Journal of KOSSE. (2023. 6) Vol. 19, No. 1 pp. 29-38
DOI: https://doi.org/10.14248/JKOSSE.2023.19.1.29
www.kosse.or.kr

ISSN (print) : 1738-480X
ISSN (online) : 2288-3592

NOR-STA 도구를 활용한 체계적 철도시스템 독립안전성 평가 방안

엄정규[1)*], 박범[1)], 김영민[1)]
1) 아주대학교 시스템공학과

A Systematic Method for Independent Safety Assessment of Railway System by Applying NOR-STA Tool

Jung Kyou Um[1)*], Peom Park[1)], Young Min Kim[1)]
1) Department of Systems Engineering, Ajou University

Abstract : Independent Safety Assessment (ISA) is a third-party assessment that is to confirm that the system satisfies the safety requirements in the defined operational context. The process of this assessment often brings about many complex arguments that should be supported by evidence and justification. The communication between arguments and evidence is of the most importance in the context of safety case. This study illustrates how NOR-STA can be used for ISA process, showing the effective structure of safety compliance. The study outlines the steps to breaks down the top goal into many elements such as arguments, sub-goals, justification, context and assumptions. It concludes that the evidence-based safety conformance process utilizing NOR-STA provides a more effective and systematic representation of the independent safety assessment process in conformance cases.

Key Words : Goal Structure Notation, Safety Case, Independent Safety Assessment, NOR-STA, SIL

Received: February 18, 2023 / **Revised**: April 28, 2023 / **Accepted**: June 6, 2023
* 교신저자 : Jung Kyou Um / Systems Engineering, Ajou University / jungkyou.um@lampcompany.co.kr

1. 서 론

철도분야의 독립안전성평가 (Independent Safety Assessment, ISA)는 제품, 시스템 또는 전체 철도가 안전과 관련한 산업적, 법률적 및 규제적 기준들을 만족하는지를 제 3자가 수행하는 행위이다. 독립안전성평가의 절차 및 내용은 IEC 62278 표준서에서 정의되어 있으며[1], 철도시스템에 대한 추가적인 신뢰수준을 제공함을 목적으로 하고 있다. 일반적으로 ISA는 자격인정(Accreditation)을 받은 기관에 의해 수행되고 있으며, 자격인정은 유럽 내 공공기관이 Commission Implementing Regulation (EU) No 402/2013를 준수하는지를 판단하여, ISA의 절차 및 내용에 따라 수행할 자격이 있음을 인정하고 있다.

독립안전성평가의 주요 활동 및 업무 내용은 다음과 같다.

- 제품/시스템 및 개발과정에 대한 이해
- RAMS 검증 계획의 적합성 평가
- 철도 RAMS 입증 및 요구사항을 정의한 IEC 62278에 대한 적합성 평가
- 독립적 평가에 의한 요구사항의 적합성과 편차에 대한 식별 및 평가
- 평가 결론 및 안전성 관련 적용조건의 제한사항 분석
- 해당 제품 또는 시스템의 품질 및 안전성 절차의 수명주기 단계별 요건에 대한 적합성 여부 감사

즉, 제품 또는 시스템 제작자(또는 개발자)는 특정 RAMS 내용을 이해하면서 요구사항에 부합하는 업무, 공정 및 산출물을 생성하고, ISA 기관은 안전성 평가 과정 동안 제품 또는 시스템의 안전무결성 수준(Safety Integrity Level, SIL)에 따른 공정 및 결과가 IEC 62278[1], IEC 62279[2], IEC 62425[3]의 요구사항에 부합하는지는 평가하여 안전무결성수준에 대한 확신을 독립적으로 제공하여야 한다.

결국 개발자의 수행결과에 대한 ISA의 평가가 단계별로 진행되면서 개발자와 독립안전성평가자 간에 의견교환이 이루어지며 종종 적합성에 대한 논쟁이 발생하기도 한다. 피평가자와 평가자 간에 의견충돌이 발생하기 마련이고, 어떤 사항에 대한 객관성 정도에 대한 이해충돌을 해결하는 것이 ISA 과정의 중요한 요소이다. 경우에 따라서는 논증의 기반이 되는 요소들이 서로 복잡한 관계성을 포함하는 경우가 있다.

ISA 과정에서 피평가자 및 평가자 간의 이해충돌은 주로 정성적 논증 시 충분한 논리적 근거가 부족한 경우에 발생한다. 즉, 정성적 평가 시, 한 개인의 경험 및 지식에 근거한 주관적 판단을 주장하는 경우인데, 충분한 논리적 근거(Rationale)에 의한 합리적 판단으로 객관성 확보하려는 노력이 이해충돌을 회피할 수 있다.

이러한 문제로 인하여 발생되는 이해충돌을 저감하기 위해서는, 개발자는 결과물에 대한 충분한 논리 및 근거자료를 제시하여야 하는 한편, 평가자는 적합성 여부에 대한 논거를 제시하여 요구사항에 대한 부합여부를 적절하게 판단하여야 한다. 이러한 평가자와 피평가자 간의 의사소통이 기존에는 평가자의 주관적 요소가 포함된 LOP(List of Open Points) 방식에 따라 수행되어왔다.[4]

본 연구에서는 ISA과정에서 발생할 수 있는 이해충돌을 해소하고 복잡한 관계를 갖는 각 논증에 대한 주장들에 기반한 평가과정을 상호 가시적이고 객관적인 방법을 적용하여 적합성에 대한 이해충돌을 가시적이면서 객관적으로 해결할 수 있는 방법을 제시하고자 한다.

따라서, 연구내용은 어떤 목표(즉, 요구사항 부합)를 성취하기 위해 근거에 의한 추론적이고 확실성 있는 논거 방법을 검토하고, 그 방법을 실제 사례에 적용하여 독립안전성평가 과정에 대한 적용성 여부를 연구하였으며, 다음의 주요 내용을 포함한다.

- Assurance Case 논거의 Safety Case 적용성 검토

- GSN(Goal Structure Notation)의 Safety Case 논거에 대한 적용성 검토
- 결론적으로 GSN 의 독립성안전성평가 과정에 대한 활용성 평가

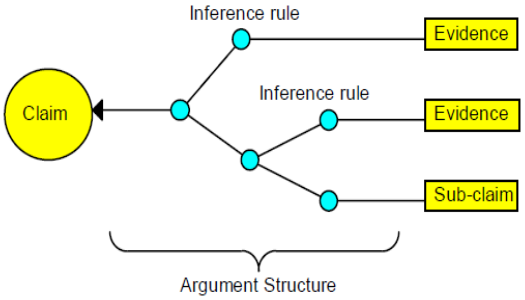
본 연구목표의 달성을 위해 본 논문에서는 Assurance Case 관리 도구를 사용하여 안전성 논증 및 증거를 가시적으로 표현하는데 집중하였다.

2. Assurance Case와 Safety Case

Assurance Case는 "시스템, 행위 또는 조직이 규정된 환경에서, 정의된 적용에서 목적하는 바대로 운영됨을 보증하는, 근거에 의한 추론적이고 확실성 있는 논거로 정의된다.[5] 대개의 경우 안전성(Safety), 보안(Security), 신인성(Dependability), 신뢰(Trust) 등과 연결하여 적용된다.

철도분야 뿐만 아니라, 많은 경우에 표준서들은 시스템 특성(Attribute)의 허용 수준이 요건에 부합된다는 보증(Assurance)을 요구하고 있다. 철도시스템에 대한 RAMS 표준서인 IEC 622778에서는 안전성에 대한 보증인"Safety Case"를 요구하고 있다. 피평가자는 개발하는 제품의 근거와 논거를 기반으로 Safety Case를 통하여 제품의 안전성을 주장하고, 평가자는 해당 근거와 논거가 적합한지 평가하게 된다.

일반적으로, Assurance Case는 다음과 같은 구성요소를 갖는다. 즉, Assurance Case는 시스템의 목표를 주장하는 "Claim", Claim의 증거가 되는 "Evidence", 그리고 "Claim"과 "Evidence"를 연결하는 "Argument"등으로 구성된다. 이때, "Evidence" 대신 "Sub-claim"으로 구성될 수 있다. 또한, "Argument"를 명확하게 하는 "Assumption"과 "Judgement"가 추가될 수 있으며, 그림 1과 같은 추론규칙을 형성하는 구조로 표현된다.[6] 추론규칙(Inference Rule)은 복수의 Argument를 허용한다.



[Figure 1] Elements of Assurance Case

이러한 논리적 관계는 GSN(Goal Structure Notation)라는 그래픽 기호를 사용하여 논거에 대하여 구조적으로 표현할 수 있다. 즉, GSN은 일반 텍스트 형태보다 더 명확한 형식으로 안전성 목표가 성취됨을 증명하거나 문서화하는데 그래픽 형태로 표현할 수 있는 도구이다. GSN을 활용하여 목표(Goal)를 성취하기 위한 전략(Strategy)과 증거(Evidence) 간의 관계를 구조적으로 표현하여 명시적으로 논증의 구조를 문서화할 수 있다. GSN은 최초 University of York에서 개발되었으며, 교통량 관리 또는 원자력발전분야에서 안전성 보증을 추적하는 데 활용되어 왔으며, 2014년까지 Safety Case의 표준적 그래픽 문서로 인정되어 왔으며, 다양한 분야에서 활용되었다.[7] 그림 2는 GSN이 구성된 일반적 구조를 예시하고 있으며, Goal, Strategy, Assumption, Justification, Solution, Context 간의 관계를 설명하고 있다.

GSN의 목적은 목표가 어떤 방식으로 성공적으로 분해되어, 최종적으로 가용한 증거(즉, Solution)에 의해 해결되는지를 구조적으로 표현하기 위함이다. 즉, GSN은 논증의 과정을 가시적으로 표현하기 때문에 규제기관의 평가자로 하여금 논증의 근거를 파악하는데 도움이 될 수 있다. 증거로 시작하여 상향적으로 논증이 확인될 수 있으며, 결국에는 최상위 목표가 성취됨을 가시적으로 확인할 수 있다.

Safety Case는, "특정 시스템(선박 또는 설비 등)이 다음과 같은 자료에 의해서 안전성이 입증됨을 보장할 목적으로 구성된 포괄적이고 구조적인 안전성 문서의 집합"으로 정의되며 다음 사항들을 포

[Figure 2] Generic Structure of GSN

함하고 있다.[8]

- 안전성 계획 및 조직
- 안전성 분석
- 표준서 및 모범 사례에 대한 부합성
- 승인 시험
- 감사
- 검사
- 의견에 대한 조치
- 비상상황을 포함한 안전한 운영을 위한 규정

또한 IEC 62425에서는 철도 분야에서 Safety Case를 구성하는 문서의 구조를 기술하고 있으며, Safety Case의 목적은 문서적인 증거를 통하여 최종 안전에 대한 보증을 제공하여 안전에 대한 승인을 받기 위함이다.[3]

Safety Case의 주요 3요소는 요구사항(Requirements), 논거(Argument) 및 증거(Evidence)이다. 이때, 논거는 안전성에 본질적이고 명확하여야 한다. 즉, 철도시스템이 특정 환경에서 운영될 경우, 허용할 수 있는 안전성 수준을 만족한다는 명확하고 보편적이고 필수 불가결한 논거가 Safety Case에 기술되어야 한다. 허용할 수 있는 안전성 수준이면서 확신할 수 있는 사례(Case)는 고수준의 논거(Argument)와 이를 뒷받침하는 증거(Evidence)를 필요로 한다. 증거없는 논거는 신뢰할 수 없으며, 논거없는 증거는 설명될 수 없기 때문이다.

GSN 기법을 적용하여 Assurance Case 관리 도구로 개발된 것 중의 하나가 NOR-STA라는 도구이며, 본 논문에서는 Safety Case 목표를 보다 체계적이고 객관적으로 입증할 수 있는 NOR-STA 도구를 소개하고, 이를 이용한 독립평가 방안을 제안한다. 독립안전성평가를 위해 NOR-STA를 제안하는 이유는 다음과 같다.

첫째, NOR-STA는 명확하고 확신할 수 있는 기술적 논거(Argument) 전개 환경을 제공한다. 정량적 논거뿐만 아니라 정성적 논거에 대하여 기술적 환경 및 방법을 제공하기 때문이다. 둘째, 문서 형식만의 Safety Case는 논리적 추론에 대한 추적성 확인을 위해서는 여러 관련된 문서 또는 논거를 조합하여 판단해야 하는데, 가시적으로 논거관계 설정할 수 있기 때문이다.

3. NOR-STA 기반의 독립안전성평가

NOR-STA는 내부적으로는 TRUST-IT 이라는 Assurance Case 메타모델을 사용하고, GSN을 적용한 Assurance Case 관리 도구이다.

NOR-STA는 ARGEVIDE (www.argevide.com)에서 서비스를 제공하고 있으며, 해당 기업은 2014년에 설립된 이후에 자동차, 항공, 교통, 석유 및 가스, 사이버 보안 분야의 고객에게 서비스를 제공하고 있다.

TRUST-IT은 명확하고 가시적 논쟁(Argument)이 될 수 있도록 증거 및 수단을 통합적으로 제공하여 가상공간에서 “Live”한 논쟁을 가능하게 하여 신뢰를 증진시키는 진보적 접근방안이다. 여기서 논쟁(또는 논거, Argument)은 상대에게

특정사안을 설득하고 이해시키는 상호 의견교환의 한 방법으로서, 특정 결론에 대한 논리 및 근거가 동시에 제공된다.

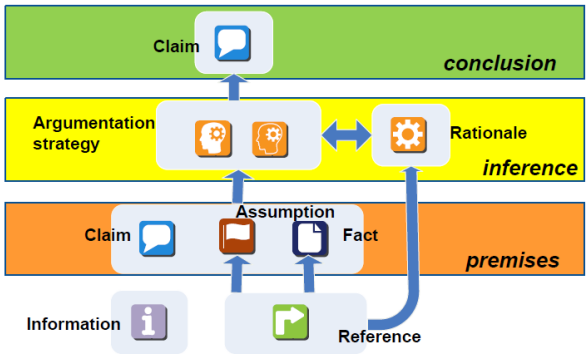
NOR-STA는 웹환경에서 제공되는 다음의 기능을 사용하여 Assurance Case를 개발할 수 있다. 이때, NOR-STA 시스템은 표 1과 같이 GSN의 기호와 대응되는 기호를 정의하고 있다.

- 논거를 전개하고 타인과 공유
- 증거와 함께 보증사례 통합
- GSN 다이어그램 생성
- 분석을 수행하고 결과 교환
- 논거 모듈 관리 및 템플릿 사용
- 타 도구와 보증절차 통합

<Table 1> Symbols of GSN and NOR-STA

GSN 표현		NOR-STA 표현	
	Goal (또는 Sub-goal)	Claim (또는 Sub-claim)	
	Strategy	Argument	
	Context	Claim에 대한 설명	
	Solution	Evidence	
	Justification	Argument에 대한 설명	

NOR-STA 상에서 Claim과 연관된 타 요소와의 관계는 그림 3과 같다. 일반적인 GSN 구조에서는 Goal (or Claim)하위에 Sub-goal로 다음 단계에 바로 분해할 수 있는 반면에, NOR-STA에서는 Goal (Claim) 하위에 Sub-goal을 직접 연결하지 못하고, Argument (or Strategy)를 통하여 연결할 수 있다.



[Figure 3] Relations of Elements in NOR-STA

표 2는 Claim, Argument 및 Evidence로 설정할 수 있는 사례이다.

<Table 2> Examples of Claim, Argument and Evidence

구분	사례
Claim 형식	• 신뢰성, 가용성, 보전성 • 외부 공격에 의한 보안 • 고장-안전 • 기능적 적합성 • 정확성 • 반응시간 • 과부하에 대한 강건성 • 변경 용이성
Argument 형식	• 결정론적 논거 • 확률적 논거 • 정성적 논거
Evidence 형식	• 설계 • 개발프로세스 • 신뢰성시험 등 가상의 경험 • 사전 현장 경험

4. NOR-STA의 독립안전성평가 적용

NOR-STA를 활용하기 위한 예시는 다음과 같은 목표를 가정하여 논거 및 증거와의 관계를 구성하여 보자.

목표 G1:

"제어시스템 A는 IEC 62278 기준으로 안전무결성수준(Safety Integrity Level, SIL) 4를 만족함"

본 목표를 성취하기 위해서는 다음과 같은 절차와 각 절차에서 생성되는 하위 목표(Sub-Goal) 및 그것을 뒷받침하는 논거와 증거, 정당화 등의 요소를 식별하여 관계를 형성하는 작업이 필요하다.

1) 단계 1

제어시스템 A는 하위 설비 A1과 A2로 구성되어 있다고 가정하면, 시스템 A의 SIL 수준을 만족하는 A1, A2 설비의 SIL 수준을 정의하여야 한다. 이를 위하여 SIL 할당과정이 필요하며, 목표에 대한 논거(S1) 및 S1에 대한 Context C1은 다음과 같이 생성된다.

▶ 목표 G1-제어시스템 A는 IEC 62278 기준으로 SIL 4를 만족함

- 논거 S1-시스템 A가 SIL 4를 만족하기 위해 서브시스템(A1, A2)에 대한 SIL 할당에 대한 논거
- Context C1-SIL 할당방법

2) 단계 2

단계 1에서 SIL 할당과정을 통하여 설비 A1 및 A2의 SIL 수준이 각각 4와 2로 정의되었다고 가정하며, 단계 1의 논거에 의하여, 하위 설비 A1 및 A2에 대한 하위 목표와 그것을 뒷받침하는 논거 및 Context는 다음과 같이 생성된다.

▶ 목표 G2.1-설비 A1은 IEC 62278 기준으로 SIL 4를 만족함

- 논거 S2.1-설비 A1의 모든 위험원은 제거 또는 허용수준 이하로 저감됨의 논거
- 타당성 A2.1-SIL 허용수준 목표
- 논거 S2.2-설비 A1의 소프트웨어는 SIL 4에 맞게 개발됨의 논거
- 증거 E2.2: SIL 4에 준하는 개발절차
- Context C2.2-IEC 62278에 정의된 절차를 안전관리계획서에 기술함

▶ 목표 G2.2-설비 A2는 IEC 62278 기준으로 SIL 2를 만족함

- 논거 S2.3-설비 A2의 모든 위험원은 제거 또는 허용수준 이하로 저감됨의 논거
- 타당성 A2.1-SIL 허용수준 목표
- 논거 S2.4-설비 A2의 소프트웨어는 SIL 2 에 맞게 개발됨의 논거
- 증거 E2.4: SIL 2 에 준하는 개발절차
- Context C2.2-IEC 62278에 정의된 절차를 안전관리계획서에 기술함

위에서 논거 S2.1 및 S2.3은 새로운 하위 목표를 생성하고, 논거 S2.2 및 S2.4는 하위 목표를 생성하지 않고 증거로 종결된다고 가정하였다.

3) 단계 3

단계 2에서 논거 S2.1은 설비가 SIL 4 수준이기 때문에 하위 목표 G3.1과 G3.2를 필요로 하여 2개의 하위 목표가 생성된 반면에, 논거 S2.3은 설비가 SIL 2 수준이기 때문에 1개의 목표만 필요로 하는 것으로 가정하였다. 따라서, 단계 2의 논거에 의하여, 하위 목표와 그것을 뒷받침하는 논거 및 Context는 다음과 같이 생성된다.

▶ 목표 G3.1-A1계통 위험원 H1은 제거됨

- 논거 S3.1-설비 A1의 위험원 H1 위험원의 사고 시나리오 타당성 논거
- 증거 E3.1-Formal 검증

▶ 목표 G3.2-설비 A1 기타 위험원은 허용수준 이하

- 논거 S3.2-설비 A1의 기타 위험원의 위험결과의 타당성 논거
- 증거 E3.2: 설비 A1의 위험원에 대한 사건수목 분석
- 논거 S3.3-설비 A1의 기타 위험원의 위험발생률에 대한 논거
- 증거 E3.3: 설비 A1의 위험원에 대한 고장수목 분석

▶ **목표 G3.3-설비 A2 기타 위험원은 허용수준 이하**

- 논거 S3.4-설비 A2의 위험원의 위험결과의 타당성 논거
- 증거 E3.4: 설비 A2의 위험원에 대한 사건수목 분석
- 논거 S3.5-설비 A2의 위험원의 위험발생률에 대한 논거
- 증거 E3.5: 설비 A2의 위험원에 대한 고장수목 분석

이상과 같이 목표 G1: "제어시스템 A는 IEC 62278 기준으로 안전무결성수준(Safety Integrity Level, SIL) 4를 만족함"에 대한 논거를 전개하고, 논거에 대하여 필요한 경우 하위 목표를 생성하고 다시 하위 목표에 대한 논거를 생성하는 방법을 설명하였다.

표 3은 NOR-STR 시스템이 지원하는 다양한 평가방법이다. 본 연구 사례에서는 Three-value compliance assessment의 평가방법을 적용하였다. Three-value compliance assessment는 compliance 평가를 위해 전용으로 사용되는 평가방법이며, 평가에 대해서는 non-compliant, unknown, 그리고 compliant의 세 가지 값으로 구성된다.[9]

그림 4는 상기의 내용을 NOR-STA에 입력한 화면이고, 그림 5는 입력 내용을 GSN 형태로 표현한 것이다.

<Table 3> NOR-STA Assessment methods

No	평가방법	설명
1	Dempster-Shafe	Dempster-Shafer의 증거 이론에 근거하여 Gdansk 공과대학 에서 개발한 논거 평가방법
2	Three-level assessment	적합성 사례에 사용된 적합성 값 3개의 간단한 척도
3	Rating scale	각 평가 요소에 대해 개별 평가 척도를 사용한다. 정당성을 무시한 부분성적을 합산해 평가 결과를 산출한다.
4	Three-value compliance assessment	Compliance 평가를 위해 사용되며, 평가에 대한 세 가지 값으로 구성된다. 계산된 결론 평가는 모든 전제가 적합하다고 평가될 때 "준수"된다.

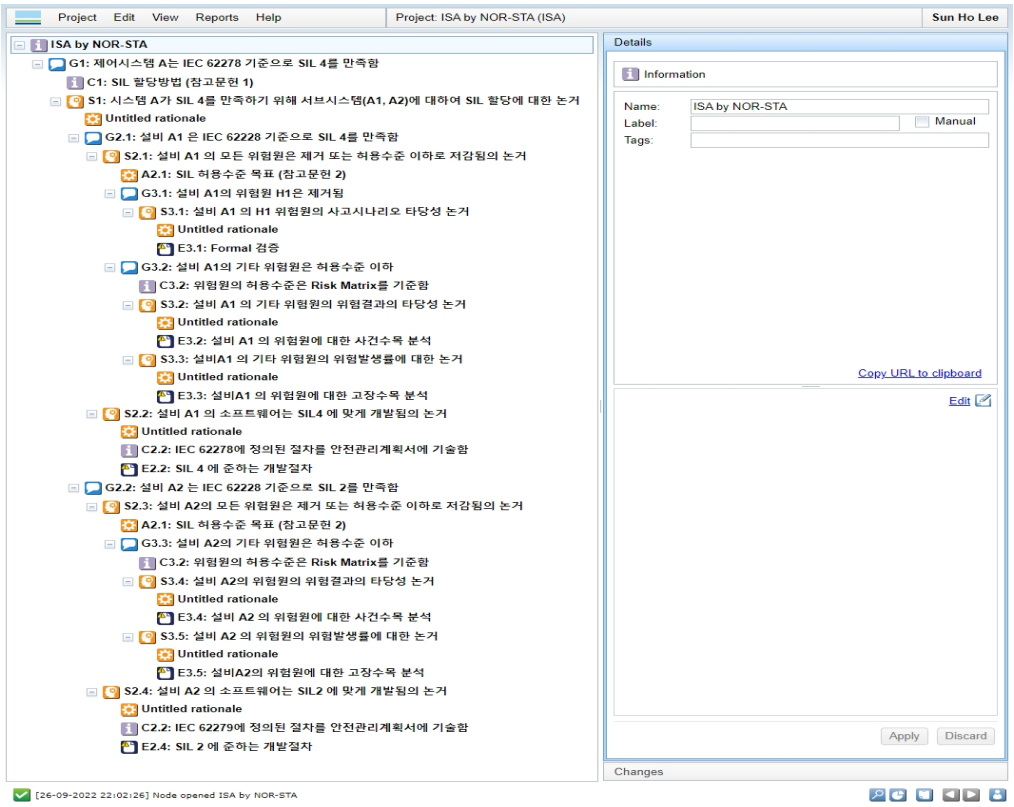
상기의 예제는"제어시스템 A는 IEC 62278 기준으로 안전무결성수준(Safety Integrity Level, SIL) 4를 만족"하기 위하여 개발자(피평가자)가 제출한 문서 및 논거에 대하여 독립안전성평가자가 목표를 검증하기 위한 활동으로 목표에 대한 모든 논거를 표시한 것이다.

또한 각 논거에 대한 타당성 및 Context를 연결하고 필요시 증거를 제공하여 논거를 종결하는 방법을 예시하였다. 다만 주의할 것은 목표 G1에 대하여 하향적으로 전개하는 방식 및 논거의 구성은 분석하는 관점에 따라 상이할 수 있다. 중요한 것은 논거는 최종적으로 증거에 의하여 종결된다는 점이다.

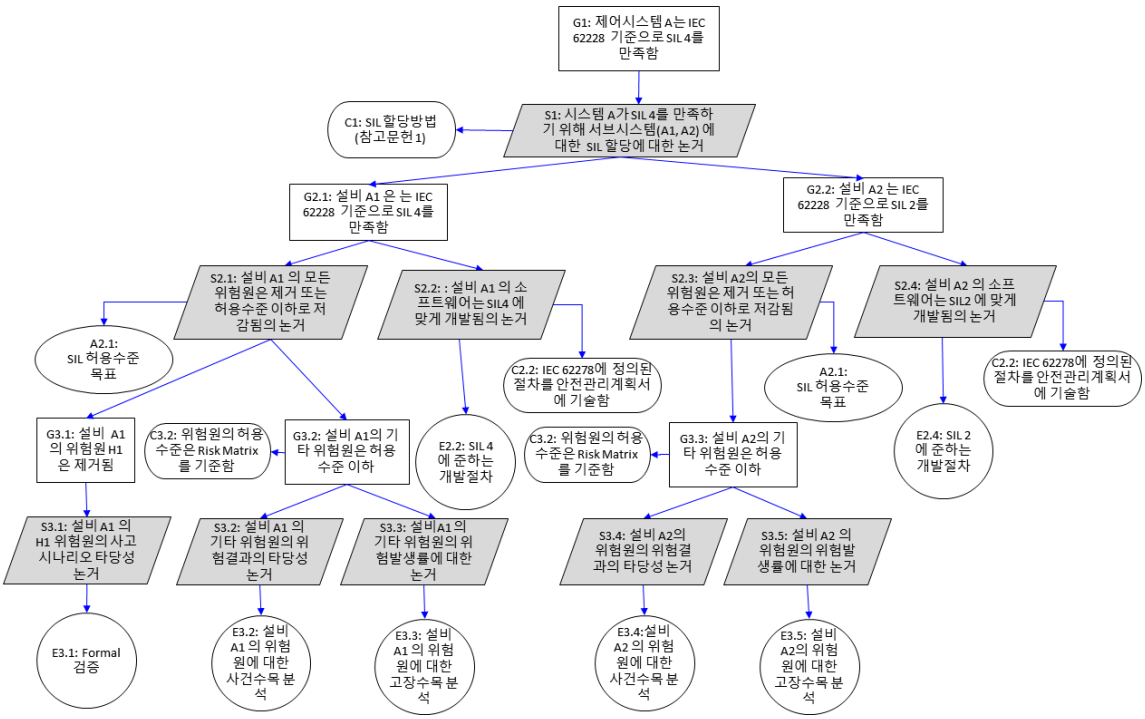
위 사례에서는 몇개 안되는 논거와 증거를 예시하였지만 대개의 경우 한 시스템의 안전성을 평가하기 위해서는 수 십 종의 문서와 복잡한 논거가 제출되며 독립안전성 평가자는 이를 각각 추적하여 논거의 적합성을 평가하게 되는데 GSN 기반의 NOR-STA는 다음과 같은 이점을 제공한다.

첫째, 평가자 입장에서는 피평가자가 제공하는 모든 산출물, 논거 및 증거들을 가시적인 다이어그램을 통하여 표현함으로써 가시적이고 체계적인 논거의 추적이 가능하다.

둘째, 피평가자가 제공한 증거에 기반하여 논거의 적합성을 판단할 경우 논리적 결함을 쉽게 발견할



[Figure 4] Input Screen of NOR-STA



[Figure 5] GSN Diagram Produced in NOR-STA Presenting Argument Elements

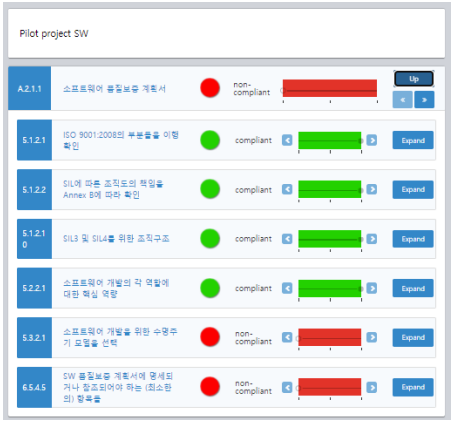
수 있다.

셋째, 피평가자-평가자 간의 이해충돌 시 평가자 판단의 적절성을 피평가자에 효과적으로 제시할 수 있으며, 반대로 피평가자는 논거 및 증거에 대한 부적절성을 쉽게 발견하여 이해충돌의 여지를 저감할 수 있다.

넷째, 독립안전성평가는 피평가자와 평가자 간의 오랜 시간의 논쟁으로 진행되며 동시에 여러 관련자들과 연계하면서 진행되는데, 평가자의 의견에 따라 피평가자는 관련된 산출물과 증거를 수정한다. 이때, 평가도구를 이용하여 고객(평가 신청자)과의 소통은 웹사이트를 통하여 가능하다. 고객이 웹사이트에 접속하면 그림 6과 같이 Basic View가 제공된다. Basic View에서 고객은 발견사항에 대하여 답변을 기술할 수 있다. 또한, 평가가 이루어지는 현황을 웹사이트를 통하여 확인할 수 있다.

고객이 답변 기술 후 제출해야 할 산출물을 메일 등으로 제출할 수도 있지만, 평가도구를 이용하여 산출물을 제출할 수도 있다. 결국 GSN 기반의 NOR-STA는 그 과정에 소요되는 노력과 시간을 절약할 수 있게 하며 해당 당사자들에게 뿐만 아니라, 타 관련자들에게도 효과적인 인터페이스 환경도 제공한다.

한편, 기존의 LOP 방식에서는 사용되지 않는 추가적인 도구를 익히고 사용해야 한다는 단점도 존재한다.



[Figure 6] Basic View of NOR-STA

5. 결론

독립안전성평가(ISA)시 철도 국제표준규격 IEC 62278[1], IEC 62279[2], IEC 62425[3]에 기반하여 요구되는 사항에 대한 적합성 여부를 판단한다. 그리고 철도 안전수명주기에 기준과 연관된

활동의 적합성을 평가한다. 이때 고객 또는 철도용품 제작사는 수명주기 동안 생성하는 산출물 제출하고 평가의견을 교환한다.

본 논문에서는 ARGEVIDE의 NOR-STA 시스템을 독립안전성평가 시에 활용할 수 있는 방안을 제시하였다. 제시된 도구의 가장 큰 장점은 첫째, 명확하고 확신할 수 있는 기술적 논거(Argument) 방안을 제공한다. 정량적 논거뿐만 아니라 정성적 논거에 대하여 기술적 환경 및 방법을 제공하기 때문이다. 둘째, 문서 형식만의 Safety Case는 논리적 추론 또는 명확성이 저감되기 쉬운데, 이를 보완할 수 있는 가시성이 향상된 논리적 입증 방안을 제공한다. 셋째, 독립안전성평가자의 개인적 관점에 의한 평가를 최소화하는 평가 프레임을 제공하고, 평가자의 전문성을 고객이 공유하고 체계적으로 소통하는 효율적인 절차를 제공함으로써 독립안전성평가의 객관성을 향상시킬 수 있다.

본 연구에서는 NOR-STA를 독립안전성평가에 적용하였지만, 향후 피평가자와 평가자가 동시에 본 도구를 사용할 경우에도 의견교환 방법 및 효율성을 평가할 필요가 있다.

References

1. IEC 62278, Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS), IEC, 2002
2. IEC 62279, Railway applications - Communication, signalling and processing systems - Software for railway control and

protection systems, IEC, 2015
3. IEC 62425, Railway applications-Communication, signalling and processing systems-Safety related electronic systems for signalling, IEC, 2007
4. 김유호, 이수환, 박강훈, 고태국, 철도 시스템 기능 안전(Functional Safety) 및 인증, 전기학회 논문지 제63P권 제4호, p226~235, 2014
5. The Assurance Case Working Group (ACWG), GSN Community Standard. Version 2, p10, 2018
6. Peter Bishop, et. al., A Methodology for Safety Case Development. Safety and Reliability, Taylor & Francis, p35, 2000
7. Timothy Patrick Kelly, Arguing Safety-A Systematic Approach to Managing Safety Cases, Ph D. Thesis, University of York, p42, 1998
8. Joint Service Publication 430, Management of Ship Safety and Environmental Protection, Issue 1, 2010
9. NOR-STA User's Manual, https://manual.argevide.com/display/ND/Setting+the+assessment+method