원자력발전소의 디지털계측제어시스템의 사이버보안을 위한 디지털 자산분석 방법

구인수* · 김관웅* · 홍석붕* · 박근옥* · 박재윤*

Digital Asset Analysis Methodology against Cyber Threat to Instrumentation and Control System in Nuclear Power Plants

In-Soo Koo* · Kwan-Woong Kim* · Seok-Boong Hong* · Geun-Ok Park* · Jae-Yoon Park*

요 약

원자력발전소의 계측제어계통은 제어, 감시기능을 수행하여 안전운전을 위한 두뇌 역할을 하는 핵심적인 분야이다. 최근 계측제어계통은 마이크로프로세서기반의 디지털 기술을 받아들여 디지털화되었다. 그러나 계측제어계통의 디지털시스템은 아날로그 기반 시스템에 비해 사이버위협에 매우 취약하여, 사이버공격에 의해 발전소 안전에 부정적인 영향을 받을 수 있다. 따라서 사이버침해에 대응할 수 있는 사이버 보안 대책이 계측제어계통에 요구된다. 사이버 보안성이 우수한 계통 설계를 위해서는 계측제어계통을 구성하는 자산에 대한 효과적인 자산분석이 요구된다.

본 연구에서는 원자로 계측제어설계의 사이버보안 적합성을 분석하기 위한 전 단계로 계측제어계통의 디지털 자산을 분석하기 위한 방법론을 제안한다. 제안된 디지털자산 분석 방법은 자산식별, 식별된 자산에 대한 평가방법으로 구성된다. 제안된 자산분석방법은 원자력발전소 계측제어계통의 사이버보안을 위한 자산분석에 응용하였다.

ABSTRACT

Instrumentation & Control(I&C) System in NPP(Nuclear Power Plant) plays a important role as the brain of human being, it performs protecting, controling and monitoring safety operation of NPP. Recently, the I&C system is digitalized as digital technology such as PLC, DSP, FPGA. The different aspect of digital system which use digital communication to analog system is that it has potential vulnerability to cyber threat in nature. Possibility that digital I&C system is defected by cyber attack is increasing day by day. The result of cyber attack can be adverse effect to safety function in NPP.

Therefore, I&C system required cyber security counter-measures that protect themselves from cyber threat efficiently and also cyber security design should be taken into consideration at concept stage in I&C system development process.

In this study, we proposed the digital asset analysis method for cyber security assessment of I&C system design in NPP and we performed digital asset analysis of I&C system by using the proposed method.

키워드

I&C, Cyber security, Asset Identification, Asset Valuation, Asset Analysis Method
계측제어계통, 사이버 보안, 자산식별, 자산평가, 자산분석방법

* 한국원자력연구원(iskoo@kaeri.re.kr)
* 한국원자력연구원(kwkim@kaeri.re.kr),
* 한국원자력연구원(boong@kaeri.re.kr)
* 한국원자력연구원(gopark@kaeri.re.kr)
* 한국원자력연구원(pakjy1@kaeri.re.kr)

접수일자 : 2011. 10. 15 심사(수정)일자 : 2011. 11. 30 게재확정일자 : 2011. 12. 12

Ⅰ. 서 론

원자력발전소 계측제어계통은 원자로 운전의 보호, 제어 및 감시기능을 수행한다. 최근 원자력발전소 계측 제어 계통은 디지털 기술을 적극적으로 적용하고 있다. 동시에 첨단 정보기술인 통신기법을 적용할 수 밖에 없는 실정이다. 따라서, 아나로그 시스템에 비해 속성상 의도적인 사이버 공격이나 테러에 상당히 취약하므로 발전소의 안전성 확보에 부정적 영향을 미친다 [1].

2003년에 원자력발전소에 대한 사이버 공격의 대표적인 사례는 미국 오하이오 주에 위치한 Davis-Besse 원자력발전소의 MS-SQL Slammer worm이 감염된 컴퓨터를 통해 네트워크 과 부하를 일으켜 발전소 안전계통 감시시스템인 SPDS(Safety Parameter Display System)과 PCS (Plant Process Computer)가 기능이 상실된 사고가 발생하였다[2, 3].

또한 2009년에는 이란 등에 원자력시설을 공격하기 위해 설계된 것으로 의심되는 바이러스 프로그램인 StuxNet에 의해 공격받은 사례가 있다 [4].

StuxNet은 특정제조사의 PLC(Programmable Logic Controller)를 공격할 목적으로 제작되었으며, 제어컴퓨터를 감염시킨 후 사용자 몰래 PLC의 제어로직을 변경하였다. 제어로직은 제어대상인 모터의 오동작을 일으켜, 제어시스템의 고장을 유발하였다. 감염경로는 네트워크가 아닌 엔지니어의 이동식저장장치를 통해 침투하였으며, 악성코드는 정상적인 시스템 드라이버 소프트웨어로 위장하여 장기간 발견되지 않았다. 2011년에는 전력관련 산업체의 기밀정보를 수집하기 위한 악성코드인 W.32 duqu가 발견되었다[5].

위의 사례와 같이 네트워크 뿐 아니라 사회공학(Social Engineering) 등 다양한 방법을 이용한 원자력시설에 대한 사이버공격에 의한 위협이 나날이 증대되고 있으며, 국내외 원자력 관련 기관은 이의 대처 방안 마련에 부심하고 있다.

최근 원자력 규제기관은 사이버 공격에 취약한 디지털 시스템에 대해 설계 초기부터 사이버 위협에 대응하는 방안을 반영하도록 관련 지침이나 기준을 발표하고 있다 [6~8].

따라서, 본 논문은 사이버 보안성이 우수한 디지털 계측제어 계통을 개발하기 위해 초기단계로 개발한 계측제어 계통의 효과적인 자산분석이 필요하며, 이를 위한 자산분석 방안을 제안한다.

이 자산분석 방안은 자산식별과 식별한 자산의 평가방법으로 구성하였다. 자산분석 방안을 개발중인 원자로 계측제어계통의 일부 계통에 적용하여 그 유효성을 점검하였다.

2장에서는 사이버 보안 설계를 위한 대상, 개략적 평가 절차, 전략, 등급기준, 영향성 기준에 대해 기술하고, 3장에서는 계획단계에서 수행할 자산식별 및 자산평가 절차에 대해 기술한다. 4장은 계측제어 계통의 자산 분석 결과를 기술하고, 5장에서 결론을 기술한다.

Ⅱ. 원전 제어계측의 사이버보안 개념

원자력발전소의 계측제어계통을 사이버보안 위협으로부터 효과적으로 보호하기 위해서는 계측제어계통의 개발단계에서부터 사이버보안을 고려한 설계가 반영되어야 한다. 2장에서는 계통의 사이버보안 설계를 위한 계획, 방법 및 절차에 대해 기술한다.

2.1. 사이버보안대상

미국 원자력규제위원회의 규제지침 5.71에 근거하여 계측제어 계통의 안전 및 안전에 관련한 기능을 수행하는 시스템 또는 기기를 필수 계통으로 분류하고, 필수 계통은 사이버 공격이나 테러 등 위협에 고유 기능 수행에 영향을 받지 않도록 대처해야 한다 [7]. 따라서, 사이버 보안은 이런 기능을 수행하는 시스템 중 디지털 기술을 사용하거나 안전에 영향을 주는 디지털 시스템을 필수 디지털 자산으로 분류하고, 의도적인 공격에 충분히 보호할 수 있도록 설계에 반영해야 한다.

다음과 같은 기능을 수행하는 시스템 및 기기가 필수디지털자산으로 볼 수 있다.

1) 안전 및 정상 출력 운전 기능을 수행하는 기기나 계통
2) 안전 및 정상 출력 운전 기능에 영향을 미치는 기기나 계통

3) 1)항과 2)항의 기능을 지원하는 기기나 계통
4) 1)항, 2)항 및 3)항의 기기나 계통의 보안 기능을 수행하는 기기, 계통 및 통신망

계측제어계통에 대한 사이버보안 설계의 첫 단계로 보안대상의 식별이 수행되어야 한다.

2.1. 사이버보안성 평가 절차

IEC 27001은 시스템에 대한 사이버 위해 수준을 평가하기 위한 상위 수준의 방법 및 절차를 기술하고 있다 [6].

계측제어 계통의 사이버 위험 평가는 그림 1과 같이 위험 식별과 위험 평가의 두 단계로 구성한다. 사이버 위험 평가를 위한 초기 자료인 자산 분석은 필수 디지털 자산 식별과 필수 디지털 자산에 대한 가치 평가인 필수 디지털 자산 분석 평가 단계로 구성한다.필수 디지털 자산 분석 결과는 사이버 위험 식별과 위험 평가 수행 단계의 입력으로 사용한다.

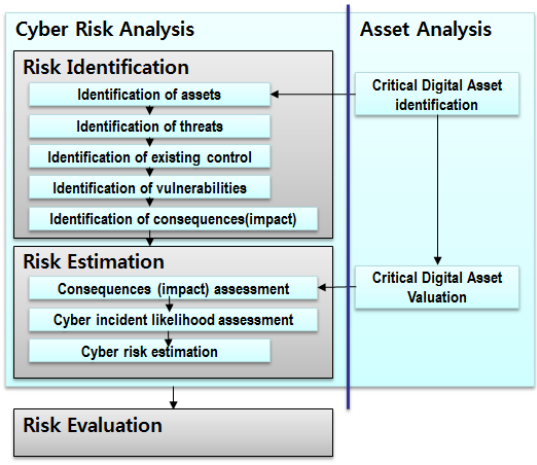

그림 1. 사이버 위험 평가와 자산분석 절차
Fig. 1 Cyber-related Risk Analysis and Asset Analysis Procedure

위험 식별 단계는 1) 위험 자산 식별, 2) 사이버 위험 식별, 3) 현재의 보안 통제 식별, 4) 취약점 식별, 5) 영향성 식별로 구성하며, 위험 평가 단계는 1) 자산 손상으로 인한 결말(consequence) 평가, 2) 사이버 사고 가능성 평가, 3) 사이버 위험 평가 등으로 구성한다.

2.2. 심층방어보호전략

심층 방호 보호 전략은 사이버 공격에 대응하고 사이버 공격으로 인한 피해를 완화하고, 복구를 위한 총체적 보호 전략이다. 심층 방호 보호 전략의 심층 방호 구조는 방벽으로 보호하는 다중의 계층 구조로서 단일 보호 방벽의 훼손 또는 단일 보안 통제의 무력화가 원자력발전소의 안전 및 안전 관련 기능에 손상을 주지 않는다[7,8]. 디지털 계측제어 계통의 심층 방호 모델은 그림 2와 같다.

각 계층간의 경계는 논리적, 물리적으로 분리하며, 계층의 중요도 또는 영향성에 따라 하위 계층과 자료 흐름을 통제한다.

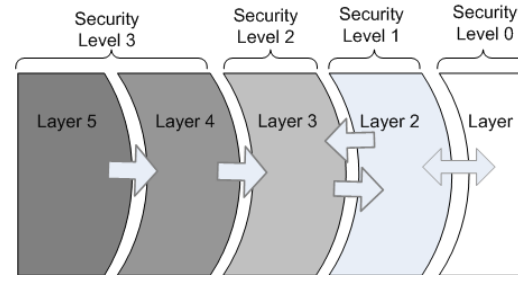

그림 2. 계측제어계통의 심층방어모델
Fig. 2 Defense in depth protective model in I&C system

2.3. 사이버보안 등급 접근법

사이버 보안 등급 기준은 심층 방호 모델의 보안수준을 정의하며 각 계층의 보안 준위를 정의하여 각 계층에 필요한 상위 수준의 요건을 마련한다. 그림 2와 같이 보안 등급은 네 개의 보안 준위로 분류한다.

(1) 보안준위(Security level) 3

보안 준위가 가장 높은 디지털 자산으로 안전 기능을 수행하는 계통들이다.

- 통신망을 통한 보안 준위가 낮은 외부 및 계통에서 자료 수신은 금지한다. 단방향 통신을 이용하여 외부로 자료 전송은 필요에 따라 허용한다. 핸드쉐이

킹을 수행하는 통신 규약(예: TCP)은 배제한다. 단, 동일 준위의 계통 또는 기기는 허용할 수 있다.
- 보수 유지를 위한 원격 접근은 허용하지 않는다.
- 계통으로 물리적 접근은 엄격히 통제한다.
- 디지털 시스템의 변경 등 제반 작업은 반드시 2인이 같이 수행해야 한다.
- 모든 작업 및 활동은 감시하고, 기록한다.
- 하드웨어 유지 보수, 소프트웨어 변경 등의 각 및 계통 변경시에는 엄격한 감독 절차를 마련하여 준수한다.

(2) 보안 준위 2

다양한 컴퓨터 위협에서 보호해야할 높은 보안 준위인 계통으로 발전소 정상운전과 관련한 계통, 주제어실의 실시간 감시계통이 해당한다.
- 상위 보안 준위에서 송신하는 자료 수신은 허용한다. 같은 준위의 기기나 계통은 양방향 자료 송수신을 허용한다.
- 단방향 통신을 이용한 외부로 자료 전송은 허용한다. 핸드쉐이킹이 있는 통신 규약(예: TCP)인 경우 통신용 제어 자료(SYN, FIN 등)는 허용한다. 또한 종단간 연결 설정을 위한 지원 규약(ARP, ICMP, IGMP 등)은 보안 영향성 평가를 통해 허용할 수 있다. 하위 준위에서 자료 수신은 필요성과 보안성 평가 후 예외 허용이 가능하다.
- 유지보수를 위한 원격 접속은 개별 접속 만 허용한다. 이 경우 강력한 암호화 기법 등 보호 수단을 사용하고, 사용자는 보안 정책을 따라야 한다.
- 시스템으로 연결하는 물리적 연결은 통제한다.

(3) 보안 준위 1

다양한 사이버 위협에 대해 중간 정도의 보안 수준에 해당하며, 방호 수단 및 보안 정책은 다음을 포함한다.
- 적절한 보호 수단(방화벽, 침입 탐지, 보안 소프트웨어 등)의 적용 조건하에 접속을 허용한다.
- 주요 자원감시를 위해 로깅과 감사 기록을 유지한다.
- 외부 또는 보안 준위 0에서 유입하는 통제 않되는 트래픽은 보안 게이트웨이를 사용하여 허가할 수 있고, 확인한 트래픽만 유입을 허용한다.
- 외부로 원격 접속을 허용하나, 반드시 보호 수단을 사용하여 통제한다.
- 시스템으로 연결하는 물리적 연결은 통제한다.
- 두 종류 이상의 보안 시스템으로 다단계 보안 체계를 구축한다.

(4) 보안 준위 0
- 제어나 운전에 직접 또는 간접적으로 관련 없는 기능을 수행하는 디지털 자산으로 사무 자동화 기기 등이다. 이 준위는 보안 중요도가 가장 낮은 디지털 자산으로 다음과 같은 요건을 적용한다.
- 적절한 보호 수단(방화벽, 침입 탐지, 보안 소프트웨어 등) 적용 조건하에 접속을 허용한다.
- 적절한 보안 통제가 있는 환경에서 인가한 사용자에 한해 원격접속을 허용한다.

2.4. 영향성 기준

영향성 기준은 계통의 취약성에 대한 위협이 실현되었을 때 계통에 부정적인 영향의 결과를 측정하는 기준이다. 영향성 기준은 다음과 같은 사항을 고려하여 안전 기능 또는 정상 출력 운전에 미치는 영향에 따라 표 1의 준위 I1, I2, I3로 평가하며, 계통의 영향성 준위는 필수 디지털 자산의 가치이다.

- 계통의 임무
- 계통과 정보의 심각도(criticality)
- 계통과 정보의 민감도

계측제어계통의 영향성 수준은 안전기능 또는 정상 출력운전에 미치는 영향수준에 따라 표 2와 같이 분류한다.

표 1. 사이버 침해 영향성 준위
Table 1. Cyber security impact level

영향성	영향
I1	원자력발전소의 안전에 영향을 미침
I2	원자력발전소의 정상출력운전에 영향을 미침
I3	원자력발전소의 정상출력운전에 사소한 영향을 미침

표 2. 영향성, 보안수준과 필수디지털자산 간의 관계
Table 2. Relation between Impact, security level and CDA

영향성	보안 수준	자산 분류	비고
I1	보 안 준위3	필수디지털 자산	안전 기능 수행 또는 안전기능에 영향을 주는 경우
I2/I3	보 안 준위2	필수디지털 자산	I3 기기 또는 계통이 I2에 영향을 주는 경우
I3	보 안 준위1	디지털자산	발전소 운전 영향이 매우 낮은 업무 또는 사무자동화와 같은 일반 업무용

III. 계측제어계통 자산분석절차

디지털자산 분석 과정은 그림 4와 같이 디지털자산을 식별하고 사이버 보안 대상계통을 선정하는 자산식별 과정과 식별된 자산의 영향성을 평가하고 보안수준 할당 과정으로 나눌 수 있다.

3.1. 자산식별절차

디지털자산 식별을 위해 계측제어계통를 구성하는 계통들을 식별하고 계통 요건 정보를 기반으로 계통의 수행 기능을 식별한다.

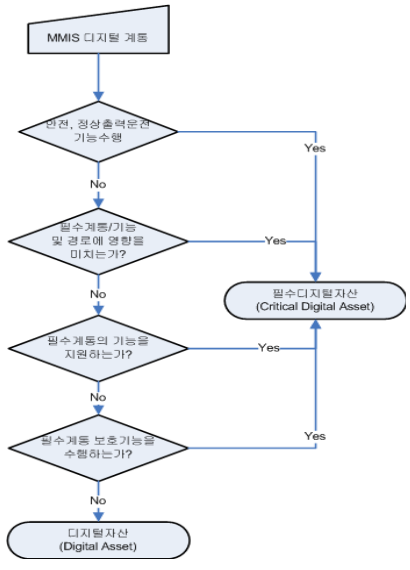

그림 3. 필수디지털 식별절차
Fig. 3 The CDA identification procedure

식별된 계통에 대한 자산분류를 수행하기 위하여 수행기능에 따라 그림 3과 같은 자산분류절차에 따라 필수디지털자산과 일반디지털자산으로 분류한다.

계통의 설계 요건과 시방을 입력으로 계통의 구조, 연계정보, 사용되는 데이터 통신을 분석하여 계통의 구성기기 및 연결성 정보를 생성한다. 연결성 정보는 시스템 간 연계되는 정보, 물리적 통신경로, 통신 프로토콜을 포함한다. 연결성분석의 결과는 계통 및 기기의 취약점을 식별하기 위한 정보로 활용된다.

3.2. 자산평가 절차

(1) 영향성평가

자산식별 절차에서 생성한 계통기능 정보와 1)의 연결성 정보를 입력으로 사이버 공격에 의한 계통의 손상이 발생하였을 때 안전기능과 타 계통에 미치는 영향을 평가하여 표 1의 영향성 수준 기준에 따라 디지털자산의 영향성 수준을 할당한다.

(2) 보안 수준 할당

계통에 할당된 영향성 수준과 자산분류에 따라 표 5.6의 기준으로 계통에 대한 보안레벨을 할당한다.

디지털 계측제어시스템은 할당된 보안레벨에 따라 그림 1과 같이 심층방어모델의 해당 계층에 위치시킨다.

계통설계자는 담당계통의 보안수준 및 심층방호모델의 해당 계층의 요건을 검토하여 계통설계에 반영한다. RG 5.71[7]의 부록 B의 Technical Security Control의 보안통제 정책을 계통 설계에 반영한다.

(3) 보안수준 적합성 평가

계통의 구성기기 및 연결성정보를 입력으로 참고문서 3.2.1에 기술된 보안 수준 별 요건에 대한 계통 설계의 적합성을 검토한다. 검토결과는 계통의 위험수준 평가와 계측제어계통의 설계개선 검토의견의 입력으로 활용된다.

IV. 계측제어계통 자산분석 적용사례

3장의 자산분석 방법과 절차를 이용하여, 원자력발전소의 계측제어계통을 구성하는 계통들에 대한 자산

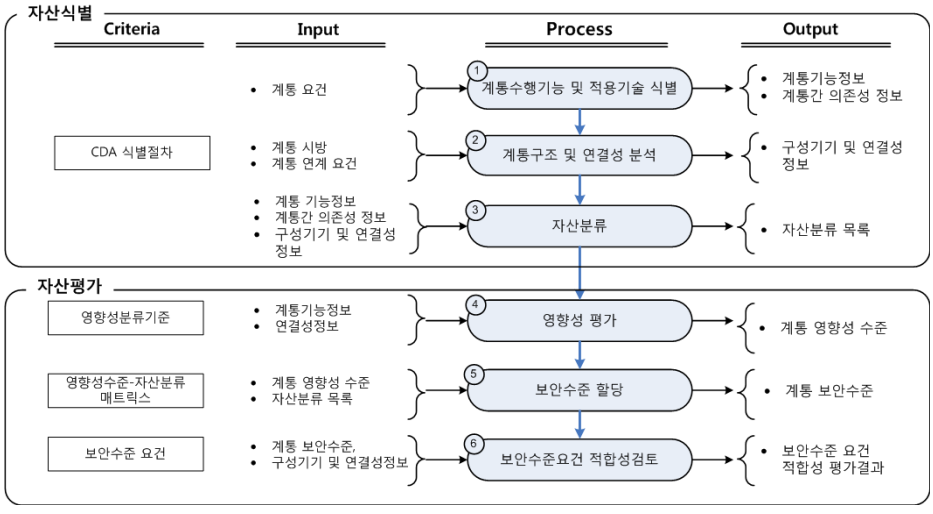

그림 4. 계측제어계통의 자산분석 절차
Fig. 4 The digital asset analysis procedure of I&C system

식별 및 분석을 수행하였다.

4.1. 사고후감시계통 자산식별

자산분석의 예제로 발전소 사고를 감시하는 사고후감시계통(PAMI : Post-Accident Monitoring Instrumentation)의 자산분석과정 및 결과를 기술한다.

(1) 계통수행기능 및 적용기술식별

사고후감시계통 설계요건을 기반으로 계통의 기능에 대한 분류를 표 3과 같이 수행한다.

표 3. 사고후감시계통 기능분석
Table 3. Fuctional analysis of PAMI

기능	기능분류	적용기술
노심출구온도 계산 및 표시	안전기능	디지털
원자로용기 수위계산 및 표시	안전기능	디지털
과냉각여유도 계산 및 표시	안전기능	디지털
기타 사고후감시변수 감시	안전기능	디지털

(2) 계통의 구조 및 연결성 분석

기능분석이 완료되면, 계통의 설계요건과 설계시방을 입력으로 그림 5와 같이 계통의 구조를 분석 및 기기간 또는 계통 간 연결성을 분석한다. 표 4는 사고후감시계통의 계통간 연결성정보의 분석결과이다. 분석된 결과는 계통간 또는 기기간 의존성을 평가하는 입력으로 활용된다.

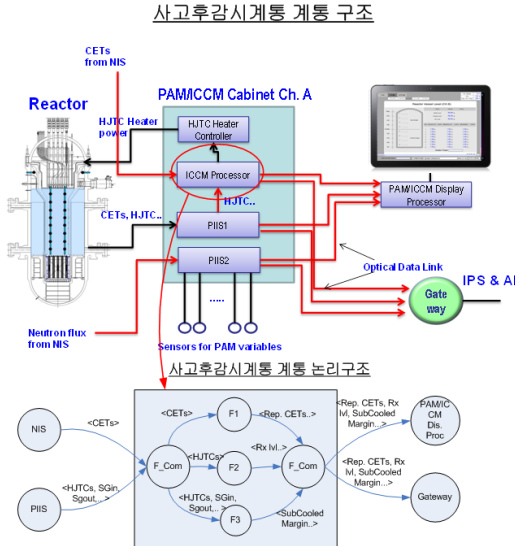

그림 5. 사고후감시계통 구조 및 연결성분석 예
Fig. 5 An example of structural & connectivity analysis of PAMI system

표 4. 사고후감시 계통 연결성 및 연계정보
Table 4. Connectivity and interface information of PAMI

연계계통	연계신호	신호 흐름	연결성 정보	연결기기
핵계측 계통	중성자속, 노심출구온도	입력	광 데이터 링크	PIIS1, PIIS2
정보처리 계통	PAM&ICCM 상태 및 주요변수	출력	단방향 광데이터 링크	게이트웨이
경보지시 계통	PAM&ICCM 상태 및 주요변수	출력	단방향 광데이터 링크	게이트웨이

* PAM : Post-Accident Monitoring
* ICCM : Inadequate Core Cooling Monitoring

(3) 자산분류

계통의 기능과 구조 및 연결성분석의 결과를 입력으로 계통의 자산분류를 수행한다. 사고후감시계통의 자산분류결과는 표 5와 같다.

표 5. 사고후감시 계통 자산분류
Table 5. Asset classification of PAMI components

기기	수행기능	의존성	자산분류
ICCM 프로세서	노심출구온도, 원자로용기수위, 과냉각여유도 계산	핵계측계통, PIIS	필수디지털 자산
PIIS	사고후감시변수 계측 및 처리	핵계측계통	필수디지털 자산
PAM/ICCM 표시처리기	PAM&ICCM 상태 및 주요변수 표시	PIIS, ICCM 프로세서	필수디지털 자산
HJTC Heater Controller	HJTC 전열기제어 (아날로그)	ICCM 프로세서	필수자산

* PIIS : PAM&ICCM (nstrumentation System
* HJTC : Heated Junction Thermo-Courple

4.2. 사고후감시계통 자산분석

계통의 자산식별과정에서 생산한 정보를 기반으로 계통이 사이버공격에 의해 피해가 발생했을 때, 발전소 안전과 타 시스템에 미치는 영향성을 표 6과 같이 분석한다. 계통의 영향성과 자산분류결과를 기반으로 계통에 대한 보안준위를 할당한다.

표 6. 사고후감시계통 영향성평가
Table 6. Impact analysis of PAMI

손상유형	발전소에 대한 영향	영향성준위
기능상실	사고후감시 기능상실 및 노심상태 및 원자로냉각재 수위감시 기능 상실	I1
오동작	잘못된 정보제공에 따른 운전원의 오동작 유발	

상기의 자산분석 결과를 바탕으로 전체 계측제어계통의 보안수준할당은 표 7의 예문과 같다. 이는 그림 6과 같이 각 계통의 사이버 심층방호모델을 의미한다.

계통에 대한 보안수준이 할당되면, 계통설계가 2.3절의 보안수준요건에 적합하는 지에 대한 평가를 수행하며, 평가결과는 계통설계에 반영하여. 설계측면에서 사이버보안성을 향상할 수 있다.

표 7. 계통 보안수준 할당 예
Table 7. An example of system security level allocation

보안수준	계측제어계통
보안준위 3	원자로보호계통, 다양성보호계통, 공학적 안전설비제어계통, 사고후감시계통, 핵계측계통, 안전등급공정계측계통
보안준위 2	출력제어계통, 공정제어계통, 이차제어계통, 정보처리계통, 경보지시계통, 비안전등급 통신망
보안준위 1	비상대응설비(ERF), 기술지원실(TSC)

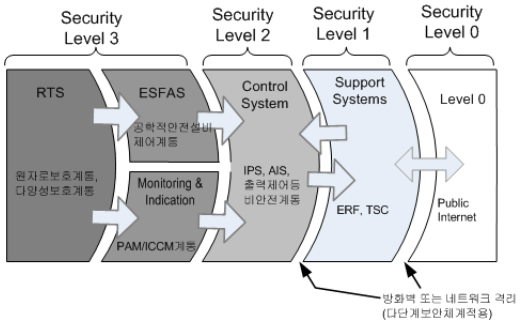

그림 6. 계측제어계통의 심층방어모델 예
Fig. 6 An example of I&C systems mapping in defense in depth

V. 결 론

국가의 중요한 인프라인 전력망, 발전소등에 대한 사이버 공격에 대한 보안위협이 증가하고 있다[10,11].

또한 원자력발전소의 계측제어시스템을 나날이 증가하고 있는 사이버 위협으로부터 보호하기 위한 체계적인 사이버보안대책이 요구된다. 본 논문에서는 계측제어계통의 사이버보안설계를 위한 자산분석 방법 및 절차를 제안하였다. 제안된 자산분석방법은 자산식별을 위한 자산분류기준과 영향성기준을 정립하였고, RG 5.71에 부합하는 사이버보안 심층방어모델을 수립하였다. 또한 체계적인 자산분석절차를 제공하여 원자력발전소 계측제어계통의 사이버보안 평가와 보안 요건을 개발하기 위한 기반을 마련하였다. 향 후, 사이버보안성 평가를 위한 취약성 평가 및 사이버위험평가에 대한 체계적인 방법 및 절차의 개발이 필요하다.

참고 문헌

[1] D. Dzung, M. Naedele, T. Von Hoff, and M. Crevatin, “Security for industrial communication systems,” Proc. IEEE, Vol. 93, No. 6, pp. 1152–1177, Jun., 2005.

[2] G. Ericsson, “Information security for electric power utilities (EPUs)—CIGRE developments on frameworks, risk assessment, and technology,” IEEE Trans. Power Del., Vol. 24, No. 3, pp. 1174–1181, Jul., 2009.

[3] Robert J. Turk, “Cyber Incidents Involving Control Systems”, INL/EXT-05-00671, Oct., 2005.

[4] Symantec Security Respon se, "W32.Stuxnet Dossier”, Rev. 1.4, Feb., 2011.

[5] Symantec Security Response, "W32.Duqu The precursor to the next stuxnet”, Rev. 1.2, Oct., 2011.

[6] ISO/IEC 27005, "Information Technology - Security Techniques - Information Security Risk Management", 2008.

[7] Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”, US-NRC, 2010.

[8] IAEA, IAEA Nuclear Security Series No.XX, “Computer Security at Nuclear Facilities”, Draft version, 2010.

[9] Gary Stoneburner, Alice Goguen, and Alexis Firnga, “Risk Management Guide for Information Technology Systems”, NIST, Jul., 2002.

[10] 서우석, 전문석, “스마트그리드(Smart Grid) 전력망과 정보통신망 융합 보안 방향”, 한국전자통신학회논문지, 5권, 5호, pp. 477-486, 2010.

[11] 차인환, “내부 정보보호를 위한 인원보안 관리 방안 연구”, 한국전자통신학회논문지, 3권, 4호, pp. 210-220, 2008.

저자 소개

구인수(In-Soo Koo)

1977년 경북대학교 전자공학과 졸업(공학사)
1996년 청주대학교 대학원 전자학과 졸업(공학석사)
2000년 충남대학교 대학원 전자공학과 졸업(공학박사)
1980년 ~ 현재 한국원자력연구원 책임연구원
2007년 ~현재 IEC SC45 위원
※ 관심분야 : 계측제어시스템, 데이터통신, 사이버보안

김관웅(Kwan-Woong Kim)

1996년 전북대학교 전자공학과 졸업(공학사)
1998년 전북대학교 대학원 전자학과 졸업(공학석사)
2002년 전북대학교 대학원 전자공학과 졸업(공학박사)
2009년 ~ 현재 한국원자력연구원 선임연구원
※ 관심분야 : 계측제어시스템, 무선통신, 사이버보안

홍석붕(Seok-Boong Hong)

1979년 성균관대학교 전자공학과 졸업(공학사)
1982년 성균관대학교 대학원 전자학과 졸업(공학석사)
2002년 성균관대학교 대학원 전자공학과 졸업(공학박사)
1987년 ~ 현재 한국원자력연구원 책임연구원
※ 관심분야 : 계측제어시스템, 사이버보안

박근옥(Geun-Ok Park)

1986년 경기공업개방대학 컴퓨터공학과 졸업(공학사)
1993년 충남대학교 대학원 전산학과 졸업(공학석사)
2006년 공주대학교 대학원 전산학과 졸업(공학박사)
1987년 ~ 현재 한국원자력연구원 책임연구원
※ 관심분야 : 인간공학, 계측제어시스템, 인간기계 인터페이스, 사이버보안, 소프트웨어 V&V

박재윤(Je-Yun Park)

1984년 경북대학교 전자공학과 졸업(공학사)
1990년 경북대학교 대학원 전자공학과 졸업(공학석사)
2002년 연세대학교 대학원 전기전자공학부(정보통신) 졸업(공학박사)
1986년 ~ 현재 한국원자력연구원 책임연구원
※ 관심분야 : 계측제어시스템, B-ISDN, 산업용통신망, 사이버보안