위해도 분석 결과의 효과적인 확인을 위한 추적성 기반 위해도 모델

정세진O, 유준범
건국대학교 컴퓨터정보통신공학과
{jsjj0728, jbyoo}@konkuk.ac.kr

Hazard model for efficiency of hazard analysis based on traceability relations

Sejin JungO, Junbeom Yoo
Division of computer science and engineering, Konkuk university

요 약

위해도 분석은 시스템 또는 소프트웨어의 사고가 될 수 있는 잠재적인 위험 상태를 분석하는 것으로 안전성이 중요한 시스템에 필수적으로 적용되고 있다. 현대의 시스템은 과거에 비해 그 복잡도가 급격하게 증가하고 있어 위해도 분석이 쉽지 않다. 따라서 현재 전체 시스템에 하나의 기법을 활용한 분석 보다는 개발 생명주기, 구조에 따라 시스템/서브시스템/컴포넌트 수준에서 여러 기법들이 사용되는 것이 일반적이다. 이 때 각각 적용한 위해도 분석은 원인-결과의 연결이나 상호 작용에 의한 관계를 가질 수 있다. 하지만 현재 이런 관계에 대해 추적성 분석 수준의 연구만 진행되고 있어 전체적인 확인이 어렵다는 문제점이 있다. 본 논문에서는 여러 위해도 분석 결과의 효과적인 확인을 할 수 있는 추적성 기반 위해도 모델을 제안한다. 위해도 모델은 분석 결과의 모델링뿐만 아니라 각 요소들의 관계를 정의해 포함하고 있다.

1. 서 론

안전 필수 시스템 (safety-critical system)은 사고로 인한 결과가 인명피해, 환경오염과 같이 심각한 문제가 되는 중대한 시스템을 의미한다. 따라서 안전 필수 시스템은 사용 전 안전성 분석 등을 통해 그 안전성에 대해 입증해야 한다[1].

위해도 분석 (hazard analysis)은 시스템/소프트웨어의 사고가 될 수 있는 잠재적인 위험 (hazard)을 분석하는 기법으로 안전성을 확보하기 위해 위험을 확인하고 제거하는 목적으로 사용하는 방법이다. 기능 안전성 표준에서는 위해도 분석을 통해 시스템의 hazard, risk를 확인하고 안전 요구사항 (safety requirement)을 할당하는 프로세스를 가지고 있어 위해도 분석은 안전 필수 시스템 개발에 필수적으로 수행되어야 한다. 위해도 분석에는 FMEA (Failure Mode & Effect Analysis), FTA (Fault Tree Analysis)와 같이 전통적으로 많이 사용되던 기법에서 STPA (System Theoretic Process Analysis), ECFA (Event Causal Factor Analysis) 등 수많은 기법들이 개발되어 적용되고 있다[2][3].

현대의 시스템은 과거에 비해 그 기능이 다양해지고 복잡도가 급격하게 증가하는 등 위해도 분석이 어려워지고 있다. 따라서 하나의 기법을 통해 전체를 분석하기 보다는 생명주기, 계층적 구조 등에 따라 다양한 기법들이 적용되는 것이 일반적이다. 시스템 이론 (system theory)에 따르면 이런 시스템은 독립적인 컴포넌트들의 단순한 집합체가 아닌 각각의 컴포넌트들이 유기적으로 상호작용하는 관계이며, 각각 적용한 위해도 분석 결과들도 효과적으로 각각의 관계를 확인 해 볼 필요가 있다. 이 때 각 위해도 분석의 결과들은 다양한 연결 고리들을 가질 수 있으며 추적 관계 분석을 통해 연결성, 관계 등을 효과적으로 확인할 수 있다[6].

하지만 현재는 주로 독립적으로 위해도 분석을 적용해 결과를 도출하거나, 계층적 구조에 대해 원인-결과의 분석 가능성에 대해서만 언급하고 있다[4]. 또는 전체 안전성 분석 측면에서 추적성을 확인하는 정도에서 그치고 있는 등[5] 연계해서 확인하는 방법이 부족하다.

이에 따라 본 논문에서는 다양한 분석 기법을 활용한 시스템/소프트웨어의 위해도 분석 결과의 상관관계 분석을 통한 다각적인 위험, 효과, 과정 (consequence) 확인 및 모델링을 위해 추적성을 기반으로 한 위해도 모델을 제안한다. 위해도 모델은 메타모델을 활용한 분석 결과의 모델링 및 각 요소들의 관계를 정의해 표현하였다. 이를 통해 여러 종류의 위해도 분석 기법을 사용한 분석에 도움이 될 수 있다.

2. 배경지식

2.1. 위해도 분석 (hazard analysis)

위해도 분석은 시스템/소프트웨어가 사고가 될 수 있는 잠재적인 위험 (hazard)을 식별하는 기법으로 현재 다양한 기법들이 사용되고 있다. 현재 주로 사용되는 기법으로는 FMEA, HAZOP (Hazard & Operability)), FTA가 있으며, STPA도 최근 많이 연구되고 있는 기법 중 하나이다.

FMEA는 subsystem, component, function의 잠재적인 고장 모드 (failure mode)가 시스템에 미치는 영향을 상위 수준으로 분석하는 귀납적 분석 방법이다[2]. FMEA를 활용해 하위의

작은 모듈/컴포넌트의 문제가 전체 구조에 어떤 영향을 미치는지 분석하는데 적합한 방법으로 의도하지 않은 상황을 확인 할 수 있다. FMEA는 주로 아래 <그림 1>과 같은 worksheet table을 활용해 분석을 수행하며, 대상의 잠재적인 failure mode 확인으로부터 시작해 그 영향 및 risk 를 분석하는 방법이다.

FMEA를 수행하기 위해서는 시스템의 functional 또는 structural decomposition이 중요하며 worksheet에서 item을 결정하는 부분이 된다. 또한 failure mode를 올바르게 확인하는 것이 중요하며 이 부분에 대한 연구들 또한 존재한다.

System:				Subsystem:					
Item	Failure mode	rate	Cause	Immediate effect	System effect	Detection	Hazard	Risk	Recommend

그림 1 FMEA worksheet 예제

STPA는 시스템 이론에 기반해 시스템의 안전을 고장의 문제가 아닌 제어의 문제로 분석하는 기법이다. 분석은 각각 컴포넌트의 고장 모드가 상위 수준에 미치는 영향을 분석하는 것이 아닌 각 컴포넌트의 컨트롤 명령 (control action)을 통해 상호작용을 모델링한 control structure를 작성하고, control structure로부터 위험이 발생할 수 있는 명령 및 원인을 분석하는 기법이다. 시스템을 STAMP (System Theoretic Accident Model and Process)기반의 모델로 작성하고 위험을 유발할 수 있는 제어 (Unsafe control action)도출 및 원인 확인으로 진행된다.

이외에도 FMEA와 유사한 worksheet을 이용하는 HAZOP 기법과 FTA와 유사한 이진 트리 형태로 분석을 수행하는 ETA (Event Tree Analysis), 문제가 발생하는 이벤트 연결 및 원인을 분석하는 ECFA, 안전성 분석의 구조적인 논증 구조를 제공하는 safety case[7] 등 다양한 기법들을 사용할 수 있다.

2.2 관련연구

위 절에서 설명한 바와 같이 위해도 분석을 위해 사용할 수 있는 기법들은 수많은 종류들이 있다. 기법에 따라 고장으로부터 그 결과를 분석하거나, 결과로부터 그 원인을 구성하는 기법 등 서로 다른 방법, 목적을 가지고 있다. 이 때 이러한 기법들을 통합해서 분석하고자 하는 노력들이 존재한다. 가장 자주 나타나는 방법은 FMEA와 FTA가 서로 반대의 분석을 목적으로 하는 과정에 착안하여 FMEA의 결과를 FTA를 통해 원인을 분석하거나, FTA의 결과를 FMEA를 통해 consequence를 재 분석하는 방법에 대한 연구들이 있다[8]. 그 외에도 STPA 분석 중 UCA의 원인 분석을 FTA를 통해 수행하는 통합에 대한 연구 또한 존재한다.

[5] 에서는 시스템 개발 시 안전성 분석 전 과정에 걸쳐 안전성 분석 결과, 개발 산출물, 안전 요구사항 및 위험 경감에 대한 추적성 분석에 대해 제안하였다. 하지만 해당 논문에서는 안전성 분석 전 과정에 더 초점을 맞추고 있어 위해도 분석의 추적성 분석에 대한 언급이 부족하다.

3. Hazard model

2.1 절에서 설명한 바와 같이 위해도 분석에 적용될 수 있는 분석 기법들은 다양한 기법들이 있으며 해당 기법들은 적용 방법, 목적 등에 조금씩 차이가 있다. 따라서 추적성 기반의 hazard model을 위해서는 각 기법에 대해 확인할 필요가 있다. 본 논문에서는 이를 모델링 하기 위해 각 위해도 분석 기법의 과정에 따라 각 기법의 1차 분류를 수행하고 각 분류를 기반으로 연결 관계 분석 및 메타모델을 개발하였다. 분류를 위해 사용한 기법은 특수 목적만을 위해 사용되는 방법을 제외하고 선정하였다.

3.1 기법의 추상화된 모델

위해도 분석에 사용되는 다양한 기법들은 서로 간의 차이점과 공통점을 가지고 분류할 수 있다. 본 논문에서는 기법들의 분석 방법의 공통점에 따라 이를 크게 5 +1 가지로 분류하였다. 본 논문에서 수행한 분류는 각 기법들의 특징을 추상화해 요소를 추출할 수 있는 기준으로 수행하였으며 이를 바탕으로 추상화된 다이어그램을 개발하였다. <표 1>은 본 논문에서 제안하는 위해도 분석 기법의 분류로 분류는 tree를 사용하는 기법들, worksheet을 사용하는 기법들, 다이어그램을 사용하는 두 분류의 기법, 그 외 시나리오 분석 및 safety case로 구성한다.

Tree 다이어그램을 사용하는 기법은 FTA, ETA와 같이 fault tree/event tree를 작성하고 이를 바탕으로 분석을 수행하는 기법들이 해당한다. Worksheet 기반의 분류는 FMEA, HAZOP과 같이 worksheet table을 이용하는 기법들이 속하며 그 외 PHA (Preliminary Hazard Analysis), FHA (Fault Hazard Analysis), SHA (System Hazard Analysis) 등이 있다. 다이어그램 분류는 fault tree외의 다이어그램을 사용하는 기법들이 속하며 위에서 설명한 STPA와 이벤트 나열을 통한 분석 기법인 ECFA/STEP 등이 해당된다.

표 1 적용 방법에 따른 위해도 분석 기법의 분류

Classification	Description	Technique
Tree diagram	Tree 형태의 다이어그램을 이용하는 분석 기법	FTA, ETA, CCA
Worksheet	Worksheet table을 이용하는 분석 기법	FMEA, HAZOP, PHA, Etc.
Diagram	STPA	-
	ECFA/STEP: Event chart를 이용하는 기법	-
Other	그 외 시나리오 분석	Checklist, What-if, Etc.
Safety case	Safety case	-

다음으로 기타 시나리오 분석 분류는 checklist, what-if analysis, scenario analysis와 같이 직접적인 위해도 분석도 가능하지만, 질문을 통해 해당 시스템이 어떤 위험을 내포하고 있는지 도움을 주는 리스트 기반의 기법으로 구성하였다. 마지막으로 safety case는 다른 기법들과 달리 직접적인 분석을 수행하는 기법은 아니지만 각 결과를 활용한 논증 구조를 작성해 safety demonstration, argument 등을 제공하는 기법이므로 분류에 포함하였다.

다음으로는 각 분류에 해당하는 기법들의 시작점 분석을 통해 분석 요소들을 추상화하였다. 시작점은 위해도 분석의 시작이 되는 지점을 정의한 것으로 FMEA는 item/component의 고장 모드로부터 그 결과를 분석하는 기법이기 때문이 처음(cause) 부분이 시작점이 된다. 반면 FTA는 failure/accident로 작성되는 top-event로부터 그 원인을 논리적으로 분석하는 기법이기 때문에 결과(result) 부분이 시작점이 될 수 있다.

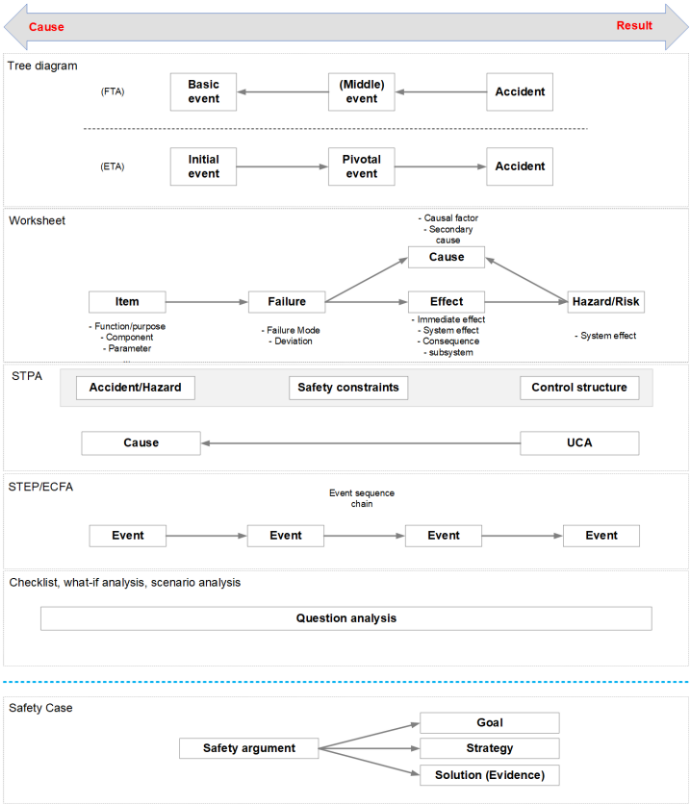

그림 2 기법의 분류에 따른 추상화 다이어그램

<그림 2>는 각 기법별로 시작점 분석의 결과로 도출된 위해도 분석의 방향에 따라 필수적인 요소들을 추출해 다이어그램으로 작성한 그림이다. Tree diagram에 속하는 FTA의 경우 accident (top event)부터 중간에 작성되는 event및 basic event로 구성되며, ETA의 경우 FTA와는 달리 초기 사건 (initial event)로부터 accident가 되는 과정의 이벤트로 구성된다. Worksheet 분류의 기법들의 경우 기본적으로 item으로부터 failure, effect, hazard/risk를 분석하는 과정으로 진행되며, 각 기법에 따라 요소들이 변화될 수 있음을 포함하고 있다.

3.2 기법의 연결 관계 분석

추적성 분석 (traceability analysis)는 소프트웨어 개발 시 요구사항과 다른 명세간의 관계를 정의하는 것으로 요구사항 명세가 디자인, 구현 단계를 거쳐 빠짐없이 구현되었는지 확인하거나, 관계 정의를 통해 요구사항의 변경을 손쉽게 반영할 수 있도록 하는 분석이다. 본 논문에서는 추적성 분석의 개념을 위해도 분석의 각 기법별로 도출되는 요소들 간에 item/component를 기준으로 추적 관계를 분석하는 것을 추적성 기반의 분석이라 한다.

추적 관계는 <그림 2>에 나타난 각 요소들을 기준으로 생각해 볼 수 있으며 본 논문에서는 이를 2 종류로 분석하였다. 첫 번째는 기본 사용 관계 (basic usage relation)으로 기존 연구에서 FMEA와 FTA를 보완관계로 사용하는 것과 같은 추적 관계이다. 다음으로는 기초 추적 관계 (basic trace relation)로 위해도 분석 결과 별 도출되는 각 요소들에 대해 item/component를 기준으로 추적 관계를 분석하는 추적성이다. Worksheet, STPA와 같이 item 항목이 명확하게 정의되는 경우는 해당 항목을 사용하며 FTA의 basic event와 같이 명확하게 정의되지 않는 경우는 간접적으로 드러나는 정보를 활용해 연결을 수행할 수 있다. 추가적으로 드러나는 이론적 의미의 추적성도 일부 포함하고 있다. 서로 다른 기법을 활용한 위해도 분석에서 같은 failure, 같은 hazard, 같은 과정의 경우를 연결하는 추적 관계이다. <표 2>는 해당 추적 관계의 일부에 대한 표이다.

표 2 각 기법의 추적 연결관계 (일부)

Relation between (from – to)	Description
(1) Basic event – (2) Failure	Failure equivalent trace
(1) Basic event – (2) Item	Component related trace
(1) Accident – (2) Hazard/Risk	Accident equivalent trace
(2) Item – (3) control structure	Basic component trace
(2) Effect/Hazard – (3) UCA/state variable	Failure relation
(2) Failure/effect/hazard – (4) Event	Failure event equivalent contents traceability
(4) Event – (5) question	Question extraction traceability
....	
2 (Hazard/Risk) -> 1 (Accident)	1 (Accident)와 연결해서 2 (Hazard/Risk) 의 원인 분석
2 (Failure) -> 1 (Accident)	1 (Accident)와 연결해서 2 (Failure) 의 원인 분석
2 (Failure) -> 4 (Event)	4 (Event)의 initial 에 2 (Failure)의 입력 으로 분석 가능
2 (Hazard/Risk) – 3 (Accident/Hazard)	2 (Hazard/Risk) can help to identify the hazard for 3 (Accident/Hazard)
....	

3.3 Hazard model의 메타모델

위해도 분석 기법들의 추상화된 다이어그램과 그 연결 관계를 모델링 하기 위한 메타모델은 다음 <그림 3>와 같다. <그림 3>는 3.1절의 다이어그램에 나타난 각 요소를 바탕으로 위해도 분석의 결과 및 추적 관계를 모델링 하도록 개발된 메타모델이다. 메타모델은 기본 분석에 따른 프로세스 관계부터 추적 관계까지 모두 표현하고 있다.

<그림 3>의 (a)는 위해도 분석 결과를 (b)는 <그림 2>에서 화살표로 표현된 요소들 간의 분석 과정을, (c)는 각 요소들의 추적 관계를 모델링 하도록 개발되었다. <그림 3>의 메타모델을 활용해 위해도 분석의 결과를 표현하고, 추적

관계에 대해 용이하게 작성할 수 있다.

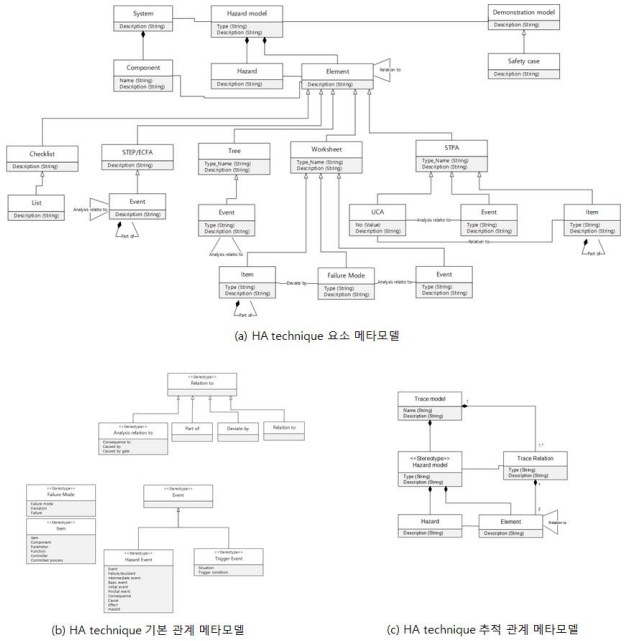

그림 3 Hazard model을 위한 메타모델

4. 사례연구

본 논문에서는 hazard model을 이용한 위해도 분석 결과의 표현을 위해 돌발상황 검지시스템 (AIDS)을 이용하여 사례 연구를 수행하였다. 현재는 제공된 정보의 한계로 인해 상위 레벨에서의 FMEA와 STPA만 적용되었다. 시스템은 교통장애를 유발하는 돌발상황을 검지하기 위한 시스템으로 시스템의 구성은 정보 수집, 처리 및 판단, 운영관리, 알림으로 구성되어 있다. <그림 4>는 돌발상황 검지시스템에 대한 FMEA와 STPA의 결과 중 일부를 메타모델을 활용해 표현한 그림이다. 아래 그림과 같이 시스템의 잠재적인 hazard에 대해 위해도 분석 요소들을 작성하는데 활용할 수 있다.

<그림 4>에 나타난 FMEA-STPA요소의 추적성은 다음과 같다. 특히 <표 3>에서 failure mode - cause 간의 추적성은 서로 다른 기법을 통해 다른 item끼리도 hazard가 연관된 추적성을 확인할 수 있음을 볼 수 있다. 이는 <표 2>에 정의한 관계 중에서 찾아볼 수 있다.

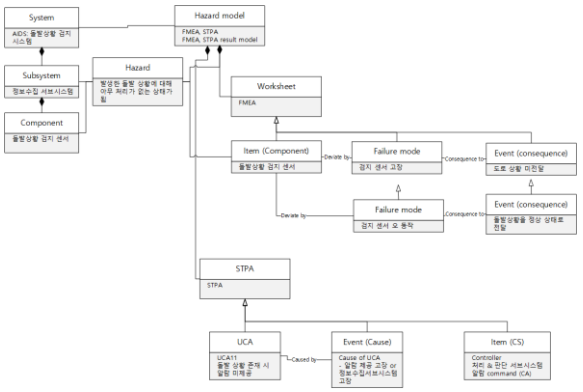

그림 4 FMEA, STPA 결과 일부에 대한 모델 표현

표 3 <그림 4>에 나타난 추적성 비교

Element		Description
FMEA	STPA	
Hazard	UCA	Same contents
Failure mode	Cause (event)	Same item traceability
Item	Cause (Event)	Implicit item traceability

5. 결론 및 향후 연구

본 논문에서는 위해도 분석 결과의 효과적인 확인 및 분석을 위해 위해도 모델을 제안하였다. 위해도 모델은 다양한 위해도 분석 기법들을 모델링하고 그 관계를 제시하였다. 이를 위해 본 논문에서는 다양한 위해도 분석 기법들을 방법, 범위에 맞게 추상화하고 추적 관계를 제시하였다. 이를 이용해 추적 관계에 대한 표현 및 작성을 용이하게 할 수 있어 위해도 파악에 도움이 될 것으로 기대한다. 향후 기법의 연결 관계에서 support 개념의 보완적 관계와 시스템 계층에 대한 고려를 포함한 모델에 대해 연구를 진행할 계획이다.

Acknowledgement

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업의 결과입니다. (NRF-2017R1D1A1B03030065)

참고 문헌

[1] Nancy G. Leveson, Jorge Diaz-Herrera, “Safeware: system safety and computers,” Addison-Wesley Reading, 1995.

[2] Clifton A. Ericson, “Hazard Analysis Techniques for System Safety”, John Wiley & Sons, 2005

[3] Nancy G. Leveson, “Engineering a Safer World: Systems Thinking Applied to Safety”, MIT Press, 2012

[4] EPRI, “Hazard analysis methods for digital instrumentation and control systems”, EPRI, 2013.

[5] Jang-Soo Lee, Vikash Katta, Eun-Kyoung Jee, Christian Raspotnig, “Means-ends and whole-part traceability analysis of safety requirements,” Journal of Systems and Software, Vol.83, No.9, pp.1612-1621, 2010.

[6] Vikash Katta, Tor St. Ihane, “A conceptual model of traceability for safety system,” 2nd International Conference on Complex Systems Design & Management, 2011.

[7] Office for Nuclear Regulation, “The purpose, scope, and content of safety cases”, An agency of HSE

[8] Fernando G Nicodemos, Carlos HN Lahoz, Martha AD and Saotome Abdala, Osamu, “Using Combined SFTA and SFMECA Techniques for Space Critical Software,” Proceedings of the 5th IAASS Conference A Safer Space for Safer World, 2012.