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

건국대학교 컴퓨터공학과 허윤아

목차

1. Introduction

차세대 지능형 교통 시스템

(Cooperative Intelligent Transportation System, C-ITS)

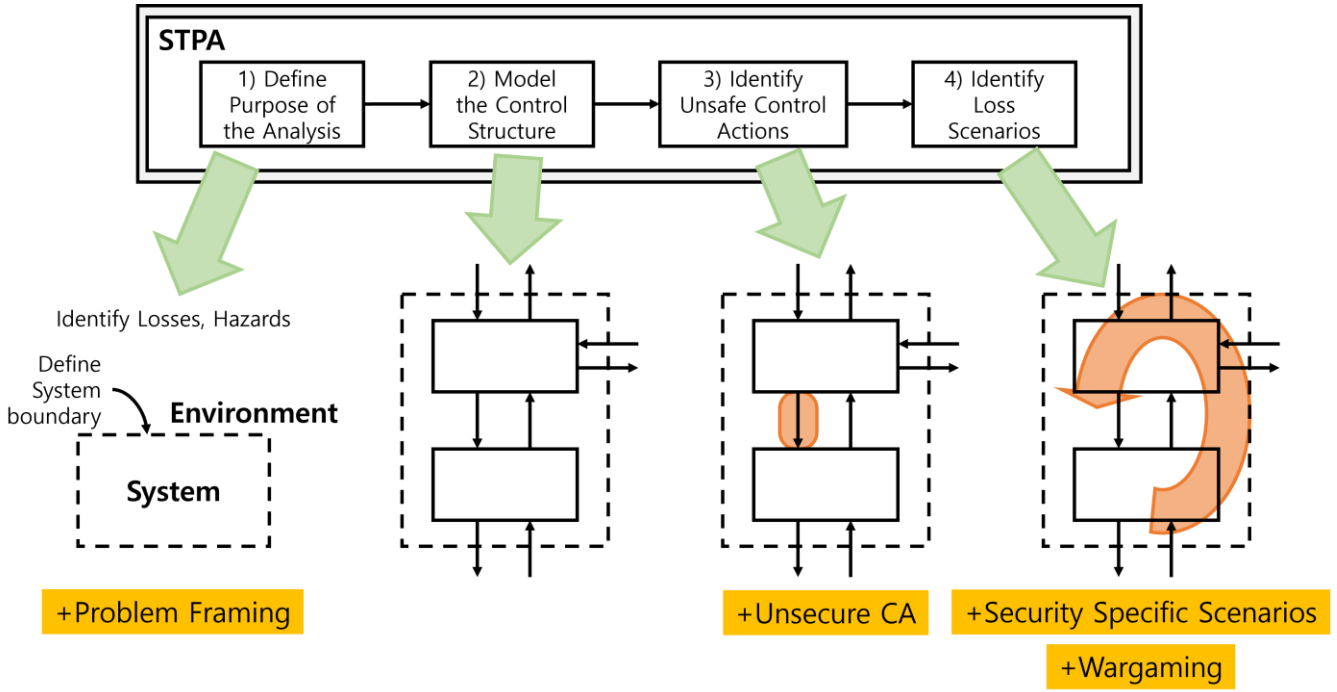
- 여러 차량 사이에서, 차량과 주변 인프라 사이에서 정보를 상호공유하는 오픈 시스템
- 목적: 기존 ITS의 목적 (일반 운전 상황의 파악 + 사고 발생 이후의 피해 경감) + 사고의 예방 및 회피

- 안전 중요 (safety-critical) 시스템 → 위험 분석 필요
- V2V, V2I 등의 '통신' 기반 → 보안 분석 필요

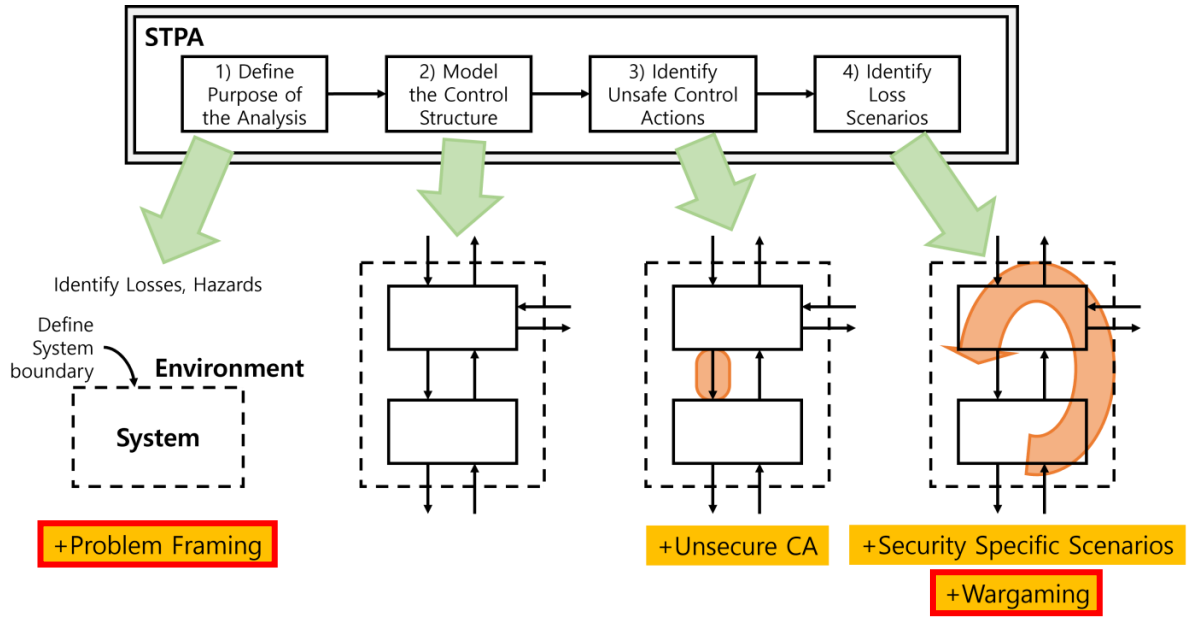
II. Background

1. STPA-Sec

- STAMP 기반의 위험분석기법인 STPA (Systems-Theoretic Process Analysis) 를 보안 측면까지 확장
- STPA와 기본적인 수행 순서는 동일



II. Background



- Problem Framing: 개발 주기 내의 전반적인 보안 컨셉 결정, 보안 목표와 보안 요구사항의 정의 및 세분화
- Wargaming: Causal scenario를 분석하여 어떤 구성요소가 어떤 공격을 받아서 해당 scenario가 발생하는지 확인

II. Background

- Security 측면에서 attack을 분류하는 기준으로 STRIDE threat model 사용
  - **S**poofing Identity: 유효한 시스템 사용자 또는 리소스를 가장하여 시스템 보안을 손상시킴
  - **T**ampering with Data: 탐지 여부와 관계 없이 시스템 또는 사용자의 데이터를 수정하는 것
  - **R**epudiation: 신뢰할 수 없는 사용자가 추적 기능이 없는 잘못된 작업을 수행하는 것
  - **I**nformation Disclosure: 사용자의 개인정보 또는 사업에 있어 중요한 정보를 손상시키는 것
  - **D**enial of Service: 시스템을 일시적으로 사용 불가능하게 만드는 것
  - **E**levation of Privilege: 권한이 없는 사용자가 시스템 전체를 손상시키거나 파괴할 수 있는 충분한 권한을 얻는 것

II. Background

2. Related Works

- Hazard Analysis and Risk Assessment (HARA)를 활용한 V2I 통신이 오작동하는 경우에 대한 위험 분석을 진행한 사례
- STPA와 Model-Based Systems Engineering (MBSE)을 결합하여 새로운 모델 기반 시스템 분석 기법을 제안, connected and autonomous vehicle의 automatic emergency braking system에 대한 분석을 진행한 사례
- 새로운 위험 및 보안 분석 기법인 Unified Safety and Security Analysis Method (US^2)를 제안하여 자율주행 차량에 대한 사례 연구를 진행한 사례
- VANET 기반의 ITS에 대한 timing 및 보안 이슈들을 모델화하여 분석을 진행한 사례

III. C-ITS에 대한 STPA-Sec 수행

1. Target System

- C-ITS
  - 차량 (vehicle): 많은 기능들을 자율적으로 수행 가능하나 운전자의 동승을 여전히 필요로 하는 level 3 수준의 자율주행 차량
    - 주변 차량과는 V2V 통신을, 도로변 인프라와는 V2I 통신을 통해 데이터를 주고받을 수 있음
  - 도로변 인프라 (roadside infrastructure): 도로 주변의 인프라 시스템
    - 차량과 V2I 통신을 통해 데이터를 주고받고 이를 central로 전달하는 역할
  - Central: 중앙의 정보 처리 시스템
    - 여러 도로변 인프라로부터 무선 통신을 통해 데이터를 수집, 처리하여 다시 인프라에 제공

III. C-ITS에 대한 STPA-Sec 수행

2. STPA-Sec 적용 과정

- Step 1
  - Goal / purpose

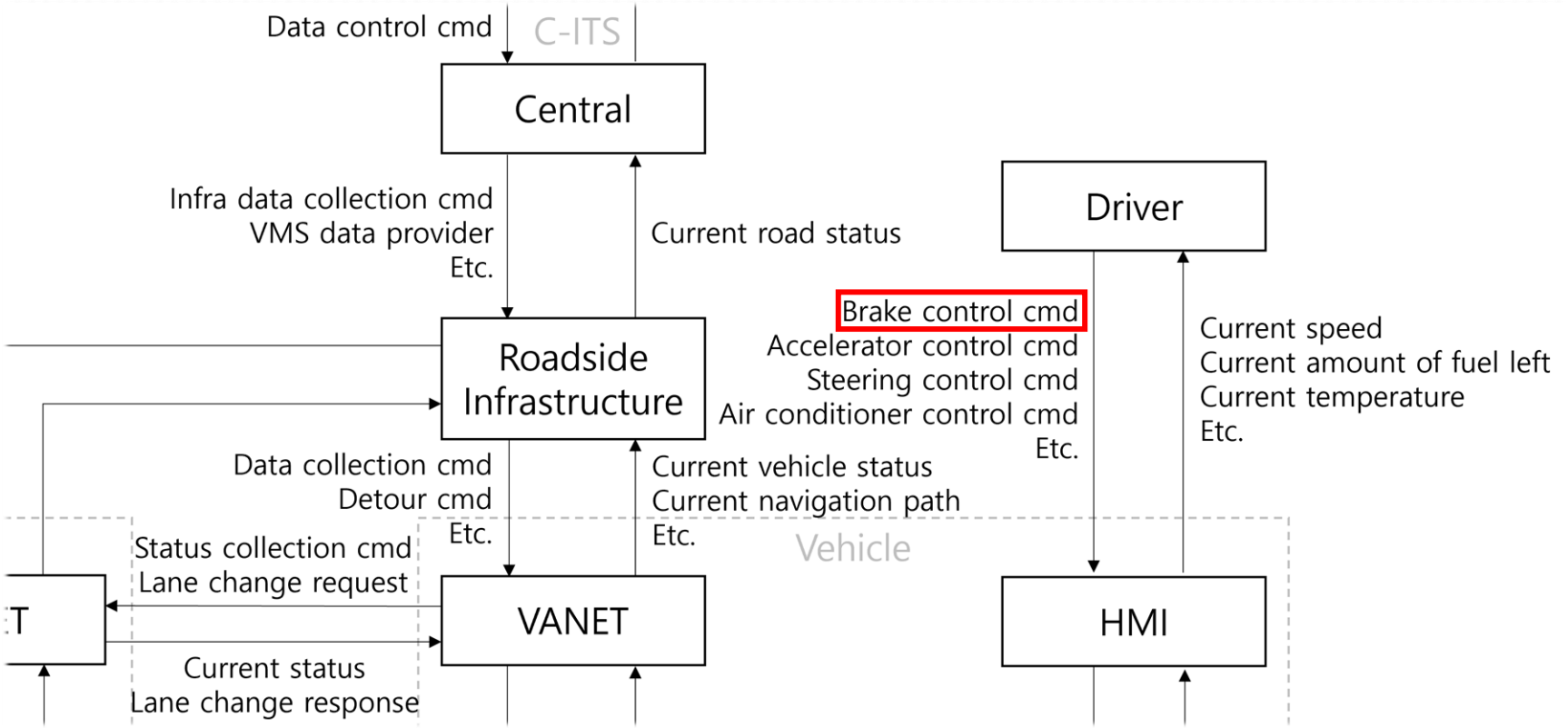
A System (무엇을)	to share information among roadside infrastructure, autonomous vehicles, central system
By means of (어떻게)	exchanging data through V2V and V2I communication and wireless communication
In order to contribute to (왜)	prevention of accident occurrence and mitigation of damage cause by an accident

III. C-ITS에 대한 STPA-Sec 수행

- Step 1
  - 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 안프라로부터 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]

III. C-ITS에 대한 STPA-Sec 수행

- Step 2
  - Control structure 중 일부



III. C-ITS에 대한 STPA-Sec 수행

- Step 3
  - Driver가 HMI에 제공하는 brake control cmd CA에 대해 분석한 Hazardous CA의 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]

- Step 4
  - Causal scenario 예시
    - HMI에서 현재 속도를 잘못 표기하여 driver가 현재 속도가 안전거리 이내에서 정차하기에 충분한 속도라고 판단함
  - Wargaming
    - Tampering attack을 통해 vehicle에 대한 attack이 성공했을 경우 HMI에서 현재 속도를 잘못 표기할 수 있음

III. C-ITS에 대한 STPA-Sec 수행

3. STPA-Sec 적용 결과

“HMI에서 현재 속도를 잘못 표기하여 driver가 현재 속도가 안전거리 이내에서 정차하기에 충분한 속도라고 판단함”

- 안전 요구사항
  - HMI는 항상 현재 속도를 올바르게 표기해야 한다
- 보안 요구사항
  - V2V 또는 V2I 통신 시에 vehicle에 tampering attack을 수행할 수 없도록 해시 인증과 같은 무결성 (integrity) 검증 단계를 거쳐 통신해야 한다

- STPA-Sec을 적용하면…
  - Controller와 controlled process 사이에 주고받는 control과 그에 따른 feedback을 파악
  - 어떤 상황에서 control이 hazardous할 수 있는지, 원인은 무엇이며, 이를 방지하기 위해 어떤 요구사항이 필요한지 분석할 수 있음

IV. Conclusion and Future Work

- Conclusion
  - STPA-Sec을 통해 human adversary에 의해서 행해질 수 있는 attack을 고려하여 hazardous control action과 causal scenario 식별
  - Causal scenario에 대한 분석을 통해 안전 및 보안 요구사항 도출 가능
  - 도출된 요구사항들을 통해 시스템을 보다 안전한 방향으로 발전시킬 수 있음

- Future work
  - STPA-Sec 뿐 아니라 다른 위험 분석 기법 및 보안 분석 기법을 수행하여 STPA-Sec을 통해 도출된 안전 및 보안 요구사항을 더 발전시킬 계획

감사합니다 ☺

Q&A

hya1202@konkuk.ac.kr