shows the cyber security plan within the V&V plan of the system.

Generally, system developers use qualified commercial-off-the-shelf (COTS) products as the platform of safety systems. Software V&V and a safety analysis only focus on logic source codes that are newly developed within the products. In the case of a security analysis, the security capability in the past does not ensure the same effectiveness currently due to continuously evolving cyber threats. Therefore, this paper recommends that the hardware and software of the COTS are included as review items in the security analysis.

3.2. A cyber security plan

This section proposes a cyber security plan including a cyber security team (CST) organization and security activities implementation. The cyber security team consists of a team leader and team members. The major missions of the team are as follows:

- supervision of the secure development environment,
- analysis of the system vulnerability and penetration test to the system,
- introducing cyber security requirements,
- tracking and resolving security issues,
- assessing security impact on the system integrity, and
- reviewing the results of development phases

The system development model for the digital system is a well-known waterfall design model, which consists of the concept, requirement, design, implementation, and test phases. This paper adds security activities to the design model to perform the security team missions. Fig. 3 shows the security activities defined in the plan.

- **Attack Path Analysis:** Used to identify accessible pathways to the system cabinet physically and logically. Non-accessible pathways by existing security controls are found in this activity. It is used as evidence for justification that the security controls used to eliminate vulnerabilities at the pathways can be excluded in the system. Detailed information about the accessible pathways is utilized as input to the penetration test of the system.
- **Penetration Test:** Used to test whether attackers can jeopardize the system through the identified pathways or not. If the cyber-attacks actually impact the system functioning, then security controls used to block the attacks are proposed in this activity.
- **Security Requirements V&V:** Hardware and software requirements for the cyber security are defined as part of the