STPA-Sec의 적용을 통한 차세대 지능형 교통 시스템의 안전 및 보안 요구사항 도출 사례연구

A Case Study on the Derivation of Safety and Security Requirements for Cooperative Intelligent Transportation System through the Application of STPA-Sec

허윤아 (건국대학교 컴퓨터공학과, 석사과정)

유준범 (건국대학교 컴퓨터공학과, 교수)

Key Words : STPA-Sec, Safety Analysis, Security Analysis, Cooperative Intelligent Transportation System (C-ITS)

목 차

I. Introduction
II. Background
III. C-ITS에 대한 STPA-Sec 수행
IV. Conclusion and Future Work

I. Introduction

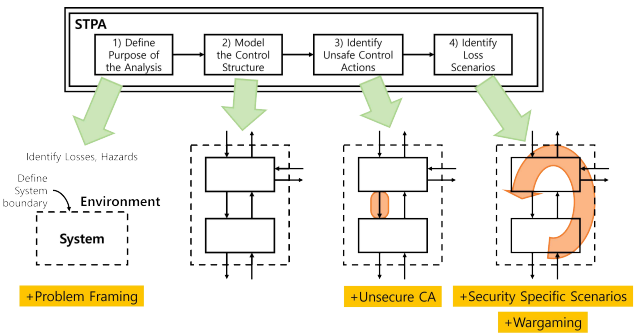
차세대 지능형 교통 시스템 (Cooperative Intelligent Transport System, C-ITS)은 여러 차량 사이에서, 그리고 차량과 주변 인프라 사이에서 정보를 상호공유하는 오픈 시스템이다[1]. ITS의 목적인 일반 운전 상황을 파악하는 것과 사고 발생 이후의 피해를 줄이는 것과 더불어, 사고가 발생하기 이전에 이를 예방하거나 회피하는 것을 목적으로 한다. C-ITS는 안전성이 중요한 시스템으로, 사고가 발생하면 인명 피해 및 인프라의 손실이 발생할 수 있기 때문에 사고가 발생하기 이전에 사고를 발생시킬 가능성이 있는 요인을 분석하는 위험 분석[2]을 필요로 한다. C-ITS는 차량과 차량 간 (Vehicle-to-Vehicle, V2V)의 통신과 차량과 인프라 간 (Vehicle-to-Infrastructure, V2I)의 통신을 기반으로 동작하기 때문에 cyber attack에 취약할 수 있다. 이 때문에 C-ITS는 위험 분석뿐 아니라 보안 분석 또한 필요로 한다.

많은 연구에서 자율주행 차량과 ITS에 대한 위험 및 보안 분석을 수행해왔으나, C-ITS 전체를 다루는 연구는 활발히 이루어지지 않았기 때문에, 본 연구에서는 C-ITS 전체를 다루는 방향으로 접근하고자 한다. 본 연구에서는 [1]에서 설명하고 있는 C-ITS를 기반으로 하는 가상의 C-ITS에 대해 위험 및 보안 분석을 위해 위험 및 보안 분석 기법인 Systems -Theoretic Process Analysis for Security (STPA- Sec)[3]를 적용하여 위험 및 보안 분석을 수행하고, 분석한 내용들을 통해 안전 요구사항과 보안 요구사항을 도출한다.

II. Background

1. STPA-Sec

STPA-Sec이란 STAMP[2] 기반의 위험 분석 기법인 STPA를 보안 측면에서까지 활용할 수 있도록 확장한 기법이다. 기본적으로 STPA와 수행 순서는 동일하고, security 측면의 분석이 추가로 더해진 형태이다. Security 측면에서 attack을 분류하는 기준으로는 STRIDE threat model[4]을 사용한다. STPA-Sec의 과정은 <그림 1>[3]을 따른다.



<그림 1> STPA-Sec Process

첫 번째 단계에서는 분석 대상이 되는 시스템의 goal/purpose와 경계(boundary)를 정의하며, loss, hazard, 그리고 constraint를 분석한다. Problem framing 단계를 통해 우리는 개발 주기 내의 전반적인 보안 컨셉을 결정할 수 있고, 보안 목표와 보안 요구사항을 정의 및 세분화할 수 있다.

Control structure는 하나 이상의 feedback-control loop으로 이루어진 시스템 모델로, controller가 controlled process에게 control action을 제공하면, controlled process가 그에 대한 feedback을 controller에게 전달하고, controller는 feedback을

기반으로 process model의 값을 업데이트하고, 그에 맞게 control action을 제공한다. Process model (internal belief)란 controller가 적절한 control action을 제공하기 위해 가지는 판단의 기준을 의미한다.

Control structure를 그리면서 각 controller가 controlled process에게 제공하는 control action을 식별하였다면, 그 control action들이 어떤 상황에서 hazardous (unsafe / unsecure)한지를 4가지 경우 (not providing causes hazard, providing causes hazard, incorrect timing or order, stopped too soon / applied too long)로 나누어서 분석한다.

마지막 단계는 loss에 대한 causal scenario를 분석하는 것, 그리고 그 결과들을 가지고 wargaming을 하는 것으로 구성되어 있다. Causal scenario란 hazardous control action이 어떤 이유로 발생했는지를 나타내는 scenario로, controller, control action, controlled process, feedback의 각 구성요소에 대해 크게 4가지 경우 (unsafe controller behavior, control path, other factors related to controlled process, causes of inadequate feedback / information)로 나누어서 분석한다. 이때 safety-related causal scenario와 security-related causal scenario는 동일할 수 있다. Wargaming 단계에서는 process 내에서 human adversary를 고려하여 이를 방지하기 위한 대책을 마련해 가면서 시스템을 보완해 나가는 것을 목표로 한다. 이때 human adversary에 의한 attack의 종류는 STRIDE threat model을 기준으로 하여 구분한다. Wargaming 단계를 통해 causal scenario를 분석하면, 어떤 구성요소가 어떤 공격을 받아서 해당 scenario가 발생하는지 확인할 수 있다.

2. Related Works

C-ITS의 내부 컴포넌트에 해당하는 시스템인 자율주행 차량과 ITS에 대한 위험 및 보안 분석은 많은 연구에서 다뤄졌다. [5]에서는 Hazard Analysis and Risk Assessment (HARA) 를 사용하여 자율주행 차량과 인프라 사이에 V2I 통신이 오작동하는 경우의 위험 분석을 진행하였다. [6]에서는 STPA와 Model-Based Systems Engineering (MBSE)를 결합하여 새로운 모델 기반의 시스템 분석 기법을 제안하였고, 이를 활용하여 connected and autonomous vehicle의 automatic emergency braking system에 대한 분석을 진행하였다. [7]에서는 Unified Safety and Security analysis method (US^2)라고 하는 새로운 위험 및 보안 분석 기법을 제안하면서 자율주행 차량에 대한 사례 연구를 진행하였다. [8]에서는 VANET 기반의 ITS에 대한 timing 및 보안 이슈들을 모델화하여 timing 및 보안 분석을 진행하였다.

III. C-ITS에 대한 STPA-Sec 수행

1. Target System

분석 대상이 되는 가상의 C-ITS는 차량 (vehicle) 및 운전자와 도로변 인프라 (roadside infrastructure), 그리고 central로 구성되어 있다. 차량은 차선 이탈 방지 기능, 가속 및 감속 기능 등의 일부 기능이 자동화되어 있고 주변 환경을 센서를 통해 탐지할 수 있는 level 3 수준[9]의 자율주행 차량으로, 주변의 차량과는 V2V 통신을 통해, 도로변 인프라와는 V2I 통신을 통해 데이터를 주고받을 수 있다. 도로변 인프라는 신호등, 도로 안내 전광판 시스템 등으로 구성되어 있고, 차량과 V2I 통신을 통해 데이터를 주고받고 이를 central로 전달하는 역할을 한다. Central은 중앙의 정보 처리 시스템으로, 여러 도로변 인프라로부터 무선 통신을 통해 데이터를 수집하고 처리하여 다시 인프라에 제공한다. Central을 관리하는 관리자 또한 별도로 존재하나, 본 연구에서는 C-ITS 전체를 시스템 레벨에서 다루므로 관리자는 고려하지 않는다.

2. STPA-Sec 적용 과정

Problem framing을 위해 필요한 C-ITS의 goal/purpose는 STPA-Sec의 작성 가이드에 따라 <표 1>과 같이 작성되었다.

<표 1> Goal/purpose of C-ITS

A System (무엇을)	to share information among roadside infra structure, autonomous vehicles, central sy stem
By means of (어떻게)	exchanging data through V2V and V2I co mmunication and wireless communication
In order to contribute to (왜)	prevention of accident occurrence and miti gation of damage cause by an accident

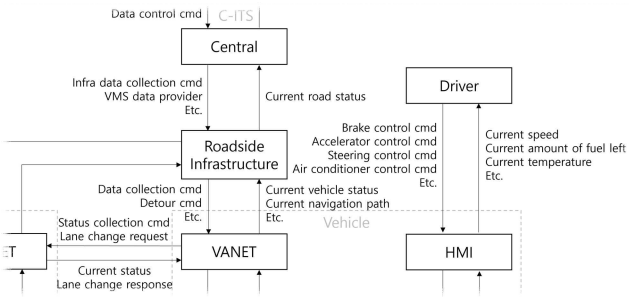
시스템의 loss와 hazard는 다음과 같이 식별되었다. Constraint의 경우 hazard에 대응하여 서로 반대되게 작성되었으므로 본 논문에서는 생략한다.

▷ Losses
- L1) 운전자의 부상 또는 사망
- L2) 보행자의 부상 또는 사망
- L3) 도로변 인프라의 손실 또는 손상
- L4) 차량의 손실 또는 손상

▷ Hazards
- H1) 차량이 다른 차량으로부터 안전거리를 유지하는 데에 실패함[L1, L4]
- H2) 차량이 보행자로부터 안전거리를 유지하는 데에 실패함[L1, L2, L4]
- H3) 차량이 도로변 인프라로부터 안전거리를 유지하는 데에 실패함[L1, L3, L4]
- H4) 도로변 인프라가 차량에게 올바른 정보를 제공하지 못함[L1, L2, L4]
- H5) 운전자가 차량에 대한 제어권을 손실함[L1, L2, L3, L4]

두 번째 단계에서는 control structure를 활용하여 분석 대상 시스템을 모델화한다. 현재 분석할 수 있는 수준의 C-ITS에 대한 전체 control structure 중 일부는 <그림 2>와 같다. <그림 2>에서 VANET (Vehicular Ad-hoc Network)은 V2V 및 V2I 통신을 위해 차량에 탑재되어 있는 네트워크이고, HMI (Human Machine Interface)는 차량의 계기판, 핸들, 브

레이크, 액셀 등을 포함하는, 차량과 운전자가 control과 feedback을 주고받기 위해서 필요한 기계 장치들을 의미한다. Driver라는 controller의 경우, control action을 제공하기 위해서 가져야 할 process model에는 앞차와의 거리, 현재 속도 등이 있다.



<그림 2> C-ITS의 control structure 중 일부

<표 2>는 driver가 HMI에 제공하는 brake control cmd라는 control action에 대해 분석한 hazardous control action의 예시이다.

<표 2> hazardous control action의 예시

Control Action	not providing causes hazard	providing causes hazard	incorrect timing or order	stopped too soon /applied too long
Brake control cmd	**Driver가 앞차와의 간격이 안전거리 이하인 상태일 때 brake control cmd를 제공하지 않음[H1]**	Driver가 주행 도중 갑자기 brake control cmd를 제공함[H1]	-	Driver가 속도가 충분히 줄어들지 않은 상태에서 brake control cmd를 멈춤[H1]

Hazardous control action의 위 예시 중 "Driver가 앞차와의 간격이 안전거리 이하인 상태일 때 brake control cmd를 제공하지 않음[H1]"에 대한 causal scenario 중 일부는 다음과 같이 도출될 수 있다.

- Driver가 미숙하여 혹은 착각하여 앞차와의 거리를 잘못 인식함
- Driver가 계기판을 잘못 보고 현재 속도가 안전거리 이내에서 정차하기에 충분한 속도라고 판단함
- HMI에서 현재 속도를 잘못 표기하여 driver가 현재 속도가 안전거리 이내에서 정차하기에 충분한 속도라고 판단함

마지막으로 위 scenario의 예시 중 세 번째인 "HMI에서 현재 속도를 잘못 표기하여 driver가 현재 속도가 안전거리 이내에서 정차하기에 충분한 속도라고 판단함"이라는 scenario의 경우, tampering attack을 통해 vehicle에 대한 attack이 성공했을 경우 HMI에서 현재 속도를 잘못 표기할 수 있다고 분석할 수 있다.

3. STPA-Sec 적용 결과

STPA-Sec의 적용 과정을 따라 위와 같이 C-ITS를 분석하여 안전 및 보안 요구사항을 도출한 결과는 다음과 같다. 위와 같은 과정으로 도출된 causal scenario들을 분석하는 단계를 거치면 우선적으로 안전 요구사항을 도출할 수 있다. 예를 들어서, 위의 scenario 예시 중 세 번째 항목인 "HMI에서 현재 속도를 잘못 표기하여 driver가 현재 속도가 안전거리 이내에서 정차하기에 충분한 속도라고 판단함"의 경우 "**HMI는 항상 현재 속도를 올바르게 표기해야 한다**"는 안전 요구사항이 도출된다. 또한, 앞서 wargaming 단계에서 도출된 결과를 분석하면, tampering attack에 대응하기 위해서는 "**V2V 또는 V2I 통신 시에 vehicle에 tampering attack을 수행할 수 없도록 해시 인증과 같은 무결성 (integrity) 검증 단계를 거쳐 통신하는 것**"이 하나의 해결책이 될 수 있음을 알 수 있다.

이처럼 어떤 시스템에 STPA-Sec을 적용하면, controller와 controlled process 사이에 주고받는 control과 그에 따른 feedback을 파악하고, 어떤 상황에서 control이 hazardous할 수 있는지, 그 원인은 무엇인지, 이를 방지하기 위해서 어떤 요구사항이 필요한지 분석할 수 있다. 그리고 이렇게 분석한 요구사항을 통해 시스템을 어떻게 보다 안전한 방향으로 발전시킬 수 있을지에 대해 생각해볼 수 있다.

IV. Conclusion and Future Work

C-ITS란 중앙 시스템과 도로변 인프라, 차량 간의 통신을 통해 데이터를 주고받으며 사고의 발생을 예방하고 사고가 발생했을 경우 피해를 최소화하기 위한 시스템이다. 이 시스템은 안전성과 보안이 중요하기 때문에, 위험 분석과 보안 분석이 진행되어야 한다. STPA-Sec을 통해, 우리는 human adversary에 의해서 행해질 수 있는 attack을 고려하여 hazardous control action과 causal scenario를 식별하고, causal scenario에 대한 분석을 통해 안전 요구사항뿐 아니라 보안 요구사항까지도 도출할 수 있다. 이렇게 도출된 요구사항들은 시스템을 보다 안전한 방향으로 발전시키는 데에 사용될 수 있다.

추후에는 C-ITS에 대한 좀 더 깊은 연구를 통해 도메인에 대한 이해를 더 넓히고, STPA-Sec 뿐만 아니라 다른 위험 분석 기법 및 보안 분석 기법을 수행하여 STPA-Sec을 통해서 도출된 안전 및 보안 요구사항을 더 발전시킬 계획이다.

참고문헌

1. 조순기. *C-ITS의 정의와 구성요소*. 교통기술과 정책. 11. 5. 72-77. 2014.
2. Nancy G. Leveson. *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press. 2016.
3. William Young Jr., Reed Porada. *System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA*. 2017 STAMP Conference. 2017.
4. Loren Kohnfelder, Praerit Garg. *The threats to our*

products. Microsoft Interface. April 1, 1999. Retrieved 18 August 2018.

5. Dae-ryong Ahn, Seong-geun Shin, Yun-seok Baek, et al.. Hazard Analysis of Autonomous Vehicle due to V2I Malfunction. The Journal of The Korea Institute of Intelligent Transport Systems. 18. 6. The Korea Institute of Intelligent Transport Systems. 251-261. 2019.
6. Duan Jianyu, Zhang Hongjun. Model-Based Systemic Hazard Analysis Approach for Connected and Autonomous Vehicles and Case Study Application in Automatic Emergency Braking System. SAE International Journal of Connected and Automated Vehicles. 4. 12-04-01-0003. 23-34. 2021.
7. Jin Cui, Giedre Sabaliauskaite. *US^2: An Unified Safety and Security Analysis Method for Autonomous Vehicles*. Future of Information and Communication Conference. 600-611. 2018.
8. Bowen Zheng, Muhammed O. Sayin, Chung-Wei Lin, et al.. *Timing and security analysis of VANET-based intelligent transportation systems: (Invited paper).* 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). 984-991. 2017.
9. *Automated Driving: Levels of Driving Automation*. Standard J3016. SAE International. Accessed: Oct. 2022. Available: https://www.sae.org/standards/content/j3016