Evaluation of Physical Protection System Effectiveness in Nuclear Power Plant

ZOU Bowen EMAIL: zoubowen@scut.edu.cn

OKAYAMA UNIVERSITY

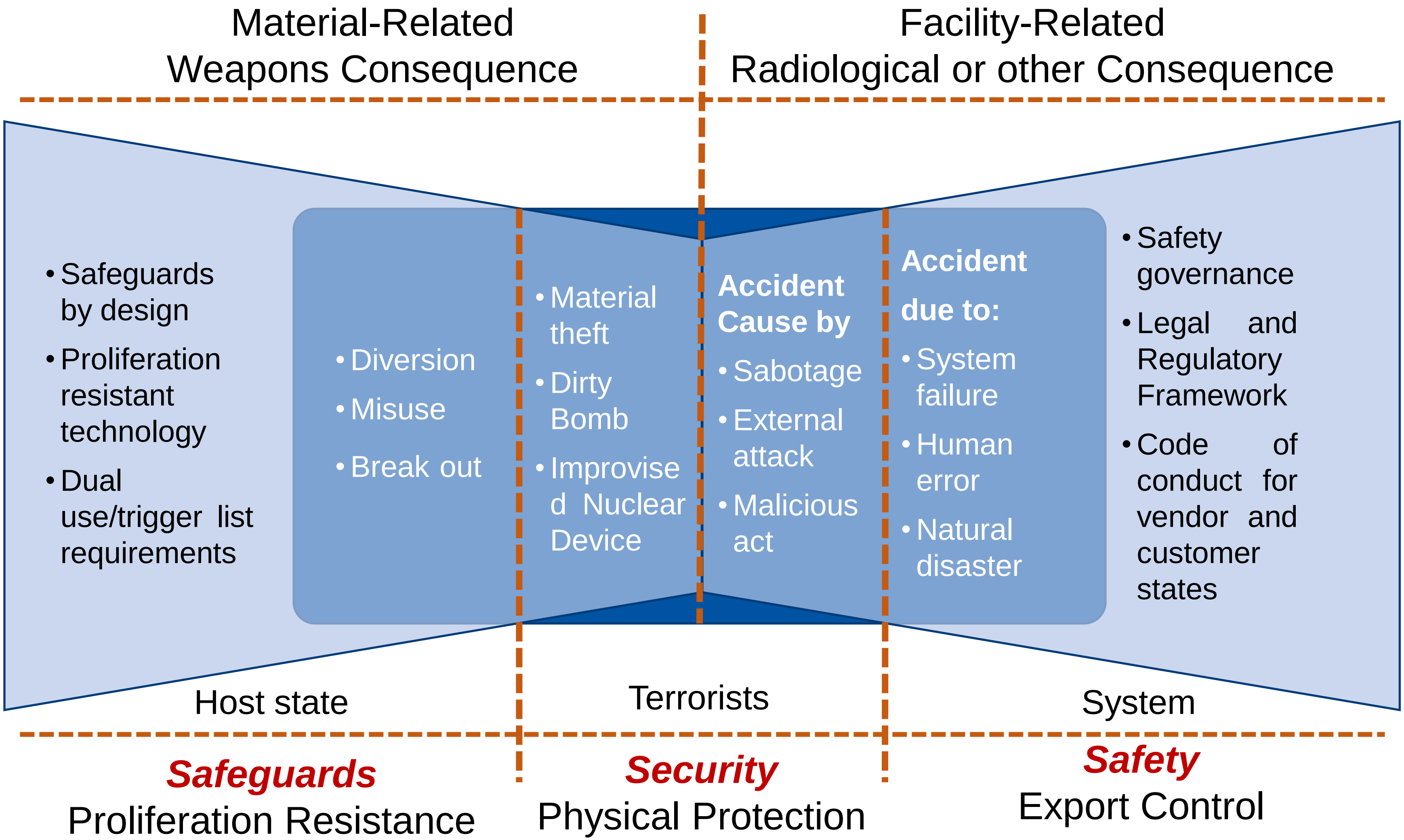
CONTENTS

PART ONE

Introduction

01 Introduction

1 Nuclear Security and NPPs Safety System

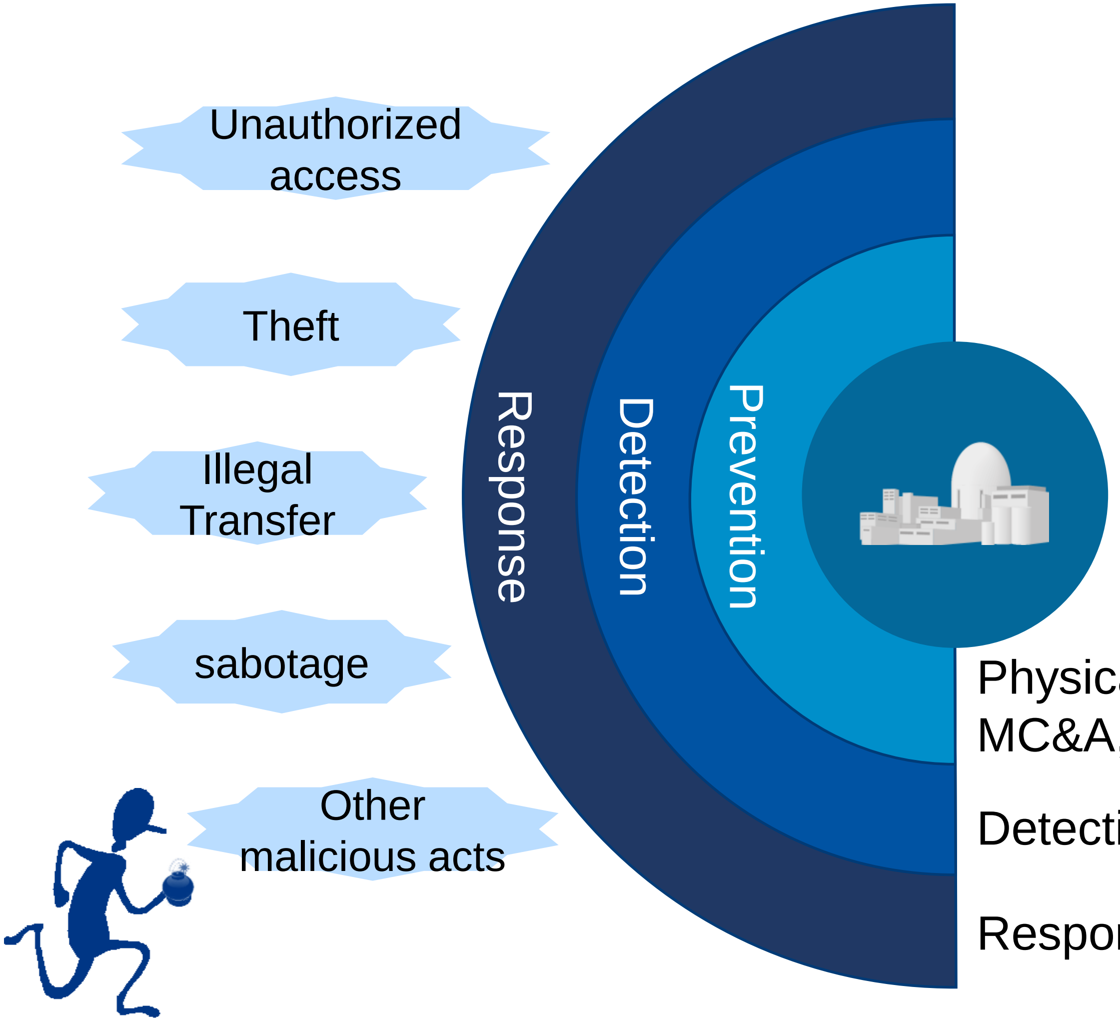


International Initiative on 3S-based Nuclear Energy Infrastructure was First Proposed in the G8 Summit 2008 at Chitose, Hokkaido, Japan.

01 Introduction

2 Physical Protection Systems

- A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks.



Physical Protection (RF, S&M), D&IT, MC&A, SSAC

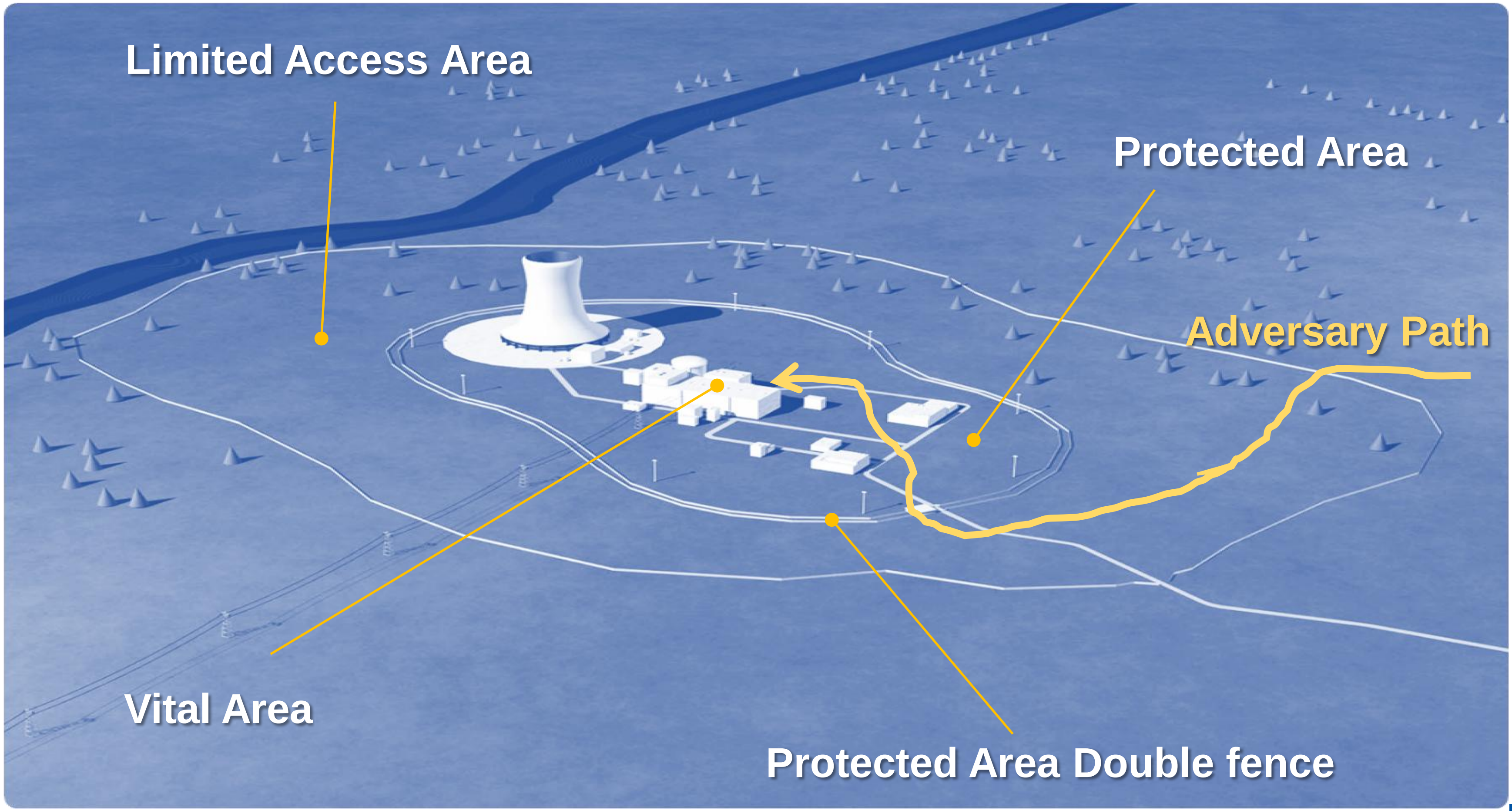
Detection at Borders, facilities, etc.

Response at facilities, borders, etc.

01 Introduction

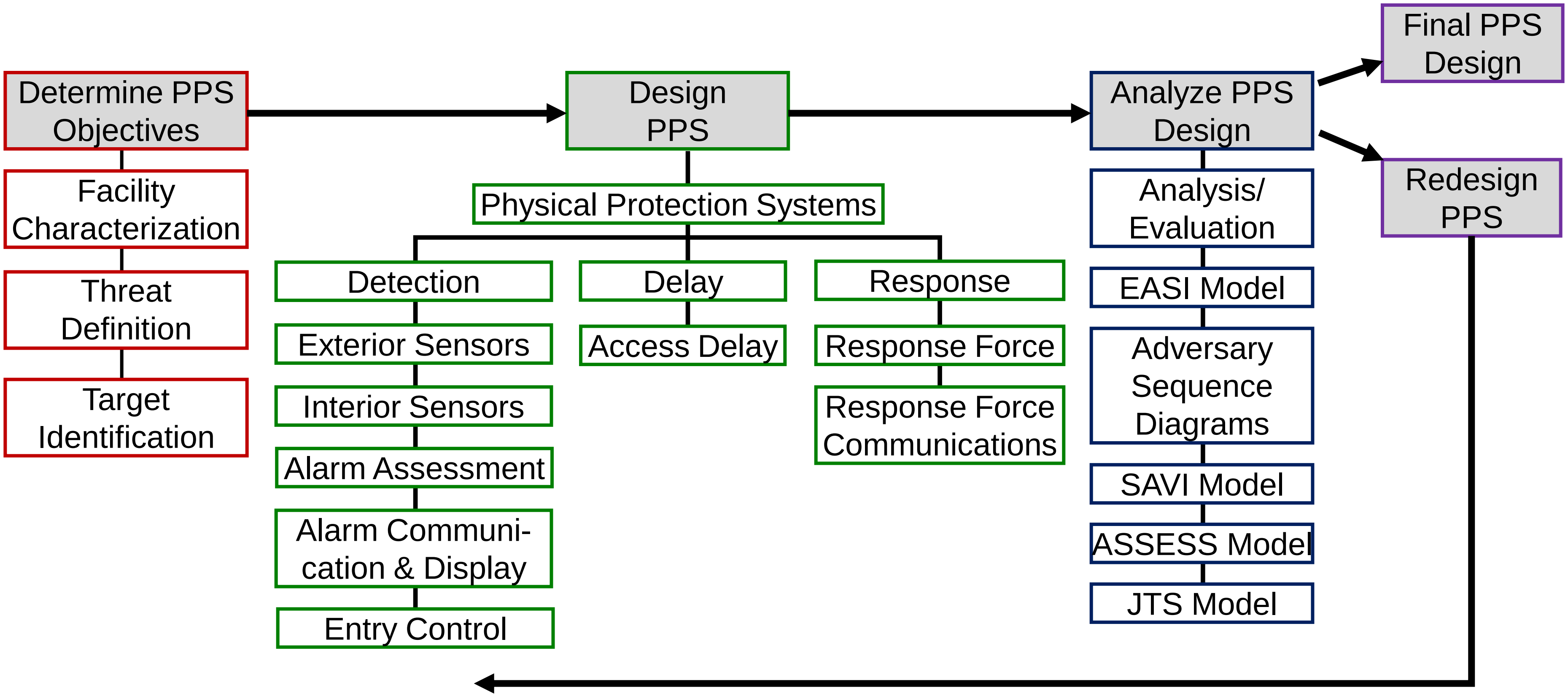
2 Physical Protection Systems

- A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks.



01 Introduction

3 Design and Evaluation Process for Physical Protection Systems



Design & Evaluation Process of a PPS

The process starts with determining objectives, then designing a system to meet the objectives, and ends with an evaluation of how well the system performs compared to the objectives

01 Introduction

4 Physical Protection Systems Policies

In the 1970S

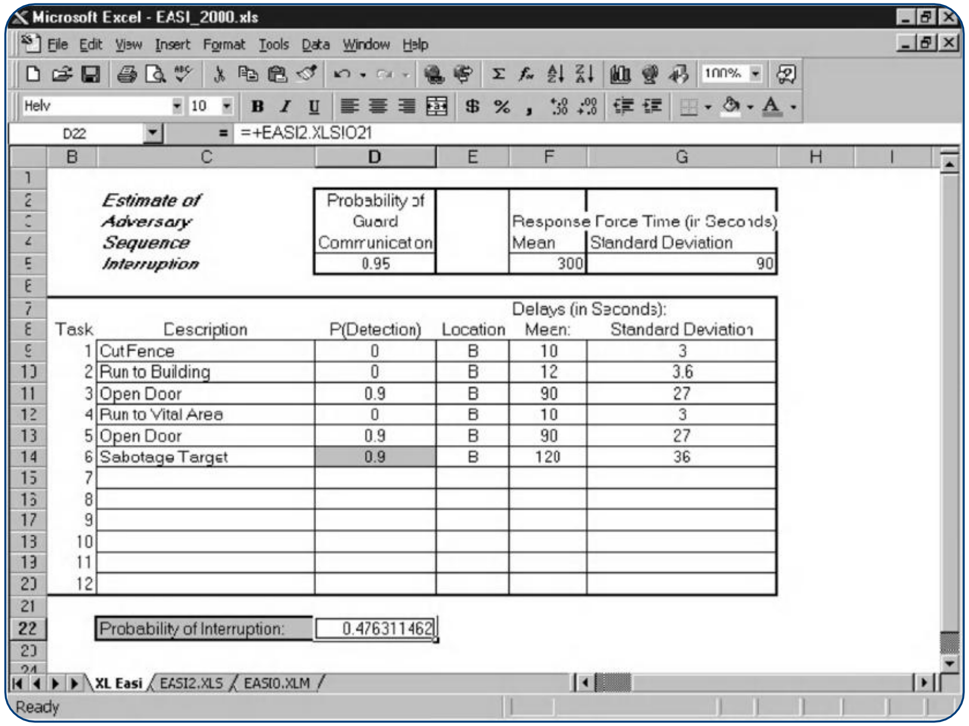
- First works in the area of the qualitative and quantitative evaluation of PPS effectiveness were completed in the ***Sandia National Laboratory*** (SNL).
- The development of PPS design and evaluation methodology called "***Design and Evaluation Process***" (DEPO), which is based on PPS one-dimensional models, is considered to be one of the most notable results of these activities.
- The SNL activities in this period resulted in introducing the frequently used method of PPS effectiveness evaluation called "***Estimate of Adversary Sequence Interruption***" (EASI).

01 Introduction

4 Physical Protection Systems Policies

In the 1980S

- SNL developed a method which evaluated PPS effectiveness by using an adversary sequence diagram called “***Systematic Analysis of Vulnerability to Intrusion***” (SAVI).
- SAVI enables users to analyze all possible paths of an attack to meet the objective, and evaluate the most vulnerable paths including the position of a critical detection point along each path.



Probability of Guard Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0.95		300	90

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Cut Fence	0	B	10	3
2	Run to Building	0	B	12	3.6
3	Open Door	0.9	B	90	27
4	Run to Vital Area	0	B	10	3
5	Open Door	0.9	B	90	27
6	Sabotage Target	0.9	B	120	36
7					
8					
9					
10					
11					
12					

Probability of Interruption: 0.476311462

Results of EASI Analysis for

4 Physical Protection Systems Policies

In the 1990S

- The SAVI modules are part of apparently the most complex method and software tool called “***Analytic System and Software for Evaluating Safeguards and Security***” (ASSESS). Software ASSESS consists of six modules: Facility, Insider, Outsider, Neutralization, Colluding Insider, Manager.
- A state-of-the-art proprietary model, in use by the DOE, that incorporates the insider threat into an advanced methodology. The output is a ranking of the threat paths of a facility. This model also analyzes the force-on-force encounters between adversaries and security forces and provides a probability of defeat. This model incorporates the EASI algorithm to predict system performance.

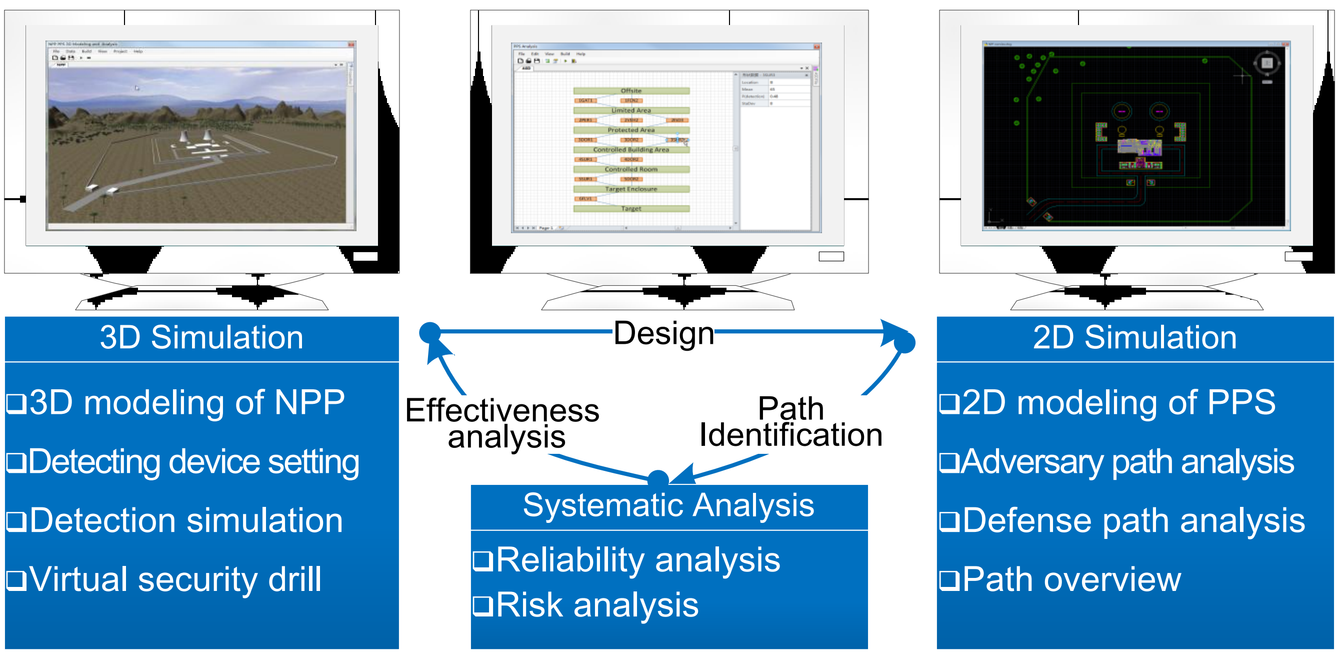
PART TWO

Effectiveness Analysis of PPS

02 Analysis of PPS Effectiveness

1 Integrated Platform for Analysis and Design of PPS

- The system includes three modules for three-dimensional (3D) simulation, two-dimensional (2D) simulation and systematic analysis of a NPP and its PPS, respectively.
- Under this framework, the process of PPS design, adversary path identification and effectiveness evaluation of PPS is organized as an interactive and closed cycle which will provide a convenient visualization environment for the design and the continuous improvement of PPS.



Interactive and closed-cycle framework

02 Analysis of PPS Effectiveness

2 3D Simulation Module

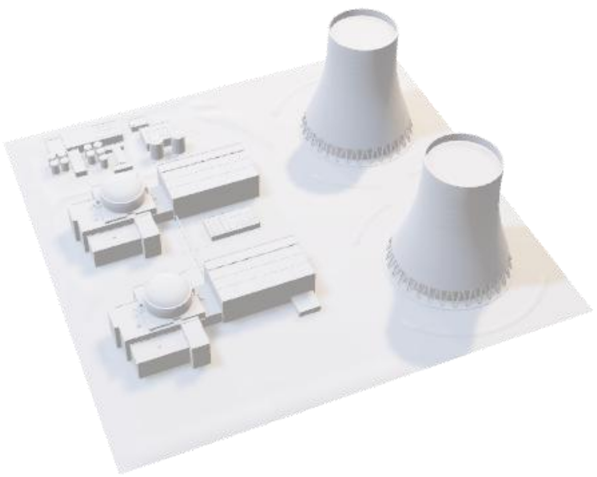
- The 3D simulation module enables the designers to establish the 3D scene model of a NPP by the following procedures:

① Divide the 3D scene into buildings, nuclear facilities, adversaries, response force and other entities;

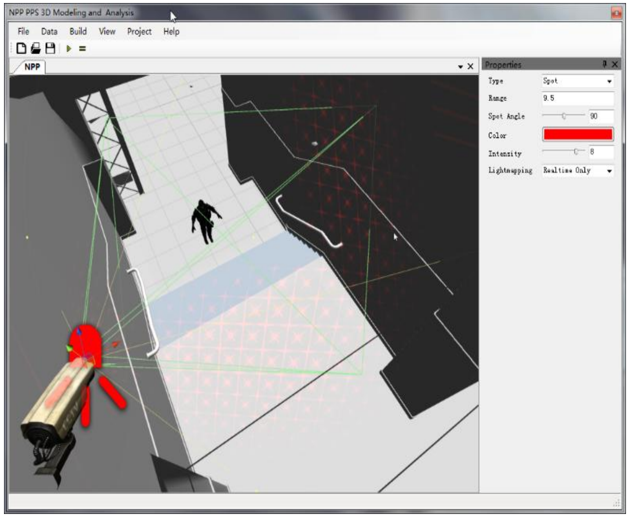
② Determine the geometry of the various entities, spatial location and the connection between entities;

③ Determine the hierarchical structures of the PPS model;

④ Describe the entities. The material parameters of buildings and device, as well as the characteristics of adversary and response force should be consistent with the actual situation in order to achieve a realistic effect.



3D model of NPP

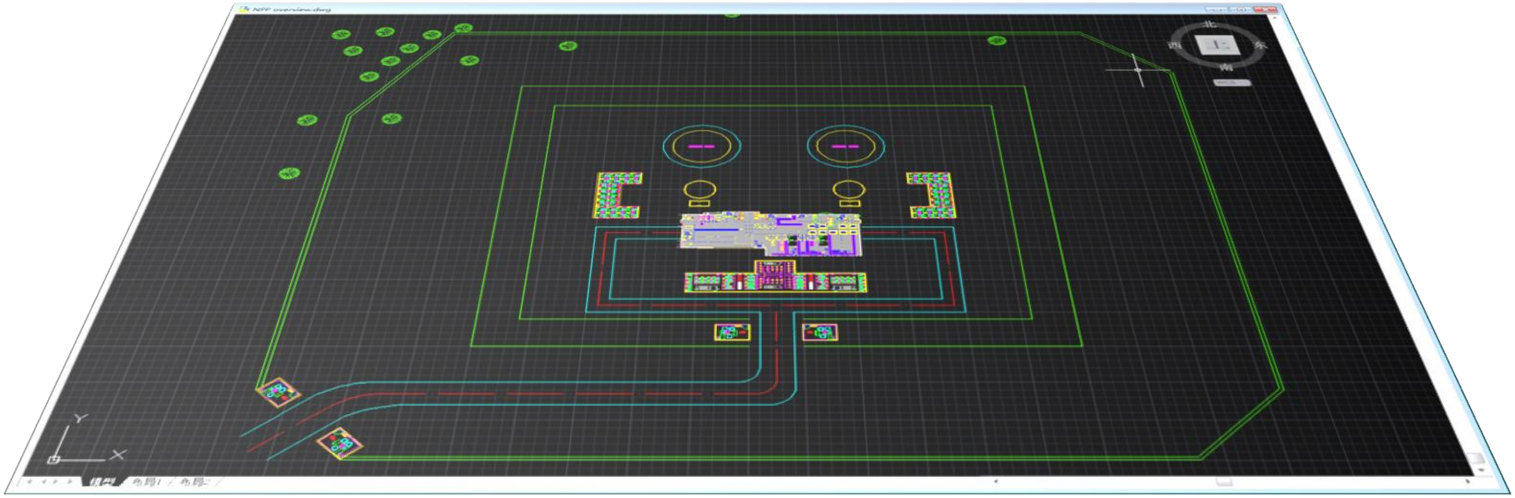


Simulation of detecting device settings and effects

02 Analysis of PPS Effectiveness

2 2D Simulation Module

- As shown in Figure, designers can generate 2D CAD graphic design drawings from the AutoCAD based 3D models of NPP by the secondary development using .NET technology.
- Since the 2D CAD design drawings contains the basic spatial information of detecting and delay devices, it will provide the basis for the further analysis and display of the possible adversary paths and the best defense path of response force.



Example of a 2D graphic design drawing of PPS

02 Analysis of PPS Effectiveness

3 Systematic Analysis

- A systematic analysis method based on the 2D CAD design drawings. Systematic analysis module provides the following functions for the reliability analysis and risk analysis of PPS.

① **Adversary path identification**: Adversary Sequence Diagrams (ASD) can be identified on the basis of the PPS defense layers and facility layout. An ASD indicates a path from the current location of adversaries to the terminal target.

② **Reliability parameters settings**: The systematic analysis module enables the analysts to input the reliability parameters of defense devices, such as probability of detection, mean time to penetrate a defense and travel a certain distance, etc.

③ **Reliability analysis**: The systematic analysis module supports the probability calculation of each adversary path to be successfully interrupted.

④ **Risk analysis**: This function is to calculate the risk of nuclear material and nuclear facilities suffered by adversary sabotage in case of PPS failures.

02 Analysis of PPS Effectiveness

4 Risk Analysis

- Security Risk Equation:

$$R = P_A \times (1 - P_E) \times C$$

- where: R is risk of the undesired event
  P_A is the likelihood of adversary attack
  P_E is the overall PPS effectiveness
  C is the consequence of undesired event.

- If either the consequence (‘C’) or attack likelihood (‘P_A’) becomes higher, the overall PPS effectiveness (‘P_E’) is required to be higher in order to keep the risk (‘R’) the same.

02 Analysis of PPS Effectiveness

5 Effectiveness Analysis

- Three metrics are commonly used for the evaluation of PPS performance:

① System Effectiveness (PE)

✓ The probability that the PPS will prevent the adversary from completing the undesired event.

$$P_E = P_I \times P_N$$

✓ For a PPS to be effective against theft and sabotage, the response force must both interrupt "AND" neutralize the adversary.

✓ i.e. if $P_I = 1$ (ideal and timely) but $P_N = 0$, $P_E = 0$

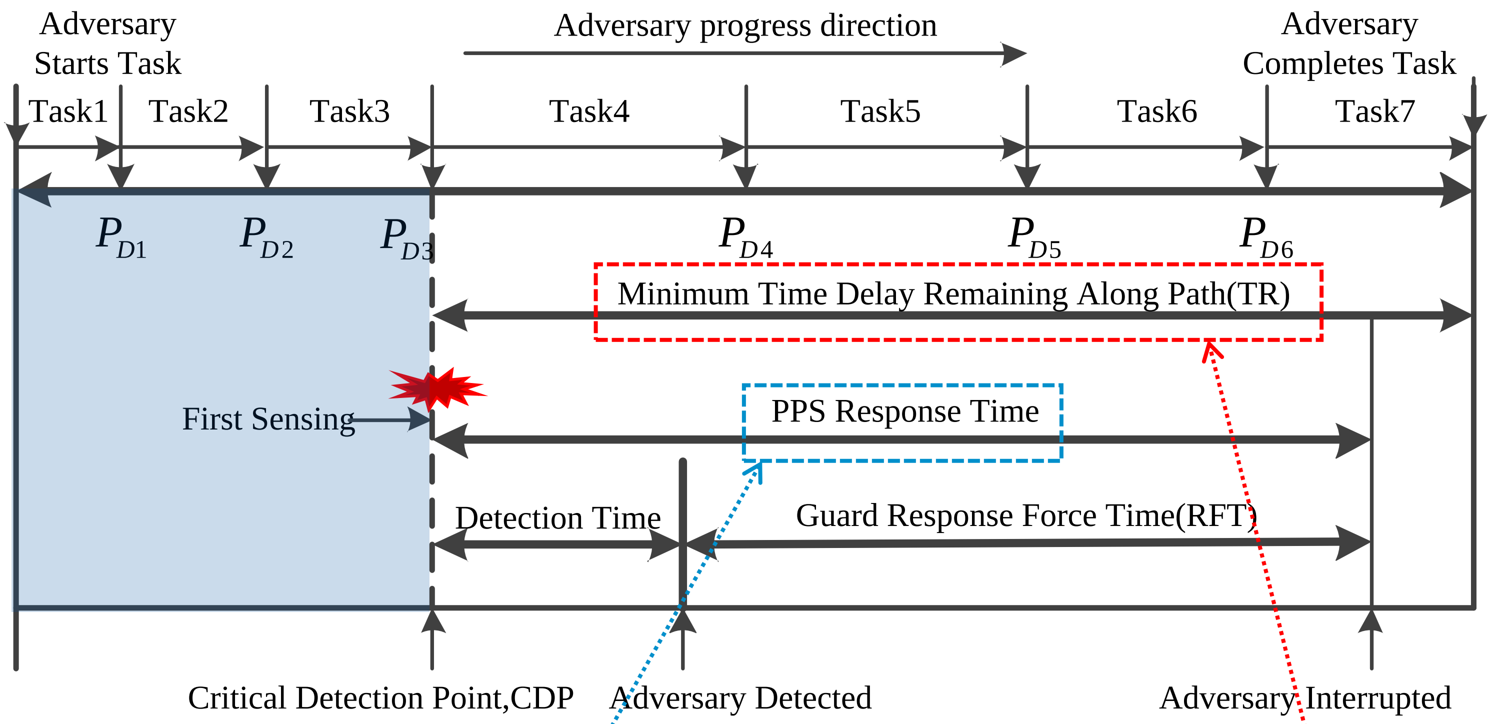
① Probability of Interruption (P_I)

② Probability of Neutralization (P_N)

02 Analysis of PPS Effectiveness

5 Effectiveness Analysis

- Adversary and PPS Timelines



- A sensing opportunity on a path is timely if ***Response Force Time*** **<** ***Adversary Task Time Remaining*** After First Sensing.

02 Analysis of PPS Effectiveness

5 Effectiveness Analysis

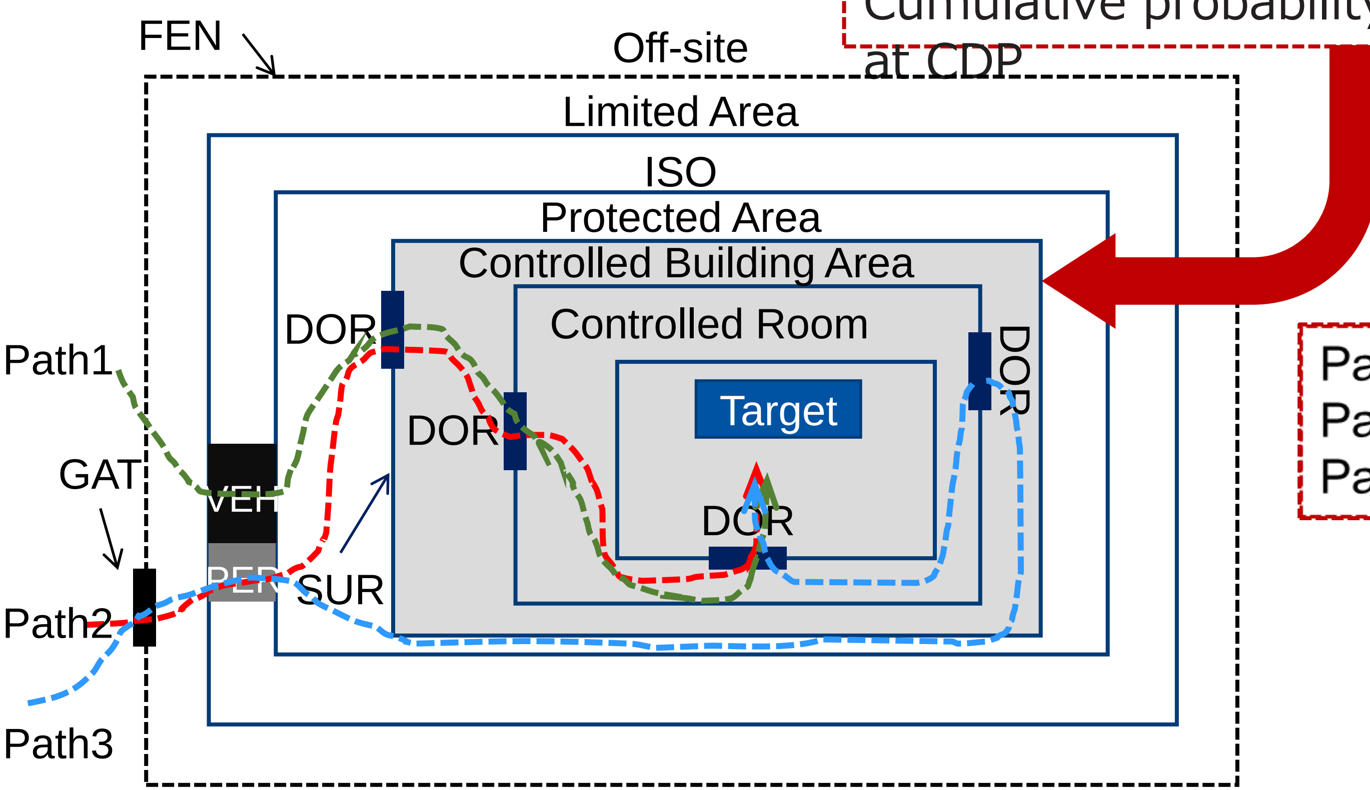
A. Probability of Interruption (P_I)

- ✓ The cumulative probability of detection along a path up to and including the Critical Detection Point.

$$P_I = 1 - (1 - P_{D1}) \times (1 - P_{D1}) \times \ldots (1 - \boldsymbol{P_{DCDP}})$$

- ✓ where P_{Dj} is the probability of detection at the j^{th} opportunity

Cumulative probability of detection at CDP



Path1: $P_I = 0.856$
Path2: $P_I = 0.806$
Path3: $P_I = 0.903$

02 Analysis of PPS Effectiveness

5 Effectiveness Analysis

B. Probability of Interruption (P_I)

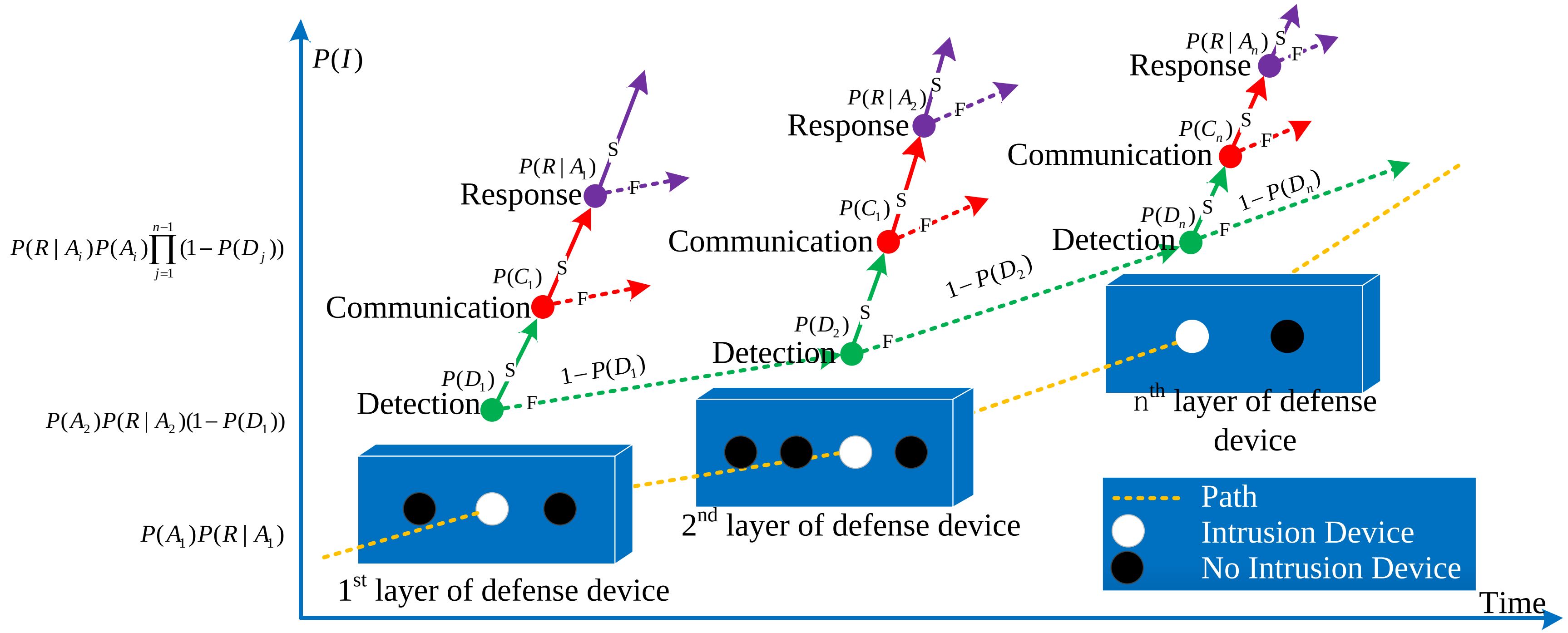
✓ In the case of a single detection sensor (or other possible means of detection), the probability of an adversary action sequence interruption is given by

$$P_I = P(R|A) \times P(D) \times P(C)$$

✓ $P(R|A)$ = probability of response force arrival prior to the end of the adversary's action sequence, given an alarm. $P(C)$ =probability of communication to the response force.

02 Analysis of PPS Effectiveness

5 Effectiveness Analysis



Principle of PPS reliability analysis

For two or more sensors, The general formula for P(I) based on similar reasoning is

$$P_I = P(R|A_1) \times P(D_1) \times P(C_1) + \sum_{i=2}^{n} P(R|A_i) \times P(C_i) \times P(D_i) \prod_{i=1}^{i-1} (1 - P(D_i))$$

02 Analysis of PPS Effectiveness

5 Effectiveness Analysis

- ☐ Probability of Neutralization (P_N)
  - ✓ The probability that the response force will gain complete physical control of the adversary, given interruption of the adversary by the response force.

$$P_N = \frac{N_{win}}{N_{engagements}}$$

- ☐ Assuming:
  - ✓ $N_{engagements}$ is a statistically significant number of engagements
  - ✓ All engagements have the same initial conditions
  - ✓ Two possible outcomes per engagement: win or less

Dependent on the weapons, armors, proficiency, tactics, postures, etc.

02 Analysis of PPS Effectiveness

6 Heuristic Path-finding Algorithm

- **Insufficient** of EASI method
- ✓ The EASI method is used the enumeration method to seek the vulnerability adversary path, but when the size of the intrusion node becomes larger, the computation becomes larger and the solution speed becomes slower.

- Using A* algorithm for path-finding will not seek the most vulnerable intrusion path if heuristic information is considered. However, for non-heuristic information, A* algorithm will be equivalent to the Dijkstra algorithm that can seek the most vulnerable intrusion path which is described in detail.

- A* algorithm:

$$F(n) = G(n) + H(n)$$

- ✓ $G(n)$ is the cost function of the path from the start node to node (known function, it is breadth-first search);
- ✓ $F(n)$ is a heuristic that estimates the cost of the cheapest path from n^{th} node to the target node (unknown function, it is depth-first search).

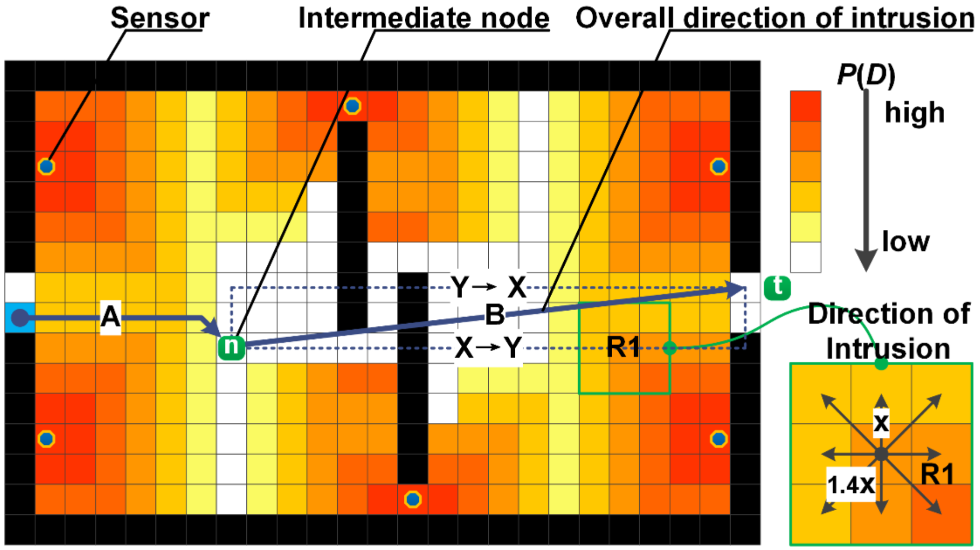
For the algorithm to find the actual shortest path quickly, the heuristic function $\mathrm{H}(n)$ should be more accurate.

02 Analysis of PPS Effectiveness

6 Heuristic Path-finding Algorithm

- Probability of Detection
- ✓ Detection probability of sensors is only considered to estimate whether the adversary intrusion path is vulnerable or not.

$$\begin{cases} P(D) = P(D)_G + P(D)_H \\ P(D)_G = P(D_1) + P(D_2) \times [1 - P(D_1)] + P(D_n) \times \prod_{i-1}^{n} [1 - P(D_{n-1})] \\ P(D)_H = h(p) \times \prod_{i-1}^{n} [1 - P(D_{n-1})] \end{cases}$$



Sketch map for the grid generation, the detection distribution, and direction of movement.

02 Analysis of PPS Effectiveness

6 Heuristic Path-finding Algorithm

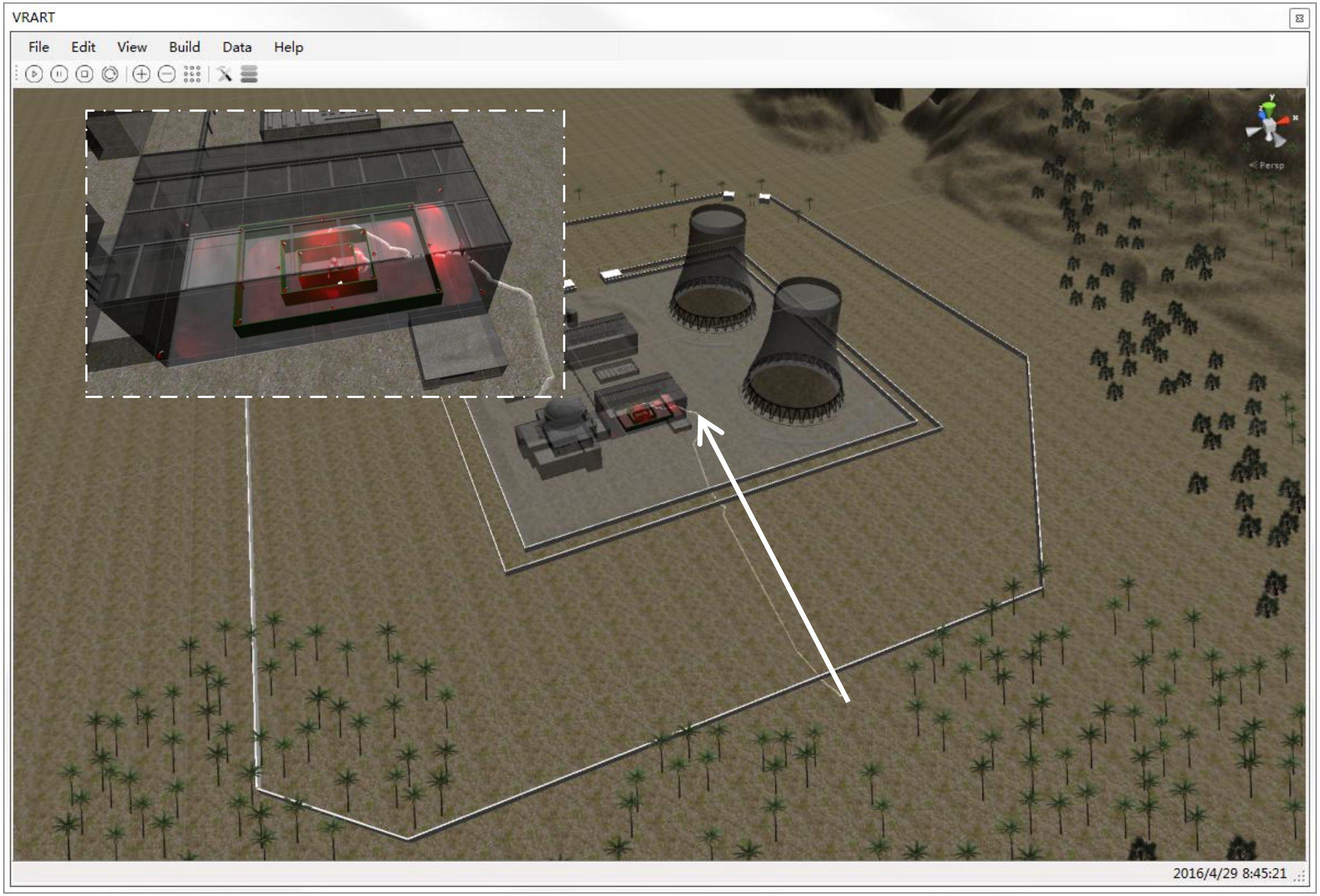
- Probability of Interruption
- ✓ On the basis of the EASI approach, the probability of interruption is used for the comprehensive evaluation of the PPS effectiveness. The higher the probability of interruption, the more effective the PPS protects the nuclear facilities and materials.

$$
\begin{cases}
P(I) = P(I)_G + P(I)_H \\
P(I)_G = P(R|A_1) \times P(D_1) \times P(C_1) + \sum_{i=2}^{m} P(R|A_i) \times P(C_i) \times P(D_i) \prod_{j=1}^{i-1} (1 - P(D_j)) \\
P(I)_H = 0
\end{cases}
$$

- $P(I)_G$ is regarded as cost functions of A* algorithm ($G(n)$), which is used to compute the probability of effectiveness from the start node to n.
- $P(I)_H$ is equaled to the heuristic function $H(n)$ and it is difficult to find an optimal function to describe it because more than one parameter should be calculated. Thus, $P(I)_H = 0$.

02 Analysis of PPS Effectiveness

6 Heuristic Path-finding Algorithm



Simulate intrusion in 3D Scene.

PART THREE

Scenario Analysis of PPS

03 Scenario Analysis of PPS

1 What Is Scenario Analysis?

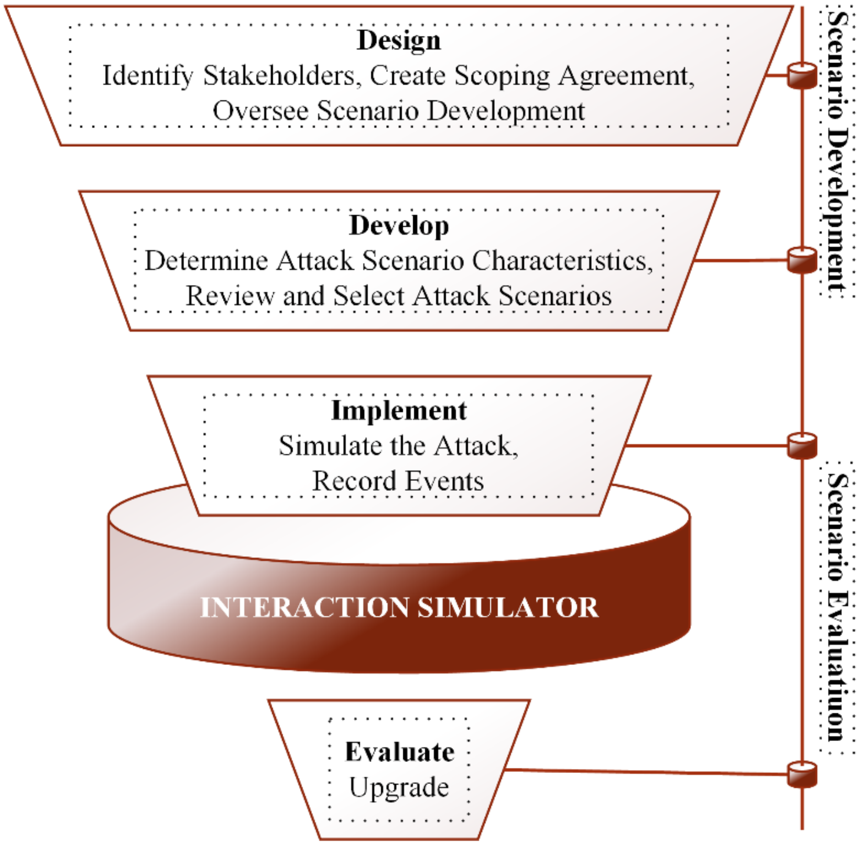
- Scenario Analysis
  - ✓ A methodology for analyzing PPS effectiveness by considering several possible adversary scenarios.

- Scenario Analysis
  - ✓ Allows more detailed analysis of the attack, defense, and results of path analysis
    - Path analysis can be used to help determine the scenarios to be analyzed
  - ✓ Focuses on identifying vulnerabilities
  - ✓ Contributes to
    - Overall PPS design
    - Contingency plans
    - Policies and procedures
    - Interagency coordination

03 Scenario Analysis of PPS

2 Scenario Analysis Simulator

- Figure shows the improvement on scenario analysis process which includes four steps, design, develop, implement and evaluate. In the phase of scenario development, the security risk simulator constructs a knowledge base for the description of the current status of PPS.

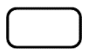


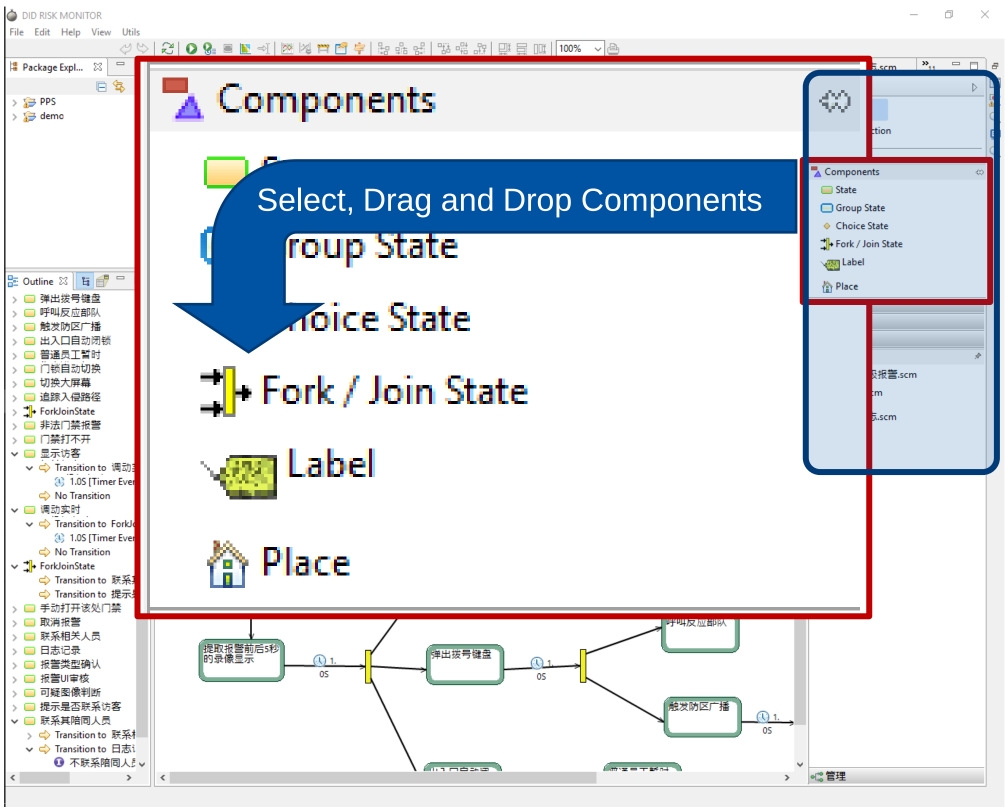
Process of Scenario analysis in interaction simulator

03 Scenario Analysis of PPS

3 DID Risk Monitor

- Proposed by Prof. Hidekazu Yoshikawa

SYMBOL	TERM	DEFINATION
	State	State represents the condition of an object at a particular point in time, including simple state, initial state, final state, composite State.
	Decision	Decision state accepts tokens on one or two incoming edges and selects one outgoing edge from one or more outgoing flows.
	Merge	Merge state brings together multiple incoming alternate flows to accept one outgoing flow.
	Fork	Fork state makes parallel processing states.
	Join	Join state synchronizes all input side parallel state and makes transition to one state.
	Transition	Transition is an arrow line connecting between states. Events and actions are hold in the transition line.

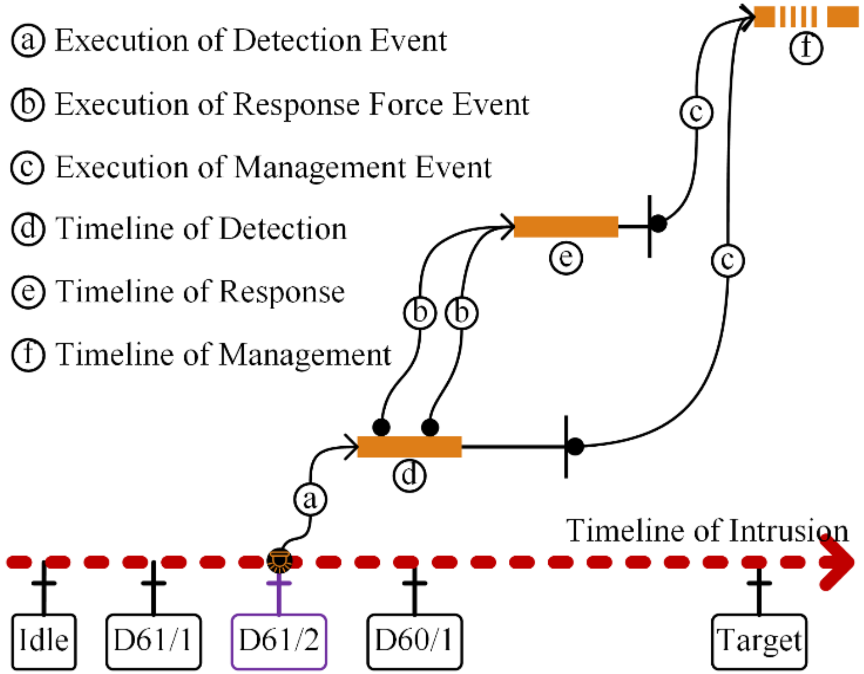


Snapshot of DID Risk Monitor

03 Scenario Analysis of PPS

4 Case Study

- During the simulation of security risk, the required time for each state is set on the security risk simulation platform. In the case of considering internal threats, in can be assumed that a protection device has failed.
- For example, an alarm occurs in D61/2, if D60/1 element is the internal insider’s jurisdiction or the adversary can easily penetrate, the delay time is set to 0.0s on the security risk simulation platform to simulate the internal threat mode as shown in figure.

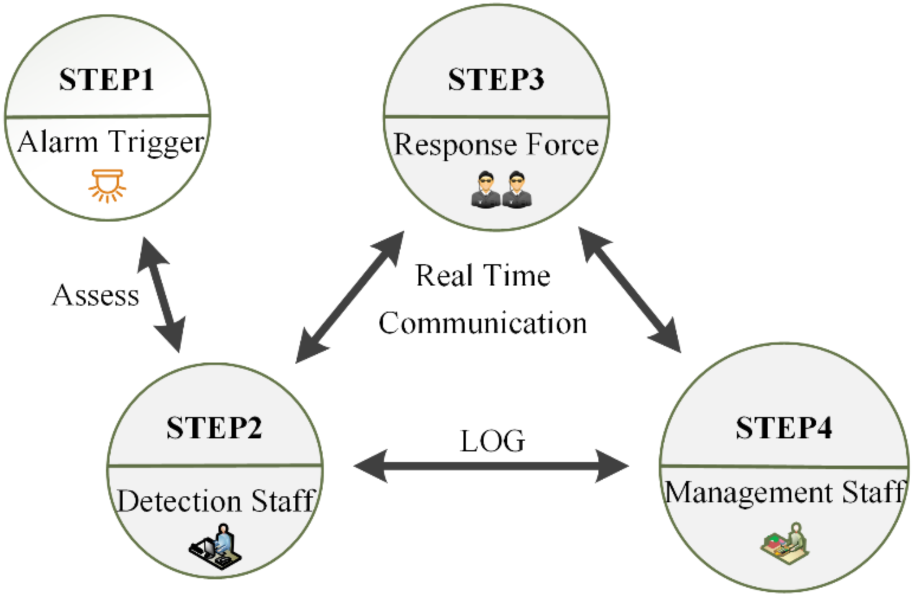


An area where adversary is detected in the adversary intrusion path

03 Scenario Analysis of PPS

4 Case Study

- A scenario analysis of PPS, as showed in figure, can effectively bundle management staff, detection staff and response force to achieve real time cooperation, interaction of comprehensive information and response of emergency.
- In engineering, the nuclear power plant develops an integrated management platform to supervise and manage the three roles which can reduce the consequences of failure of defense against adversary intrusion caused by human error.

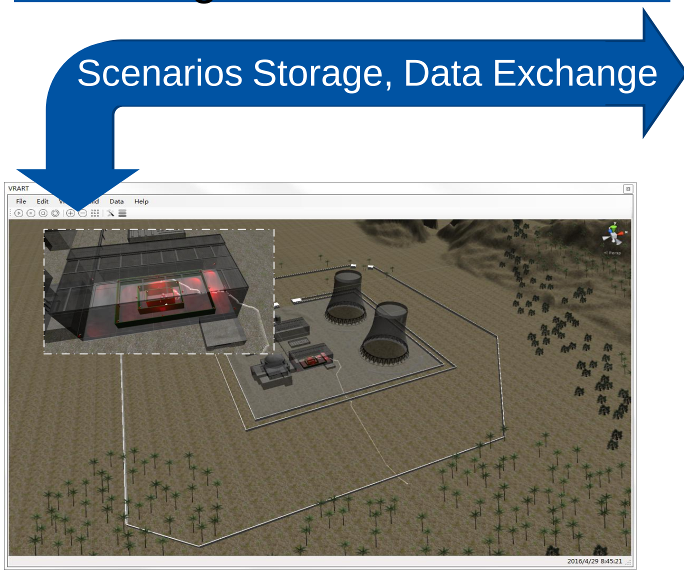


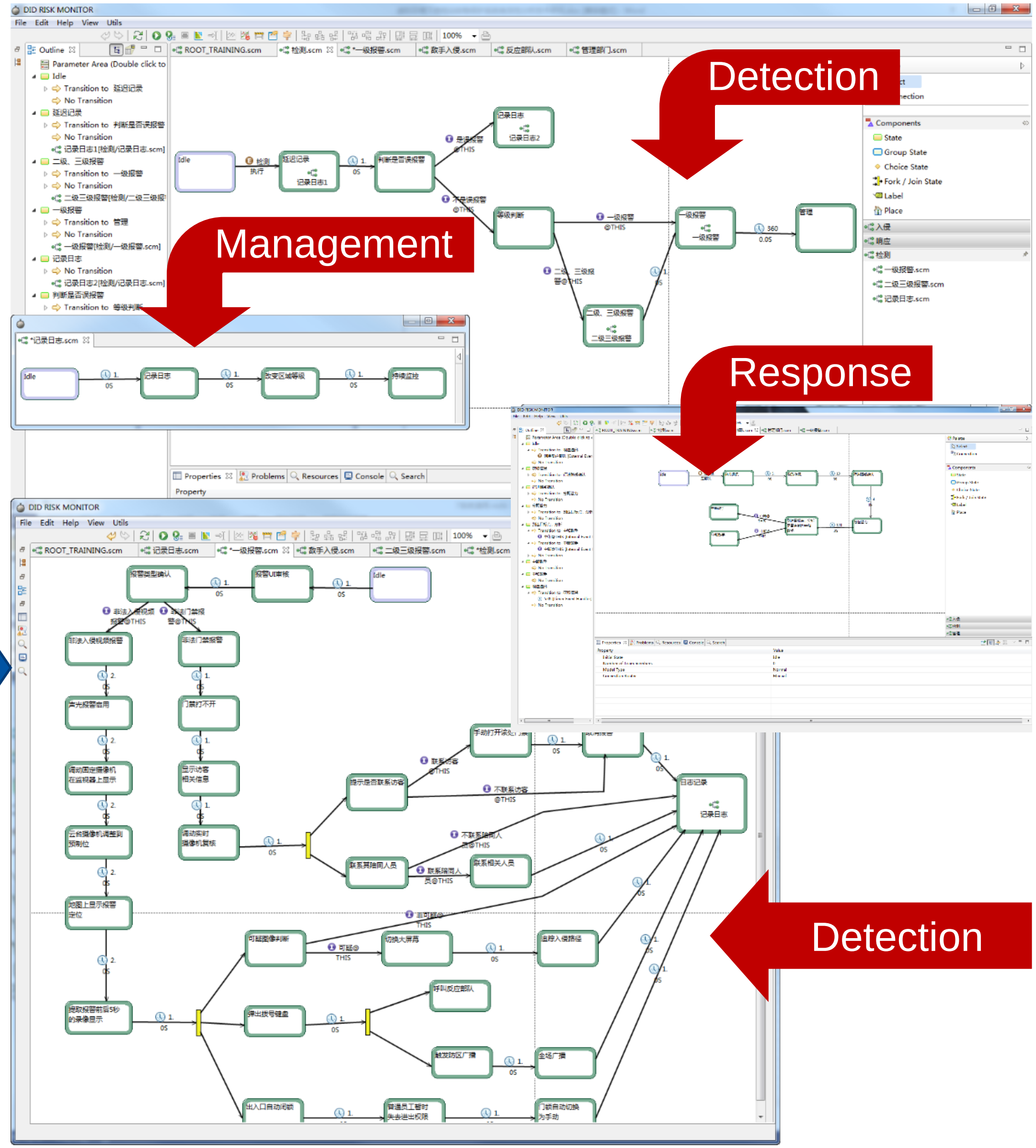
Security management methods in NPPs

03 Scenario Analysis of PPS

4 Case Study

- The detection regulation is based on a NPP comprehensive security management patent which proposed by Shanghai Nuclear Engineering Research & Design Institute.





Detailed flowchart of integrated security management methods for NPPs.

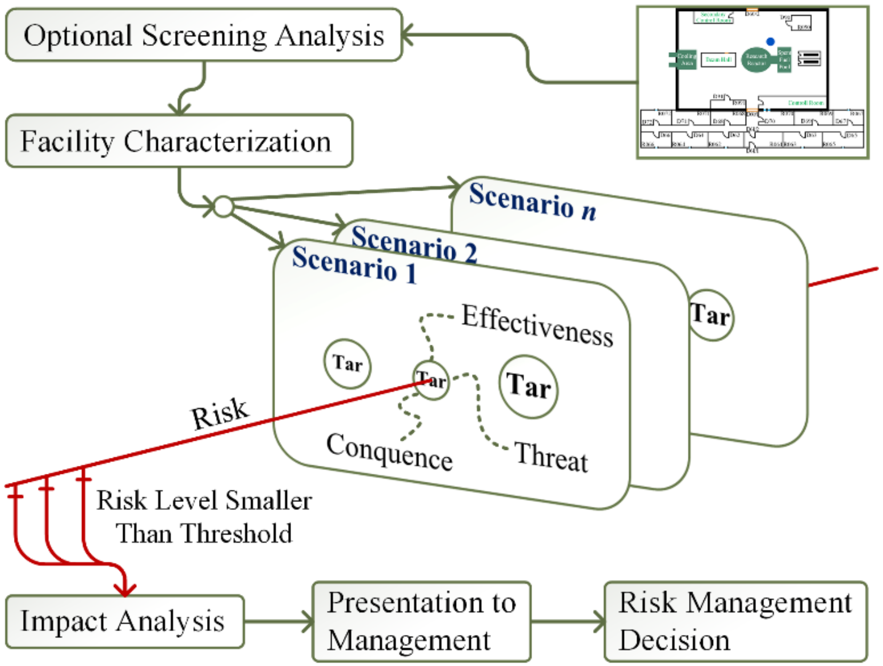
03 Scenario Analysis of PPS

4 Case Study

- The steps include optional screening analysis, facility characterization, (threat analysis, consequence analysis, effectiveness analysis), impact analysis, presentation to management, and risk management decision. The basic risk equation proposed by Sandia Laboratory is

$$R = p(A) \times [1 - P(E)] \times C$$

- The figure is an analytic process of system risk under different design basis threats. The results of risk assessment are used to assist managers for analysis.



Risk Assessment Process.

PART FOUR

Conclusions

Conclusions

① An ***integrated platform*** for analysis and design (IPAD) of PPS was proposed.

② A novel ***heuristic path-finding method*** was proposed for the evaluation of a vulnerable intrusion path in PPS.

③ The ***DID risk monitor*** is used for the scenario analysis of PPS. The interaction simulator integrates all discrete subsystems of PPS to form an intermodulation chain of intrusion-detection-response-interruption. Adversary intrusion strategies and defense strategies are regarded as knowledge bases in the interaction simulator.


OKAYAMA
UNIVERSITY
THANK U
ありがとうございます