KCSE 2020
2020년 2월 03일(월) ~ 05일(수),
강원도 평창 한화리조트 (휘닉스파크점)

STPA를 이용한 군집 운행 시스템의 안전성 분석 사례 연구

김의섭, 유준범

Konkuk University

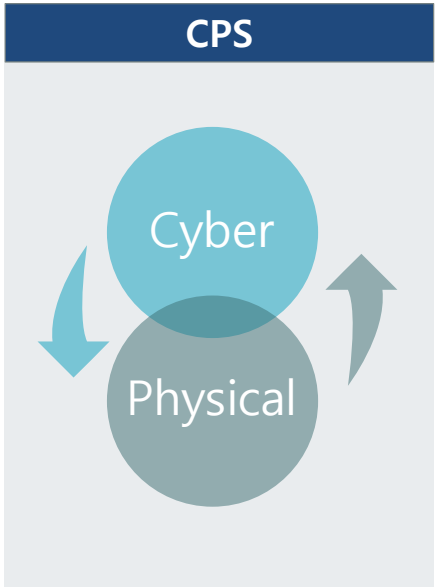
Dependable Software Laboratory

서론

STPA를 이용한 군집 운행 시스템의 안전성 분석 사례 연구

- **RQ**: 시스템의 구성 요소가 동적으로 조합이 되는 CPS (Cyber-Physical System)에 기존 안전성 분석 기법(STPA)의 적용에 어려움이 없을까?

- **타겟**: 군집 운행 시스템 (Platoon system)
- **분석 방법**: STPA (Systems Theoretic Process Analysis)



+ **STPA**

안전성 분석

적용 가능성
- 적용이 잘 될까?

문제 식별
- 적용이 어렵다면 무엇이 문제일까?

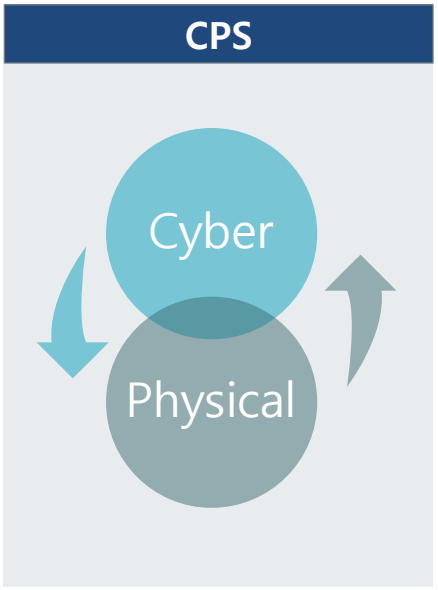
해결 방법
- 어떻게 해결 할 수 있을까?

사이버-피지컬 시스템

사이버-피지컬 시스템 (CPS – Cyber Physical System)

- 현실 세계의 다양한 물리, 화학 및 기계공학적 시스템(physical systems)이 컴퓨터와 네트워크(cyber systems)를 통해 커뮤니케이션 하여 → 피지컬 시스템을 자율적, 지능적으로 제어하는 시스템 – 네이버 백과사전

- 현실 세계의 정보를 실시간으로 수집(sensing) 하여 지능적, 자율적 연산(cyber process) 후 현실 세계(physical process)에 피드백 하여 운용되는 시스템 및 패러다임

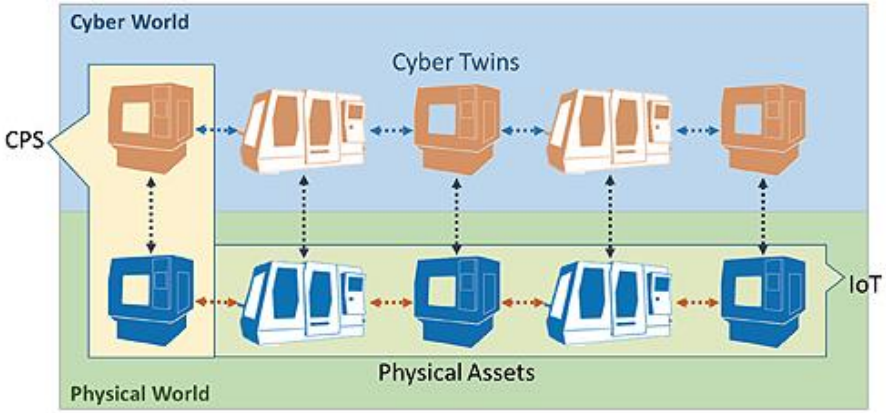


[출처] 융합의 또 다른 이름,
사이버 물리 시스템, 손상혁, 2016

사이버-피지컬 시스템의 예

- 스마트 그리드
  - 효율적인 에너지 관리 및 제공
- 스마트 공장
  - 효율적인 유지보수 지원
  - 안전성 동작 지원
- 도로 교통 통제 시스템
  - 돌발상황 감지 및 교통량 제어

[출처] 융합의 또 다른 이름, 사이버 물리 시스템, 손상혁, 2016



[출처] A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems - Jay Lee, Behrad Bagheri, Hung-An Kao

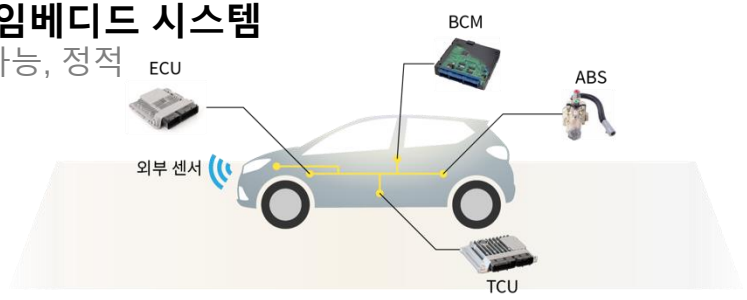
기존 임베디드 시스템과 차이점

기존 임베디드 vs. 사이버-피지컬 시스템

- **기존 임베디드 시스템:**
  - 사용자 및 이벤트에 의해 정해진 동작을 수행하는 **단순 제어 시스템**
  - 시스템들은 실시간 처리, 소형화, 저전력 운용, 저비용을 특징으로 하며 다른 **시스템과의 상호작용 없이 특정 목적을 달성하기 위해 독자적으로 동작**
  - 사용자 요구에 따라 동작하기 때문에 **단방향이고 폐쇄적인 물리 시스템 (+중앙 집중형)**
  - **시스템의 상황 변화를 고려하지 않음**
  - 물리 시스템은 **환경, 시간 및 인간과의 상호작용**에 따라 시스템의 상태가 변화하게 되는데 임베디드 시스템의 경우 이런 요인들에 따른 결과에 대해 **종합적인 고려 없이 주어진 기능만을 수행**

단일 임베디드 시스템
중앙 집중, 정적

복합 임베디드 시스템
예측 가능, 정적



기존 임베디드 시스템과 차이점

기존 임베디드 vs. 사이버-피지컬 시스템

- **사이버-피지컬 시스템:**
  - **시스템의 상태를 인지하여 필요한 동작을 수행하는 시스템**
  - 물리 세계 정보를 습득, 가공, 계산, 분석하여 그 결과를 엑츄에이터를 통해 물리 세계에 적용, 사이버 세계와 스마트 오브젝트, 인간, 운영 환경을 포함하는 **물리 세계의 긴밀한 상호작용**을 위한 실시간 자율제어 시스템
  - CPS는 **물리 세계에서 발생하는 변화를 감지**할 수 있는 다양한 센서를 통해 환경 인지 기능을 수행

사이버-피지컬 시스템

예측 불가능, 이종 장치, 동적

해결 해야 될 문제		
다양성	**복잡성**	**가변성**
다양한 사이버, 현실 공간의 SW 체계 연동 문제	초연결, 분산 환경에서의 CPS SW 복잡성 문제	사이버, 현실 공간 SW 체계의 가용성과 QoS 변화 대응 문제
필요한 것: 안전성 확보		

안전성 분석

안전성 분석

- **안전 필수 시스템(Safety-Critical System)**
  - 시스템의 오동작, 설계 미흡 등 문제가 발생할 경우 인명 피해나 막대한 재산 손실, 환경 파괴와 같은 중대 손실을 미칠 수 있는 시스템

- **안전(Safety)**
  - 사고를 유발할 수 있는 **위험(Hazard)으로부터 자유로운 상태** (IEEE 1228:1994)
  - 수용할 수 없는 리스크로부터 자유로운 상태 (IEC 61508)

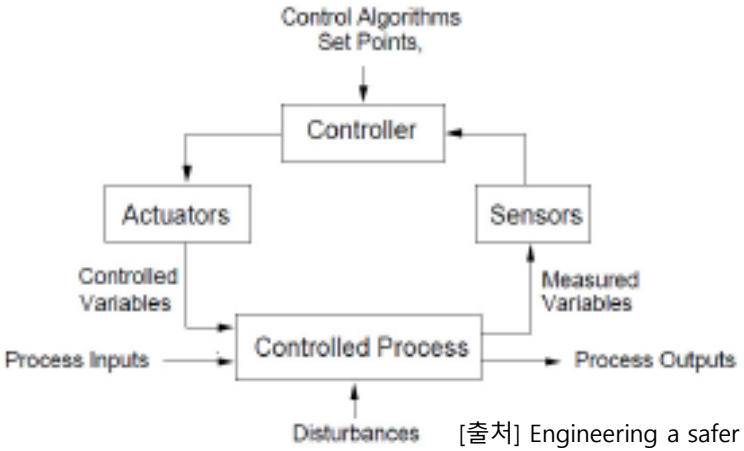
- **안전성 확보**
  - Safety-Critical System을 안전한 상태로 유지하기 위해서는 시스템에 **잠재된 위험을 개발단계부터 미리 식별하고 관리**하는 노력이 필요

STPA

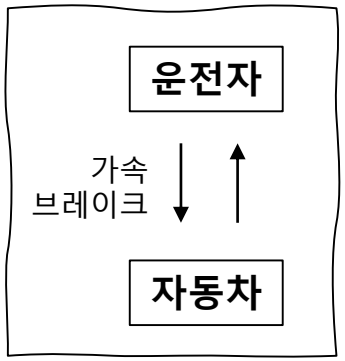
STPA (Systems Theoretic Process Analysis)

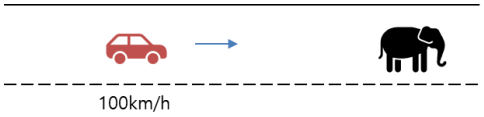
- STPA: Systems Theoretic Process Analysis, Nancy G. Leveson, 2012

- 개념: 시스템의 사고를 특정 컴포넌트의 실패 보다는 시스템 또는 컴포넌트 간 제어 문제 (Control Problem)로 접근
  - 부적절한 제어에 의해 시스템 위험이 발생하지 않도록,
    Unsafe Control Action을 식별하고
    Unsafe Control Action의 원인을 분석,
    발생을 방지하기 위한 안전 제약사항을 도출하는 활동으로 구성



[출처] Engineering a safer world, Nancy G, Leveson, 2011





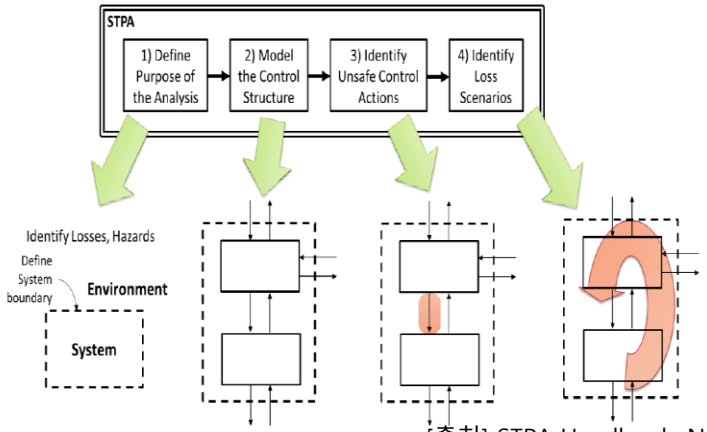
가속
When 전방에 장애물이 있을 경우

감속(브레이크)을 하지 않음
When 전방에 장애물이 있을 경우

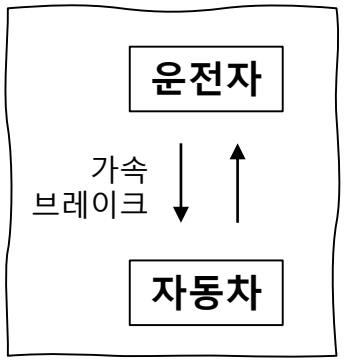
STPA

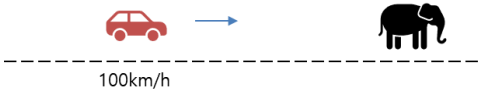
STPA의 4단계

- **1) Define Purpose of the Analysis:**
  - Losses와 System-level hazards, system-level constraints를 식별한다
- **2) Model the Control Structure 작성**
  - 시스템을 컨트롤러와 컨트롤, 피드백을 중심으로 추상화 및 재구성
- **3) Identify Unsafe Control Actions:**
  - 4가지 유형에 따른 Unsafe Control Action을 도출
- **4) Identify Loss Scenarios:**
  - 3에서 식별된 Unsafe Control Action의 발생 원인을 도출



[출처] STPA Handbook, Nancy G, Leveson, 2018





가속
When 전방에 장애물이 있을 경우
Why? 페달을 잘못 밟음
Why? 전방 시야 확보 실패 (안개)
Why? 잘못된 속도 정보 제공
감속(브레이크)을 하지 않음
When 전방에 장애물이 있을 경우

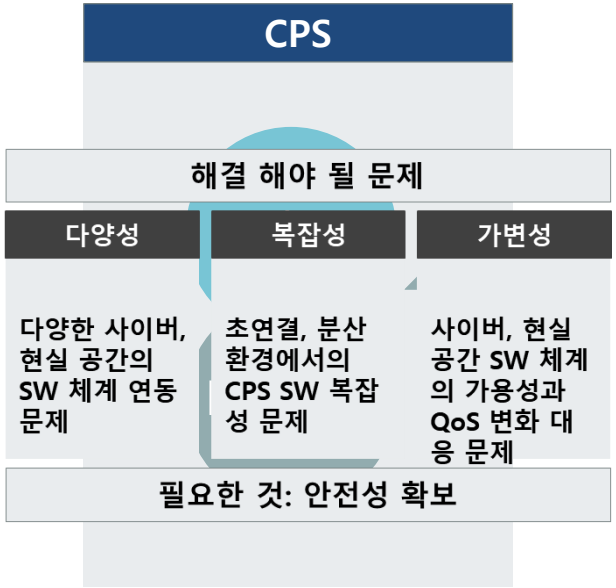
군집 운행 시스템에 STPA 적용

본론

STPA를 이용한 군집 운행 시스템의 안전성 분석 사례 연구

- RQ: 시스템의 구성 요소가 동적으로 조합이 되는 CPS (Cyber-Physical) 에 기존 안전성 분석 기법(STPA)의 적용에 **어려움**이 없을까?

- 타겟: **군집 운행 시스템 (Platoon system)**
- 분석 방법: **STPA (Systems Theoretic Process Analysis)**



+

STPA

안전성 분석

적용 가능성
- 적용이 잘 될까?

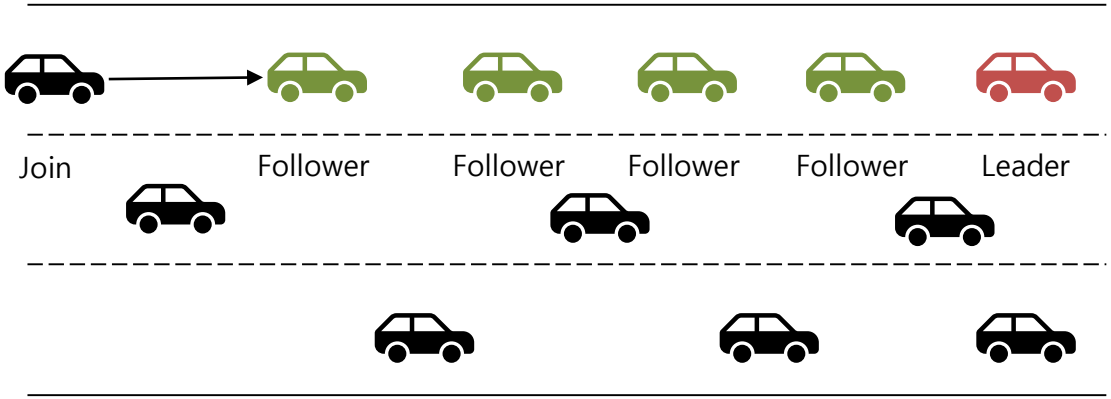
문제 식별
- 적용이 어렵다면 무엇이 문제일까?

해결 방법
- 어떻게 해결 할 수 있을까?

군집 운행 시스템

군집 운행 시스템

- **의미**: 두 대 이상의 차량이 일정한 차량 간격을 유지하며 하나의 그룹을 이루어 주행하는 시스템
  - 차량 간 통신 커뮤니케이션의 발전과 자율주행 기술의 발전
- 이점:
  - 앞차와의 거리를 줄여 공기저항을 줄여 연비 개선을 도모
  - 자율운전으로 인해 운전자의 피로도를 줄임
  - 졸음 및 부주의한 운전으로부터 생길 수 있는 사고를 미연에 방지

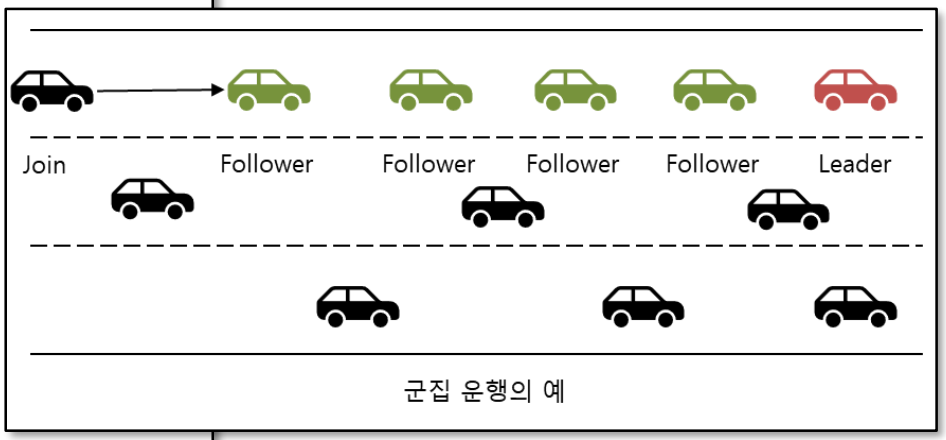


군집 운행의 예

군집 운행 시스템

군집 운행 시스템의 기능

1. **A. Join (차량 합류)**
    1. 그룹의 마지막에 합류
    2. 그룹의 중간에 합류
2. **Leave (차량 이탈)**
    1. 마지막 Follower 차량의 이탈
    2. 중간 Follower 차량의 이탈
    3. Leader의 이탈
3. **Merge (군집 통합)**
4. **Split (군집 분할)**
5. **군집 주행 제어 기능**
    1. 군집의 가속 및 감속 제어
    2. 군집의 차선 변경 제어
6. **자율 주행 제어 기능**
    1. 차간거리를 유지
    2. 차선 유지
7. **돌발 상황 제어 기능**
    1. Non-member 차량의 cui-in/off 대처 기능
    2. 돌방상황 전파 및 군집 내 일부 차량 제어 기능
    3. 도로 인프라로부터 돌발상황 대처 기능

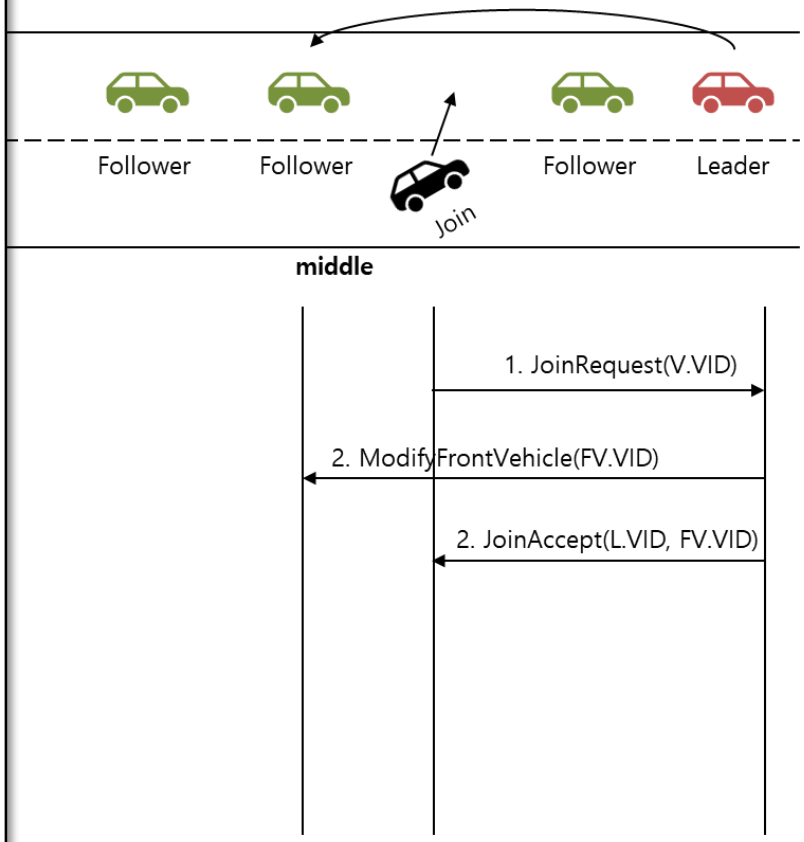


군집 운행의 예

군집 운행 시스템

Join (차량 합류) 기능

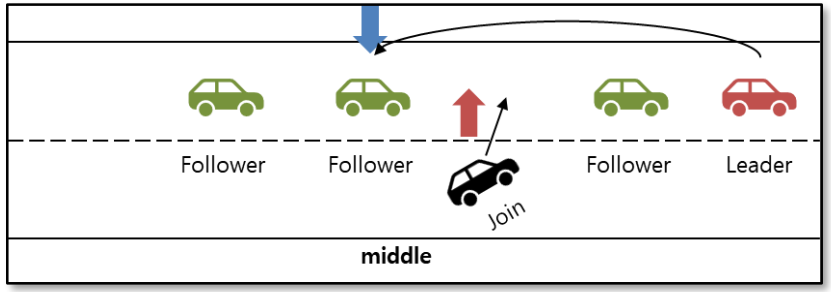
- **Non-member vehicle은 platoon 그룹의 중간 및 마지막에 합류 가능함**
- **그룹의 중간에 합류**
- Non-member 차량이 leader에게 join 허락 메시지 전송
- **Leader는 join 차량의 후행 차량에게 '차간거리 늘림' 제어 명령 전송**
- join 차량의 후행 차량이 충분한 차간거리를 확보하였다면, leader에게 차간거리 확보 메시지 전송
- Leader는 join 차량에게 합류 허락 메시지 전송
- Join 차량은 차선 이동을 통해 그룹에 합류 후 합류 완료 메시지를 leader에게 전송
- Join 차량은 선행 차량과 연결을 맺음 (정보 송수신)
- Join 차량의 후행은 join 차량과 연결을 맺음 (정보 송수신)
- Join 차량은 운전자 모드에서 자율주행 모드로 전환

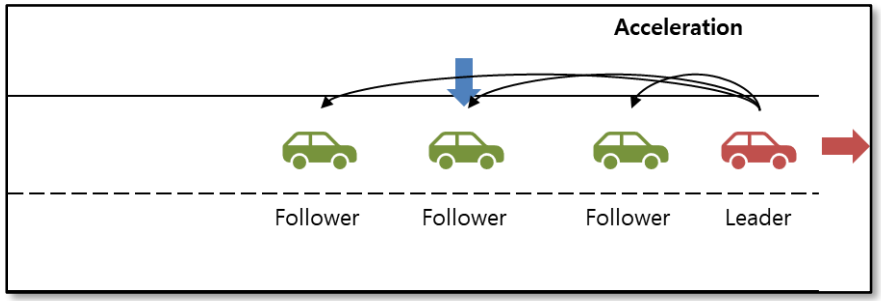


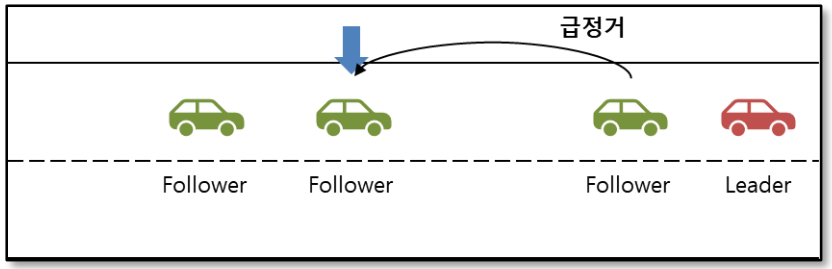
Join (차량 합류) 기능

군집 운행 시스템

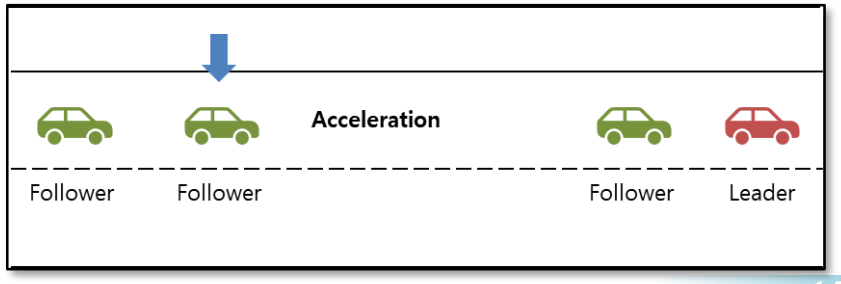
- **Join**
  - 그룹의 중간에 합류
  - Leader는 join 차량의 후행 차량에게 '차간거리 늘림' 명령 전송
- **Platoon control**
  - Leader의 가감속을 바탕으로 platoon 그룹을 제어
- **돌발상황 제어**
  - 급정거시 후행 차량에게 급정거
- **군집 통합/분리**





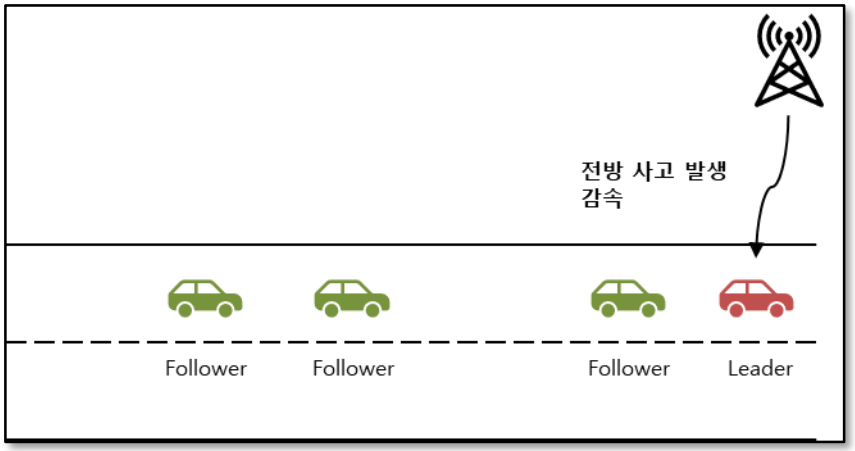


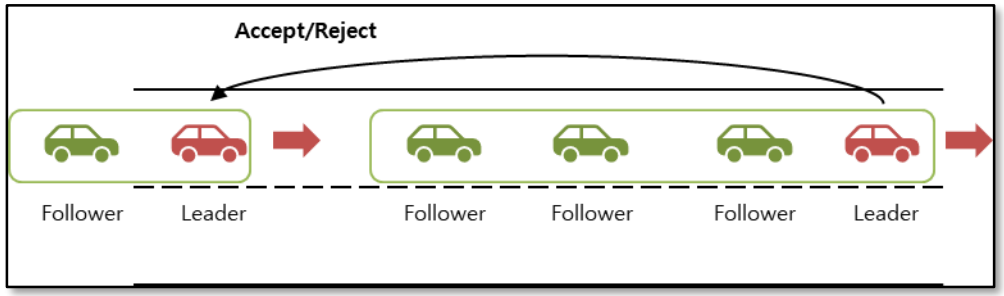
- **Cruise control**
  - 차간거리가 멀 경우 가속을 통해 차간거리 유지
- **운전자 제어**
  - 자율운행 중 운전자의 명령은 우선순위로 수행
- **도로 인프라로부터 돌발 제어**



군집 운행 시스템

- **Join**
  - 그룹의 중간에 합류
  - Leader는 join 차량의 후행 차량에게 '차간거리 늘림' 명령 전송
- **Platoon control**
  - Leader의 가감속을 바탕으로 platoon 그룹을 제어
- **돌발상황 제어**
  - 급정거시 후행 차량에게 급정거
- **군집 통합/분리**





- **Cruise control**
  - 차간거리가 멀 경우 가속을 통해 차간거리 유지
- **운전자 제어**
  - 자율운행 중 운전자의 명령은 우선순위로 수행
- **도로 인프라로부터 돌발 제어**

STPA 적용

Step 1) Define Purpose of the Analysis:
- Losses와 System-level hazards, system-level constraints를 식별한다

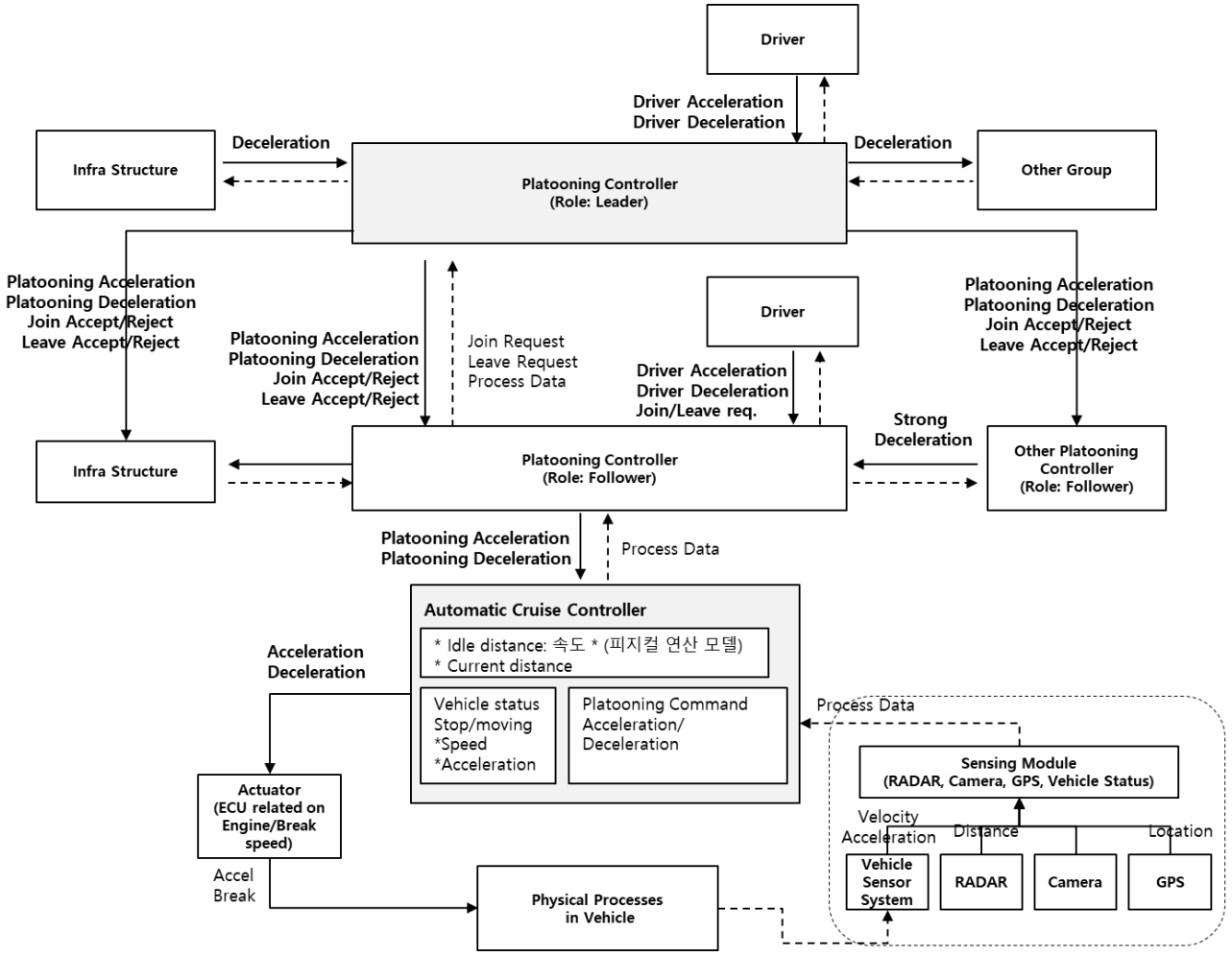
- **Accident 1: 자동차 전방 추돌 사고 (안전거리 미확보)**
  - **Hazard 1: 전방 차량과의 거리가 일정 수준 이하일 경우**
  - Hazard 2: 적절하지 않은 급 감속
  - Hazard 3: 적절하지 않은 급 가속

- Accident 2: 자동차 측면 추돌 (차로 위반)
  - Hazard 4: 측면 인프라와의 거리가 일정 수준 이하일 경우
  - Hazard 5: 측면 차량과의 거리가 일정 수준 이하일 경우
  - Hazard 6: 절절하지 않은 차선 변경 및 이탈
  - Hazard 7: 곡선 및 분기점에서의 동작 고려 無

- Accident 3: 시스템 목적 달성 실패
  - Hazard 8: Platooning 유지 실패 (효율적인 운행 실패)
  - Hazard 9: 허가되지 않은 차량과의 Platooning 유지
  - Hazard 10: 시스템의 제어 실패

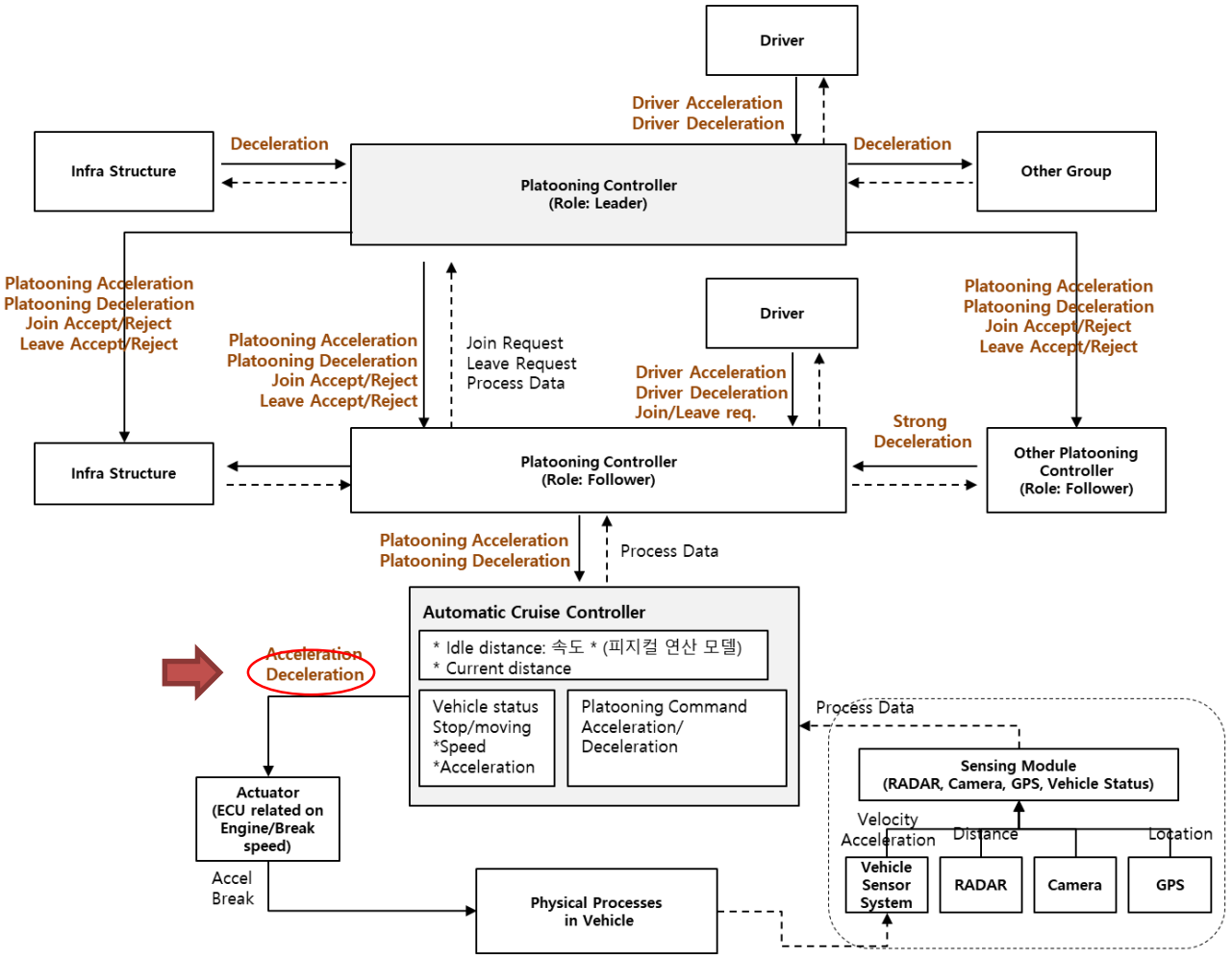
Control Structure

Step 2) Control Structure 작성
- 시스템을 컨트롤러와 컨트롤, 피드백을 중심으로 추상화 및 재구성



Control Structure

Step 3) Identify Unsafe Control Actions:
- 4가지 유형에 따른 Unsafe Control Action을 도출



Unsafe Control Actions

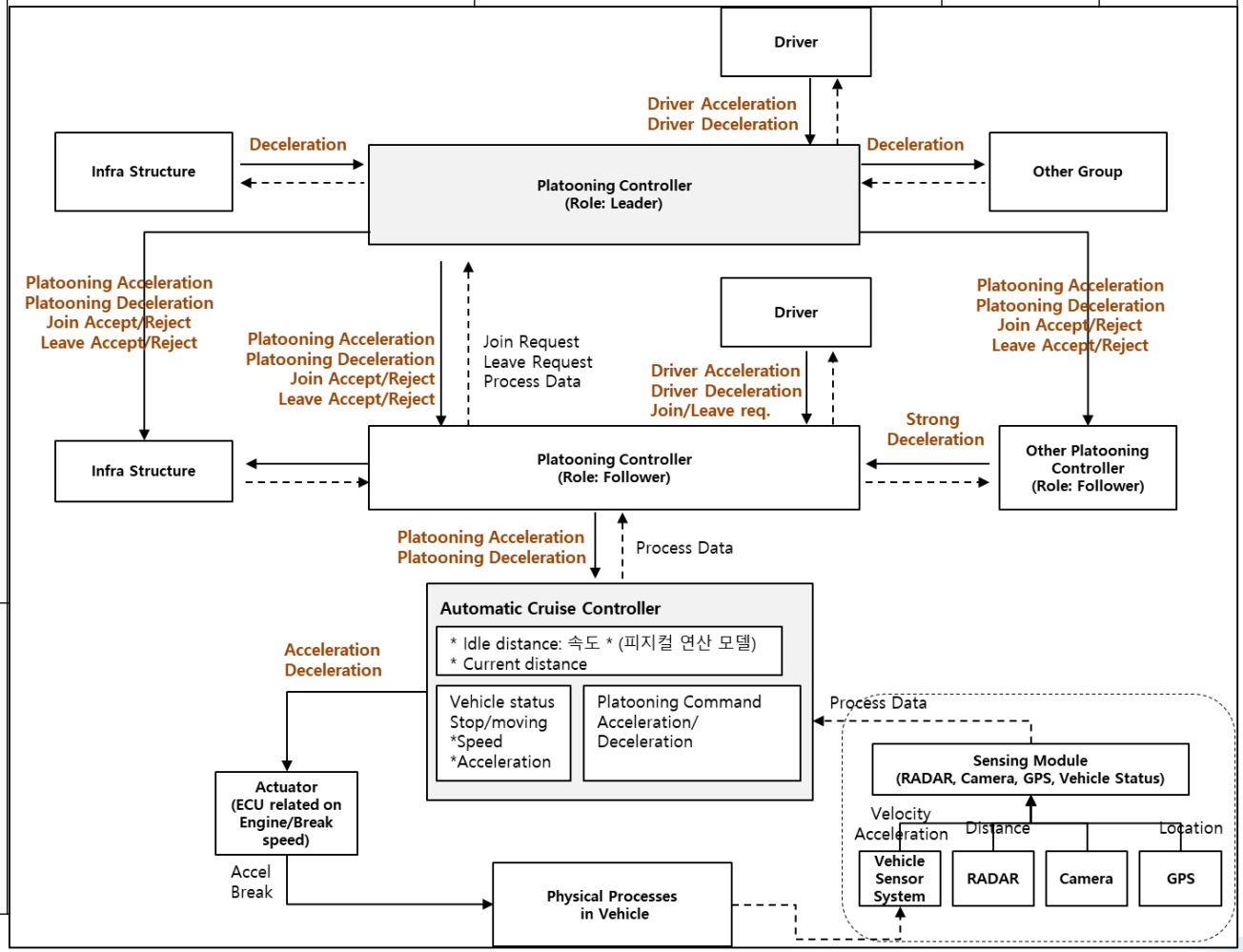
Unsafe Control Actions	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Deceleration ACC → ECU	Adaptative Cruise Controller가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** Deceleration을 제공하지 않음. [H1] Adaptative Cruise Controller가 **전방 차량이 급감속 중일 때,** Deceleration을 제공하지 않음. [H1] Adaptative Cruise Controller가 **전방 차량이 Join 중일 때,** Deceleration을 제공하지 않음. [H1] Adaptative Cruise Controller가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** **전방 차량이 급감속 중일 때,** **전방 차량이 Join 중일 때,** **리더는 군집 가속 중일 때** Deceleration을 제공하지 않음. [H1] • • •			
Acceleration				

Unsafe Control Actions

Unsafe Control Actions	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Deceleration **Leader → Follower** **Leader → other Leader** **Infrastructure → other Leader** **Front V → Back V** **Driver → Platoon System** **ACC → ECU** …	Platoon System (Follower) 가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** Deceleration을 제공하지 않음. [H1] Platoon System (Follower) 가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** **Driver가 Deceleration을 명령하였지만,** Deceleration가 제공되지 않음. [H3] Platoon System (Leader) 가 **Driver가 Deceleration을 명령하였지만,** Deceleration가 제공되지 않음. [H3] Platoon System (Front) 가 **돌발상황에서** Deceleration을 제공하지 않음. [H1]	Platoon System (Follower) 가 **후방 차량이 Join/Leave 중일 때** Deceleration을 제공함. [H1]		
Acceleration		Platoon System (Follower) 가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** Acceleration을 제공함. [H1] Platoon System (Follower) 가 **Driver가 Deceleration을 명령하였지만,** Acceleration을 제공함. [H3] Platoon System (Follower) 가 **후방 차량이 Join/Leave 중에** Acceleration**을 제공함** [H2] Platoon System (Leader) 가 **Join/Leave 중에 전방 차량에게** Acceleration을 제공하지 않음. [H2]		

Unsafe Control Actions

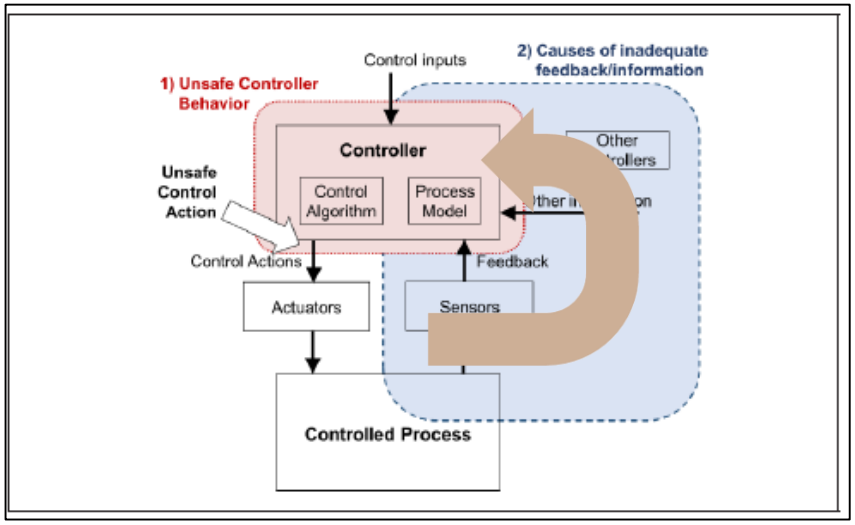
Unsafe Control Actions	Not providing causes hazard	Providing causes hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Deceleration **Leader → Follower** **Leader → other Leader** **Infrastructure → other Leader** **Front V → Back V** **Driver → Platoon System** **ACC → ECU** …				
Acceleration				

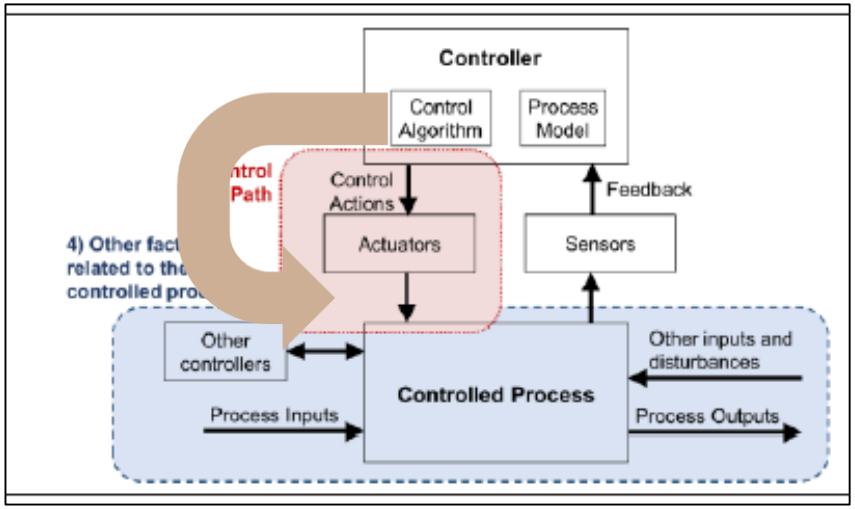


Loss Scenarios

Step 4) Identify Loss Scenarios:
- 3에서 식별된 Unsafe Control Action의 발생 원인을 도출

- **Unsafe Control Action:** ACC Controller 가
  앞차와의 거리가 Safe 차간거리보다 가까울 때,
  Deceleration을 제공하지 않음. [H1]

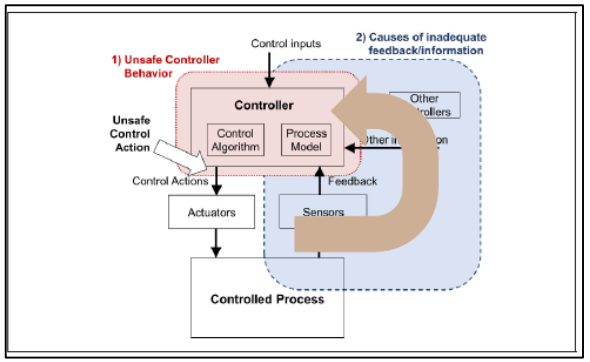




[출처] STPA Handbook, Nancy G, Leveson, 2018

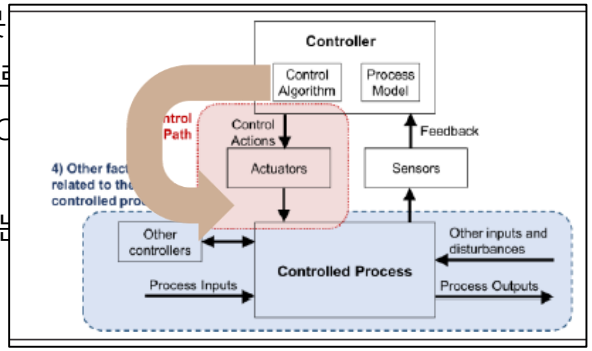
Loss Scenarios

- (1) UCA를 유발하는 시나리오 도출 (왜 UCA가 발생하는가?)
  - **1) Controller 자체에 존재하는 원인 (Unsafe Controller Behavior)**
    - 1) Controller Failure
    - 2) 잘못된 컨트롤 알고리즘
    - 3) 불안전한 상위 Controller의 제어
    - 4) 부적절한 Process Model
  - **2) 부적절한 피드백 또는 잘못된 정보**
    - 1) 피드백 또는 정보를 수신하지 못함
      - 센서가 송신한 피드백 또는 정보를 Controller에서 수신하지 못함
      - 센서가 상태 정보를 감지 하였으나 Controller로 송신하지 않음
      - 센서가 상태 정보를 감지하지 못함
      - 피드백 또는 정보 자체가 없거나 상태를 감지하는 센서가 없음
    - 2) 부적절한 피드백 또는 정보를 수신함
      - 센서가 적절하게 피드백 또는 정보를 수신하였으나 Controller가 잘못된 피드백 또는 잘못된 정보를 받음
      - 센서가 잘못된 피드백 또는 잘못된 정보를 송신함
      - 센서가 필요한 피드백 또는 정보를 송신하도록 설계되지 않음



Loss Scenarios

- (2) Control Action이 부적절 하게 수행 되거나 Control Action이 수행되지 않은 경우의 시나리오
  - **3) Control Path에서 발생 가능한 시나리오**
    - 1) Control Action이 수행되지 않음
      - Controller에서 Control Action을 송신하였으나 Actuator에서 수신하지 못함
      - Actuator에서 Control Action을 수신하였으나 Controlled Process로 송신하지 안음
      - Actuator에서 Control Action을 송신하였으나 Controlled Process에서 수신하지 못하거나 수신된 Control Action이 수행되지 않음
    - 2) Control Action이 잘못 수행됨
      - Controller에서 Control Action을 송신하였으나 Actuator에서 잘못
      - Actuator에서 Control Action을 수신하였으나 Controlled Process
      - Actuator에서 Control Action을 수신 후 정상적 응답을 하였으나 C Action이 적용되지 않거나 Controlled Process에서 잘못된 응답을
      - Controller에서 Control Action을 송신하지 않았으나, Actuator 또 Process로 응답함



  - **4) Controlled Process에서 발생 가능한 시나리오**
    - 1) Control Action이 수행되지 않음
      - Controlled Process가 Control Action을 수신하였으나 응답하지 않음
    - 2) Control Action이 잘못 수행됨
      - Controlled Process가 Control Action을 수신하였으나 잘못 응답함
      - Controlled process가 Control Action을 수신하지 않았으나 수신한 상황과 같이 응답함

CF ID #2	
Controller	Automatic Cruise Controller
Control Action	Automatic Cruise Controller → **Deceleration** → Vehicle
Unsafe Control Action	Automatic Cruise Controller가 앞차와의 거리가 Safe 차간거리보다 짧을 때, Deceleration을 제공하지 않는다. [H1]

1) Controller Failure
(물리적 기계적 오류 – 노후화, 전원 부족, 네트워크 장치 부식 등)

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
Controller를 포함하는 Platooning 시스템의
물리적 오류로 (과전류)
Deceleration을 제공하지 않음

2) 잘못된 컨트롤 알고리즘
(알고리즘 구현상의 결함 or 시간에 따른 성능저하)

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
Safe 차간거리를 계산하는 알고리즘의 오류로 차간거리가 충분한 것으로 해석,
Deceleration을 제공하지 않음

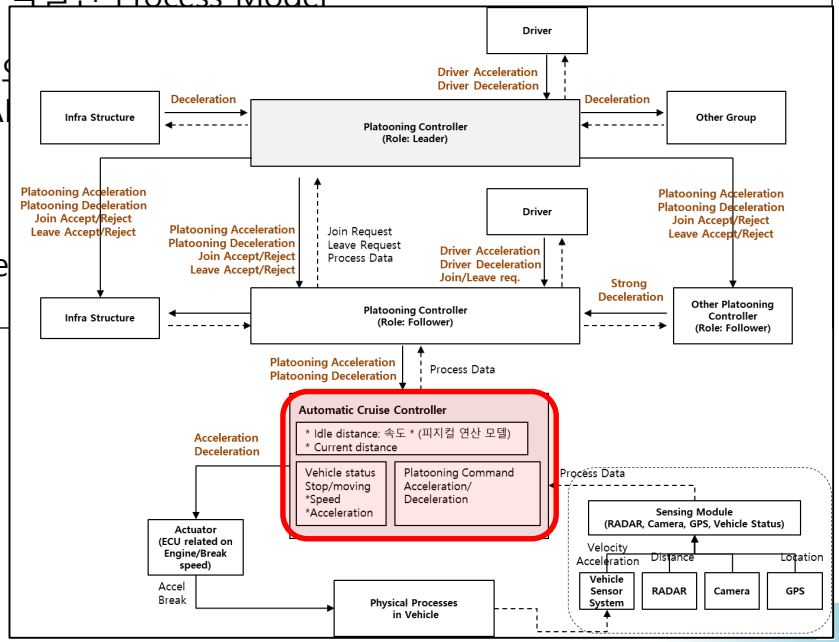
3) 불안전한 상위 Controller의 제어

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
Manual command (Acceleration)가 있음에도 Platoon controller가 감속을 제공하지 않음
Deceleration을 제공하지 않음

4) 부적절한 Process Model

앞차
LIDA
해당
함

Dece



CF ID #2	
Controller	Automatic Cruise Controller
Control Action	Automatic Cruise Controller → **Deceleration** → Vehicle
Unsafe Control Action	Automatic Cruise Controller가 앞차와의 거리가 Safe 차간거리보다 짧을 때, Deceleration을 제공하지 않는다. [H1]

1) 피드백 또는 정보를 수신하지 못함
- 센서가 송신한 피드백 또는 정보를 Controller에서 수신하지 못함

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
LIDAR 센서의 정보가 CAN 통신 지연으로 인해,
정확한 시간에 controller가 이를 수신하지 못하여,
Safe 차간거리에 대한 판단을 내리지 못함
Deceleration을 제공하지 않음

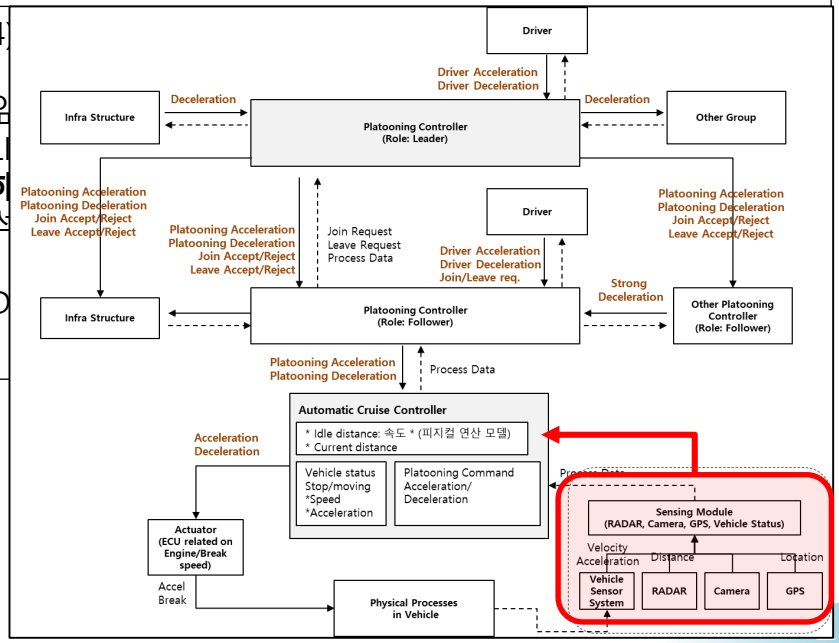
2) 피드백 또는 정보를 수신하지 못함
- 센서가 상태 정보를 감지하지 못함

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
LIDAR 센서가 환경적 영향 (복잡한 환경)
반향파가 센서로 직진하지 않고, 주변의 다른 벽면을 여러 번 반사되어(2차 3차 반사) 정확한 센싱을 수행하지 못함
Safe 차간거리가 충분한 것으로 잘못 판단 내림
Deceleration을 제공하지 않음

1) 피드백 또는 정보를 수신하지 못함
- 센서가 상태 정보를 감지하지 못함

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
LIDAR 센서가 Cut In 차량에 대한 센싱 실패
정확한 센싱을 수행하지 못함
Safe 차간거리가 충분한 것으로 잘못 판단 내림
Deceleration을 제공하지 않음

4)



CF ID #2	
Controller	Automatic Cruise Controller
Control Action	Automatic Cruise Controller → **Deceleration** → Vehicle
Unsafe Control Action	Automatic Cruise Controller가 앞차와의 거리가 Safe 차간거리보다 짧을 때, Deceleration을 제공하지 않는다. [H1]

2) 부적절한 피드백 또는 정보를 수신함
- 센서가 적절하게 피드백 또는 정보를 수신하였으나 Controller가 잘못된 피드백 또는 잘못된 정보를 받음

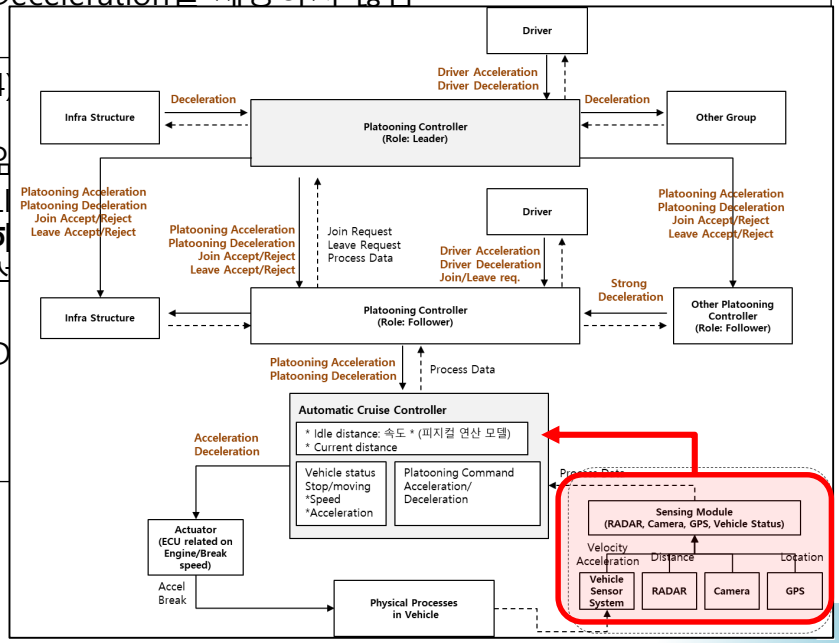
앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
LIDAR 센서의 정보가 CAN의 과부화에 따른 통신 오류로 인해,
정확한 센싱값을 수신하지 못함
Safe 차간거리가 충분한 것으로 잘못 판단 내림
Deceleration을 제공하지 않음

2) 부적절한 피드백 또는 정보를 수신함
- 센서가 적절하게 피드백 또는 정보를 수신하였으나 Controller가 잘못된 피드백 또는 잘못된 정보를 받음

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
LIDAR 센서의 정보가 CAN의 보안 공격으로 인해
정확한 센싱값을 수신하지 못함
Safe 차간거리가 충분한 것으로 잘못 판단 내림
Deceleration을 제공하지 않음

2) 부적절한 피드백 또는 정보를 수신함
- 센서가 잘못된 피드백 또는 잘못된 정보를 송신함

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
차량의 전력 부족 및 LIDAR 센서의 정보가 전력 부족(저전압)으로 인해,
센싱값이 변조되어 송신됨.
Safe 차간거리가 충분한 것으로 잘못 판단 내림
Deceleration을 제공하지 않음



CF ID #2	
Controller	Automatic Cruise Controller
Control Action	Automatic Cruise Controller → **Deceleration** → Vehicle
Unsafe Control Action	Automatic Cruise Controller가 앞차와의 거리가 Safe 차간거리보다 짧을 때, Deceleration을 제공하지 않는다. [H1]

1) Control Action이 수행되지 않음
- Controller에서 Control Action을 송신하였으나 Actuator에서 수신하지 못함

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
Controller가 control을 송신 하였으나
Actuator 내부 오류로 수신하지 못하여
Deceleration을 수행하지 않음

1) Control Action이 수행되지 않음
- Actuator에서 Control Action을 수신하였으나 Controlled Process로 송신하지 않음

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
Controller가 control을 송신 하였고, Actuator 수신 하였으나,
Actuator의 파워 부족으로 실제 장치에 명령이 전달 되지 않음
Deceleration을 수행하지 않음

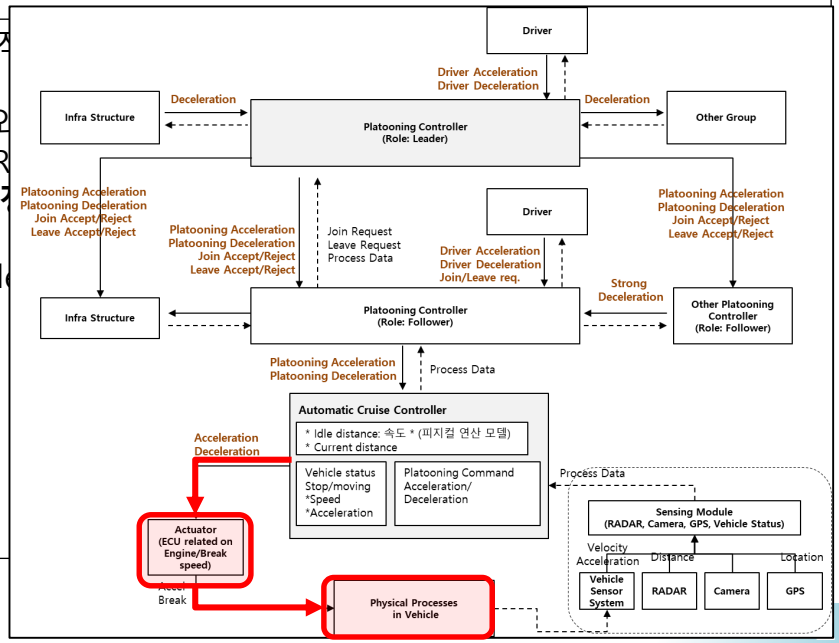
2) Control Action이 잘못 수행됨
- Actuator에서 Control Action을 수신하였으나 Controlled Process로 잘못된 응답을 송신함

앞차와의 차간거리가 Safe 차간거리보다 짧을 때,
Controller가 Deceleration을 송신 하였고, Actuator가 이를 잘 수신하였으나,
CAN 통신 오류(노이즈, 병목 현상, 신호 간섭)로 & 보안 공격 & 전력 부족 등으로 인해
Actuator 가 Acceleration을 수신 함
Deceleration을 수행하지 않음 & Acceleration을 수행함

4) 부

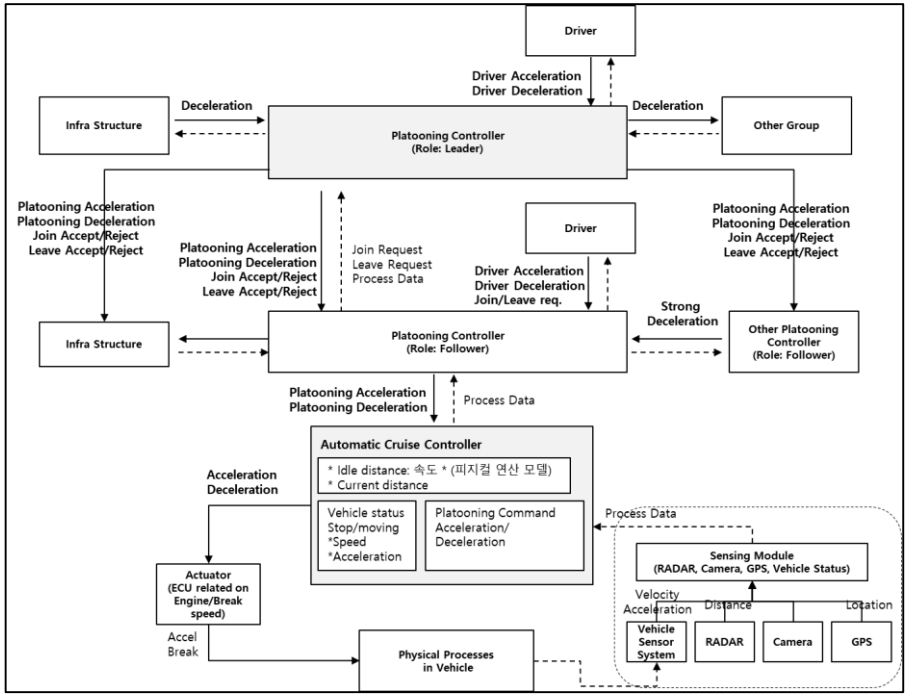
앞차와
LIDAR
해당

Decel



고찰

1) Control Structure의 불확실성 (Dynamic Uncertainty)



Unsafe Control Actions	Not providing causes hazard	Providing causes hazard	Too too out sequ
Deceleration ACC → ECU	Platoon System (Follower) 가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** Deceleration을 제공하지 않음. [H1] Platoon System (Follower) 가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** **전방 차량이 급감속 중일 때,** Deceleration을 제공하지 않음. [H1] Platoon System (Follower) 가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** **전방 차량이 Join 중일 때,** Deceleration을 제공하지 않음. [H1] Platoon System (Follower) 가 **앞차와의 거리가 Safe 차간거리보다 가까울 때,** **전방 차량이 급감속 중일 때,** **전방 차량이 Join 중일 때,** **운전자가 감속 제어를 수행할 때,** Deceleration을 제공하지 않음. [H1] ...		
Acceleration			

해결 해야 될 문제

다양성	복잡성	가변성
다양한 사이버, 현실 공간의 SW 체계 연동 문제	초연결, 분산 환경에서의 CPS SW 복잡성 문제	사이버, 현실 공간 SW 체계의 가용성과 QoS 변화 대응 문제

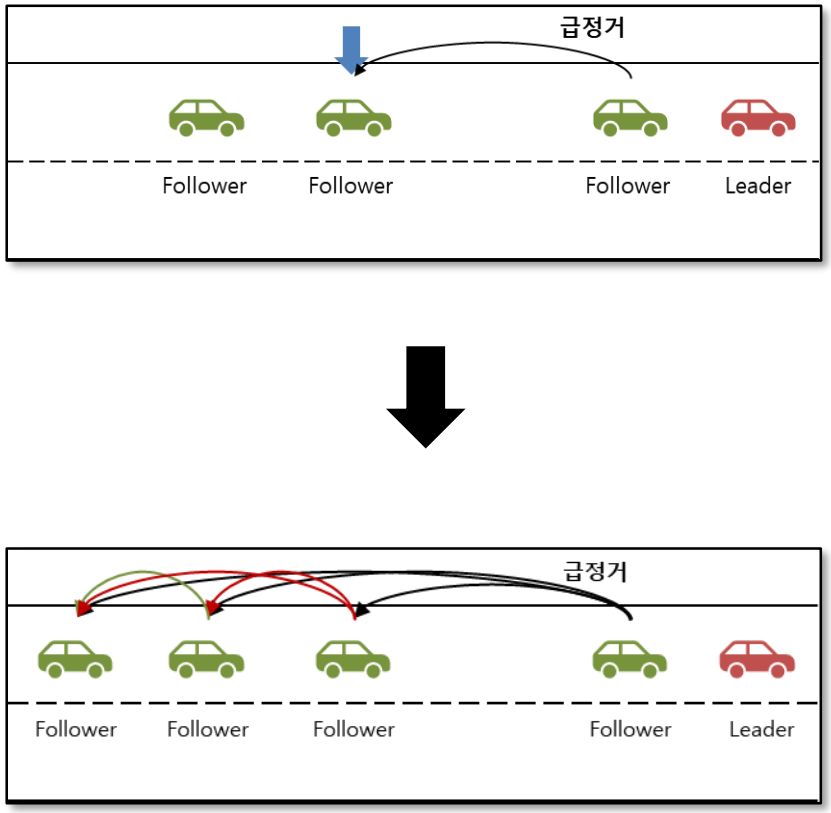
필요한 것: 안전성 확보

+ **STPA**

안전성 분석

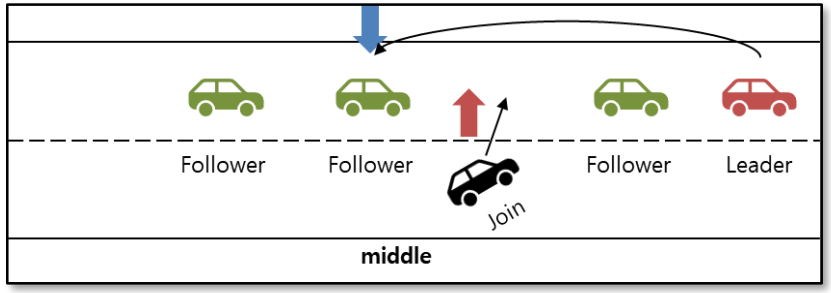
군집 운행 시스템

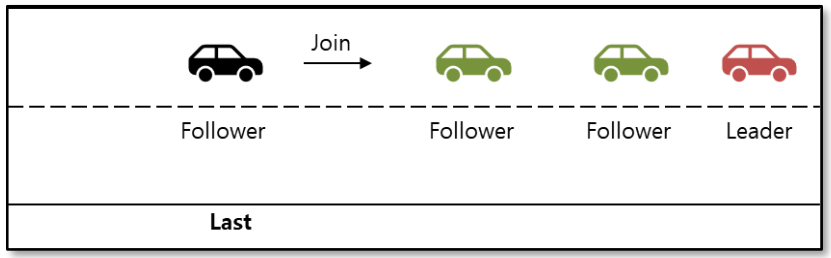
- Join
  - 그룹의 중간에 합류
  - Leader는 join 차량의 후행 차량에게 '차간거리 늘림' 명령 전송
- Platoon control
  - Leader의 가감속을 바탕으로 platoon 그룹을 제어
- **돌발상황 제어**
  - **급정거시 후행 모든 차량에게 급정거 지시**
- 군집 통합/분리
- Cruise control
  - 차간거리가 멀 경우 가속을 통해 차간거리 유지
- 운전자 제어
  - 자율운행 중 운전자의 명령은 우선순위로 수행
- 도로 인프라로부터 돌발 제어



군집 운행 시스템

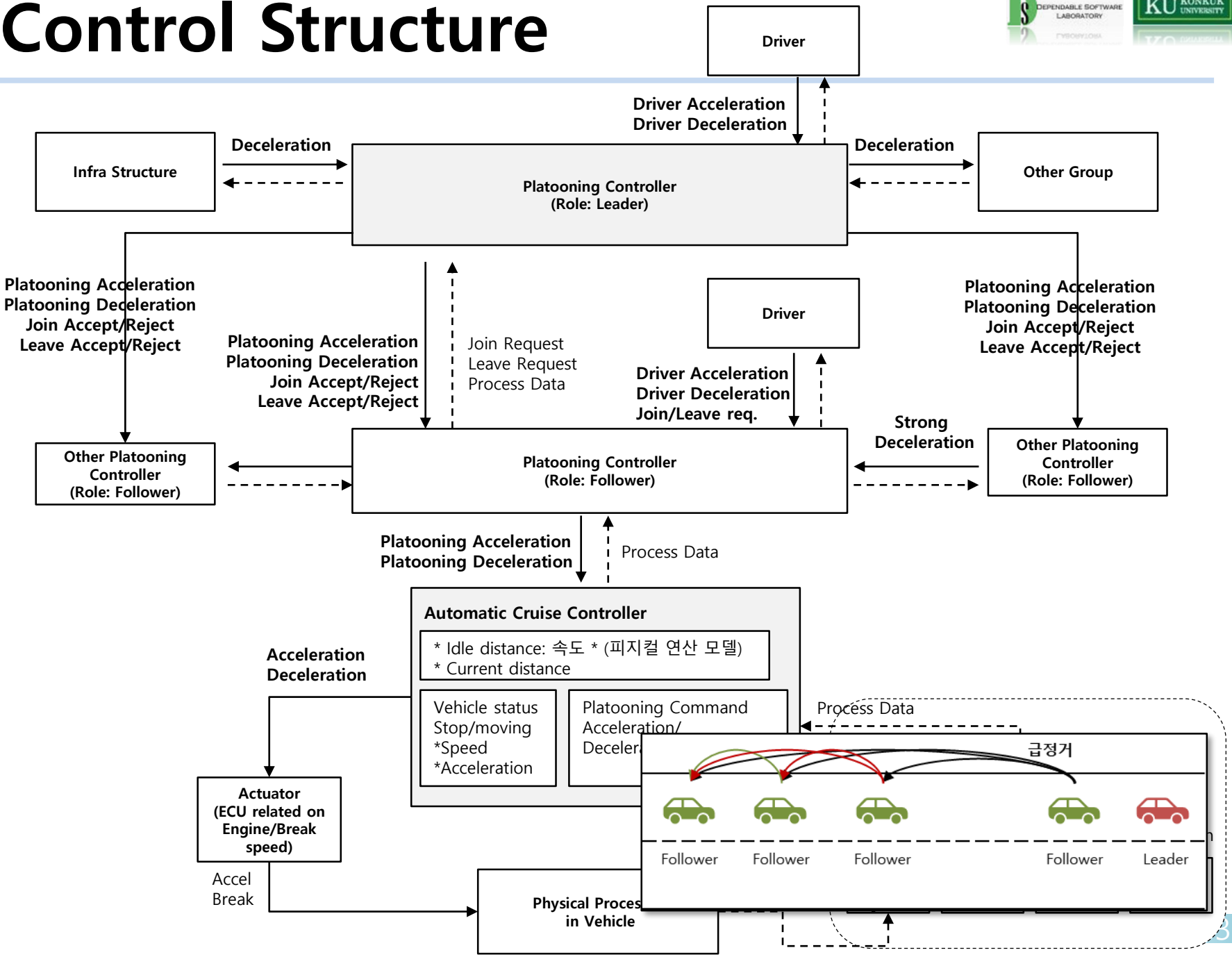
- **Join**
  - **그룹의 중간에 합류**
  - **Leader는 join 차량의 후행 차량에게 '차간거리 늘림' 명령 전송**
- Platoon control
  - Leader의 가감속을 바탕으로 platoon 그룹을 제어
- 돌발상황 제어
  - 급정거시 후행 차량에게 급정거
- 군집 통합/분리



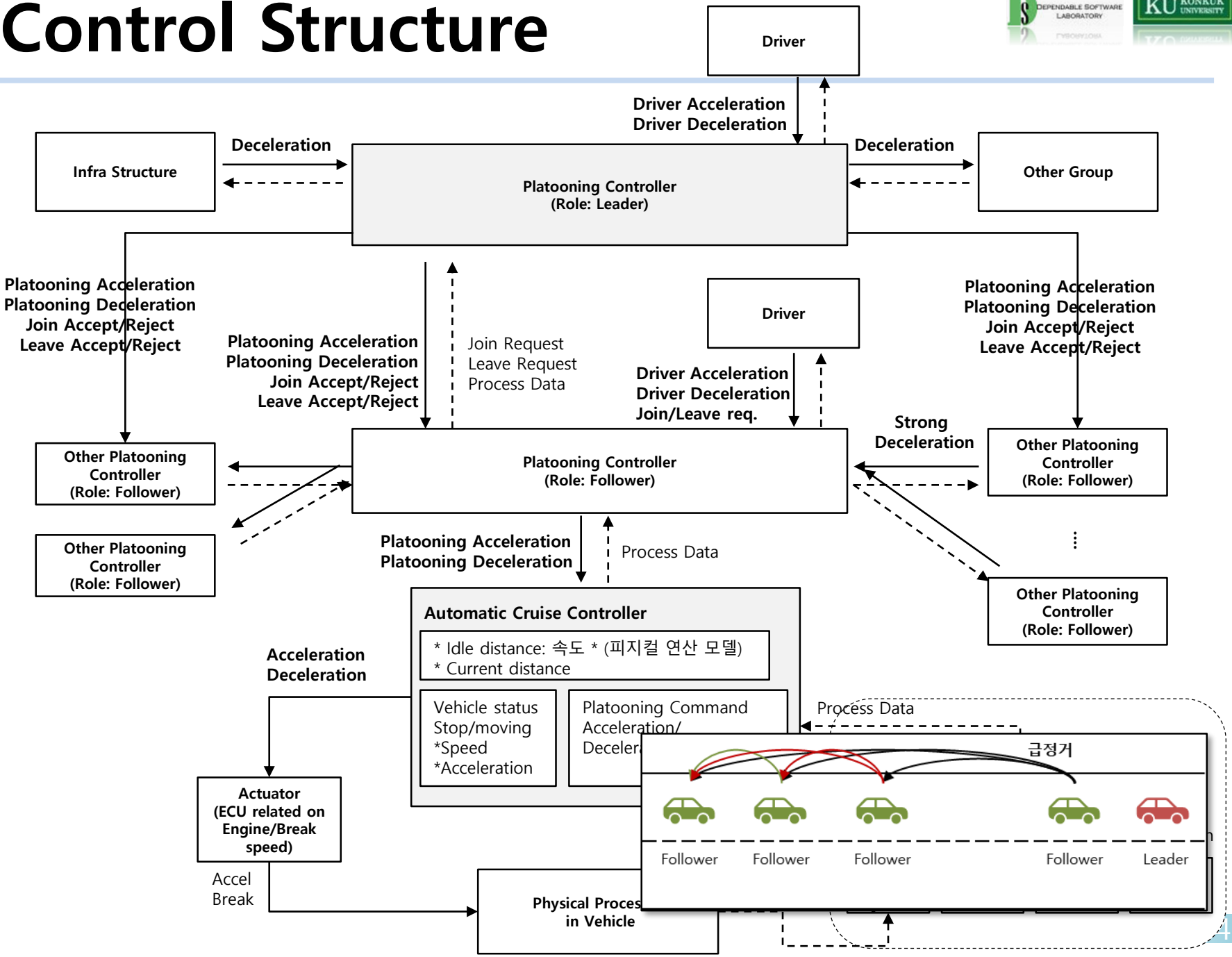


- Cruise control
  - 차간거리가 멀 경우 가속을 통해 차간거리 유지
- 운전자 제어
  - 자율운행 중 운전자의 명령은 우선순위로 수행
- 도로 인프라로부터 돌발 제어

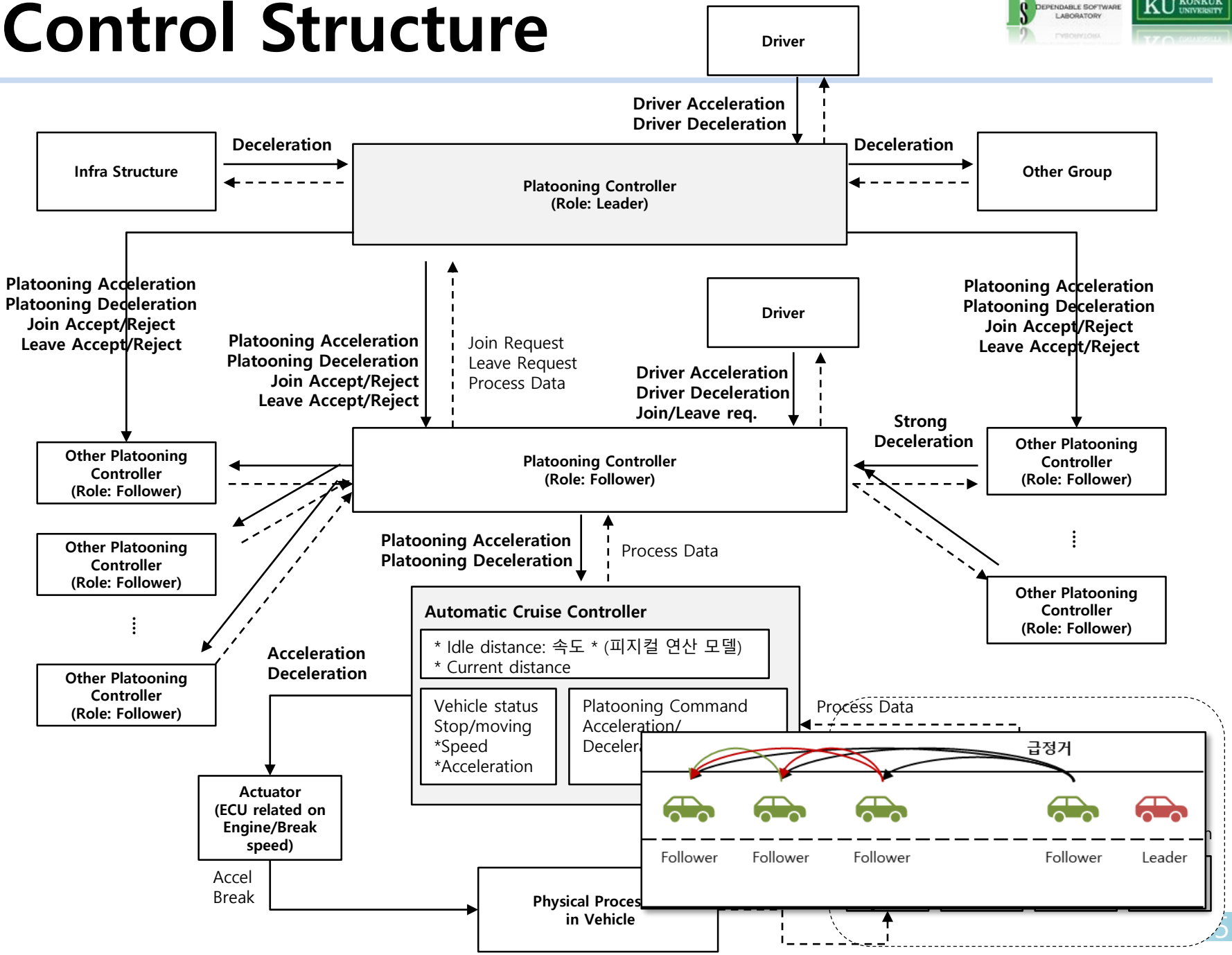
Control Structure



Control Structure



Control Structure



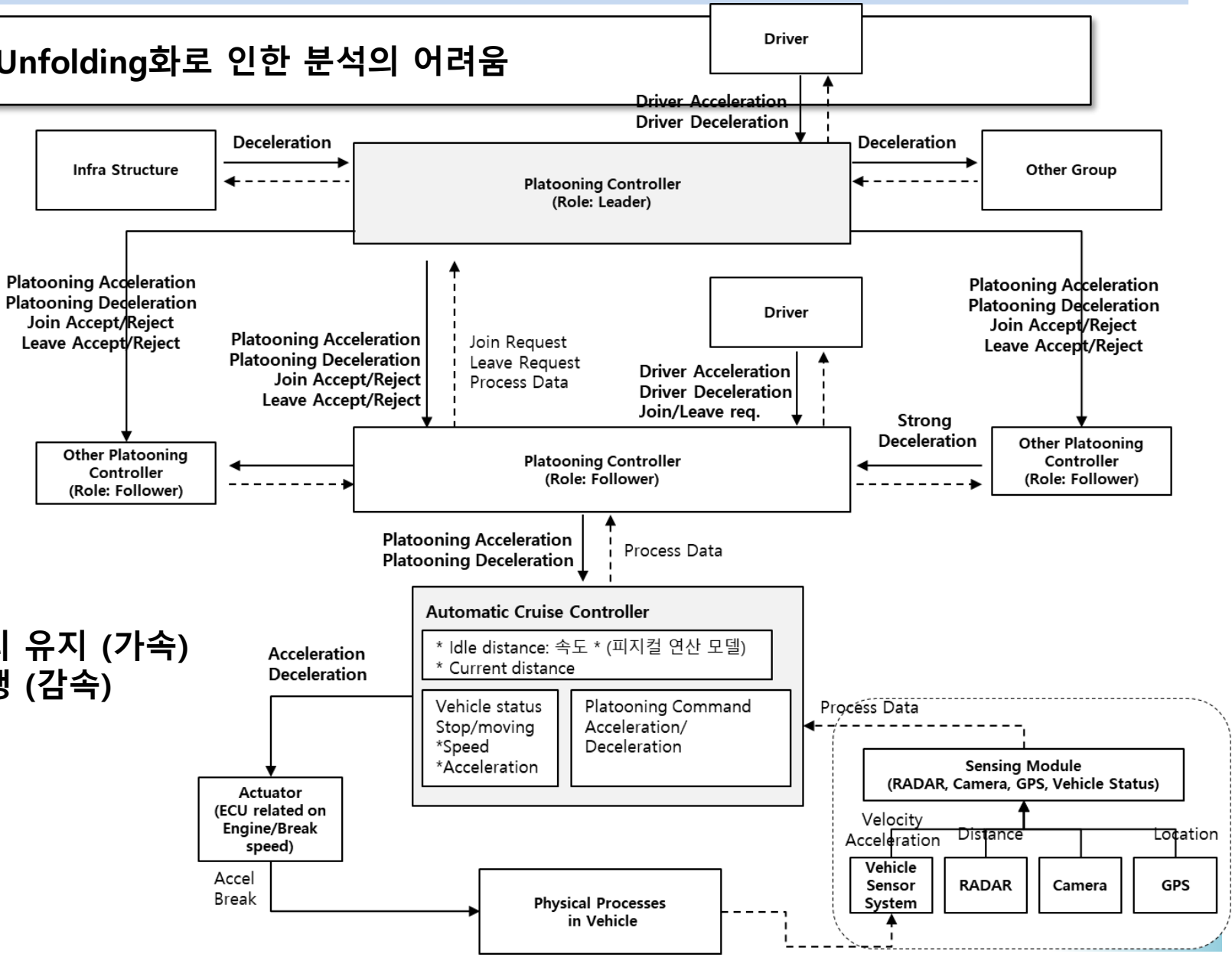
고찰

2) 정보의 Unfolding화로 인한 분석의 어려움

3대의 군집

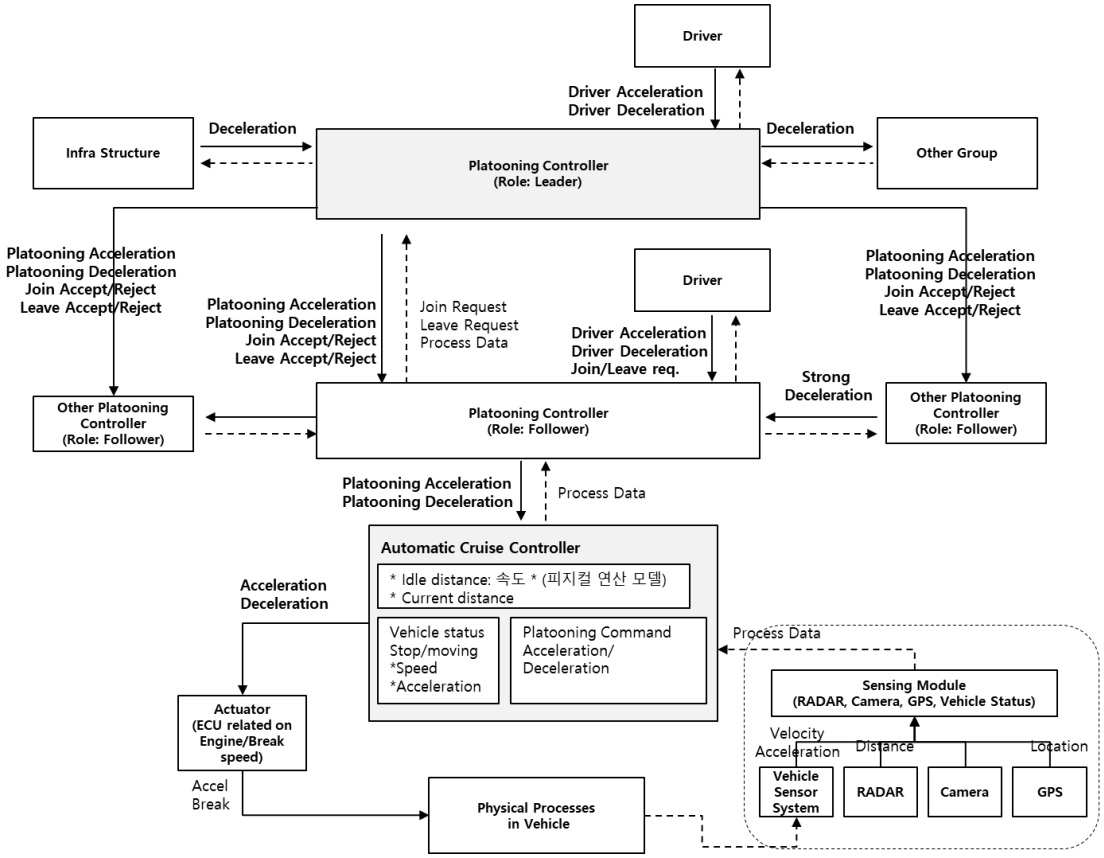
4대의 군집

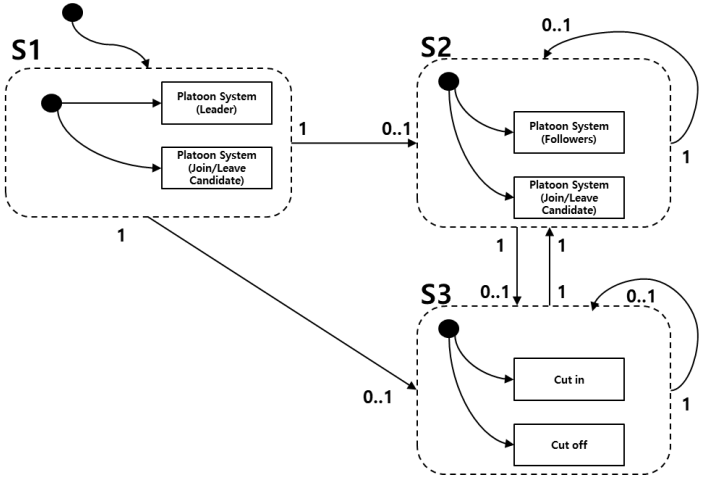
5대의 군집
리더: 가속
2번째: 급감속
3번째: Join
4번째: Leave
5번째: 차간거리 유지 (가속)
Infra: 사고 발생 (감속)



고찰

Unfolding 정보의 fording 방안

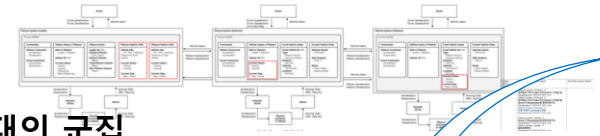




Path (Max path length = 5)						
S1						Scenario 1
S1	S2					Scenario 2
S1	S4					Scenario 3
S1	S2	S2	S2			Scenario 4
S1	S2	S4	S2	S2		...
...						...
S1	S3	S2				...
...						Scenario n

고찰

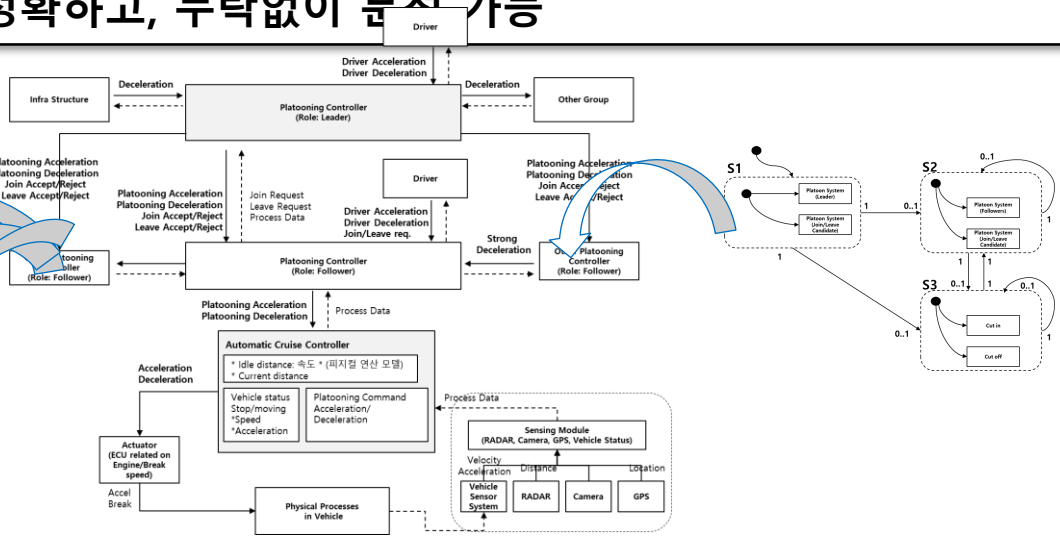
Unfolding 정보의 fording 방안
- 분석 수 증가,
- 보다 compact한 정보를 바탕으로 정확하고, 누락없이 분석 가능



3대의 군집
리더: 가속, 2번째: 급감속, 3번째: 차간거리 유지 (가속)

3대의 군집
리더: 가속, 2번째: Join, 3번째: 차간거리 유지 (가속)

4대의 군집
리더: 가속, 2번째: None, 3번째: Join, 4번째: Leave, 5번째: 차간거리 유지 (가속)
Infra: 사고 발생 (감속)



Path (Max path length = 5)						
S1						Scenario 1
S1	S2					Scenario 2
S1	S4					Scenario 3
S1	S2	S2	S2			Scenario 4
S1	S2	S4	S2	S2		...
...						...
S1	S3	S2				...
...						Scenario n

결론 및 향후 연구

STPA를 이용한 군집 운행 시스템(CPS)의 안전성 분석 수행

- 시스템의 구성 요소가 동적으로 조합이 되는 CPS (Cyber-Physical)에 기존 안전성 분석 기법(STPA)의 수행
- **타겟**: 군집 운행 시스템 (Platoon system)
- **분석 방법**: STPA (Systems Theoretic Process Analysis)
  - 적용 가능성
  - 문제 식별
    - Control Structure의 불확실성 (Dynamic Uncertainty)
    - Control Structure의 Unfolding화
  - 해결 방법 고찰

향후 연구

- Control Structure의 불확실성 (Dynamic Uncertainty) 해소를 위한 작성 방안
- Unfolding 정보의 fording 방안
  - 보다 compact한 정보를 바탕으로 정확하고, 누락없이 분석 가능

Q & A

감사합니다.

atang34@Konkuk.ac.kr
http://dslab.Konkuk.ac.krs