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

손준익[O1] 정세진[1] 유준범[1] 이영준[2]
[1]건국대학교 컴퓨터-정보통신 공학부, [2]한국 원자력 연구원
{sji6227, jsjj0728, jbyoo}@konkuk.ac.kr, yjlee426@kaeri.re.kr

NuSCPI: A CASE tool for Constructing the Safety Case Pattern for Digital I&C Software of Nuclear Power Plant

Junik Son[O1] Sejin Jung[1] Junbeom Yoo[1] Young Jun Lee[2]
[1]Division of Computer Science and Engineering, Konkuk University
[2]Korea Atomic Energy Research Institute

요 약

원자력발전소의 디지털 계측제어 소프트웨어는 안전 필수 시스템에서 핵심적인 부분으로 안전성에 대한 분석이 반드시 요구된다. 다양한 안전 필수 분야에서 사용이 되는 safety case는 안전성 분석 기법으로서 시스템이 용인되는 수준의 안전성을 갖췄는지 보이기 위한 논증 구조를 표현하는 기법이다. 유사한 시스템의 경우 safety case 논증 구조에 반복적인 구조들이 나타난다. safety case pattern은 잘 작성된 safety case의 반복적인 구조의 재사용을 통해 효율적인 논증 구조를 작성하는 방법으로 패턴의 구조 작성에 필요한 요소와 패턴의 인스턴스화에 대한 많은 연구가 진행 중이다. 본 논문에서는 디지털 계측제어 소프트웨어를 위한 safety case pattern을 위해 몇몇 추가된 GSN (Goal structuring notation) 요소 및 매개변수 작성규칙을 제안하고, safety case pattern 작성 및 인스턴스화의 부분적인 자동화를 지원하는 CASE 도구인 NuSCPI를 소개한다.

1. 서 론

원자력발전소의 디지털 계측제어 시스템 (I&C: Instrumentation and Controller)은 안전 필수 시스템(Safety Critical System)으로 사고가 발생할 시 돌이킬 수 없는 인명피해나 환경오염을 초래할 수 있는 중대한 시스템이다. 이러한 특징 때문에 계측제어 시스템에서 핵심적인 부분인 소프트웨어에 대한 안전성 또는 위험성 분석을 통해 안전성을 높이는 활동이 반드시 필요하다.

Safety case[1]는 다양한 안전 필수 분야에 사용이 되는 근거 기반 방법론 혹은 목표 기반 방법론으로 시스템이 안전하다는 것을 증명할 수 있는 하나의 방법이다. safety case는 다양한 안전 필수 분야에 사용이 되는데, safety case를 이용한 시스템 또는 소프트웨어의 안전 논증을 수행하는 데에 있어 많은 비용과 노력이 필요하다. 유사한 시스템의 경우 safety case 논증 구조에 반복적인 구조가 나타난다. 이러한 반복 구조를 임의로 재사용 하는 것은 일관성 부족, 부적절한 재사용 등의 문제를 유발한다. 이러한 문제를 해결하기 위해, 잘 작성된 safety case내에서 사용되는 반복 구조를 패턴화 하여 safety case의 논증 구조를 작성하는 방법으로 safety case pattern[2] 방법이 있다.

Safety case pattern은 전체적으로 재사용 가능한 safety case를 작성하는 것이 아닌 safety case 내의 요소, 주제 및 구조화 개념만을 정의하는 것을 목적으로 한다. 이를 위해 GSN에 추상화를 지원할 수 있는 요소를 추가하여 추상화된 구조를 작성한다. 또한, 패턴의 적절하지 못한 재사용 문제를 막기 위하여 패턴의 의도, 상황 및 적용 가능성을 문서화 할 수 있도록 pattern language도 작성한다. safety case pattern 분야는 새로운 연구 분야로서 패턴 작성에 사용되는 GSN 요소의 확장과 safety case pattern의 인스턴스화를 위한 여러 연구가 진행되고 있다[3][4].

본 논문에서는 원자력발전소의 디지털 계측제어 소프트웨어를 대상으로 개발 중인 safety case pattern을 위해 추가한 GSN 요소 및 매개변수 작성규칙을 제안하고, safety case pattern의 작성 및 인스턴스화를 위한 CASE 도구인 NuSCPI를 소개한다.

2. Safety case & Safety case pattern

Safety case는 시스템이 용인되는 수준의 안전성을 갖췄는지 보이기 위한 구조화된 논증 구조이다. 기존의 Safety case는 서술 형식으로 작성되었는데 복잡한 논증 구조를 정확하게 표현하고, 또 그 의미를 정확하게 이해하는 것에서 어려움이 존재하여 시각적으로 표현하는 표기법이 개발되었다. GSN[6]과 CAE (Claim, Argument, Evidence)[7]는 safety case를 시각적으로 표현하는 대표적인 표기법이다. 본 논문에서는 safety case pattern에 사용되는 GSN 표기법에 대해서만 소개를 한다. <표 1>은 GSN의 요소에 대한 표기법 및 설명을 나타낸다.

표 1. GSN 요소

요소 및 표기법	설명	요소 및 표기법	설명
G Goal	안전, 신뢰도 등 시스템 속성에 대한 요구조건/목표	J Justification	Goal, Strategy에 대한 타당성을 설명
S Strategy	Goal을 나누는 기본 논리, Goal과 sub-goal을 연결시키는 논리	A Assumption	Goal, Strategy를 도출하는데 쓰인 가정
S Solution	테스트, 시뮬레이션, FTA 등 분석결과로 Goal에 대한 근거 자료	C Context	Goal, Strategy에 대한 맥락적 추가 설명
In Context Of	Goal, Strategy와 Context, Justification, Assumption간의 연결에 사용되며 부가적인 내용 전개에 사용	Solved By	Goal, Strategy, Sub-goal, Solution 간의 연결에 사용되며 주요한 논지 전개에 사용

Safety case pattern은 잘 작성된 safety case의 구조를 패턴화 하여 효율적으로 safety case를 작성하는 방법이다. Safety case pattern에서는 safety case의 구조의 추상화를 위해 multiplicity, optionality를 사용하고 있고 요소의 추상화를 지원하기 위해 uninstantiated entity와 undeveloped entity를 사용하고 있다. 각 요소에 대한 표기법 및 설명은 <표 2>에 설명되어 있다. 또한, safety case pattern에서는 GSN 요소에 작성되는 내용에 매개변수 표현을 할 수 있다. 매개변수 표현은 {Class X} 로 작성이 되며 패턴을 safety case로 인스턴스화 할 때 X를 정의하여 safety case에 반영한다.

표 2. 추상화를 위해 확장된 GSN 요소

요소 및 표기법	설명
n Multiplicity	GSN 요소 간의 연결 방법 중 하나로 GSN의 하나의 요소가 여러 개의 다른 요소로 나타내는데 사용
Optionality	목표 시스템에 따라서 서로 다른 sub-goal로 전개될 수 있는 가능성을 표현할 때 사용
Uninstantiated Entity	goal 아래에 표현되어 해당 goal이 인스턴스화 되지 않은 매개변수 표현식을 가지고 있음을 나타낼 때 사용
Undeveloped Entity	goal 아래에 표현되어 해당 goal이 추가적인 전개가 필요할 때 사용

3. NuSCPI

본 논문에서는 원자력 발전소 디지털 계측제어 소프트웨어를 대상으로 하는 safety case pattern 작성을 위해 두 가지 GSN 요소를 추가 하였다. 또한 도구의 자동화를 위한 매개변수 작성 규칙을 제안한다. 추가된 GSN 요소와 매개변수 작성 규칙은 NuSCPI 도구를 통해 구현되었다.

3.1 추가된 GSN 요소

Safety case pattern 작성 시 safety case 구조의 추상화를 지원하는 feedback loop 요소와 safety case pattern을 인스턴스화 할 때, safety case의 논증 구조의 세밀함 정도를 결정할 수 있도록 도와주는 horizontal choice 요소를 추가하여 GSN을 확장하였다. <표 3>은 추가된 2개의 요소의 표기법 및 설명을 보여준다.

표 3. 추가된 GSN 요소

요소 및 표기법	설명
Feedback Loop	goal과 strategy가 반복되는 구조를 표현할 때 사용
Horizontal Choice	동일한 GSN 요소의 수평적으로 연결이 되며 두 개의 요소 중 하나의 요소를 선택할 때 사용

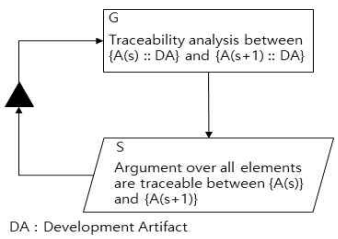

그림 2. Feedback Loop

<그림 2>는 feedback loop의 실제 사용 예를 보여준다. feedback loop은 safety case 논증 구조에서 시스템 속성에 대한 요구조건/목표를 의미하는 goal과 goal의 sub-goal을 연결하는 논리를 의미하는 strategy가 계층적으로 반복되는 구조를 추상화하기 위한 요소이다. 예를 들어, 소프트웨어 개발 산출물 중 SRS, SDS 및 코드까지 연결되는 계층적 구조가 동일한 목표와 동일한 논리로 펼쳐질 경우 사용이 된다. feedback loop의 제약사항으로는 feedback loop과 연결되어 있는 요소에 다중 매개변수 표현식이 작성되어 있어야 한다.

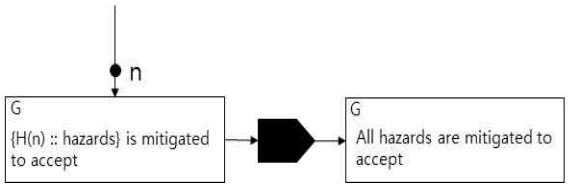

그림 3. Horizontal Choice

<그림 3>은 horizontal choice의 실제 사용 예를 보여준다. horizontal choice는 safety case 논증 구조에서 논증 구조를 펼쳐야 할 사항에 대해서 각 사항들에 대해서 각각 논증 구조를 펼칠지 아니면 전체 사항을 묶어서 하나의 논증 구조로 펼칠지 결정하게 하는 요소이다. 예를 들어, 소프트웨어의 위해요인(hazard)을 완화시키는 안전 논증 구조를 펼칠 때 모든 위해요인에 대해서 하나의 논증 구조로 풀어나갈지 아니면 각각의 위해요인에 대해서 논증 구조를 풀어나갈지 결정할 때 사용이 된다.

3.2 매개변수 작성 규칙

Safety case pattern에서는 인스턴스화 할 때 정의해야 할 매개변수를 GSN 요소에 표현한다. 매개변수 표현이 multiplicity, feedback loop의 요소와 같이 사용될 경우 해당하는 매개변수 표현이 다중 매개변수 표현인지 아니면 하나의 매개변수 표현인지 문맥상으로 구분하기 어렵다는 문제가 있다. 따라서 도구의 자동화를 위해 각 경우에 대한 매개변수 작성 규칙을 정의하였다. <표 4>은 매개변수 작성 규칙 및 설명을 보여준다.

표 4. 매개변수 작성 규칙 및 설명

작성 규칙	설명
{X :: Class}	GSN 요소에서 단일 매개변수를 표현하기 위해 사용
{X(n) :: Class}	multiplicity와 연결되어 있는 GSN 요소에서 다중 매개변수를 표현하기 위해 사용
{X(s) :: Class} (X(s), X(s+1))	feedback loop과 연결되어 있는 GSN 요소에서 다중 매개변수를 표현하기 위해 사용
<X> definition	GSN 요소에 작성된 매개변수 표현식에 대한 context, assumption의 내용 작성 시 매개변수에 대한 정의가 반드시 요구되는 부분에 사용
'{X :: Class }'	safety case pattern의 GSN 요소에 작성된 내용 안에 있는 매개변수 표현식을 인스턴스화 하지 않고 safety case 내의 요소에 바로 작성하기 위해 사용

3.3 NuSCPI 구현

NuSCPI는 Eclipse 용 plug-in 으로 개발된 도구로서 safety case pattern 및 safety case 작성 시 필요한 GSN 요소의 내용, 속성 편집 및 자원 관리를 위해 Eclipse Modeling Framework (EMF)를 사용하였고 Graphical Modeling Framework (GMF)를 사용하여 그래픽 편집을 할 수 있다. NuSCPI는 기존에 제안되어 있던 확장된 GSN 요소의 본 논문에서 추가한 GSN 요소 및 매개변수 작성 규칙들을 적용하여 safety case pattern을 인스턴스화 할 때, 일부 절차를 자동화 하였다.

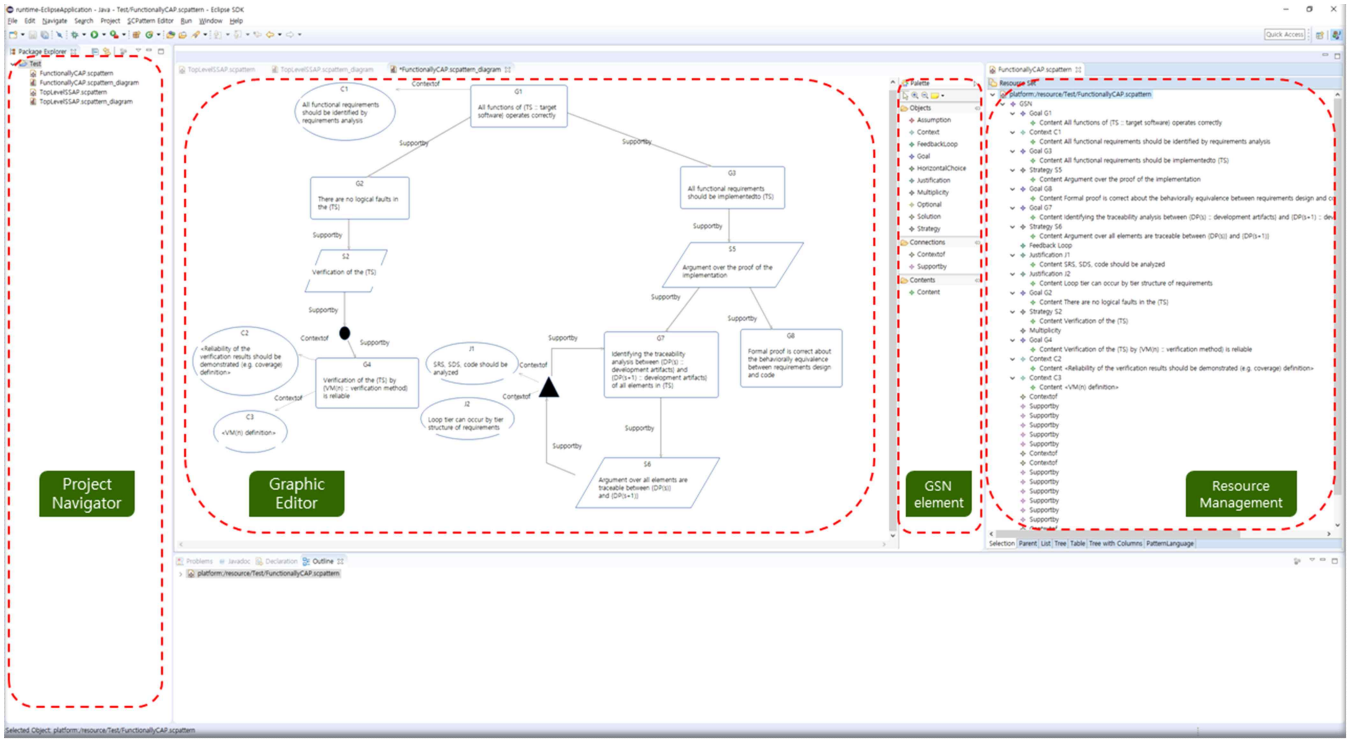

그림 4. NuSCPI 화면 구성

NuSCPI는 safety case pattern을 작성하는 plug-in과 safety case를 작성하는 plug-in 2개로 구성이 되어 있다. 각 플러그인은 EMF의 ecore model을 사용하여 GSN 요소를 정의하였다. <그림 4>는 NuSCPI 중 safety case pattern plug-in의 화면 구성을 나타내고 있다. 각 프로젝트의 파일을 관리할 수 있는 Project Navigator가 있고 중앙에는 확장된 GSN 요소를 이용해 safety case pattern을 작성할 수 있는 Graphic Editor가 있으며 기존의 GSN 요소와 확장된 요소를 모아둔 GSN element List가 있다. 우측의 Resource Management는 safety case pattern 구조 안에 있는 요소들의 이름, 내용 및 속성을 수정할 수 있고 safety case pattern의 pattern language도 작성할 수 있다. 우리는 NuSCPI 도구의 유용함을 확인하기 위해 기존에 제안되었던 safety case pattern[8]을 작성을 해 보았고 safety case로의 인스턴스화를 수행해 보았다.

4. 결론 및 향후 연구

본 논문에서는 원자력발전소의 디지털 계측제어 소프트웨어를 대상으로 개발된 safety case pattern 작성을 위해 feedback loop, horizontal choice 요소를 추가하여 GSN을 확장하였고 GSN 요소 안에 작성되는 매개변수에 관한 작성규칙을 제안하였다. 확장된 GSN 요소와 매개변수 작성규칙은 NuSCPI 도구로 구현이 되었다. NuSCPI는 safety case와 safety case pattern의 기본적인 작성을 지원하며 기 작성된 safety case pattern을 이용하여 safety case로 인스턴스화를 지원하도록 개발되었다. 향후 연구로서 safety case 작성 시 다른 표기법으로 작성된 safety case와의 통합, safety case의 해당 요소와 관련 있는 산출물간의 링크와 같은 연구를 진행할 계획이다.

사 사

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업(NRF-2017M3C4A7066479)과 2017년 정부(미래창조과학부)의 출연금으로 지원을 받아 수행된 주요 연구사업의 연구결과입니다.

참고 문헌

[1] Bishop, Peter and Robin Bloomfield. "A methodology for safety case development." Safety and Reliability. Vol. 20. No. 1. Taylor &Francis, 2000.

[2] Kelly, Tim and John A. McDermid. "Safety case construction and reuse using patterns." Safe Comp 97. Springer, London, 1997. 55-69.

[3] Matsuno, Yutaka. "A design and implementation of an assurance case language." Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on. IEEE, 2014.

[4] Denney, Ewen and Pai, Ganesh. "A formal basis for safety case patterns." International Conference on Computer Safety, Reliability, and Security. Springer, Berlin, Heidelberg, 2013.

[5] 이동아, 유준범, 이장수. “원자력 계측제어 소프트웨어의 안전성 분석을 위한 Safety Case 의 Arguments 개발 절차”, 2016 한국소프트웨어공학학술대회 (KCSE2016), p476-477, 2016.

[6] Kelly, Tim and Weaver, Rob. “Goal Structuring Notation - A Safety Argument Notation,” in DSN-2004: Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, 2004.

[7] Bloomfield, Robin and Bishop, Peter. Safety and assurance cases: Past, present and possible future - an Adelard perspective. In Proceedings of the Eighteenth Safety-Critical Systems Symposium, Bristol, UK, 2010.

[8] Kelly, Tim. “Arguing safety: a systematic approach to managing safety cases.” Diss. University of York, 1999.