IAEA Physical Protection Conference CN-152(14 Tue. Nov., 2017)

Application to Vital Areas Identification of Nuclear Power Plants based on PSA

KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL
PHYSICAL PROTECTION DIVISION

Minho KANG

KINAC
KOREA INSTITUTE OF NUCLEAR NONPROLIFERATION AND CONTROL

Contents

KINAC

Background

- Enforcement Decree of The Act on Physical Protection and Radiological Emergency [*Article 2. Definition*]

  : The term "vital area" means those areas, in the protected area, fixed for the protection of nuclear facilities, etc. that may produce, directly or indirectly, an unacceptable radiological consequence due to sabotage.

- INFCIRC-225/Rev.5 (2011)

  : An area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences (HRC)

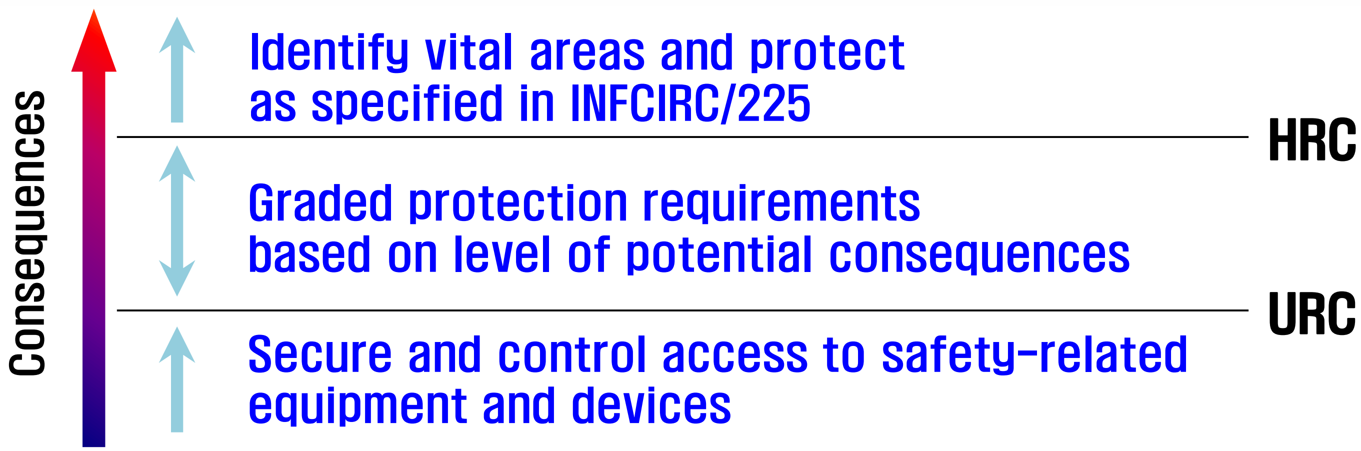
Background

- URC (Unacceptable Radiological Consequences)

  : Establish at the national level as the radiological impact of the lowest standard requiring physical protection measures

- HRC (High Radiological Consequences)

  : Establish at the national level as the radiological impact of the basis for identifying vital areas



※ Approach for Physical Protection Against Sabotage
(IAEA Nuclear Security Series No. 13)

Vital Area Identification (U.S. and ROK)

- United States
  - Identification of Vital Areas based on Minimal Prevention Sets calculated by using Fault Tree Methodology
    - U.S. Vital Area Identification starts with the NUREG-1178 Assumptions

      ※ NUREG-1178, "Vital Equipment/Area Guidelines Study", Feb. 1988
    - Published Sandia Report* described process of VAI

      ※ SAND2008-5644, "Vital Area Identification for U.S. NRC Nuclear Power Reactor Licensees and New Reactor Applicants", Sep. 2008

- ROK
  - Re-Identifying of Vital Areas of NPP in operation and under construction based on PRA(Probabilistic Risk Assessment) Methodology
    - Developing technical standards to meet international standards

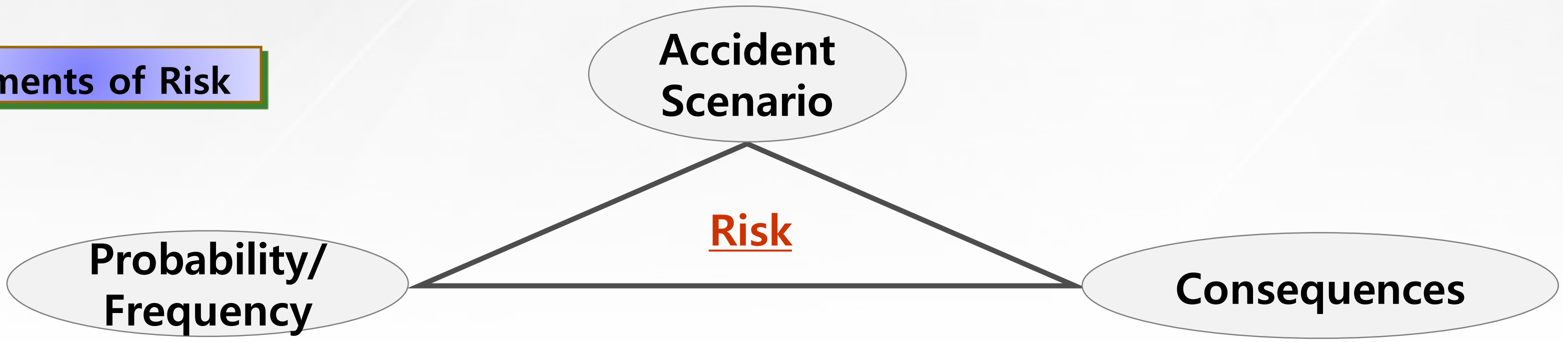
Overview of PRA

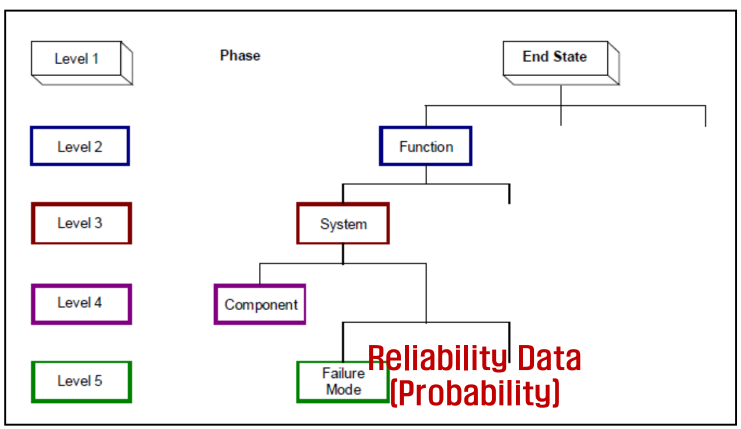
■ Definition and Key Elements of PRA

Definition

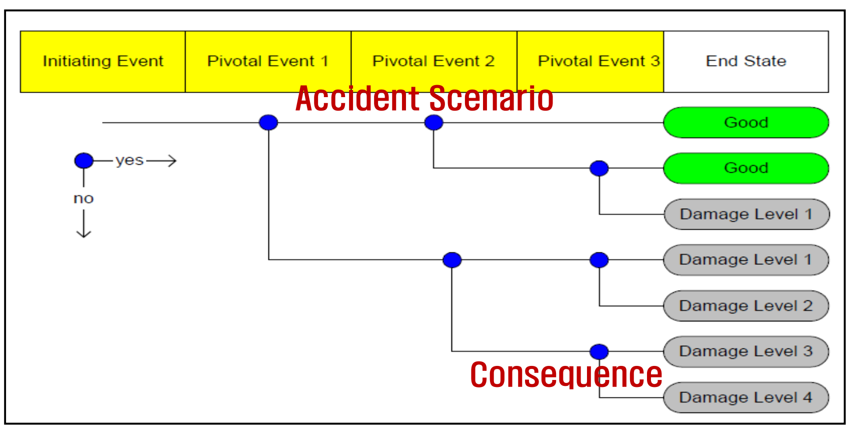
Risk = Probability of an Accident X Consequences

Elements of Risk





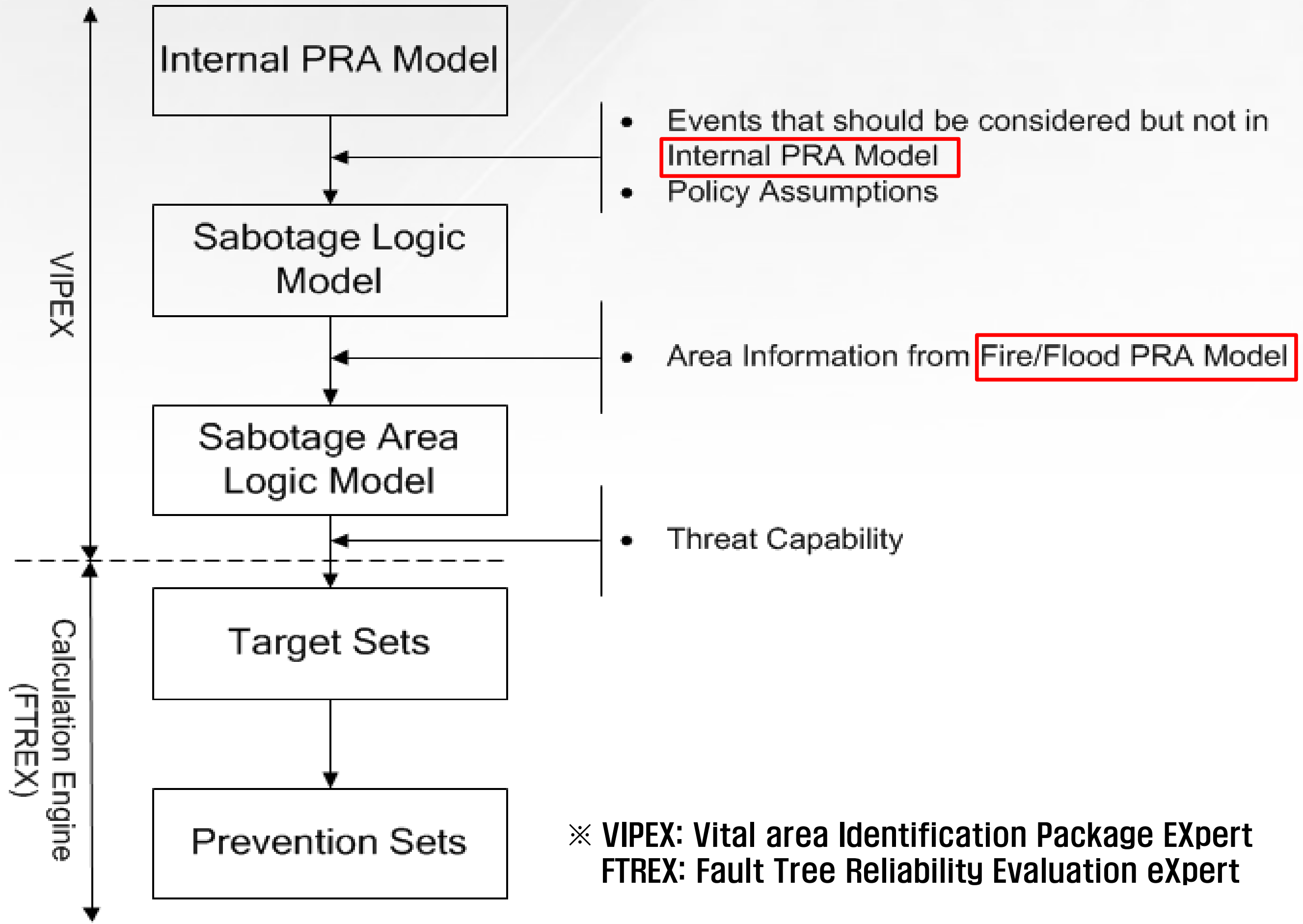
<Fault Tree>



<Event Tree>

Vital Area Identification based on PRA

Process of VAI



※ **VIPEX: Vital area Identification Package EXpert**
FTREX: Fault Tree Reliability Evaluation eXpert

KINAC

Vital Area Identification Process

Development of Sabotage Logic Model

- Development of Sabotage logic model based on Internal PRA model
  - Identify any initiating events of malicious origin(IEMOs) with mitigating system disablements that would lead to HRC
  - Find a list of the safety function needed to respond to IEMOs and then identify a list of front line system and support systems that perform each safety function
  - Describe system success criteria for front line systems and support systems with each IEMO

IEMO	Front-Line System	Support System	Success Criteria	Support Document	Special Characteristics
Loss of off-site power	Waste tank cooling system		One of two trains delivering cooling water at 100% of design flow (80% of pump max flow)	HAWSF DSA extract	Both coolant pumps are flow-cooled and self-lubricating.
	Train A	440 VAC Bus A (standby power)	90 kilowatts of power from Standby Diesel Generator A (125 kilowatts nominal power)	Design specifications for Train A cooling pump (see Figure C-3)	
	Train B	440 VAC Bus B (standby power)	90 kilowatts of power from Standby Diesel Generator B (125 kilowatts nominal power)	Design specifications for Train B cooling pump (see Figure C-3)	

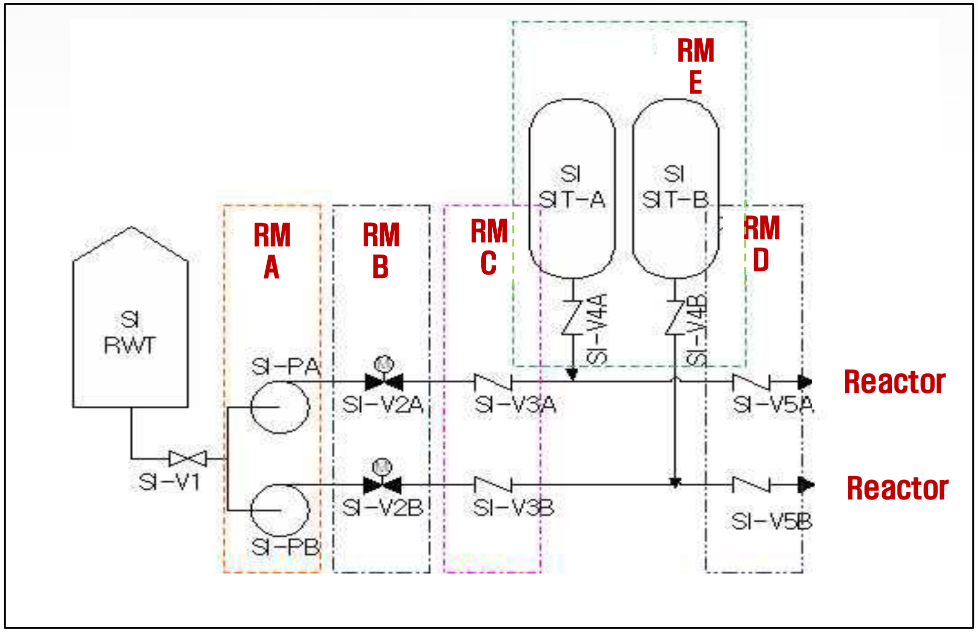
<Example : Success Criteria of IEMO/System>

Vital Area Identification Process

■ Development of Sabotage Area Logic Model

➢ Conversion from Sabotage logic model to Sabotage Area logic model

- Identify the locations(areas) in which IEMOs and the other events in the sabotage logic model can be accomplished
- Replace the events in the sabotage logic model with their corresponding areas



※ Solve the sabotage area logic model to identify the combinations of locations that should be protected.

Ex) Room A destroyed
⇒ SI Pump A/B is failed

AND

Room E destroyed
⇒ SI Tank A/B is failed

Core Damage

Vital Area Identification Process

- Identify Target Sets and Prevention Sets
  - ➢ Solve the Sabotage area logic model via calculation software
    - Find Target Sets

      ⇒ Minimal cut set(MCS) of the sabotage area logic model is combination of target sets
    - Find Prevention Sets

      ⇒ If the adversary is prevented from gaining access to all the areas in one prevention set, he will not be able to complete any of the sabotage attacks
    - Select the vital area set from the candidate vital area sets identified as prevention sets that will be protected to prevent sabotage leading to HRCs

      ※ Consideration Factor : Low difficulty of providing protections / High effectiveness o f protection measures and etc.

Thank You.

Q&A