

## 물리적 방호시스템 평가용 전산 프로그램의 개발현황

### The developing status of software for evaluation of physical protection system

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

#### 요약문

원자력시설의 물리적 방호시스템은 핵물질의 탈취나 사보타주를 비롯한 불법행위를 사전에 방지하고 유사시 최대한 방호할 수 있는 체계로 설계되고 구축되어야 한다. 이런 관점에서, 원자력 시설에서의 물리적 방호시스템은 내·외부 위협 행위에 대한 정량적인 평가가 선행되어야 하며, 미국을 비롯한 몇몇 국가에서 유효성 평가용 소프트웨어를 개발해 왔다. 본 연구에서 개발하고 있는 KAVI 프로그램은 EASI, PIGSAM 및 SAVI에서 적용한 평가요소인 저지확률(PI), 최후방호설비(CDP), 그리고 저지후 남은시간(TRI)을 토대로 운용하는 체계를 갖고 있다. 동 프로그램이 향후 실제로 적용 가능한 프로그램으로서 실효성을 증대하기 위해서는 이와 관련된 Data 생산을 비롯한 방법론이 구체화되어야 한다.

#### Abstract

The ultimate objective of a physical protection system (PPS) is to prevent the accomplishment of unauthorized overt or covert actions. In this regard, when a physical protection system is incorporated into a nuclear facility, its objective is to prevent radiological sabotage and theft of nuclear materials used or stored at the facility. There has been increasing needs to evaluate quantitatively the performance of PPS designed for the nuclear facilities. Few countries as well as USA have been developing the software for evaluation of PPS effectiveness. The evaluating approach applied to KAVI which is used for EASI, PIGSAM,

and SAVI is the use of variables, that is, Probability of Interruption(PI), Critical Detection Point(CDP) and Time Remaining after Interruption(TRI). To apply to the nuclear facilities, KAVI have the needs to be improved through producing data from the nuclear sites.

### 1. 서론

하나의 시스템은 일반적으로 각종 구성요소나 설비 등으로 이루어 졌다. 이 시스템 은 하나의 목적을 가지고 서로 유기적인 역할 하게되는데 이때, 어떠한 불법적인 행위를 막기 위해 시스템이 설계되어 졌다면, 이를 물리적 방호시스템이라 할 수 있다. 물리적 방호시스템의 최종적인 목표는 잠재적인 혹은 직접적인 외부의 침입 으로부터 시설을 방호하는 것이다. 방호하는 시설이 원자력시설이라고 하면, 물리적 방호시스템의 최종목표는 시설 내에 있는 특정 핵물질의 탈취 및 시설 파괴에 의한 대량의 방사성 물질의 외부로의 방출을 막는 것이다.[1]

물리적 방호의 목적을 달성하는 최선의 방법은 불법행위의 발생을 미연에 방지하는 것이다. 불법행위의 발생을 미연에 방지하기 위한 방법에는 원자력 Public Acceptance, 광고활동 등이 있다. 그럼에도 불구하고, 원자력시설에 대한 어떠한 불법행위가 발생한 경우의 영향이 막대함을 고려한다면, 물리적 지연설비, 감시장치, 그리고 비상대응병력 등 물리적 수단이 강구되어야 한다. 물리적 방호 시스템의 기본원칙은 가능한한 최대로 침입자의 불법행위를 탐지하여 신속하게 대응하거나 그 목적 달성을 지연시키는데 있다. 즉, 물리적 방호 시스템의 주요기능은 지연(delay), 탐지(detect), 대응(response)이라 할 수 있다. 이를 그림 1에 도시하였다.

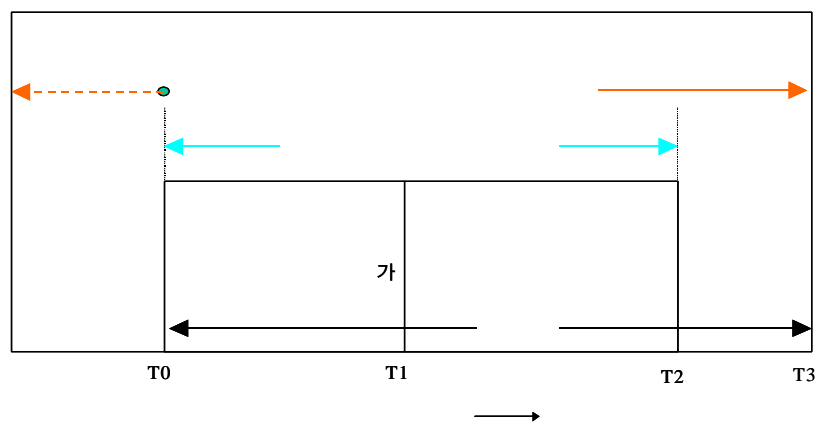


그림 1. 물리적방호시스템의 기본설계

물리적 방호 시스템의 평가는 시스템의 요구사항을 중심으로 시스템을 확인 방법과

각 기능요소들이 상호 유기적으로 연계되는 성능을 검증하는 방법이 있다. 일반적으로 원자력 시설의 방호시스템은 시스템의 요구사항이 시스템에 잘 적용되었는지를 확인하는 방법으로 평가되고 있다. 평가방법의 대표적인 예는 탐지, 지연, 대응의 방호기능을 담당하는 각 방호설비가 적절히 배치되도록 설계되었는지, 각 설비가 설계시 요구조건에 맞는지 그리고 적소에 배치되고 운용되고 있는지 등을 조사하는 것이다. 이러한 확인방법은 다양한 표준이나 지침을 기반으로 작성된 일련의 체크리스트를 활용하는 것이 보편적이다.

이러한 방호설비들이 실제 핵물질의 탈취나 핵시설의 파괴행위 등을 막아낼 수 있는지를 분석하는 것은 시스템의 요구사항에 따라 설치된 방호시스템이 탐지, 지연 및 대응이라는 기능을 발휘하는지를 검증하는 것이다.[2, 3]

물리적 방호시스템의 성능을 검증하기 위한 도구는 EASI, PIGSAM, SAVI, ASSESS, Turbo EVA, Intrabuster 등이 있다. 이중 EASI와 SAVI는 미국의 Sandia National Lab.에서 개발한 대표적인 소프트웨어 프로그램이며 PIGSAM은 EASI를 기반으로 한국원자력연구소에서 개발하였다. Turbo EVA는 EASI 기반으로 French Atomic Energy Commision (CEA)에서 개발하였고, Intrabuster는 아르헨티나에서 개발되어졌다.

침입세력은 시설내로 통하는 어떠한 경로로 움직여서 경로상에 설치된 방호설비들을 파괴시킴으로써 그들의 목표를 달성할 것이다. 따라서 앞서 언급한 대부분의 소프트웨어들은 경로분석을 하기 위한 ASD(Adversary Sequence Diagram: 침입자 사용할 수 있는 여러 가지 경로를 설명하는 일종의 그래프)를 사용하여 시설의 물리적 방호 시스템을 평가하는 것이다.[4]

## 2. 유효성 평가 소프트웨어[5, 6]

### 가. 침입세력 및 침입경로

침입세력은 설계기준위협(Design Basis Threat)에 의해 결정된다. 설계기준위협이란 원자력시설을 포함한 국가 중요시설에 설치된 물리적 방호시스템에 가해질 수 있는 잠재적인 위협이다. 예로, 테러리스트, 범죄조직, 정신병자, 그리고 외국 스파이 등이 해당될 수 있다. 설계기준위협은 시간적, 공간적으로 변화할 수 있고 변화하는 DBT에 따라 물리적 방호시스템의 유효성평가가 주기적으로 반복적으로 이뤄져야 한다. 침입세력의 능력은 침입세력의 구성인원, 무장상태, 훈련정도 등에 의해 결정되고 잘 훈련된 인원이 많은 경우 침입세력의 능력은 높을 것이며 반면에 훈련이 덜 된 적은 인원일 경우는 침입세력의 능력이 낮을 것이다. 또한, 강력한 도구, 예를 들면 중화기와 다양하고 강력한 폭발물로 무장한 침입세력은 소화기로 무장한 침입세력보다 침입능력이 우월하다고 할 수 있을 것이다. 침입세력의 능력을 결정

짓는 또 다른 요소는 전술이다. 전술이란 침입대상이 되는 목표물을 사전에 인지하고 침입경로 등을 치밀하게 계획하여 경비 및 방호시설을 속이거나 은밀하게 침입하는 것과 월등한 화력을 사용하여 방호세력을 무력화시키는 것을 말한다. 마지막으로 침입세력의 능력을 결정짓는 요소로 지원세력의 유무이다. 침입대상물 혹은 시설의 종사자 이외의 인원으로 구성된 침입세력이 보다 침입대상 시설 내의 종사자 혹은 내부 공모자의 도움을 받는 침입세력이 보다 높은 침입능력을 발휘할 수 있을 것이다.

침입경로는 침입세력이 방호시스템의 외부로부터 침입을 시도하여 침입목적물 달성하기까지 수행하여야 하는 활동을 순차적으로 표시한 것으로 정의된다. 일반적으로 침입경로의 시작점은 방호시스템의 외부로부터 정의되며 종료점은 목표물의 성공적인 탈취나 파괴공작으로 결정된다. 특정의 침입능력을 가진 침입세력이 목적을 달성하는 방법은 다양할 것이므로 한 침입세력에 대해 다수의 침입경로가 존재한다. 침입세력은 다수의 침입 경로 중 침입세력의 목적을 달성하는데 최소한의 시간이 소요되는 하나의 경로를 선택하게 될 것이다.

#### 나. 물리적 방호시스템의 유효성

물리적 방호 시스템의 성능을 검증하는 것은 명확히 규정할 수 있는 측정 및 판단 기준이 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. 대부분의 물리적 방호 시스템의 평가에 활용된 종속변수는 저지확률인 Probability of Interruption(PI), Critical Detection Point(CDP) 그리고 Time Remaining after Interruption(TRI) 등이다. 물리적 방호 시스템의 유효성이란 바로 이러한 성능 측정치들과 판단기준에 의해 결정된다. 판단기준은 기본적으로 위험분석을 토대로 결정된다. 위험분석은 가중치와 피해를 주요인자로 하는 단순한 연산으로 수행될 수 있는데, 일반적으로 가중치와 피해의 정량화에는 전문가의 판단이 개입된다. 판단기준을 만족하는 성능 측정치를 얻은 경우에 그 방호 시스템은 유효하다고 할 수 있다.

#### 다. 종속변수

물리적방호시스템의 유효성을 평가하는데 사용되는 종속변수로서, CDP, PI, TRI 등이 있다. 이런 변수는 현재 EASI, PIGSAM, SAVI, KAVI에 적용되어 사용되고 있다.

##### 1) 최후 방호설비(Critical Detection Point : CDP)

CDP는 침입세력의 침입을 저지하기 위하여 침입사실을 감지해야 하는 최후의 지점을 말하는 것이고 대부분의 경우 침입감지 센서가 장치된 방호설비를 말한다. 즉, 침입세력을 저지하기 위해서는 적어도 CDP 이전의 방호설비에서 침입사실을 감지해야 한다. CDP는 침입세력이 방호시스템의 목표물까지 침입을 완료하는 걸리는 시간과 침입사실을 발견한 후의 대응팀의 대응시간을 근거로 계산된다. 침입세력이 침입을 완료할 수 있는 예상시간에서 대응팀이 침입세력의 침입을 감지하여 적당한 대응조치를 취하는데 걸리는 시간을 뺀 시점보다 앞에 있는, 침입세력의 침입을 감지할 수 있는 방호설비를 CDP라고 한다.

## 2) 저지확률 (Probability of Interruption : PI)

물리적방호 시스템의 유효성을 평가하기 위한 가장 기본적인 평가척도는 침입세력에 대한 저지확률 PI이다. PI는 침입세력이 침입을 완수하기 전에 침입에 대한 적절한 대응조치를 취할 확률로 정의된다. 침입을 감지하여 적절한 대응조치를 완수한 시점이 침입세력이 침입을 완수한 시점보다 빠르다면 침입을 제지한 결과가 된다.

침입경로가 outside, 설비1, 설비2, ....., CDP, ... target 이고  $P_i$ 가 설비 i에서의 침입을 감지할 확률이라면, 침입을 저지할 확률은 1에서 각 설비에서 감지못할 확률을 빼준 값이 된다.

$$P(I) = 1 - (1 - P_1)(1 - P_2) \dots (1 - P_{CDP})$$

## 3) 저지후 남은시간(Time Remaining after Interruption : TRI)

TRI는 CDP에 해당하는 방호설비에서 침입을 감지하였다고 가정하였을 때, 이론적으로 침입을 제지한 이후에 남아있는 시간을 말한다. CDP 이후의 누적 지연시간에 대응팀의 대응시간(Response Forece Time : RFT)을 뺀 값이 TRI 값이 된다.

$$TRI = CDP - RFT$$

## 3. Korean Analysis of Vulnerability to Intrusion, KAVI

KAVI는 미국 SNL(Sandia National Lab.)에서 개발한 SAVI (Systematic Analysis of Vulnerability to Intrusion)를 기초로 한국원자력연구소에서 개발한 원자력 시설의 물리적 방호 시스템의 유효성을 평가하는 소프트웨어이다.

### 가. Adversary Sequence Diagram, ASD

ASD는 시설의 물리적 방호시스템을 형상화시킨 일종의 그래프이다. KAVI에서의

ASD는 GUI(Graphic User Interface)를 사용하여 형상화되었다. ASD 작성에 앞서, 시설의 세부적인 현장상황에 대해 면밀한 분석이 이뤄져야 한다. ASD는 침입의 시작점인 시설외부와 침입세력이 통과해야되는 방호시설, 그리고 최종 목표물로 구성 되어있고 각 지점을 연결하는 물리적인 경로로 이루어져 있다. 외부의 적이 왼쪽에서 오른쪽으로 침투하는 것으로 가정하여 시작점인 시설외부(outside)는 화면의 왼쪽에 위치하고 목표물인 target은 화면의 오른쪽에 배치하였다.

### 1) 방호설비

물리적 경로를 지정해주기 앞서, 각 영역별로 방호설비를 설정해주어야 한다. 방호설비는 사용자가 이해하기 쉬운 아이콘으로 형상화하였다. 표 1에서 몇가지 예를 설명하였다. KAVI에서 아이콘으로 형상화된 방호설비들은 대부분 SAVI에서 사용된 설비들을 기초로 개발하였다. 각 방호설비는 설비의 외부영역, 내부영역, 중간영역등 세 영역에 각종 센서 등을 설치하는 것으로 가정하였다. 예를 들어, 방호설비가 철조망일 경우는 2중으로 된 철조망을 생각할 수 있고, 각 영역별로 센서를 설

표 1. KAVI의 아이콘 디자인의 예

방호설비	의미	디자인(아이콘)
outside	원자력발전소 외부모양을 표현, 침투의 시작점	
Emergency Evacuation Corral	비상시에 위험을 막아주는 개념을 표현	
Fence Line	철조망 형태의 모양을 형상화	
Emergency Portal	비상시에 나가는 큰 문의 모양을 형상화	
Gateway	큰 아치형 문을 형상화	
Vehicle Portal	차량과 큰 문의 모양 표현	
Surface	벽돌 벽의 이미지로 표현	
Target	표적의 모양을 표현	

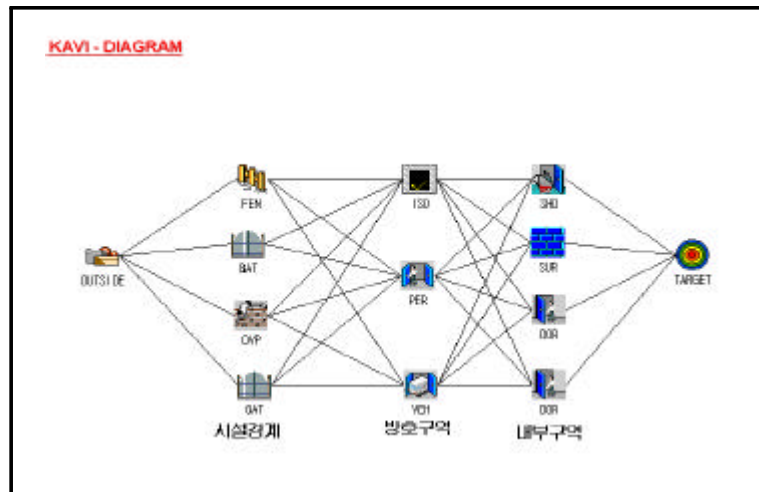


그림 2. KAVI의 ASD의 예

치할 수 있게 되어있다.

## 2) 침입경로

하나의 시설에서 모든 방호설비가 정의되어졌다면, 외부의 적이 침투 가능한 물리적인 경로를 추가하여야 한다. KAVI는 여러 가지 침투 가능한 경로 중 하나의 경로를 통해서 침투하는 과정에 대해 분석할 수 있게 되어있다. 즉, 침입자는 한번에 하나의 경로만을 사용하는 것을 원칙으로 하고 있다. 사용자가 현장분석을 바탕으로 모든 가능한 침투경로를 직접 설정해 주므로써, KAVI 물리적으로 의미있는 경로에 대해서만 분석한다. 거리가 서로 다른 침투경로들은 예상되는 소요시간으로 정의하여 서로 다른 의미를 가지게 하였다. 외부의 적이 정문에서 정문, 정문에서 후문으로 침투할 때 실제로 서로 다른 시간이 소요되기 때문이다. 그림 2는 KAVI의 ASD의 예를 보여주고 있고 침투경로는 왼쪽에서 오른쪽이고 시설경계, 방호구역, 그리고 내부구역 그리고 목표물 순서로 설정되었다.

## 나. 분석

KAVI는 취약성 분석과 민감도 분석을 통해 모형화된 시설의 물리적 방호시스템의 유효성을 평가한다. 분석하기 앞서 침투할 적의 위협수준을 정의해주어 한다. KAVI는 외부의 적을 12가지로 분류하고 있다. 예로, 위협기준을 Land Vehicle로 설정하고, 취약경로수는 10개로 설정하고 RFT를 정의한다. 즉, 위협요소는 차량침입, Response Force Time은 최대 10분에서 최소 5분으로 설정한다. 또한, 침입세력은 감지센서를 최대한 피하면서 필요한 경우에만 방호설비를 파괴하는 방법으로 침투하고 대응 전략인 적을 감지 및 확인이 끝나면 적을 직접적으로 저지한다고 설정

한다. 이러한 설정화면은 그림 3에서 확인할 수 있다.

표 2. KAVI의 위협기준

위협(외부의 적)	
Independent	Land Vehicle
No equipment	Helicopter
Metal Contraband	Small Arms
High Explosive	Light Antitank weapons
Vehicle Contraband	Hand Tools
Radioactive Contraband	Power Tools

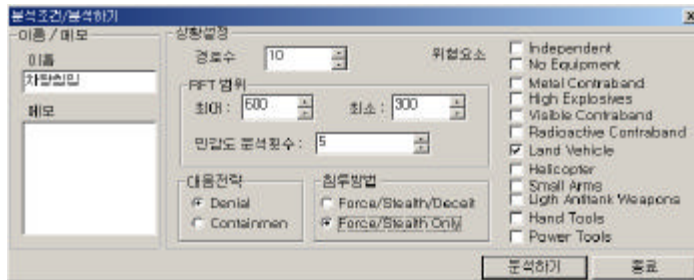


그림 3. 분석조건/분석하기 설정 예

### 1) 취약성 분석

취약성 분석은 침입세력의 침입경로에 대해 가장 취약한 경로의 순서로 방호시스템을 분석하는 방법을 말한다. 분석조건이 입력에서 경로의 수를 지정하면 지정된 경로의 수만큼 가장 취약한 경로에서부터 분석이 수행된다. 우선, 분석결과를 보고서 형태로 보여주고 예로 설정된 10개의 경로에 대해서 가장 취약한 순서대로 그래프로 보여준다. 그림 4는 10개 경로중 가장 취약한 침입경로에 대한 보고서이다. 침입경로는 outside에서 시설경계구역의 Fence를 지나서 방호구역인 ISO(isolation zone : 침입감지센서가 설치되어 있는 통제구역)를 통과하여 내부구역의 SHD(발전소의 Shipping/Receiving area)를 지나 목표지점까지 침투하는 경로이다. 보고서에 따르면, 방호구역인 ISO에서 침입 감지된 이후의 지연시간이 190sec로 이다. 최종적으로 침입자가 목적 달성하는 데 걸리는 시간을 190sec라 할 수 있고 출동 대응시간은 이보다 빨라야 한다. 분석조건이 최소 출동시간이 300sec이므로 가장 취약한 경로라 할 수 있다.



**KAVI-REPORT**

Interruption Possibility (PI) = 0.00  
 Time Remaining after Interruption(Seconds) TRI = 0  
 Critical Detection Point CDP = 0.00  
 Cumulative Path Delay after CDP(Seconds) = 0  
 Vulnerable Path [ 1 of 10 ]

시퀀스번호	종류	시퀀스번호	시퀀스번호	시퀀스번호	시퀀스번호	시퀀스번호	시퀀스번호	시퀀스번호	시퀀스번호
OUTSIDE	OUTSIDE	0	0.00	0	0.00	0	0.00	0	0.00
FEA	FEA	0	0.00	10	0.00	0	0.00	0	0.00
ISO	ISO	0	0.00	0	1.00	10	0.00	0	0.00
SHD	SHD	0	0.00	0	0.00	0	0.00	0	0.00
TARGET	Target	0	0.00	0	0.00	0	0.00	0	0.00

그림 4. KAVI Report

2) 민감도 분석

KAVI는 대응군의 출동 및 저지가능한 시간을 최대 값과 최소 값으로 설정하여, 값의 변화에 따른 방호시스템의 유효성을 평가할 수 있다. 이 때, 시간에 따른 분석을 민감도 분석이라 정의한다. 민감도 분석은 최대 10 구간으로 나누어 할 수 있다. 그림 5는 전체 10개 경로중 5번째 취약경로에 대한 민감도 분석 그래프이다. 최대 대응시간 10분에서 최소 대응시간 5분 사이에 대응시간 변화에 따라 PI의 변화율을 나타낸다. 그림에서 보듯이 출동병력이 최대 525sec 내에 대응을 해야 적의 침입을 저지 할 수 있다.

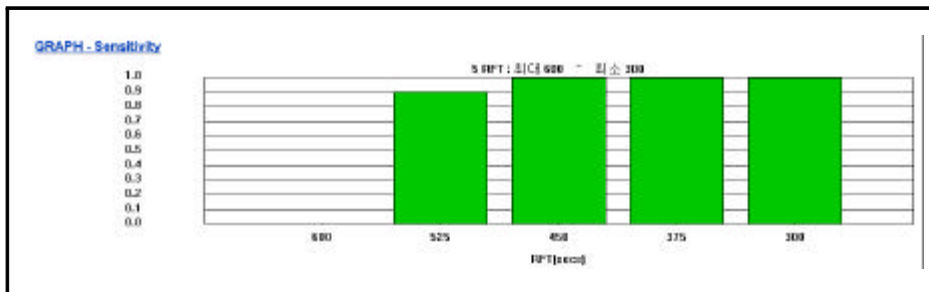


그림 5. 민감도 그래프

5. 결론 및 향후방향

핵물질의 사용 및 보관시설에 대한 핵 테러 행위의 방지를 위해 국제원자력기구인 IAEA는 국제 물리적 방호협약을 강화하고 있으며, 미국의 9.11테러 이후 국내에서도 핵시설의 물리적방호에 대한 관심이 고조되고 있다.[7] 이러한 시점에서 국내 국가 중요시설의 물리적방호 시스템을 정량적으로 평가할 수 있는 소프트웨어 개발의 필요성이 제기되었다. KAVI는 미국 SNL에서 개발한 EASI 및 SAVI에 사용되는 개념을 기초로 개발되었으며, KAVI의 Data Base도 SAVI의 것을 바탕으로 개발되어진 것이다.

KAVI프로그램이 실제 국내 중요시설의 물리적 방호 시스템 평가에 적용하기 위해

선 KAVI 프로그램의 검증이 필요하다. 우선, 국내 원자력 시설의 방호설비현황 및 지리적 여건을 파악 해야한다. SAVI Database에 있는 데이터 변수에서 국내시설에 맞는 데이터 변수를 설정한 후, 실험을 통한 데이터 생산을 하므로써 KAVI 프로그램의 검증방법을 찾아야 할 것이다.

## 6. 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] 물리적 방호 시스템의 유효성 평가 프로그램 개발, KAERI/CM-553/2001.
- [6] 이현철 외; 물리적 방호 시스템의 유효성 평가 프로그램 개발(Development of A Effectiveness Evaluation Program for Physical Protection System), 2002 한국원자력학회 춘계발표회, 2002. 5.
- [7] IAEA, The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, May 1980.