SCADA(Supervisory Control and Data Acquisition)시스템 사이버 보안 통제 지원을 위한 스키마 설계

정현미*, 한경수**, 이강수**

요약

스카다 시스템은 일반 정보시스템과는 차별성을 보인다. 따라서 스카다 시스템의 보안 통제를 구축하기 위해서는 '보안 규제 가이드'를 기반으로 한 모델링 활동이 필요하다. 본 논문에서는 '스카다 시스템의 사이버 보안 통제를 지원하기 위한 시스템 설계'를 위하여 보안규제 가이드를 기반으로 역할, 보안통제 별 및 문서간의 관계 (즉, 관계스키마)를 설계하였다. 설계된 스키마는 보안규제가이드를 준수하기 위한 '스카다 시스템 사이버 보안통제 구축 지원 시스템'을 계획, 설계, 구현을 지원하는 데이터베이스와 내용으로 활용된다.

A Schema Design for Supporting The Cyber Security Control of SCADA

Hyun Mi Jung*, Kyung Su Han**, Gang Soo Lee**

ABSTRACT

As to SCADA system, there is the differentiation with the other information system. Therefore, the modeling activity is needed based on the security control guide in order to build control and instrumentation system security control. In this paper, and the role and by the security control designed the relationship (that is, the relation schema) between the document for 'The system for supporting the cyber security control of SCADA system design' based on the security control guide. The designed schema plans 'The system for supporting the cyber security control of SCADA system' for observing the security control guide, and is used as the database and content that it supports the design and implementation.

Key Words : cyber security , security control ,SCADA security, relation schema, reg. guide

* 한국과학기술정보연구원(✉hmjung@kisti.re.kr)
** 한남대학교 컴퓨터공학과
· 제1저자(First Author) : 정현미 · 교신저자(Correspondent Author) : 이강수
· 접수일(2012년 10월 5일), 수정일(1차 : 2012년 11월 6일), 게재확정일(2012년 12월 18일)

Ⅰ. 서 론

SCADA(Supervisory Control and Data Acquisition)는 대개 생산 공정을 감시하고 제어하는데 사용되는 대규모 소프트웨어 패키지, 또는 플랜트 상태를 감시하고 제어하기 위해 산업체에서 사용되는 시스템으로서, 기록을 남기기 위한 설비가 제공된다[1]. 이러한 특징으로 스카다 시스템은 설계단계에서부터 정보시스템 기기와는 차별성을 보인다. 그들은 독립된 운영체제를 사용하며 물리적으로 분리되고 독립된 네트워크상에 있다. 그리고 강력한 접근제어(독립적인 망)에 의하여 보호된다는 특징을 지니고 있다. 따라서 대부분의 스카다 시스템은 일반 정보시스템과는 서비스응답, 통신 프로토콜, 네트워크 구조 등 에서 상이한 특성을 지니므로 보안에 관하여, (특히 사이버 보안), 을 특별히 고려하지 않고 설계되고 있다[2,3]. 그러나 2010년 지멘스 산업의 소프트웨어 및 장비를 공격한 "스턱스넷(Stuxnet)"이 이란의 원전 시설을 불 능화 시켰다. 이후 이와 유사한 악성코드 '듀큐(Duqu)"는 산업용 제어시스템 제조업체와 같은 조직에 침투해 설계문서 등 핵심정보 자산을 수집, 향후 제 3자 공격을 쉽게 감행 할 수 있도록 준비하는데 목적을 두고 있다[4]. 이와 같이 스카다 시스템은 이미 사이버보안에 관하여 취약점이 계속 노출되고 있다. 이제는 더 이상 스카다 시스템도 사이버 보안의 안전지대가 아니라는 의미이다. 이에 본 논문에서는 설계 단계부터 사이버 보안을 고려하여 스카다 시스템을 구성하는 방법을 제안한다[5,6].

사이버 보안을 고려한 시스템 설계를 위해서는 시스템 개발 시에 정책을 기반으로 하여야 하며 정책을 기반으로 스카다 시스템 설계를 도와주는 '사이버보안 통제 구축 지원 도구'를 개발하고자 한다. 개발된 '사이버보안 통제 구축 지원 도구'는 스카다 시스템을 설계단계에서부터 사이버 보안을 고려하게 되어 더욱 안전한 시스템으로 개발 할 수 있게 한다. 이러한 구축지원도구 개발을 위하여 우선 설계하고자 하는 스카다 시스템 설계 정책이 되는 보안 규제가이드를 기반으로 스키마를 설계하여야 한다. 설계된 스키마를 바탕으로 '스카다 시스템 사이버 보안 통제 구축시스템 프로세스'를 제안하고 앞으로 제안된 스키마와 프로세스를 이용한 '보안 통제구축지원도구'를 개발하고자 한다.

Ⅱ. 본 론

2.1 스키마 인스턴스

일반적으로 '사이버 보안 통제 구축 지원 도구'를 개발하기 위해서는 아래와 같은 문서와 과정이 필요하며 설계문서 단계에서 스키마 설계를 포함한 다.

1) 요구사항명세서
2) 설계문서
- DB 설계(스키마 설계)
- 구조설계
- UI설계 후
- 업무 및 자료 흐름 설계
3) 구현
4)시험문서
5) 시스템 / 사용자 매뉴얼

본 논문에서는 '사이버보안 통제 구축지원 도구를 개발하기 위한 스키마' 설계를 위하여 첫 번째로 사이버보안 정책인 보안규제가이드를 기반으로 권한과 역할을 정의 하였다. 이 후 정의된 권한을 기반으로 각 역할 별 권한을 설정한 후 스키마 생성을 위한 테이블 형성 및 관계를 설계한다. 위의 작업을 위하여 본문에서는 사이버 보안 정책의 기본이 되는 보안규제가이드로 원전 제어 계측시스템을 위한 사이버 보안 규제가이드 'REGULATORY GUIDE 5.71'을 이용한다[7,8].

본 스키마 설계를 위한 예시로 표준 DB 설계에 관

한 내용을 표1에서 보인다. 또한 기본적인 스키마의 예는 그림1에서 보인다.

표 1. DB 설계 예시

Table 1. Example of DB

표준 DB (참조 DB)		위험분석 DB (X 시스템의 위험 분석시)
DB명	활용자료 (예시)	
표준 자산 목록	자산분류표	X시스템 자산목록
표준 자산소유자 목록	-	X시스템 자산소유자목록
표준 보안대책 목록	800-53, CC,	X시스템 보안대책목록
표준 위협 목록	위협DB, 취약성DB	X시스템 위협목록
-	-	X시스템 위험목록
표준설문	800-53 보안통제변형 (5등급)	X시스템의 설문 (자체 위험분석용)
표준 참여자목록	-	X시스템 참여자

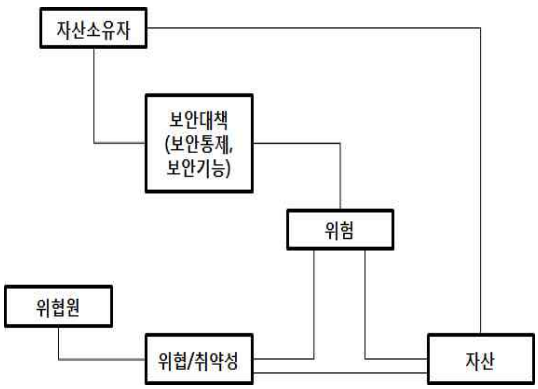

그림 1. 스키마의 예

Fig. 1. Example of schema

2.1.1 역할 도출

스키마 설계를 위한 첫 번째 작업으로 보안 규제 가이드를 기반으로 도출한 역할은 표 1과 같다. 보안 정책자를 비롯한 모든 역할은 하나의 조직 또는 1명으로 구성된다[9]. 도출된 역할 중실제적으로 설계된 스키마를 통해 구현된 '사이버 보안 통제 구축 지원 도구'를 사용하는 역할은 '보안통제 개발자'가 된다.

2.1.2 각 역할별- 권한 매핑

스키마 생성 시 각 역할(표2 역할분류 참조) 별 권한이 주어진다. 권한은 아래 3가지로 정의 한다.

- 생성(production)의 개념 : 문서에 접근 권한이 있으며 지침을 기반으로 문서를 생성, 허가(배포) 변경 할 수 있다.
- 참조(reference)의 개념 : 문서에 접근 권한이 있지만 생성된 문서를 참조하여 업무를 수행한다.
- 기타(other)의 개념 : 문서에 원칙적인 접근 권한은 없지만 권한을 위임 받았을 경우 위임 받은 생성, 참조 권한을 수행 할 수 있다.

표 2. 역할 분류

Table 2. Role set-up

역할 #	역할분류	주요업무
P.*policy*	보안 정책자	모든 보안 정책 및 계획을 수립 하고 배포 등
R.*procedure*	보안절차 수립자	보안 절차 수립, 배포 등
O.*operator*	보안 운영자	보안 정책 및 절차의 실현
D.*developer*	보안통제 개발자	접근통제 구현, 암호 구현자
E.*evaluator*	보안통제 평가자	보안통제 평가자
M.*manager*	보안 관리자	정책, 계획, 운영 상태 체크

각 역할 별 권한 생성을 위해 역할에 대한 권한 매핑이 필요하며 표 3과 같다.

표 3. 각 역할별 권한 매핑
Table 3. Mapping recommended to each role

역할 별 권한	분류기호
P. *production* P. *reference* P. *other*	P. production → P. reference ⊃ P. other ∀
R. *production* R. *reference* R. *other*	R. production→ R. reference⊃ R. other∀
O. *production* O. *reference* O. *other*	O. production→ O. reference⊃ O. other∀
D. *production* D. *reference* D. *other*	D. production→ D. reference⊃ D. other∀
E. *production* E. *reference* E. *other*	E. production→ E. reference⊃ E. other∀
M. *production* M. *reference* M. *other*	M. production→ M. reference⊃ M. other∀

2.1.3 스키마 생성을 위한 테이블 구성

다음 표 4는 스키마 생성을 위한 테이블의 구성 내용이다. 설계하고자 하는 스키마의 테이블은 각각 문서표, 역할표, 통제표로 구성되어 있으며 앞서 분석한 역할, 권한과 함께 스키마의 관계 설정에 쓰인다.

표 4. 스키마를 위한 테이블구성내용
Table 4. Content of table for the schema

객체	테이블
문서표	DOC_1..... m (m개의 문서생성 가능)
역할표	P, R, O, D, E, M (각 역할별 기호)
통제표	CON_1..... m (m개의 보안통제 적용가능)

2.1.4 연산파악

다음 표5는 스키마 설계를 위한 각 테이블 별 관계연산을 위한 관계표이다.

표 5. 관계표
Table 5. Relational table

관계표	연산 예
통제 - 문서표	CON → DOC CON ⊃ DOC CON ∀ DOC
문서 - 통제표	DOC (→, ⊃, ∀) CON
문서 - 역할표	DOC (→, ⊃, ∀) P. *production*
역할 - 문서표	P.*production*(→, ⊃, ∀) DOC
통제 - 역할표	CON (→, ⊃, ∀) R. *reference*
역할 - 통제표	R. *reference*(→, ⊃, ∀) CON

이러한 관계 표에 의하여 다음 그림2와 같이 보안통제 스키마의 인스턴스를 생성할 수 있다.

2.2 스키마 및 프로세스 설계

2.2.1 질의 요구사항

"사이버 보안 통제구축지원도구" 의 스키마 설계를 위한 질의 사항은 다음과 같으며 본 논문에서는 일부만 표시 한다 .

<지침검색 모드>

- 'B.1.8 시스템 사용 고지' 통제를 위한'문서' 목록은?
- 'B.1.8 시스템 사용 고지' 통제는 누구와 어떤 문서에 관련되는가?
- '개발자'는 어떤 '문서'를 개발 또는 참조하는가?

<구축지원 모드>

- 'B.1.8 시스템 사용 고지' 통제를 평가하기위해 X 원전의 제어시스템의 실제 문서파일들(예: 보안정책서)을 필요자(예: 개발자, 계획자)에게 전달한다.

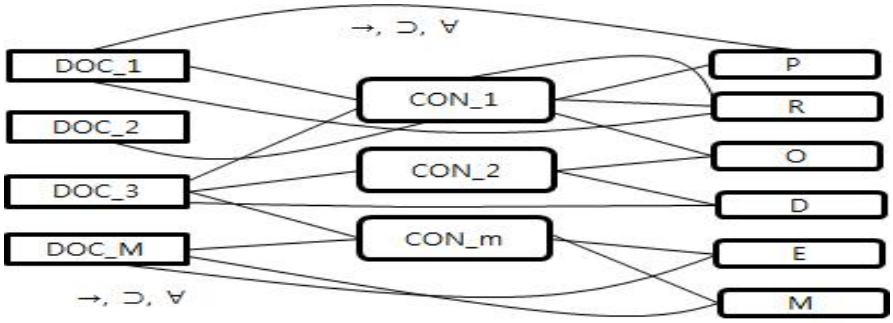

그림 2. 보안통제 스키마의 인스턴스
Fig. 2. Instant of the security control schema

- 평가자 '홍길동'이 'B.1.8 시스템 사용 고지' 통제의 평가결과(합격/불합격/유보)를 입력한다.
- 개발자 '홍길서' 및 계획자 '홍길남'이 'B.1.8 시스템 사용 고지' 통제를 구현하기위해 필요한 문서(예: 보안정책서, 실제 고지시스템)를 작성(템플리트 이용)하여 문서테이블에 저장한다.

2.2.2 스키마 설계 및 특징

2.1장의 보안통제스키마의 인스턴스 와 2.2.1 질의 요구사항을 종합하여 설계한 사이버 보안 통제 구축 지원 시스템의 프로세스는 다음 그림 3과 같다.

이후 이 프로세스를 근간으로 설계한 스키마는 그림 4와 같다. 이 스키마는 스카다 시스템에서 보안통제(보안규제가이드)를 구축하기 위한 활동을 모델링 한 것으로 역할, 보안통제별, 문서간의 관계를 설계하였다. 보안 통제(보안규제가이드)를 준수하기 위한 '스카다 사이버보안 통제 구축'시의 계획, 설계, 구현 및 평가를 지원하는 '구축지원도구'의 개발 데이터베이스와 내용으로 활용된다. 이 스키마에서 보안통제부분에 보안 정책을 보완하여 역할별, 문서별 검색이 가능하도록 하였다. 이 스키마는 보안 규제 가이드를 기반으로 최적화되어있으므로 시스템 설계 시 빠른 검색 및 가이드를 제공한다. 또한 앞으로 설계된 스키마를 기반으로 표 4에 제시된 각각의 문서표, 역할표-표 3 통제표를 생성하여 표 5 기반으로 각 테이블별 관계를 수립하여야 한다.

III. 결 론

향 후 본 논문에서 제시된 '사이버 보안통제 구축지원시스템 스키마'를 통하여 사이버 보안통제 구축 지원 도구를 개발하고자 한다. 이러한 도구에는 성능 요구사항과 기능요구사항을 분리하여 명세 하는 선행작업이 필요하다. 성능요구사항에는 대화적 질의(What -if분석), 표준성 확보를 위한 위험분석 모델 에 적용 및 자산 , 자산 가치, 위험의 시각화, 정량화, 객관화 등이 필요하며 기능요구사항에는 '보안정책 및 계획서' 생성지원, 각종 분석 결과보고서 자동생성, 가능한 위협을 제공할 수 있는 데이터베이스, 기존의 취약성 데이터베이스와 연동 기능 등이 제공 되어야 한다. 제시된 스키마는 기본적으로 보안규제가이드를 기반으로 한 보안 통제를 효율적으로 검색하고 연동할 수 있는 효율적인 방법을 제시하고 있으며 향후 성능요구사항과 기능요구사항을 만족 시킬 수 있는 도구를 개발하여야 한다.

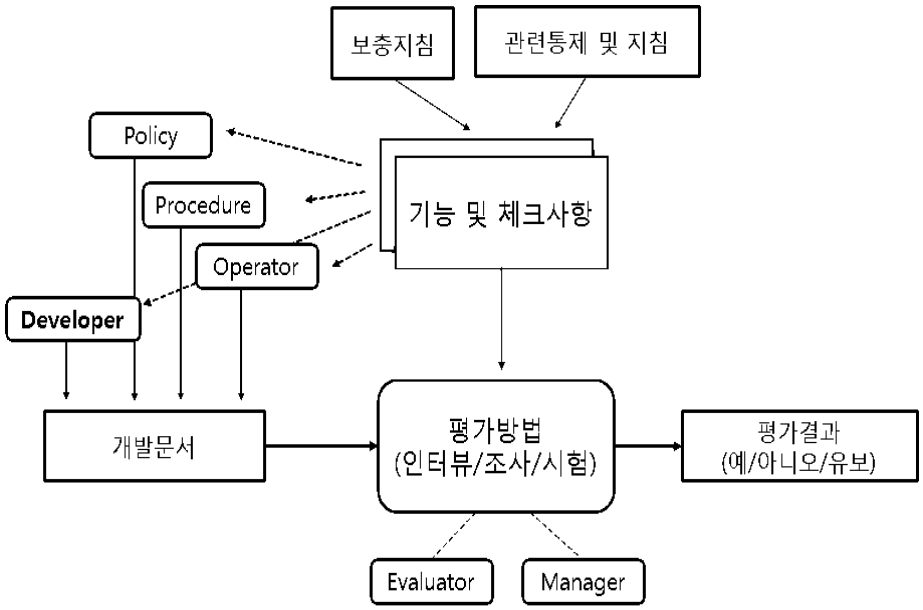

그림 3. 사이버보안통제 구축지원을 위한 시스템의 프로세스
Fig. 3. Process of System

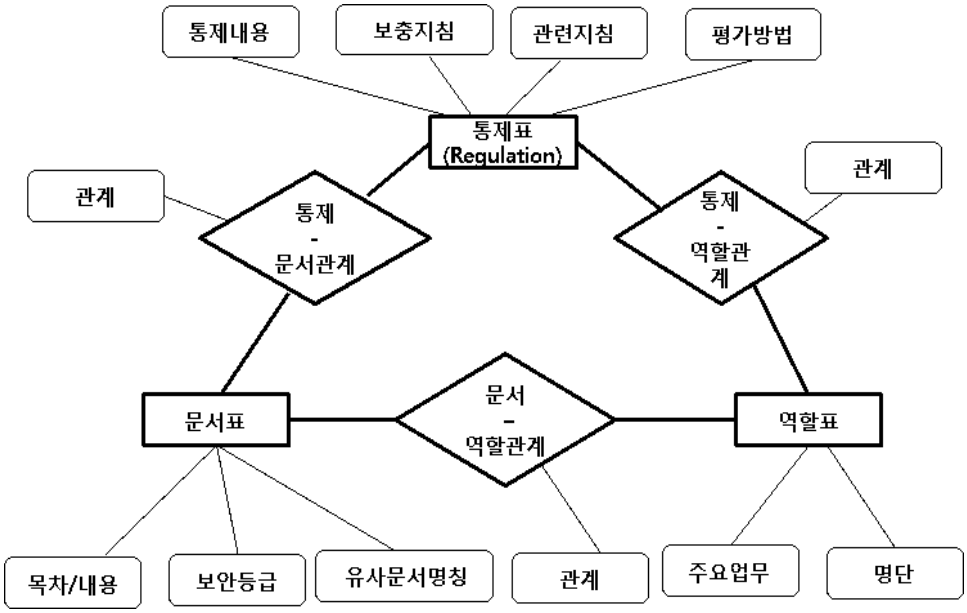

그림 4. 스키마 설계
Fig. 4. Design of schema

이러한 '사이버 보안 통제 지원 도구' 개발은 앞으로 SCADA 시스템을 설계단계에서부터 사이버 보안을 고려한 안전한 시스템을 설계할 수 있도록 도와주는 최상의 방법이 될 것이다.

참고문헌

[1] http://en.wikipedia.org/wiki/SCADA

[2] National Cyber Security Center, Cyber Security, 2005,p.14-16.

[3] Hyun Mi Jung, Kyung Su Han, Gang Soo Lee, "The Response Methods for SCADA System Threats", Korea Knowledge Information Technology Society, Vol 7,No 1, pp 119-128, 2012

[4]http://www.symantec.com/ko/kr/about/news/release/article.jsp?prid=20111020_02

[5] Gang Soo Lee, Hyun-mi Jung, Kyung-su Han, Cheol-kwon Lee and Dong-young Lee, "Classification Schemes of Security Controls for Nuclear Power Plant Control Systems", JCICT &The first Yellow Sea International Conference on Ubiquitous Computing, August 2011

[6] Cheol-kwon Lee, Jae-gu Song, Dong-young Lee, Hyun-mi Jung, and Gang-soo Lee,"A Cyber-Security Implementation Framework for Nuclear Power Plant Control Systems", *ICHIT 2011*, Korea, September 22-24, 2011.

[7] *Regulatory Guide 5.71,* Cyber security programs for nuclear facilities, U.S. Nuclear Regulatory Commission, Jan. 2010.

[8] NIST SP 800-53, R.3, Recommended security controls for federal information systems, 2009.

[9] 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 Funture Game Technology,* VOL 2, NO 1, pp 147-152, March 2012

저자소개

정 현미 (Hyun Mi Jung)

1998 : 한남대학교 컴퓨터공학과 (공학사)
2010 : 한남대학교 컴퓨터공학과 (공학 석사)

2010 ~ 현재 : 한남대학교 컴퓨터공학과 박사과정
2012 ~ 현재 : 한국과학기술정보연구원 연구원
과학기술사이버안전센터 연구원
※ 관심분야 : 소프트웨어공학, 보안공학, 위험분석 및 지식보안 컨설팅, IT 보안시스템 개발

한 경수 (Kyung Su Han)

2011 : 한남대학교 컴퓨터공학과 (공학사)

2011 ~ 현재 : 한남대학교 컴퓨터공학과 석사과정
※ 관심분야 : 소프트웨어공학, 보안공학, 위험분석 및 지식보안 컨설팅, IT 보안시스템 개발

이 강수 (Gang Soo Lee)

1983 : 서울대학교 전산학 (이학 석사)
1989 : 서울대학교 전산학 박사 (이학 박사)

1987 ~ 현재 : 한남대학교 컴퓨터공학과 교수
※ 관심분야 : 소프트웨어공학, 보안공학, IT 보안시스템 개발, 멀티미디어교육