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

정세진, 손준익, 유준범

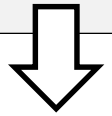
Dependable software laboratory
건국대학교 컴퓨터공학과

{jsjj0728, sji6227, jbyoo}@konkuk.ac.kr

Introduction

- 안전필수 시스템 (safety-critical system)의 소프트웨어 역할 증가
  - Safety demonstration of the software is also important for safety
  - **How demonstrate the software is safe among several development artifacts?**
    - 검증, 안전성 분석, 개발 등을 통해 다양한 산출물을 가지고 안전성을 어떻게 판별할 것인가
    - Safety case (안전 논증) 작성이 많이 사용됨
  - Safety case (안전 논증) 작성법을 통해 대상 system/SW의 안전성을 보증하는 활동들이 수행됨
    - ISO 26262, IEC 표준들 에서 safety case를 활용한 내용들이 포함되고 있음
- Safety case pattern
  - 논증 구조의 반복되는 부분 재사용, instance 작성의 효율성 증대, 일정 수준 이상의 instance 작성의 평가, 등의 이유로 많은 연구가 진행 중

Problem: **Which scope/contents** are appropriate for safety case patterns (for nuclear power plants)? (어떤 범위/수준을 가지고 패턴을 작성해야 하는가 하는 연구는 부족) – 패턴 개발에 혼동이 생길 수 있음

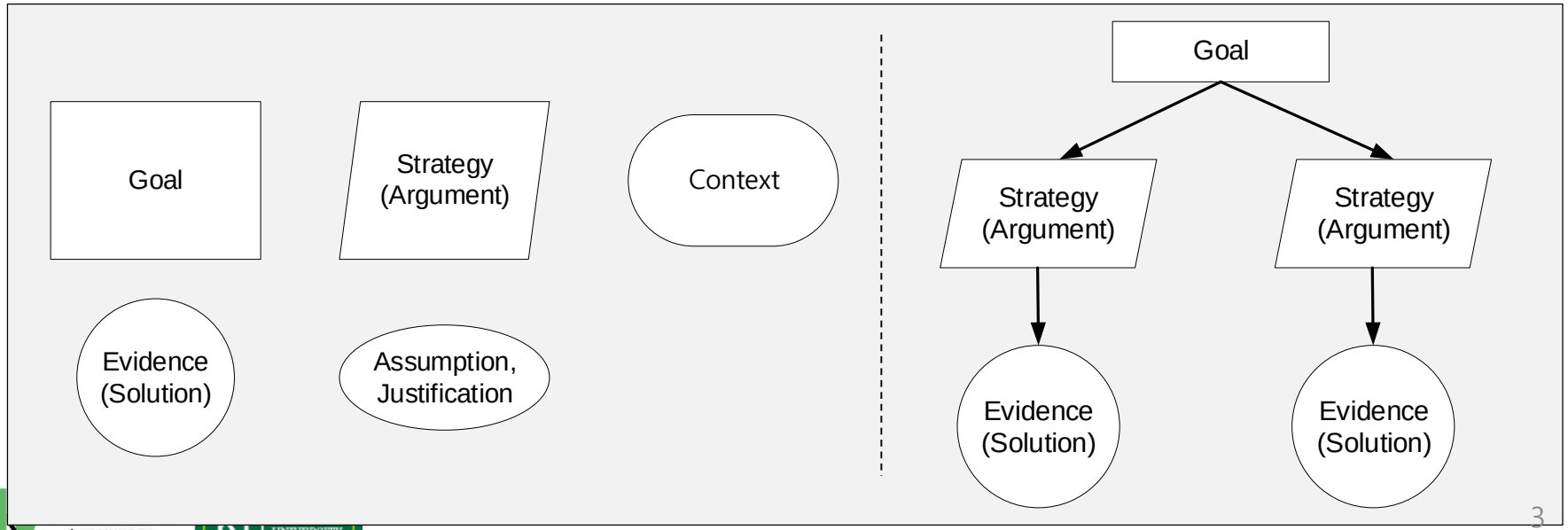


Safety case pattern의 문헌 조사/리뷰 및 분석을 통해 pattern 작성의 범위 분류 및 이에 대한 고찰

Safety case

- 시스템이 안전함을 설득하기 위한 **구조적**이고 **명시적**인 자료 구조
  - 목표 (Goal)를 달성하기 위한 전략 (Strategy)과 근거 (Solution/evidence)를 구조적으로 제시
    - 주로 system/software의 **acceptably safe**를 판단하기 위한 체계적인 작성 방법
  - Goal, Argument, Evidence로 이루어진 구조적 체계
    - Goal : 명제로 표현된 달성하고자 하는 목표
    - Argument : 목표가 달성됨을 보이기 위한 전략 (Strategy)
    - Evidence : 목표 달성을 뒷받침 할 수 있는 근거 (Solution)

- GSN (Goal structuring notation)
  - Safety Case의 구조를 시각적으로 표현하기 위한 방법 중 하나



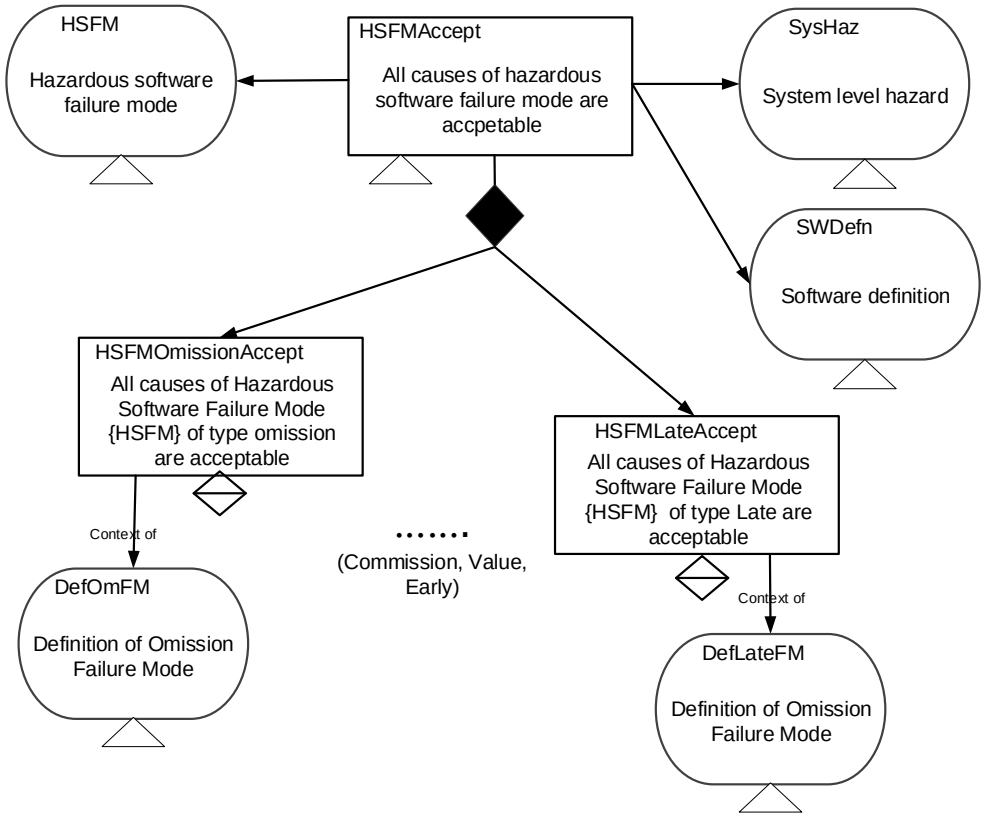
Safety case pattern

- Safety case structure를 효율적으로 재사용하기 위해 제안된 구조
  - Design pattern language를 기반으로 refine됨
  - The process of safety case construction and reuse can be made more systematic

- GSN/CAE 구조에서 pattern화를 위한 추가 구조도 포함
  - Uninstantiation, undeveloped
  - Multiplicity
  - Expression
  - Optional extension

Pattern language in existed paper

Pattern name and classification
Intent
Motivation
Applicability
Structure
Participants
Collaborations
Consequences
Implementation
Text
Known uses
Related patterns



문헌 조사를 통한 패턴 리뷰

- Safety case pattern과 관련된 다양한 논문/보고서 확인
  - 약 40여 편

- 다양한 목적으로 작성된 논문들 분류

분류	명세	비고
1. Safety case pattern and pattern-based approach for safety case	Safety case 작성을 위한 pattern 제안 및 적용에 관련된 논문	13 편
2. Pattern-based approach of safety/assurance argument	직접적인 safety case pattern 이외의 패턴 기반의 argument, assurance 작성을 위한 논문들	2 편
3. Other perspectives for software safety case (with simple pattern)	Safety case 작성을 위한 principle, review에 관련된 논문들	4 편

(기타 safety case application 관련 10여 편 및 safety case modelling, tool 등 pattern과 연관성이 떨어지는 논문 제외)

Classification of the pattern structure/contents

- Specification 정도에 따라 분류를 수행함: **패턴 작성의 적정한 정도를 평가하기 위해**
  - 4 개의 분류 기준을 제안

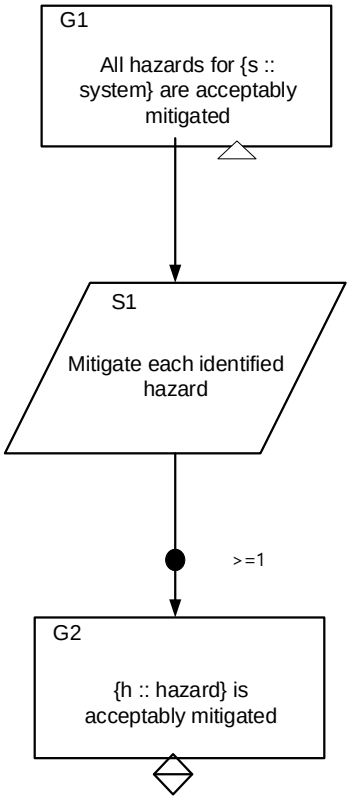
  - Specification 수준 (detail) 이 증가할 수록 직접작성이 필요한 instantiation contents 감소
    - Instance 작성의 자유도가 제한되지만, 일정 내용(수준)으로 반복해 작성 가능
    - 재사용의 확장성에 대한 고민이 생기게 됨

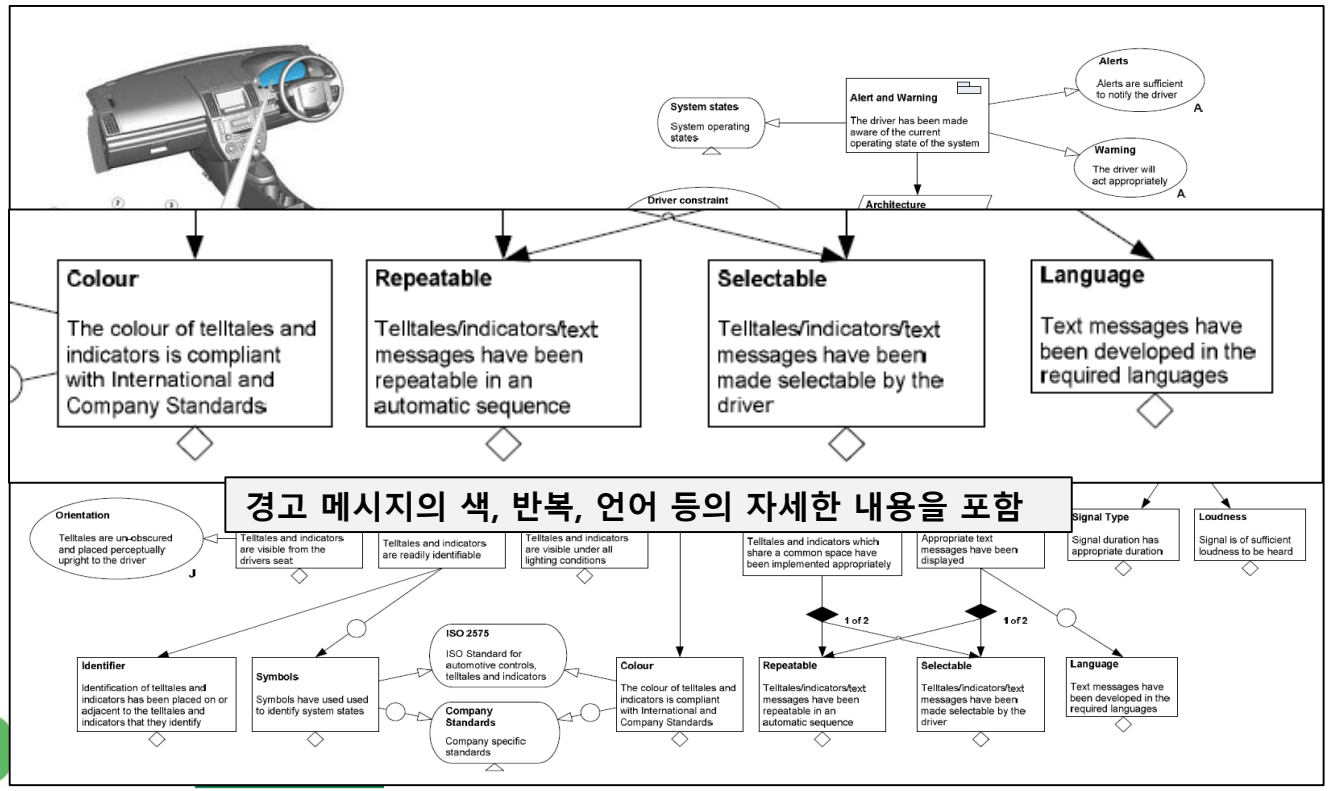
  - Specification 수준이 감소할 수록 직접 작성이 필요한 내용이 증가
    - 대상 (target)에 따라 필요한 내용을 구성해가며 작성에 용이
    - 제공되는 내용의 정도에 따라 패턴을 사용하는 의미가 감소할 수 있음

No.	Classification	Description	비고(편-개수)
1	**Structural** composition	Notation들의 구조 (structure)만으로 구성	2-11 ([4][5])
2	**High-level contents** composition	높은 수준에서 추상화 (abstraction)된 내용만 제공 (e.g. All hazard mitigation)	10-36 ([5][7] 등)
3	**Concrete contents** composition	대상 도메인에 specific한 내용을 포함한 abstraction (e.g. failure type 정의)	4-11 ([3] 등)
4	**Detailed contents** composition	가장 낮은 수준의 abstraction, safety case의 instance에 근접	1-3 ([6])

Classification of the pattern structure/contents

- **Structural decomposition**
  - 구조적인 면에 중심으로 하여 제공되는 패턴들
  - 옆의 그림과 같은 구조 여러 개 제안 + 각 구조들의 결합 방법 제시
  - 구조만을 사용
- **Detailed contents composition**
  - Safety case instance에 근접한 컨텐츠로 제공
  - 적은 instantiation

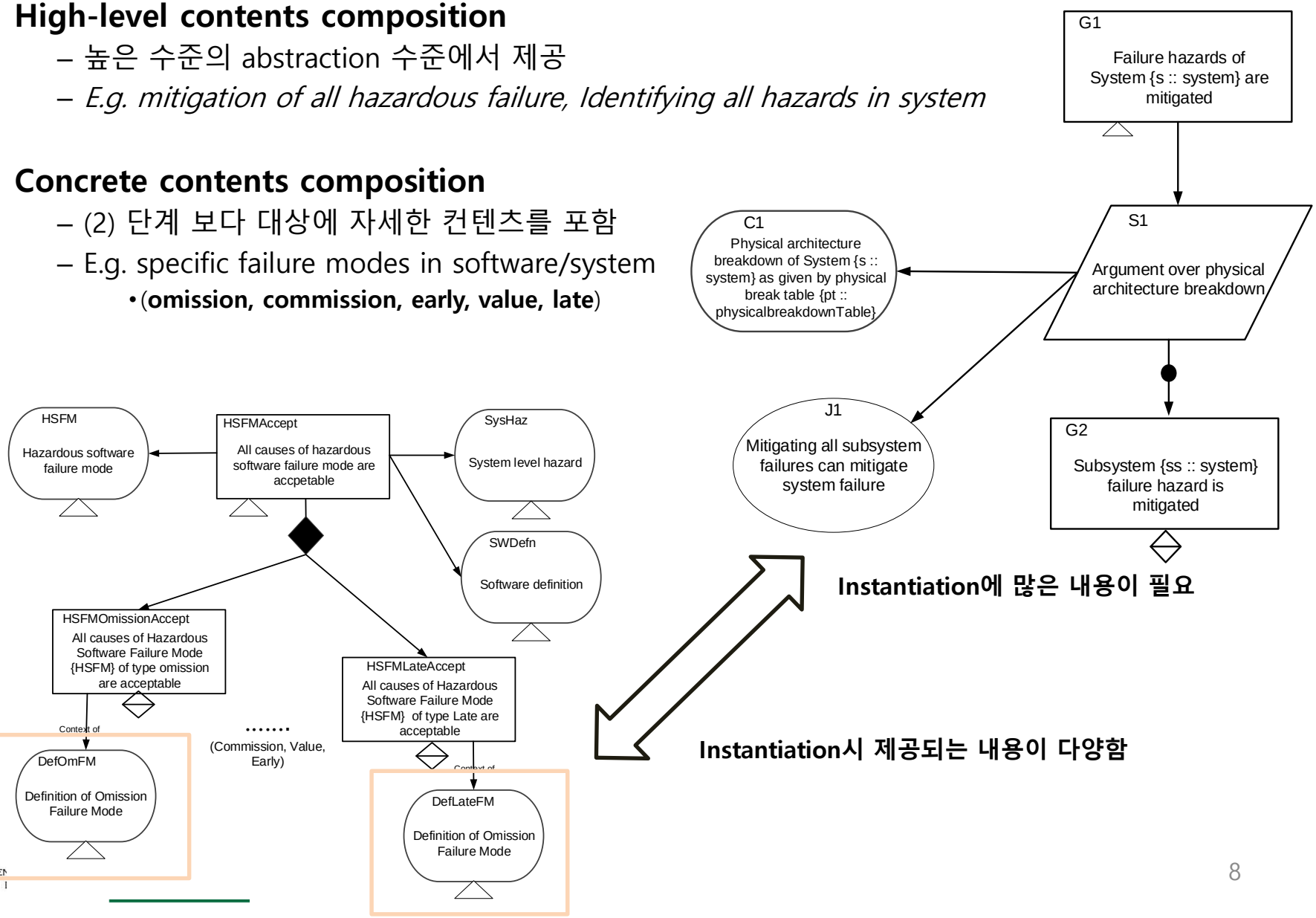




Classification of the pattern structure/contents

- **High-level contents composition**
  - 높은 수준의 abstraction 수준에서 제공
  - *E.g. mitigation of all hazardous failure, Identifying all hazards in system*

- **Concrete contents composition**
  - (2) 단계 보다 대상에 자세한 컨텐츠를 포함
  - E.g. specific failure modes in software/system
    - (**omission, commission, early, value, late**)



Considerations of the classification

- 각 분류 별 고려할 점들

No.	Classification	Description
1	Structural composition	- 패턴의 구조적인 내용만을 제공하기 때문에 많은 내용이 포함되지 않음
2	High-level contents composition	- 높은 수준의 abstraction으로 인해 다양한 대상, 도메인 적용의 여지가 높음 - 여러 도메인에 쉽게 적용 가능 - 재사용성이 높지만, 분석가가 직접 작성해야 하는 내용이 많아 짐 → 일정 수준 이상의 safety case 작성의 의도가 약해질 수 있음 - 주로 범용의 패턴개발에 적합
3	Concrete contents composition	- 해당 도메인에 구체적인 내용이 포함되어 유사한 도메인, 대상에 대한 재사용성이 높음 - 일정한 내용을 지속적으로 제공할 수 있음 - 패턴의 재사용이 자주 발생되는 도메인, 대상의 정해진 경우에 적합 → 자주 사용되는 argument 들이 정해질 경우
4	Detailed contents composition	- 구체적이고 자세한 내용으로 인해 instance 생성이 쉬움 - 패턴이 타겟으로 하는 대상에만 적용이 용이하고, 재사용성이 낮아짐 - 실제 instance를 개발하는 것 과의 차이점 X - 적용 범위가 좁다는 단점 존재

Considerations of the classification

- SW in nuclear power plants
  - 표준에 따라 다양한 개발 산출물이 도출됨: 이를 바탕으로 safety demonstration을 위한 논증이 필요
    - Hazard analysis, safety requirements, V&V, formal verification, Etc.

- 원자력 발전소 safety SW를 대상으로 작성된 safety case 사례 확인

Case	Strategy	Sub-goal
(1)	Argument by satisfaction of all the desired **safety requirements**	Desired **safety requirements** for BP are not missed at all development phases The BP SW satisfies all the identified **safety requirements**
	Argument by **safety analysis activities**	Important SW contributable system **hazards** are not missed Remaining or newly introduced **hazards** through lifecycle are **managed**
(2)	Argument over V&V to demonstrate **functional correctness**	There is no **logical fault** in BP Formal proof that the software requirement satisfies **safety properties**
	Argument over **elimination or mitigation of hazards** Argument over **reliability demonstration** activities Argument over software **development process**	Etc.
두 경우 모두 SW를 대상으로 하고 있지만 다양한 strategy, sub-goal 들이 다르게 나타남 (safety demonstration을 위해 다양한 argument들을 바탕으로 함)		

이에 맞추어 패턴도 다양성을 커버
→ Domain specific 한 패턴 or 범용적 수준의 패턴에서 다양성을 커버하는 수준에서 작성이 바람직

결론 및 향후 연구

- Safety case pattern 작성의 범위 분류에 대한 고찰
  - For safety software in nuclear power plants
  - 다양한 문헌 조사를 바탕으로 수행
  - 4 단계로 구분: structural, high-level contents, concrete contents, detailed contents

- 현재는 수준에 대한 분류만을 수행
  - Pattern의 의미에서 구조적 작성(1) 및 contents 제공 (2, 3) 사이에서 혼란이 생길 수 있음
  - 향후 safety case pattern 작성 프로세스에 대한 연구를 계획 중

  - 원자력발전소의 소프트웨어를 대상으로 한 safety case pattern개발 또한 진행

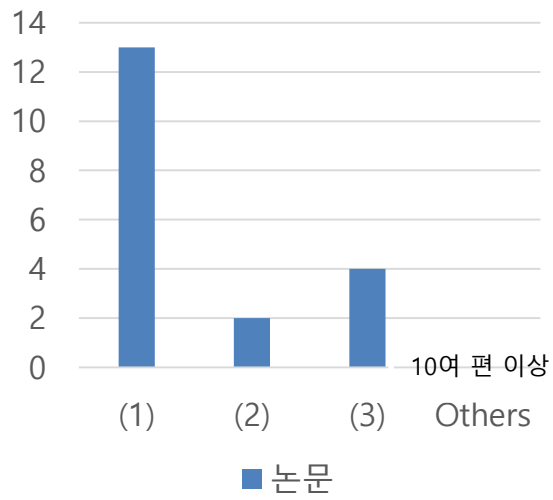
문헌 조사를 통한 패턴 리뷰

(1)
A Safety Case Pattern for Model-Based Development Approach
Composition of Safety Argument Patterns [4]
Applying Safety Case Pattern to Generate Assurance Cases for Safety-Critical Systems
A Security Argument Pattern for Medical Device Assurance Cases
Arguing from Hazard Analysis in Safety Cases: A Modular Argument Pattern
Assurance of Automotive Safety – A Safety Case Approach [6]
Arguing Software Compliance with ISO 26262
Accident Avoidance Pattern: Improving Knowledge for Safety Critical Domains
A Software Safety Argument Pattern Catalogue
The Safety of Software – Constructing and Assuring Arguments [3]
Arguing safety - a systematic approach to managing safety cases [5]
Safety Case Patterns: Theory and Applications [7]
Safety Cases for Advanced Control Software: Safety Case Patterns

(2)
Rethinking of Strategy for Safety Argument Development
Argument Schemes in Computer System Safety Engineering

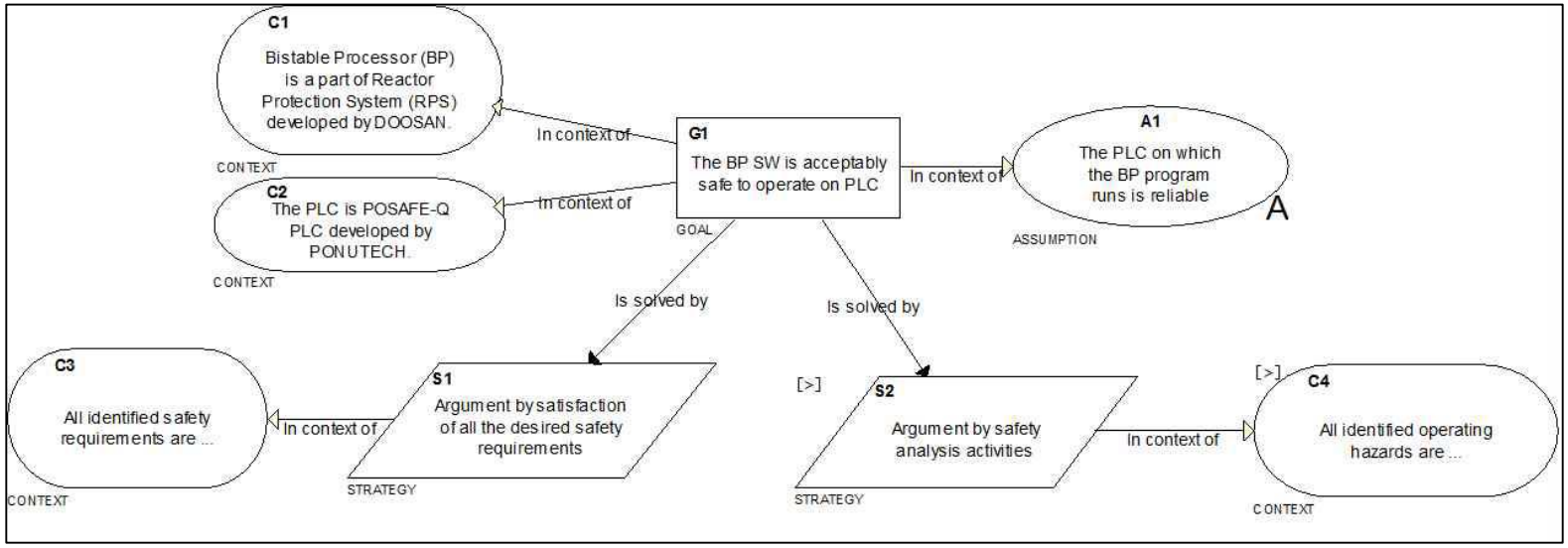
(3)
Principled Construction of Software Safety Case
Safety Cases: A review of Challenges
A Systematic Approach for Developing Software Safety Arguments
Software Safety Arguments: Toward a Systematic Categorization of Evidence

등



참고

- (1)원전 디지털 원자로보호계통 소프트웨어 안전보증 패러다임
  - Argument by satisfaction of all the desired safety requirements
    - Desired safety requirements for BP are not missed at all development phases
      - Design specification for BP includes all the desired safety requirements
      - Software requirements specification includes all the desired safety requirements
      - Software design specification include all the desired safety requirements
    - The BP SW satisfies all the identified safety requirements
      - Argument by V&V activities
  - Argument by safety analysis activities
    - Important SW contributable system hazards are not missed
    - Remaining or newly introduced hazards through lifecycle are managed



참고

- (2) 원자력 계측제어 소프트웨어의 안전성 분석을 위한 Safety Case 의 Arguments 개발 절차
  - Argument over V&V to demonstrate functional correctness
    - There is no logical fault in BP
    - Formal proof that the software requirement satisfies safety properties
  - Argument over elimination or mitigation of hazards
  - Argument over reliability demonstration activities
  - Argument over software development process