# A Classification Method of Technical Security Controls for Digital I&C Systems in NPPs

J. G. Song, J. W. Lee, G. Y. Park, K. C. Kwon, D. Y. Lee and C. K. Lee*
*Korea Atomic Energy Research Institute*
*989-111 Daedeok-daero, Yuseong-gu, Daejeon, 305-353, Republic of KOREA*
**Corresponding author:cklee1@kaeri.re.kr*

## 1. Introduction

The instrumentation and control (I&C) systems in nuclear power plants (NPPs) are a key facility to monitor plant state, control plant devices, and prevent accidents [1]. Recent I&C systems have been composed of digital systems in order to enhance the effectiveness of operation and maintenance of NPPs. An assessment method for the analysis of security controls is needed to respond to potential cyber attacks against digital I&C systems [2,3].

RG 5.71 "Cyber Security Programs for Nuclear Facilities" published by U.S.NRC in 2010 presents a comprehensive set of security controls for NPPs [4]. Although this document provides the requirements of security controls, a guidance describing which security controls should be applied to specific digital assets and how to implement them is still needed for the I&C system design and development .

In this paper, a classification method of the technical security controls listed in RG 5.71 is proposed to provide a guide useful for the application of the controls during the design and implementation phases of I&C systems.

## 2. Classification Method of technical security controls for Digital I&C Systems in NPPs

Technical security controls in RG 5.71 are grouped at a high level as follows;

- Access Controls
- Audit and Accountability
- Critical Digital Asset and Communications Protection
- Identification and Authentication
- System Hardening

These items contain a total of 71 controls at the lower level. Then the contents of controls can be further classified by more than 200 detail items by considering their relations to the security policies or the design and implementation of security features that should be included in the I&C systems during the development phases. Criteria for their classification are necessary since no detail description about the application of these technical control items in specific digital assets is available in RG 5.71. Without the classification criteria the assessments of cyber security for I&C systems may become ambiguous.

In this paper, the technical control items were analyzed and classified in aspects of "Phase," "System," "Function," and "Checklist Type." Details of this classification are described in Table 1 as below.

Table 1: Classification Scheme

| Group | Abbr. | Classification | Description |
|---|---|---|---|
| Phase | DP | Design Phase | System Design |
| | IP | Implementation Phase | Component Design & Equipment Supply |
| System | SS | Safety System | - |
| | NS | Non Safety System | - |
| Function | C | Control System | I&C S/W, PLC, DCS |
| | I | Information System | HMI PC, Server, Database, IT Systems |
| | N | Network | All networks in MMIS |
| | O | Operating Environment | - |
| Checklist Type | M | Mandatory | Mandatory checklist |
| | R | Recommended | Recommended checklist |

Each technical control item then can be classified through a procedure as shown in Fig.1.

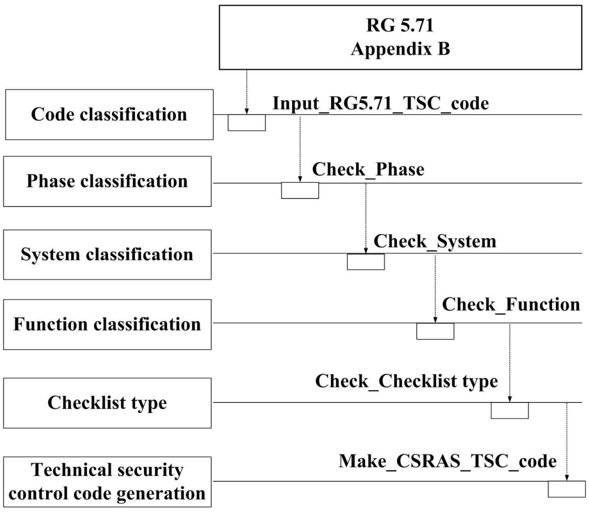

Fig. 1. A procedure for the classification of technical security controls.

This classification scheme considers the development phases for new NPPs, which are the design phase and the implementation phase. The level of depth for technical control design can be graded during these two phases.

Based on the proposed classification scheme, the technical control items can be defined in detail as shown in Table 2.

Table 2: Classification Scheme

| | |
|---|---|
| Control Item Code | B.1.1_2 |
| Vulnerability Code | NPPCS-DP-SS-C/I/N/O-002-M-P/D/M |
| Condition | - |
| Applicability | O |
| Phase | Design Phase/ Implementation Phase |
| Function | C/I/N(PLCs OS, EWS, Software with Accounts) |
| Security Subject | Managerial/Technical(Access Control) |
| CSRAS Assessment Type | Design Phase->C, Implementation Phase->CP |
| Assessment Item | Contents of controls in Design Phase |
| | Contents of controls in Implementation Phase |
| References | RG 5.71, SP 800-53, DHS ICS Security Guide, Korea Communications Commission, NIST, " Guide to enterprise password management" |

The detail contents of Control item code B.1.1_2 may include the followings [5,6];

1) Contents of controls in Design Phase

Evaluate that the design includes security function which inhibits unauthorized access to the digital I&C systems.

References : Password Security Guide

- An administrator should change passwords periodically. The change period less than 6 months is recommended.
- In case that an initial password is assigned by the system developers, the administrator should change the password immediately after the installation.

2) Contents of controls in Implementation Phase

Evaluate the techniques used for controlling unauthorized access.

- Use of safe passwords

1. character strings with a length of more than 8 characters and having more than three different types of characters

2. character strings with a length of more than 10 characters and having more than two different types of characters

- Prohibition of vulnerable password uses

1. passwords composed of well-known computer terminologies, sites, name of companies, etc.

2. passwords in specific patterns by repeating same characters or by using characters located sequentially on a keyboard

- Application of data encryption algorithm

1. SEED block encryption(128 bit, 256 bit)

2. ARIA block encryption (128 bit, 256 bit)

3. HIGHT block encryption (128 bit, 256 bit)

References : Guide for the selection and use of passwords, data encryption algorithm

The assessments based on the above classification scheme can be performed by using qualitative methods. The CDA analysis by I&C experts will act the most important role in the assessments.

## 3. Conclusions

This paper proposes a classification scheme of technical security controls that can be applied to the I&C systems in NPPs. This classification scheme can be applied to the controls mentioned in RG 5.71 and also in NIST 800-53.

When analyzing the controls by using the proposed classification scheme, it is possible to meet controls that cannot be defined properly or to get the same or similar analysis results for control items repeatedly. A further study to classify and manage these similar control items will be needed.

The results from this study will be used as assessment criteria being included in CSRAS(Cyber Security Risk Assessment/Analysis System), which is under development as a tool for the assessments of cyber security for NPP I&C systems.

## Acknowledgement

This work was supported by the nuclear Technology Development Program of the Korea Institute of Energy Technology Evaluation and Planning(KETEP) grant funded by the Korea government Ministry of Knowledge Economy (No. 2010161010001E).

## REFERENCES

[1] IAEA Nuclear Technology Review issued for the 2008 IAEA General Conference - Annex 5: Instrumentation and Control (I&C) Systems in Nuclear Power Plants: A Time of Transition, 2008.

[2] IAEA Nuclear Security Series No.17 Technical guidance, Computer security at nuclear facilities, 2011.

[3] Jung-Woon Lee, Cheol-Kwon Lee, Jae-Gu Song, and Dong-Young Lee, Cyber Security Considerations in the Development of I&C Systems for Nuclear Power Plants, The International conference on Security and Management(SAM), 2011.

[4] USNRC Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, 2010.

[5] NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, August 2009.

[6] NIST Special Publication 800-118(Draft), Guide to enterprise password management, April 2009.