A Practice of Secure Development and Operational Environment Plan

Jaekwan Park [a*], Sangmun Seo [a], Yongsuk Suh [a], Cheol Park [a]
[a]*Korea Atomic Energy Research Institute (KAERI), Daedeok-Daero 989-111, Yuseong-Gu, Daejeon, 305-353, Korea*
[*]*Corresponding author: jkpark183@kaeri.re.kr*

1. Introduction

Recently, nuclear instrumentation and control system (I&C) has been faced with two licensing issues, cyber security (CS) and secure development and operational environment (SDOE). Many studies related to the cyber security have been introduced. However, few studies on SDOE establishment have been proposed because specific regulatory positions have been recently arranged to avoid confusion with cyber security and to align with software V&V. Therefore, various studies related to systematic processes to comply with the SDOE requirements during the development and operational phases are necessary.

This paper suggests a practice of plan for SDOE establishment in a nuclear I&C. First, it is necessary to perform a requirements analysis to define key regulatory issues and determine the target systems. The analysis includes a survey to find out the applicable measures credited internationally. Based on the analysis results, this paper proposes an implementation plan including a process harmonizing security activities with legacy software activities and applicable technical, operational, and management measures for target systems.

2. Requirements Analysis and Implementation Plan

2.1 Requirements Analysis

The regulatory body requires safety systems to comply with IEEE Std. 603 [1]. IEEE Std. 603 contains clause 5.6.3 addressing independence between safety systems and other systems, and clause 5.9 addressing control of access. RG 1.152(R3) [2] provides an acceptable method complying IEEE Std. 603 clause 5.6.3 and clause 5.9. In addition, U.S. NRC standard review plan (NUREG-0800) appendix 7.1-D, "guidance for evaluation of the application of IEEE Std. 7-4.3.2," defines the security analysis as SDOE and mentions RG. 1.152(R3) for specific guidance on SDOE. RG 1.152(R3) contains five regulatory positions regarding the establishment of an SDOE to ensure the high functional reliability of digital safety systems to support compliance with the above regulations.

Basically, application targets of the above codes and standards are digital safety systems. They are not mandatory requirements in non-safety systems. However, digital systems performing functions protecting reactor, such as an alternate protection system (APS) and automatic seismic trip system (ASTS) are strongly recommended to consider the SDOE requirements.

SDOE is divided into two key concepts, a secure development environment (SDE) and secure operational environment (SOE). SDE is the condition of having appropriate physical, logical, and programmatic controls during the system development phases to ensure that unwanted, unneeded and undocumented functionality is not introduced into the system. SOE is the condition of having appropriate physical, logical, and administrative controls within a facility to ensure that the reliable operation of the system is not degraded by undesirable behavior of connected systems and events initiated by inadvertent access to the system. The establishment of a SDOE for a digital safety system refers to the following:

- ✓ measures and controls taken to establish a secure environment for the development of a digital safety system against undocumented, unneeded, and unwanted modifications, and
- ✓ protective actions taken against a predictable set of undesirable acts (by human or by connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system.

The measures and actions for a SDOE establishment include the adoption of protective design features into the digital safety system design to preclude inadvertent access to the system and protection against undesirable behavior from connected systems when operational.

2.2 Implementation Plan

This paper introduces a practice of SDOE establishment planning for a nuclear facility. The planning includes SDOE activities during development phase, applicable measures, and a documentation plan.

2.2.1. Key Considerations

A SDOE plan for I&C should be prepared and submitted to the regulatory body during a review of the preliminary safety analysis report (PSAR). The plan aims to provide a systematic process analyzing potential susceptibility and implementing protective means against three concerns as follows:

- ✓ Unnecessary codes during the development phases
- ✓ Inadvertent accesses during the operational phases
- ✓ Undesirable behavior during the operational phases

2.2.2. SDOE activities and susceptibility analysis

As shown in Figure 1, a potential susceptibility analysis is performed as the initial activity of the SDOE plan. The key points in this analysis are to determine a predictable set regarding the system life cycles and to introduce specific SDE and SOE requirements for the target systems. This analysis is performed based on the system design documents before equipment procurement and manufacturing. The additional requirements are incorporated and implemented through the system verification and validation (V&V).

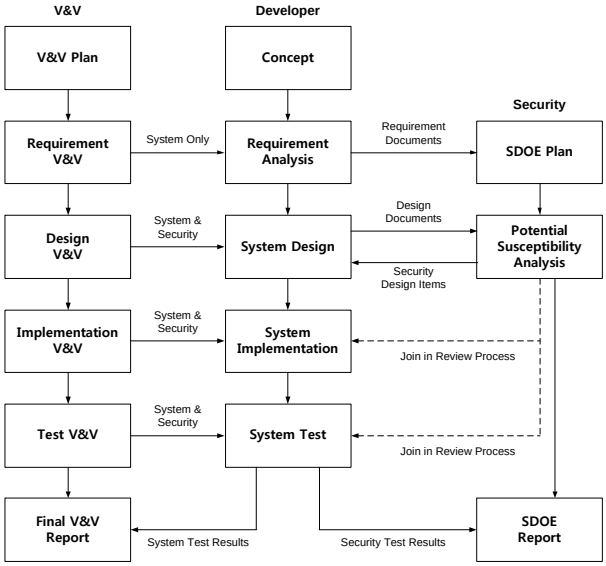

Fig. 1. Harmonizing V&V and Security Activities

2.2.3. Applicable Measures

Applicable measures against unnecessary codes are considered in the plan. For digital safety systems, simpler systems are better because they result in more predictable and deterministic behaviors. Unnecessary code in a system is considered to be a potential source of unpredictable behavior, such that the reliable operation of the digital safety system could be affected. Thus, a SDE is established for the digital safety system such that there is reasonable assurance that unnecessary code is not incorporated into the system.

There are two types of software codes, pre-developed software (i.e., platform software) manufactured by the equipment supplier, and application software implemented by the component designer. For the pre-developed software, SDE is addressed by the high-quality software processes used in digital safety system development. For this purpose, the plan includes a review of the platform documents such as a CGI dedication, secure development environment, and software configuration management. For the SDE of the application software, the plan includes software V&V, configuration management of the code, requirement traceability, and control of the test environment.

Moreover, measures against inadvertent access of human and undesirable behavior of connected systems are prepared in the plan. Malicious activity is addressed under the cyber security programs [3]. Inadvertent access is postulated to be an event involving the facility personnel or an on-site contractor without a criminal motive. Physical points of access include open communication ports on the system that someone from the licensee's workforce may mistakenly attempt to connect into. Logical points of access include any points of human interface on systems connected to the same network on which the digital safety system resides. Connected systems perform various behaviors under normal and abnormal conditions such as a failure and exception handling. Such behaviors can affect the safety systems and cannot be handled by them.

An SOE is established for a digital safety system such that it can be demonstrated that reasonable measures have been taken to prevent inadvertent access to the system and prevent undesirable behavior from connected systems from affecting its reliable operation.

Barriers and alarms protecting physical and logical access to digital safety systems are designed as counter measures of inadvertent access. The barriers include cabinet installation in a restricted area, cabinet door locking, a hardware-based key switch for a software download, an administrative procedure for cabinet key management, and blocking open ports. The alarms include alerts related to cabinet door open and software downloads.

Considerations regarding undesirable behavior protections are also described in the plan. First, some design restrictions are provided for secure operation. A minimization of the data communication between safety and non-safety systems is strongly recommended in an I&C design. Remote access and wireless communication are excluded. In addition, applicable technical controls for undesirable behavior protections are considered in the plan. The controls include isolation of the digital safety system [4], hardware-based devices that enforce one-way communication, software-based protocols for one-way communication, CRC checks on the software code, channel deviation alerts, and self-diagnostic alerts.

Requirement traceability, barrier design, and isolation implementation of the safety system are the most creditable and essential protection controls for SDOE establishment according to the review results both domestically and overseas.

2.2.4. A Documentation Plan

The potential susceptibility analysis is performed based on the proposed measures to establish an SDE and SOE. Additional measures can be found and documented through a detailed analysis process. Thus,

a set of SDOE requirements are defined in the potential susceptibility analysis report.

As shown in Figure 1, the software program manual is prepared such that it refers to the potential susceptibility report for the SDOE requirements. The controls are then continuously verified and validated through the software V&V processes together with the system requirements. Tracing and V&V results for the SDOE requirements are documented within the V&V reports during the development phase. In particular, a final SDOE report separated from the final V&V report is recommended to provide sufficient demonstration regarding SDOE.

3. Conclusions

Recently, nuclear I&C has been faced with two security issues, cyber security (CS) and secure development and operational environment (SDOE). Unlike cyber security, few studies on planning SDOE have been presented. This paper suggests a plan for establishing an SDOE in a nuclear I&C. This paper defines three key considerations to comply with the regulatory position of RG. 1.152(R3) and proposes a process harmonizing the security activities with legacy software activities. In addition, this paper proposes technical, operational, and management measures applicable for SDOE.

REFERENCES

[1] IEEE Std. 603-1998, Criteria for Safety Systems for Nuclear Power Generating Stations, 1998.
[2] US NRC Regulatory Guide 1.152, Rev.3 Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, 2011.
[3] US NRC Regulatory Guide 5.71, Rev.0 Cyber Security Programs for Nuclear Facilities, 2010.
[4] US NRC DI&C-ISG-04, Rev.1, Highly-Integrated Control Rooms – Communications Issues (HICRc), 2009.