# 제어계측 시스템 환경에서의 사이버 보안 통제 지원 시스템

# A System  for Supporting The Cyber Security Control of I&C System

정현미*, 김석훈**, 성 경***0

Hyun-Mi Jung*, Seok-Hun Kim**, and Kyung Sung***0

## 요 약

제어계측 시스템과 정보시스템은 서로 차이가 있으며 두 시스템의 보안설계가 다르다. 이러한 문제점을 해결하기 위해 제어계측 시스템의 보안통제를 설계하기 위해서는 보안통제가이드를 기본으로 한 정책 설정 및 모델링 작업의 필요성이 대두되고 있다. 본 논문에서는 제어계측시스템 환경에서 사이버 보안 통제를 지원하기 위하여 보안규제 가이드를 기반으로 역할, 보안 통제 별 및 문서간의 관계스키마를 설계하였고, 설계된 스키마는 보안규제가이드를 준수하기 위한 사이버 보안 통제 구축 지원 시스템의 계획, 설계, 구현을 지원 하는 데이터베이스와 내용으로 활용이 가능하다. 이후 제안된 스키마를 활용하여 시스템 프로세스를 설계하고 제어계측 시스템에 최적화된 보안통제지원 시스템을 개발한다.

## Abstract

I&C (Instrumentation & Control) system is different from information system and  the security design of the two systems are also different. The modeling activity is needed based on the security control guide in order to build I&C system security control. In this paper, the role and by the security control, we designed the relationship (that is, the relation schema) between the documents for ‘The system for supporting the cyber security control of I&C system design’ based on the security control guide. The designed schema plans ‘The system for supporting the cyber security control of I&C system’ for observing the security control guide, and is used as the database and content that supports its design and implementation. The process and system of the proposed schema is utilized and designed. The design of the schema and system is intensified in the design phase with the proposed mode and supporting the I&C system cyber security design.

Key words : 사이버보안(cyber security), 제어계측 시스템 보안(security management), 관계스키마 (regulatory guide), 역할기반 스키마(relational schema), 보안통제가이드(role - based schema)

## I. Introduction

Provided is the equipment for leaving the software package which is used to control and monitor the production process known as I&C(Instrumentation & Control) system. This is used in industries to control plant conditions that it monitors as registers [1, 2]. It is within a network that becomes independent and

* 한국과학기술정보연구원(Korea Institute of Science and Technology Information)
** 수원여자대학교 모바일미디어과(Department of MobileMedia, Suwon Women's College)
*** 목원대학교 컴퓨터교육과(Department of ComputerEducation, Mokwon University)
· 제1저자 (First Author) : 정현미(Hyun-Mi Jung)
0 교신저자 (Corresponding Author) : 성 경(Kyung Sung, Tel : +82-10-5377-6307, email:skyys04@mokwon.ac.kr)

· 접수일자 : 2013년 7월 15일 · 심사(수정)일자 : 2013년 7월 15일 (수정일자 : 2013년 8월 26일) · 게재일자 : 2013년 8월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.4.442

physically separated and uses its own operating system and the feature that it is protected by a powerful access control. Thus, since carrying the different characteristics in a service response, communication protocol, network structure, and etc. from the general information system, most of I&C systems does not consider (particularly, the cyber security) and are designed with regards to security. However, for an I&C system, the weakness about cyber security is continuously exposed. Thus, systems become unsafe in terms of cyber security. For example of threats, There are Indiscretion by personnel, Bypass Controls, Authorization violation, Man-in-the-middle, Resource exhaustion and so on. In this paper, the method that I&C systems are constructed considering cyber security from the design phase is proposed.

First, the schema is designed in order to develop ‘The system for supporting the cyber security control’ helping with I&C system design based on the security control guide. When designing the schema, the existing role-based access control policy is analyzed for the role relation production and is the predecessor for the item role relation production to be used as security restriction guide. ‘The system and process for supporting the cyber security control of I&C system’ is proposed based on the schema which then is designed.

We first introduce I&C(Instrumentation & Control) system, access control and policy model in general, in section 2. In section 3, we propose a schema and system development in I & C system. That is refer to modified access control and policy model. Finally we summarize our result.

## Ⅱ. Access control policy model

The three principles of access which ISO 15489 presents are as follows [3]. First, an official guideline is prescribed in which it allows to approach the register from any kind of environment. Then, effectually, the access condition has to be given to the register and all people to control the access. Finally, the time of recording must be appropriate as it approaches and search for effectively. The first and second principles take care of the access control while the third principle takes care of the access offer [4, 5, 6, 7]. Table 1 shows comparison of access control policy.

표 1. 접근통제 정책 비교
Table 1. Comparison of access control policy

| Classification | Access control | Feature |
|---|---|---|
| MAC (Mandatory Access Control) | Security Label | The focus is adjusted on the security for the confidentiality of the graded information. |
| DAC (Discretionary Access Control) | Permission | The access privilege is according to the owner of the object and it can be arbitrarily changed. |
| RBAC (Role-Based Access Control) | Role | Accepting as the model advanced above 2 models. |

It is accepted in the access control policy as the model in which the RBAC((Role-Based Access Control) model is progressive till now most and which is efficient.

However, it is difficult to determine the specific I&C system whether what purpose can this kind of subject must have and what kind of object it can approach or not under any kind of condition in order to apply the security control guide.

In this existing role based model, whereas the reason why the design is difficult to assign permission through each role security category (that is, it is seen as the relation from the guideline schema for designing) and each of the security category can succeed with authority, since each authority has to be set up according to the security restriction guide, the schema is designed with the concept of each role and authority assignment rather than the concept of the authority inheritance of each role. Thus, in this paper, the role-based relationship is produced and the schema is designed based on the security control guide.

## Ⅲ. SCHEMA AND SYSTEM DESIGN

### 3-1 Role and relationship design of the security control guideline base

In this section, the authority and role is defined based on the security control guide for I&C system[8]. Each role's authority is set and defined. In this door, 'REGULATORY GUIDE 5.71(CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES)' is used as the security control guide for the practical example [9, 10].

- Role set-up

The role is drawn based on the security control guide is shown in Table 2. All roles, including the security policy personnel are comprised of one organization or only one person. The user of 'The cyber security control construction support systems' implemented through the actually designed schema is the security control developer itself [11].

표 2. 역할설정
Table 2. Role set up

| The role # | The role classification | Contents |
|---|---|---|
| P .policy | Policy of security | All security policies and plan is established and it distributes. |
| R. procedure | Procedure of security | The security procedure establishment and distribution. |
| O .operator | Operator of security | The practice of the security policy and procedure. |
| D. developer | Security control developer of the I&C system | The access control and code Implementation. |
| E .evaluator | Security evaluator of the I&C system | RG 5.71 security control evaluator |
| M. manager | Security manager | The policy, plan, and operational checking state. |

- Mapping recommended each role

Each role's authority is given in the schema generation. The three authorities are defined as follows.

- The production concept: the access privilege is in the document and the document can be produced based on the guideline and the permission (distribution) and can be changed.
- The reference concept: the access privilege is in the document but the business is performed with reference to the generated document.
- The other concept: there is none, but in case of being entrusted with the authority the access privilege is defined in the document and can perform the entrusted production and reference authority.

The recommended mapping to each role is shown in Table 3.

표 3. 각 역할별 기호
Table 3.Mapping recommended to each role

| Permissions | Expression |
|---|---|
| *. production | *. *production* → |
| *. reference | *. *reference* ⊃ |
| *. other | *. *other* ∀ |

- Table organization for the schema generation

Table 4 depicts the configuration content of the table for the schema generation.

표 4. 스키마 테이블 구성
Table 4.Contents of table for the schema

| Object | Name of table |
|---|---|
| Document table | DOC_1······ m |
| Role table | P, R, O, D, E, M |
| Control table | CON_1...··· m |

- Operation

Table 5 depicts the relational table that defines the relational operations for the schema design.

표 5. 관계 테이블
Table 5. Relational table

| Relational table | Example of operation |
|---|---|
| The Control – Document table | CON → DOC<br>CON ⊃ DOC<br>CON ∀ DOC |
| The Document – Control table | DOC (→, ⊃, ∀) CON |
| The Document – Role table | DOC (→, ⊃, ∀) P. *production* |
| The Role – Document table | P. *production* (→, ⊃, ∀) DOC |
| The Control – Role table | CON (→, ⊃, ∀) R.*reference* |
| The Role – Control table | R.*reference*(→, ⊃, ∀) CON |

## 3-2 Requirement of schema design

The questionnaire for the guidelines of the database schema design of 'The cyber security control construction support systems' is indicated in the next section.

- Guideline retrieval mode

- "The document list" for 'the B.1.8 system use announcement' control?

ex) DOC_ m⊃ CON_B.1.8

- Who and what type of document does 'the B.1.8 system use announcement' control relate to?

ex) CON_B.1.8 & *. Production & DOC _ m

- Does the 'developer' develop any kind of 'document' or does refer to?

ex) D. reference → DOC _ m ∥ D. reference⊃ DOC _ m

- Construction support mode

- The actual document file (in the example, the security policy) of the control system for the nuclear power plant is delivered to the necessary person (in the example, the developer and projector) in order to evaluate 'the B.1.8 system use announcement control'.

- The developer A and projector B does the necessary document (in the example, the security policy, in actual, the annunciation system) with the preparation (the template use) and in order to implement 'the B.1.8 system use announcement' control is stored in the document table.

## 3-3 Schema design

Figure 1 shows the integration of the requirements and the quality of the formation of relationship in chapter 2 and 3.

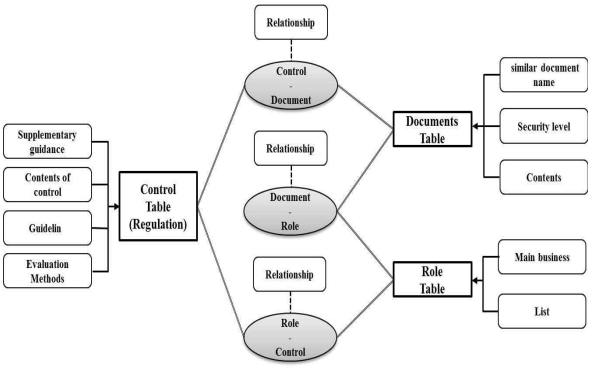


그림 1. 스키마
Fig. 1. Design of schema

## 3-4 Cyber security control construction support system

The design of the process of 'The cyber security control construction support system' based upon the designed schema is shown in Figure 2.

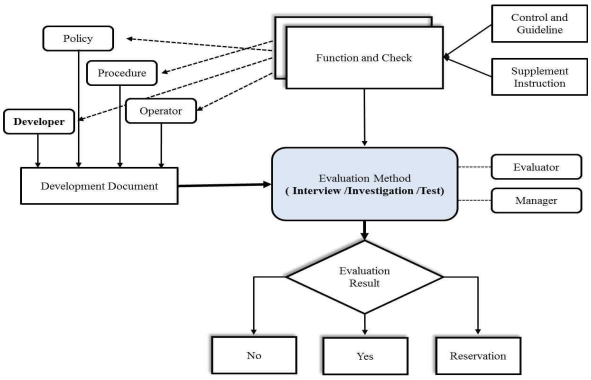


그림 2. 시스템 프로세스
Fig. 2. Process of 'Cyber security control construction support system'

The following Figure 3, 4, 5, 6 shows the implemented example of 'System for supporting I&C

system cyber security control construction system' designed by using the schema. The check-list (the security restriction guideline base) is indicated in one methods among the interview / investigation / test if the designer attempts the implementation in the I&C system design. It shows that the system is designed with security if the answer type is "Yes". Supplement instruction and control & guideline are shown if the answer is "No".

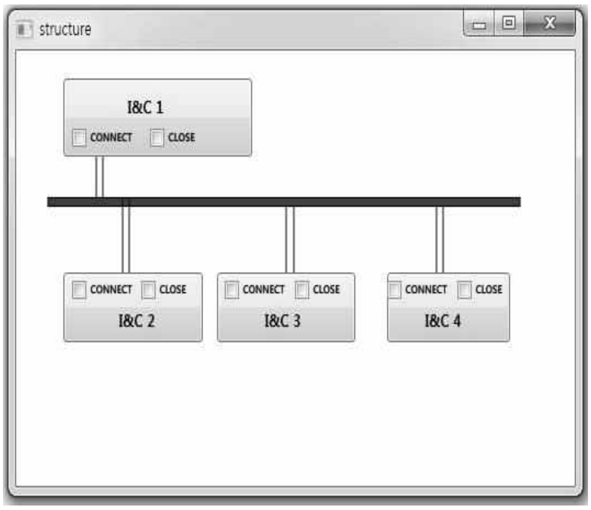


그림 3. 시스템 기본 구조
Fig. 3. System main frame

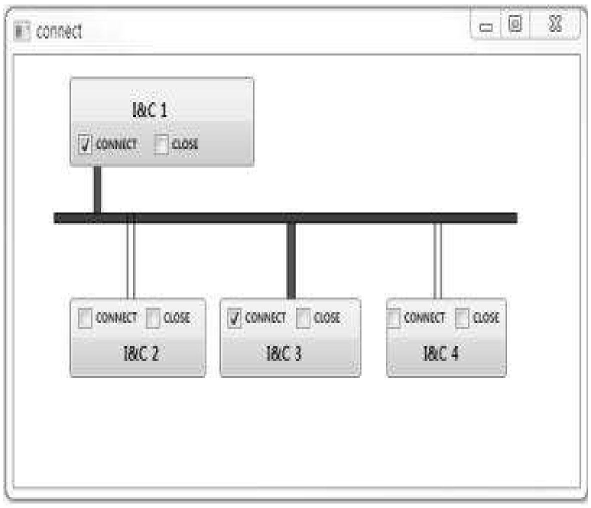
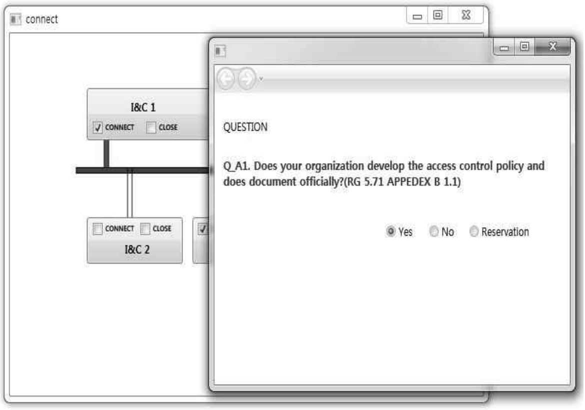


그림 4. I & C 시스템 설계 화면
Fig. 4. Display of I&C system design

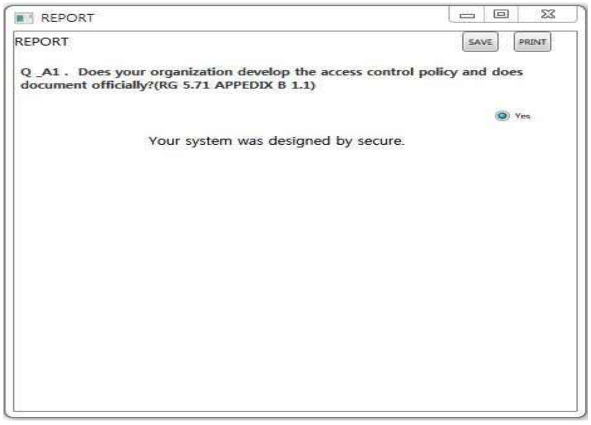


QUESTION

Q_A1. Does your organization develop the access control policy and does document officially?(RG 5.71 APPEDEX B 1.1)

● Yes ○ No ○ Reservation

그림 5. 시스템 응답화면
Fig. 5. Response



REPORT

Q _A1 . Does your organization develop the access control policy and does document officially?(RG 5.71 APPEDIX B 1.1)

● Yes

Your system was designed by secure.

그림 6. 결과보고
Fig. 6. Report

## IV. CONCLUTION

In this paper, the activity for building the security control in I&C system based on the security control guide was modeled. The role of each horn and relationship (that is, the guideline schema) between (that is, the security control in RG 5.71) the security control and document are designed. This paper can be used as the database schema and contents when developing the 'The construction support systems' supporting the plan of 'The interval security control construction', for observing the security control guide design, and implementation and evaluation. In addition, the designed schema producing the rule at the role-based and with applying the existing RBAC model was efficiently designed.

The comparison of merits and demerits on the way of using the role-based authority setting with the RBAC model for this schema design is shown in Table 6.

표 6. 비교분석
Table 6. Comparison

| Item | RBAC | The suggested role – based authority setting |
|---|---|---|
| The access authorizer | Central Authority | The task corresponding people of the security control |
| Decision criterion | Role | Role |
| Feature | The office separation and least privilege.<br>It is efficient and being more flexible. | The annual production about the role and document.<br>The search is fast and it is easy in the schema design. |
| The schema | It is useful to the commercial and information system. | It is optimizes in the I&C system. |

The security control and other features are supplemented in this schema and system design process by using security control guide and by role, the search by document becomes possible, fast and easy. In addition, by designing I&C system considering the cyber security based on the security control guide, the risk factor can be removed from the system design phase.

## References

[1] 2004 The White Paper of National Information Security, http://www.nist.go.kr

[2] Ron Derynck , "Cyber-Security and System Integrity for Transportation Networks," *VeronoWhitepaper, 2004*

[3] Sylvia Osborn, Ravi Sandhu, Qamar Munawer, " Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies," *ACM Transactions on Information and System Security,* vol. 3, No. 2, Pages 85-106, 2000

[4] National Institute of Standards and Technology , http://hissa.nist.gov/prject/rbac.html

[5] http://www.ecs.syr.edu/chin/cse774 /readings/rbac/ p34-ferraio.pdf

[6] National Institute of Standards and Technology , http://csrc.nist.go.kr/rbac

[7] http://en.wikipedia.org/wiki /Role-based_access_control

[8] Hyun-Mi Jung, Kyung-Su Han and Gang-Soo Lee ," A Schema Design for Supporting The Cyber Security Control of SCADA ," *Journal of Korea Knowledge Information Technology,* vol 7, No 6, 2012

[9] The Nuclear Regulatory Commission, http://nrc-stp.ornl.gov/slo/regguide571.pdf

[10] Cyber security programs for nuclear facilities; Regulatory Guide 5.71, U.S. Nuclear Regulatory Commission , 2010

[11] Hyun-Mi Jung , Kyung-Su Han, Gang-Soo Lee and Su-Jin Jang "A role-based access analysis for the cyber security management," *Journal of Future Game Technology (JFGT),* vol. 2, No. 1, 2012

### 정 현 미 (Hyun-Mi Jung)

2010년 8월 : 한남대학교 컴퓨터공학과 (공학석사)
2010년 9월~현재 : 한남대학교 컴퓨터공학과 박사과정
2012년 10월 ~ 현재 : 한국과학기술정보연구원 연구원, 과학기술사이버안전센터 연구원
관심분야 : 소프트웨어공학, 보안공학, 보안관제, 보안관제고도화 시스템 개발

### 김 석 훈 (Seok-Hun Kim)

2003년 : 한남대학교 컴퓨터공학과 (공학석사)
2006년 : 한남대학교 컴퓨터공학과 (공학박사)
현재 : 수원여자대학교 모바일미디어과 조교수
관심분야 : 모바일컴퓨팅, VoIP 등

성 경(Kyung Sung)

2003년 한남대학교 컴퓨터공학과 (공학박사)
1994년~2004년 : 동해대학교 컴퓨터공학과 교수
2004년~현재 : 목원대학교 컴퓨터 교육과 교수
관심분야 : 정보보호 및 정보관리, 컴퓨터네트워크, 신경회로망, 컴퓨터 교육 등