2002 춘계학술발표회 논문집
한국원자력학회

물리적방호시스템의 유효성평가 프로그램 개발

Development of A Effectiveness Evaluation Program for Physical Protection Systems

이현철, 안진수, 황인구, 최영명
한국원자력연구소
대전광역시 유성구 덕진동 150

정광태
한국기술교육대학교
충남 천안시 병천면 가전리 307

요 약

물리적방호시스템의 유효성평가는 실사, 체크리스트, 혹은 소프트웨어 등을 사용하여 수행할 수 있다. 소프트웨어 프로그램을 활용하는 경우 다른 방법보다 정량화되고 또한 일관성 있는 결과를 얻을 수 있다. 한국원자력연구소에서는 물리적방호시스템의 유효성을 평가하기 위해 사용되어온 기존의 소프트웨어보다 모델링과 사용자 인터페이스 측면에서 보다 개선된 성능을 제공하는 KAVI를 개발하였다. KAVI는 방호시설의 입력과 분석을 통합하였고 네트워크를 이용한 시설모델링 방법을 사용하고 있으며 사용자의 입력을 위해 GUI를 제공하고 있다. 또한, 유효성평가의 척도인 PI, TRI, CDP 등을 분석결과로 제공하고 민감도분석을 수행할 수 있도록 해준다.

Abstract

The effectiveness evaluation for a physical protection system can be carried out work-through, check-lists, or a software program. In case that a software program is used for the effectiveness evaluation, quantitative and consistent results can be obtained in contrast to the other methods. Korea Atomic Energy Research Institute developed a software program, called KAVI, that provides more improved performance compared with other programs used for the effectiveness evaluation of a physical protection system in aspects of modelling methods and user interfaces. KAVI integrates facility data input and effectiveness analysis functions, adopts a network-based facility modelling method, and provides graphical user interfaces for

user input. In addition, effective measures, such as PI, TRI, CDP and etc., are generated as analysis results and sensitivity analysis can be done by KAVI.

1. 서 론

핵물질과 원자력 시설에 대한 물리적 방호(physical protection)란 「핵물질의 탈취 등에 의한 불법적 이전 및 원자력시설 등의 운영에 대한 방해, 파괴행위를 방지함과 동시에 불법적 이전 또는 방해가 발생할 우려가 있는 경우, 또는 발생한 경우에는 신속하고 총체적인 대응조치를 강구할 수 있는 체제를 정비하고 유지하는 것」으로 정의되는데, 이러한 목적으로 구축된 시설, 장비, 혹은 조치로 구성되는 통합적인 시스템 혹은 체제를 물리적 방호시스템이라 한다[1].

일반적으로 시스템의 평가는 확인 및 검증(verification and validation)이라는 두 가지 활동으로 구분할 수 있다[2]. 확인(verification)이란 시스템의 요구사항이 설계(design)나 설치물(installation)에 적절히 반영되어 있는 지를 조사하는 것으로 설계된 시스템 혹은 설치물이 시스템 요건에서 구비하도록 요구한 구성품(components)이나 특성을 갖추고 있음을 보장하는 것이다. 따라서 확인활동은 시스템요건으로부터 추출된 구성품이나 특성에 대한 구비목록이 필수적인 평가도구이다. 목록내의 각 항목에 대해 구비여부를 판단하여 구비하지 못하고 있는 항목을 찾아내고 시스템에 추가하도록 하는 것이 주요 평가활동이다. 반면에 검증은 일반적으로 확인활동이 완료된 후에 실시하는데, 설계된 시스템이나 설치물이 시스템의 목적이나 기능을 만족하는 지를 조사하는 것으로 상호 연관된 시스템의 구성물들이 유기적으로 작용하여 발휘하는 성능(performance)을 보장하는 것이다. 따라서 검증활동은 시스템의 성능에 대한 측정(measurement) 및 판단기준(decision criteria)이 필수적인 평가도구이다. 설계시 고려된 조건하에서 설계된 방호시스템 혹은 설치물의 성능을 측정하고 그 측정치와 만족여부를 판단할 수 있는 기준치을 비교하여 불만족시 시스템의 성능 향상을 위한 설계수정이나 시스템 개선을 요구하는 것이 주요 평가활동이다.

물리적 방호시스템의 평가의 확인 및 검증을 적용하는 경우, 확인은 탐지(detection), 지연(delay), 대응(response) 등의 방호기능을 담당하는 각 방호설비가 적절히 배치되도록 설계되었는 지를 조사하는 것이며 검증은 이러한 방호설비들이 설정된 특정의 침입세력으로 부터 핵물질 혹은 핵시설의 절취나 파괴공작(sabotage)을 막아낼 수 있는 지를 분석하는 것이다. 따라서 방호시스템의 확인은 각 설비가 요구되는 사양의 제품을 사용하여 적소에 배치되고 설치시 유의사항을 준수하여 설치되고 운용되고 있는 지 등의 항목을 조사하고 불만족 사항을 발견하는 경우 이를 반영하도록 하는 것이며, 검증은 특정의 침입세력에 대한 방호력을 나타낼 수 있는 특정의 성능을 측정하고 이를 판단기준과 비교하여 성능의 만족여부를 결정하는 것으로 간주할 수 있다. 확인시 사용할 수 있는 구비목

록은 방호시스템의 구성품별로 구성품의 시방, 설치방법 및 고려사항, 운용조건 및 체제 등을 항목으로 작성하고 이를 통해 구비여부 혹은 항목의 만족여부를 판단할 수 있을 것이다. 이러한 확인활동은 다양한 표준(standards)이나 지침(guidelines)을 기반으로 작성된 일련의 체크리스트(checklist)를 활용하는 것이 보편적이다.

가. 물리적 방호시스템의 유효성

검증활동은 명확히 규정할 수 있는 측정 및 판단기준이 필수적인 요소이다. 판단기준은 방호시스템으로부터 얻은 측정치를 적합/비적합 혹은 통과/실패로 구분할 수 있는 기준점으로 측정치와 동일한 단위를 사용한다. 하나의 측정치에 의해 방호시스템의 성능을 평가하는 경우에는 일반적으로 하나의 측정기준이 필요하지만 다수의 측정치에 의해 방호시스템의 성능을 평가하는 것이 일반적이므로 다수의 측정기준이 정의되어야 한다. 현재까지 물리적 방호시스템의 평가에 활용되어온 종속변수(측정치의 속성, 측정변수, 혹은 척도)는 저지확률(Probability of Interruption; PI), CDP(Critical Detection Point), TRI(Time Remaining after Interruption), CPD(Cumulative Probability of Detection) 등이 있다[3]. 물리적 방호시스템의 유효성(effectiveness)이란 바로 이러한 성능 측정치들과 판단기준에 의해 결정된다. 판단기준은 기본적으로는 위험분석(risk analysis)을 토대로 결정된다[4]. 위험분석은 가중치와 피해를 주요 인자로 하는 단순한 연산으로 수행될 수 있는데, 일반적으로 가중치와 피해의 정량화에는 전문가의 판단이 개입하게 된다. 판단기준을 만족하는 성능측정치를 얻은 경우에 그 방호시스템은 유효하다라고 할 수 있으며 반대의 경우에는 시스템개선의 필요가 있는 것이다.

나. 물리적 방호시스템의 성능과 침입세력

물리적 방호시스템의 성능은 조건부로 결정되어 진다. 물리적 방호시스템은 물리적인 배치 및 운용체계 등이 정적이지만 방호시스템의 성능은 침입세력의 능력에 따라 다르게 측정평가 되기 때문이다. 침입세력의 능력이 낮은 수준인 경우 방호시스템의 성능이 높을 수 있으나 침입세력의 능력이 높은 수준인 경우 성능은 저하될 수 있다. 따라서 물리적 방호시스템의 유효성평가는 하나의 절대적인 수치를 찾아내기보다는 특정 침입세력에 대한 상대적인 시스템의 방호능력을 조사 분석하는 작업임을 주지하여야 한다. 침입세력의 능력은 설계기준위협(Design Basis Threat; DBT)에 의해 결정되는데, 설계기준위협 또한 시간적, 공간적으로 변화하는 성질이 있다. 따라서 물리적 방호시스템의 유효성평가는 변화하는 설계기준위협에 따라 주기적 혹은 반복적으로 수행되어야 한다.

물리적 방호시스템에 대한 침입세력의 능력은 다수의 변화하는 차원(dimension)을 포함한다. 첫 번째 차원은 침입세력의 자원(physical resource)이다. 침입세력의 구성인원, 무장상태, 훈련정도 등이 이에 속한다. 잘 훈련된 인원이 많은 경우 침입세력의 능력은

높을 것이며 반면에 훈련이 덜 된 적은 인원으로 구성된 침입세력의 능력은 낮을 것이다. 또한 강력한 도구, 예를 들면 중화기와 다양하고 강력한 폭발물로 무장한 침입세력은 소화기로 무장한 침입세력보다 침입능력이 우월하다고 할 수 있을 것이다. 두 번째 차원은 전술(strategy)이다. 침입의 대상이 되는 목표 혹은 핵물질 혹은 핵시설에 대한 지식 혹은 침입목적에 대한 확고한 정신무장 뿐만 아니라 경비상태에 대한 사전지식을 기반으로 한 최적/최단의 침입경로 및 침입방법을 설정하고 대응인력의 무력화 내지는 우회방안을 강구하는 등의 계획을 수립하는 침입세력의 능력이다. 세 번째 차원은 지원세력의 유무이다. 침입대상물 혹은 시설의 종사자 이외의 인원(outsider)으로 구성된 침입세력 보다는 침입대상시설내의 종사자 혹은 내부 공모자(insider)의 도움을 받는 침입세력이 보다 높은 침입능력을 발휘할 수 있을 것이다. 물리적 방호시스템의 유효성평가는 이러한 침입세력의 능력을 정의하는 다양한 차원 및 차원내의 속성을 고려하여 수행하여야 한다.

다. 유효성평가 프로그램 (KAVI)

물리적방호시스템의 유효성을 정량적으로 평가하기 위해서 소프트웨어 프로그램이 사용되어 왔다. PI, CDP, TRI등의 척도를 계산하고 민감도분석을 수행하는 등의 평가작업은 컴퓨터 프로그램을 통해 신속하고 일관성있게 수행할 수 있다. 한국원자력연구소는 국내고유의 유효성평가 소프트웨어인 KAVI를 개발하였다. 개발목적은 미국의 SNL(Sandia nationl lab.)에서 개발한 SAVI(System Analysis of Vulnerability to Intrusion)와 같은 프로그램으로는 국내 방호시설 데이터를 충분히 만족할 만한 수준으로 입력하여 평가하기가 곤란하고 따라서 국내의 방호시스템의 성능을 정확히 평가할 수 없다고 판단하였기 때문이다. 또한 주기적으로 수행하여야 하는 유효성 평가활동을 위해서는, 발전하는 보안설비분야가 계속적인 신제품을 개발한 경우 이를 반영하거나 과거의 운용실적에 따라 방호설비에 대한 성능을 수정 및 보완해야 하는데 이를 SAVI가 지원하기 힘들기 때문이다. 그리고 새로운 분석방법이나 평가척도를 구현하기가 곤란하다. 그러나 고유의 소프트웨어를 개발함으로써 사용상의 한계를 극복할 수 있으며 국내 방호대상시설에 관한 지속적이고도 유연한 평가도구를 확보하게 되고, 아울러 개발과 함께 확보될 방호시스템 평가기술은 국내외 타 산업분야에 응용할 수 있는 기반기술이 될 수 있을 것이다.

2. 유효성평가 소프트웨어의 종류 및 특징[2][3]

물리적 방호시스템의 유효성 평가를 위한 도구는 주로 미국이 오래 전부터 개발되어 왔고 많은 종류가 있다. EASI와 SAVI는 SNL에서 개발한 대표적인 소프트웨어 프로그램이며 한국원자력연구소에서는 1999년도에 PIGSAM를 개발한 바 있고, 2001년도에는 KAVI를 개발하였다. 여기에서는 유효성평가에서 사용되는 침입경로의 의미를 설명하고 이어서 기존의 유효성평가 소프트웨어 프로그램의 특징을 살펴본다.

가. 침입경로(Adversary Path)

침입경로는 침입세력이 방호시스템의 외부로부터 침입을 시도하여 침입목적을 달성하기까지의 수행하여야 하는 활동을 순차적으로 표시한 것으로 정의된다. 따라서 침입경로는 시작점은 방호시스템의 외부로 정의되며 종료점은 목표물의 성공적인 탈취나 파괴공작으로 결정된다. 특정의 침입능력을 가진 침입세력이 목적을 달성하는 방법은 다양할 것이므로 한 침입세력에 대해 다수의 침입경로가 존재한다. 즉, 침입세력은 다수의 침입경로 중 하나의 경로를 선택하게 될 것이다. 침입세력이 수행하는 활동은 결국 방호시스템 내의 방호설비(Protective Element or Path Element; PE)를 무력화시키거나 혹은 우회하는 것으로 침입세력은 목적을 달성하기 위해 최소한의 시간이나 자원을 소요하는 침입경로를 선호할 것이다. 다음의 그림 1은 특정의 침입세력이 특정 방호시설내의 펌프를 파괴하기까지의 하나의 침입 경로를 보여주며 표 1에서는 침입경로에 대응하는 방호설비(지연설비 및 감지설비)를 나타낸다.

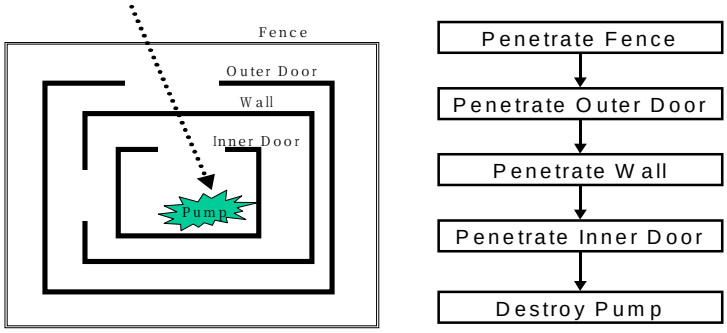

그림 1. 침입경로의 예
(a) 침입대상시설의 약도 및 경로표시
(b) 침입경로

나. EASI 모델

EASI(Estimate of Adversary Sequence Interruption) 모델은 물리적 방호시스템을 분석/평가하기 위해 개발한 경로수준모델(path-level model)이다. 즉, 일회에 하나의 침투경로(path) 혹은 하나의 가상 침투시나리오(one adversary scenario)에 대한 방호시스템의 성능을 분석하기 위해 고안되었으며 PC에서 작동될 수 있도록 작성되어 있다. 핵물질의 탈취나 방해/파괴행위를 방지하기 위해서는 대응인력(response force)은 그 불온한 시도

표 1. 침입경로와 방호설비(지연설비 및 감지설비)

Sequence	Adversary Action	Delay Element	Detection Element
1	Penetrate Fence	Fence Fabric	Fence Sensor
2	Penetrate Outer Door	Door Hardness	Sensors on Door
3	Penetrate Wall	Wall Hardness	Personnel Hear Noise
4	Penetrate Inner Door	Door Hardness	Sensors on Dor
5	Destroy Pump	Time Required to Sabotage Pump	Loss of Pump

를 제지할 수 있는 충분한 시간을 확보해야만 한다. 따라서 경보전달과 대응인력에게로의 통보 등이 분석에 포함되어야 하는 요소이다. EASI모델에서는 물리적 방호시스템이 적절히 작용한다면 침입자(adversary)의 시도는 막강한 대응력에 의해 제지되는 것으로 평가된다(대응력은 충분히 커서 불온한 시도를 탐지하는 경우 반드시 이를 제지할 수 있다고 가정한다). EASI 모델은 정량적인 계산이 가능하다는 장점이 있으나, 신뢰성 있는 입력데이터의 확보에 매우 의존적이다. 또한 일회에 하나의 경로에 대한 분석만이 가능하므로, 입력데이터의 영향을 알아내기 위해서는 다수의 반복수행이 필요하며, 가능한 모든 경로 중에서 가장 취약한 경로를 탐색하기 위해서는 다른 모델 혹은 분석방법이 필요하다는 단점이 있다.

다. PIGSAM

PIGSAM(Probability of Interruption Generator with Sensitivity Analysis Module)은 한국원자력연구소에서 1999년에 개발한 취약성분석 소프트웨어로서, EASI 모델을 기반으로 민감도분석을 수행할 수 있도록 개선한 것이다. EASI 프로그램은 정규분포의 분포함수(Distribution Function)를 구하기 위하여 근사식을 사용하고 있으며 또한 반복적인 프로그램시행에 따라 민감도분석을 실시할 수 있도록 설계되어 있다. 그러나 PIGSAM은 정규분포의 분포함수를 보다 정밀하게 계산하기 위해서 수치해석코드를 사용하고 있으며 감지확률(detection probability)에 대한 민감도분석 결과를 함께 보여준다. 또한 PI에 대한 각 감지확률(detection probability)의 공헌도를 미리 예측할 수 있는 민감도분석결과를 PIGSAM에서는 제시해준다. 민감도분석결과는 현재의 감지확률이 PI에 공헌하고 있는 경우 한 단위 증가시켰을 때에 PI의 증분(increment)을 보여주며, 감지확률이 현재의 PI에 공헌하지 못하고 있는 경우에는 감지확률이 0.9로 설정되었을 때에 예측되는 PI값을 제시해 준다.

PIGSAM은 EASI모델을 기반으로 저지확률을 계산해주고 또한 감지확률의 민감도를 제시해주는 역할을 하고 있으나 통합시스템인 물리적 방호시스템의 성능을 완전히 분석하고 평가하기에는 미흡하다. 탐지확률에 대한 민감도를 제시해주기는 하지만 기본적으로 단일침투경로에 대한 분석을 기반으로 하기 때문에 가능한 모든 침투경로에 대한 분석을

수행하기에는 불편하다.

라. SAVI

SAVI(System Analysis of Vulnerability to Intrusion)는 ASD(Adversary Sequence Diagram)을 사용하여 방호대상시설에 관한 데이터 및 침입세력에 대한 데이터를 입력받아 제지확률 PI와 CDP, TRI 등을 분석해 주는 소프트웨어로 버전 4.0이 사용되고 있다.

SAVI는 침입세력이 활용할 수 있는 전술로 Force/Stealth Only와 Force/Stealth/Deceit 등의 두 가지 중 하나를 선택할 수 있게 해준다. Force/Stealth Only는 침입세력이 방호설비의 기능을 우회하거나 혹은 무력으로 제거하는 침입방법만을 사용하는 것이며, Force/Stealth/Deceit는 Force/Stealth전술을 포함하면서 출입통제설비와 같은 인증설비에 대해서는 위조된 출입증을 사용하는 등의 위장전술을 사용하는 것이다. SAVI에서는 방호시스템의 한 요소기능인 대응(Response)에 선택을 할 수 있도록 하고 있다. 대응은 Containment와 Denial로 구분되는데, Containment는 침입세력을 고립시켜 더 이상의 침입 및 도주가 불가능하도록 하는 것이며 Denial은 침입세력이 목표물에 도달하지 못하도록 막아내는 것을 목적으로 하는 대응전략이다. 따라서 Containment는 핵물질의 탈취에 주로 사용되는 대응전략이며, Denial은 핵시설에 대한 파괴공작에 대응하기 위한 전략이다.

SAVI는 방호시스템을 ASD에 의하여 표현하도록 하고 있다. ASD는 침입의 시작점인 시설외부를 맨 위에 그리고 목표물을 맨 아래에 위치시키고 침입세력이 대면해야하는 방호시설을 방호구역별로 정의하도록 하고 있다. ASD를 작성하는 순서는 우선 방호시스템을 인접하는 물리적 구역(Physical Area)로 구분하고, 방호계층(Protection Layer)를 정의하고 물리적 구역사이에 존재하는 방호설비(Protection Element)를 정의하는 것이다. SAVI는 최대 10개까지의 물리적 구역을 정의할 수 있으며 15개의 방호설비(Protection Element; Path Element; PE)를 하나의 방호계층에 입력할 수 있다. SAVI에서 사용할 수 있는 방호설비 총 20개이다. SAVI는 두 개의 실행파일을 제공하는데, Facility.exe와 Outsider.exe이다. Facility.exe는 ASD를 생성하고 각 방호설비에 대한 데이터를 입력하는데 사용된다. Outsider.exe는 궁극적인 소프트웨어의 기능인 유효성분석을 수행하기 위해 사용되는데, Facility.exe에서 생성된 ASD와 입력데이터를 우선적으로 입력받도록 되어있다. ASD는 침입경로를 즉시 나열해 주지 않고 단순히 방호설비를 방호구역별로 나누어 입력하도록 요구하고 이를 통해 가능한 침입경로를 자체적으로 생성하기 위해 사용된다.

사용자가 입력한 방호시스템에 관한 데이터는 pps라는 확장자를 갖는 파일로 저장되는데 텍스트파일이 아닌 이진파일로 작성된다. 이 파일은 SAVI에서 분석을 위해 사용되는 실행파일인 Outsider.exe에 입력파일로 활용된다. 물리적 방호시스템의 유효성분석을 수행하는 Outsider.exe는 Facility.exe에서 작성한 방호시스템 데이터, 대응팀이 침입세력을

저지할 때까지 소요되는 시간인 RFT(Response Force Time), 분석조건, 침입세력의 능력 및 전술, 대응전략 등을 사용자로부터 입력받아서 제지확률 PI와 TRI(Time Remaining after Interruption) 등을 제시하여 주고 취약성분석 및 민감도분석을 도표로 제시하여 준다. 그림 2는 한 가상시설에 대해 RFT를 300초로 대응전략을 Denial로, 침입세력을 Terrorist Vehicle/Helicopter로, 침입세력이 적용할 전술로는 Force/Stealth/Deceit를 설정하였을 때 분석결과를 보여준다.

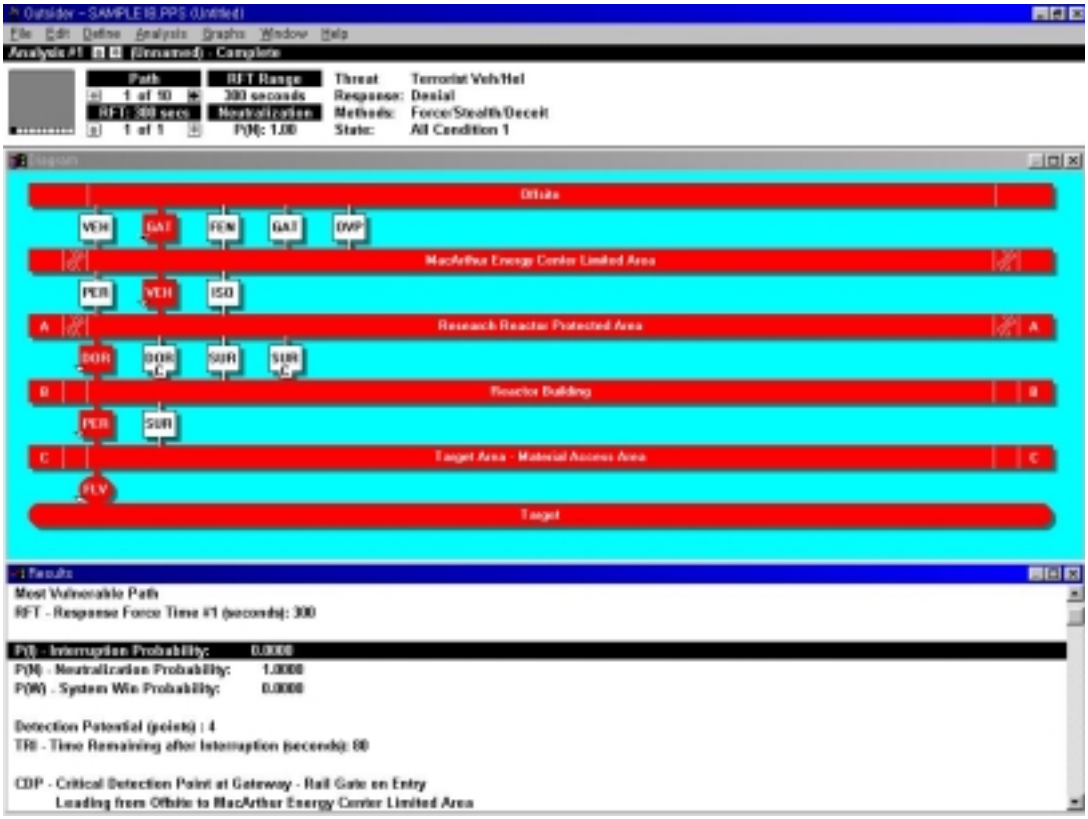

그림 2. SAVI의 분석화면 예

SAVI는 PI, TRI등을 제시해주는 분석화면이외에 그래프 형태로 취약성(Vulnerability) 분석결과 및 민감도(Sensitivity) 분석결과를 보여주는 Graphs 기능이 있다. 취약성분석 그래프는 가장 취약한 10개의 침입경로에 대한 제지확률 PI와 TRI를 보여주며 민감도분석 그래프는 RFT(Response Force Time)이 변화하는 경우 특정 침입경로에 대한 PI를 보여준다. 민감도분석은 따라서 대응인력의 소요시간을 단축하는 경우 방호시스템이 어떻게 개선되는 지를 제시해준다.

3. KAVI

한국원자력연구소에서 개발한 유효성평가 소프트웨어 프로그램인 KAVI의 개발요건은 다음과 같다.

◦ 국내 원전의 방호시스템 실정에 맞고, 사용하기 편하게 개발
◦ 원전 시설에 대한 데이터 입력 가능
◦ 국내 방호시설을 용이하게 반영할 수 있는 구조로 입력모듈 개발 (네트웍 구조)
◦ 입력데이터의 완전성 및 일관성 유지
◦ GUI 방식 채택
◦ 성능데이터 활용 가능
◦ DB 작성 및 활용 가능
◦ 효과적 탐색 및 수정방법 지원
◦ 기존의 평가척도 (PI, TRI, CDP 등) 포함
◦ 민감도 분석, 취약성 분석기능 제공

가. 방호설비 성능데이터

KAVI는 SAVI와 달리 하나의 실행파일로 시설데이터입력 및 유효성분석을 수행할 수 있다. KAVI의 실행중 방호설비의 성능데이터를 조회하기 위해 데이터베이스 파일에 접근하도록 되어 있다. 이 데이터파일은 Berkely DB를 이용하여 작성되었으며, 11종류의 침입세력의 능력에 대한 77개의 방호설비의 성능데이터를 포함하고 있다[3].

나. 사용방법

(1) 네트워크 기반 ASD의 작성

KAVI에서는 ASD를 네트워크 형태로 구성함으로써 침투세력의 침투 경로 표현에 대한 유연성(flexibility)을 높였으며, ASD작성의 편의성도 개선하였다. 네트워크로 표현하는 경우 불합리한 경로의 생성을 막을 수 있는 장점이 있다. SAVI의 경우 10개의 취약경로를 생성해 주는데 이중 몇 개가 불합리한 경로로 판단되는 경우가 종종있었다. 이런 경우 10개의 경로만 보여주는 SAVI로서는 활용상의 불편이 따르는데, KAVI는 이러한 문제점을 설비입력과정에서 네트워크 모델링을 사용함으로써 제거할 수 있다.

1) 방호설비 입력

메뉴바에서 '방호설비-입력하고자 하는 방호설비'를 선택한 후에, 방호설비를 입력하고자 하는 다이어그램 영역의 위치에서 마우스 왼쪽 버튼을 누르면 선택된 방호설비를 다이어그램 영역에 입력할 수 있다. 또는, 툴바에서 원하는 방호설비를 선택후 입력하고자 하는 위치에서 마우스 왼쪽 버튼을 누르면 입력할 수 있다. 그림 3은 방호설비의 입력이

끝난 화면으로서, 침투세력이 좌측에서 우측으로 침투한다는 가정하에 가장 좌측에는 시설외부가 입력되었고, 가장 우측에는 목표물이 입력되어 있다.

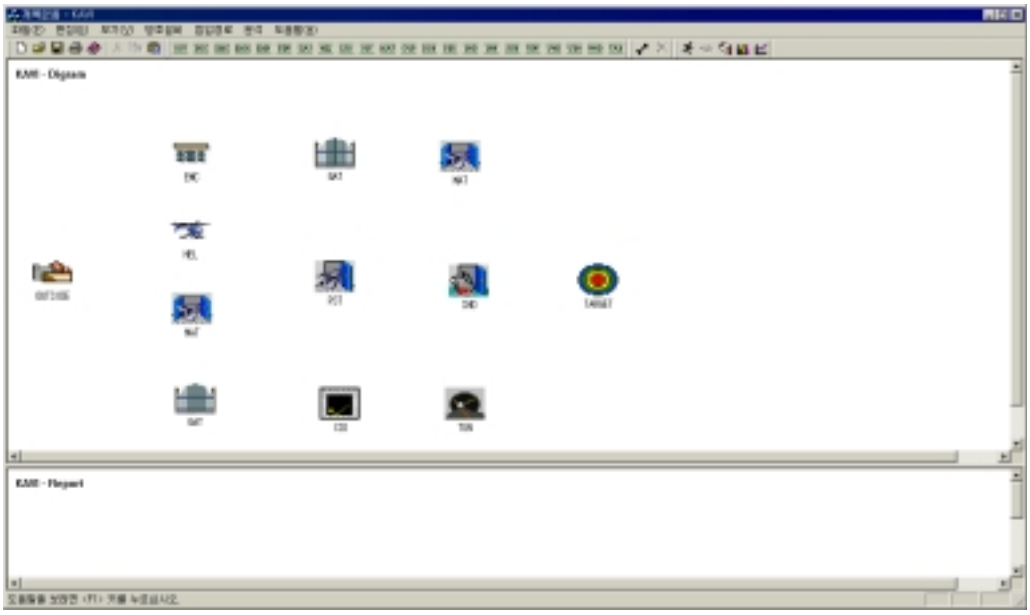

그림 3. 방호설비의 입력을 완성한 화면

KAVI에서의 ASD 작성을 위하여 각각의 방호설비들은 아이콘으로 표시되는데, ASD에서 표시되는 아이콘은 각각의 방호설비가 갖고 있는 의미를 컨셉으로 본 연구에서 새롭게 디자인되었다.

2) 침입경로의 정의

KAVI에서 ASD의 작성을 완성하기 위해서는 방호시설을 입력한 후에, 침입세력의 침입경로를 지정하여야 한다. 침입경로의 지정은 메뉴바에서 '침입경로-침입경로 추가'의 메뉴항목을 선택한 후에 연결을 원하는 두 개의 방호설비를 차례로 선택하면 된다. 또는 툴바에서 침입경로 추가에 해당하는 버튼을 누른 후에 동일한 방법에 의하여 임입경로를 지정할 수 있다. 침입경로의 설정을 위하여 '침입경로 추가' 메뉴항목을 선택한 후에, 경로의 시작점에 해당하는 방호설비를 선택하면 해당 설비와 마우스 포인터 사이에 녹색의 선이 그어지는데, 그때 포인터를 경로의 종착점에 해당하는 방호설비에 놓고 왼쪽 버튼을 클릭하면 두 개의 방호설비 사이에 경로가 설정된다.

3) 방호설비의 속성입력

방호설비에 대한 입력 및 경로가 완성된 후, 사용자는 각각의 방호설비에 대한 속성을 입력하여야 한다. 방호설비에 대한 속성 입력이 이루어지지 않은 상태에서는, 각각의 방

호설비의 속성이 하나도 지정되지 않은 상태로, 단지 해당 방호설비가 ASD상에 존재한다는 것만이 정의된 상태이며, 어떠한 특성 또는 방호능력을 가진 설비인지에 대해서는 하나도 정의되지 않은 상태이다.

방호설비의 속성 입력은 해당 방호설비를 더블클릭하여 생성되는 윈도우를 통해 수행할 수 있다. 속성의 입력내용은 일반사항, 시설외부, 시설중앙, 시설내부로 구성되어 있으며, 일반사항에서는 해당 방호설비에 대한 명칭과 위치정보, 기타사항들을 입력된다. 그리고, 시설외부, 시설중앙, 시설내부에서는 해당 방호설비에 대한 각종 사양을 입력할 수 있다. 그림 4는 시설외부에 해당하는 속성입력 윈도우를 나타낸 것이다. 시설에 대한 속성을 결정하는데 있어, 기본적으로 각 속성의 값은 데이터베이스에 입력된 값이 활용되지만 특정한 속성의 값이 바뀌어야 한다면 사용자 입력 버튼을 누르고 해당 속성의 값을 변경할 수 있다. 그림 5는 방호설비의 입력과 경로설정, 그리고 속성의 입력이 완성된 ASD를 나타낸 것이다.

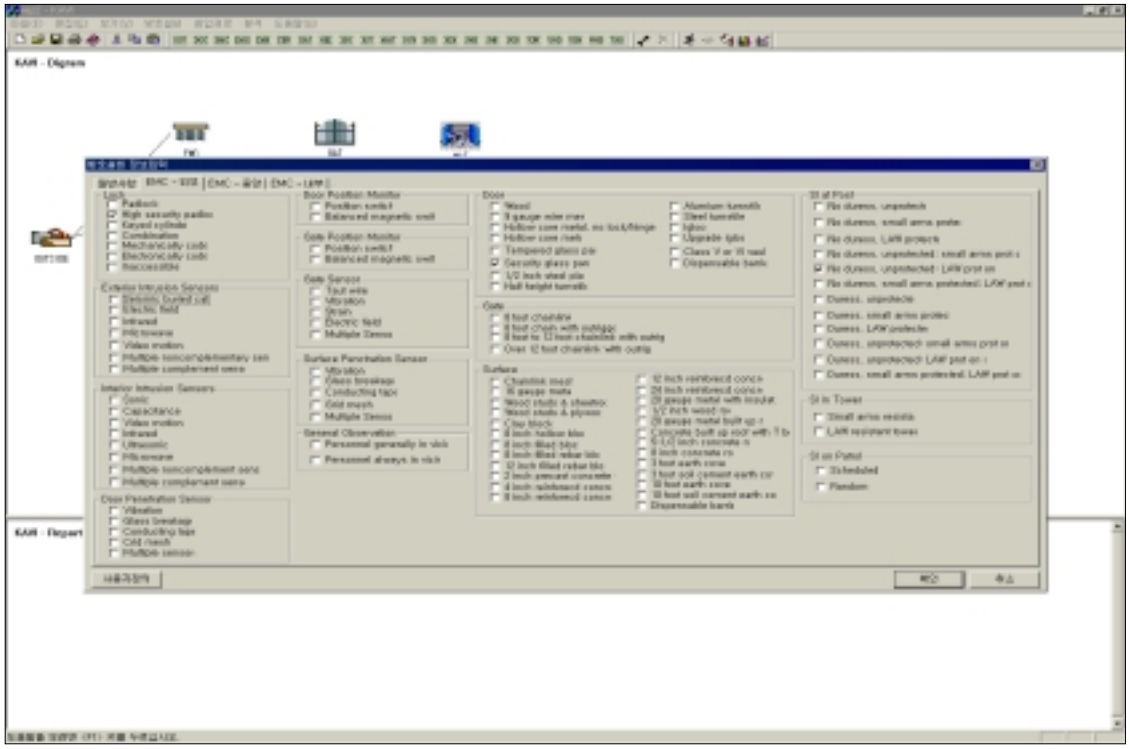

그림 4. EMC의 시설외부 속성 입력 윈도우

(2) 분석하기

ASD의 작성이 끝났으면, 침입세력의 침입에 대한 방호시스템의 유효성을 평가할 수 있다. 방호시스템의 유효성을 분석하기 위하여 메뉴바에서 '분석-분석하기' 메뉴항목을 선택하거나 툴바에서 분석하기에 해당하는 버튼을 누르면 된다. 그러면 그림 6과 같은 분

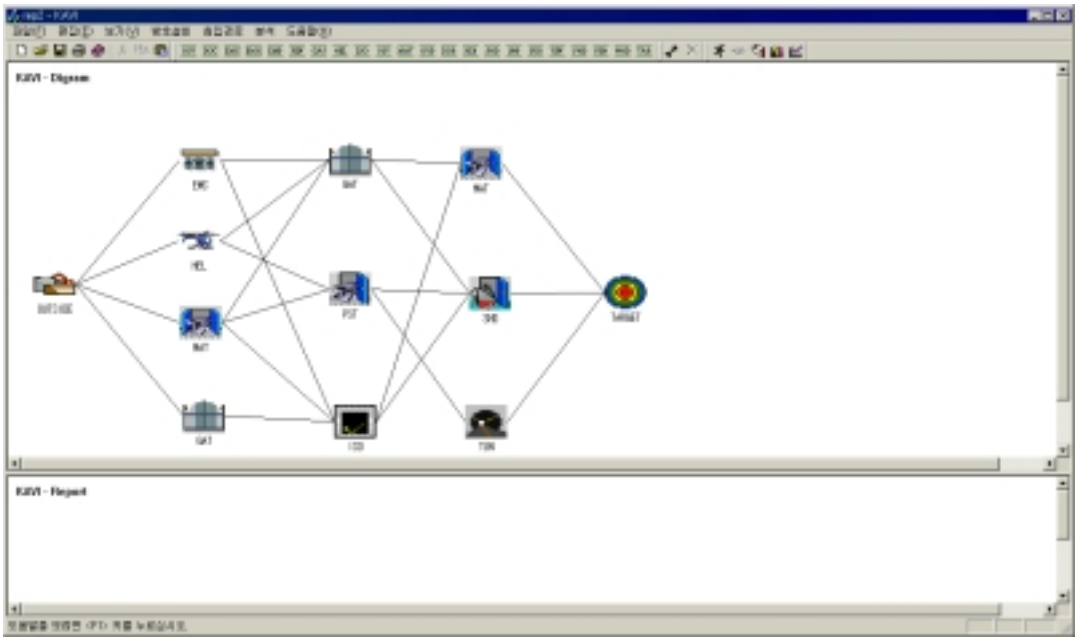

그림 5. 완성된 ASD

석창이 뜨게 되는데, 여기에서 분석에 필요한 각종 조건들을 선택한 후 윈도우의 아랫부분에 있는 '분석하기'버튼을 누르면 된다.

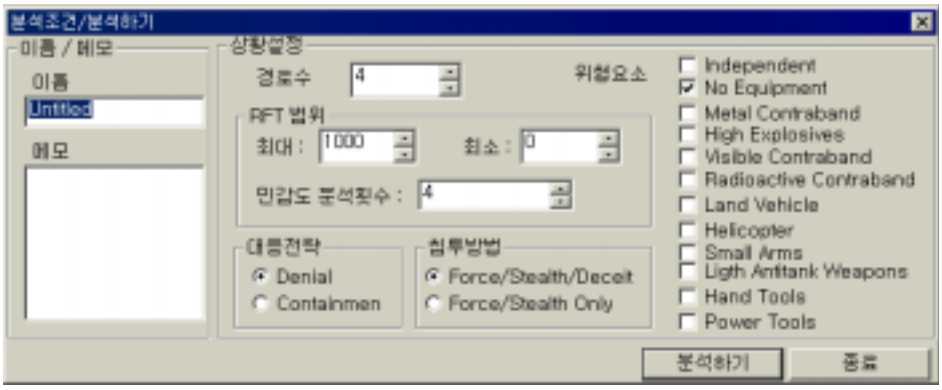

그림 6. 분석 윈도우

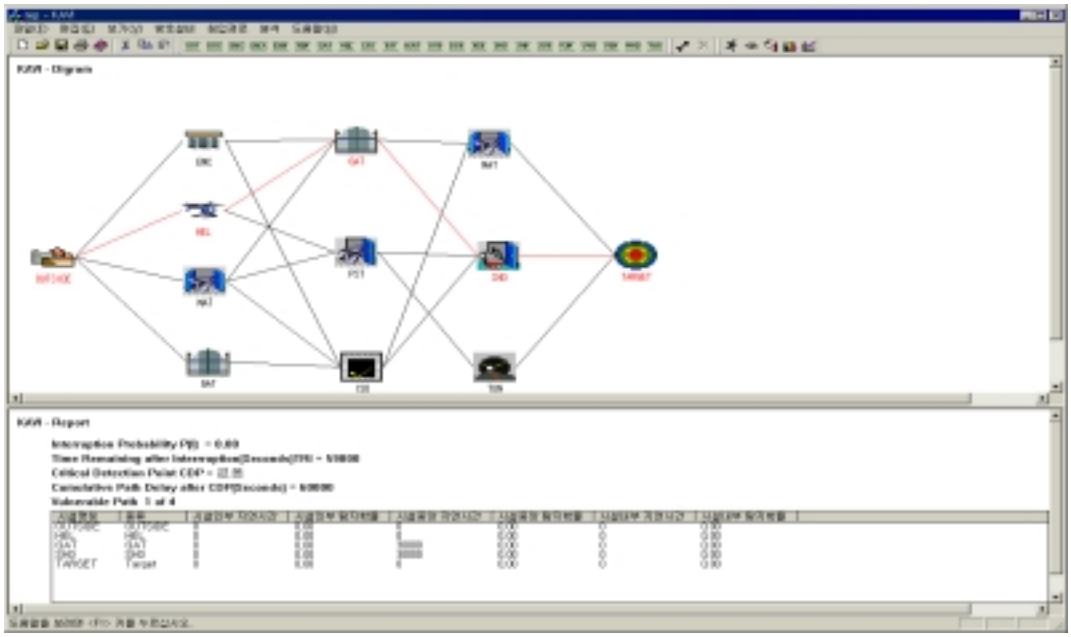

그림 7. 분석이 수행된 화면

분석을 위한 윈도우에서는 위협요소, 대응전략, 침투방법, 그리고 분석을 위한 각종 상황 설정이 정의되어야 한다. 그러한 조건들이 정의된 후, 분석을 수행하면 그림 7과 같은 결과를 얻을 수 있다. 여기에서, 침입세력이 침투하는데 가장 취약한 경로는 각각의 방호설비가 빨간색으로 표시된 경로이다.

(3) 민감도 분석

KAVI에서는 RFT(Response Force Time)의 변화에 따른 방호시스템의 유효성을 평가할 수 있는 민감도 분석(Sensitivity Analysis) 기능이 제공된다. 민감도 분석을 위해서는 분석 윈도우에서 RFT의 최대값과 최소값, 그리고 분석간격을 지정하여야 한다. 각각의 값이 지정되면, KAVI에서는 RFT의 최대값과 최소값사이를 지정된 분석간격수만큼 RFT 값의 변화에 따라 민감도 분석을 수행하게 된다.

(4) 결과보기

분석결과에 대한 텍스트 형태의 분석결과와 그래프 형태에 대한 분석결과를 선택하여 볼 수 있다. 물론, 분석을 수행하면 보고서 영역에는 기본적으로 텍스트 형태의 분석결과가 제시되지만 '분석-그래프-민감도 그래프' 또는 '분석-그래프-취약성 그래프'를 선택하면 해당 결과에 대한 그래프 형태의 결과를 보고서 영역에서 볼 수 있다. 그림 8은 예제로 분석된 한가지 방호시스템에 대한 분석결과를 취약성 그래프로 표시한 결과이다. 그리고, 그림 9는 RFT(Response Force Time) 값에 따른 민감도 분석 결과를 그래프로 나타낸 것이다.

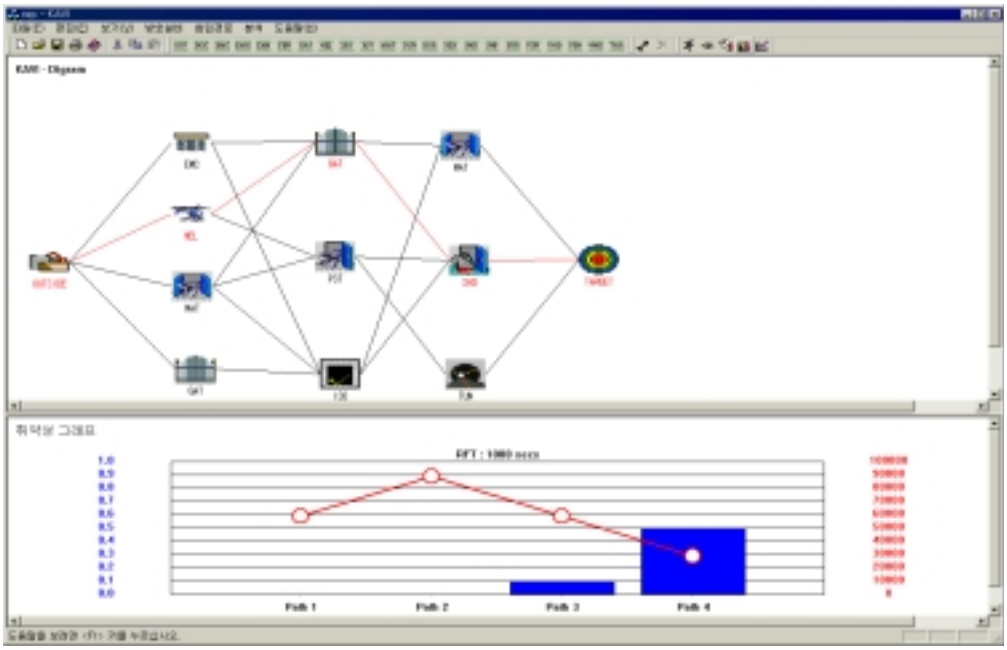

그림 8. 취약성 그래프로 표시된 분석결과

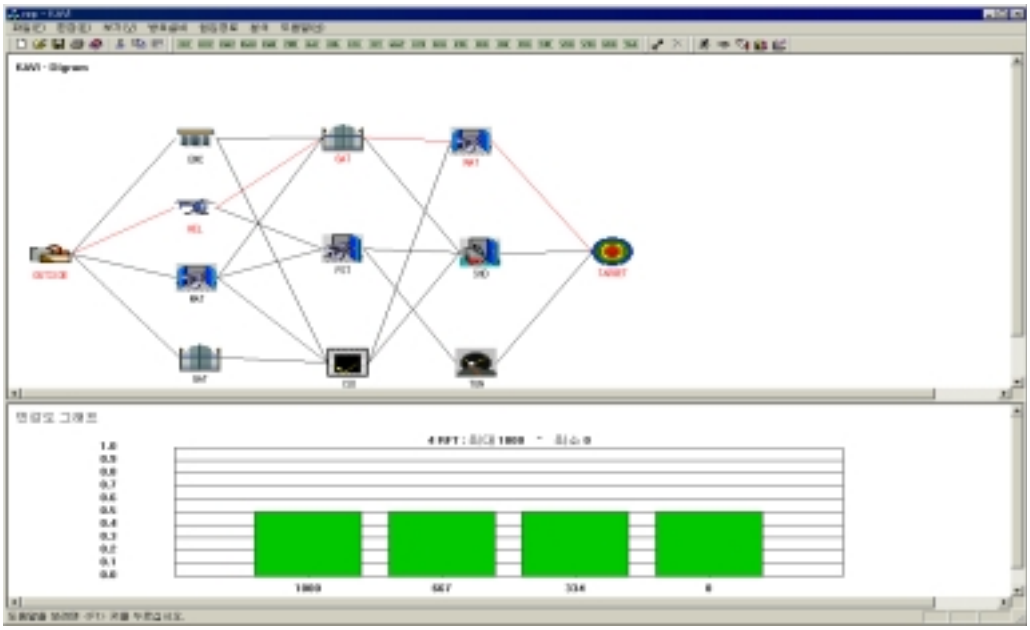

그림 9. 민감도 그래프로 표시된 분석결과

4. 결 론

핵물질 사용 및 보관시설에 대한 핵 테러 행위의 방지를 위해 IAEA는 물리적방호협약

(IAEA-INFCIRC 274)[5]을 강화하고 있으며, 국내에서도 핵시설의 물리적방호에 대한 관심이 미국의 9.11테러이후 고조되었다. 개발된 물리적방호시스템의 취약성분석 소프트웨어인 KAVI는 방호시스템의 객관적인 성능을 평가하는데 활용할 수 있는데, 국내 모든 원자력시설 뿐만아니라, 고도의 방호능력이 요구되는 국가시설 및 산업체에서도 활용할 수 있다.

5. 참고문헌

[1] 원자력 검사과, 핵물질 물리적방호(번역서), 1991.

[2] 물리적 방호시스템의 설계 및 유효성 평가, KAERI/TR-1848/2001, 2001.

[3] SNL, Physical Protection System Design, Workshop Material on Physical Protection System Design Methodology, SNL, 1996.

[4] 한국원자력연구소, 물리적 방호시스템의 평가에 사용되는 취약성 분석 소프트웨어 개발을 위한 해외 출장 귀국 보고서, KAERI/OT-541/2000, 2000.

[5] IAEA, The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, May 1980 .