디지털산업정보학회 논문지 제19권 제3호-2023년 9월
http://dx.doi.org/10.17662/ksdim.2023.19.3.025

공격 트리를 이용한 다양성보호계통 사이버보안 위험 평가

정 성 민* · 김 태 경**

Cybersecurity Risk Assessment of a Diverse Protection System Using Attack Trees

Jung Sungmin · Kim Taekyung

〈Abstract〉

Instrumentation and control systems measure and control various variables of nuclear facilities to operate nuclear power plants safely. A diverse protection system, a representative instrumentation and control system, generates a reactor trip and turbine trip signal by high pressure in a pressurizer and containment to satisfy the design requirements 10CFR50.62. Also, it generates an auxiliary feedwater actuation signal by low water levels in steam generators. Cybersecurity has become more critical as digital technology is gradually applied to solve problems such as performance degradation due to aging of analog equipment, increased maintenance costs, and product discontinuation.

This paper analyzed possible cybersecurity threat scenarios in the diverse protection system using attack trees. Based on the analyzed cybersecurity threat scenario, we calculated the probability of attack occurrence and confirmed the cybersecurity risk in connection with the asset value.

Key Words : Instrumentation and Control Systems, Cybersecurity, Attack Tree, Nuclear Power Plant, Diverse Protection System

Ⅰ. 서론

원자력 발전소는 핵분열을 이용하여 열과 전기를 생산하는 시설이다. 핵분열은 원자핵을 물리적으로 분할하여 에너지를 방출하는 과정으로 원자로 내부의 핵연료에서 핵분열 반응이 일어난다. 이를 통해 발생한 열은 수증기를 생성하여 터빈을 회전시키고, 터빈은 전기를 생산하는 발전기를 구동한다. 계측제어시스템은 원자력 발전소를 안전하고 효율적으로 운영하는 데 중요한 역할을 하는데, 이를 위해 다양한 계측 계통과 제어 계통이 통합하여 구성된다[1].

계측제어시스템은 오랫동안 수많은 연구와 개발이 진행되어 높은 수준의 안정성과 성능을 보장하고 있다. 하지만, 최근 아날로그 장비들이 성능 저하, 유지비용 증가, 부품 단종 등 다양한 문제가 발생하면서 점차 디지털 장비가 계측제어시스템에 적용되고 있

* 명지전문대학 인터넷보안공학과 교수(제1저자)
** 명지전문대학 인터넷보안공학과 교수(교신저자)

다. 디지털 장비는 앞서 언급한 아날로그 장비의 문제점을 해결하였지만, 반대로 디지털 장비를 목표로 하는 사이버보안 위협이 증가하였고, 사이버보안 공격의 성공은 단순히 장비의 고장이나 정보의 유출만이 아니라 방사능과 관련하여 큰 위협이 될 수 있으므로, 원자력 발전소의 사이버보안 위협 대비는 지속해 연구되어야 한다. 최근 대부분의 연구는 각 계통을 구성하고 있는 요소인 제어기 또는 네트워크의 관점에서만 사이버보안을 확인하고 있다. 계측제어시스템 자체가 수많은 계통이 유기적으로 여러 기능에 연관되기 때문에, 사이버보안의 입장에서는 제어기 또는 네트워크의 관점보다는 계통의 기능별로 위협을 확인하는 것이 필요하며, 이 기능별로 위협을 분석하기 위해서는 연계 사항 확인이 선행되어야 한다[2].

본 논문에서는 계측제어시스템의 주요 계통으로 원자로 안전과 관련된 다양성보호계통(DPS, Diverse Protection System)의 주요 연계와 기능을 확인하고 사이버보안 위험을 분석한다. 2장에서는 관련 연구로 사이버보안 의미 및 공격 트리와 다양성보호계통의 연계와 구성을 확인한다. 3장에서는 보안 위협 분석 방법과 공격 트리를 바탕으로 보안 위협 시나리오를 알아본다. 4장에서는 공격 트리를 바탕으로 각 시나리오에 따라 위험을 정량적으로 분석하고, 마지막으로 5장에서는 연구내용을 정리하고 추후 연구 방향을 기술한다.

II. 관련 연구

2.1 사이버보안

미국 원자력 규제위원회(NRC, Nuclear Regulatory Commission)는 컴퓨팅 환경을 교란, 파괴, 제어할 목적으로 사이버 공간을 통해 공격하는 것을 사이버공격이라고 정의하고, 사이버보안은 사이버공격으로부터 사이버 공간을 보호하는 능력으로 정의한다. 미국 원자력 규제위원회는 원자력 발전소의 안전 및 보안을 감독하고 규제하는 주체로써, 원자력 발전소의 사이버보안도 그 중요한 역할 중 하나이다. 특히, 원자력 발전소는 컴퓨터 시스템과 디지털 장비를 사용하며, 이들 시스템과 장비가 사이버보안 공격에 노출될 때 심각한 결과를 초래할 수 있다. 따라서 위원회는 이러한 사이버보안 위험을 최소화하기 위해 RG 5.71의 규제 지침을 발표하였다. RG 5.71의 내용은 주로 원자력 발전소의 사이버보안 요구사항, 취약점 분석, 보안 감사, 위험 관리 등에 대한 정보를 포함하고 있다[3].

한국 원자력 통제기술원(KINAC)은 국내의 원자력 발전소 사이버보안 규제를 담당하고, RG 5.71을 바탕으로 KINAC/RS-015 규제 지침을 발표하였다. 이 지침을 통해 원자력 시설의 운영자가 사이버보안 공격의 대상인 필수 디지털 자산을 보호하기 위해 운영적, 관리적, 그리고 기술적 방안을 이행하도록 한다[4].

이 밖에도 미국 국립 표준 연구소(NIST, National Institute of Standards and Technology)는 SP 800-53 문서를 통해 산업제어 시스템에 대한 보안 요구 사항과 위험 분석을 통해 보안 대책을 제시하고 있고, 국제 원자력 기구(IAEA, International Atomic Energy Agency)는 NSS No.17 문서를 통해 원자력 시설에 대한 악의적인 공격 행위로부터 중요한 디지털 자산의 보호를 위해 적절한 요건 권고 및 이행에 관한 기술적 지침을 제시하였다. 또한, 미국 원자력 에너지 연구소(NEI, Nuclear Energy Institute)는 NEI 08-09나 NEI 13-10의 문서를 통해 원자력 시설 내에서 사이버보안의 대상이 되는 자산의 식별이나 사이버보안 평가 방법을 제시하고 있다[5-8].

2.2 공격 트리

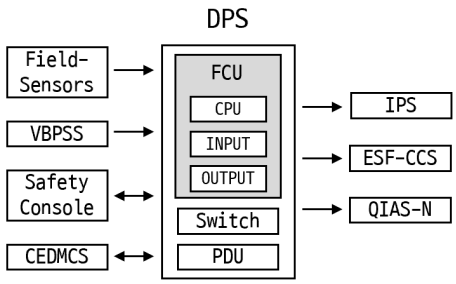
브루스 슈나이어(Bruce Schneier)에 의해 개발된

공격 트리 모델은 보안 위협과 공격을 시각적으로 분석하는 도구로 사용된다. 이 모델은 공격자의 사이버 보안 위협 시나리오를 트리 구조로 나타내며, 각 노드는 특정한 공격 단계나 목표를 나타낸다. 이 모델을 사용하여 시스템 내에서 가능한 공격 경로와 그에 대한 대비책을 식별하고 평가할 수 있다. 슈나이어의 공격 트리 모델의 주요 요소는 노드, 간선, 커넥터이다. 각 노드는 공격을 나타내며, 루트 노드는 공격의 최종적인 목표이고, 리프 노드는 공격의 시작 혹은 취약점을 의미한다. 각 노드의 하위 자식 노드들은 부모 노드의 목표를 이루기 위한 공격이며, 각 부모 노드는 상위 노드에 해당하는 공격을 위한 방법이 된다. 간선은 공격을 연결하는 선으로 공격 간의 연계를 말한다. 커넥터는 논리합(OR)과 논리곱(AND)으로 나눌 수 있는데, 하나의 노드가 2개 이상의 자식 노드, 즉 2개 이상의 공격 수단을 갖는 경우에 논리합은 해당 공격 수단 중 하나만 선택된다고 해도 공격의 성공, 즉 부모 노드로 도달하는 것을 의미한다. 반면에 논리곱의 경우에는 2개 이상의 자식 노드, 즉 2개 이상의 공격 수단이 모두 선택될 때 공격이 성공함을 의미한다. 슈나이어의 공격 트리 모델은 시스템의 취약점과 위협을 시각적으로 분석하고 이해하는 데 도움을 준다[9-10]. 이를 계측제어시스템의 사이버보안의 분석에 적용하면 적절한 사이버보안 전략을 개발하거나 사이버보안 위협을 대비하는 데 유용하게 활용할 수 있다.

2.3 다양성보호계통

다양성보호계통은 원자로의 정지불능 예상과도의 위험을 완화할 수 있도록 원자로와 터빈 정지 및 보조급수 작동 기능을 수행하며, 다양성을 만족시키기 위해 원자로보호계통(RPS, Reactor Protection System)과는 다른 종류의 제어기 및 센서와 논리를 사용하게 된다[11]. 다양성보호계통은 디지털 제어기와 디지털 통신망을 사용하고, 비안전 계통이지만 원자로 정지에 관여한다. 만약, 사이버보안 공격이 성공하여 공격자가 다양성보호계통을 악의적으로 조작한다면 원자로가 정지되어야 하는 상황에서도 정지되지 않는 위험한 상황을 가져올 수 있다. 따라서, 다양성보호계통의 사이버보안 위협에 관한 연구와 대비는 매우 중요하다.

다양성보호계통은 2개의 채널로 구성되는데 각 채널은 하나의 캐비닛에 위치하며, 크게 연산을 위한 비안전등급 제어기(FCS, Field Control Unit), 모듈에 전원을 공급하기 위한 전원공급장치(PDU, Power Distribution Unit), 통신을 위한 스위치(Switch)로 구성된다. 그리고 각 채널은 다른 계통과 물리적 또는 논리적으로 연계된다. 연계 계통으로는 현장 센서(Field-Sensor), 필수모선전원공급계통(VBPSS, Vital Bus Power Supply System), 안전 제어반(SC, Safety Console), 제어봉구동장치제어계통(CEDMCS, Control Element Drive Mechanism Control System), 정보처리계통(IPS, Information Processing System), 공학적안전설비 기기제어계통(ESF-CCS, Engineered Safety Features - Component Control System), 주요변수지시 및 경보계통-비안전(QIAS-N, Qualified Indication and Alarm System-Non Safety)이 있다[12]. <그림 1>은 다양성보호계통의 채널 구성 및 연계를 간단하게 보여준다.



<그림 1> 다양성보호계통 채널 구성 및 연계

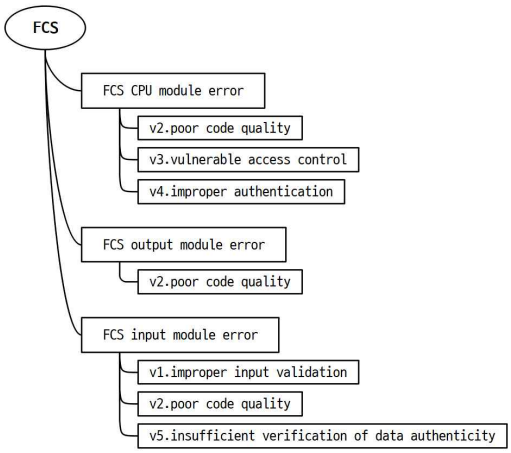
2.3 소프트웨어 연계 위협 요소

다양성보호계통을 구성하는 요소 중 비안전등급 제어기(FCU)에 대한 사이버보안 위협을 분석하기 위해 미국 국토안보부(DHS, Department of Homeland Security)의 사이버 위협 분류 및 관련 취약성을 적용한다[13]. 분류된 소프트웨어 취약성에서 암호화 적용, 인증 정보 관리, 소프트웨어 보안패치의 항목은 다양성보호계통에서 사용하는 비안전등급 제어기와는 관련이 적기 때문에 <표 1>과 같이 해당 취약성 제외하고 입력값의 검증 오류, 취약한 코드 사용, 취약한 접근제어, 부적절한 인증, 데이터 무결성 검증 오류만 고려한다.

<표 1> 비안전등급 제어기 사이버보안 취약점

DHS 분류	사이버보안 취약점	FCS의 대상 모듈
V1	입력값 검증 오류	입력 모듈
V2	취약한 코드	CPU, 입력/출력 모듈
V3	취약한 접근제어	CPU 모듈
V4	부적절한 인증	CPU 모듈
V5	데이터 무결성 검증 오류	입력 모듈

사이버보안 관점에서 제어기를 목표로 하는 공격 트리를 확인하기 위해 CPU 모듈, 입력 및 출력 모듈에 대해 <그림 2>와 같이 정리한다. 비안전등급 제어기의 CPU 모듈의 오류는 취약한 코드 사용, 취약한 접근제어, 그리고 부적절한 인증이 원인이 될 수 있다. 제어기의 입력 모듈은 입력값 검증 오류, 취약한 코드 사용, 그리고 데이터 무결성 검증 오류가 원인이 될 수 있고, 마지막으로 제어기의 출력 모듈은 취약한 코드 사용에 대해서만 고려한다. 각 요소는 논리합(OR)로 적용되고, 제어기의 CPU 모듈, 입력 및 출력 모듈의 취약성은 다양성보호계통의 전체적인 공격 트리에서 공격발생 확률을 계산하는데 단말노드로서 적용된다.



<그림 2> 비안전등급 제어기(FCU)의 소프트웨어 취약성

Ⅲ. 위협 시나리오 분석

다양성보호계통의 주요 기능은 보조급수 작동, 원자로 및 터빈 정지, 정보처리계통과 주요변수지시 및 경보계통-비안전으로 감시 및 상태신호의 전달이다. 공격 트리를 이용하여 각 기능에서 발생할 수 있는 사이버보안 위협을 분석한다.

3.1 사이버보안 위협 분석 방법

FIPS PUB 199는 보안의 목적을 기밀성, 무결성, 가용성으로 구분하고, 사이버보안 사고시 시스템에 관한 잠재적인 영향도를 낮음(Low), 보통(Moderate), 높음(High)으로 정의한다. 본 연구에서는 다양성보호계통의 사이버보안 위협을 분석하기 위해 이와 같은 위험 평가 방법을 준용하고, 연계 위험도 추가하여 타 계통의 자산 가치를 평가한다. 연계 위험은 다양성보호계통에 연계된 타 계통이 사이버보안 공격의 영향을 받았을 때, 계통의 기능을 바탕으로 다양성보호계통에 영향을 주는 정도를 나타내었다[14].

자산 가치의 계산은 <표 2>와 같이 낮음(Low), 보통(Moderate), 높음(High)의 3점 분류 방식을 적용하여 기밀성, 무결성, 가용성, 그리고 연계 위협 별로 영역별 점수를 결정한다. 각각의 점수를 합산하여 총 4점에서 12점을 확인할 수 있고 총점수에 비례하여 자산 가치를 1부터 3까지 나눈다.

<표 2> 자산가치 평가 기준

분류	Low	Moderate	High
기밀성	1	2	3
가용성	1	2	3
무결성	1	2	3
연계 위험	1	2	3

일반적으로 계측제어시스템은 가용성이 우선순위가 높다. 따라서 연계된 계통의 가용성이 침해받는 경우 원자력 발전소의 정상적인 운전에 주는 영향을 고려하여 가치를 산정한다. 가치 산정에 고려되어야 할 사항은 디지털, 이중화, 명령 입력 등의 요소이다. 기밀성은 계통에서 주고받는 데이터가 노출되었을 때, 원자력 발전소나 연계된 계통에 대한 영향을 나타내고, 무결성은 계통에서 다루는 데이터가 변조되는 경우 원자력 발전소나 연계된 계통에 주는 영향을 의미한다. 현장 센서나 필수모선전원전원공급계통은 구성과 기능에서 운전에 미치는 영향이 다른 계통에 비해 적다. 그리고 보수시험반과 정보처리계통은 운전에 부분적인 영향을 미칠 수 있다. 마지막으로 원자로의 정지 기능에 직접적으로 관련이 있는 안전제어반, 제어봉구동장치제어계통, 공학적안전설비-기기제어계통에 대한 가용성의 침해는 경우에 따라 원자력 발전소 운전에 큰 영향을 미칠 수 있다. 각 연계 계통의 기능과 역할 및 중요도에 따라 계산된 점수와 자산 가치 등급은 <표 3>과 같이 계산할 수 있다.

<표 3> 다양성보호계통과 연계된 계통의 자산 가치 등급

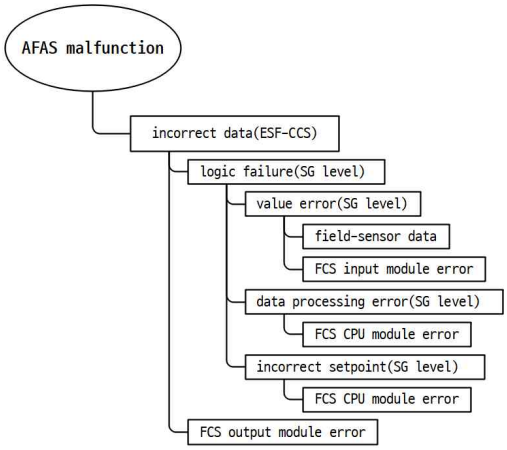
분류	가용성	기밀성	무결성	연계 위험	합계	자산 등급
Field -Sensors	1	1	1	1	4	1
VBPSS	1	1	1	1	4	1
CEDMCS	3	1	1	1	6	1
IPS	2	3	2	2	9	2
ESF-CCS	3	3	1	1	8	2
SC	3	3	3	3	12	3
QIAS-N	2	3	2	2	9	2

3.2 보안 위협 시나리오

3.2.1 보조급수작동 오류

증기발생기(SG, Steam Generator)의 수위가 미리 설정된 값 이하로 떨어질 때, 다양성보호계통은 보조급수 작동신호(AFAS, Auxiliary Feedwater Actuation Signal)를 공학적안전설비-기기제어계통으로 보낸다. 다양성보호계통과 공학적안전설비-기기제어계통에서 독립적으로 발생하는 보조급수 작동신호는 각 계통이 보조급수를 작동시킬 수 있도록 논리합(OR) 회로를 사용한다. 보조급수 작동신호가 오류인 경우는 증기발생기 수위가 정상임에도 불구하고 불필요한 작동신호의 발생으로 원자로의 정상적인 운전에 영향을 줄 수 있고, 반대로 증기발생기 수위가 설정치 이하임에도 작동하지 못하는 경우는 원자로 손상 등의 피해를 가져올 수 있다.

<그림 3>은 보조급수 작동신호 발생에 대한 공격 트리를 보여준다. 사이버보안의 관점에서 다양성보호계통이 오작동하여 공학적안전설비-기기제어계통에 잘못된 값을 전달하는 경우는 비교 논리가 실패하거나 비안전등급 제어기의 출력 모듈에서 오류가 발생하는 경우의 논리합(OR)으로 생각할 수 있다.



<그림 3> 보조급수작동 공격 트리

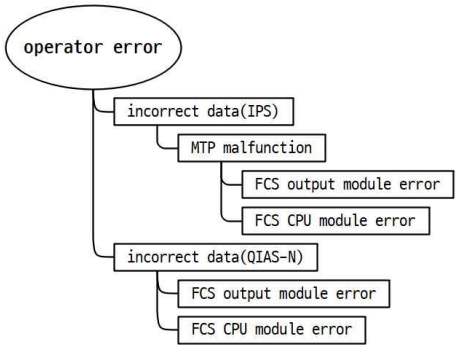
첫 번째, 비교 논리의 실패는 잘못된 데이터 입력, 데이터 처리의 결함, 그리고 잘못된 기준값 설정이 원인이 될 수 있다. 현장 센서에서 관련 변수값이 정상적으로 들어왔으나, 제어기의 입력 모듈에서 오류가 발생하여 잘못된 값을 입력받는다면 다양성보호계통으로 잘못된 데이터가 입력될 수 있다. 비안전등급 제어기의 CPU 모듈에 오류가 발생하여 입력된 데이터를 처리하는데 문제가 생기거나 잘못된 기준값이 설정된 경우도 비교 논리의 실패가 발생할 수 있다.

두 번째로, 내부의 논리 연산이 정상적으로 수행되어도 비안전등급 제어기의 출력 모듈의 오류로 정확한 결과값을 전달하지 못하여 공학적안전설비-기기제어계통이 잘못된 기능을 수행할 수 있다.

3.2.2 운전원 실수

다양성보호계통은 정보처리계통과 주요변수지시 및 경보계통-비안전으로 계통의 주요 변수값과 연관계통의 상태를 전달한다. 주요 변수값은 운전원이 원자로의 상태를 정확하게 파악하여 예상치 못한 사고에 대비하고, 관련 사고시 적절한 대처를 하여 원자로를 안전하게 운영할 수 있도록 한다. 하지만, 잘못된 변수값이 관련 계통으로 전달된다면, 운전원의 잘못된 판단으로 원자력 발전소의 정상적인 운영을 방해하게 된다.

<그림 4>는 잘못된 감시변수의 전달에 대한 공격 트리를 보여준다. 사이버보안의 관점에서 잘못된 감시변수의 전달은 보수시험반의 오작동, 비안전등급 제어기의 CPU 모듈 및 출력 모듈의 오류로 발생할 수 있다.



<그림 4> 운전원 실수 공격 트리

3.2.3 제어봉구동장치제어계통 오류

다양성보호계통은 원자로 정지와 관련하여 가압기 압력, 원자로건물 압력, 그리고 터빈 정지 등의 변수를 감시한다. 가압기 압력이나 원자로건물 압력이 미리 설정된 값을 초과할 때 원자로 정지를 개시한다. 또한, 터빈이 정지되는 경우 터빈 정지에 의한 원자로 정지 기능이 설정되어 있다면 원자로를 정지시킨다. 터빈 정지에 의한 원자로 정지 기능은 원자력 발전소의 주제어실(MCR, Main Control Room)에서 수동으로 선택할 수 있다. 다양성보호계통은 제어봉구동장치의 전동기 발전기 장치에 있는 출력접점을 개방시키는 논리회로를 사용하여 제어봉구동장치로 공급되는 전원을 차단한다. 제어봉구동장치제어계통은

공급되는 전원이 차단된 것을 감지하여 터빈 정지 신호를 발생시킨다.

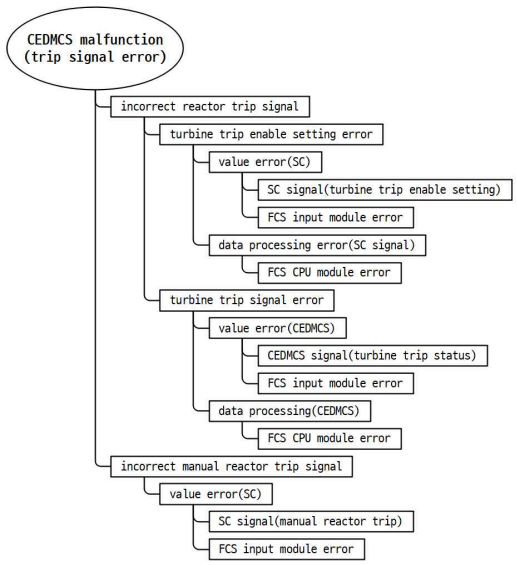
원자로의 정지 기능은 원자력 발전소의 안전과 관련하여 가장 중요한 기능이다. 만약, 예상하지 못한 사고나 기기의 고장이 발생하여 원자로의 정지가 필요한 경우 원자로 노심에 제어봉을 삽입하여 핵분열 연쇄반응을 안전하게 중지시켜야 한다. 하지만, 이 경우에 원자로가 안전하게 정지되지 못한다면, 노심 손상이나 방사능 유출 등의 심각한 상황을 가져올 수 있으므로 반드시 원자로 정지 기능이 올바르게 수행되어야 한다. 반대로 원자로의 정지가 필요하지 않음에도 원자로가 정지되는 경우는 원자로 중지에 따른 손실, 재가동을 위한 점검 및 검사에 드는 추가 비용 등 사업자의 금전적인 손실을 가져온다.

<그림 5>와 <그림 6>은 잘못된 제어봉구동장치제어계통 오작동에 대한 공격 트리를 보여준다. 사이버보안의 관점에서 제어봉구동장치제어계통 오작동은 잘못된 원자로 정지신호, 잘못된 원자로 수동 정지신호, 가압기 압력 및 원자로 건물 압력 변수에 대한 비교 논리 실패의 논리합(OR)으로 발생할 수 있다.

첫 번째, 잘못된 원자로 정지 신호는 터빈 트립시 원자로 정지 설정의 오류와 터빈 트립 신호의 오류 중 하나로 발생할 수 있다. 터빈 트립시 원자로 정지 설정의 오류는 안전 제어반에서 잘못된 값이 입력되거나, 입력된 값을 처리하는 과정의 문제로 발생할 수 있다. 안전 제어반에서 신호가 정상적으로 전달되어도 제어기의 입력 모듈에서 오류가 발생하는 경우를 생각해 볼 수 있는데, 데이터 처리의 오류는 비안전등급 제어기 CPU 모듈의 오류로 데이터를 정상적으로 처리하지 못할 때 발생할 수 있다.

터빈 트립 신호의 오류는 제어봉구동장치제어계통에서 잘못된 값이 입력되거나 데이터 처리의 오류로 발생할 수 있다. 제어봉구동장치제어계통의 트립 상태 신호가 정상적으로 전달되어도 비안전등급 제어기 입력 모듈에 오류가 발생하는 경우에 잘못된 값이 입력될 수 있고, 비안전등급 제어기 CPU 모듈에 오류가 있는 경우 데이터를 정상적으로 처리하는데 문제가 생길 수 있다.

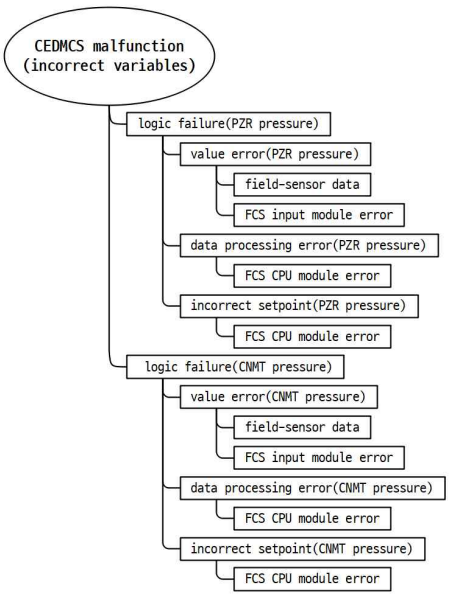
두 번째, 잘못된 원자로 수동 정지 신호가 입력되는 경우는 안전 제어반에서 정상적으로 신호가 입력되지만, 비안전등급 제어기의 입력 모듈의 오류가 있는 경우 잘못된 원자로 수동 정지 신호가 입력될 수 있다. <그림 5>는 정지 신호와 관련된 공격 트리를 보여준다.



<그림 5> 제어봉구동장치제어계통 공격 트리(원자로정지 신호)

세 번째, 가압기 압력 변수에 대한 비교 논리 실패의 경우는 잘못된 값의 입력, 데이터 처리 오류, 잘못된 기준치 설정 중 하나로 발생할 수 있다. 현장 센서에서 가압기 압력값이 정상적으로 입력되었으나, 비안전등급 제어기의 입력 모듈에서 오류가 발생할 때 다양성보호계통으로 잘못된 데이터가 입력될 수 있다. 비안전등급 제어기의 CPU 모듈에 문제가 생겨 입력된 데이터가 제대로 처리되지 못하거나, 잘못된 설정치가 입력되는 경우도 비교 논리의 실패를 가져온다.

네 번째, 원자로건물 압력 변수에 대한 비교 논리 실패의 경우도 세 번째로 살펴본 가압기 압력 변수의 경우와 마찬가지로 잘못된 값의 입력, 데이터 처리 오류, 잘못된 설정치 중 하나가 원인이 될 수 있다. <그림 6>은 잘못된 변수값에 의한 제어봉구동장치제어계통의 공격 트리를 보여준다.



<그림 6> 제어봉구동장치제어계통 공격 트리(잘못된 변수값)

Ⅳ. 다양성보호계통 보안 위험 평가

다양성보호계통의 보안 위험을 평가하기 위해 슈나이어의 공격 트리를 이용한다. 3장에서 공격 트리를 살펴보았는데, 각 노드의 공격 목표 달성을 위한 논리합(OR)과 논리곱(AND) 커넥터를 통해 공격발생확률(AOP, Attack Occurrence Probability)을 다음과 같이 계산한다[15].

① 자식 노드가 하나로 단말노드인 경우

AOP = 1

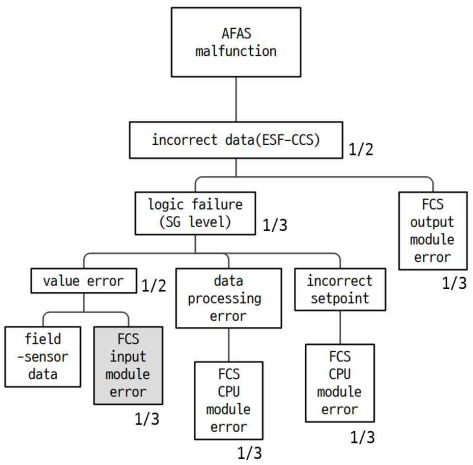
② 자식 노드가 두 개 이상으로 논리곱(AND) 조합

AOP = 논리곱(AND) 조합수 / 자식 노드 수

③ 자식 노드가 두 개 이상으로 논리합(OR) 조합

AOP = 1 / 자식 노드 수

3장에서 살펴본 보조급수 작동에서 설명된 공격 트리의 경우를 예시로 공격발생 확률을 계산하면 다음과 같다. <그림 7>과 같이 취약한 코드와 관련된 제어기의 입력 모듈에 취약점으로 현장 센서의 측정값이 잘못 전달되고, 결국 비교 논리가 실패하여 보조급수 작동계통의 오작동이 일어난 경우 공격발생 확률은 다음과 같이 계산할 수 있다.



<그림 7> 공격발생 확률 계산(취약한 코드)

먼저, 비안전등급 제어기의 입력 모듈의 공격발생 확률은 2장의 설명처럼 입력값 검증 오류, 취약한 코드 사용, 그리고 데이터 무결성 검증 오류의 경우가 있으므로 1/3로 생각할 수 있다. 상위 노드인 측정값의 오류는 현장 센서의 오류 또는 비안전등급 제어기

입력 모듈의 오류를 나타내는 두 개의 자식 노드 중 하나만 성공하면 되므로 공격발생 확률은 1/2이 된다. 그리고, 비교 논리의 실패는 3가지 경우 중 하나이므로 공격발생 확률은 1/3이 되고, 공학적안전설비-기기제어계통으로 잘못된 값의 전달은 비교 논리 실패 혹은 비안전등급 제어기의 출력 모듈의 오류로 발생할 수 있다고 할 수 있으므로 공격발생 확률은 1/2이 된다. 따라서 보조급수 작동의 오작동은 다음 수식과 같이 2.78%의 공격발생 확률로 계산할 수 있다.

$$AOP = \frac{1}{3} \times \frac{1}{2} \times \frac{1}{3} \times \frac{1}{2} = \frac{1}{36} \times 100 = 2.78\%$$

3장에서 살펴본 공격 트리에서 각각의 경우 공격발생확률(AOP)을 계산하고, 평가 등급 구분을 위해 <표 4>를 이용하여 영역별로 공격발생 확률을 낮음(Low), 보통(Moderate), 그리고 높음(High)로 등급을 결정한다.

<표 4> 공격발생확률 평가 기준

분류	Low	Moderate	High
	1	2	3
AOP	1~10%	11~20%	21~100%

앞에서 계산된 보조급수작동계통의 오작동 공격발생 확률은 2.78%로 평가 기준은 낮음(LOW)으로 등급을 갖는다. 사이버보안 위협 시나리오에 따라 위험도(Risk)는 다음 수식과 같이 자산 가치와 공격발생 확률을 곱하여 정량적으로 분석한다.

$$Risk = Asset\_value \times AOP$$

다양성보호계통과 연계된 자산과 다양성보호계통의 기능에 따라 분석된 사이버보안 위협 시나리오에 따라 분석한 위험도는 <표 5>와 같다. 위험도 등급의 분석된 결과를 살펴보면 비안전등급 제어기의 출력 모듈이 취약한 코드 사용의 취약점으로 오류를 발생할 때 공학적안전설비-기기제어계통으로 잘못된 데이터가 전달되어, 보조급수 작동계통이 오작동을 일으키는 경우가 가장 높은 위험도를 나타내고 있다. 따라서, 사업자는 해당 사이버보안 위협에 대처하기 위하여 비안전등급 제어기의 출력 모듈의 소프트웨어 검증 및 오류를 줄이기 위한 방안을 우선 수립하여야 한다.

Ⅴ. 결론

계측제어시스템은 원자력 발전소를 안전하고 효율적으로 운영하기 위해 원자력 시설의 주요 변수를 계측하고 제어한다. 다양성보호계통은 10CFR50.62의 설계요건을 만족시키기 위해 정지불능 예상과도에 대한 위험을 감소시킬 수 있도록 가압기-고압력에 의한 원자로정지 및 터빈정지와 증기발생기-저수위에 의한 보조급수 작동을 수행한다. 계측제어시스템은 기존에는 아날로그 장비가 사용되어 사이버보안에 대한 고려가 중요하지 않았으나, 아날로그 장비의 노후화에 따른 성능저하, 유지비용 증가, 부품 단종의 문제점을 해결하기 위해 점차 디지털 장비가 사용되면서 사이버보안은 매우 중요해졌다.

본 논문에서는 다양성보호계통의 연계와 기능을 분석하고, 연계된 계통의 자산 가치를 계산하였다. 또한, 공격 트리를 활용하여 다양성보호계통에서 발생할 수 있는 사이버보안 위협 시나리오를 분석하였다. 분석된 위협 시나리오를 바탕으로 공격발생 확률을 계산하고, 자산 가치와 연계하여 사이버보안 위험도를 확인하였다. 원자력 발전소 사업자는 다양성보호계통과 관련하여 자산의 중요도와 위험도에 따라 적절한 사이버보안 대응 방안을 마련할 수 있을 것으로 기대한다. 동일한 자산 가치에도 위협의 심각성에 따

<표 5> 다양성보호계통의 위험도 평가

공격자산	사이버보안 위협 시나리오				자산 등급	공격발생 확률	위험도 평가
CEDMCS (incorrect variables)	logic failure (PZR pressure)	value error	field-sensors	-	1	1	1
			FCS input module	-	1	1	1
		data processing error	FCS CPU module	-	1	1	1
		setpoint	FCS CPU module	-	1	1	1
	logic failure (CNMT pressure)	value error	field-sensors	-	1	1	1
			FCS input module	-	1	1	1
		data processing error	FCS CPU module	-	1	1	1
		setpoint	FCS CPU module	-	1	1	1
AFAS	incorrect data (ESF-CCS)	logic failure (SG level)	value error	field-sensors	2	1	2
				FCS input module	2	1	2
			data processing error	FCS CPU module	2	1	2
			setpoint	FCS CPU module	2	1	2
		FCS output module	-	-	2	2	4
CEDMCS (trip signal error)	incorrect reactor trip signal	turbine trip enable setting error	value error	SC signal	1	1	1
				FCS input module	1	1	1
			data processing error	FCS CPU module	1	1	1
		turbine trip signal error	value error	CEDMCS signal	1	1	1
				FCS input module	1	1	1
			data processing error	FCS CPU module	1	1	1
	incorrect manual reactor trip signal	value error(SC)	SC signal	-	1	3	3
			FCS input module	-	1	1	1
operator error	incorrect data (IPS)	MTP malfunction	FCS output module	-	2	1	2
			FCS CPU module	-	2	1	2
	incorrect data (QIAS-N)	FCS output module	-	-	2	1	2
		FCS CPU module	-	-	2	1	2

라 위험이 달라지기 때문에 공격의 가중치에 대한 적용을 위해 추후 위협에 대한 분석을 바탕으로 각 공격 노드에 대한 가중치를 정량적으로 적용할 수 있는 방안을 마련하고자 한다.

참고문헌

[1] 이철권, “원전 계측제어시스템 사이버보안 기술 동향,” 한국정보보호학회, 정보보호학회지, 제22권, 제5호, 2012, pp.28-34.

[2] 송재구, 신진수, 이정운, 이철권, 최종균, “원자력 발전소 디지털 제어기의 사이버보안 기능 적합성 시험방법 연구,” 한국정보보호학회, 정보보호학회 논문지, 제29권, 제6호, 2019, pp.1425-1435.

[3] U.S. NRC, “Cyber Security Programs for Nuclear Facilities,” Regulatory Guide 5.71, 2010.

[4] 한국원자력통제기술원, “원자력 시설 등의 컴퓨터 및 정보시스템 보안 기술기준,” KINAC RS-015, 2016.

[5] NIST, “Guide for assessing the security controls in federal information systems,” SP800-53A Revision 1, 2010.

[6] IAEA, “Computer security at nuclear Facilities,” Nuclear Security Series No.17, 2011.

[7] NEI, “Cyber Security Control Assessments,” NEI 13-10 Revision 6, 2017.

[8] NEI, “Cyber Security Plan for Nuclear Power Reactors,” NEI 08-09 Revision 6, 2010.

[9] Bruce. Schneier, “Attack Trees”, Dr. Dobb’s Journal, Vol.24, No.12,1999, pp.21-29.

[10] 김경아, 이대성, 김귀남, “공격 트리를 이용한 산업 제어 시스템 보안 위험 분석,” 한국융합보안학회, 융합보안 논문지, 제11권, 제6호, 2011, pp.53-58.

[11] Yanggyun Oh, Jinkwon Jeong, Changjae Lee, Yoonhee Lee, “Fault-tolerant design for advanced diverse protection system,” Nuclear Engineering and Technology, Vol. 45, No. 6, 2013, pp.795-802.

[12] 정성민, “원전 다양성 보호계통 사이버보안 테스트베드 설계,” 한국정보처리학회, 2020온라인 춘계학술발표대회 논문집, 제27권, 제1호, 2020, pp.292-294.

[13] DHS, “Common Cybersecurity Vulnerabilities in Industrial Control Systems,” 2011.

[14] NIST, “Standards for Security Categorization of Federal Information and Information Systems,” FIPS PUB 199, 2004.

[15] Indrajit Ray and Nayot Poolsapassit, “Using Attack Trees to Identify Malicious Attacks from Authorized Insiders,” 10th European Symposium on Research in Computer Security, LNCS 3679, 2005, pp.231-246.

■ 저자소개 ■

정 성 민
(Jung Sungmin)

2020년 9월~현재
명지전문대학 교수
2014년 3월~2020년 8월
한국원자력연구원 선임연구원
2014년 2월 성균관대학교
전자전기및컴퓨터공학과(공학박사)

관심분야 : 산업시설보안, 제어시스템보안, 센서네트워크, 클라우드 컴퓨팅
E-mail : smjung@mjc.ac.kr

김 태 경
(Kim Taekyung)

2017년 9월~현재
명지전문대학 교수
2008년 3월~2017년 8월
서울신학대학교 교수
2006년 3월~2008년 2월
서일대학 정보전자과 교수
2005년 8월 성균관대학교
전자전기및컴퓨터공학과(공학박사)

관심분야 : 네트워크보안, 클라우드 보안, 개인정보보호
E-mail : tkkim@mjc.ac.kr

논문접수일 : 2023년 9월 4일
게재확정일 : 2023년 9월 12일