NuSCPI: 원자력발전소의 디지털 계측제어 소프트웨어를 대상으로 개발된 Safety Case Pattern 작성을 위한 CASE 도구

손준익 * , 정세진 * , 유준범 * , 이영준 * *

* 건국대학교 컴퓨터공학과
** 한국 원자력 연구원

{sji6227, jsjj0728, jbyoo}@konkuk.ac.kr
yjlee426@kaeri.re.kr

목차

서론 및 배경지식

서론

- 원자력 디지털 계측제어 시스템은 안전 필수 시스템 (Safety Critical System)으로 해당 시스템의 **소프트웨어에 대한 안전성 분석**은 필수
  - 표준 : IEEE 1228
  - 규제기관 : NUREC-6430

- Safety case : 시스템이 용인되는 수준의 안전성을 갖췄는지 보이기 위한 목표 기반 방법
  - safety case를 작성하는데 **많은 비용과 노력이 필요**

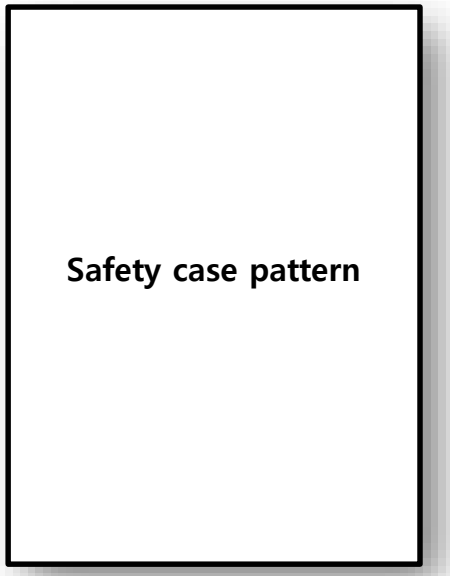
→ **Safety case pattern** : safety case 구조를 패턴화 하여 safety case를 작성하는 방법

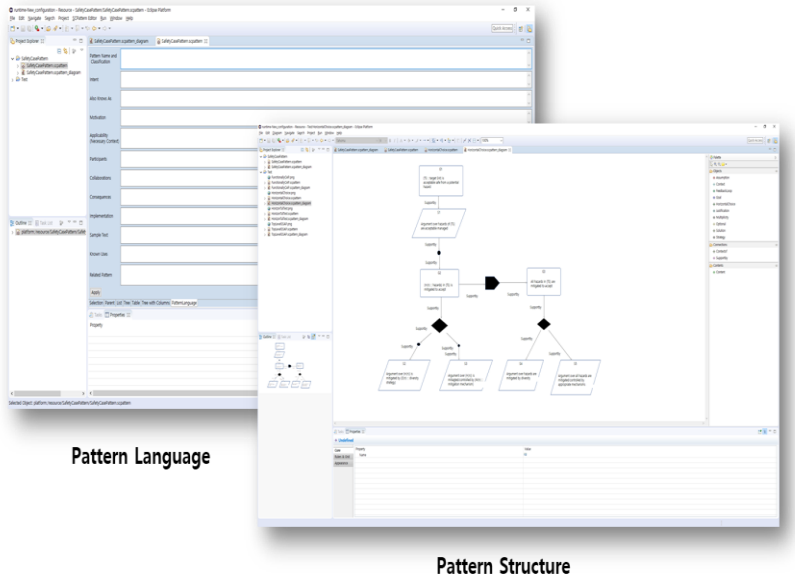
서론

- 원자력발전소 디지털 계측제어 소프트웨어를 대상으로 safety case pattern 개발
  - 해당 safety case pattern 작성을 지원하기 위한 CASE 도구 필요

NuSCPI : 원자력발전소의 디지털 계측제어 소프트웨어를 대상으로 개발된 Safety case pattern 작성을 위한 CASE 도구

- **추가적인 GSN 요소 정의**
- **매개변수 작성 규칙 정의**





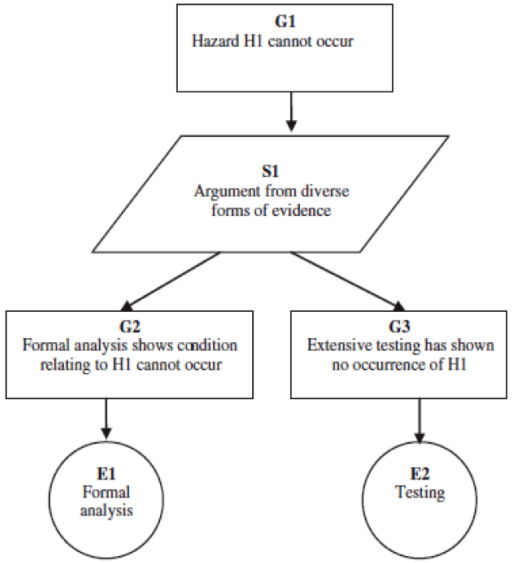
Safety case

- 시스템이 안전하다는 것을 증명하기위한 **구조적이고 명시적인 자료 구조**
- **Goal, Argument, Evidence로 이루어진 구조적인 논증 구조**
  - **Goal** : 명제로 표현된 달성하고자 하는 목표
  - **Argument** : 목표가 달성됨을 보이기 위한 전략
  - **Evidence** : 목표 달성을 뒷받침 할 수 있는 근거

- **Safety Argument** : Safety case의 요소들이 어떻게 연관되어 있는지 보여주는 것

```
The Defence in Depth principle (P65) has been
addressed in this system through the provision of
the following:
• Multiple physical barriers between hazard source
  and the environment (see Section X)
• A protection system to prevent breach of these
  barriers and to mitigate the effects of a barrier
  being breached (see Section Y)
...
```

서술 형식



시각적 형식

Safety case

- **GSN(Goal Structuring Notation)**

  : Safety case의 논증구조를 시각적으로 표현하기 위한 방법

  cf. CAE (Claims Arguments and Evidence)

  - **Goal**

    : 안전, 신뢰도 등 시스템 속성에 대한 요구조건/목표

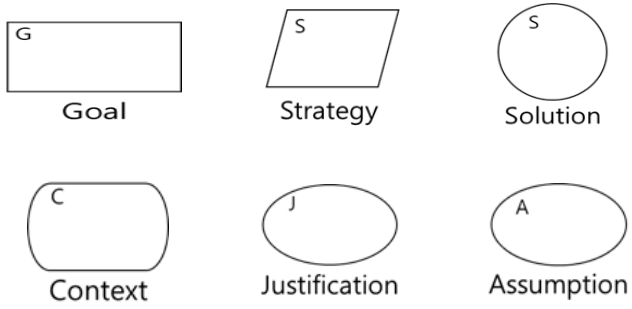
    - 예 : *"The system is acceptably safe"*
  - **Strategy (Argument)**

    : Goal 달성을 위한 합리적인 전략

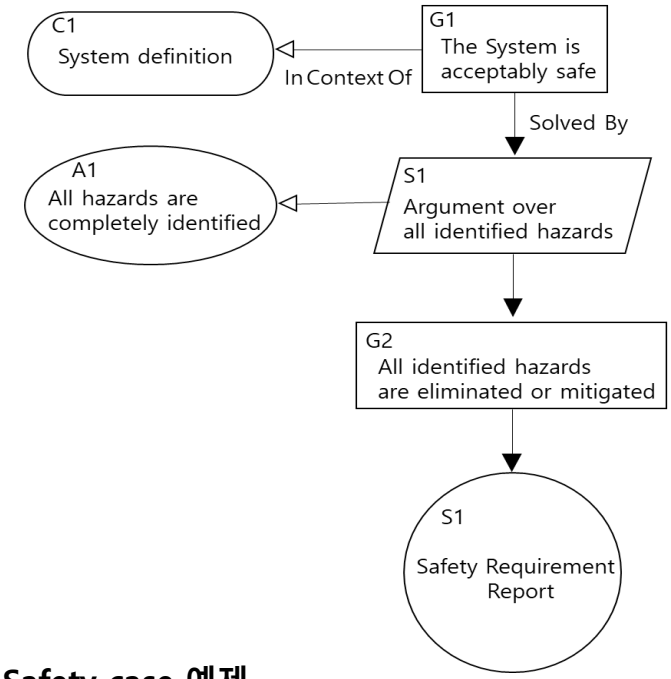
    - 예 : *"Argument over the safety requirement X"*
  - **Solution (Evidence)**

    : Goal을 뒷받침 할 수 있는 근거

    - 예 : *"Safety requirement report"*
  - **Context, Justification, Assumption**



GSN 요소



Safety case 예제

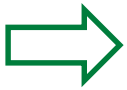
Safety case pattern

- 잘 작성된 Safety case의 구조를 패턴화 하여 safety case를 작성하는 방법
  - 패턴의 적절하지 못한 재사용 문제를 막기 위하여 pattern language 작성

- **Pattern language**

Pattern Name	
Intent	
Also Known As	
Motivation	
Applicability	
Structure (GSN)	
Participants	
Collaborations	
Consequences	
Related Pattern	

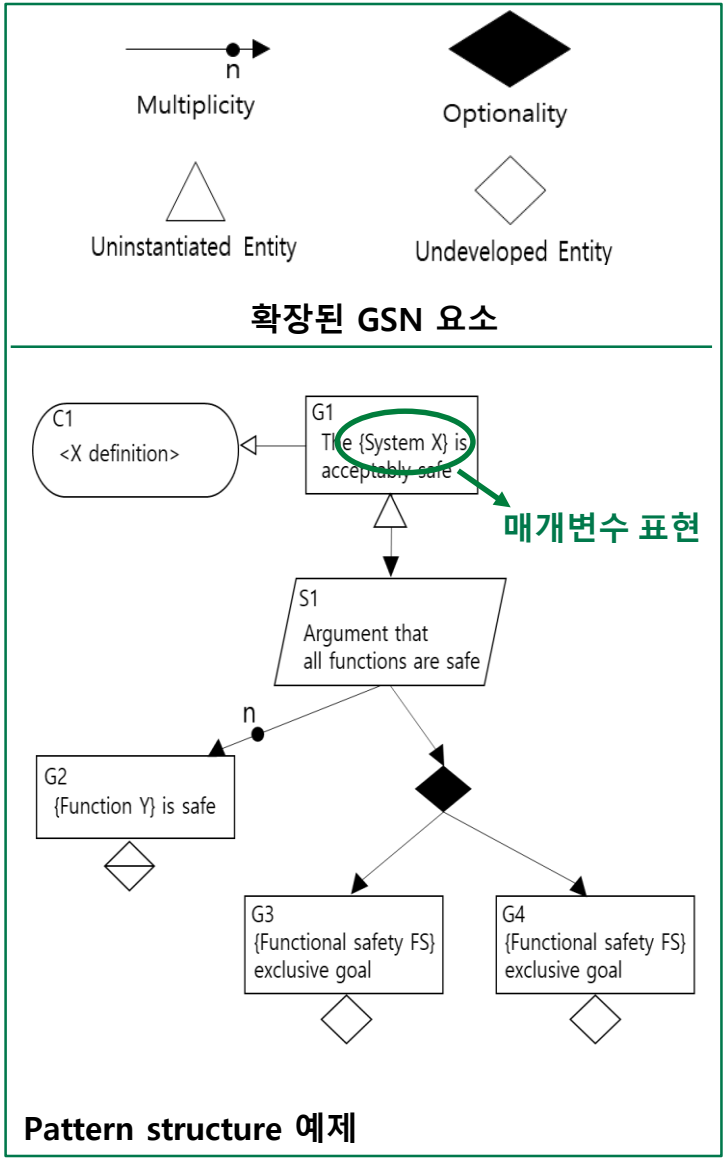
Pattern language 형식



작성된 Pattern

Safety case pattern

- **Pattern Structure**
  - 일반적으로 GSN을 사용
  - Safety case 논증 구조의 추상화를 위해 **GSN 확장**
- **확장된 GSN**
  - **Multiplicity**
    : 하나의 GSN 요소가 다수의 GSN 요소와 관계 되어있음을 나타냄
  - **Optionality**
    : 논증 구조를 만족시키는 가능한 선택지를 나타냄
  - **Uninstantiated Entity**
    : Goal 아래에 표현되어 해당 goal이 인스턴스화 되지 않은 매개변수 표현식을 가지고 있음을 나타냄
  - **Undeveloped Entity**
    : Goal 아래에 표현되어 해당 goal이 추가적인 전개가 필요함을 나타냄
- **매개변수 표현**
  - {Class X} 로 작성되며 인스턴스화 될 때 X를 정의



NuSCPI: 원자력발전소의 디지털 계측제어 소프트웨어를 대상으로 개발된
Safety Case Pattern 작성을 위한 CASE 도구

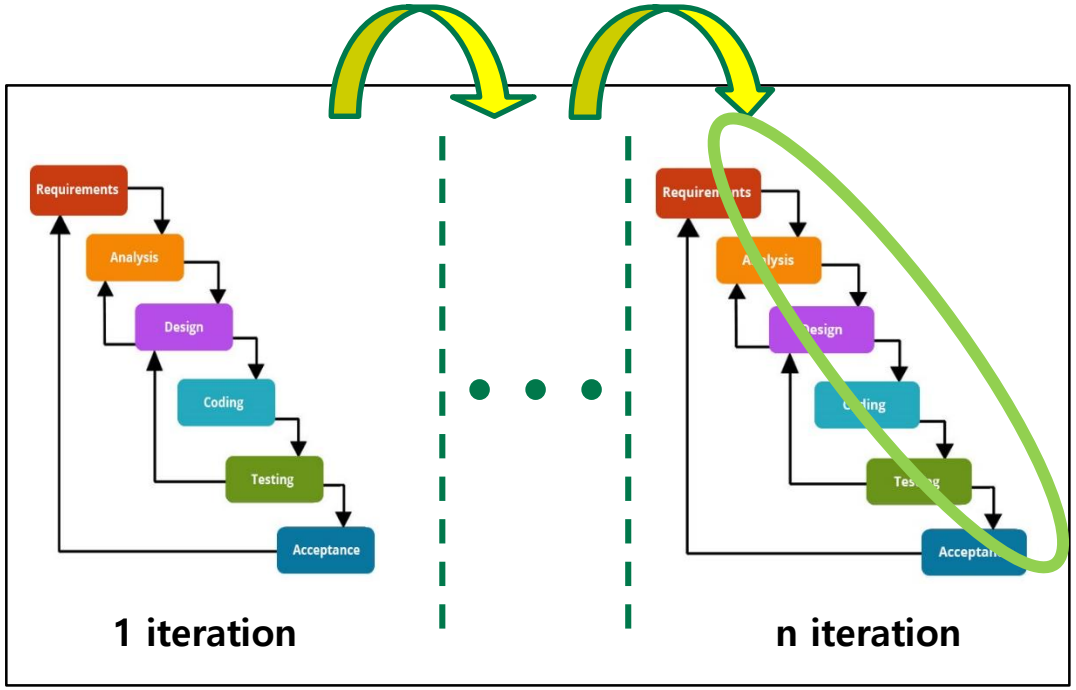
NuSCPI

NuSCPI

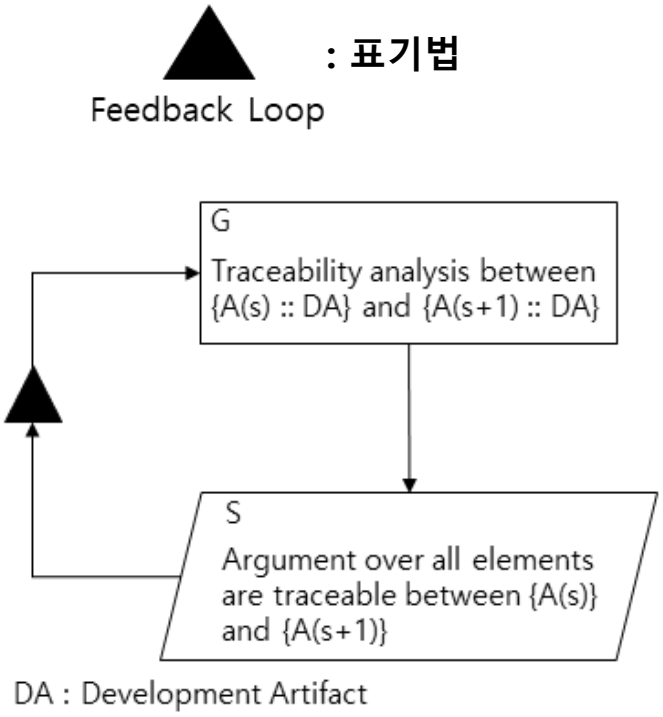
- **NuSCPI** : 원자력 디지털 계측제어 소프트웨어를 대상으로 작성된 safety case pattern 작성을 지원하는 CASE 도구
  - 목표 도메인의 safety case pattern 구조의 추상화를 위한 **추가적인 GSN 요소 정의**
  - Pattern Structure의 safety case로의 인스턴스화의 자동화를 위한 **매개변수 작성 규칙 정의**

NuSCPI : 추가된 GSN 요소

- **Feedback loop**
  - 반복되는 논증 구조를 나타냄
  - **필요성** : SW 개발시 각 단계별 or 각 iteration 사이의
    산출물 간의 반복적인 논증 구조가 필요할 시 이를 추상화 하기 위함



SW 개발 프로세스

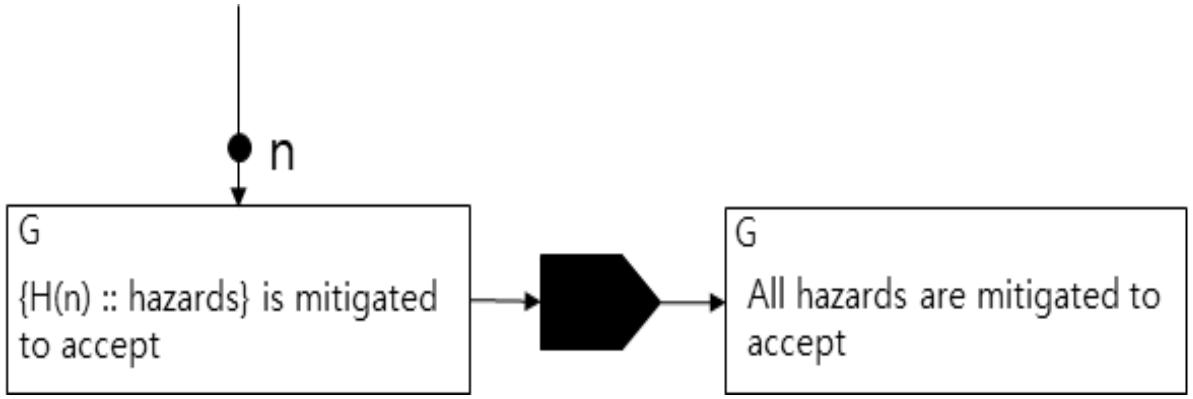


Feedback Loop 예제

NuSCPI : 추가된 GSN 요소

- **Horizontal Choice**
  - 연결된 요소 중 하나의 요소만 무조건적으로 선택됨을 나타냄
  - **필요성** : 목표 시스템 또는 소프트웨어에 따라 여러 목표(Goal) 또는 전략(Strategy) 중 하나의 요소만 선택 되어야 하는 경우를 표현하기 위함

: 표기법

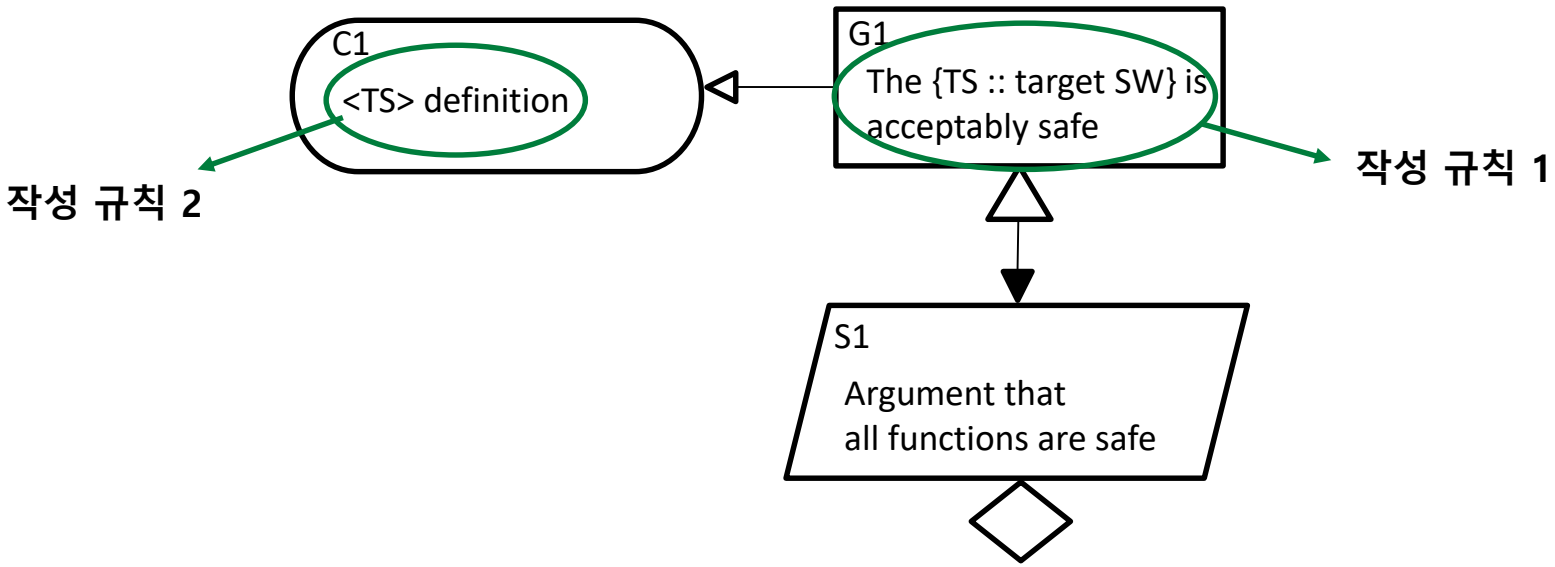


Horizontal Choice 예제

NuSCPI : 매개변수 작성 규칙

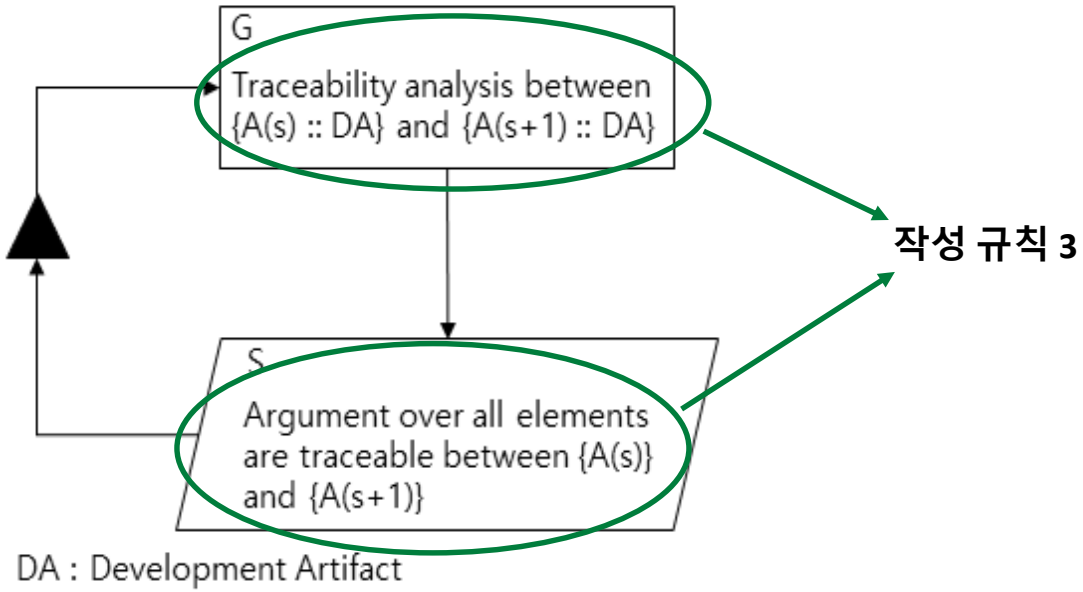
- 작성 규칙 1 : {X :: Class}
  - 설명 : GSN 요소에서 단일 매개변수를 표현하기 위해 사용

- 작성 규칙 2 : <X> definition
  - 설명 : GSN 요소에 작성된 매개변수 표현식에 대한 context, assumption의 내용 작성 시 매개변수에 대한 정의가 반드시 요구되는 부분에 사용



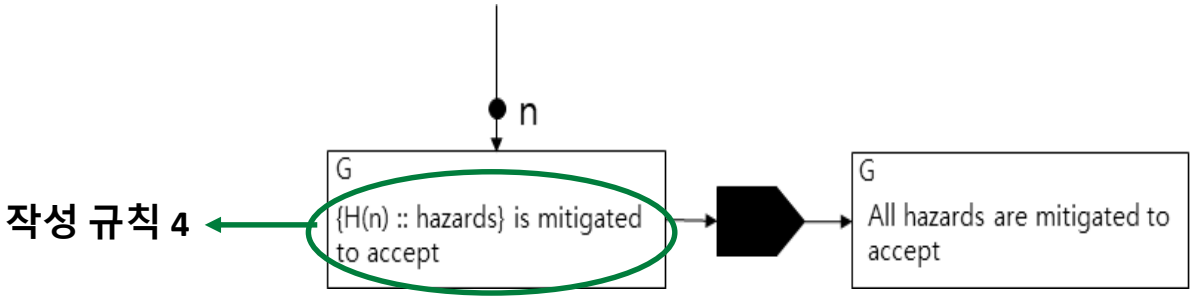
NuSCPI : 매개변수 작성 규칙

- 작성 규칙 3 : {X(s) :: Class}, {X(s+1) :: Class}
  - 설명 : feedback loop과 연결되어 있는 GSN 요소에서 다중 매개변수를 표현하기 위해 사용



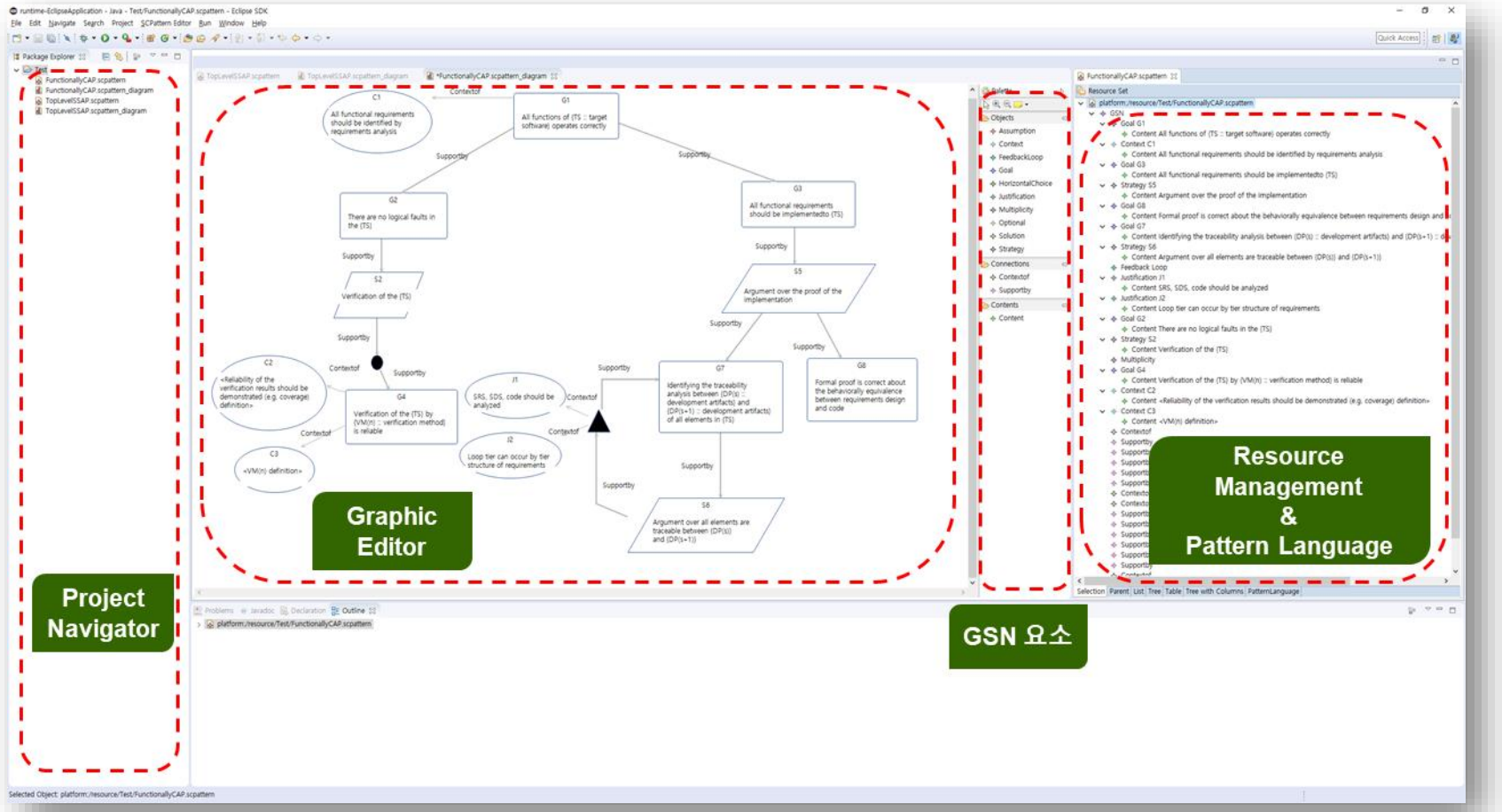
NuSCPI : 매개변수 작성 규칙

- 작성 규칙 4 : {X(n) :: Class}
  - 설명 : multiplicity와 연결되어 있는 GSN 요소에서 다중 매개변수를 표현하기 위해 사용



- 작성 규칙 5 : '{X :: Class}'
  - 설명 : safety case pattern의 GSN 요소에 작성된 내용 안에 있는 매개변수 표현식을 인스턴스화 하지않고 safety case 내의 요소에 바로 반영하기 위해 사용

NuSCPI : 구현


Project Navigator
Graphic Editor
GSN 요소
Resource Management & Pattern Language

NuSCPI : 구현

- **NuSCPI** : Safety case editor + Safety case pattern editor

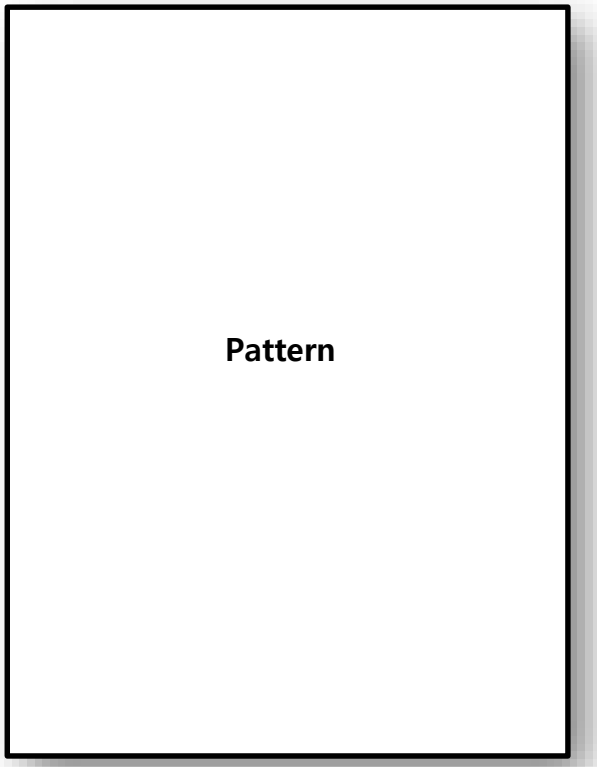
- **Safety case Editor**
  - Rich Client Platform
  - Graphical Modeling Framework (GMF)
  - Safety case pattern의 safety case로의 기계적인 **인스턴스화** 및 safety case 작성 지원

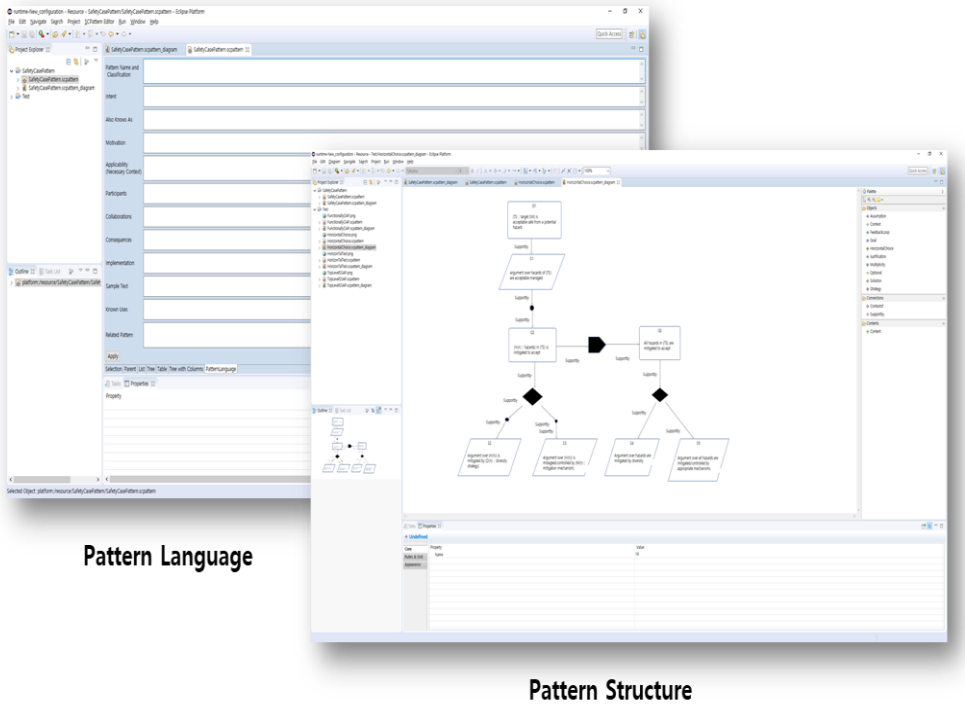
- **Safety case pattern Editor**
  - Eclipse Plug-in
  - Graphical Modeling Framework(GMF)
  - Pattern structure + Pattern language 작성 지원

NuSCPI : Case Study

- 원자력발전소의 디지털 계측제어 소프트웨어를 대상으로 개발된 Safety case pattern을 이용하여 safety case pattern 및 safety case 작성 수행

1. Safety case pattern 작성 - Pattern Language 및 Pattern Structure 작성





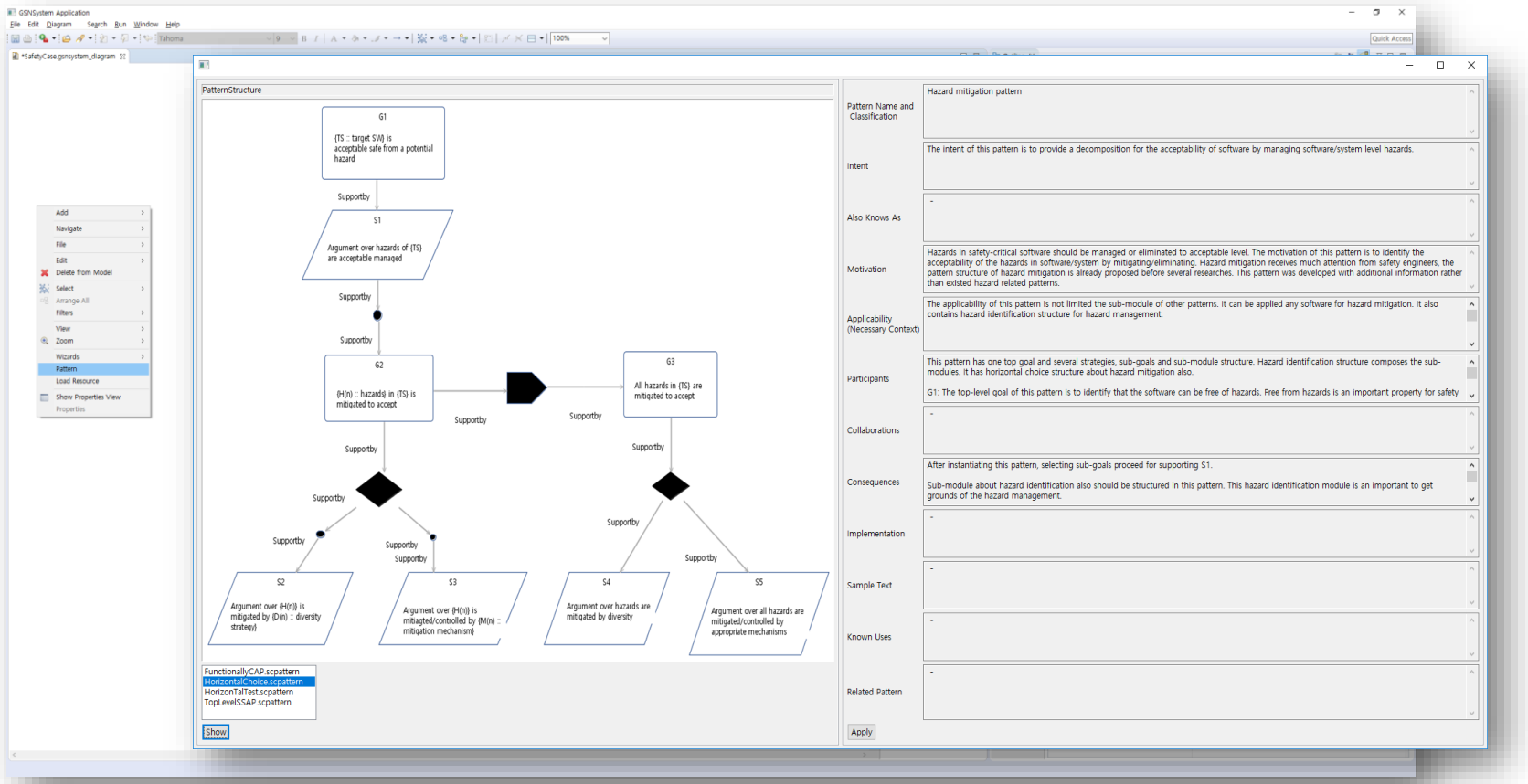
Pattern Language

Pattern Structure

NuSCPI : Case Study

- 원자력발전소의 디지털 계측제어 소프트웨어를 대상으로 개발된 Safety case pattern을 이용하여 safety case pattern 및 safety case 작성 수행

2. Safety case pattern의 safety case 로의 인스턴스화

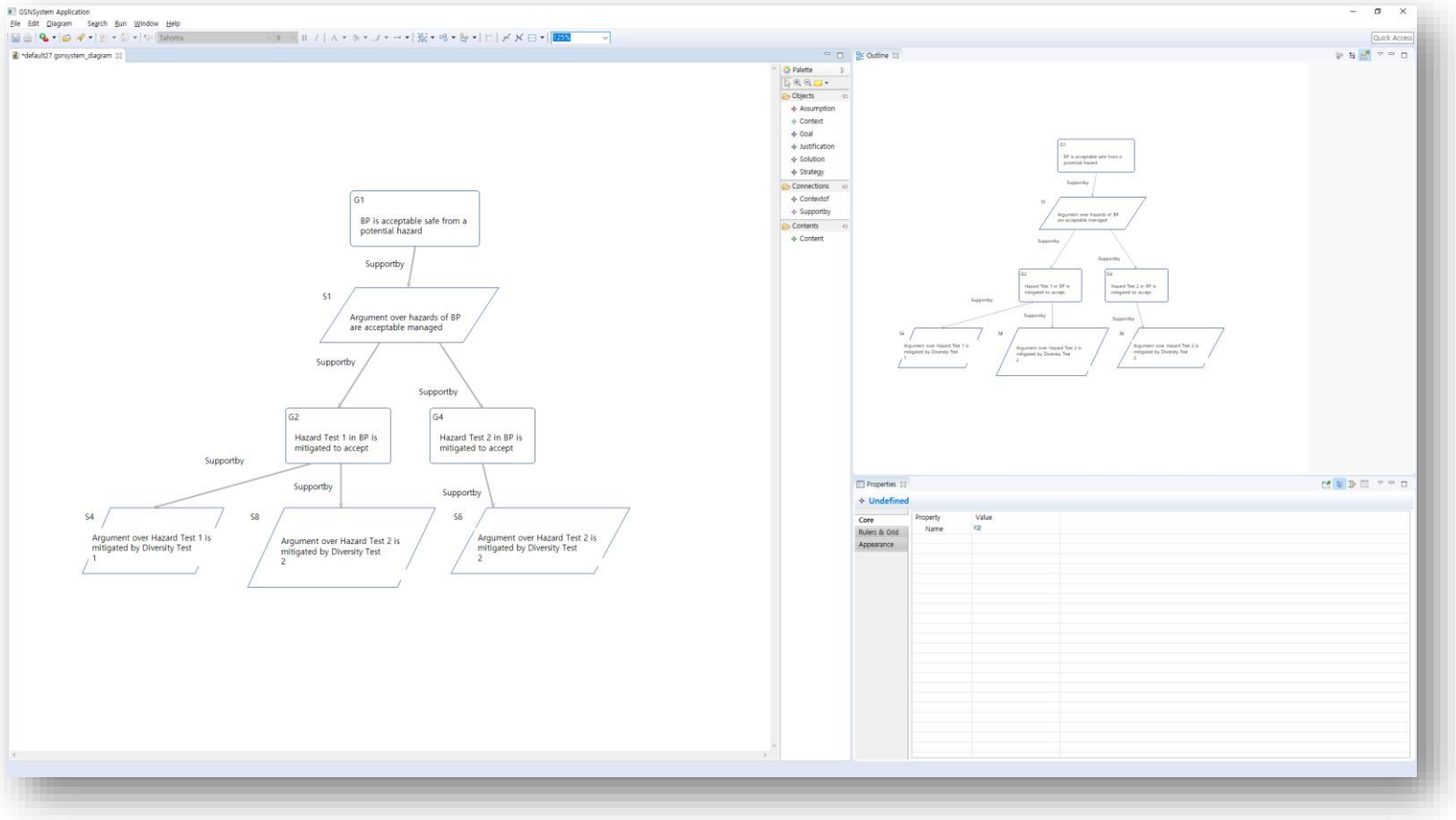


추상화 요소 및 매개변수 표현 정의

NuSCPI : Case Study

- 원자력발전소의 디지털 계측제어 소프트웨어를 대상으로 개발된 Safety case pattern을 이용하여 safety case pattern 및 safety case 작성 수행

3. Safety case 작성



결론 및 향후 연구

결론 및 향후 연구

- 원자력 디지털 계측제어 소프트웨어를 대상으로 작성된 safety case pattern 작성을 지원하는 NuSCPI 개발
  - Pattern structure의 추상화를 지원하기 위한 추가적인 GSN 요소 정의
  - Safety case pattern의 safety case로의 인스턴스화의 자동화를 위한 매개변수 작성 규칙 제안

- 도구의 유용함을 확인하기 위해 safety case pattern 및 safety case 작성 수행

- 향후 연구
  - safety case의 요소와 관련 있는 산출물의 연결
  - 원자력 도메인의 특징을 반영할 수 있는 방법

손준익
sji6227@konkuk.ac.kr

Dependable Software Laboratory
건국대학교

Thank you

2017 한국소프트웨어 종합학술대회 (KSC 2017)
2017. 12. 20 ~ 22