The MDTA Method for Analysing Diagnosis Failures in NPP Emergencies

APCRMS '05, Hong Kong
Dec. 1-2, 2005

J.W. Kim, W. Jung, J. Ha
(E-mail: jhkim4@kaeri.re.kr)

Integrated Safety Assessment Division
Korea Atomic Energy Research Institute

Introduction (1)
– event diagnosis

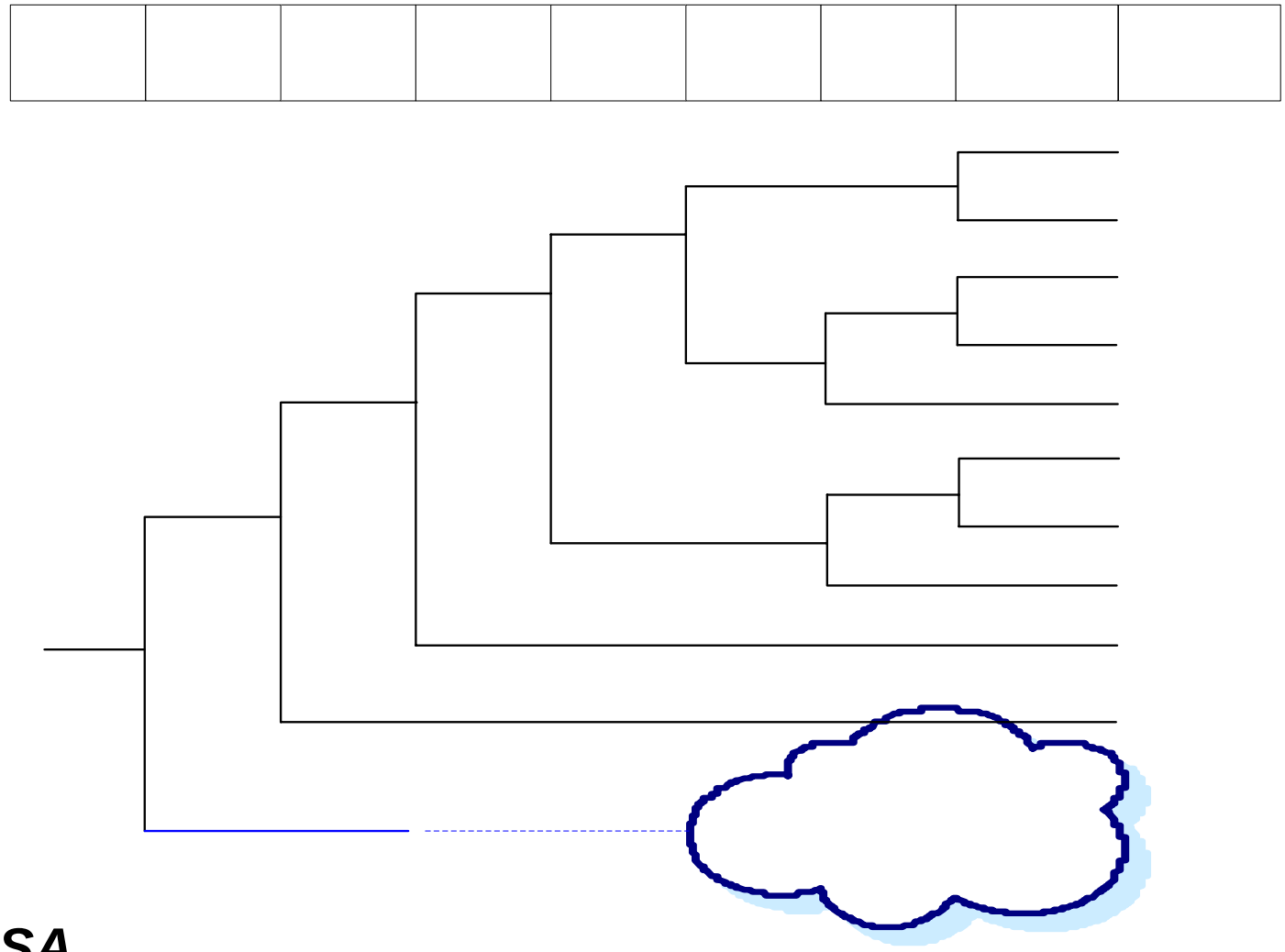
- **Importance of Event Diagnosis**
  - **Diagnosis of an event (or events) is crucial for managing or controlling the plant to a safe and stable state.**
  - **Diagnosis failure (/misdiagnosis) of the event(s), if not recovered, can cause the operators' inappropriate actions, (e.g. TMI-2: PORV LOCA, Palo Verde 2: SGTR, Fort-Calhoun: PSV LOCA, UCN-4: SGTR, …)**
- **Status of HRA in Conventional PSA**
  - **Diagnosis failure (/misdiagnosis) are not considered adequately in a current PSA/HRA (c.f. diagnosis error probability such as in THERP)**
  - **Impacts of diagnosis failure on the operator actions such as errors of commission (EOC) are not modeled (Only errors of omission (EOO) are modeled).**

Introduction (2)
–operating experience

Events	Event Type	Major Human Events	Human Failure Mechanisms & Context
TMI-2 (1979)	PORV LOCA with Loss of MFW	Inappropriate termination of HPSI (EOC)	▪ Diagnosis Failure : -PORV stuck-open: PZR level high and rising -PORV indicated CLOSED (design problem) -Proc.: No direct guidance for PORV LOCA -Train.: No training for PORV LOCA
Fort Calhoun (1992)	PSV LOCA with Electrical Fault	Inappropriate termination of HPSI (EOC)	▪ Potential for Diagnosis Failure -RCS pressure indicator fails high -> RCS sub-cooled margin (SCM) indicated sufficient -Computer displays for RCS sub-cooling parameters malfunctioning
Crystal River 3 (1991)	Pressurizer spray valve failure to close	Bypassing of ESF/ Securing of HPSI (EOC)	▪ Diagnosis Failure - Fail to make a correct sit. ass. due to instrumentation failure - Misdiagnosed the given symptoms
UCN 4 (2004)	SGTR	Reset of HPSI setpoint (EOC)	▪ Delayed Diagnosis & Violation : -RCS pressure dropped rapidly; -Delayed response of radiation monitor (design problem)

Introduction (3)
– event scenarios

- **New event scenarios could be caused by diagnosis failures**



Introduction (4)
– objective of the study

- To suggest a method for assessing diagnosis failures and modeling human unsafe actions into a PSA model

Model and Taxonomy (1)
- contributing factors

[Operating Experience]

Event	Contributing Factors	Error Mechanism
TMI-2 (PORV LOCA)	PORV indication failure Delayed response of RDT	Diagnosis Failure
Fort Calhoun (PSV LOCA)	RCS pressure indicator lags Delayed response of RDT	Potential for a Diag. Failure
Palo Verde 2 (SGTR)	Delayed radiation alarm on major detectors	Delayed Diagnosis
UCN 4 (SGTR)	Delayed response of radiation monitor	Delayed Diagnosis

[Simulator Study]

Event	Contributing Factors	Error Mechanism
SGTR -> GT	Misunderstanding of the diagnostic step 14	Diagnosis Failure
SGTR -> FRP	N16 Radiation alarm disappeared during diagnosis	Diagnosis Failure
LOCA ->ESDE	Procedural deficiency	Diagnosis Failure
LOAF ->ESDE	Communication error, too early diagnosis	Diagnosis Failure

[Categorizing Contributing Factors to Diagnosis Failures]

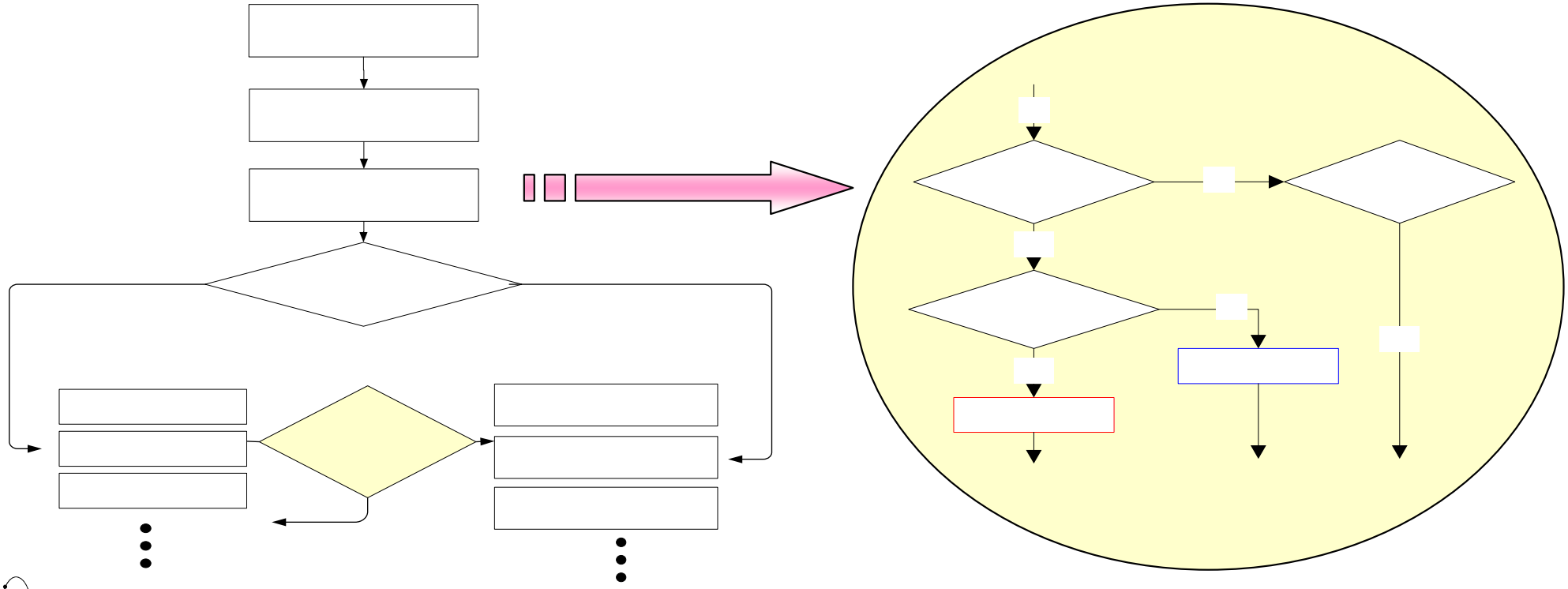
1. Plant Dynamics (PD)
- Temporal Characteristics or Symptom masking due to plant dynamic behaviors

2. Operator Errors (OE)
- Errors during information gathering or interpretation

3. Instrumentation Failure (IF)
- Unavailability of the instrumentation system

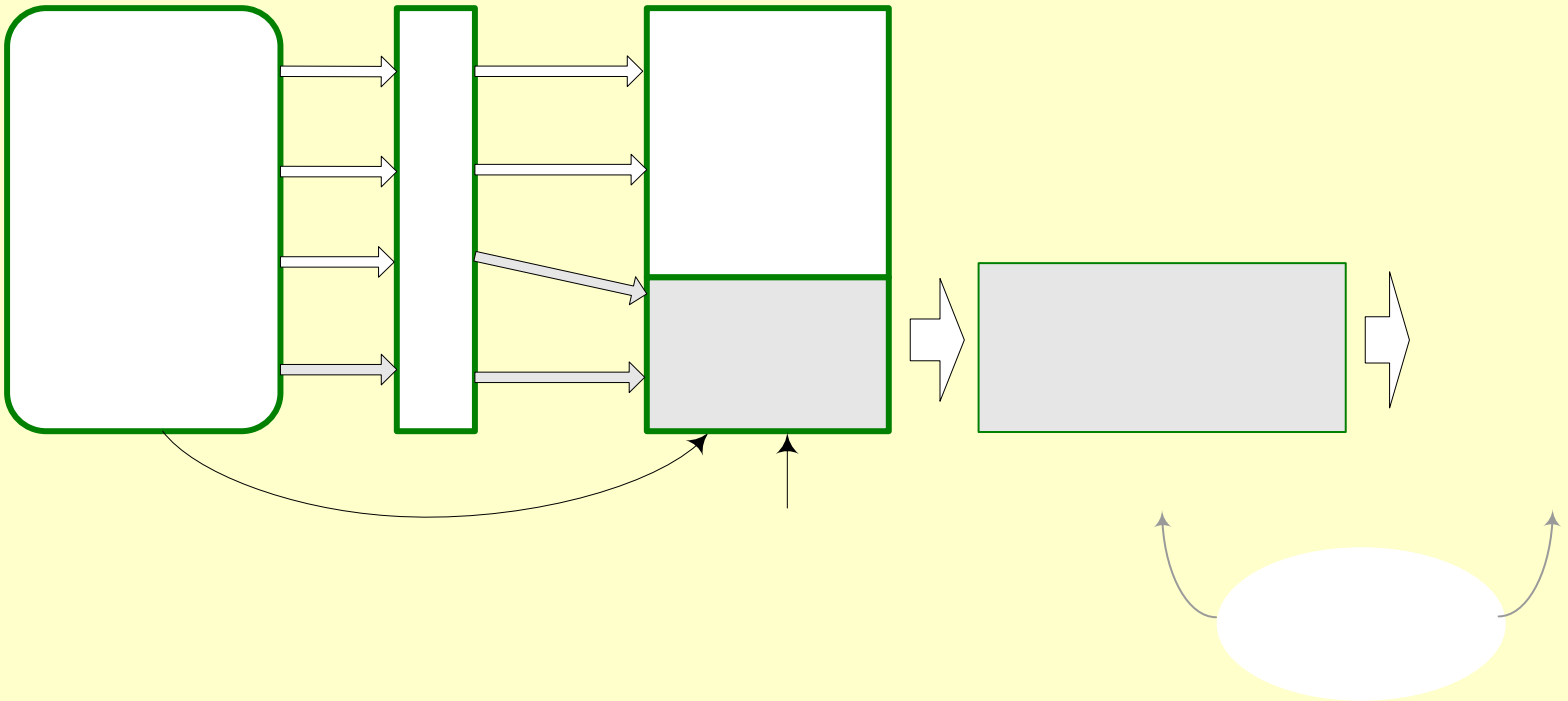
Model and Taxonomy (2)
- EOP structure

- **The EOP Structure of the KSNP**
  - **The KSNP EOP structure follows the CE-type EOPs, in which an initial diagnosis, using the flowchart-based procedure, determines the response procedure.**
  - **The initial diagnosis can only be altered (into FRP) through the safety function status checking.**



Model and Taxonomy (3)

for analysing diagnosis failures and their consequences

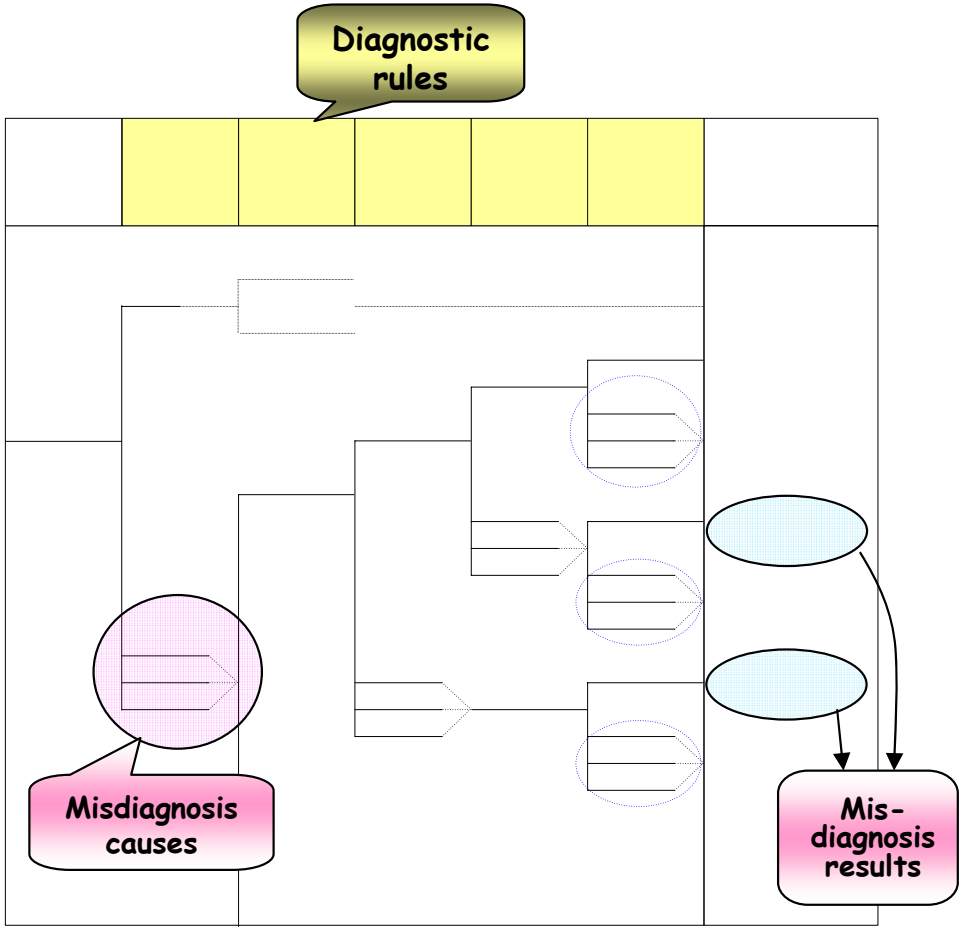


Plant Dynamics

MMI (signa
indicator, Cl

Method

- **Steps for Analysis**
  - **Step 1:** Assessing the potential for diagnosis failures
  - **Step 2:** Identification of the human failure events (HFEs) from diagnosis failures
  - **Step 3:** Quantification of the HFEs
- **Step 1:** Assessing the potential for diagnosis failures
  - Using the MisDiagnosis Tree Analysis (MDTA) method
    - Construction based on the diagnostic rules of EOP
    - Application of three causes to each decision parameter:
      - Plant Dynamics (PD)
      - Operator Error (OE)
      - Instrumentation Failure (IF)
    - Final results: Diagnosis results including misdiagnosis events, and associated decision paths & causes



Method-Step 1:
Guidelines for Assessing the PD

- **Contribution of PD to Diagnosis Failures**
  - Fraction of an event spectrum where the behavior of a decision parameter does not match the established criteria of a decision rule, due to the plant dynamic features.
- **Steps for Analysing PD**
  - Step 1: Classification of an event into sub-groups
    - According to the characteristics of the plant behavior, e.g. the break location (or the failure modes) and the status of the required mitigative systems
  - Step 2: Identification of suspicious decision rules
  - Step 3: Quantitative evaluation
    - Establish the range of an event spectrum that shows a mismatch with the established criteria of a decision parameter

<An Example of event classification for the SLOCA event>

Event category (e.g. break location)	Status of Mitigative Systems
RCS pipeline LOCA	– 2 trains of HPSI – 1 train of HPSI – All trains in failed state
PZR steam-space LOCA	– 2 trains of HPSI – 1 train of HPSI – All trains in failed state

Method-Step 1:
Guidelines for Assessing the OE

- **Contribution of OE to Diagnosis Failures**
  - **Selection of Influencing Factors:** Errors during 'Information Gathering' and 'Rule Interpretation'
  - **Assignment of error probabilities** using Expert Judgment and the CBDTM [EPRI]

Cognitive function	Detailed items	Basic HEP
Information gathering	Existence of confusing information	BHEP = 1.0E-2
	Information on more than one object is required	BHEP = 1.0E-2
Rule interpretation	Logic of a decision rule	(CBDTM, p_cg)
	- AND or OR	BHEP = 3.0E-4
	- NOT	BHEP = 2.0E-3
	- NOT & (AND or OR)	BHEP = 6.0E-3
	- AND & OR	BHEP = 1.0E-2
	- NOT & AND & OR	BHEP = 1.6E-2

Method-Step 1:
Guidelines for Assessing the IF

- **Contribution of IF to Diagnosis Failures**
  - **A single channel failure is assumed to be identified by the MCR operators during normal and abnormal operations**
  - **Only the possibility of CCF during normal operation is considered**
- **Assessing the Contribution of IF**
  - $Q_{CCF} = \beta * Q_T \cong \beta * (\frac{1}{2} \cdot \lambda \cdot T)$

β : the Beta factor

λ : The failure rate of the sensor and transmitter
(no data on the indicators)

T : The test interval

Method-Step 2: Identification of HFEs

- **Classification of Unsafe Actions (UAs)**
  - **UA-1: Unsafe actions related to required functions**
    - **Failure to initiate required functions**
    - **Failure to maintain required functions**
  - **UA-2: Unsafe actions related to unrequired or unnecessary functions**
    - **Manual initiation of unrequired functions**
- **Steps for Identifying UAs and HFEs**
  - **Step 1: Construction of a table of the required functions for both the actual event and the misdiagnosed event**
  - **Step 2: Identification of UAs**
    - **For UA-1, Identify the essential functions for the actual event that are not those for the misdiagnosed event,**
    - **For UA-2, Identify the required functions that are not required by the actual event but are required by the misdiagnosed event**

Required functions for SLOCA (the actual event)		Required functions for ESDE (the misdiagnosed)	
On the PSA event sequence	On the EOP (LOCA)	On the PSA event sequence	On the EOP (ESDE)
Reactor trip	Reactor trip	Reactor trip	Reactor trip
HPSI	HPSI	(None)	HPSI
LPSI in case of HPSI failure	(None)	(None)	(None)
(None)	Isolation of LOCA	(None)	Isolation of faulted SG
RCS cooldown using SG	RCS cooldown using SG	RCS cooldown using SG	RCS cooldown using SG
RCS cooldown using SCS	RCS cooldown using SCS	RCS cooldown using SCS	RCS cooldown using SCS

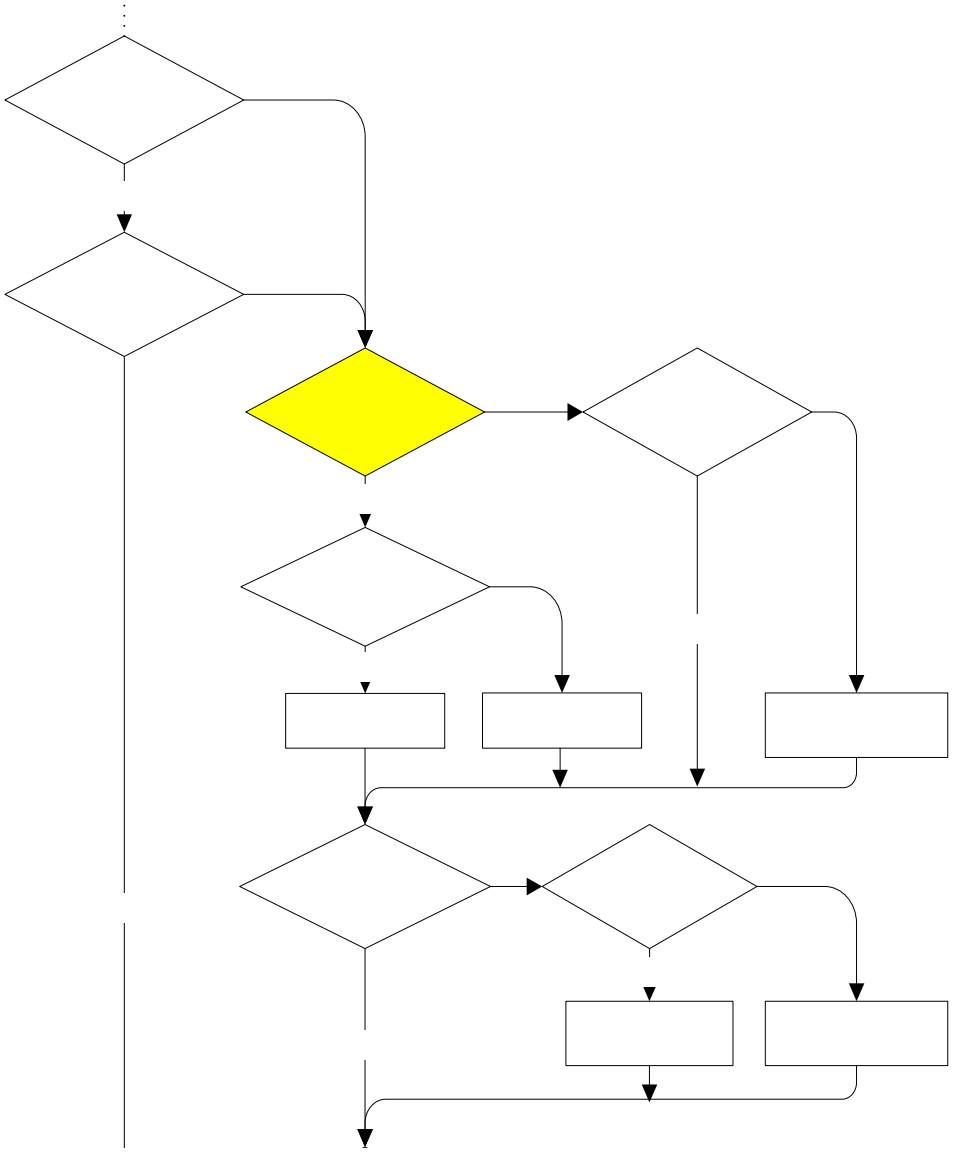
Method-Step 3: Quantification of HFEs

- **A Rough Quantification Scheme for Assessing a Risk Impact of Diagnosis Failures**
  - **Probability of a HFE = (Probability of a diagnosis failure) * (Probability of an unsafe action under the diagnosis failure) * (Probability of a non-recovery)**
  - **Probability of a diagnosis failure: already given**
- **Probability of an Unsafe Action**
  - **In the case that there is no procedural rules for the actions: 1.0**
  - **In the case that there are procedural rules for the actions:**
    - **Plant dynamics satisfy the procedural rules for committing UA: 1.0**
    - **Plant dynamics do not satisfy the procedural rules for committing UA: 0.1 ~ 0.05**
- **Probability of a Non-recovery [adapted from CBDTM]**

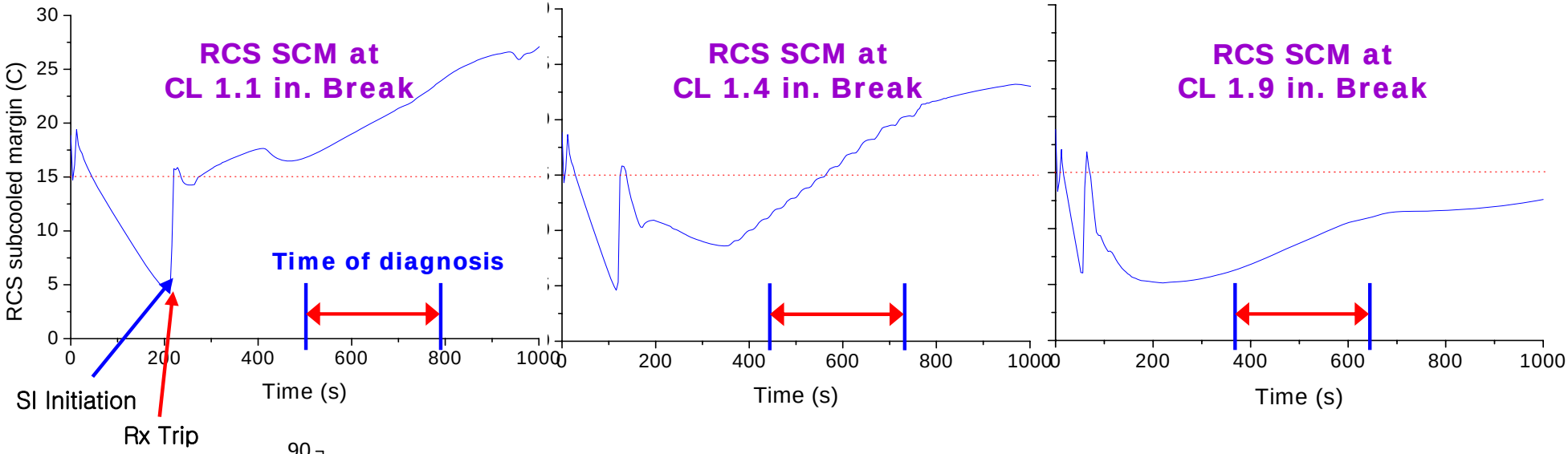
Recovery Path (RP)	Available time	Probability of non-recovery
RP1: The procedural guidance on the recovery	T_a > 30 min	0.2
RP2: The independent checking of the status of the critical safety functions	30 min < T_a < 1 hr T_a > 1 hr	0.2 0.1

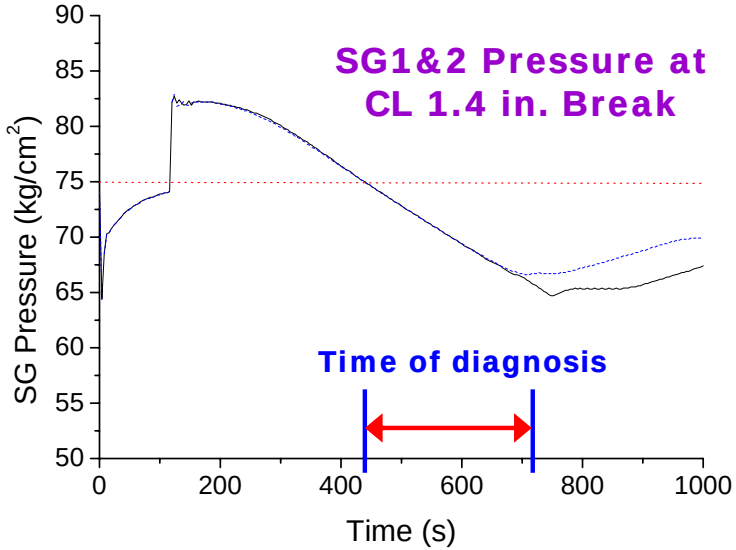
Case Study for SLOCA (Step 1)

- **Analysing PD**
  - Generally, SLOCA can be categorized into the RCS pipeline LOCA and the Pzr steam space LOCA
  - In this study, only the RCS pipeline LOCA is considered for an illustrative purpose
    - SLOCA Range: 0.38 in. ~ 1.91 in. (0.74 cm^2 ~18.58 cm^2)
  - Suspicious decision rules: the RCS subcooled margin (SCM)
  - T/H analysis using the MARS code
    - Condition: All charging and Safety Injection systems are operating normally
  - Results:
    - RCS SCM: In an increasing trend over the full range; 0.38 ~ 1.40 in. : > 15 ^oC (at the time of diagnosis)
    - SG Pressure: In a decreasing trend (a symptom of ESDE)



Case Study for SLOCA (Step 1)





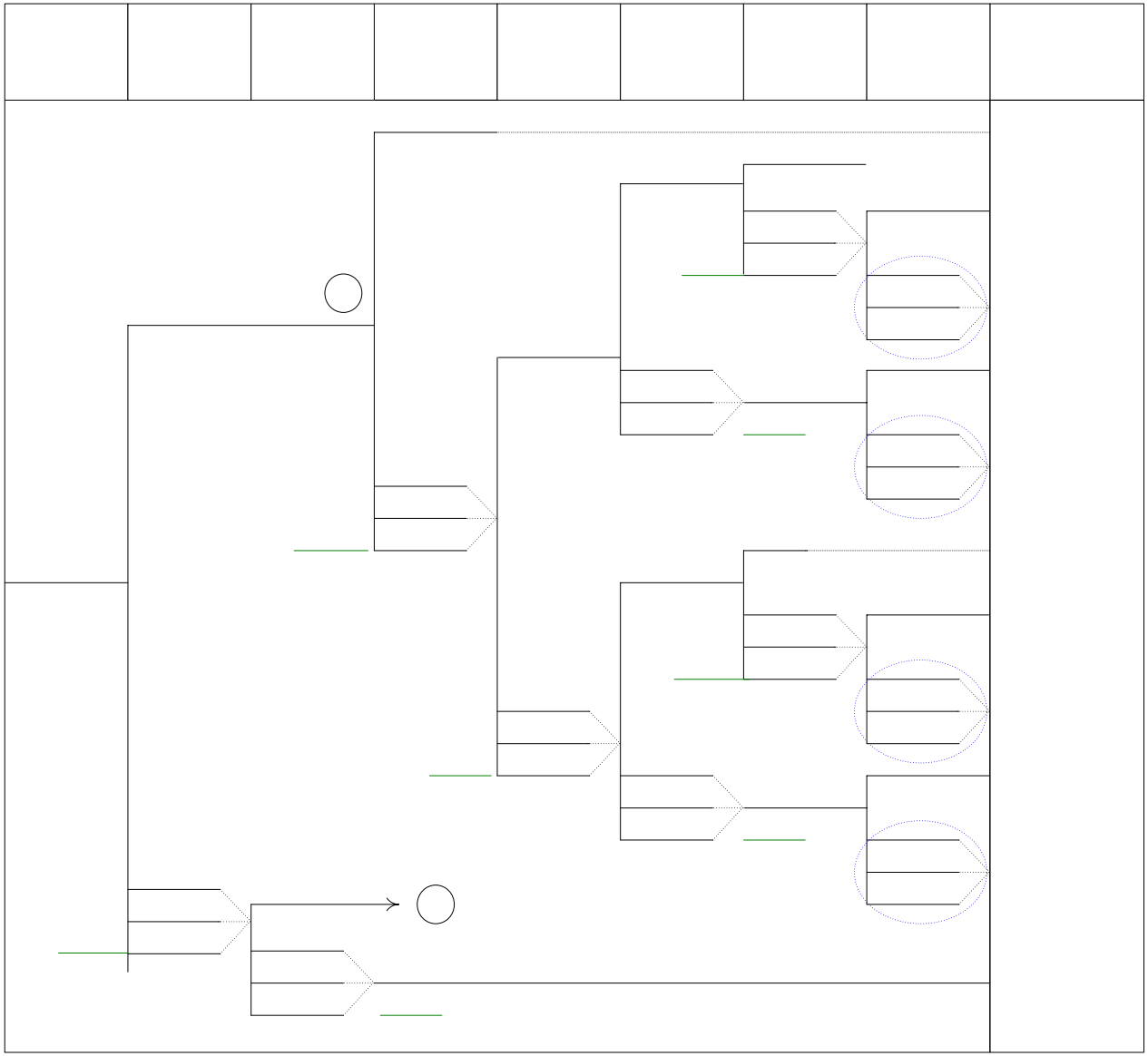
* **Diagnosis Rule**
  - **Is RCS SCM < 15 C and NOT rising?**
    - **Yes -> LOCA**
    - **No -> ESDE**
  - **Are both SG P > 75kg/cm² and constant or rising?**
    - **Yes -> Transient**
    - **No -> ESDE**

Case Study for SLOCA (Step 1)

- **Analysing OE**
  - Error probabilities are assigned at each decision point
- **Analysing IF**

Instrument	Failure rates	Q_{CCF}
Pressure	3.30e-07	**2.14e-04**
Level	5.10e-07	**3.31e-04**
Temp.	1.90e-06	**1.23e-03**
Radiation	1.06e-05	**3.82e-04**

- **Diagnosis Failure Probabilities**
  - **SLOCA->ESDE: 6.44E-03**
  - **SLOCA->GTRN: 3.0E-05**



Case Study for SLOCA (Step 2)

- **Identification of HFEs**
  - **Misdiagnosis as an ESDE**
    - **Premature termination of HPSI (EOC)**
    - **Failure to generate SIAS manually (EOO)**
    - **Failure to initiate an aggressive cooldown (EOO)**
    - **Isolation of the Intact SG (EOC)**
  - **Misdiagnosis as an GTRN**
    - **Premature termination of HPSI (EOC)**
    - **Failure to generate SIAS manually (EOO)**
    - **Failure to initiate an aggressive cooldown (EOO)**

Required functions for SLOCA (the actual event)		**Required functions for ESDE (the misdiagnosed)**	
On the PSA event sequence	On the EOP (LOCA)	On the PSA event sequence	On the EOP (ESDE)
Reactor trip	Reactor trip	Reactor trip	Reactor trip
HPSI	HPSI	(None)	HPSI
LPSI in case of HPSI failure	(None)	(None)	(None)
(None)	Isolation of LOCA	(None)	Isolation of faulted SG
RCS cooldown using SG	RCS cooldown using SG	RCS cooldown using SG	RCS cooldown using SG
RCS cooldown using SCS	RCS cooldown using SCS	RCS cooldown using SCS	RCS cooldown using SCS

Case Study for SLOCA (Step 3)

- **Quantification of HFEs**

Misdiagnosis	HFEs	Procedural rules for the action?	Plant dynamics?	Recovery potential		P(UA)[1] * P(NR)[2]
				Procedural guidance?	Indep't checking	
SLOCA -> ESDE	Premature termination of HPSI	Yes	Yes	Yes: (T_a > 30 min)	T_a > 1 hr	**2.0E-2**
	Failure to generate SIAS manually	Yes	No	Yes (T_a > 30 min)	T_a > 1 hr	**2.0E-3 ~ 1.0E-3**
	Failure to initiate aggressive cooldown	No	N/A	No	T_a < 30 min	**1.0**
	Isolation of the Intact SG	Yes	No	No	No	**0.1 ~ 0.05**
SLOCA -> GTRN	Premature termination of HPSI	Yes	Yes	Yes (T_a > 30 min)	T_a > 1 hr	**2.0E-2**
	Failure to generate SIAS manually	Yes	No	Yes (T_a > 30 min)	T_a > 1 hr	**2.0E-3 ~ 1.0E-3**
	Failure to initiate aggressive cooldown	No	N/A	No	T_a < 30 min	**1.0**

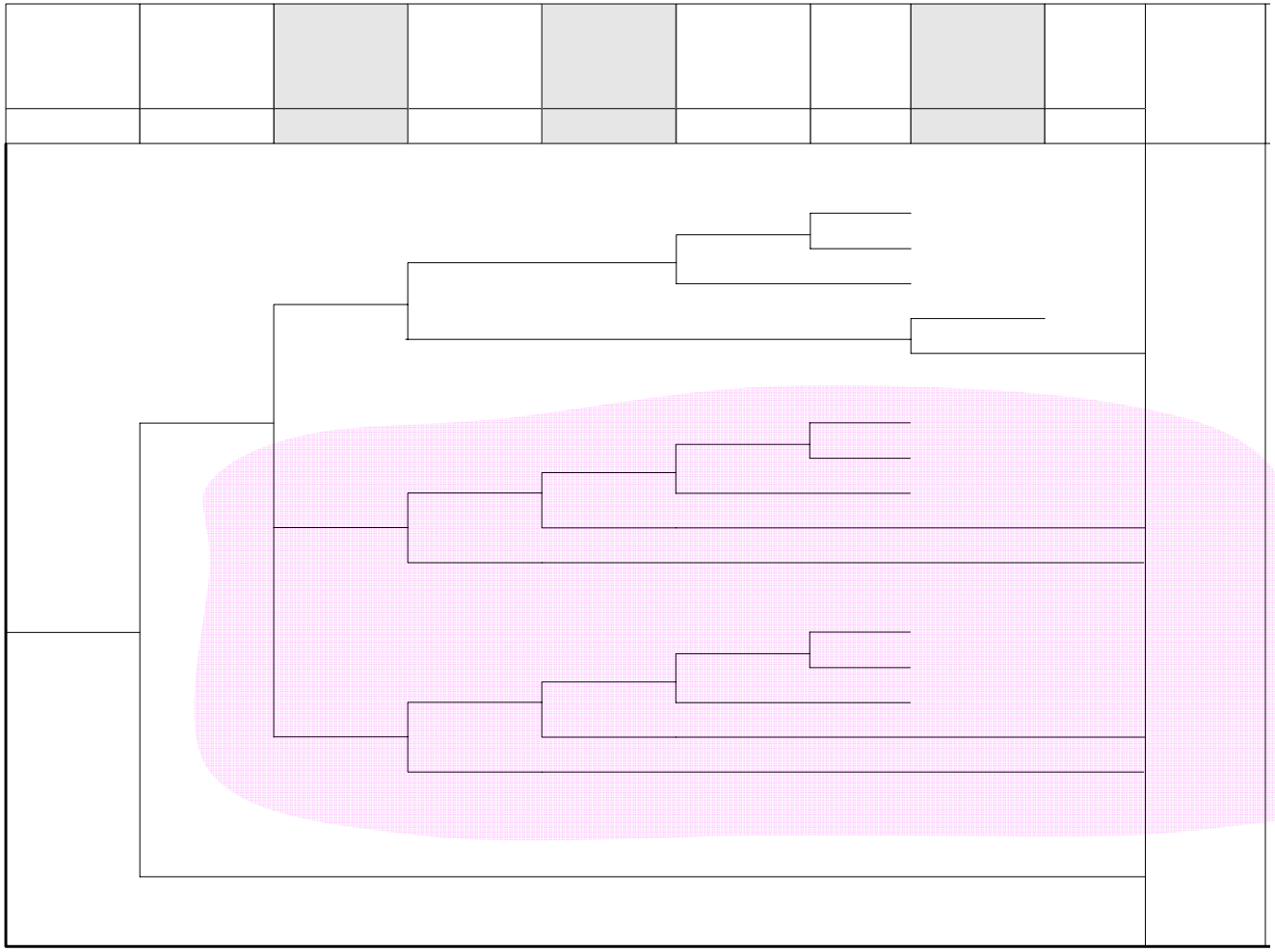
1. P(UA): Probability of performing an unsafe action under the diagnosis failure
2. P(NR): Probability of non-recovery

Case Study for SLOCA (Modeling into PSA)

- **Modeling into PSA**
  - Premature termination of HPSI (*ET*)
  - Failure to initiate an aggressive cooldown (*ET*)
  - Failure to generate SIAS manually (*FT*)
  - Isolation of the Intact SG (*not modeled*)
- **Risk Impact of Diagnosis Failures**
  - CDF of the misdiagnosis event sequences:

    4.0E-7

    (5.4% of total CDF)



Conclusions

- ***The MDTA-based Method***
  - **An MDTA-based method for assessing the potential for diagnosis failures and their risk impacts was introduced.**
  - **The MDTA method is a structured one for identifying possible diagnosis paths and combinations of causes leading to misdiagnosis esp. for a flowchart-based diagnostic procedure**
- ***Pilot Application to SLOCA***
  - **According to the pilot application to the SLOCA event, the risk impact of diagnosis failure seems not to be negligible**
  - **Effective measures need to be developed to reduce or eliminate the possibility of diagnosis failures, which may include a revision of the diagnostic procedure or training program**