STPA를 이용한 군집 운행 시스템의 안전성 분석 사례 연구

김의섭[O], 유준범
건국대학교 컴퓨터공학과
atang34@konkuk.ac.kr, jbyoo@konkuk.ac.kr

A Study on Application of STPA in Safety Analysis of Platoon System

Eui-Sub Kim, Junbeom Yoo
Division of Computer Science and Engineering

요 약

본 연구는 군집 운행 시스템에 STPA를 이용하여 안전성 분석을 수행한 결과를 기술하고자 한다. 군집 운행 시스템에서의 사고는 사람의 생명을 위협하고 큰 재산의 손실을 유발하기 때문에, 반드시 안전성 분석을 통해 발생할 수 있는 다양한 사고 원인과 위협원을 사전에 식별하고, 이를 제거 및 감소시키는 노력이 필요하다. 하지만 군집 운행 시스템의 복잡성과 복합적인 상호 운용성은 기존의 단순 컴포넌트 수준의 안전성 분석 기법으로는 위협원을 식별하기 쉽지 않다. 본 논문에서는 시스템 수준의 통합적인 관점을 가지고 있는 STPA 방법을 이용해 해당 시스템을 적용 과정과 이를 통해 식별한 위협 시나리오의 예를 기술하고자 한다.

1. 서 론

차량 간 통신 커뮤니케이션의 발전과 자율주행 기술의 발전으로 인해 군집주행 기술이 다양한 곳에서 연구 개발 중이다. 군집 주행이란 두 대 이상의 차량이 일정한 차량 간격을 유지하며 하나의 그룹을 이루어 주행하는 것을 의미한다. 군집 주행을 통해 앞차와의 거리를 줄여 공기저항을 줄이고, 이를 통해 연비 개선을 도모할 수 있다. 또한, 자율운전으로 인해 운전자의 피로도를 줄이고, 졸음 및 부주의한 운전으로부터 생길 수 있는 사고를 미연에 방지할 수 있다[1, 2, 3].

군집 운행 시스템은 다양한 이점이 있는 반면, 해당 시스템에서의 사고는 사람의 생명을 직접적으로 위협하며 재산상의 큰 손실을 유발하는 안전 필수 시스템이기 때문에, 반드시 안전성 분석을 통해 발생할 수 있는 다양한 사고 원인과 위협원을 식별하고, 사전에 제거 및 감소시키는 노력이 필요하다. 하지만 군집 운행 시스템의 복잡성과 상호 운용성은 개발 시 의도하지 않은 오동작을 유발시킬 수 있다. 따라서 개발 설계 단계부터 안전성 분석을 통해 안전 요구사항을 식별하고 이를 개발에 반영하도록 하는 안전성 분석 기반 개발이 수행되어야 한다. 이러한 시스템을 분석하기 위해서는 단일 컴포넌트 수준이 아닌 전체 시스템 수준에서 분석을 수행하는 것이 중요하다.

본 논문에서는 시스템 이론 기반의 안전성 분석 기법인 STPA (System-Theoretic Process Analysis) [4, 5, 6]를 이용해 군집 운행 시스템의 안전성 분석을 수행하고, 이를 통해 밝혀낸 시스템의 위협 시나리오와 STPA를 군집 운행 시스템과 같은 동적 변화가 심한 시스템의 적용에 어려움에 대해 기술한다.

2. STPA (System-Theoretic Process Analysis)

STPA는 기존 안전성 분석 기법들의 개념인 '컴포넌트의 실패' 보다는 '시스템 또는 컴포넌트 간 제어 문제'에 의해 사고가 발생한다고 보고, 시스템을 컨트롤 관계를 중심으로 구조화하여 위험 분석을 수행한다. 따라서 단순 컴포넌트의 나열 후 분석을 수행하기 보다 안전에 영향을 미치는 컨트롤을 식별하고 이를 중심으로 시스템을 추상화하여 분석함으로써 보다 규모가 크고 복잡한 시스템을 분석하는데 용의한 분석 방법이다.

STPA의 단계는 그림 1과 같이 크게 4단계로 구성된다.
1) Define Purpose of the Analysis: Losses와 System-level hazards, system-level constraints를 식별한다
2) Model the Control Structure: 시스템을 안전에 영향을 주는 컨트롤러와 컨트롤, 피드백을 중심으로 Control Structure를 작성한다.
3) Identify Unsafe Control Actions: 4가지 유형에 따른 Unsafe Control Action을 도출한다. 4가지 유형은 다음과 같다. ⓐ Control action is not provided, ⓑ Unsafe Control Action is provided, ⓒ Control Action is too early, too late, out of sequence, ⓓ Control

Action is stopped too soon, applied too long.
4) Identify Loss Scenarios: 3에서 식별된 Unsafe Control Action의 발생 원인을 도출한다. 해당 단계에서는 위험을 유할 할 수 있는 Unsafe Control Action이 왜 발생하게 되었는지를 분석함으로써 시스템의 위험요소를 식별하고 시스템의 안전성을 확보하는데 기여할 수 있다.

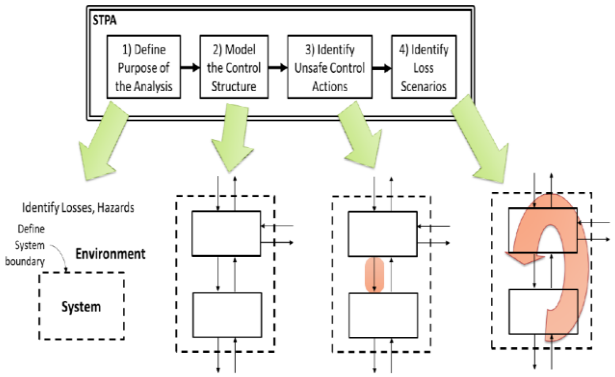

그림 1. Overview of the basic STPA Method [4]

3. 군집 운행 시스템의 안전성 분석

3.1 타겟 시스템

타겟으로 하고 있는 군집 운행 시스템의 주요 기능은 다음과 같다.

1) 군집 합류: 군집 외 차량이 군집의 끝 또는 중간에 합류하는 기능. 합류하고자 하는 차량의 운전자로부터 합류 요청을 받아 리더의 허락 하에 합류가 이루어진다. 합류 후에는 리더는 해당 차량의 정보를 저장하고, 합류 차량은 자율 주행 모드로 전환된다.
2) 군집 운행 유지: 리더가 군집의 속도를 제어하는 기능. 리더의 운전자는 운전을 직접 수행하며, 리더의 운전자에 의해 변경된 속도를 군집 내 모든 차량에게 전파하여 군집의 속도를 전체적으로 제어한다. 이를 통해 보다 전체적인 속도 제어를 할 수 있어 효율적인 군집 운행이 가능하다.
3) 군집 이탈: 군집 내 차량(리더 포함)이 군집을 이탈하는 기능. 이탈하고자 하는 차량의 운전자로부터 해당 요청이 이루어지며, 리더의 허락 하에 이탈이 수행된다. 이탈 후에는 자율주행 모드에서 수동 주행 모드로 변경되며, 리더의 경우 리더의 뒤 차량에게 리더를 인계하는 과정이 수반된다.
4) 자율 주행: 군집 내 차량들이 스스로 차간거리를 유지하며 군집 운행이 이루어지도록 제어하는 기능이다. 해당 시스템의 아키텍처는 그림 2와 같다. 해당 시스템은 차량내 위치하게 되며 외부와의 V2X 커뮤니케이션과 차량 내 Sensor, 운전자로부터 입력을 받아 차량 내 ECU에게 명령을 전송한다. 크게 군집 운행을 관리하는 Platooning Controller와 자율 주행을 담당하는 Adaptive Cruise Controller로 구성되어 있다.

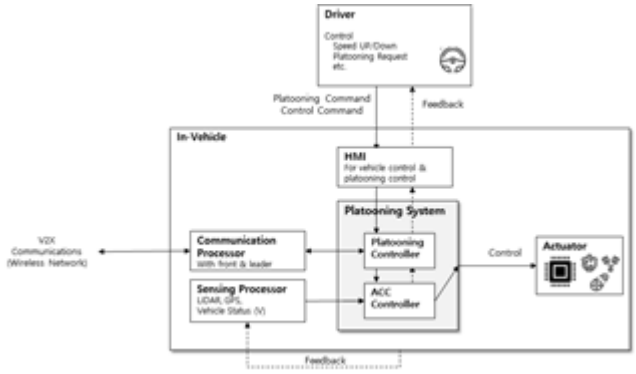

그림 2 군집 운행 시스템의 아키텍처

3.2 STPA 적용

3.2.1 Define Purpose of the Analysis

타겟 시스템의 accident와 hazard는 아래와 같고, 개략적인 내용은 기존 논문들[7, 8]을 참고 하여 작성하였다.

A-1) people die or become injured
A-2) damage to vehicle
A-3) fail of the platooning
H-1) Vehicles collide with each other
H-1.1) inappropriate distance interval with front vehicle
H-1.2) inappropriate distance interval with back vehicle
H-1.3) fail to measure distance surrounding vehicles
H-2) Vehicles dash to pedestrian
H-3) fail to communication between vehicles

3.2.2 Model the Control Structure

Platoon 시스템에서 차간거리 유지를 컨트롤하는 컨트롤러인 Adaptive Cruise Controller (ACC)를 중심으로 작성된 Control Structure는 그림 3과 같다.

3.2.3 Identify Unsafe Control Actions

작성한 Control Structure를 바탕으로 Unsafe Control Action에 대해 4가지 Type으로 작성을 진행하였다 <표 1>. 표를 살펴보면, ACC는 앞차와의 거리가 Safe 차간거리보다 가까울 경우 감속 Control Action을 제공해야 한다. 이를 제공하지 않을 경우 앞차량과의 추돌로 이어지기 때문에 사고가 발생할 수 있다. 해당 경우는 제공되어야 할 Control Action이 제공되지 않아 사고가 발생할 수 있는 Unsafe Control Actions으로 식별을 진행할 수 있다. 마찬가지로 앞차와의 차간거리가 Safe 차간거리보다 가까울 경우, 가속 Control Action이 발생한다면 H.1.1과 연관된 Unsafe

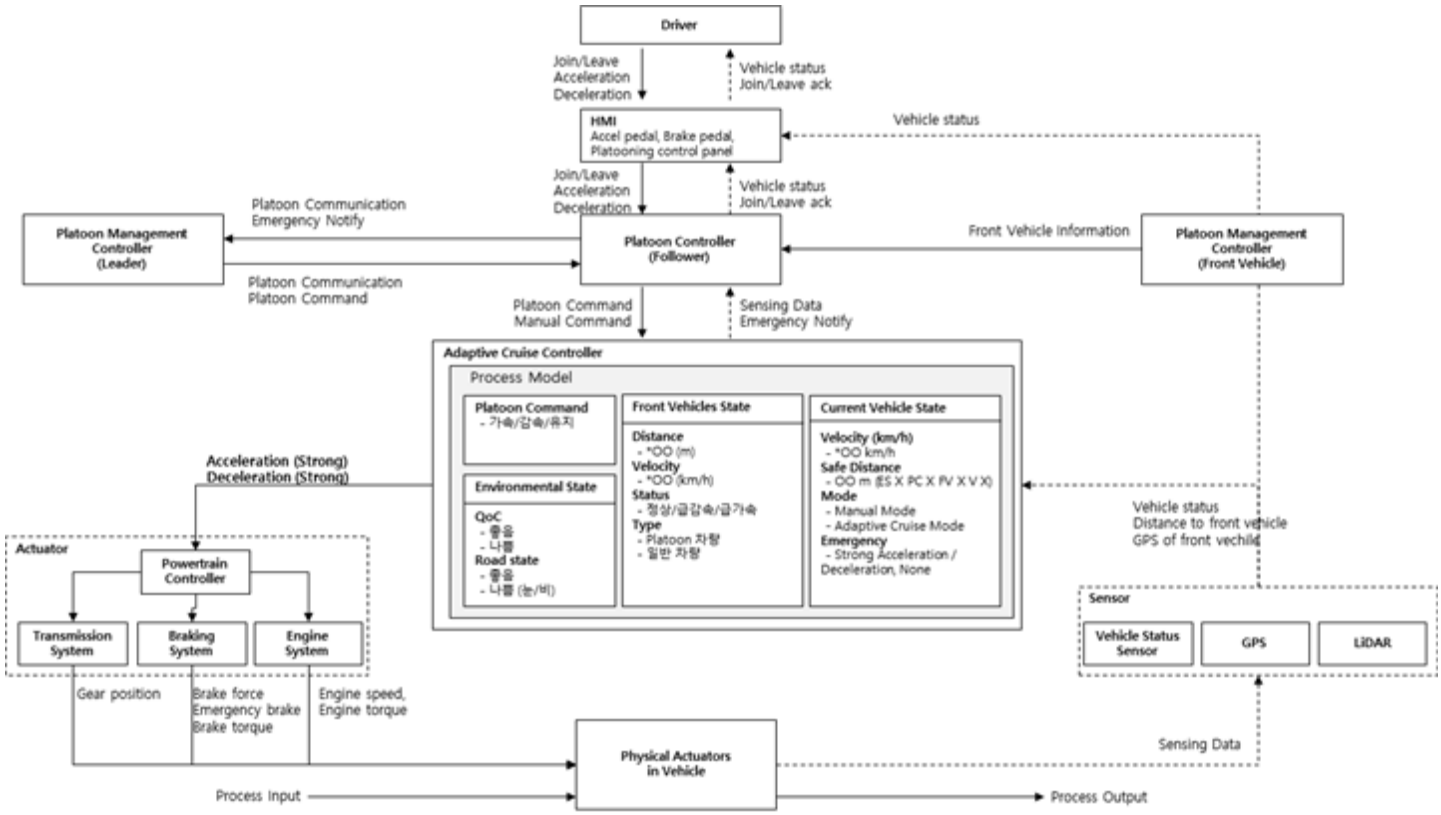

그림 3 Platoon 시스템의 Control Structure

Control Action으로 분석할 수 있다.

3.2.4 Identify Loss Scenarios

마지막으로 3.2.3에서 분석한 Unsafe Control Action이 왜 발생하게 되었는지 분석한다. 크게 두가지 유형으로 분류를 할 수 있다. 1) 왜 Control Action이 Unsafe하게 제공되었는가? 2) Control Action이 왜 부적절하게 수행되거나 제대로 수행되지 못했는가? 해당 분석을 바탕으로 Causal Scenario를 작성해 낼 수 있다. 표1의 Unsafe control action 중 하나인 “Adaptive Cruise Controller가 앞차와의 거리가 Safe 차간거리보다 가까울 때, Deceleration을 제공하지 않는다.”에 대해서 식별한 Causal Scenario는 다음과 같다.

o (Controller receives incorrect feedback/information) 앞차와의 거리가 Safe 차간거리보다 가까울 때, 산악지대라 앞차와의 통신 상태가 좋지 못해, 앞차의 속도 및 GPS 값을 수신하지 못해서, Safe distance 계산을 실패하였다. 따라서 Deceleration을 제공하지 않는다.

o (Controller receives correct feedback/information but interprets it incorrectly or ignores it) 앞차와의 거리가 Safe 차간거리보다 가까울 때, Cut in 차량과 Leave 차량이 동시에 있을 경우, Cut in 차량을 기준으로 safe distance를 측정해야 하는데, Leave 차량을 고려하여 safe distance를 계산 Distance가 충분히 멀다고 판단하여, Deceleration을 제공하지 않는다.

o (Controller does not receive feedback/information when needed (delayed or never received)) 앞차와의 거리가 Safe 차간거리보다 가까울 때, CAN의 연결되어 있는 다른 장비의 통신 과사용으로 인해, Sensing 정보가 제대 들어오지 못해, Safety distance를 계산하여, Distance가 충분히 멀다고 판단, Deceleration을 제공하지 않는다.

o (Feedback/info sent by sensor(s) but not received by controller) 앞차와의 차간거리가 Safe 차간거리보다 짧을 때, LiDAR 센서의 정보가 CAN의 보안 공격으로 인해 정확한 센싱 값을 수신하지 못함 Safe 차간거리가 충분한 것으로 잘못 판단 내림, 따라서 Deceleration을 제공하지 않았다.

o (Control action is not applied or received by the controlled process but the process responds as if the control action had been applied or received) 앞차와의 차간거리가 Safe 차간거리보다 짧을 때, Automatic Cruise controller는 아무것도 송신하지 않았지만, 타 시스템 (후방 차량 감지 시스템)의 영향으로 Acceleration을 수행함, Deceleration을 수행하지 않음 & Acceleration을 수행함 (Manual vs. Automatic)

또한, “Automatic Cruise Controller가 앞차와의 거리가 Safe 차간거리보다 가까울 때, Deceleration을 너무 늦게 제공하였다.”에 대해서도 원인 분석을 해보면, 앞차의 급정거가 Sensor가 반응하기에 또는 Physical

표 1 Unsafe Control Action 도출

Unsafe Control Actions	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Deceleration	Adaptive Cruise Controller가 **앞차와의 거리**가 **Safe 차간거리**보다 가까울 때, **Deceleration**을 제공하지 않는다. [H1] Adaptive Cruise Controller가 **앞차가 급 감속 중** 일 때, **Deceleration**을 제공하지 않는다. [H1] Adaptive Cruise Controller가 **앞 공간에 Join 요청이 있을 경우에**, **Deceleration**을 제공하지 않는다. [H1]	Adaptive Cruise Controller가 **Driver가 감속 명령**을 했을 때, **Deceleration**을 제공하지 않는다. [H1]	Automatic Cruise Controller가 **앞차와의 거리**가 **Safe 차간거리**보다 가까울 때, **Deceleration**을 너무 늦게 제공하였다. [H1] Automatic Cruise Controller가 **앞차가 급 감속 중** 일 때, **Deceleration**을 너무 늦게 제공하였다. [H1]	
Acceleration	Adaptive Cruise Controller가 **Driver가 가속 명령**을 했을 때, **Acceleration**을 제공하지 않는다. [H1]	Automatic Cruise Controller가 **앞차와의 거리**가 **안전 차간거리**보다 가까울 때, **Acceleration**을 제공한다. [H1] Automatic Cruise Controller가 **앞차가 급 감속 중** 일 때, **Acceleration**을 제공한다. [H1]		

Process가 반응하기에 너무 빠른 경우도 원인으로 분석할 수 있다. 또한, 앞차의 앞차의 급정거가 전파되어 차간거리를 유지하는 Control Action이 Unsafe Control Action이 되는 원인으로 작용할 수 있다. 이럴 경우 앞차와의 간격을 센서만으로 식별하기 보다 급정거에 대한 정보를 리더 차량에 전달하여 급정거 후방의 차들이 적절한 대응을 할 수 있도록 안전 요구상항을 만들어 시스템에 반영하는 것이 안전성을 보장하는데 도움이 될 것으로 판단 내릴 수 있다

본 논문에서는 차간거리와 관련된 Hazard를 중심으로 STPA를 분석을 진행하였다. 하지만 A-3) fail of the platooning 과 같이 차간거리가 아닌 다른 컨트롤에 대해 분석하려면 해당 컨트롤과 관련 있는 Control Structure를 다시 작성하여 분석을 수행해야 하는 번거로움이 있다. 또한, 군집 운행과 같이 다양한 조합과 다양한 상황이 발생하는 경우 각각의 상황을 모두 계획하여 다시 분석해야 하는 어려움이 있다. 이런 가변적인 모든 상황을 고려하여 분석하는 것은 시간과 노력 측면에서 매우 비효율적인 모습을 가질 수 있다. 따라서 가변적으로 조합되어 상호 운용되는 시스템에 대해서 효과적으로 표현하고 분석하는 추가적인 방안이 필요할 것이다.

4. 결 론

본 논문에서는 군집 운행 시스템에 대해 STPA를 이용하여 안전성 분석을 수행한 과정과 일부의 결과를 기술하였다. 안전성 분석의 결과로 Loss Scenarios까지 도출한 결과의 일부를 도출하였으나, STPA의 분석 시 군집 운행과 같은 동적으로 다변하고 조합되어 상호 운용되는 시스템을 분석하기에 제한적인 모습이 있다는 것도 알 수 있었으며, 추후 이런 제한적인 부분에 대해 연구하여 효과적으로 군집 운행과 같은 사이버-피지컬 시스템을 분석하는데 도움이 되는 연구를 진행 하고자 한다.

사 사

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업 (NRF-2017M3C4A7066479)의 지원을 받아 수행한 연구임.

참고 문헌

[1] Kit, Michal, et al. “An architecture framework for experimentations with self-adaptive cyber-physical systems.” Proceedings of the 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems. IEEE Press, 2015.

[2] Muccini, Henry, Mohammad Sharaf, and Danny Weyns. “Self-adaptation for cyber-physical systems: a systematic literature review.” Proceedings of the 11th international symposium on software engineering for adaptive and self-managing systems. ACM, 2016.

[3] Bergenhem, Carl, et al. “Overview of platooning systems.” Proceedings of the 19th ITS World Congress, Oct 22-26, Vienna, Austria. 2012.

[4] Nancy G. Leveson, “Engineering a Safer World.” MIT Press (MA), 2011.

[5] Nancy G. Leveson, “STPA: A new hazard analysis technique.” MIT Press, 2012.

[6] Leveson, Nancy G., and John P. Thomas. “STPA handbook.” Cambridge, MA, USA, 2018.

[7] Abdulkhaleq, Asim, and Stefan Wagner. “Experiences with applying STPA to software-intensive systems in the automotive domain.” 2018 3rd International Conference on System Reliability and Safety (ICSRS), 2013.

[8] Stoltz-Sundnes, Max, “STPA-Inspired Safety Analysis of Driver-Vehicle Interaction in Cooperative Driving Automation”, KTH, School of Industrial Engineering and Management (ITM), TRITA-ITM-EX, 2019:687, 2019.