에너지 시스템의 사보타지 표적 인식 기법의 현황 및 전망

김성호, 최영, 정우식, 김길유, 양준언
한국원자력연구원

Current Status and Prospect of Techniques for Identification of Sabotage Targets

Seong Ho KIM*, Y. Choi, W.S. Jung, K.Y. KIM, J.E. Yang
Korea Atomic Energy Research Institute
(*Corresponding author: well48@hanmir.com)

초 록

미국 911 테러 발생 이후로, 국가 기반시설(예: 송/배전 전력망, 석유/가스 파이프라인, 원자력 발전소, 정보통신 시설, 교통 시설, 금융 시설, 매스미디어 시설 등)에 대한 테러리스트의 사보타지 리스크를 관리하는 도전문제에 정부 차원이나, 기업 차원에서 국내외적으로 뜨거운 이목이 집중되고 있다. 그 가운데 에너지 시스템, 특히 원자력 발전소의 물리적 보안은 국가 안보 차원에서 매우 중대한 이슈가 되고 있다. 이는 사보타지로 인한 이러한 시스템의 파손이 국민, 작업자, 또는 외부 환경에 방사성물질 누출과 같은 중대한 결말을 초래할 수 있기 때문이다.

원전과 같은 복잡 시스템에서 **설계 기준 위협**이 초래할 수 있는 이러한 결말은 그 시스템의 특정 **핵심** 표적(예: 부품, 구역, 자산, 행위, 인원)의 방호를 통해 효과적으로 방어될 수 있다. 다시 말하면, 표적 인식에서는 어떻게 방어할 것인가에 앞서서 **무엇을 방어할 것**인가를 다루려는 것이다. 이 연구의 주요 목적은 여태까지 개발된 다양한 표적 인식 기법의 개발 추세를 소개하고 향후 전망을 제시하는 데에 있다. 이를 통해 표적 인식 기법의 수월성, 신뢰성, 및 경제성을 제고할 수 있으리라 본다.

표적 인식 기술의 활용성 측면에서 볼 때, 표적 인식은 하드웨어적이거나 소프트웨어적인 방호 시스템의 설계에 필수적이므로, 신뢰성 높은 표적 인식은 다음과 같은 **긍정적인** 파급 효과를 줄 수 있다: 1) 사보타지 리스크 감소에 직간접적으로 기여할 수 있다; 2) 제한적인 보안 재원을 효율적으로 할당할 수 있다; 3) 보안 대응군대의 훈련 시나리오를 개발할 수 있다; 4) 발전소 규제요건인 안전조치 계획을 비용이나 보안 측면에서 향상시켜 **국민 안심** (public easiness)을 도모할 수 있다. 향후에는 보다 더 광의적인 복잡 시스템 사이에서 상호 연계적인 사보타지에 대한 표적 인식의 기법들이 점검될 필요성이 있다고 본다.

주제어: 사보타지 리스크, 표적 인식, 설계 기준 위협, 핵심 구역, 복잡 시스템, 국민 안심

1. 서론

에너지 시스템(예: 원자력 발전소, 화력발전소, 수력 발전소)은 시스템의 복잡성(complexity)을 특성으로 가지고 있다. 다시 말해, 이 시스템을 구성하고 있는 하드웨어/소프트웨어(사람 포함) 부품 간에는 상호작용, 상호의존성, 상호연결성 등이 존재하고 있고, 이를 통해 시스템의 성능이 동태적(dynamic)으로 나타나고 있다.

에너지 시스템과 같은 복잡 시스템에서 사보타지의 대상이 되는 표적을 파악하려면, 우선 관심 시스템의 특성에 바탕을 두고, 설계 기준 위협이 초래할 수 있는 결말(consequences) 등이 분석되어야 한다. 즉, 결말 평가가 수행되어야 한다. 여기서, **사보타지**란 사용/저장/수송 중에 있는 핵 시설이나 핵 물질 등을 향한 보건/안전/환경 측면에서 종사자/국민을 직간접적으로 위험하게 할 수 있는 고의적인 행동을 의미한다[1]. **설계 기준 위협**(Design Basis Threat; DBT)이란 핵 물질의 비인가된 제거나 사보타지를 시도할 수 있는 잠재적인 반대자에 대항한 물리적 방어 시스템의 설계나 평가시에 고려되어야 하는 이러한 반대자의 속성 및 특성을 뜻하고 있다[1].

표적 인식이란 테러리스트의 습격이나 사보타지로부터 방어되어야 하는 물질, 구역(areas), 재산(assets), 행위(actions), 또는 인원(personnels) 등을 찾는 과정을 의미한다. 보통, 표적 인식 기술은 표적이 가지고 있는 **정보의 특징**(features)에 따라 구별될 수 있다. 관심 표적은 다양한 정보의 특징 집합으로 구성되어 있다. 정보의 특징이란 정보의 종류(예: 이미지 정보, 문자 정보, 논리 정보 등)에 따라 상이할 수 있지만, 컴퓨터 인식에서는 이진법 숫자들로 전환된다.

표적 인식 시스템 설계는 다음과 같은 4-단계 절차를 통해 구현될 수 있다. 첫째, 문제 정의 단계에서는 표적, 정보의 특징 집합, 유사성 판단 기준 등을 정의한다. 둘째, 특징 추출 단계에서는 **대용 표적**(surrogate targets)을 구성한다. 특징 집합에서부터 몇 가지 주요 특징 요소들을 추출하고, 이들로 대표되는 대용 표적을 구성한다. 실제적으로는 이러한 대용 표적이 다뤄진다. 셋째, 표적 찾기 단계에서는 유사성 판단 기준에 부합되는 대용 표적 대안들을 찾아간다. 마지막으로, 표적 해석 단계에서는 전문가 판단을 통한 대용 표적 대안들의 선별이 이뤄진다. 이러한 선별을 통해 표적의 인식 신뢰성을 제고하고, 보다 현실적으로 대상 표적의 물리적 보안 시스템을 설계하게 된다.

2. 사보타지 표적 인식 기법의 현황 평가

예를 들어, 원자력 발전소(NPPs)가 사보타지의 대상이라고 하자. 일반적으로, NPPs는 방사능을 띤 핵물질을 평화적으로 사용하여 기저부하용 전기를 생산하고 있는 시설의 하나이다. 전과정(life cycle) 개념에서 NPPs를 보면, 건설 단계, 운영단계, 재처리 단계, 폐기 단계 등이 있다.

핵 물질 확산과 방사성핵종 누출 등의 결말을 초래하는 사보타지 리스크의 **위협 대상**(threats)은 주로 운영 단계, 재처리 단계, 또는 폐기 단계와 관련되고 있다. 운영 단계에서는, 국내로 수입되는 핵연료 물질의 수송, 성형 가공 단계의 핵연료 제조, 제조된 핵연료의

국내 수송, 발전소 내 보관된 핵연료, 발전 과정에서 생성되는 방사성핵종, 중저준위 방사성 폐기물, 사용후 연료와 같은 고준위 방사성폐기물 등이 위협의 대상이 될 수 있다. 재처리 단계에서는, 사용후 연료 수송, 사용후 연료의 재처리 시설 운영, 재활용 핵물질 제조/수송 등이 위협의 대상이 된다. 폐기 단계에서는, 사용후 연료 수송, 사용후 연료 처리 시설, 사용후 연료 처분 시설 등이 위협의 대상이 될 수 있다. 이론적으로 이러한 위협의 대상은 동태적이므로 동태적 표적 인식이 필요하다. 그러나 실제적으로는 기술 개발의 난이 때문에, 시스템 경계는 정태적으로 설정되고 정태적 표적 인식 접근법이 시도되고 있다.

NPPs에 있는 이들 위협의 대상에 대한 **사보타지의 결말**로 환경 측면에서는 방사성 물질의 누출을 통한 방사능 오염, 보건 측면에서는 이로 인한 작업자 피폭이나 국민 피폭을 통한 조기 사망자 및 암 사망자 발생, 경제 측면에서는 국가 전력 공급 불안정, 사회 측면에서는 국민 불안 조성, 국가 에너지 공급 위기, 삶의 질 저하 등이 초래될 수 있다. 이러한 심각한 결말의 초래 가능성은 NPPs의 노심 손상 방지 관리를 통해 통제될 수 있다.

NPPs에서 이러한 심각한 결말의 초래를 막기 위해 사보타지로부터 방어되어야 하는 특정 구역의 인식 과정이 바로 표적 인식의 하나인 **핵심 구역 인식**(vital area identification; VAI)이라고 불리고 있다 [2]. 여기서 핵심 구역(vital area)이란 심각한 결말을 직간접적으로 초래할 수 있는 사보타지의 대상이 되는 설비, 계통, 장비, 또는 핵 물질 등을 포함하고 있는 방어 구역(protected area) 내에 있는 구역으로 정의되고 있다 [1].

사보타지의 **정태적 핵심 구역 인식 기법**은 크게 두 가지 접근법으로 분류되고 있다 [2]: 1) 목록 접근법; 2) 논리 다이어그램 접근법. 여기서는 주로 대형 시스템의 VAI 기법으로 사용되고 있는 논리 다이어그램 접근법의 연구 개발 현황을 소개하고자 한다. 이는 표적 인식 기술과 관련된 문헌 가운데 입수 가용한 연구 개발 자료의 검토를 통해 수행되었다.

현재 사용되고 있는 **논리 다이어그램 접근법**은 1970년대에 적용되기 시작한 **고장 수목 분석**(Fault Tree Analysis; FTA) 기법에 바탕을 두고 있다. 논리 다이어그램의 하나인 고장 수목(FT)은 부울 대수식으로 서술되는 그래픽 표현법을 사용하고 있다. 이 기법으로 얻어진 최소 구역 집합(minimal areas set)이 핵심 구역으로 간주되고 있다. 일반적인 VAI 기법의 절차는 1) 시설 특성 파악; 2) 설계 기준 위협 결정; 3) 위협-기반 결말 분석; 4) 결말-기반 표적 인식; 5) 표적 인식의 활용. 활용 단계에서는, 표적 대안들의 최우선이나 순위 등을 통한 물리적 안보 시스템의 설계 [3], 기존 물리적 안보 시스템의 변경 등이 수행될 수 있다.

이러한 FTA 기법은 주로 집중된 표적, 상호 독립적인 위협, 시간-독립적인 정태적 표적 등에만 적용되고 있다는 것이 **FTA 기법의 제약 사항**이 될 수 있다. 그러나 이러한 제약 안에서도 이 기법은 구조적인 분석법이며 소프트웨어 도구들이 가용하므로, 규범적이고 논리적이며 반복적인 적용이 가능하다는 것이 **FTA 기법의 장점**이 될 수 있다. 반면에, 이 기법으로 결과를 얻는 과정은 매우 시간-소모적이고, 그 결과는 분석자에 따라 상이할 수 있으므로 분석-의존적이라고 볼 수 있다. 이는 **FTA 기법의 단점**이 된다.

현재 개발된 표적 인식 기법은 1) SNL 접근법; 2) BNL 접근법; 3) NSP 접근법; 4)

KAERI 접근법 등으로 분류되어 서술될 수 있다.

SNL 접근법: 고장 수목 분석 기법이 처음으로 핵심 구역 인식 기법에 도입되어 개발되었다. 1970년대에 사보타지 고장 수목(SFT)이라는 용어를 사용하면서, 정점 사건으로 사보타지-기인 사건이 고려되었다 [4]. 이러한 SFT의 논리적 표현은 부울 사건-대수식에 해당한다. 이 사건-대수식의 기본 사건을 위치로 변환하면, 위치-대수식이 산출된다. 이러한 위치-대수식에서 Type k-최소 구역 집합(minimum areas set)이 산출된다(여기서, k=1 또는 2). 이 기법에서는 FT 기법의 단점인 시간-소모적 과정 및 분석-의존적인 결과 산출 등을 개선하기 위해, 우선 일반 SFT 접근법이 제안되었다. 이에 따르면, 고려 대상인 시스템의 특정 차이점에 이러한 일반 SFT에 반영되어 모델링이 실행된다.

2000년대에 문헌[5]에서는 표적 집합, 즉 최소 단절 집합(MCSs)로부터 방어 집합(protection sets), 즉 핵심 구역 집합을 산출하기 위해 정점 사건 방지 분석(Top event prevention analysis; TEPA) 기법이 도입되었다. 이 기법에서는 5-단계 절차가 제안되었다: 1) 고장 수목 구축; 2) 표적 집합, 즉 최소 단절 집합(MCSs)을 산출하기 위한 고장 수목 풀이; 3) 사건의 조합으로 구성된 MCSs로부터 방지 집합(prevention sets), 즉 방어 집합을 산출하기 위해 TEP 도구를 사용한 TEP 풀이; 4) 방지 집합과 관련된 구역 데이터의 적용; 5) 방지 집합의 선별.

BNL 접근법:

1995년도 문헌[6]에서는 레벨 L_k-방지 집합을 산출하는 TEPA 기법이 도입되었다. 여기서는 노리 모델로 FT 대신에 신뢰도 블록 다이어그램(RBD)이 사용되었다. 이러한 TEPA 기법은 5-단계로 분류되어 적용되었다: 1) 논리 모델 개발 및 단절 집합 산출; 2) 방지 기준 설정; 3) MCS별 방지 기준 적용 및 논리식 산출; 4) 방지 집합 산출; 5) 선별 판단 기준(예: 비용 최소화)에 따른 방지 집합의 선정 및 최소 방지 집합(MPS) 산출.

NSP 접근법:

이 기법은 미국 Northern States Power Company(NSP)가 운전하고 있는 몬티첼로 원자력 발전소의 방어 요건(예: 10 CFR 73의 55절, 부록 B, 부록 C)을 수정하는 데에 사용하기 위해 개발되었다. 1999년도에 발표된 문헌[7]에 따르면, 방사성 물질 누출 대신으로 대용 결말인 노심 손상이 사용되었다. 여기서는, DBT로 발전소 계통/부품의 기능 상실이 노심 손상을 유발하는 경우에, 이러한 발전소 계통/부품이 표적으로 정의되었다. 적용된 TEPA 기법은 5-단계 과정으로 서술되었다. 모델링 단계에서는 SFT가 구축된다. 이 기법에서는 기존의 PSA FT 모델 사용 대신에 신규 모델링이 수행되었다. 그 이유는 표적 사보타지 사건에 대하여 고장 수목이 상대적으로 단순하고 요건이 기존 PSA의 요건과는 상이하기 때문이다. DB 구축 단계에서는 몇 가지 가정 사항 및 공통 위치를 반영하면서 앞의 SFT를 확장하여 확장 SFT(ESFT)가 구축되었다. 해법 단계에서는 이러한 ESFT으로부터 방지 집합이 얻어진다. 선별 단계에서는 최소 중요 표적(MCT)을 선정하기 위해 표적 판단기준으로 표적 개수, 방어 수월성 등이 방지 집합에 적용되었다. 이러한 MCT는 발전소 보안 전략 제

시, 보안 자원의 최적화, 안보군사력의 훈련 시나리오 개발 등에 활용되었다고 한다.

KAERI 접근법 (또는 PSA-기반 접근법): 2005년도에 발표된 문헌[8]에 따르면, 방사성 물질 누출 대신으로 대용 결말인 노심 손상이 사용되었다. 제안된 VAI 절차는 5-단계로 구성되었다. 모델링 단계에서는 레벨 1 PSA 결과를 활용하면서 이러한 노심 손상 FT가 구축된다. 여기서 최소 단절 집합(MCSs)이 얻어진다. DB 구축 단계에서는 m: {기본 사건}→{구역} 같은 사상(mapping)이 얻어진다. 결합 단계에서는 사상 데이터가 반영된 위치 FT가 구축된다. 해법 단계에서는 SFT 분석으로 얻어진 최소 단절 집합(MCSs)에서 방지 집합을 산출하기 위해 정점 사건 방지 분석(Top event prevention analysis; TEPA) 기법이 적용된다. 심층 방어 레벨 L_k(k=1,2,...)가 고려되어, L_k-TEP 집합이 산출된다. 이러한 L_k-TEP 집합이 바로 핵심 구역 집합 대안이 된다. 해석 단계에서는 전문가 판단을 통해 핵심 구역 집합이 선별된다. 이 기법에서는 이미 개발된 레벨 1 PSA의 고장수목 모델이 사용되므로 PSA-기반 기법으로 불리고 있다. 기존의 PSA 결과를 사용하는 특성 때문에, 이 기법은 모순이 없고 가장 완벽한 기법이라고 서술되었으나, 한편으로는 그 때문에 이 기법은 PSA 결과가 가용한 원자력 설비에만 적용될 수 있다는 제약 사항을 가지고 있다. 이 기법의 알고리즘은 VIP라는 소프트웨어 도구를 통해 구현된다.

간추려 비교하기 위해, 각 기법의 특성이 구현 단계별로 Table 1에 정리되었다. 각 접근법에서 표적 인식은 공통적으로 모델링 단계, DB 구축 단계, 결합 단계, 해법 단계를 거쳐 구현되고 있다.

Table 1: 검토-가능한 핵심 구역 인식 기법의 비교

	SNL 기법[4]	BNL 기법[6]	NSP 기법[7]	KAERI 기법[8]
모델링 단계	사보타지FT(SFT)	RBD, 최소단절집합	사보타지 FT(SFT)	노심손상FT(CDFT), 최소단절집합(MCS)
기법의 특성	일반SFT 및 특정SFT 사용	TEPA 사용, 중요도측도-기반 방지집합 선정	TEPA 사용, 방지 집합	PSA-기반 FT 사용
DB구축 단계	위치 지정	방지 기준 설정	가정 사항 및 공통-위치 반영	m:{기본사건}→{구역}
결합/해법 단계	위치 논리식, Type k-최소구역집합 (k=1, 2)	- 최소방지집합 산출	확장SFT, 최소중요표적산출	위치FT, L_k-TEP 집합
구현 도구	SETS 코드	-	CAFTA 코드	VIP 코드

3. 표적 기법의 전망 평가

원자력 발전소에서 핵심 구역이라는 특정 표적을 방어하면 핵물질 확산이나 방사성핵종 누출이라는 심각한 결말을 초래하는 사보타지로부터의 설계 기준 위협을 방지할 수 있다고 볼 수 있다. 어떤 기술의 가치는 여러 가지 기술 특성 요소로 평가된다. 표적 인식 **기술 가치 평가**는 다음과 같은 세 가지 기술 평가 요소에 바탕을 두고 평가될 수 있다: 1) 표적의 분산성 정도; 2) DBT 간의 상호의존성 정도; 3) 표적의 시간의존성 정도.

원자력 발전소의 핵심 구역 인식과 관련하여, 현재 개발되고 있는 표적 인식 기술은 집중된 표적, 독립적 위협, 정태적 표적 등을 주요 가정 사항으로 하여 개발되고 있다. 그러나

현실적인 사보타지 리스크의 특성은 분산된 표적, 상호의존적 위협, 동태적 표적 등이 조합되어 있는 양상을 띨 수 있다.

향후 표적 기법의 전망과 관련하여, 다음과 같이 세 가지 논점이 전개될 수 있다:

1) 향후 표적 기법은 분산성 정도가 높은 표적을 고려하여 개발되어야 한다. 분산된 표적을 다룰 수 있는 기법의 하나로 에이전트-기반 모델링(agent-based modeling; ABM) 기법이 적용될 수 있다. 이러한 ABM 기법은 또한 동태적 기법으로 사용될 수 있다. 예컨대, 이 기법은 미국의 국가 기반시설(예: 송/배전 전력망, 석유/가스 파이프라인, 원자력 발전소, 정보통신 시설, 교통 시설, 금융 시설, 매스미디어 시설 등)의 안보 시스템 구축에서 샌디아 국립연구소(SNL)에서 개발되고 있는 기법이다.

2) 향후 표적 기법은 상호의존성 정도가 높은 위협을 고려하여 개발되어야 한다. 상호의존적 위협을 다룰 수 있는 기법으로는 ABM 기법, 시스템 다이내믹스(system dynamics; SD) 기법, 인공 신경망 기법 등이 적용 가능하다.

3) 향후 표적 기법은 시간의존성 정도가 높은 표적을 고려하여 개발되어야 한다. 동태적 표적을 다룰 수 있는 기법으로는 ABM 기법, SD 기법 등이 적용 가능하다.

4. 결어적인 제언

현재 적용되고 있는 표적 인식 기법의 현황이 소개되었다. 이러한 표적 인식 기술의 연구개발 정책이 장래에 나아가야 할 방향은, 비록 다른 요소(예: 타 분야의 표적 기술로의 접목 활용성 정도)에서도 가능하지만, 여기서는 세 가지 기술 평가 요소(즉, 분산성, 상호의존성, 시간의존성)의 관점에서 제안되었다. 향후 나타나는 표적 인식 기술은 이러한 삼요소인 분산성, 상호의존성, 시간의존성의 조합으로 구성된 기술 가치 매트릭스 안에서 정성적으로 평가될 수 있으며, 계량 지표가 개발된다면 또한 정량적인 평가도 가능하다고 볼 수 있다.

참고문헌

1. IAEA (May 1999): The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4(Corrected).
2. M.L. Garcia (2001): Chapter 4 Target Identification, in *"The Design and Evaluation of Physical Protection Systems,"* Elsevier, PP.39-50.
3. IAEA (2007): Engineering Safety Aspects of the Protection of Nuclear power Plants against Sabotage, IAEA Nuclear Security Series No.4, Technical Guidance.
4. G.B. Varnado and N.R. Ortiz (1979): Fault Tree Analysis for Vital Area Identification, SAND79-0946, Sandia Labs., USA.
5. D.P. Blanchard et al. (2005): Risk-Informed Physical security: Dynamic Allocation of Resource, PSA'05, California.
6. R.W. Youngblood and R.B. Worrell (1995): Top event prevention in complex systems, BNL-61607.
7. EPRI (Oct 1999): An Approach to Risk-Informed Physical Security, Electric Power Research Institute, EPRI TR-113787.
8. W.S. Jung et al. (Sep 2005): Vital Area Identification Methodology for the Physical Protection of Nuclear Power Plants, IEEE International Conference on TEHOSS, Poland.