위해도 분석 결과의 효과적인 확인을 위한 추적성 기반 위해도 모델

정세진, 유준범

Dependable software laboratory
건국대학교

목차

- 서론
- 위해도 분석 (hazard analysis)
- 추적성 기반 위해도 모델 (hazard model)
  - 위해도 분석 기법의 추상화된 모델
  - 기법의 연결 관계 분석 및 메타모델
  - 사례 연구
- 결론 및 향후 연구

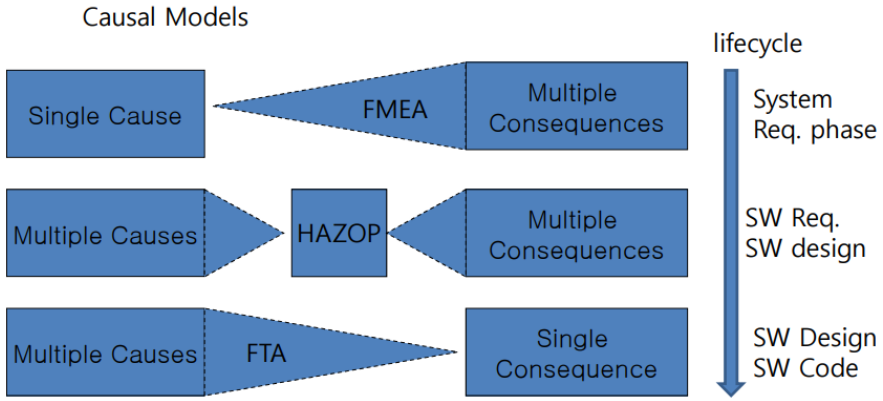
서론

- 안전필수 시스템 (Safety critical system)
  - 사용 전 safety analysis를 통한 안전성의 입증이 필수 (기능안전성 표준에 의거)
    - 상위 수준의 시스템을 대상으로 hazard analysis를 수행하고 safety requirement를 할당

Hazard: '*A potential source of harm*' (IEC 61508)
Hazard analysis: system/software의 잠재적인 위험에 대한 분석 (제거/경감/회피를 위함)

  - 안전성이 중요한 시스템/소프트웨어 개발 시 위해도 분석이 중요함
    - 다양한 기법들이 각자의 목적에 따라 시스템/소프트웨어에 각각 독립적으로 적용되기도 함

- 현대의 시스템은 규모나 복잡도가 과거에 비해 크게 증가
  - 과거에 비해 시스템/소프트웨어의 개발 생명 주기에 따라 **여러 단계에 다양한 hazard analysis들이 수행됨**
  - 시스템 이론에 따른 다양한 상호작용의 failure 확인 등 중요 요소들이 변화함



Focused HA through lifecycle
Harmonized (top-down and bottom-up) HA
Means-ends and whole-part traceability analysis of safety requirements

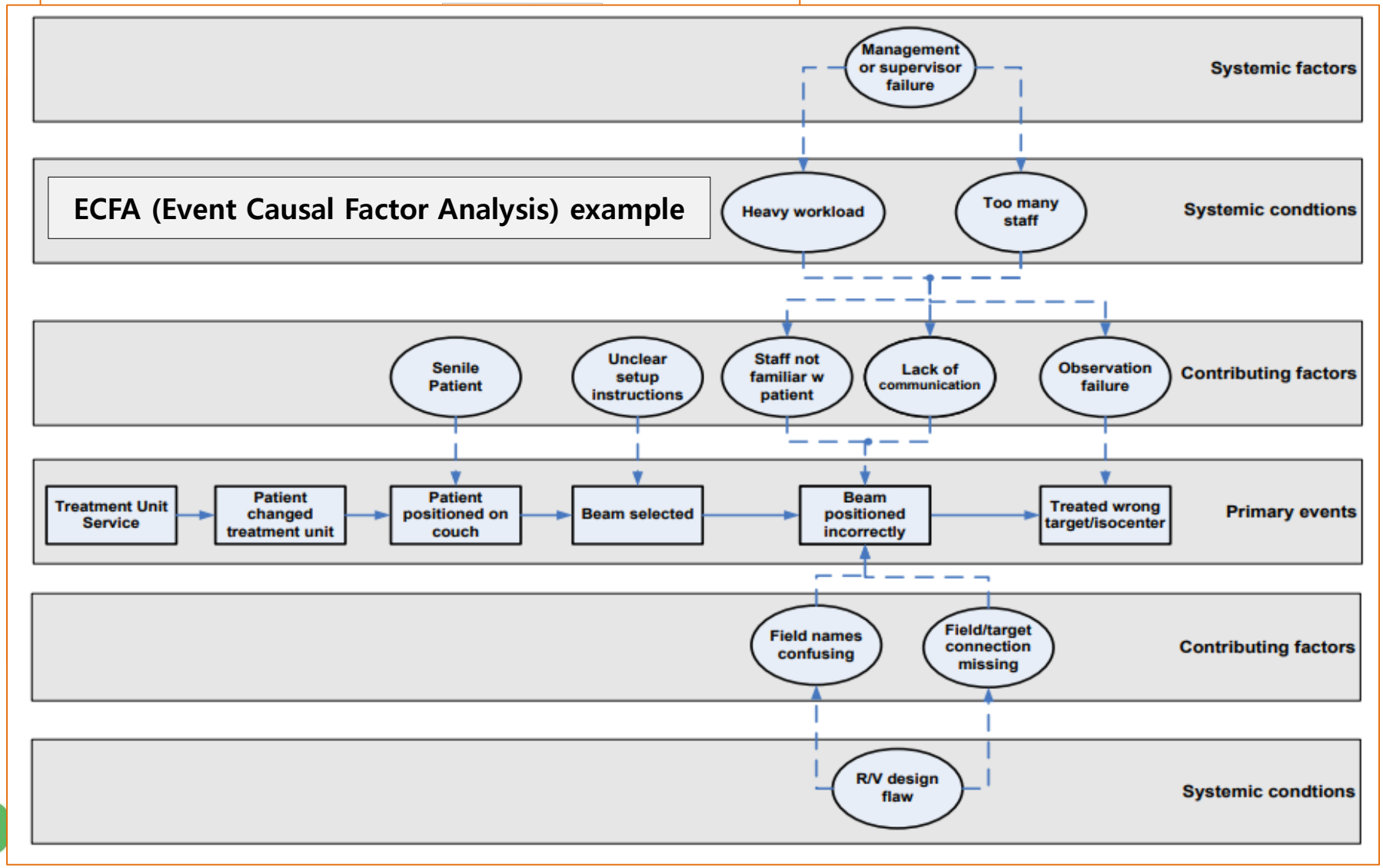
서론

- 적용되는 다양한 기법들 사이에는 여러 관계들이 성립
  - Cause-consequence chain의 추적성, 서로 다른 item에서의 failure (CCF) 등
  - 하지만 이에 대해 작성 및 모델링하는 연구는 부족
    - Safety life-cycle 상에서 개발 산출물 과의 추적성 분석
    - 시스템 계층 구조 별 독립적 적용
- 본 논문에서는 **추적성을 기반**으로 한 위해도 **모델**을 제안
  - 위해도 분석의 추상화 모델 및 메타모델 제안
  - 추적성을 기반으로 시스템/소프트웨어의 다양한 위해도 분석 결과의 상관 관계 분석
    - 각 독립적인 위해도 분석 결과의 관계 정보 표현
    - 위해도 분석의 다각적인 결과 확인

배경 지식

- **Hazard analysis**
  - *"A process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond plant design basis events by including **abnormal events** and **plant operations** with degraded equipment and plant systems."*
  - 시스템/소프트웨어의 사고/risk가 될 수 있는 잠재적인 위험을 분석하는 방법
- 다양한 기법들이 개발되어 적용
  - FMEA, FTA, STPA, 등
  - 목적에 따라 특정 방법을 사용
    - State machine analysis
    - Safety case 등
  - (+ 통합 사용을 위한 연구 또한 진행)

- Hazard analysis에는 다양한 기법들이 개발되어 적용됨
  - **FMEA, FTA, HAZOP**
  - **STPA, Safety case, ECFA 등**



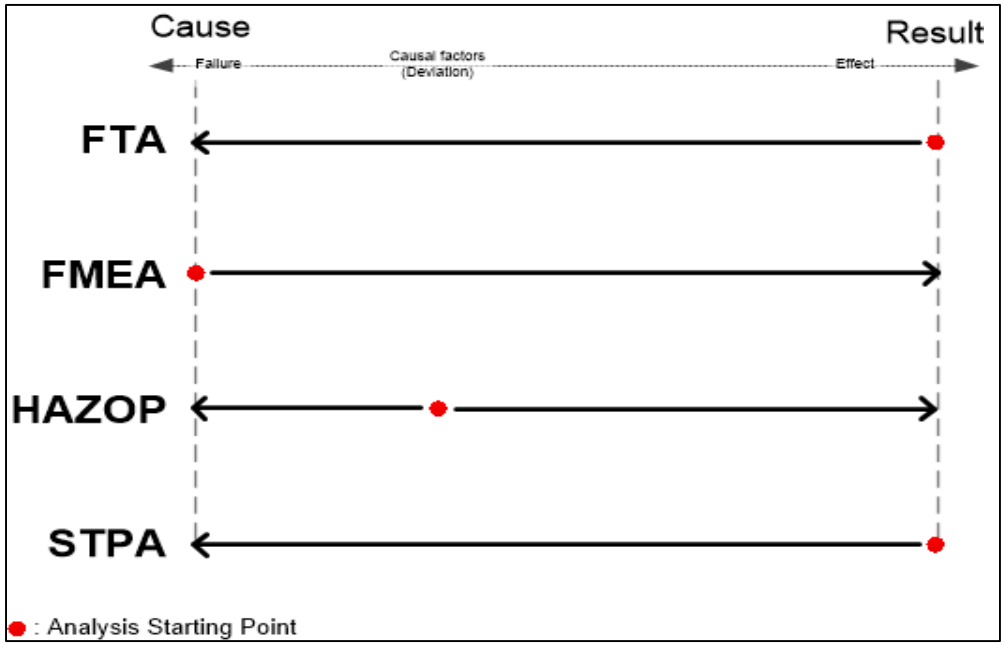
위해도 분석 기법의 추상화된 모델

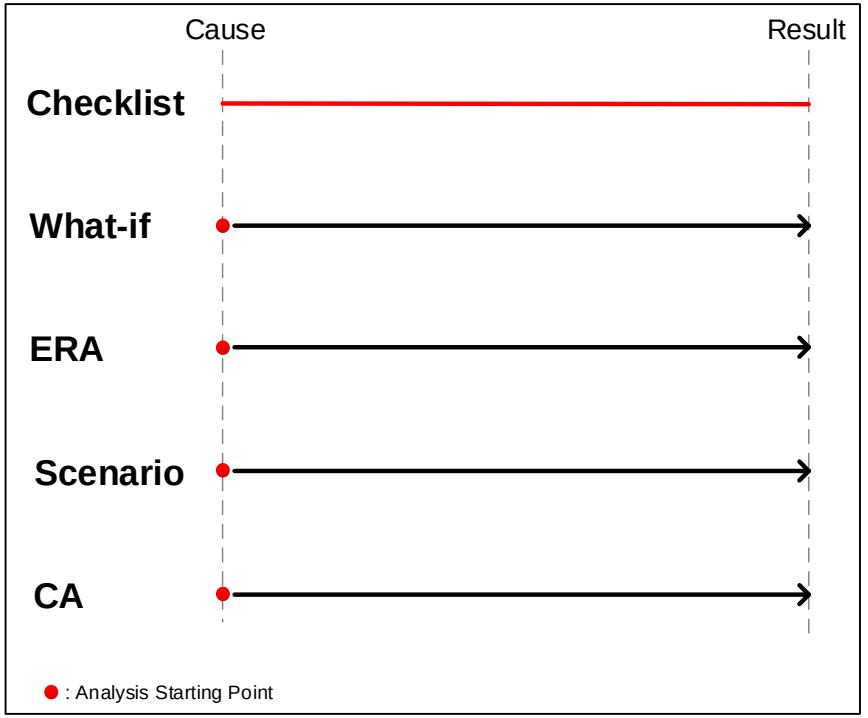
- 각 분석 기법을 추상화 화여 모델링
  - Hazard 모델을 만들기 위해서는 우선 각 분석 기법의 요소를 분석할 필요가 있음
  - 기법의 분석 방법/컨셉에 따라 분류

1. Tree-based	2. Worksheet-based
Tree 형태의 다이어그램을 이용하는 분석 기법 **FTA** **ETA** **Cause consequence analysis** **MORT**	Worksheet table을 이용하는 분석 기법 **FMEA** **HAZOP** **PHA/PHL** **Fault hazard analysis** **System hazard analysis** ~~(Safety requirement/criteria analysis)~~
3. Other diagram	**4. Others**
기타 다이어그램 이용하는 분석 기법 **Event and causal factor analysis** **Sequentially-timed event plot** ~~(Petri net analysis)~~ ~~(Sneak circuit analysis)~~ ~~(State machine hazard analysis)~~ ~~(Purpose graph analysis)~~ **STPA (별개)**	그 외 시나리오 분석 **Checklist** **Scenario analysis** **What-if analysis** (Change analysis) ~~(Interface analysis)~~ ~~(Repetitive failure analysis)~~ **Safety case (별개)**

- **시작점 분석 및 요소 추출 기반의 추상화 모델**
  - 추상화 모델의 요소 추출을 위해 시작점 분석을 수행

- 시작점 분석: hazard analysis의 분석 시작/목적 (cause-result)에 대한 분석





- **각 분석 기법을 추상화 화여 모델링**
  - 분석 시 필수적으로 나타나는 element를 기준으로 표현하여 모델링 가능
  - 다양한 위해도 분석 기법의 요소들을 추상화 하여 하나의 모델로 분류하여 표현

Tree diagram: tree 요소

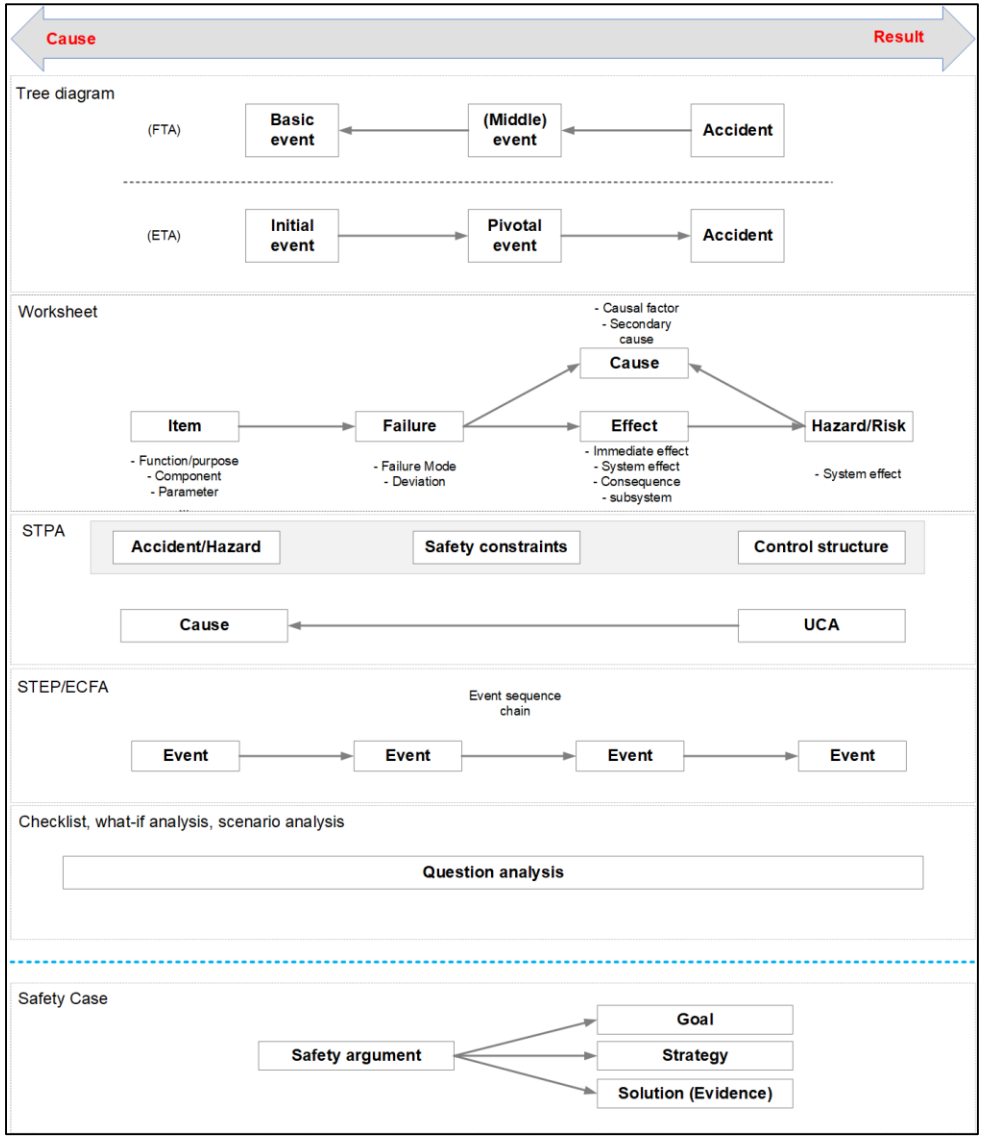
Worksheet: table 요소들

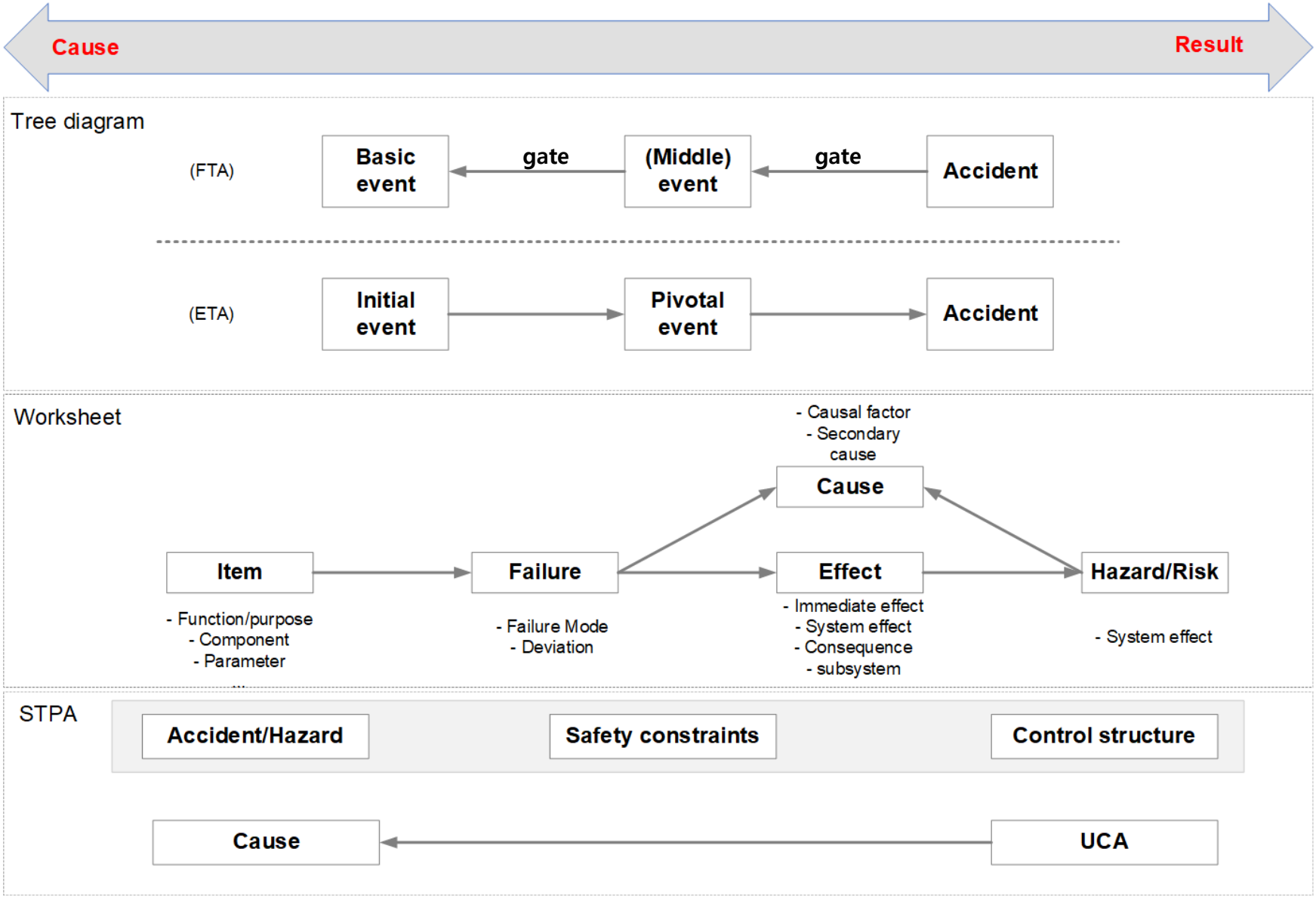
STPA: 분석 요소들

STEP/ECFA: event 요소

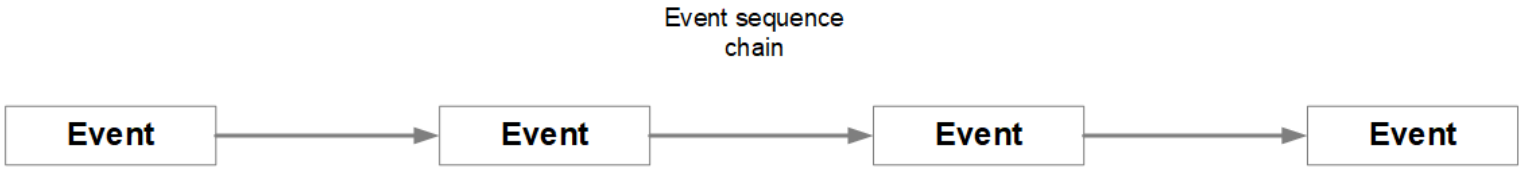
Checklist, scenario analysis: question 요소

Safety case: safety argument 요소



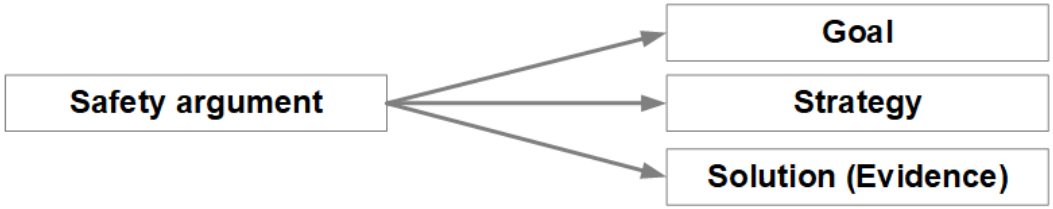

Cause
Result
Tree diagram
(FTA)
Basic event
gate
(Middle) event
gate
Accident
(ETA)
Initial event
Pivotal event
Accident
Worksheet
- Causal factor
- Secondary cause
Cause
Item
Failure
Effect
Hazard/Risk
- Function/purpose
- Component
- Parameter
- Failure Mode
- Deviation
- Immediate effect
- System effect
- Consequence
- subsystem
- System effect
STPA
Accident/Hazard
Safety constraints
Control structure
Cause
UCA

STEP/ECFA



Checklist, what-if analysis, scenario analysis

Safety Case



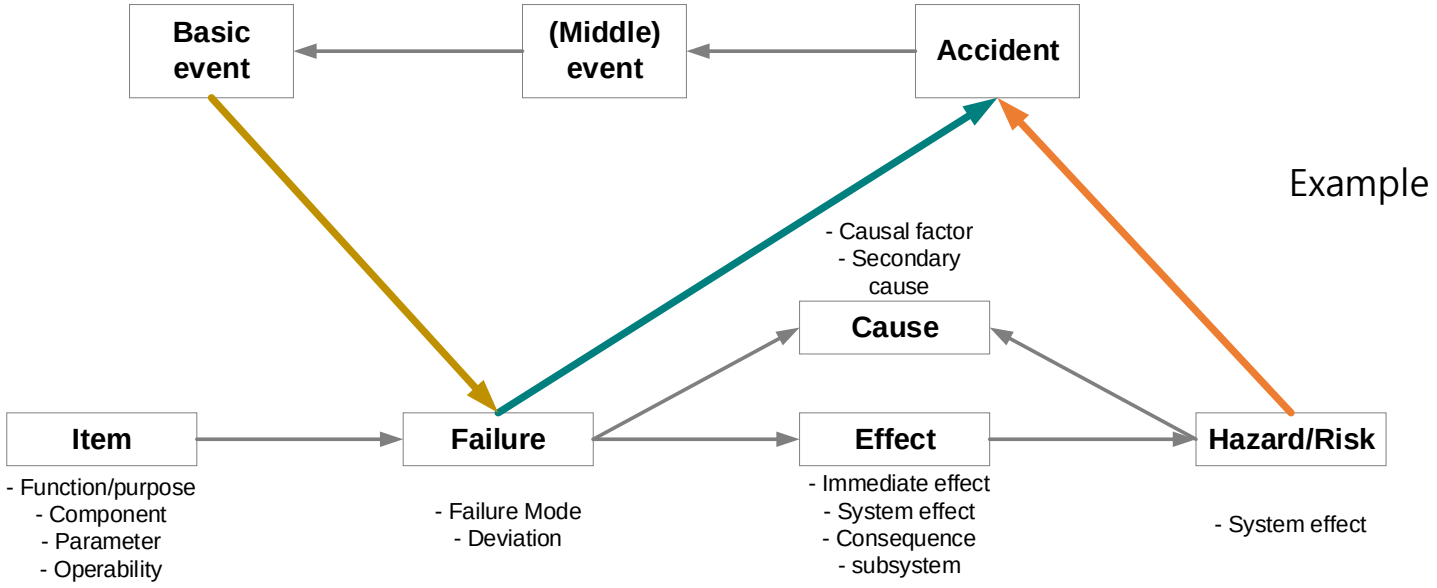
기법의 연결 관계 분석

- 2-way (+1)로 추상화된 모델에서의 관계 분석
  - 1. Basic usage relation (usage traceability)
    - 시작점을 기준으로 한 각 기법의 요소들을 원인 – 결과 체인으로 '**사용**' 하는 추적 관계

추적성: 개발 프로세스에서 요구사항 부터의 산출물 간에 성립되는 관계
(생명 주기에서 작업 산출물의 파생 경로와 할당 또는 흐름 경로)

본 논문에서는 추적성의 개념을 연결 관계 분석으로 위해도 분석 결과에 이용함

  - (3. Support rationale traceability)
    - 그 외 failure/hazard/cause 등에서 support 관계로 생각해 볼 수 있는 traceability
    - 위 2 경우에 비해 불명확한 관계로 정의



- 같은 형태로 몇몇 관계에 대해 정의

추적 관계에 대한 정의
- 추적 관계를 포함한 전체 모델링에 이용

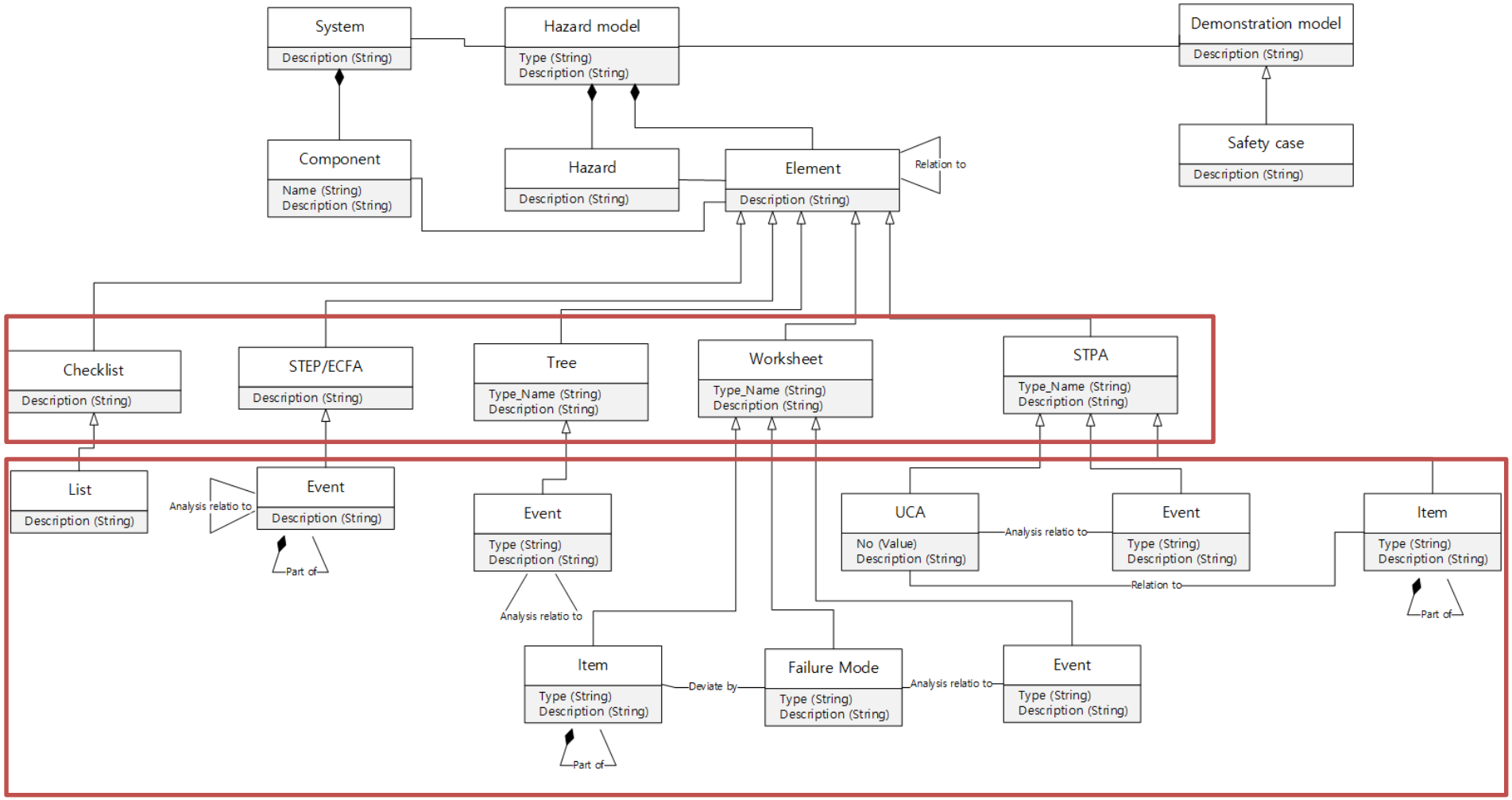
Relation between (from – to)	Description
(1) Basic event – (2) Failure	Failure equivalent trace
(1) Basic event – (2) Item	Component related trace
(1) Accident – (2) Hazard/Risk	Accident equivalent trace
(2) Item – (3) control structure	Basic component trace
(2) Effect/Hazard – (3) UCA/state variable	Failure relation
(2) Failure/effect/hazard – (4) Event	Failure event equivalent contents traceability
(4) Event – (5) question	Question extraction traceability
	….
2 (Hazard/Risk) -> 1 (Accident)	1 (Accident)와 연결해서 2 (Hazar
2 (Failure) -> 1 (Accident)	1 (Accident)와 연결해서 2 (Failure)
2 (Failure) -> 4 (Event)	4 (Event)의 initial 에 2 (Failure)의 입력 으로 분석 가능
2 (Hazard/Risk) – 3 (Accident/Hazard)	2 (Hazard/Risk) can help to identify the hazard for 3 (Accident/Hazard)
	….

2번 분류

1번 분류

위해도 모델의 메타모델

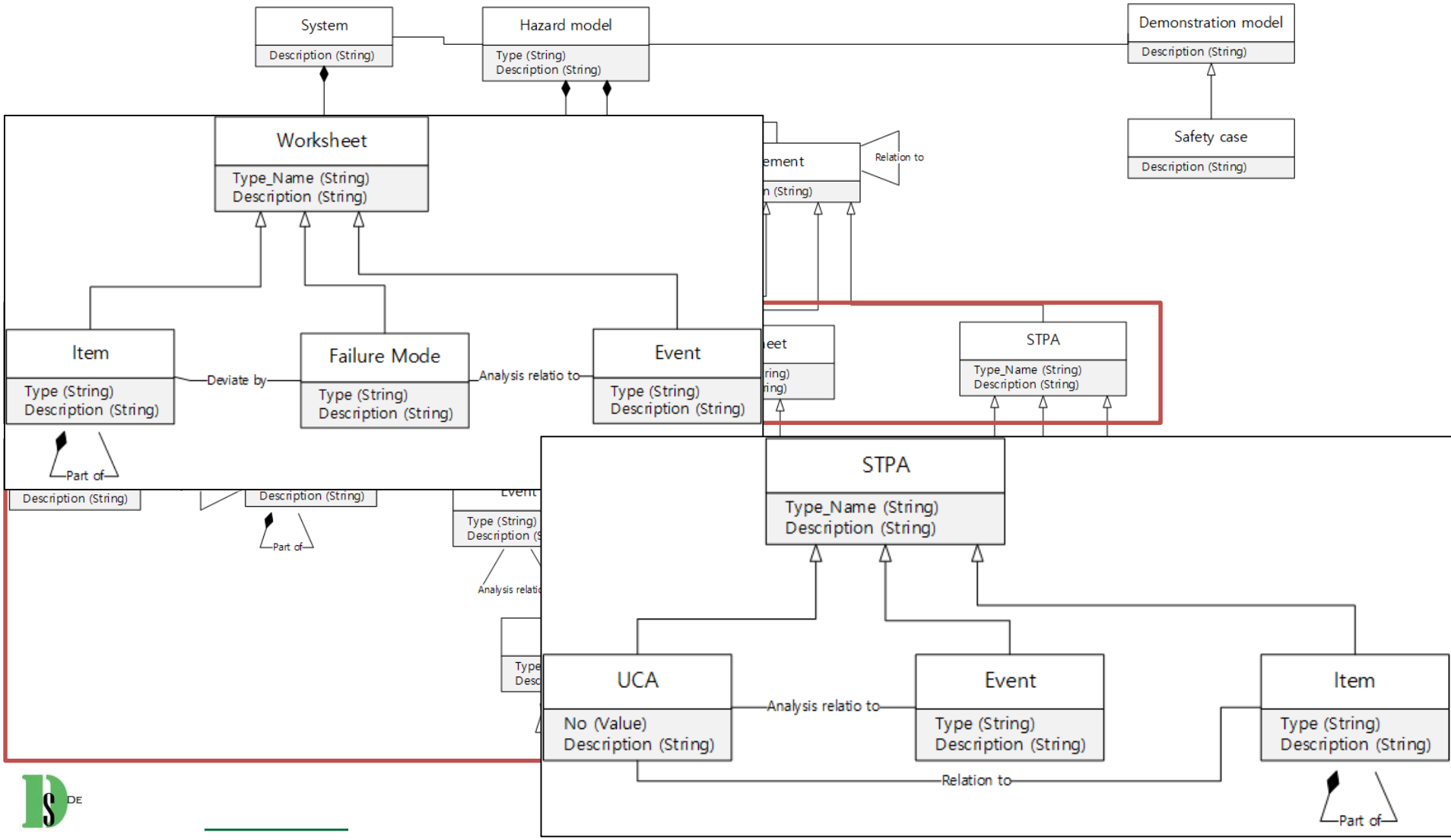
- HA technique, traceability relation을 종합적으로 표현하기 위한 메타모델 개발
  - Element들을 메타모델을 활용해서 모델링 해 표현



(a) HA technique 요소 메타모델

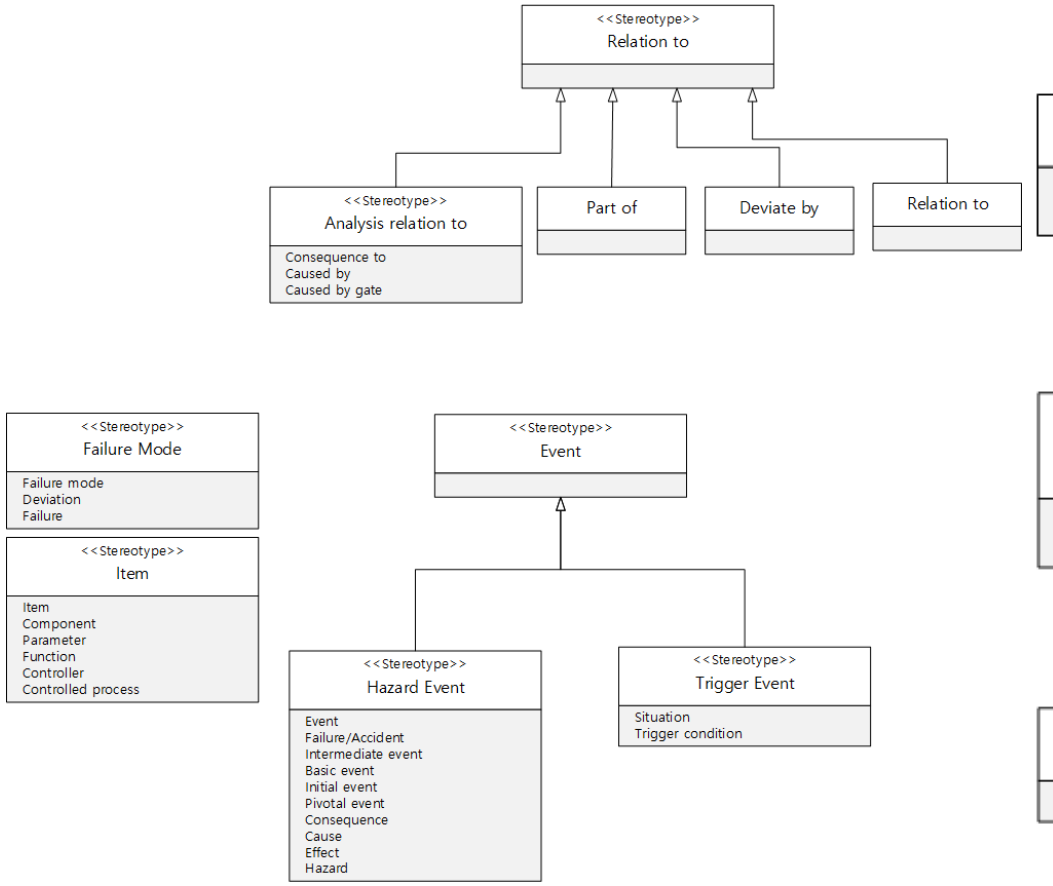
위해도 모델의 메타모델

- HA technique, traceability relation을 종합적으로 표현하기 위한 메타모델 개발
  - Element들을 메타모델을 활용해서 모델링 해 표현

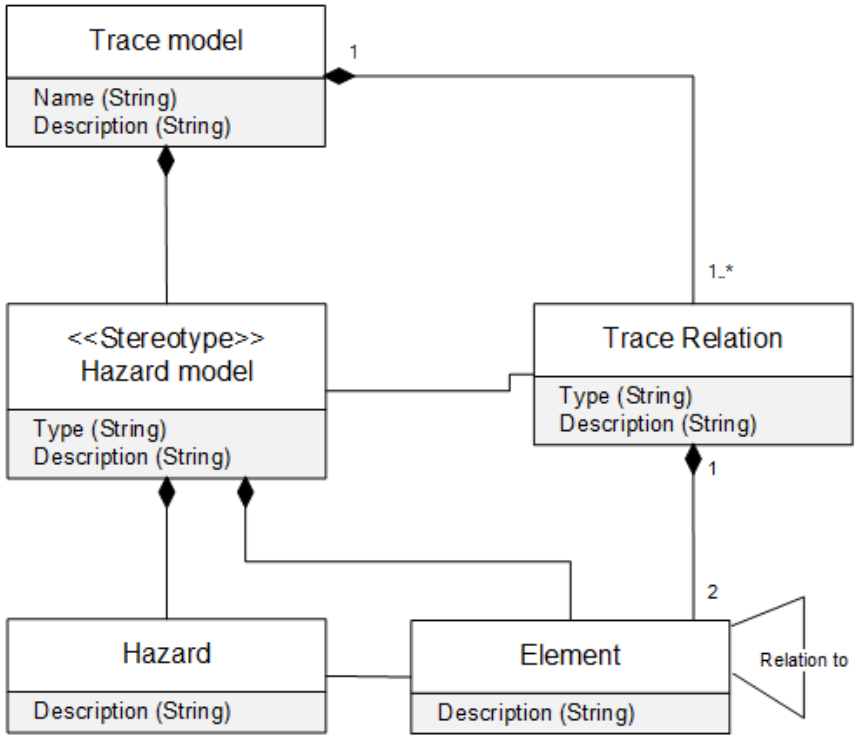


- **메타모델**

메타모델을 활용함으로써 HA result + traceability relation에 대해 표현
- 적용된 여러 종류의 HA result의 관계를 포함한 다각적 확인 가능
  > 시스템에 대해 여러 관점에서 failure – hazard – cause 의 관계 확인
  > 서로 다른 item 에서 나타나는 추적성을 바탕으로 CCA 확인 가능



(b) HA technique 기본 관계 메타모델



(c) HA technique 추적 관계 메타모델

사례 연구

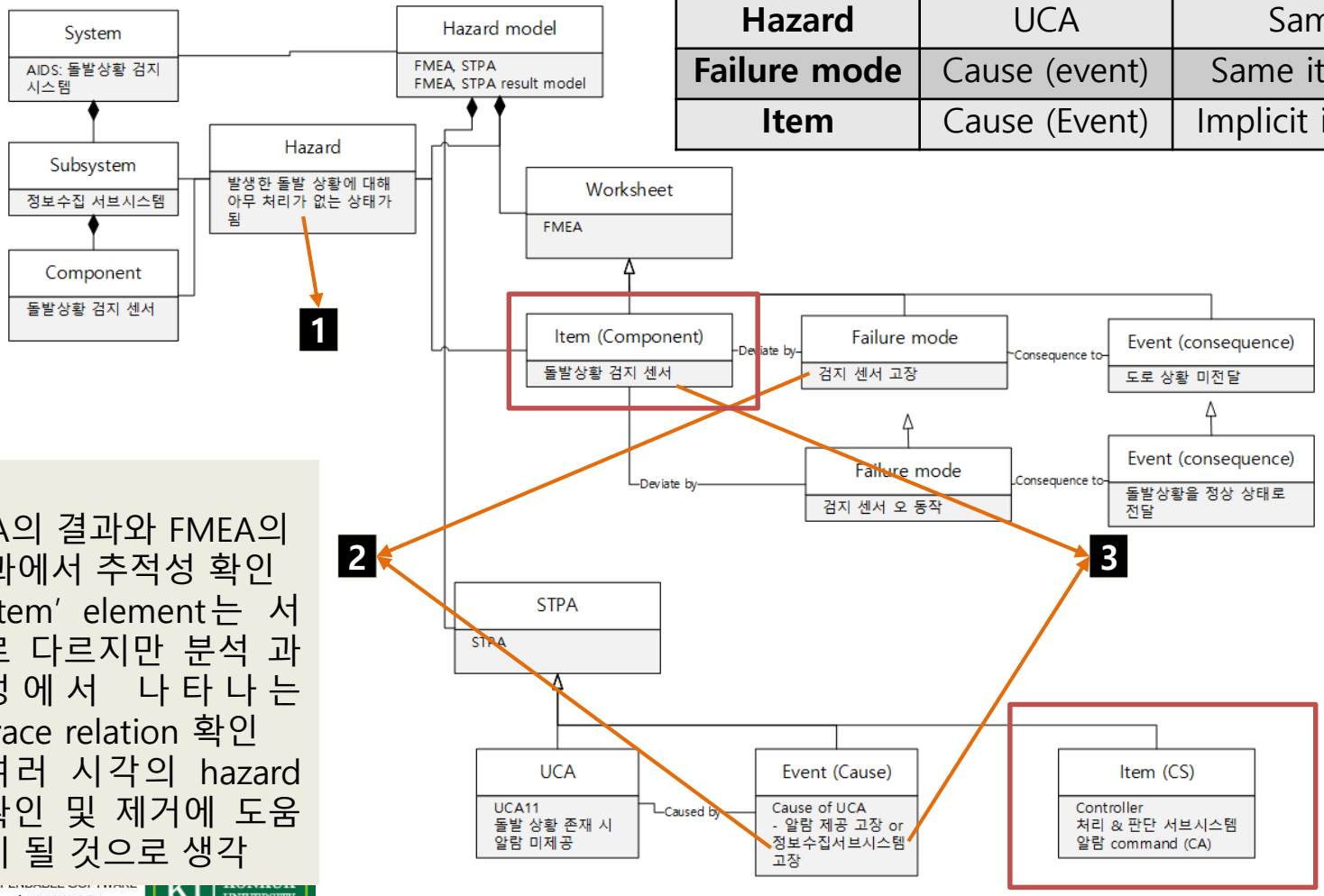
- 메타모델 형태로만 사례 연구 수행
  - 돌발상황 검지시스템 (AIDS)을 대상
  - FMEA 및 STPA 수행

CA		Provided	Not provided	Too soon/Too late		Early exited
				Soon	Late	
처리 및 판단	알람 command	**[UCA9]** 돌발상황 미존재 및 원할한 도로 상황에 주의 알람 명령 제공	**[UCA10]** 돌발 상황 존재 상황에 알람 미제공 **[UCA11]** **도로상황 혼잡 및 사고 상황에 알람 미제공**		**[UCA12]** 돌발 상황 및 도로상황 혼잡 상황에 알람을 늦게 제공	
정보수집	정보수집기 컨트롤	**[UCA13]** 돌발상황이 존재하고, 정보수집기 위치가 정상일 때 제어명령이 없는 상태에서 제어 명령 제공	**[UCA14]** 돌발상황이 존재하고, 정보수집기가 반대, 중간 상태에서 제어 명령이 있는 경우에 발생하지 않음 **[UCA15]** 돌발상황이 존재하지 않고, 정보수집기가 반대 위치에서 제어 명령이 있는 경우에 발생하지 않음		**[UCA16]** 돌발상황이 존재하고, 정보수집기가 반대, 중간 상태일 때 정보수집기로 제어 명령의 늦은 전달 발생	**[UCA17]** 돌발상황이 존재하고, 정보수집기가 반대 상태일 때, 정보수집기로의 제어 명령의 빠른 종료

사례 연구

- 메타모델 형태로만 사례 연구 수행
  - 돌발상황 검지시스템 (AIDS)을 대상
  - FMEA 및 STPA 수행

Element		Description	
FMEA	STPA		
Hazard	UCA	Same contents	1
Failure mode	Cause (event)	Same item traceability	2
Item	Cause (Event)	Implicit item traceability	3



STPA의 결과와 FMEA의 결과에서 추적성 확인

- ‘Item’ element는 서로 다르지만 분석 과정에서 나타나는 trace relation 확인
- 여러 시각의 hazard 확인 및 제거에 도움이 될 것으로 생각

결론 및 향후 연구

- 복잡한 시스템에 여러 종류로 적용되는 hazard analysis의 결과를 효과적으로 확인 할 수 있는 추적성 기반의 모델 개발
  - 기법의 추상화 모델 및 기법의 추적 관계 기반
  - 다양한 여러 위해도 분석의 결과를 여러 관점에서 다각적으로 확인 가능

- 향후 연구
  - 시스템 컴포넌트의 계층적 요소 반영
  - 추적성을 기반으로 한 모델의 시각화 방법 개발

감사합니다