시뮬레이터 훈련자료를 활용한 resilience engineering 기반 인적오류 영향인자 분석방안

2016.10.26

한국원자력연구원
박진균

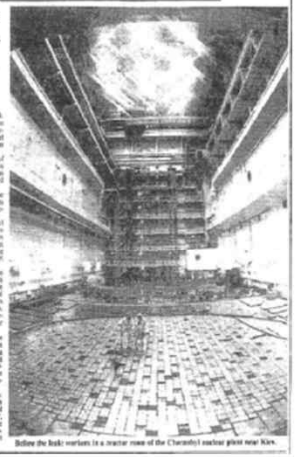
인적오류 (human error)와 대형시스템 안전성

THE TIMES

TUESDAY APRIL 29 1986

Alert 1,000 miles away in Sweden after Moscow admits casualties

Huge nuclear leak at Soviet plant



The Nuclear Accident

Radiation Continues To Leak From Crippled Plant

HARRISBURG, Pa. (AP) — Radiation leaks from the Three Mile Island nuclear power plant continued today, authorities said, as a debate grew over what was described as one of the most serious such incidents in this country's history.

"The vapor that is now going into the atmosphere is from a sump pump and is only mildly radioactive within accepted limits," said Don Curry, a spokesman for the Metropolitan Edison Co., owner of the plant. The pump is designed to remove water after it has cooled the reactor.

"We concede that it's not just a little thing," Curry said. "In terms of publicity it will probably surpass the Browns Ferry incident."

Until now, a March 1975 fire in the control room of the Browns Ferry nuclear plant in Alabama has generally been considered this nation's most dangerous incident involving a nuclear reactor.

Low level radiation was detected in the air as far as 16 miles away after an apparent valve failure Wednesday morning resulted in excessive pressure being built up in the water used to cool the reactor core at Three Mile Island.

"Some of the water vapor, through the venting system, went into the atmosphere," Curry said.

Curry said the latest radiation measurements outside the plant were at two to three millirems. Individuals are exposed to up to 30-millirems in a single X-ray examination.

Walter Creitz, president of Metropolitan Edison, said on ABC-TV's *Good Morning America* show this morning that the plant shut down safely and that the level of radiation released "would not endanger or injure any people."

Creitz said his company did not know what equipment had been disabled or what precisely caused the accident.

An aerial view of the Three Mile Island nuclear power plant. AP Photo

JAPAN'S NUCLEAR NIGHTMARE

Herald Sun

Stories start here.

MELTDOWN

Radiation spews from crippled power plant

Tens of thousands ordered to evacuate

AUSSIE EXODUS FROM THE DANGER ZONE: SPECIAL REPORTS & PICTURES – PAGES 2-7

원전 안전성 평가: 두 가지 관점

- **결정론적 관점**
  - ✓ 설계기준사고 (DBA) 및 설계기준 초과사고 (BDBA) 상황 시 보수적인 열수력학적 분석을 통해 시스템에서 요구하는 안전성 지표 (PCT 등)의 만족여부를 평가
  - ✓ 평가 결과: 만족/불만족 (YES/NO)
  - ✓ 직관적 평가결과 제공
  - ✓ 통합적 평가의 어려움
- **확률론적 관점**
  - ✓ DBA 및 BDBA의 대응과 완화를 위해 필요한 안전계통의 기능상실을 해당 계통에 포함된 기기고장 및 인간오류 확률로 모델링 한 후 사고 대응 및 완화 실패 가능성을 평가
  - ✓ 평가 결과는 노심손상빈도 (CDF)
  - ✓ 통합적 안전성 평가 가능
  - ✓ 많은 신뢰도 자료 필요

인적오류 방지: 두 가지 접근방향

Deterministic

- **Human Factors (HF) Eng. or Ergonomics**
  - ✓ "… is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance." [International Ergonomics Association]

Probabilistic

- **Focusing on critical tasks**
- **Human reliability analysis (HRA)**
  - ✓ Which human action can go wrong?
  - ✓ How likely is it?
  - ✓ If it does happen, what is its consequence?
- **Providing direct input for PSA (Probabilistic Safety Assessment)**

인간공학 관점

무질서한 기기배치, 가독성이 떨어지는 label, 일관성이 없는 설계 (stereotype 배치) 때문에 효율적인 직무 수행이 어려운 HMI (Human Machine Interface)이다.

무조건적인 설계 변경 또는 개선

유사한 인적오류 영향인자 목록 (Performance Shaping Factor, PSF) 고려

https://msquair.files.wordpress.com/

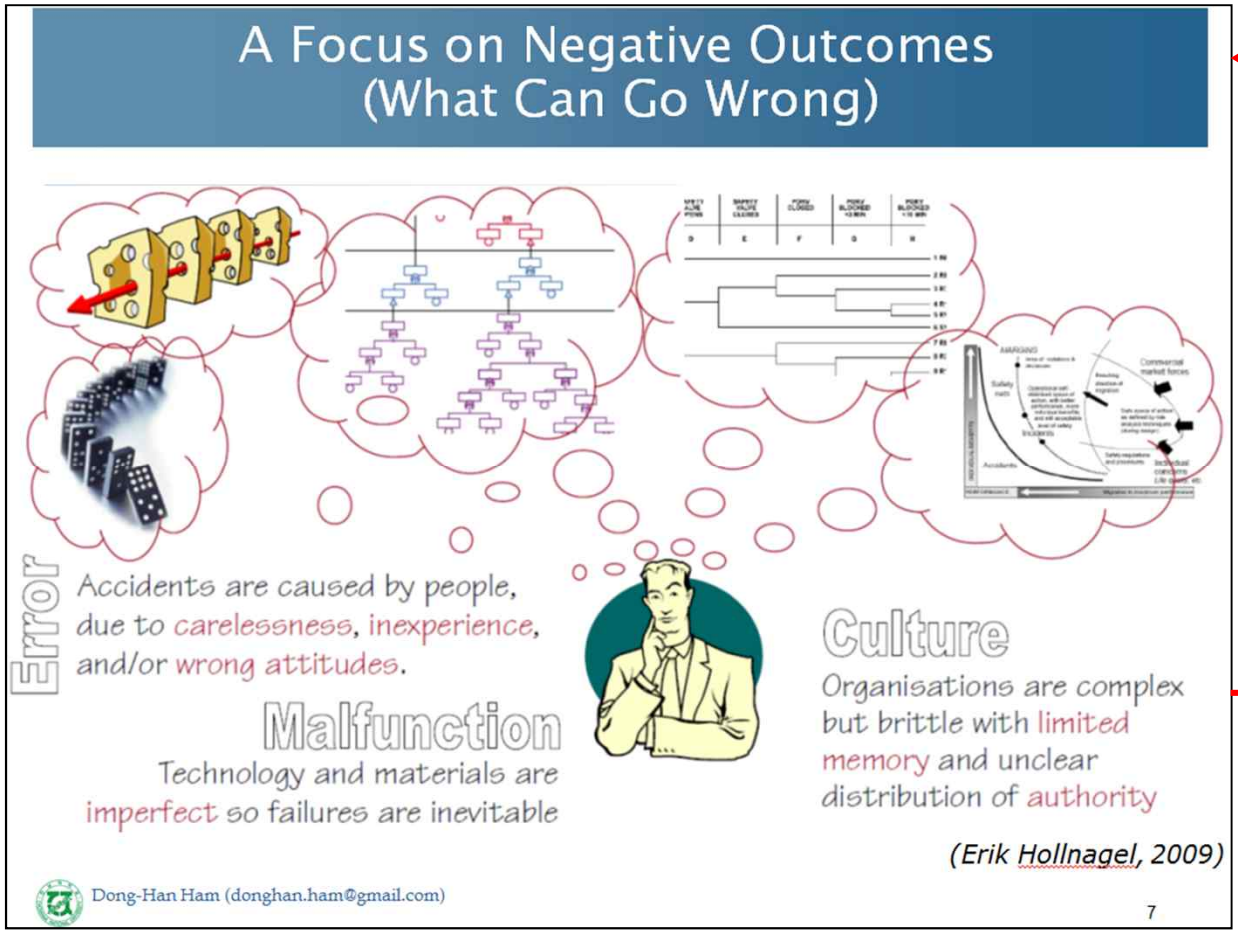
인간신뢰도분석 관점

무질서한 기기배치, 가독성이 떨어지는 label, 일관성이 없는 설계 (stereotype 배치) 등으로 인해 관련 직무 수행 오류 확률은 평균 인간오류확률 대비 10배로 예상된다.

PSA 입력 및 CDF 영향에 따른 설계개선

공통적으로 요구되는 인적오류 자료

Resilience engineering* (1/4)



*내부발표자료, 함동한, Introduction to Safety-II & Resilience Engineering, 2016-07-13

Resilience engineering (2/4)

- **Safety-I 관점**
  - ✓ Safety is the condition where the number of adverse outcomes (accidents/incidents/ near misses) is as low as possible.
  - ✓ Safety-I is achieved by trying to make sure that things do not go wrong, either by eliminating the causes of malfunctions and hazards, or by containing their effects.

- **Safety-II 관점**
  - ✓ Safety is a condition where the number of successful outcomes is as high as possible.
  - ✓ It is the ability to succeed under varying conditions.
  - ✓ Safety-II is achieved by trying to make sure that things go right, rather than by preventing them from going wrong.

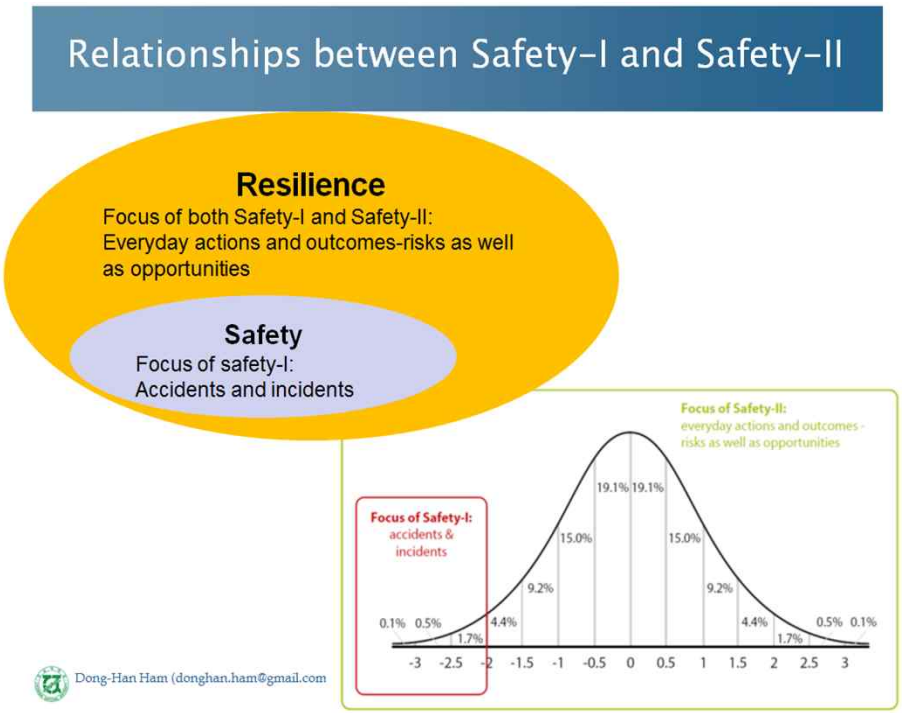
Resilience engineering (3/4)

Safety-I vs Safety-II

	Safety-I	Safety-II
Definition of safety	That as few things as possible go wrong.	That as many things as possible go right.
Safety management principle	Reactive, respond when something happens or is categorised as an unacceptable risk.	Proactive, continuously trying to anticipate developments and events.
View of the human factor in safety management	Humans are predominantly seen as a liability or hazard.	Humans are seen as a resource necessary for system flexibility and resilience.
Accident investigation	Accidents are caused by failures and malfunctions. The purpose of an investigation is to identify the causes.	Things basically happen in the same way, regardless of the outcome. The purpose of an investigation is to understand how things usually go right as a basis for explaining how things occasionally go wrong.
Risk assessment	Accidents are caused by failures and malfunctions. The purpose of an investigation is to identify causes and contributory factors.	To understand the conditions where performance variability can become difficult or impossible to monitor and control.

(Hollnagel et al., 2013)

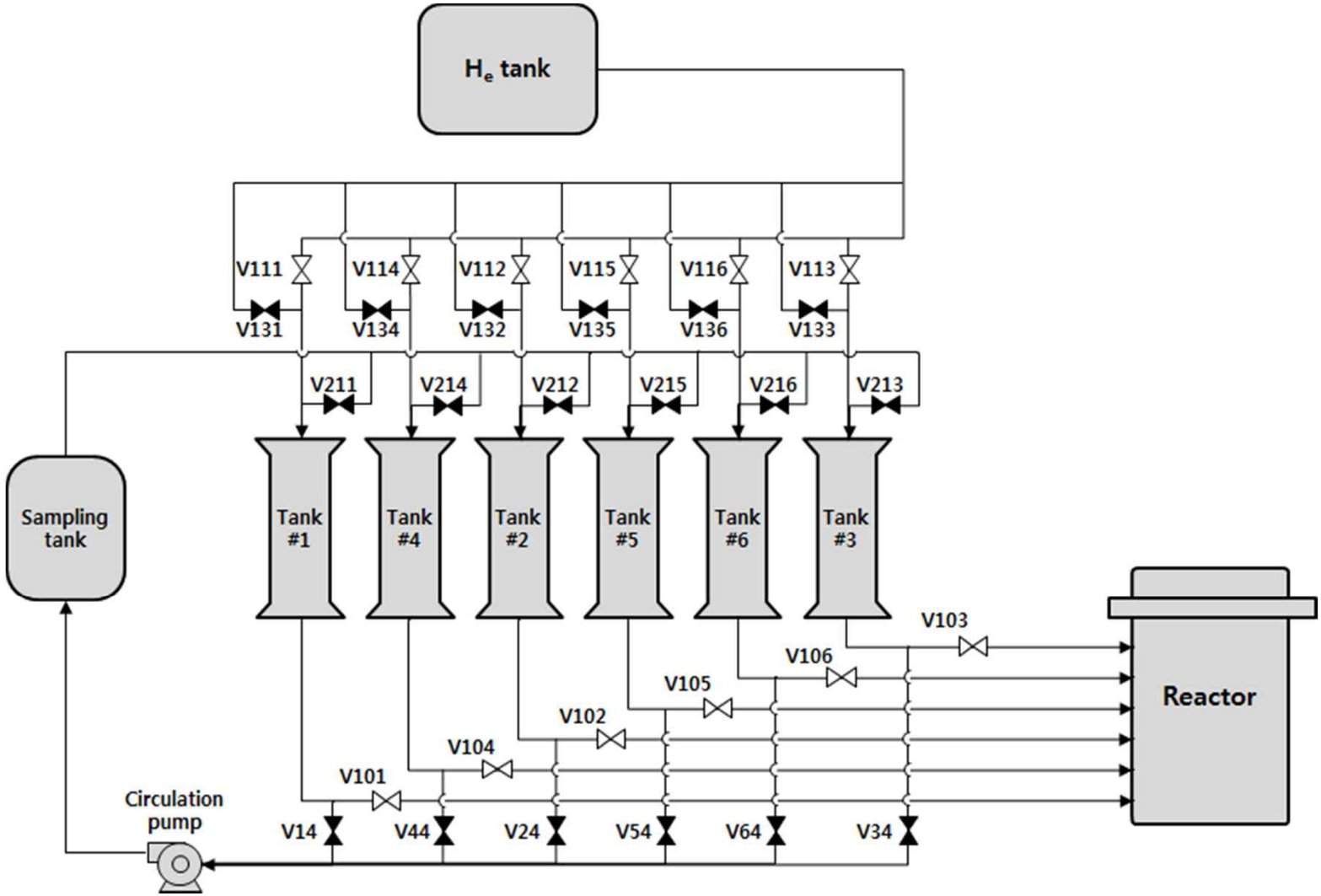
Resilience engineering (4/4)



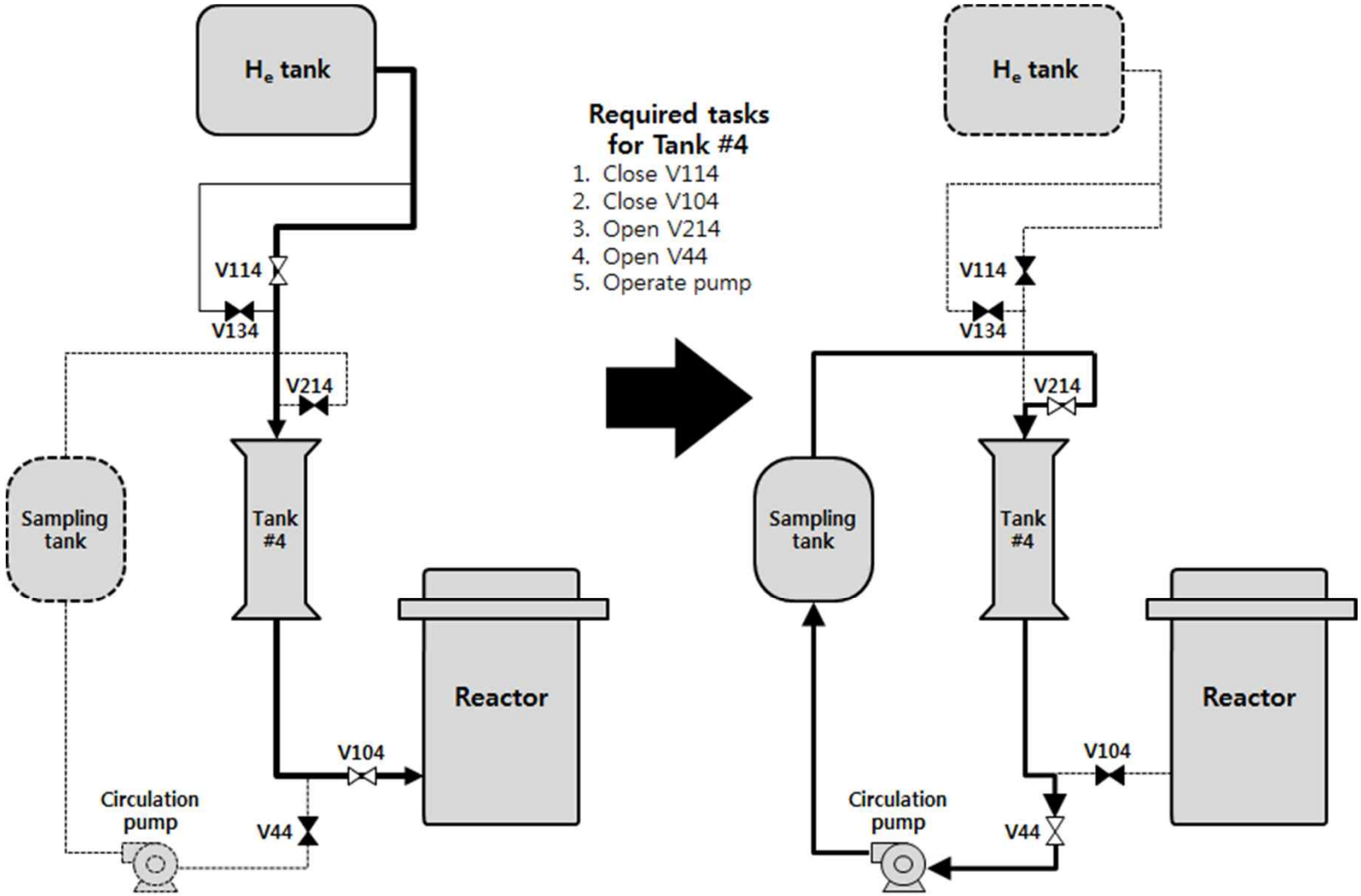
Concurrent analysis of both success and failure cases.

- **Resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions**
- **Resilience engineering is the scientific discipline that focuses on developing the principles and practices that are necessary to enable systems to be resilient.**
- **The aim of the resilience engineering is to integrate both Safety-I and Safety-II.**

분석 예시


He tank
V111
V114
V112
V115
V116
V113
V131
V134
V132
V135
V136
V133
V211
V214
V212
V215
V216
V213
Sampling tank
Tank #1
Tank #4
Tank #2
Tank #5
Tank #6
Tank #3
V103
V106
V105
V102
V104
V101
Circulation pump
V14
V44
V24
V54
V64
V34
Reactor

분석 예시


He tank
V114
V134
V214
Sampling tank
Tank #4
Reactor
V104
Circulation pump
V44
Required tasks for Tank #4
1. Close V114
2. Close V104
3. Open V214
4. Open V44
5. Operate pump
He tank
V114
V134
V214
Sampling tank
Tank #4
Reactor
V104
Circulation pump
V44

분석 예시

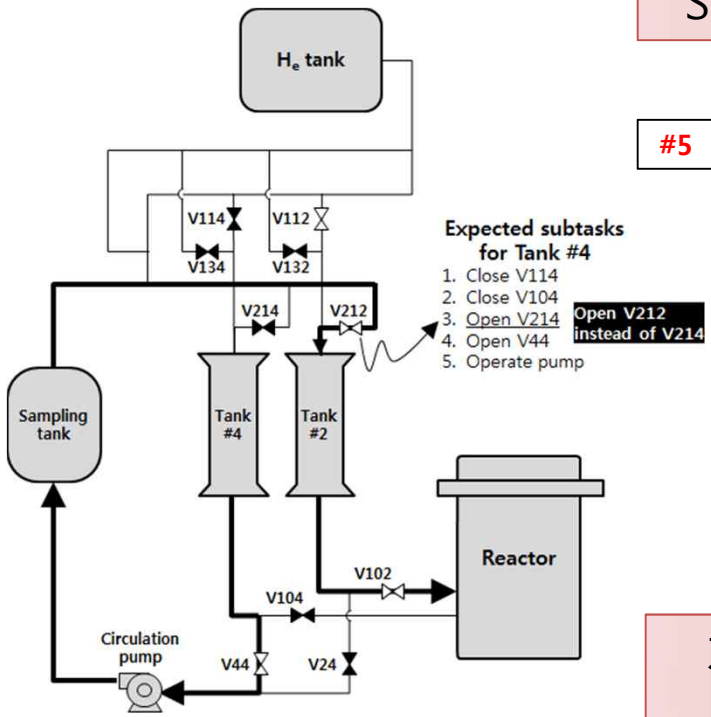
10회 훈련 시뮬레이션 중 1회 오류 발생

분석 → 정보표시(1) | 제어기능(2) | 경보(3) | 환경(4) | 의사소통(5) | 작업감독(6) ●●●

Safety-II 관점 자료수집

	(1)	(2)	(3)	(4)	(5)	(6)
#1	No	Yes	Yes	Good	Bad	Good
#2	Yes	No	Yes	Good	Bad	Good
#3	Yes	Yes	No	Bad	Bad	Good
#4	Yes	Yes	Yes	Good	Good	Good
#5	Yes	Yes	Yes	Good	Good	Bad
●●●						
#10	No	Yes	No	Good	Good	Good

광범위한 자료 수집 → Big data 분석 가능



Safety-I 관점 자료수집

	(1)	(2)	(3)	(4)	(5)	(6)
#5	Yes	Yes	Yes	Good	Good	Bad

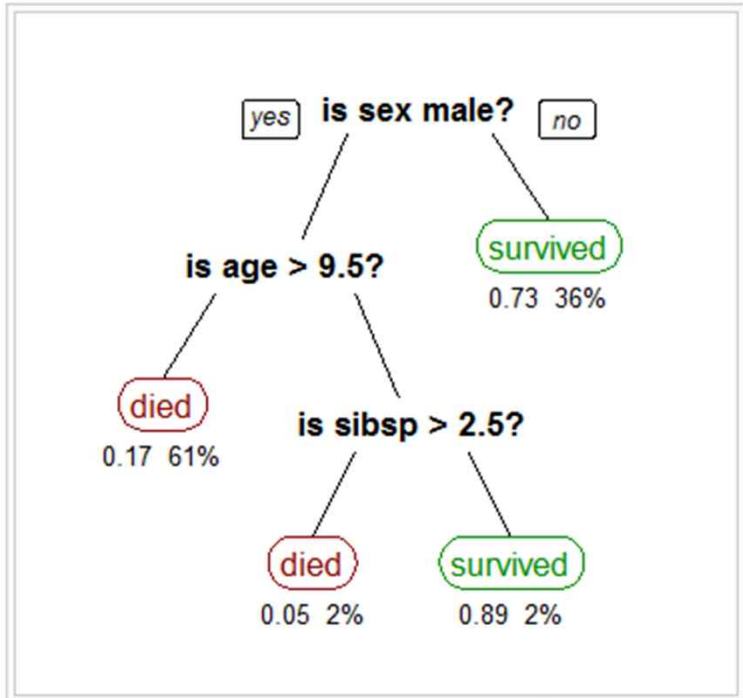
제한된 자료 수집 → 분석결과 의미 축소

Big data 분석
(CART; Classification and Regression Tree)

No	Gender	Age	Spouses	Siblings	Died?
1	Male	15	0	1	Y
2	Male	8	0	2	Y
3	Female	23	1	3	N
4	Female	4	0	0	N
…					

- 자료가 많을수록 분석정확도 급격히 증가
- 다양한 이론 및 분석 방법 제안됨 (deep machine learning; Alpha GO)

CART



A tree showing survival of passengers on the Titanic ("sibsp" is the number of spouses or siblings aboard). The figures under the leaves show the probability of survival and the percentage of observations in the leaf.

Source: wikipedia

위급한 상황에서 여자는 남자에 비해 생존 가능성이 1.75배 높다 (36% vs. 63%)
→ PSF A와 B 상황에서 오류 발생 가능성은 XX배 높아진다.

Big data 분석결과 예시

운전모드	Normal	1.0
	Abnormal	1.8
	Emergency	5.9
추가 고장기기	없음	1.0
	있음	9.7
절차서-상황 적합성 (conformity)	예	1.0
	아니오	3.9
절차서에 명확한 기기가 기술	예	1.0
	아니오	12.6
Feedback Information 제공	예	1.0
	아니오	95.9

● ● ●

1	Sim/Evt Environment	Sim/Evt Mode	MultipleInitEvent	FailedSys/Comp	TimePressure	ProcConformity
47181	No	Emergency	No	No	Before diagnosis	Yes
47182	No	Emergency	No	No	Before diagnosis	Yes
47183	No	Emergency	No	No	Before diagnosis	Yes
47184	No	Emergency	No	No	Before diagnosis	Yes
47185	No	Emergency	No	No	Before diagnosis	Yes
47186	No	Emergency	No	No	Before diagnosis	Yes
47187	No	Emergency	No	No	Before diagnosis	Yes
47188	No	Emergency	No	No	Before diagnosis	Yes
47189	No	Emergency	No	No	Before diagnosis	Yes
47190	No	Emergency	No	No	Before diagnosis	Yes
47191	No	Emergency	No	No	Before diagnosis	Yes
47192	No	Emergency	No	Yes	Before diagnosis	Yes
47193	No	Emergency	No	Yes	Before diagnosis	Yes
47194	No	Emergency	No	Yes	Before diagnosis	Yes
47195	No	Emergency	No	Yes	Before diagnosis	Yes
47196	No	Emergency	No	Yes	Before diagnosis	Yes
47197	No	Emergency	No	Yes	Before diagnosis	Yes
47198	No	Emergency	No	Yes	Before diagnosis	Yes
47199	No	Emergency	No	Yes	Before diagnosis	Yes
47200	No	Emergency	No	Yes	Before diagnosis	Yes
47201	No	Emergency	No	Yes	Before diagnosis	Yes
47202	No	Emergency	No	Yes	Before diagnosis	Yes
47203	No	Emergency	No	Yes	Before diagnosis	Yes
47204	No	Emergency	No	Yes	Before diagnosis	Yes
47205	No	Emergency	No	Yes	Before diagnosis	Yes
47206	No	Emergency	No	Yes	Before diagnosis	Yes
47207	No	Emergency	No	Yes	Before diagnosis	Yes
47208	No	Emergency	No	Yes	Before diagnosis	Yes
47209	No	Emergency	No	Yes	Before diagnosis	Yes
47210	No	Emergency	No	Yes	Before diagnosis	Yes
47211	No	Emergency	No	Yes	Before diagnosis	Yes
47212	No	Emergency	No	Yes	Before diagnosis	Yes
47213	No	Emergency	No	Yes	Before diagnosis	Yes
47214	No	Emergency	No	Yes	Before diagnosis	Yes
47215	No	Emergency	No	Yes	Before diagnosis	Yes
47216	No	Emergency	No	Yes	Before diagnosis	Yes
47217	No	Emergency	No	Yes	Before diagnosis	Yes
47218	No	Emergency	No	Yes	Before diagnosis	Yes
47219	No	Emergency	No	Yes	Before diagnosis	Yes
47220	No	Emergency	No	Yes	Before diagnosis	Yes
47221						
47222						

결론

- **객관적 근거자료 수집 중요성**
  - ✓ HF와 HRA 분야에서 가장 큰 현안 중 하나는 부족한 자료로 인한 분석결과의 높은 불확실성
  - ✓ 인적수행도 자료의 적극적 수집 필요
- **KAERI에서는 시뮬레이터 훈련자료 및 사건분석보고서를 근간으로 일상, 비정상 및 비상 상황에 대한 인적수행도 자료 수집 중**
  - ✓ Big data 분석기법 적용을 통해 Safety-II 관점의 결과 도출
  - ✓ Resilience engineering 측면에서, HF 및 HRA 지원을 위한 현실적인 분석결과 제공 기대

감사합니다

Q & A

국가 미래 에너지를 책임지는 연구원

한국원자력연구원
Korea Atomic Energy Research Institute

Functional Resonance Analysis Method (FRAM)

- To predict how resonance may lead to accidents, we must be able to describe and model the characteristic variability of the system
  → Functional resonance

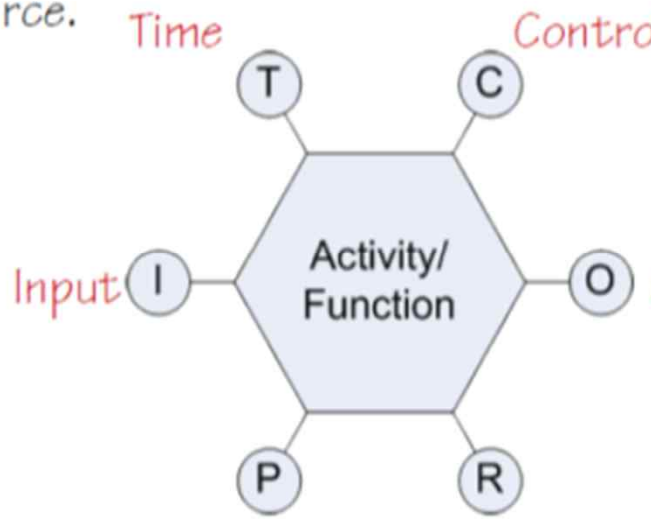
- (Functional) Resonance:
  A principle that explains how disproportionate large consequences can arise from seemingly small variations in performance and conditions .

Resilience engineering claims that we should an accident as emergent outcome rather than resultant outcome; A proper way for explaining emergence is the concept of functional resonance, which is the basis of Functional Resonance Analysis Method (FRAM).

Six Aspects of a Function: FRAM Functional Unit

Time available: This can be a constraint but can also be considered as a special kind of resource.

That which supervises or adjusts a function. Can be plans, procedures, guidelines or other functions.



That which is used or transformed to produce the output. Constitutes the link to previous functions.

That which is produced by function. Constitute links to subsequent functions.

System conditions that must be fulfilled before a function can be carried out.

That which is needed or consumed by function to process input (e.g., matter, energy, hardware, software, manpower).

(Erik Hollnagel, 2010)

Example of Instantiation of FRAM Model