원자력 계측제어 소프트웨어의 안전성 분석을 위한 Safety Case 의 Arguments 개발 절차

이동아, 유준범

건국대학교 컴퓨터정보통신공학과
서울시 광진구 능동로 120
{ldalove, jbyoo}@konkuk.ac.kr

이장수

한국원자력연구원
대전광역시 유성구 대덕대로 989 번길 111
jslee@kaeri.re.kr

요약: 원자력 계측제어 소프트웨어는 안전 필수 시스템에서 핵심적인 부분이기 때문에 안전성에 대한 분석이 반드시 요구된다. Safety Case 는 안전성 분석 기법으로서 다양한 안전 필수 분야에서 사용되지만, 분석가에 따라 분석의 수준이 결정된다. 특히 소프트웨어의 안전성은 하드웨어와 달리 마모나 확률적 계산에 근거하지 않기 때문에 기존과는 다른 소프트웨어의 안전성을 위한 분석 체계가 요구된다. 본 논문에서는 Safety Case 를 활용한 원자력 계측제어 소프트웨어의 안전성 분석을 위한 Safety Case 의 전략(Strategy) 수립 과정 및 결과를 소개한다.

핵심어: 안전성 분석, 원자력 계측제어 소프트웨어, Safety Case

1. 서론

안전 필수 시스템(Safety Critical System)이란 시스템의 사고로 인해 인명피해나 환경오염과 같이 돌이킬 수 없는 결과를 초래할 수 있는 중대한 시스템을 의미한다. 이런 특징 때문에 시스템이 가진 안전성 또는 위험성 대한 분석을 통해 시스템의 안전성을 높이는 활동이 반드시 필요하다.

본 논문에서는 대표적인 안전 필수 시스템인 원자력 발전소의 계측제어(I&C: Instrumentation & Control) 시스템의 소프트웨어에 대한 안전성 분석(safety analysis)을 수행하는 절차에 대하여 소개한다. 다양한 안전 필수 분야에서 시스템의 안전성 분석 기법으로 주목 받고 있는 Safety Case[1] 기법을 활용하여 원자력 계측제어 시스템의 소프트웨어 안전성 분석을 수행하는 절차에 대하여 소개한다. 이를 위해 원자로 보호 시스템(RPS: Reactor Protection System)의 BP (Bistable Processor) 소프트웨어를 대상으로 안전성 분석을 수행한 결과를 보인다.

Safety Case 는 안전성 분석 기법의 한 종류로서, 시스템이 용인되는 수준의 안전성(acceptably safe)을 갖췄는지 보이기 위한 논증을 명시적이고 구조적으로 표현하는 기법이다. GSN (Goal Structuring Notation) [2]은 이러한 논리적 구조를 표현하는 대표적인 방법이다. <그림 1>은 GSN 의 표기법을 나타낸다. 본 논문에서는 소프트웨어의 안전성 분석을 위해 Safety Case 작성 시 고려해야 할 전략(Strategy)을 도출하는 과정 및 결과에 대해 소개한다.

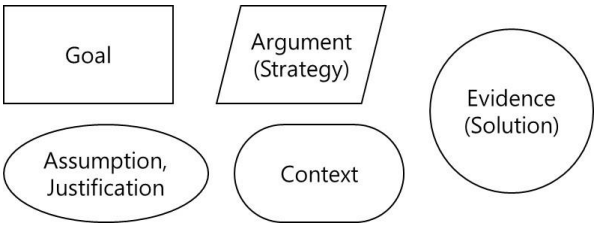

그림 1 GSN 표기법

2. Safety Case 와 GSN 을 이용한 RPS SW 안전성 분석

Safety Case 를 이용한 안전성 분석은 대상의 안전성에 대한 최상위 목표를 설정하는 것으로부터 시작된다. 일반적으로 Safety Case 의 안전성 분석은 '허용 가능한 안전성(acceptably safe)'에 대하여 다룬다. 따라서 Safety case 를 이용한 안전성 분석의 최상위 목표는 '○○○ system is acceptably safe' 형태를 따른다. 이 때, 해당 Goal 에 대한 배경지식과 제약사항이 필요한 경우 Context 와 Assumption 을 명시한다. BP 를 대상으로 최상위 Goal 을 설정한 결과는 다음과 같다.

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 finished by hardware engineers.* A4: *"Safe" means that BP is functionally and non-functionally correct.*

다음으로 설정된 최상위 Goal 을 해결하기 위한 전략을 수립한다. 소프트웨어는 논리적 연산 집합이기 때문에 안전성 분석 수행은 하드웨어와 달리 마

모나 확률적 분석을 대상으로 할 수 없다. BP 안전성 분석의 최상위 Goal 인 G1 의 제약사항 A4 에서 밝혔듯이 소프트웨어의 기능적/비기능적 정확성에 의해 안전성을 분석을 수행한다. BP 의 안전성 분석을 위해서 다음과 같은 4 가지 전략을 제시하였다.

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*

BP 의 기능적/비기능적 정확성을 보이기 위해 두 가지 전략을 각각 제시하였다. 기능적 정확성을 보이기 위해서는 V&V (Verification & Validation) 활동 및 소프트웨어 내/외부의 위험요소를 제거하는 전략을 수립하였다. 반면, 비기능적 정확성을 보이기 위해서는 소프트웨어의 신뢰성(Reliability)과 개발 절차에 대한 타당성을 보이는 전략을 수립하였다—본 논문에서는 지면의 한계로 인해 S1 에 대해서만 자세히 언급한다.

S1 은 BP 의 기능적 정확성 확인을 통해 안전성을 확보하기 위한 전략이다. BP 의 기능적 정확성을 달성하기 위해서는 BP 내부에 논리적 결함(fault)이 존재하지 않아야 한다. 이를 위해 새로운 하위 목표를 설정하였고, 새로운 하위 목표를 달성하기 위한 전략을 수립하였다.

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

G2 달성을 위해 정형 기법을 통한 요구사항 검증을 수행하는 전략을 취하고, 해당 전략 달성을 위해 BP 의 기능별 모델체킹 수행(G3– 생략)을 새로운 하위 목표로 설정한다. 최종적으로 G3 달성을 위한 해결책을 아래와 같이 제시하였다.

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

위에 소개한 절차를 통해 도출된 Safety Case 는 많은 양의 자료를 텍스트 형태로 만들어 낸다. Goal 과 Strategy, Evidence 라는 구조를 가지고 있으나 그 구조를 한 눈에 파악하기 쉽지 않다. GSN 은 Safety Case 의 구조를 쉽게 파악하기 위해, 그 구조를 도식화할 수 있도록 제안된 표현 기법이다. 본 장에서 도출한 BP 의 안전성 분석을 위한 최상위 Goal 은 그림 3 과 같이 표현할 수 있다(GSN 작성 도구: Adelard 社의 ASCE (The Assurance and Safety Case Environment)[3]).

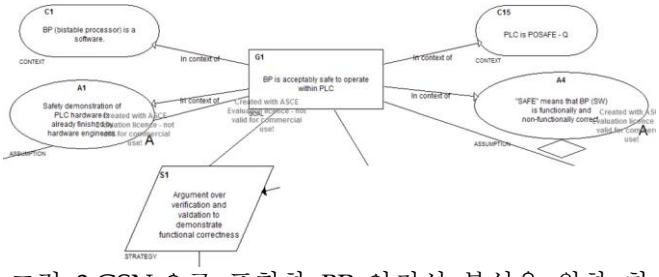

그림 3 GSN 으로 표현한 BP 안전성 분석을 위한 최상위 Goal

최상위 Goal 인 G1 을 중심으로 G1 을 설명하기 위한 배경지식(C1, C15)과 제약사항(A1, A4)이 연결된 것을 볼 수 있다. G1 해결을 위한 Strategy 중 하나인 S1 이 그 아래쪽에 연결 되어 있으며, S1 을 해결하기 위한 Sub-goal 및 Evidence 는 그림 4 와 같다. 이처럼 GSN 을 사용하면 Safety Case 구조를 보다 효과적으로 나타낼 수 있으며, 쉽게 파악할 수 있다.

3. 결 론

본 논문에서는 원자력 계측제어 소프트웨어의 안전성 분석을 위해 Safety Case 작성을 수행하는 절차에 대하여 소개하였다. Safety Case 및 GSN 을 활용한 안전성 분석은 분석가의 역량에 따라 큰 차이를 보인다. 이러한 차이를 좁히기 위하여 소프트웨어의 안전성 분석을 위해 사용되어야 할 네 가지 전략을 도출하는 과정 및 결과에 대해 소개하였고, 하드웨어 기반 시스템의 안전성 분석과의 차이를 보여주었다.

Safety Case 를 작성에서 가장 어렵고 중요한 부분이 바로 Goal 해결을 위한 타당한 Strategy 를 도출하는 부분이다. 본 연구팀은 원자력 계측제어 소프트웨어에 대한 안전성 분석 시 타당하고 효과적인 Strategy 를 사용할 수 있도록 패턴을 개발하는 연구를 향후에 수행할 예정이다.

사 사

본 연구는 한국원자력연구원의 "원자력 계측제어 계통 안전 적합성 평가체계" 사업의 지원으로 연구한 결과 입니다.

참고문헌

[1] “The purpose, scope, and content of safety cases”, Office for Nuclear Regulation, An agency of HSE
[2] http://www.goalstructuringnotation.info/
[3] http://www.adelard.com/asce/