2016 한국 소프트웨어공학 학술대회

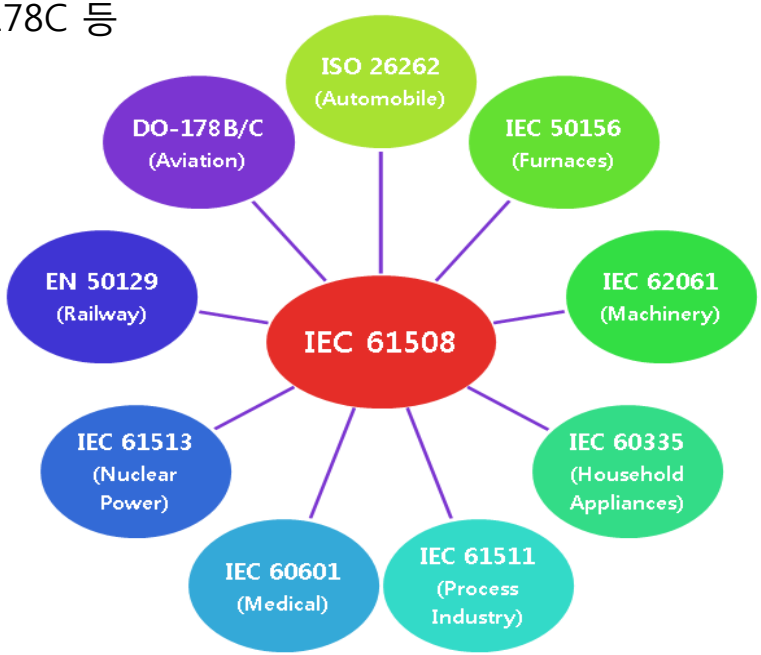
원자력 계측제어 소프트웨어의 안전성 분석을 위한 Safety Case의 Arguments 개발 절차

이동아, 유준범 (건국대학교)
이장수 (한국원자력연구원)

목차

서론

- 안전 필수 시스템(Safety Critical System)의 소프트웨어 역할 증가
- 소프트웨어 (기능) 안전을 위한 각 분야별 지침 및 표준
  - 원자력 – IEC 61513 등
  - 자동차 – ISO 26262 등
  - 항공 – DO-178C 등



- 표준 준수 = 안전성 확보 ?

배경지식 (1/3)

Safety Case

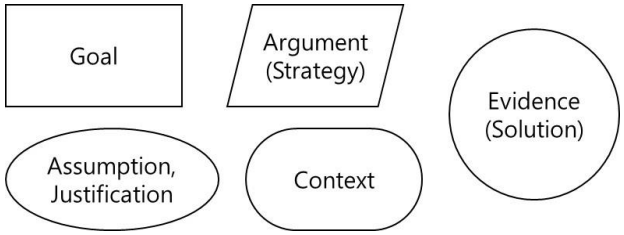
- 시스템이 안전함을 설득하기 위한 구조적이고 명시적인 자료 구조
  - 시스템이 안전함을 설득하기 위한 문서의 집합을 표현하는 용어
  - 설득하려는 시스템의 안전 수준 : ACCEPTABLY SAFE

- Goal, Argument, Evidence로 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)

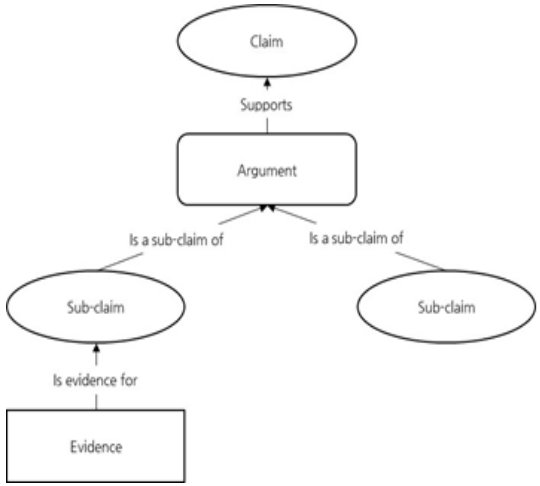
배경지식 (2/3)

GSN (Goal Structuring Notation)

- Safety Case의 구조를 시각적으로 표현하기 위한 대표적인 방법
  - cf. CAE (Claims Arguments and Evidence)



- 최상위 Goal
  - 예 : *"The system is acceptably safe"*
- Goal 달성을 위한 합리적인 Arguments 도출
  - 예 : *"Argument over the safety requirement X"*
- 이를 뒷받침 할 수 있는 Evidence
  - 예 : *"Safety requirement X is formally verified"*
- Assumption, Justification, Context, etc.



배경지식 (3/3)

- 안전 : 인명피해나 환경파괴와 같은 심각한 결과와 관련된 용어
  - 소프트웨어 단독의 오류나 실패가 안전과 관련된 심각한 결과를 초래하지 않음

- 현대의 안전 필수 시스템 : 소프트웨어가 시스템의 제어에 직접적으로 관여하기 때문에 그 결과가 물리적인 결과로 이어질 수 있음
  - 안전 필수 소프트웨어 (Safety Critical Software)

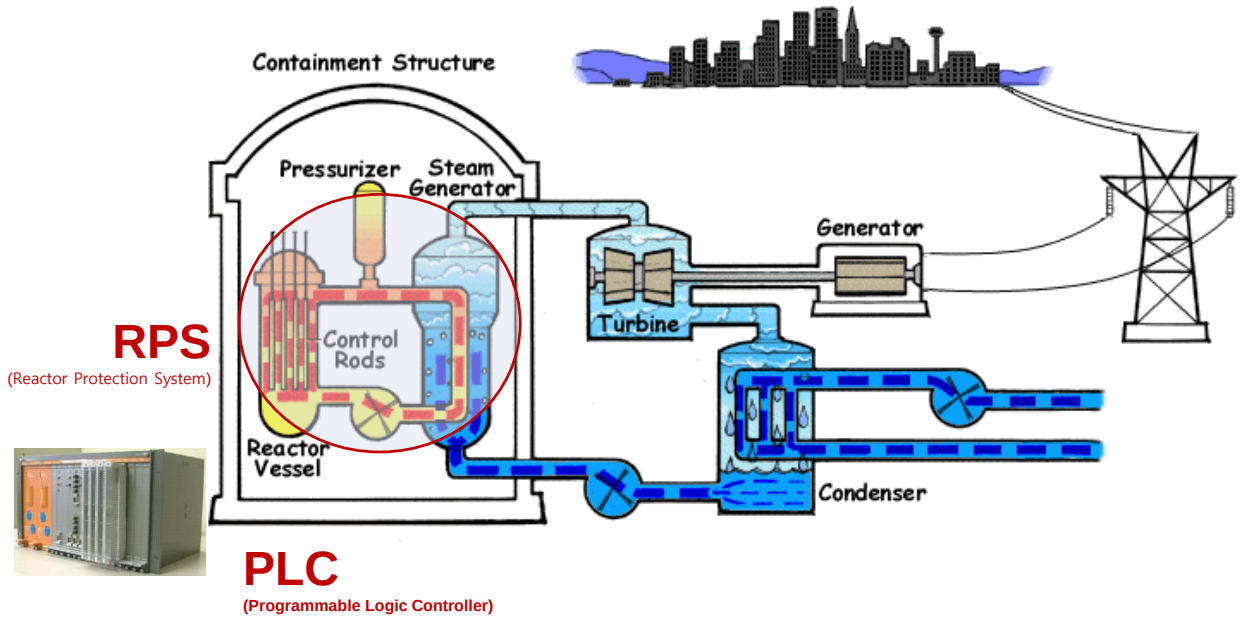
Safety Analysis of Software

- 시스템의 안전을 위협할 수 있는 기능에 대한 결함(flaw)이나 불완전성(incompleteness)에 대한 분석 수행
  - 하드웨어와 달리 마모를 고려할 필요가 없음
  - 행위의 결과에 대한 확률적 분석을 수행할 수 없음

- 원자력 계측제어 소프트웨어의 안전성 분석을 위해 요구사항부터 개발에 이르는 전 과정에 대한 분석을 수행하였음

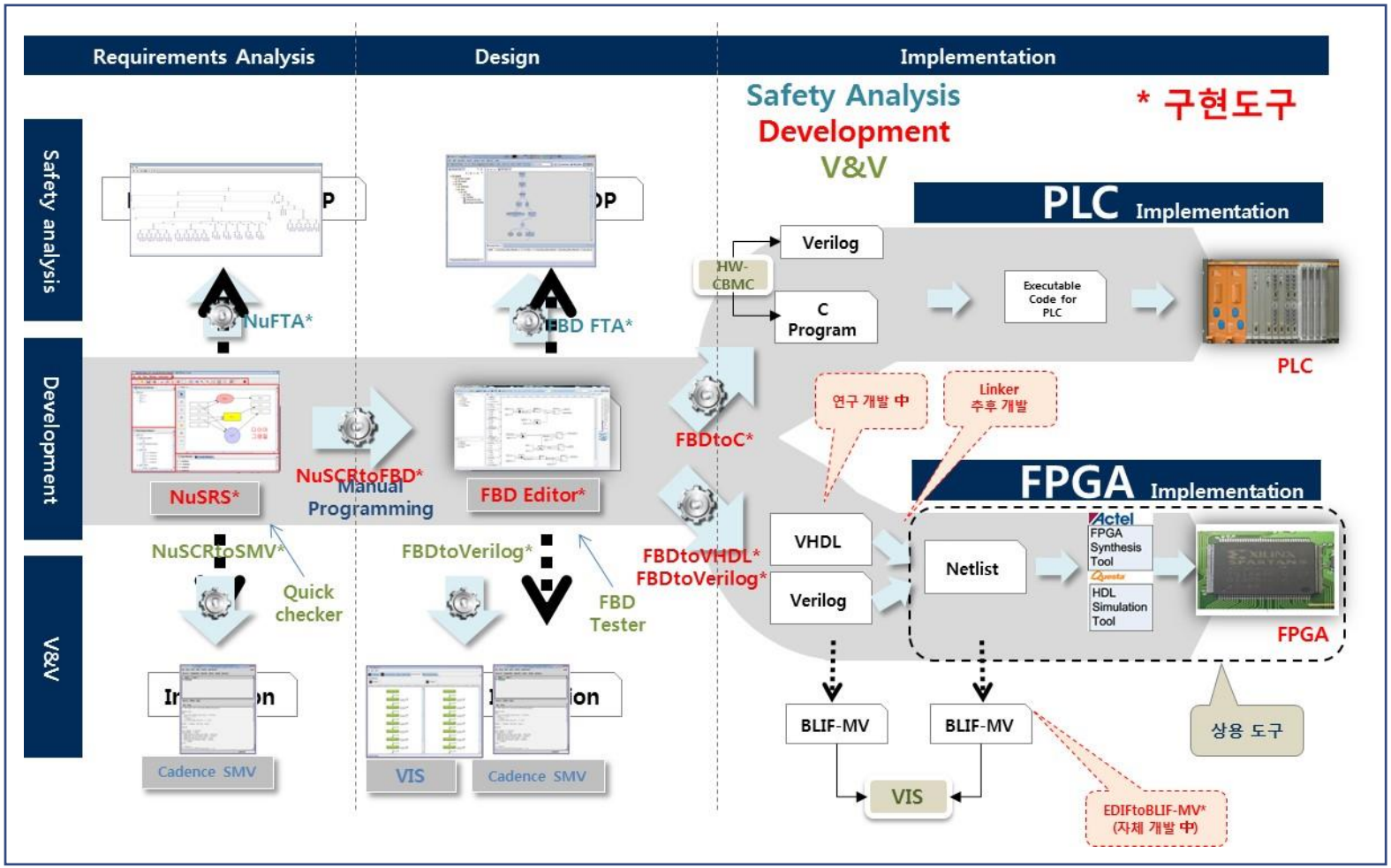
Safety Case를 이용한 RPS SW 안전성 분석

- 원자력 계측제어 소프트웨어 BP (Bistable Processor)
  - 원자로에 이상이 생겼을 경우 원자로 정지
  - 센서의 값이 트립(trip) 설정치를 초과할 경우 자동으로 트립을 개시(원자로 정지)



Safety Case를 이용한 RPS SW 안전성 분석

- 원자력 계측제어 소프트웨어 BP (Bistable Processor)
  - 원자로에 이상이 생겼을 경우 원자로 정지
  - 센서의 값이 트립(trip) 설정치를 초과할 경우 자동으로 트립을 개시(원자로 정지)



Safety Case를 이용한 RPS SW 안전성 분석

Goal	G1: BP is acceptably safe to operate within in PLC
Context	C1: BP (Bistable Processor) is a software C15: PLC is POSAFE-Q
Assumption	A1: Safety demonstration of PLC hardware is already finis hed by hardware engineers. A4: "Safe" means that BP is functionally and non-function ally correct.

- BP에 대한 안전성 분석을 수행하기 위한 첫 단계
  - 분석의 목적 설정
- BP에 대한 배경지식을 포함한 가정과 제약사항을 기술
- 안전에 대한 개념 전달
  - 기능적/비기능적 정확성에 기반

Safety Case를 이용한 RPS SW 안전성 분석

Strategy (Argument)	S1: Argument over V&V to demonstrate functional correctness
	S7: Argument over elimination or mitigation of hazards
	S11: Argument over reliability demonstration activities
	S12: Argument over software development process

- BP의 안전성을 설득하기 위한 4 가지 전략 수립

- 기능적 정확성을 보이기 위한 두 가지 전략
  - V&V 활동을 통한 안전성 주장
  - 소프트웨어 내/외부의 위험요소 제거를 통한 안전성 주장

- 비기능적 정확성을 보이기 위한 두 가지 전략
  - 신뢰성(Reliability) 확보를 통한 안전성 주장
  - 개발 절차에 대한 타당성을 통한 안전성 주장

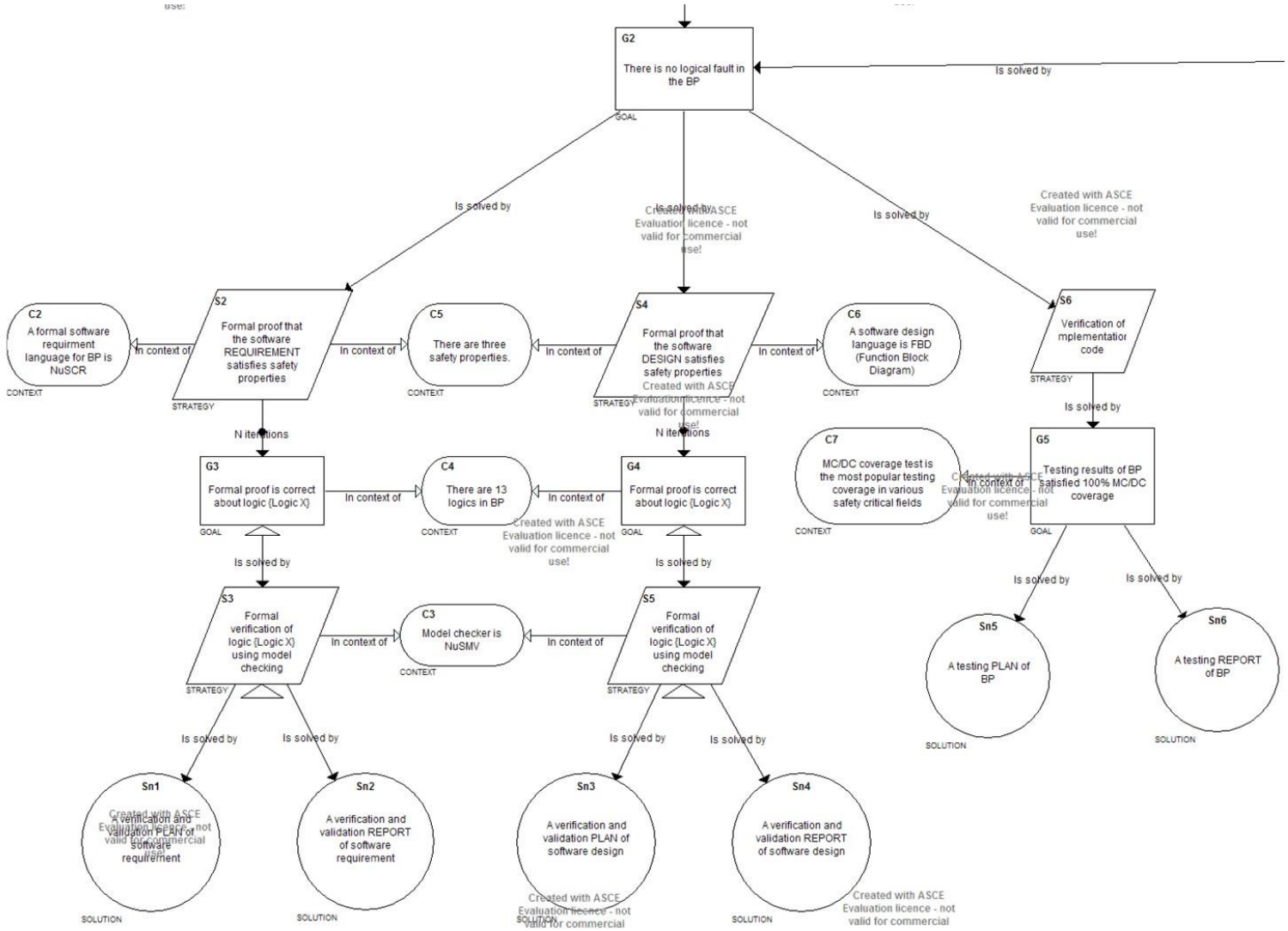
Safety Case를 이용한 RPS SW 안전성 분석

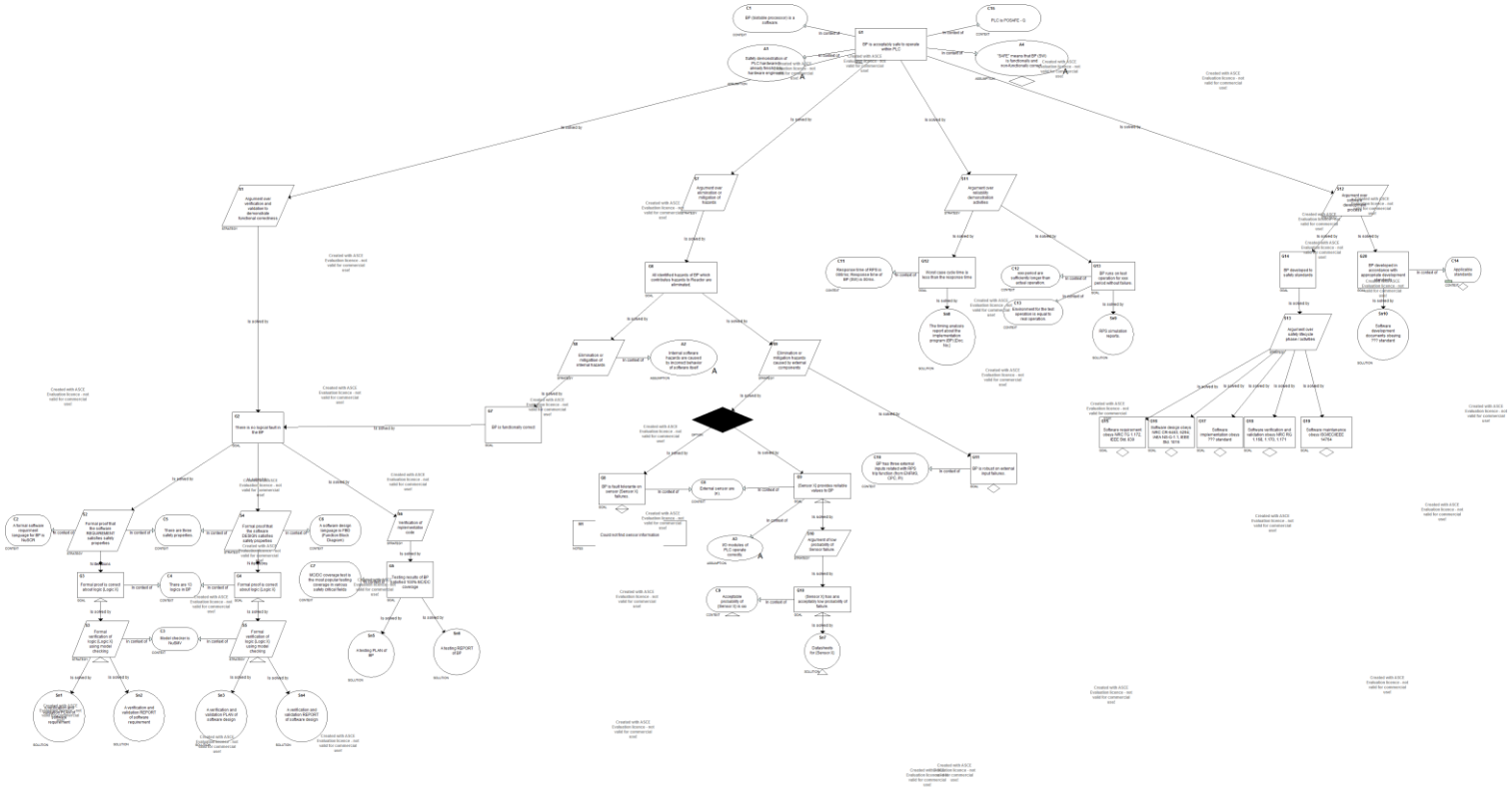
Sub-goal	G2: There is no logical fault in the BP
Strategy	S2: Formal proof that the software requirement satisfies s afety properties

Evidence (Solution)	Sn1: A V&V plan of software requirement Sn2: A V&V report of software requirement

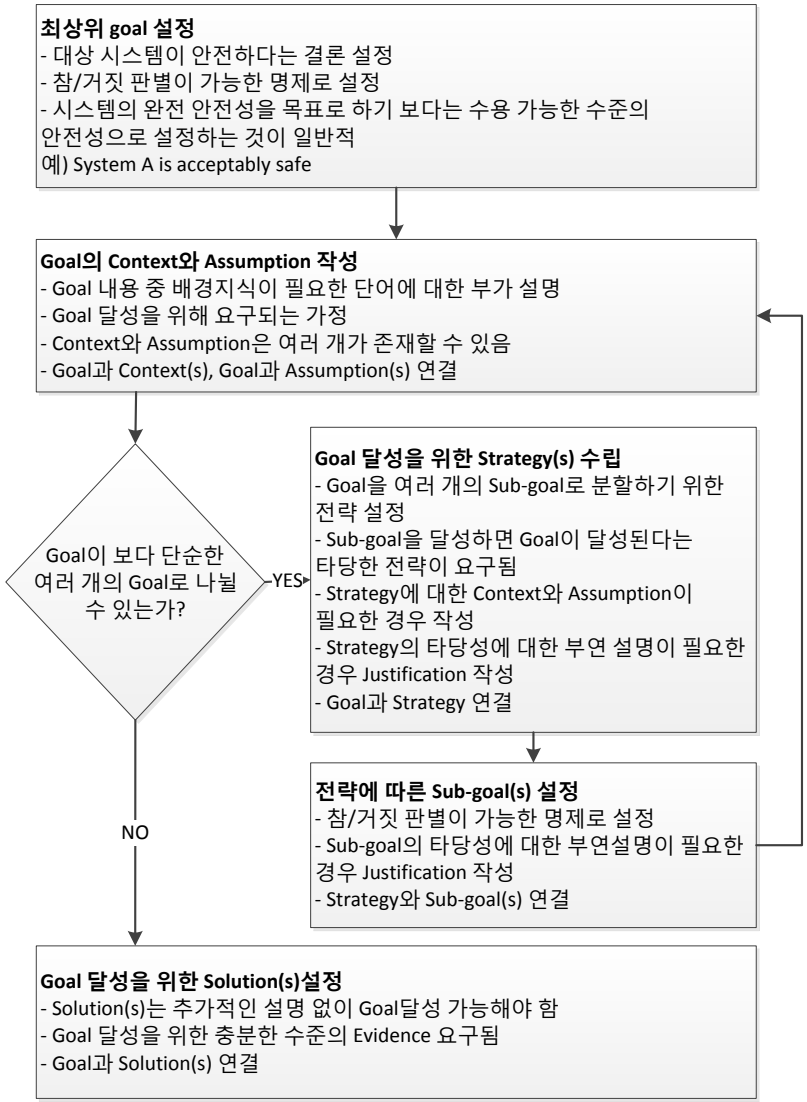
- S1을 달성하기 위한 Sub-goal 설정
  - Argument over V&V to demonstrate functional correctness
- BP 내에 논리적인 오류가 없음을 목표로 하는 Sub-goal 설정
- 정형 기법을 이용한 소프트웨어 요구사항 검증
  - NuDE 환경에서의 정형 요구사항 명세에 대한 검증 수행
- 소프트웨어 요구사항 검증 계획 및 검증 수행 보고서의 정형 검증 관련 항목 → S2의 주장을 뒷받침할 근거자료

G2 달성을 위한 전략 및 근거





Safety Case 작성 절차



결론 및 향후 연구

결론

- 원자력 계측제어 소프트웨어의 안전성 분석을 위해 Safety Case 도출
- Safety Case의 수준은 분석가의 역량에 따라 큰 차이를 보임
  - 핵심적인 부분은 목표를 어떻게 달성시킬 수 있을지에 대한 Argument (Strategy)를 타당하게 도출하는 것이 관건
- 원자력 소프트웨어의 Safety Case를 도출을 위한 네 가지 Argument 제시
  - V&V, elimination or mitigation of hazards, reliability demonstration, software development process

향후 연구

- BP 개발 시 작성한 산출물을 활용한 실제 Evidence 확보
- Safety Case Argument Pattern을 통한 효과적인 Safety Case 도출 지원

감사합니다.

이동아
ldalove@konkuk.ac.kr
Dependable Software Laboratory
건국대학교