Safety Case 패턴의 분류 카테고리에 따른 인스턴스 생성

정세진, 김의섭, 유준범
건국대학교

2019. 06. 26

목차

- 서론
- Safety Case & Pattern
- 카테고리에 따른 Safety Case Pattern의 인스턴스 생성
  - 내용 추상화 수준 분류 카테고리
  - 카테고리 별 인스턴스 생성 관계 및 과정
- 결론 및 향후 연구

서론

Safety (안전) : 인명피해나 환경파괴와 같은 심각한 결과로 부터 자유로운 상태 (Free (from accident/failure/hazard)

- **현대의 안전 필수 시스템 (safety-critical system)**
  - 소프트웨어가 제어에 직접적으로 관여하므로 소프트웨어의 안전성이 중요함
  - 여러 표준, 규제에 의해 안전필수 시스템의 소프트웨어 개발에 다양한 안전관련 activity 및 개발 활동들이 수행됨
  - 여러 다양한, 수많은 관련 결과물들이 도출
    - *e.g.* Safety/hazard analysis report, V&V report, development artifact 등
- **Safety case**
  - **구조화된 논증 구조**를 통해 시스템/소프트웨어의 안전성에 대해 '허용가능한 수준' 인지 확인하는 자료구조, 방법
  - ISO 26262와 같은 국제 표준에서도 요구
- **Safety case pattern**
  - Safety case의 'common argument structure'를 효과적으로 재사용하기 위한 패턴 기반 접근
  - 이전 연구에서는 기존에 연구된 패턴의 경향, 추상화 수준에 따라 분류 카테고리 제안
    - 4 종류의 카테고리로 구성

- **Safety case instance 생성**
  - Pattern의 분류 카테고리 별 인스턴스 생성 관계 및 정도가 여러 가지로 나타남
  - 추상화 수준에 따른 인스턴스 생성 (instantiation)의 범위/수준
  - 최종 argument 생성의 필요 정도 차
  - 등

본 논문에서는 pattern의 분류 **카테고리 별 인스턴스 생성 관계 및 과정**에 대해 제안
- 체계적으로 safety case pattern의 인스턴스 생성을 위함
- 4 종류의 카테고리에 따른 인스턴스 생성 관계 및 커버 범위 확인
- 인스턴스 생성의 필요 과정

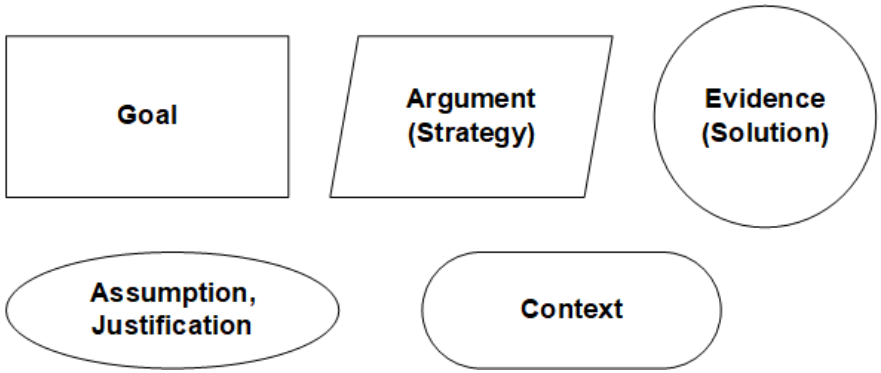
Safety Case

- 시스템/소프트웨어가 안전함을 설득하기 위한 구조적이고 명시적인 논증 구조
  - 시스템이 안전함을 설득하기 위한 관련 산출물의 집합을 논증 구조로 표현

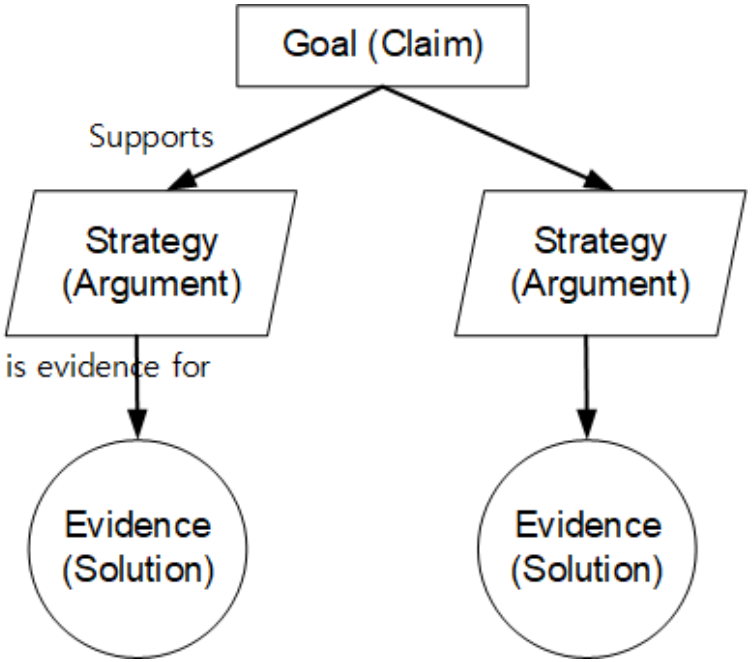
- 목표, 전략, 근거로 이루어진 구조적 논리 체계
  - **Goal** : 명제로 표현된 달성하고자 하는 목표
  - **Argument** : 목표가 달성됨을 보이기 위한 전략 (Strategy)
  - **Evidence** : 목표 달성을 뒷받침 할 수 있는 근거 (Solution)

Safety Case – Graphical Notation

- GSN (Goal Structuring Notation)
  - Safety Case의 구조를 **시각적으로** 표현하기 위한 대표적인 방법
    - cf. CAE (Claim, Argument, Evidence)



- 최상위 goal
  - "The system is acceptably safe"
- Goal 달성을 위한 합리적인 argument
  - "Argument over the safety requirement X"
- 뒷받침 할 수 있는 evidence
  - "Safety requirement X is formally verified"
- 그 외 부연 설명을 위한 notation
  - Assumption, Justification, Context, Etc.



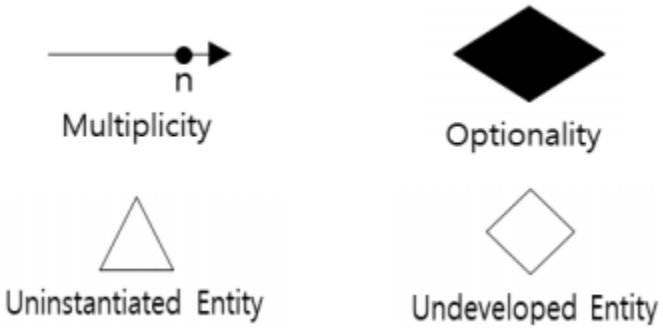
Safety Case Pattern

- Safety case pattern
  - Safety case 논증 구조에서 자주 사용되는 공통된 구조를 재사용하기 위한 접근법
  - **Meta-information**, **common argument structure**로 구성

- Meta-information
  - Design pattern language를 기반으로 "*Safety Case Construction and Reuse using Patterns*" 에서 제안

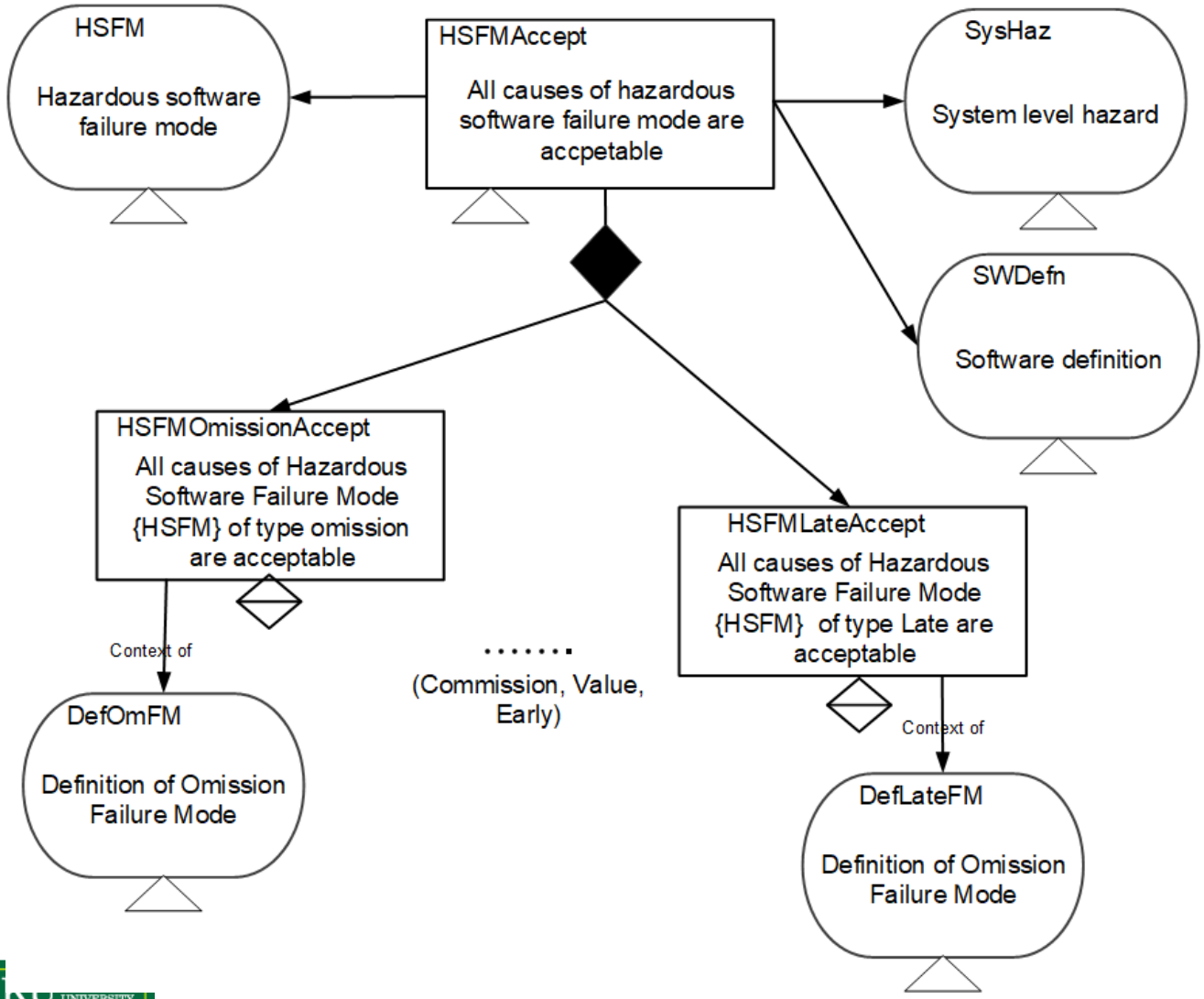
  - Name, intent, motivation, applicability, consequence, related pattern, **structure** 등으로 구성

- Common argument structure
  - Meta-information에서 structure 부분에 해당, 시각적인 safety case 구조로 주로 구성
  - Notation 내부의 내용에서 패턴의 특징인 가변성을 위한 uninstantiation contents 사용
    - 매개변수 표현
  - 확장된 GSN 요소 사용



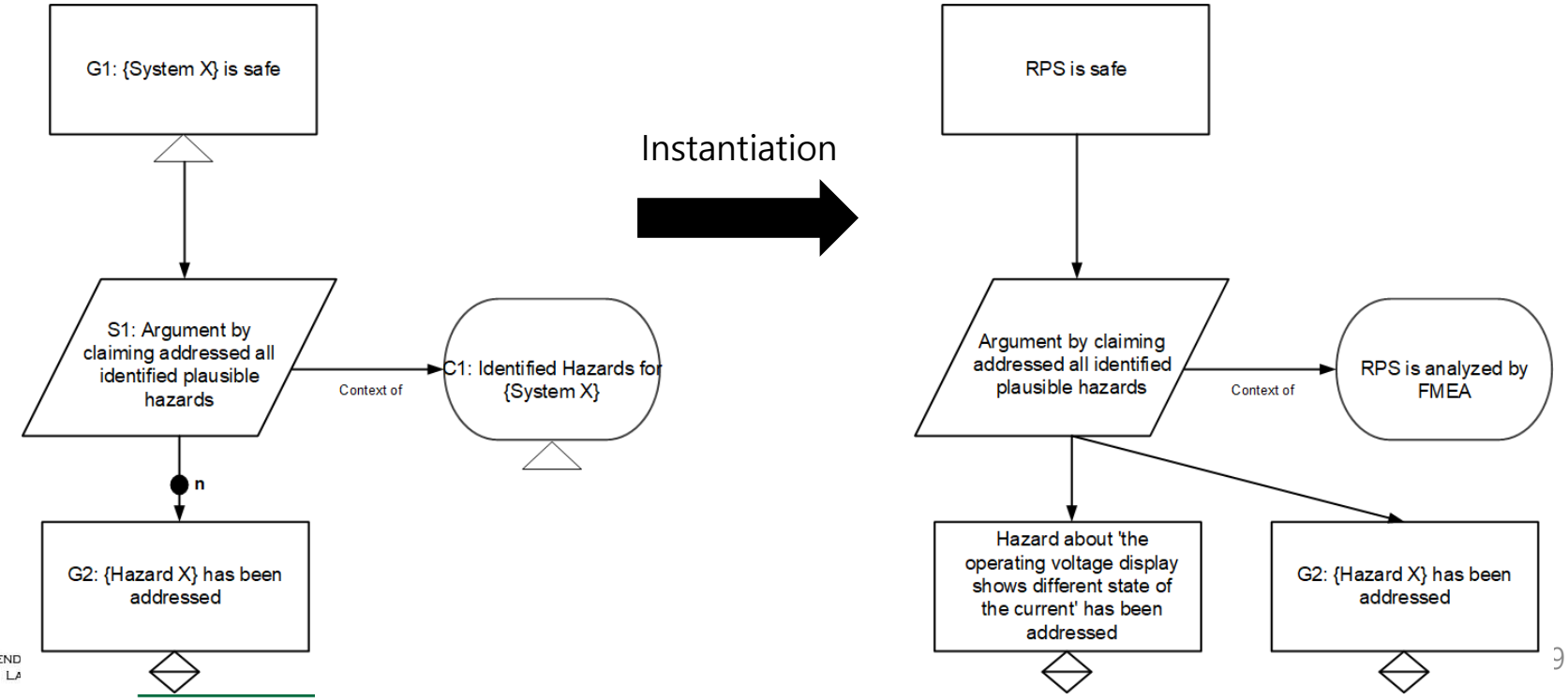
Safety Case Pattern – Structure Example

- Structure 예제 (for software failure)



Safety Case Pattern의 인스턴스 생성

- Pattern을 활용한 safety case 인스턴스 생성
  - Pattern의 매개변수, 확장된 요소를 모두 고려하여 논증 구조 작성
  - Pattern에서 제공되는 구조, 내용에 따라 인스턴스화의 variability 등의 정도가 달라짐
    - 논증 구조 결정
    - 실제 결과물을 활용한 evidence 정의 및 구성
  - 본 논문에서는 이를 **카테고리에 기반해 관계와 과정을 확인**
    - 체계적인 관계 확립 및 생성 방안



내용 추상화 수준 분류 카테고리

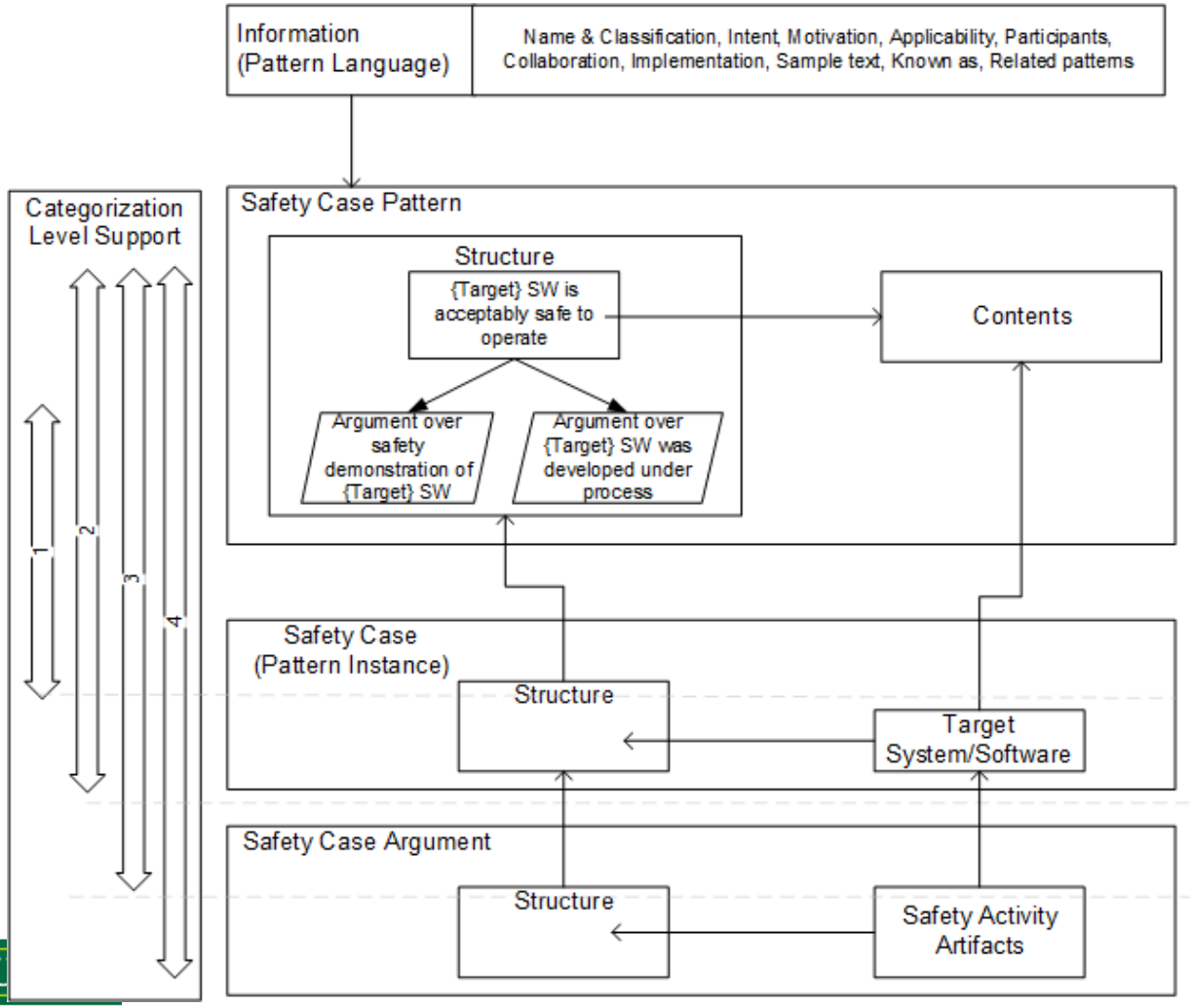
- 이전 연구에서는 기존에 제안된 safety case pattern들의 경향, 수준에 따라 카테고리화
  - 4 종류의 추상화 수준 카테고리 제안
  - 각 카테고리에 따라 추상화 수준이 다르기 때문에 이에 맞추어 인스턴스 생성이 달라짐

No.	Classification	Description
1	Structural composition	Providing notation structure or simple contents with notation structure for mechanical generation
2	High-level contents composition	Contents of high-level abstraction only
3	Concrete contents composition	Contents which have detailed information for specific domain, target, or decomposition information
4	Detailed contents composition	Detailed contents with little abstraction (similar to an instance) about detailed activity

원자력 발전소 안전 소프트웨어의 safety case pattern 작성을 위한 문헌 리뷰 기반의 pattern 작성 범위 분류

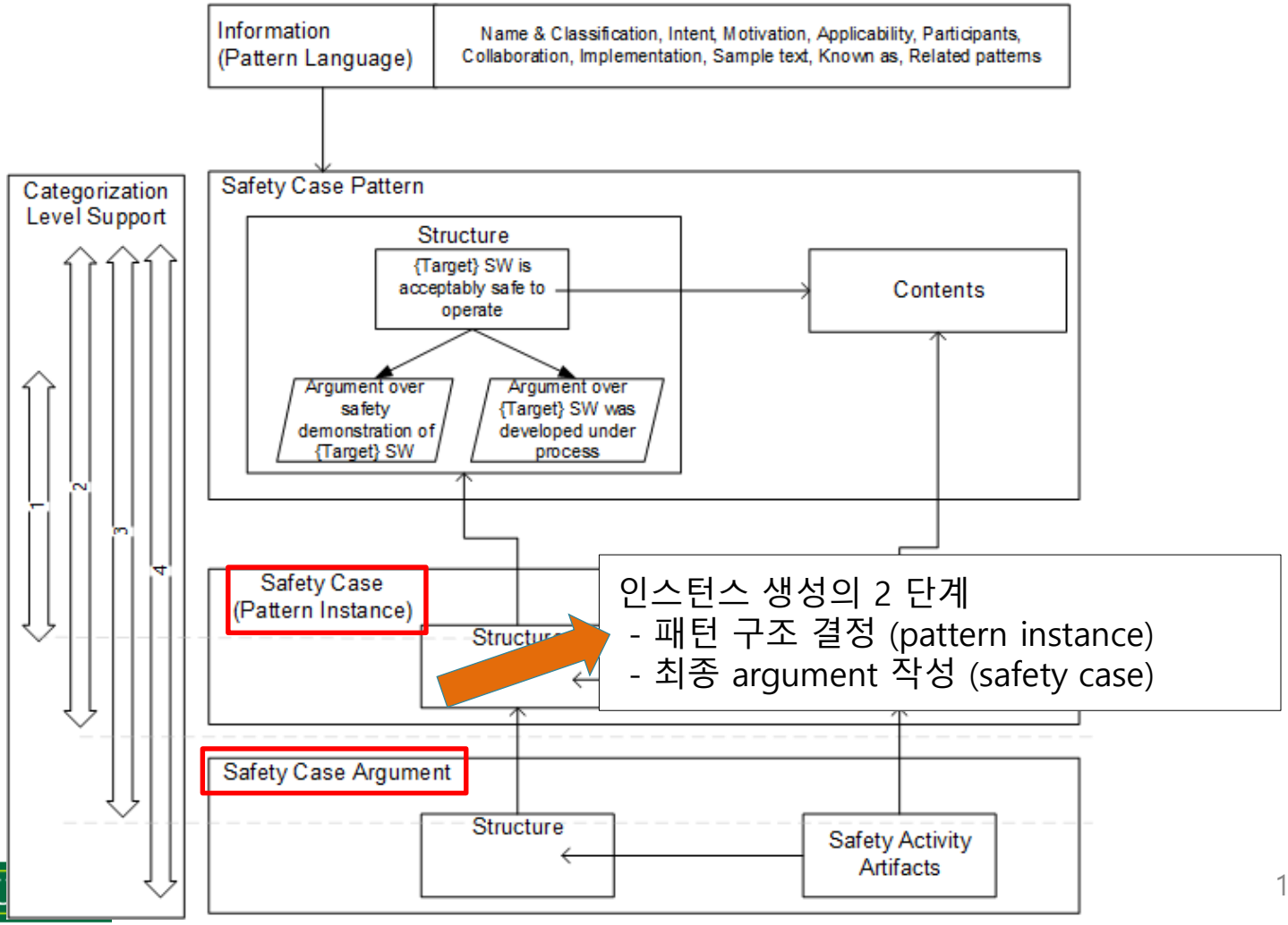
카테고리 별 인스턴스 생성 관계 및 과정

- Safety case pattern을 활용한 인스턴스 생성 관계 및 범위
  - 1. 2 단계로 구성된 인스턴스 생성 관계
  - 2. 패턴의 카테고리 별 커버 범위 정의

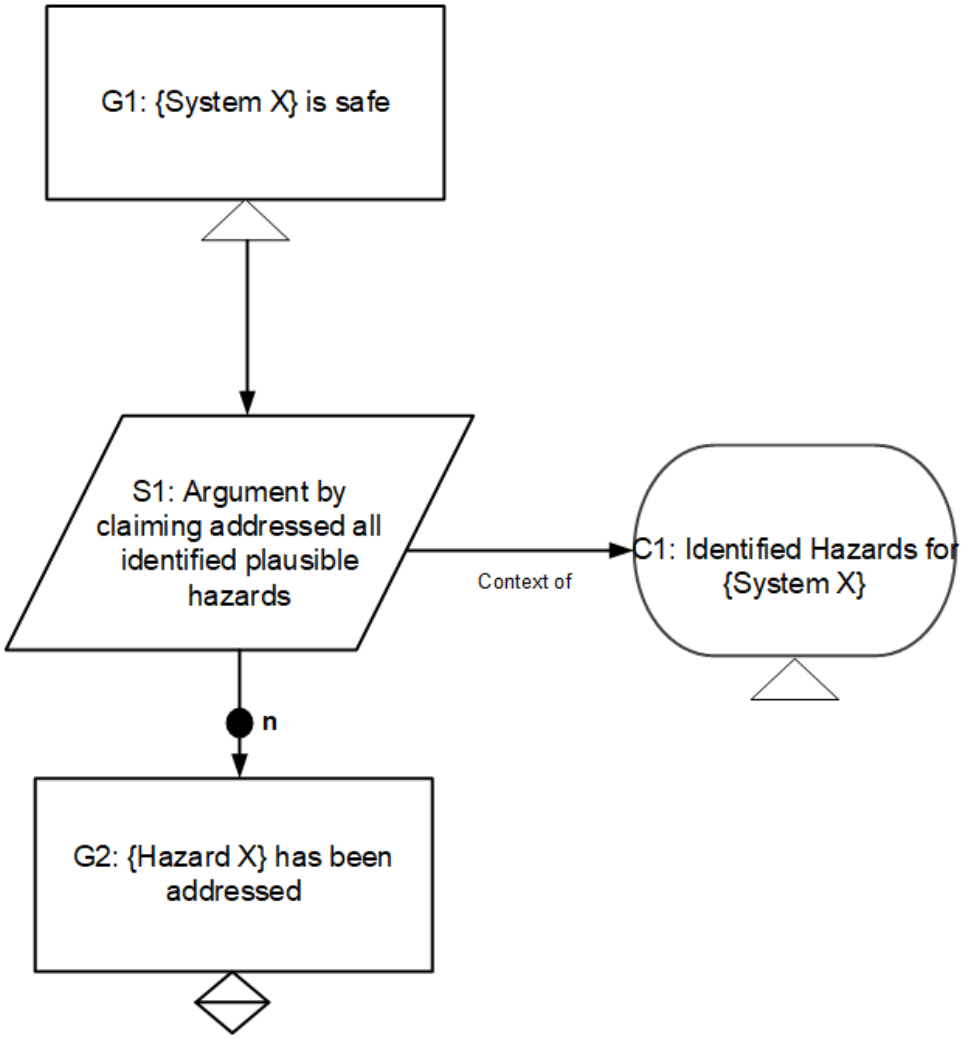


카테고리 별 인스턴스 생성 관계 및 과정

- Safety case pattern을 활용한 인스턴스 생성 관계 및 범위
  - **1. 2 단계로 구성된 인스턴스 생성 관계**
  - 2. 패턴의 카테고리 별 커버 범위 정의



카테고리 별 인스턴스 생성 관계 및 과정

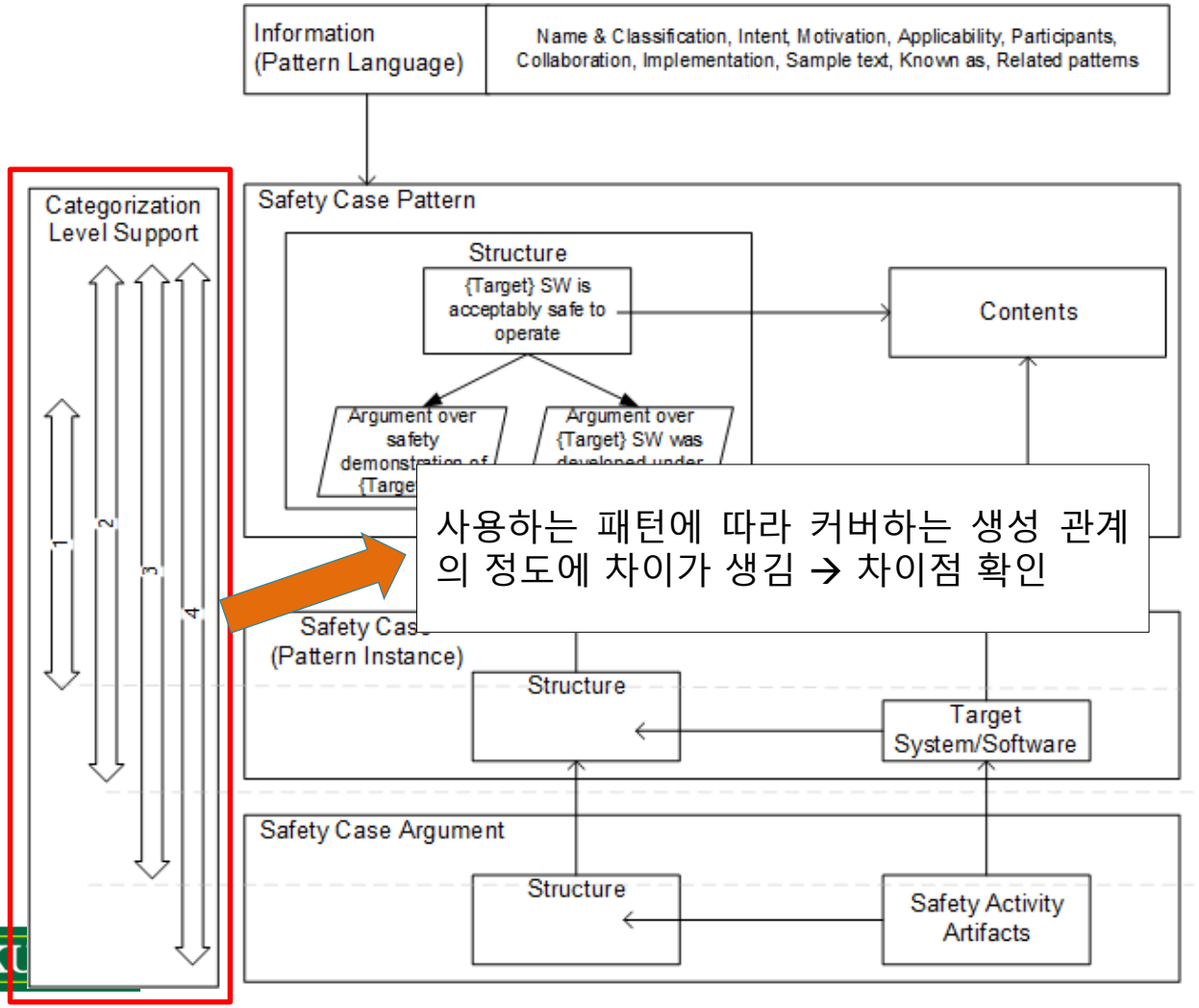


- 패턴 구조 결정 -
패턴의 매개변수, optionality와 같은 요소에 대한 variability 결정 후 논증 구조 확립

- 최종 argument 작성-
Sub-goal, strategy, evidence를 포함한 구체적 activity에 대한 논증 구조 및 safety case 완성

카테고리 별 인스턴스 생성 관계 및 과정

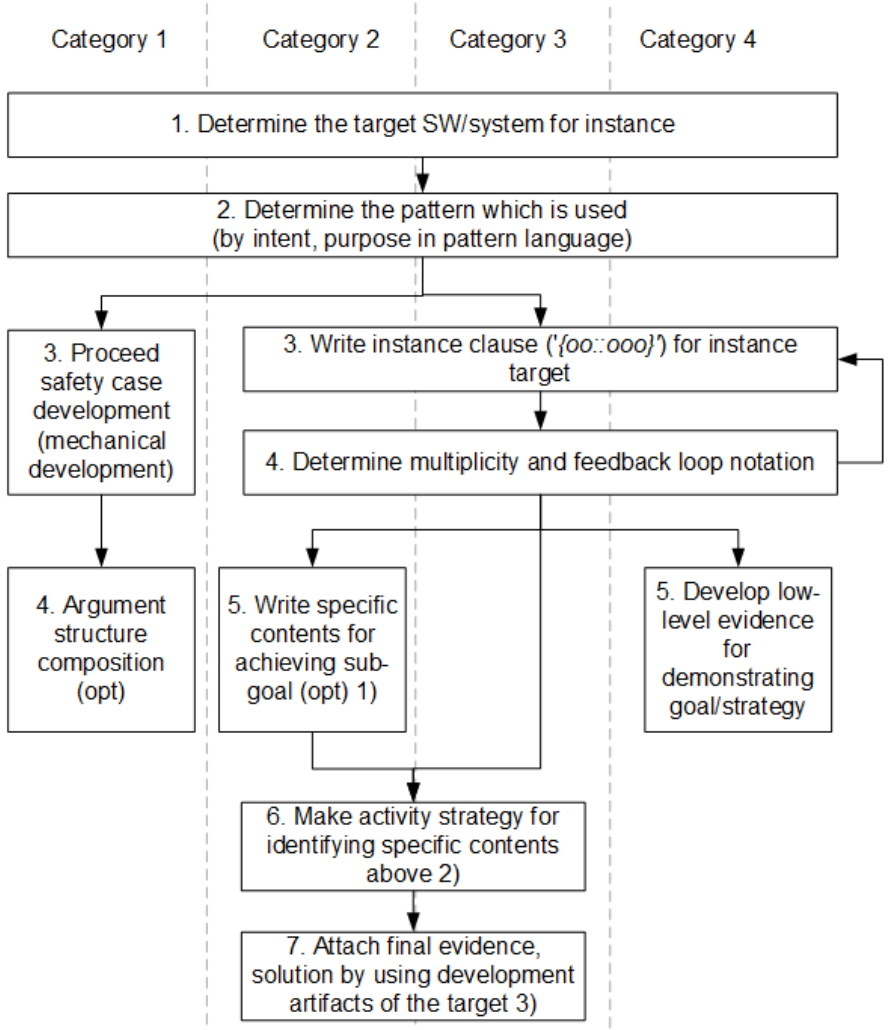
- Safety case pattern을 활용한 인스턴스 생성 관계 및 범위
  - 1. 2 단계로 구성된 인스턴스 생성 관계
  - **2. 패턴의 카테고리 별 커버 범위 정의**



카테고리 별 인스턴스 생성 과정

- 4 분류의 카테고리 별 인스턴스 생성 과정 제안
  - Specific activity 결정 부분에서 차이

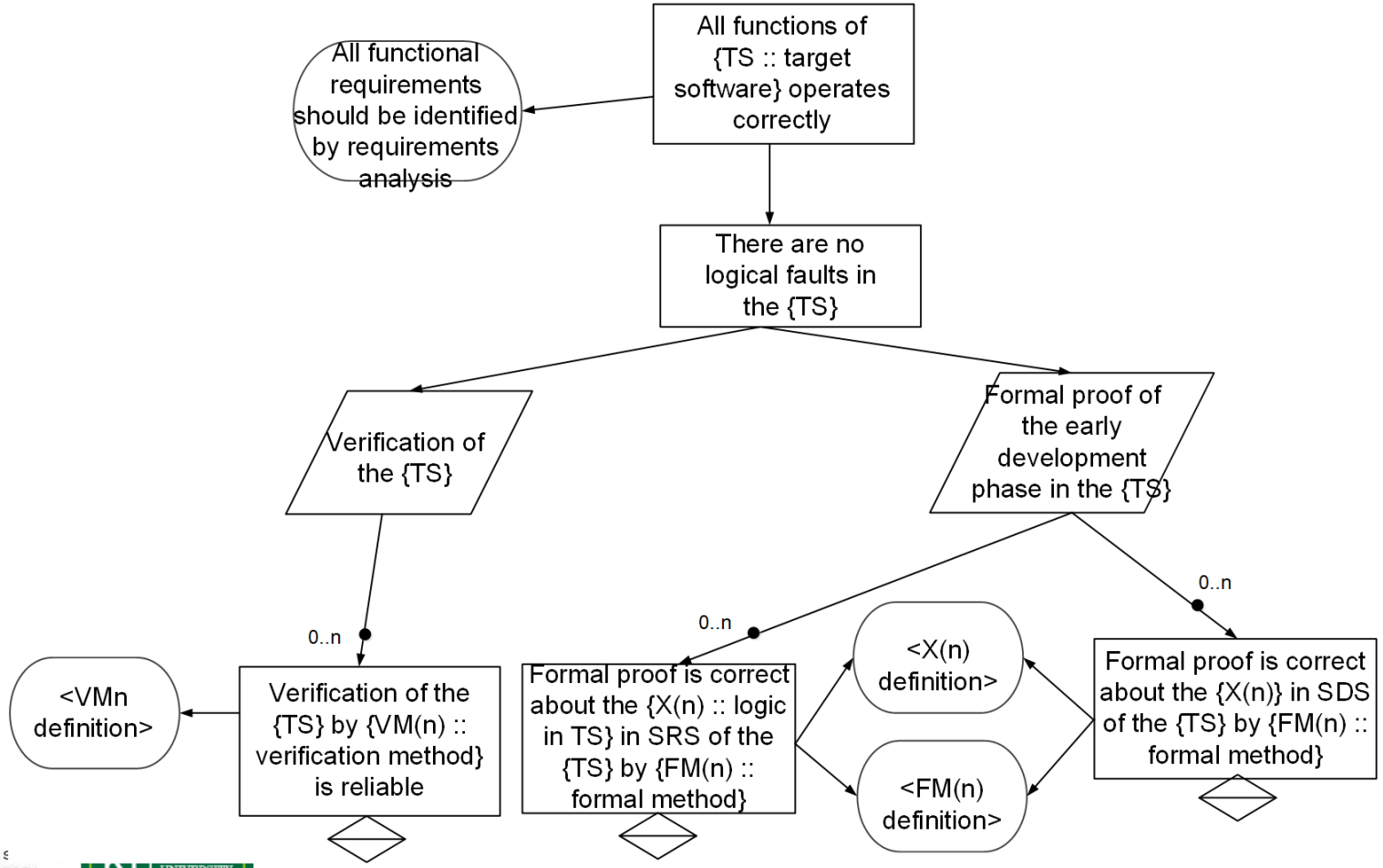
Category	Process	Description	From
2	5	Specific contents/element for supporting goal achievement	Std. or Safety artifact
2	6	Activity to achieve sub-goal	Safety artifact
2	7	Specific evidence	
3	6	Activity to achieve sub-goal	
3	7	Specific evidence	
4	5	Specific evidence	



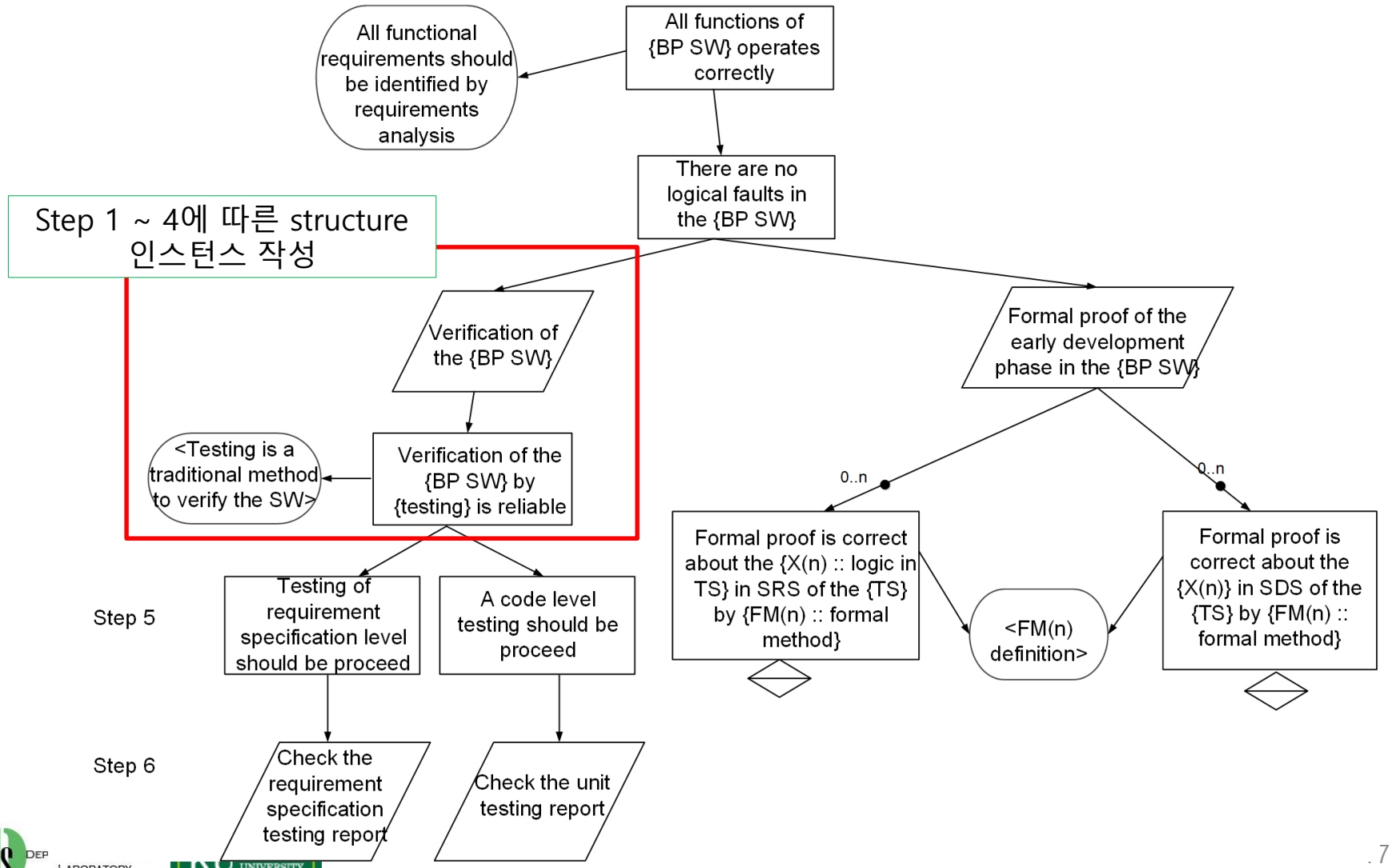
1) 표준, 규제를 기반으로 sub-goal을 뒷받침 하는데 필요한 specific elements 를 or safety activity artifact를 통해 확인한 sub-goal을 뒷받침 하는데 필요한 safety 관련 specific elements
2) 각종 artifact를 만들기 위해 실제 수행한 activity
3) Safety activity의 결과로 도출된 artifact를 이용해 구성

Safety case pattern을 활용한 인스턴스 생성 사례

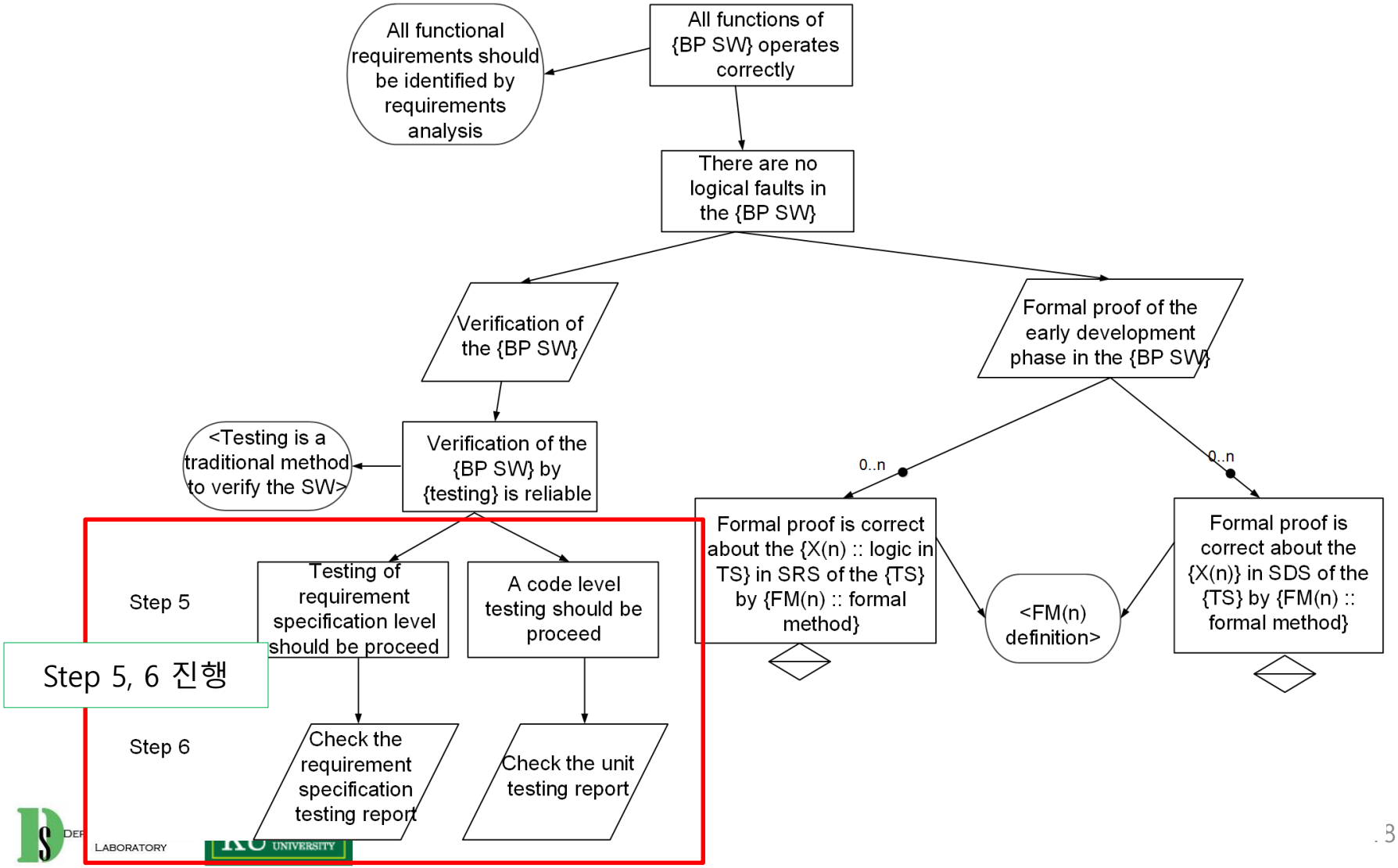
- 카테고리 2 수준의 패턴을 활용해 인스턴스 생성
  - No logical fault pattern
  - Verification, formal proof에 대한 구체적인 activity 관련 정보가 없으므로 카테고리 2 분류
  - For Bistable Processor software in nuclear power plants



Safety case pattern을 활용한 인스턴스 생성 사례



Safety case pattern을 활용한 인스턴스 생성 사례



결론 및 향후 연구

- 결론
  - Safety case pattern을 활용한 인스턴스 생성의 관계 및 과정 제안
    - 2 단계로 정의된 인스턴스 생성 관계 정의
  - Pattern에 나타난 수준에 따라 인스턴스 생성의 차이를 보임
    - 적정한 수준의 instantiation이 필요
    - 필요에 맞는 패턴 선택 및 개발이 요구됨
- 향후 연구
  - 효과적인 pattern 개발을 위해 카테고리 별로 패턴을 생성하고, 구성하는 방안 연구

감사합니다.

정세진

jsjj0728@konkuk.ac.kr

Dependable Software Laboratory

건국대학교