29th Asia-Pacific Software Engineering Conference
6 – 9 December 2022, Virtual

An approach for hazard analysis of multiple-cooperative systems considering dynamic configuration uncertainty

Sejin Jung*, Junbeom Yoo

Konkuk University

2022.12.08

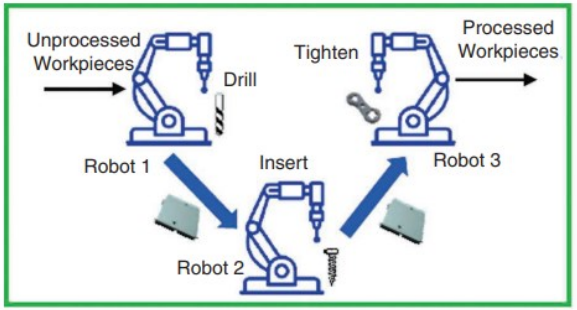
Dependable Software Laboratory
KU Konkuk University

Table of Contents

Introduction

- **Cooperative systems**
  - Operating with collaborations/cooperations between numerous heterogeneous systems to accomplish common goals of the system
  - Consisting of numerous heterogeneous cooperative dynamic constituents produced independently
    - In some cases, the system structures may appear as the constitution of multiple instances, and their collaborations at runtime

- **Safety hazard analysis** is importantly applied
  - These systems are often used to safety-related or safety-critical systems

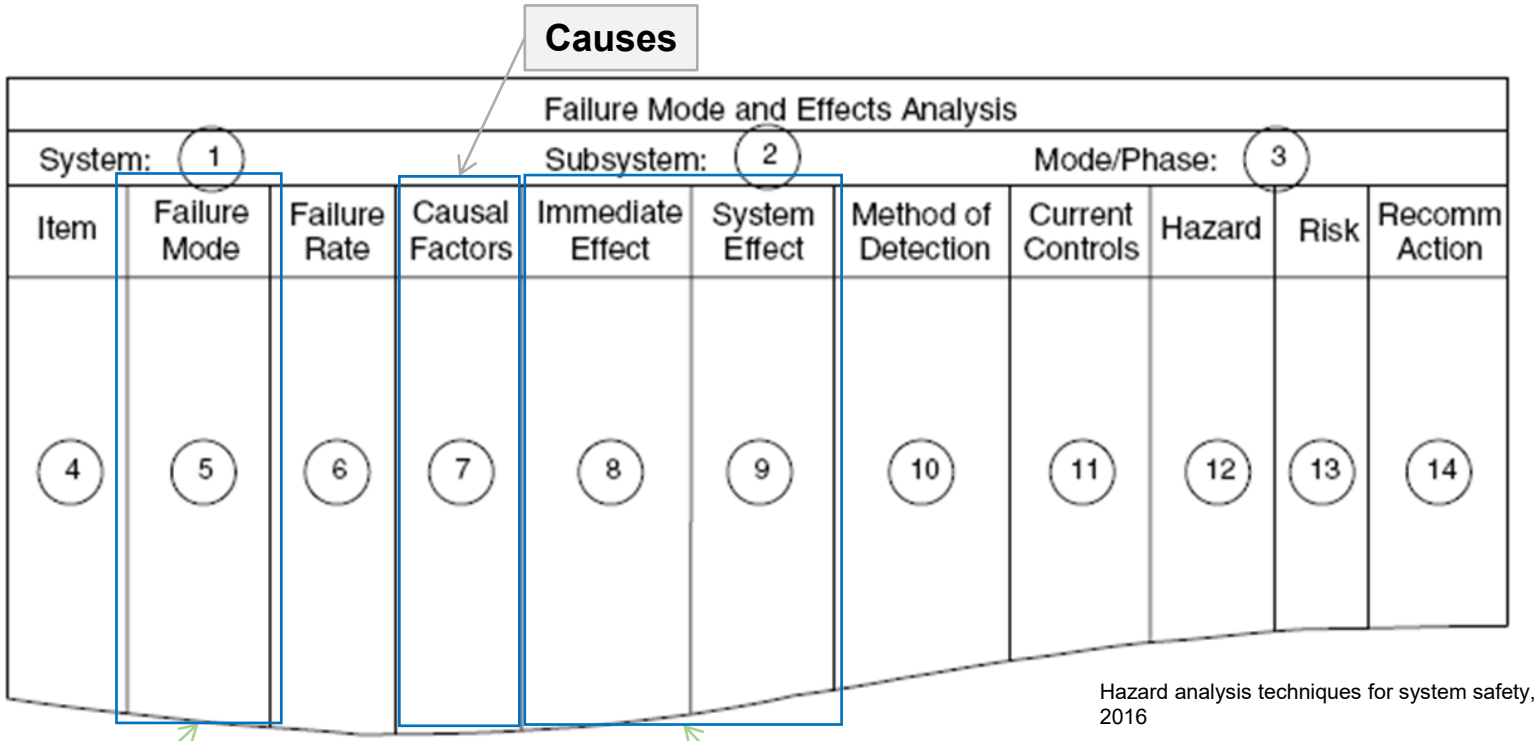


Computational intelligence
for safety assurance of cooperative systems of systems

https://www.dbpia.co.kr/pdf/pdfView.do?nodeId=NODE07190864&googleIPSandBox=false&mark=0&useDate=&ipRange=false&accessgl=Y&language=ko_KR&hasTopBanner=true (융합의 또 다른 이름, 사이버 물리 시스템)

Hazard Analysis & Techniques

Hazard analysis
- A systematic method to identify potential hazards, their effects, and mitigation methods for assuring the safety of systems
- Several hazard analysis techniques: HAZOP, FMEA, STPA, FTA, …



Hazard analysis techniques for system safety, 2016

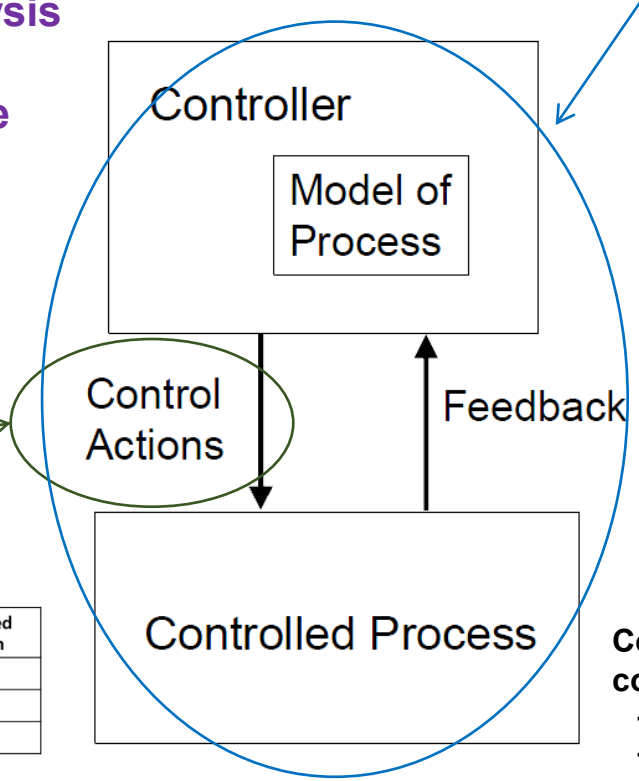
Figure 13.8 *Example FMEA worksheet 3—safety/reliability.*

STPA (System-Theoretic Process Analysis)

- Safety analysis technique based on a system-theoretic accident model and process (Engineering a Safer World, 2016)
  - Identifying unsafe control actions and their causes in the control loops
    - Between components

Preparation:

1. **Define purpose of the analysis (Identify a accident/hazard)**
2. **Construct a control structure**

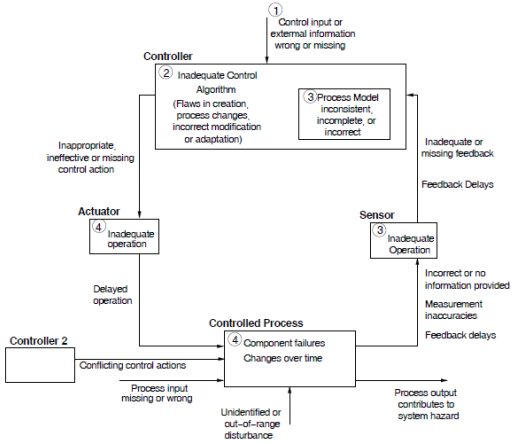


3. Identify unsafe control actions

Control Action	1. Not given or not followed	2. Given incorrectly	3. Wrong timing or order	4. Stopped too soon

4. Identify causes of unsafe control actions

For each unsafe control action, examine the parts of the control loop to see if they could cause it.



Consider how the designed controls could degrade over time through
- **Management of change procedure**
- **Performance audit**
- **Accident and incident analysis**

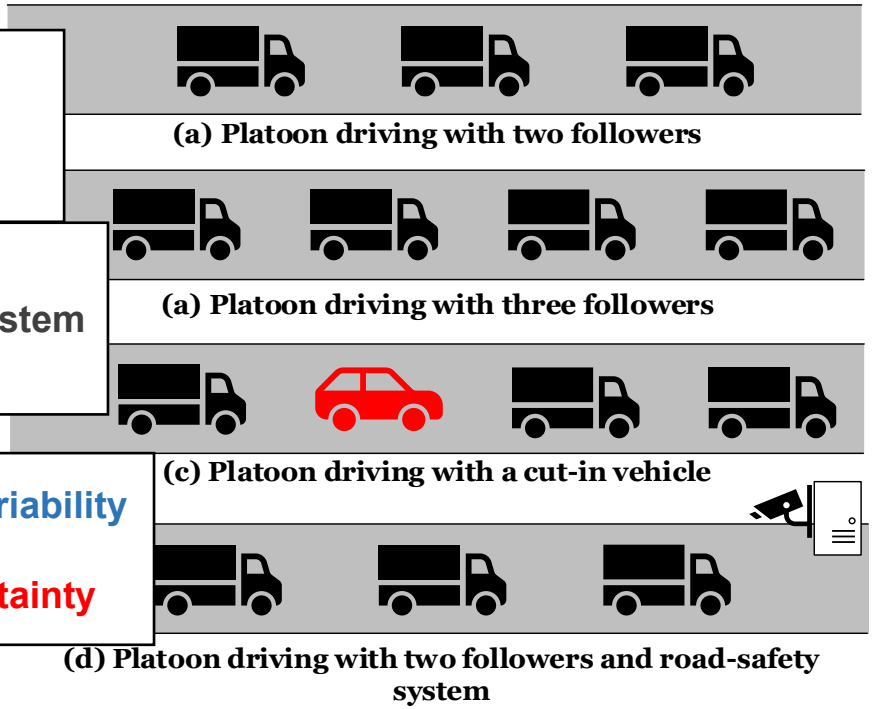
Introduction (Cont'd)

- There are several challenges need to be considered in **hazard analysis** of cooperative systems.
  - Related to **dynamic** features, cooperative aspects analysis
  - The **characteristics** of cooperative systems that need to be considered in hazard analysis
    - Such as "***dynamically changing*** *structure*," "*possibility of the* ***multiple (unknown) numbers of configurations***," "Collaborating ***multiple instances*** *of the systems*" during operation
    - that can lead to various operation circumstances with multiple dynamic structures

These features cause dynamic structures of system configurations (*i.e.* compositions), including external surrounding systems.

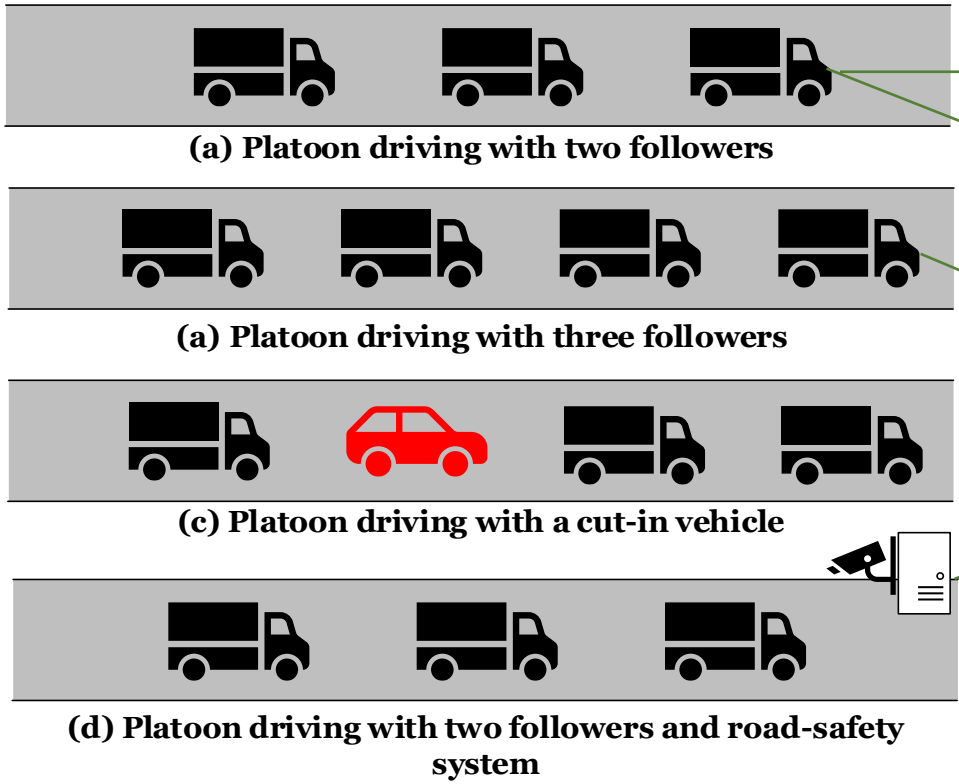
So, it reveals various operation circumstances about multiple configuration structures and system states during operation

These various circumstances are kind of variability factor causing uncertainty, which this paper regards it as a dynamic configuration uncertainty



Introduction

- The dynamic characteristics and uncertainty should be considered
  - By identifying and reflecting such circumstances
  - The variable structures and their changes can be a **hazardous state (i.e., hazard) itself** or a **triggering condition** that leads to the hazards.



Safety analysis of vehicle

Effect of failures

Unsafe Controls

What differences exist in?

Which unsafe situation can occur when other external system exists?

Introduction

- The dynamic characteristics and uncertainty should be considered
  - By identifying and reflecting such circumstances
  - The variable structures and their changes can be a **hazardous state (i.e., hazard) itself** or regard as a **triggering condition** that leads to the hazards.

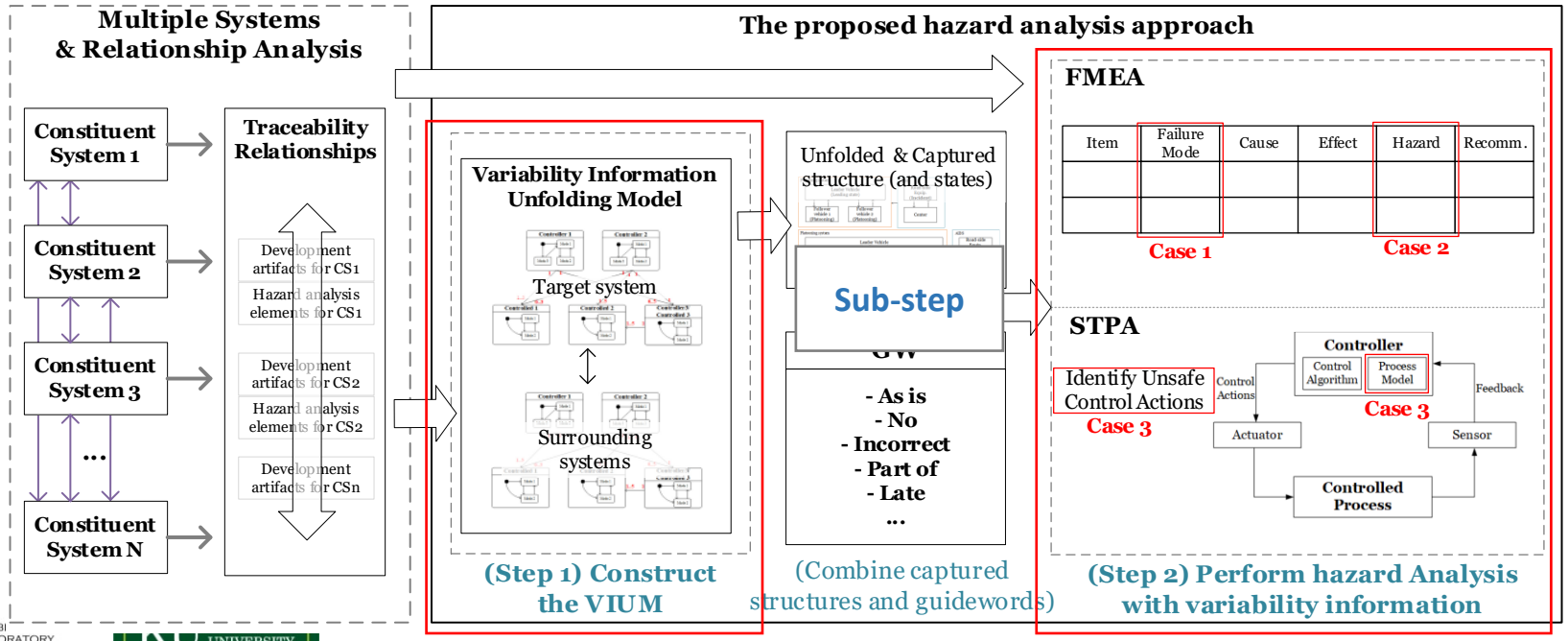
- It is difficult to thoroughly consider various situations from multiple configuration structures in conventional hazard analysis techniques
  - About dynamic features, changed & possible multiple structures, Etc.

  - There are several studies for hazard analysis for cooperative systems
    - However, they do not directly cover the uncertainties about dynamically changing structures or configurations of multiple systems

- This paper proposes **an approach for hazard analysis of cooperative systems**
  - Considering dynamic configuration uncertainty

The proposed hazard analysis approach

- An approach for hazard analysis of cooperative systems considering the dynamic configuration uncertainty
  - Supporting hazard analysis by providing supplementary information about operation circumstances from various configuration structures and application perspectives
- 2 major steps (+1 sub-step)
  - 1. **Constructing** the intermediate model
  - 2. **Performing** the hazard analysis with identified structure information



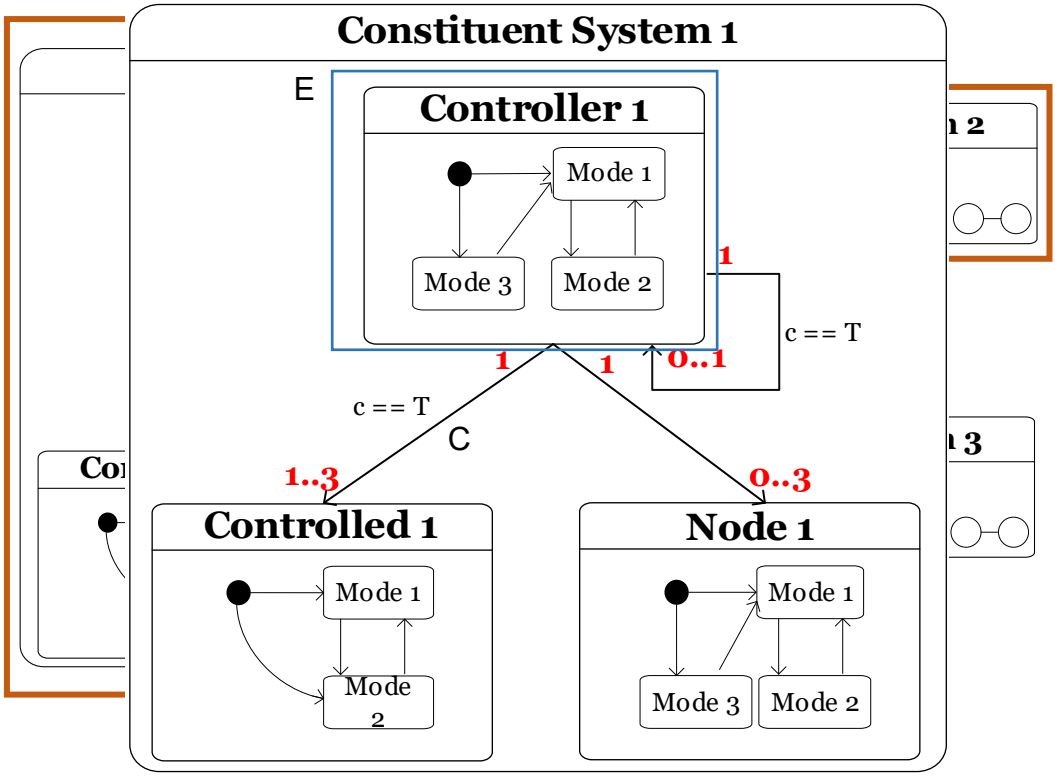
Step 1: Constructing the intermediate model

- We extend the information unfolding model (IUM)* to encompass the expressions for other external systems
  - **VIUM (Variability Information Unfolding Model)**
- For use in finding various combinations of configuration structures (changed structures)
  - It expresses the multiple **elements** of system/components entities and their **connections/interactions/control** relationships

IUM for individual systems

$N = \langle \mathrm{E}, \mathrm{C} \rangle$, where
- $\mathrm{E} = \langle S, L, T \rangle$
  - S : a finite set of states (Modes)
  - L : a set of transition labels
  - T : a set of transitions, $S \times L \times S$
- $\mathrm{C} = (T, M, c)$
  - T : a set of transitions, $\mathrm{E} \times M \times c \times \mathrm{E}$
  - M : a set of pairs of multiplicities
  - c : a label for control relationship, {T, F}

$\mathrm{VIUM} = \langle N, I, n_i \rangle$, where
- N : a set of individual systems
- I : a set of transitions, $N \times N$
- n_i : an intra system (a target system for hazard analysis), an element of N



*Unfolding Hidden Structures in Cyber-Physical Systems for Thorough STPA Analysis

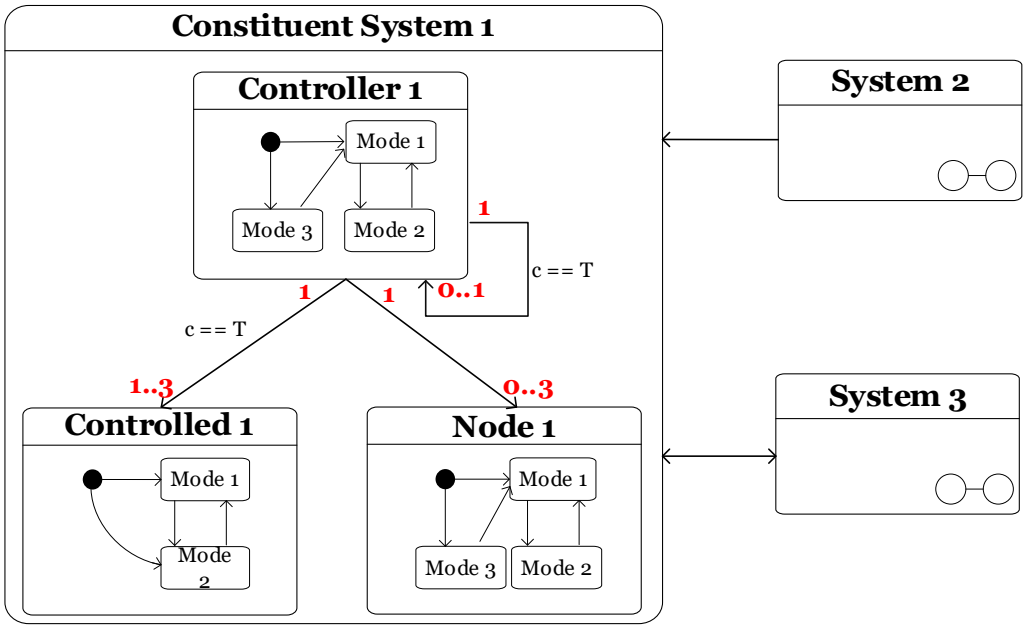
Step 1: Constructing the intermediate model

- System and software specifications should be carefully reviewed to model the VIUM.
  - This step is a manual process to construct the model

- Analysts have to consider in this step
  - **Multiplicity** of system elements that can show various configuration structures (changes)
  - **Relationships** such as controlling relations, interactions, or connections between system or system components
    - Traceability analysis results between

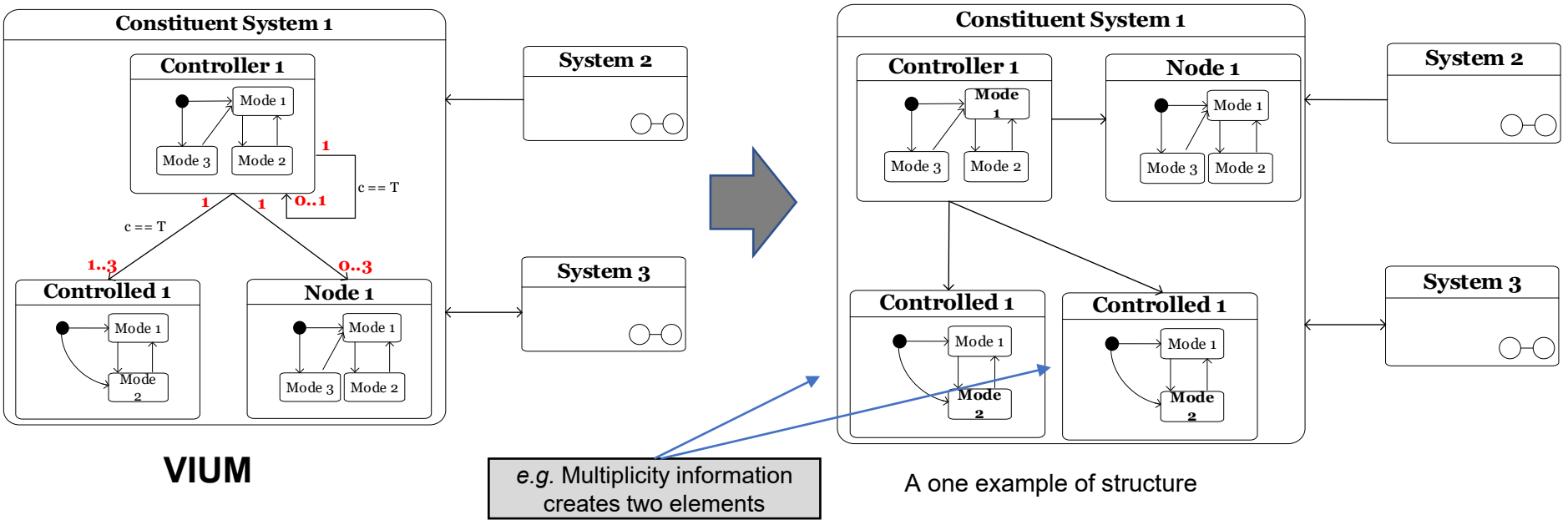
$N = \langle \mathrm{E}, \mathrm{C} \rangle$, where
- $\mathrm{E} = \langle S, L, T \rangle$
  - S : a finite set of states (Modes)
  - L : a set of transition labels
  - T : a set of transitions, $S \times L \times S$
- $\mathrm{C} = (T, M, c)$
  - T : a set of transitions, $\mathrm{E} \times M \times c \times \mathrm{E}$
  - M : a set of pairs of multiplicities
  - c : a label for control relationship, {T, F}

$\mathrm{VIUM} = \langle N, I, n_i \rangle$, where
- N : a set of individual systems
- I : a set of transitions, $N \times N$
- n_i : an intra system (a target system for hazard analysis), an element of N



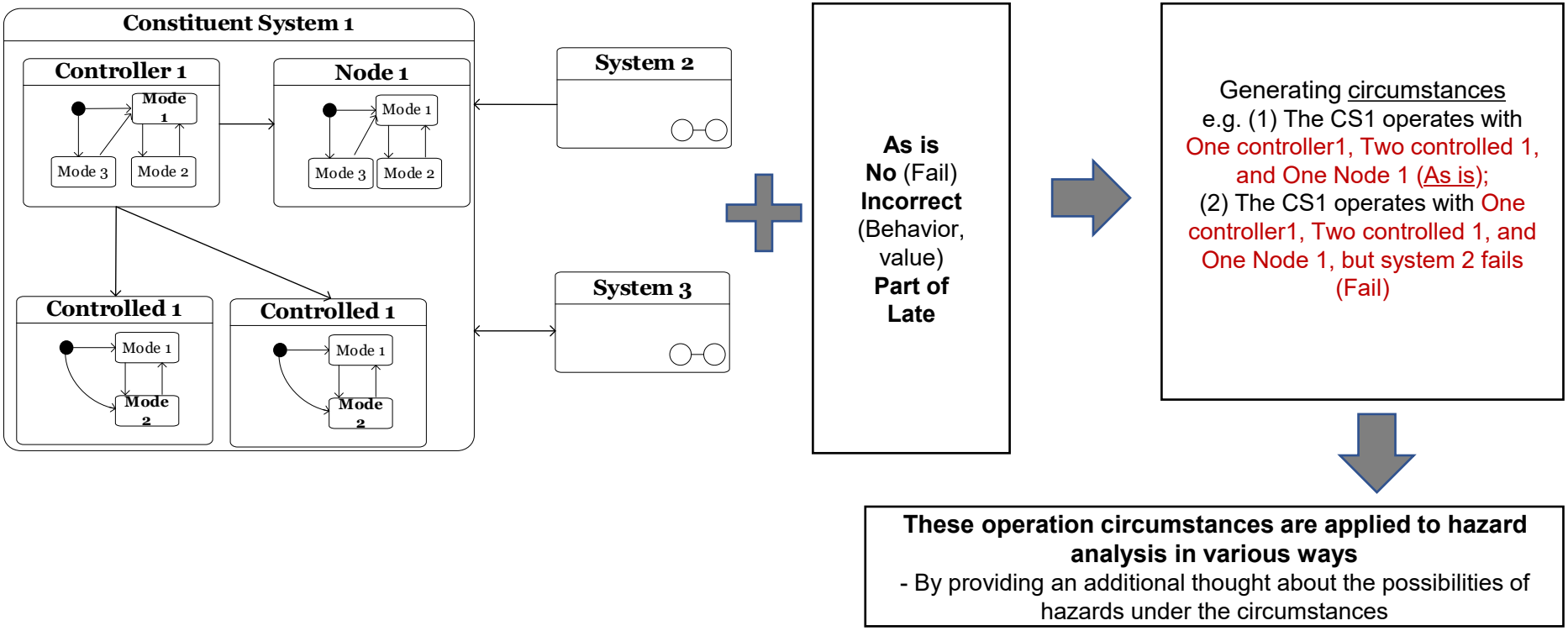
Sub-steps of the process

- After constructing the VIUM sub-steps are applied to create circumstances for the hazard analysis.
  - Unfolding & Capturing the each structure
    - Creating all possible combinations of structures according to the multiplicity in the model
  - Creating various circumstances by combining the identified **structures** with **GW**



Sub-steps of the process

- - The results are applied to hazard analysis to help analysts identify additional or potential possibilities of unsafe behavior, hazards or failures **as a context**



Step 2: Perform hazard analysis

- Performing hazard analysis with the variability information
  - that can be represented as various circumstances with guidewords
  - This paper uses two hazard analysis techniques: **FMEA** and **STPA**

Case1 of FMEA

Merge	**Other leader fails to operate (Fig. 8 (b) + No (Fail))**	TBD	-	Merging two platoons does not complete successfully	Platoon driving operates in incorrect status
Deceleration	Fails to operate deceleration	Network error of leader	Leader vehicle fails to occur deceleration to followers	Followers does not decelerate	Platoon may not maintain safe velocity **under incident (Fig. 8 (a) + As is)**

Case2 of FMEA

Too late, Too soon, Out of order
[UCA4]Leader mode platoon controller provides a lane change command too soon **when leaving and merging function has not been completed (Fig. 8 (b) + Late)**

Case3 of STPA (UCA)

Directly used for **failure modes**

Used as **contexts** of identifying unsafe/hazardous situations (When used as supplementary information)

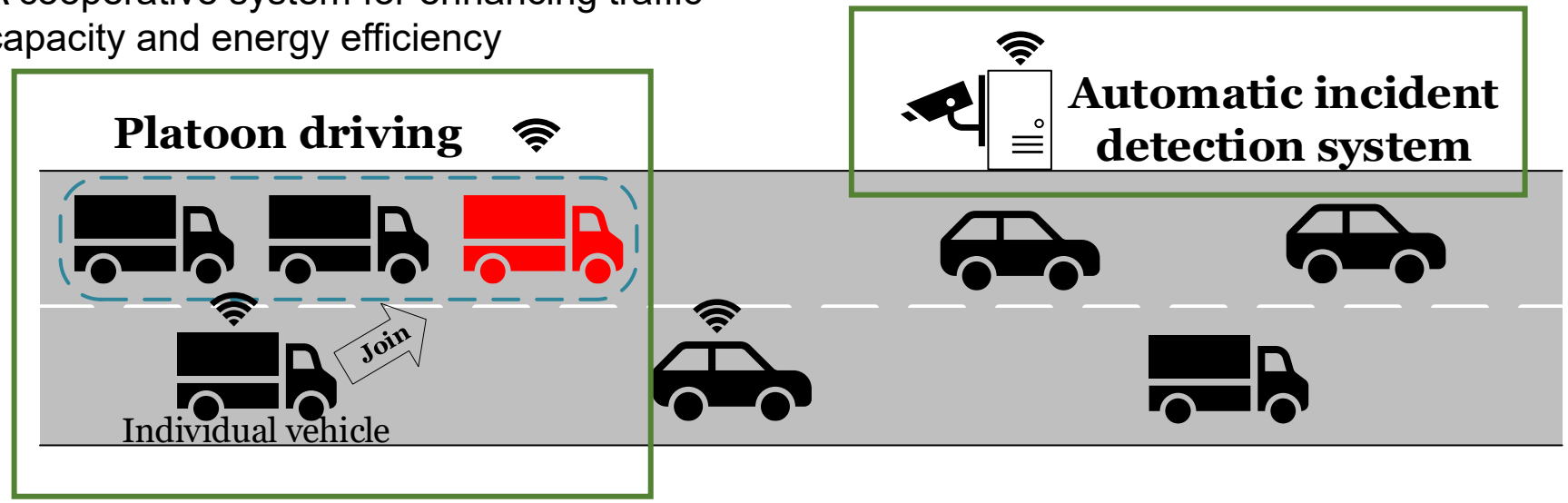
Used as **multiple control structures** or process model variables

Case Study

- Applying the proposed approach into the two systems of roads
  - To show the applicability of the proposed approach
  - **Vehicle platooning system & Automatic incident detection system**

A cooperative system for enhancing traffic capacity and energy efficiency

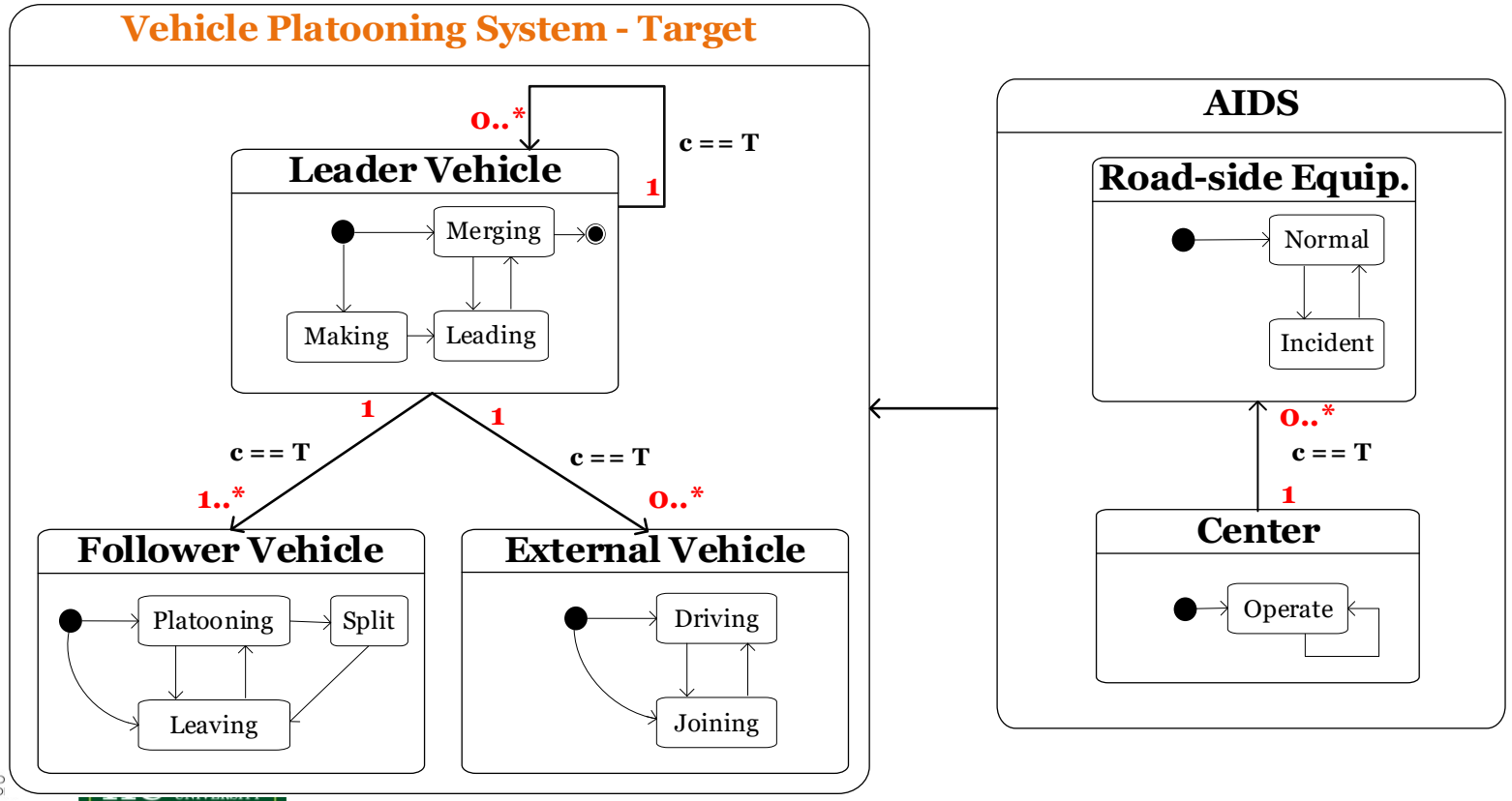
detecting several incidents on the road and sending alarms to the vehicle/drivers



It has several cooperative functions such as create/join/leave platoon, merge, split, acceleration/deceleration, leader change

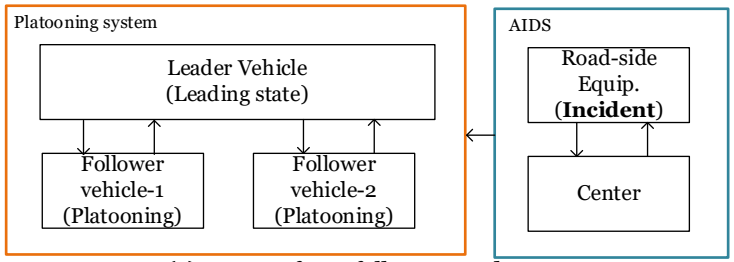
Case Study Results: Construct the VIUM

- The results of constructing the VIUM of two systems
  - The platooning system can have multiple-instances in dynamic circumstances
    - We analyzed it as 3 modes
  - Extracting various configuration structures from the VIUM thoroughly
    - By unfolding, it is a next step

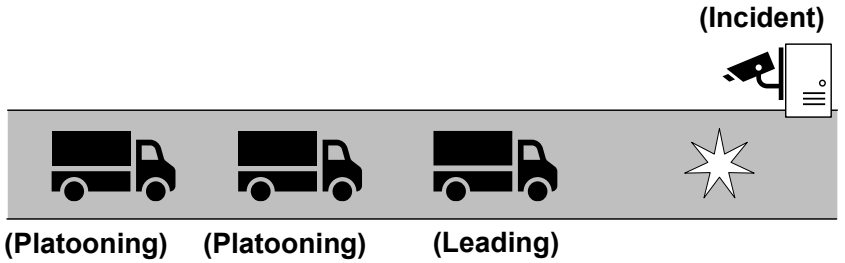


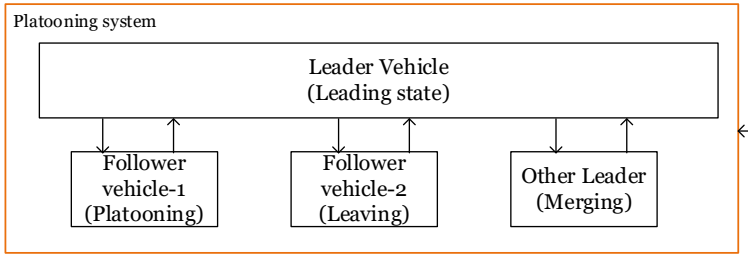
Three examples of the structures

- Unfold the VIUM and extract/capture the various structures
  - Total 6 * 5 * 6 = 180 cases of possible structures in the platooning systems (Assume * == 5)
  - Three examples of possible configuration structures
    - Including multiple-instances of vehicles in platooning system and automatic incident detection system

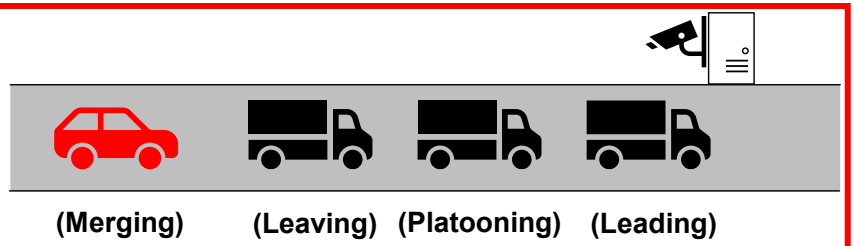


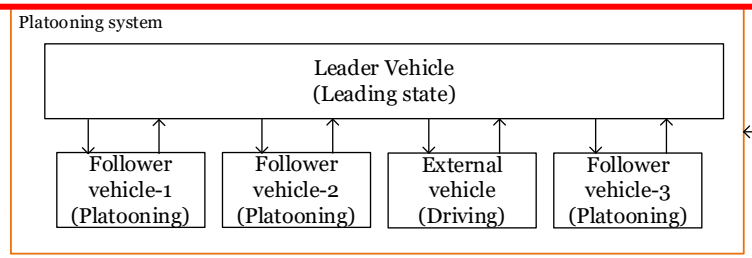
(a) A case of two followers and AIDS



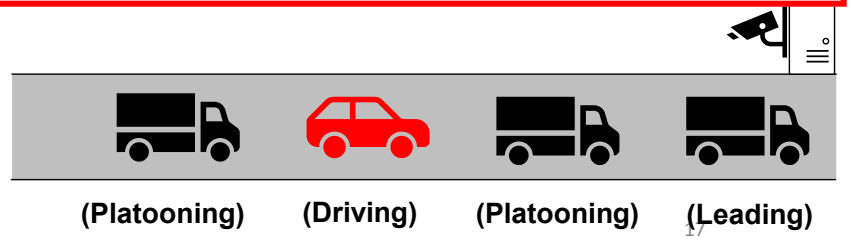


(b) A case of two followers and one other leader and AIDS





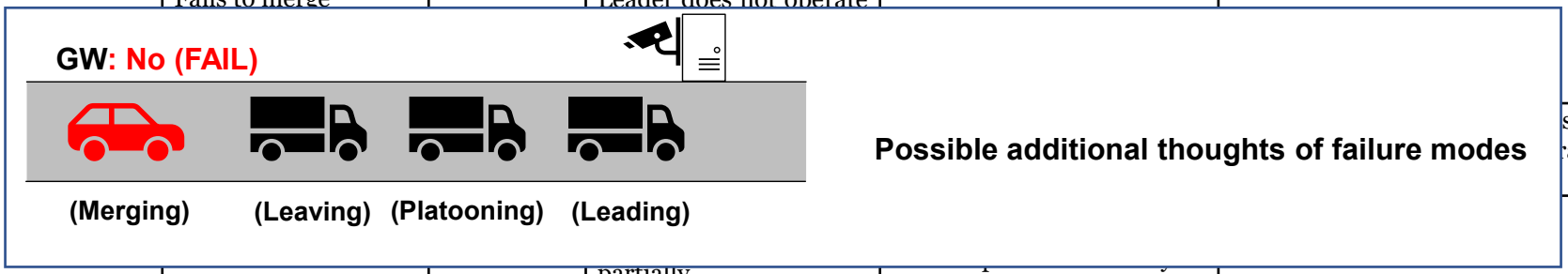
(c) A case of three followers and one external vehicle and AIDS



FMEA results

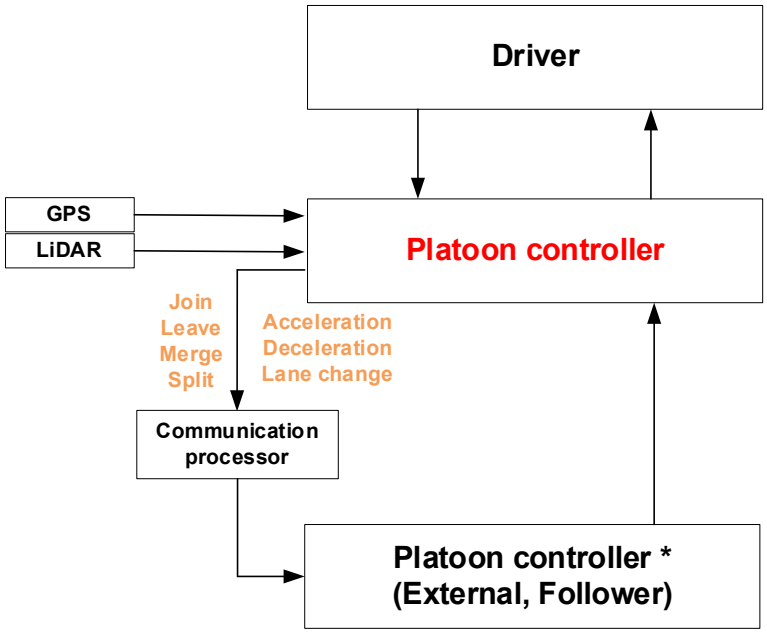
- Parts of analysis results of FMEA

System: Platoon system, Sub-system: Platoon controller, Component: Leader mode					
Function	**Failure mode**	**Causes**	**Immediate effect**	**System effect**	**Hazard**
Deceleration	Fails to operate deceleration	Network error of leader	Leader vehicle fails to occur deceleration to followers	Followers does not decelerate	Vehicle-to-vehicle distance below safe distance Platoon may not maintain safe velocity **under incident (Fig. 8 (a) + As is)**
	Incorrect value of deceleration	TBD	Leader vehicle operates decelerate function at incorrect speed	Followers decelerate incorrect speed according to the leader operation	Vehicle-to-vehicle distance does not maintain appropriately
	Fails to merge	TBD	Leader fails to merge function	Two platoons drive without merging respectively	-
			Leader does not operate partially		in
	Other leader fails to operate (Fig. 8 (b) + No (Fail))	TBD	-	Merging two platoons does not complete successfully	Platoon driving operates in incorrect status



STPA results

- STPA
  - 1) Identify the accident/hazard
  - 2) Construct the control structure



A simplified control structure for the platooning system (leader mode)

Accident

1. A injury/loss of human/property
2. Car accident

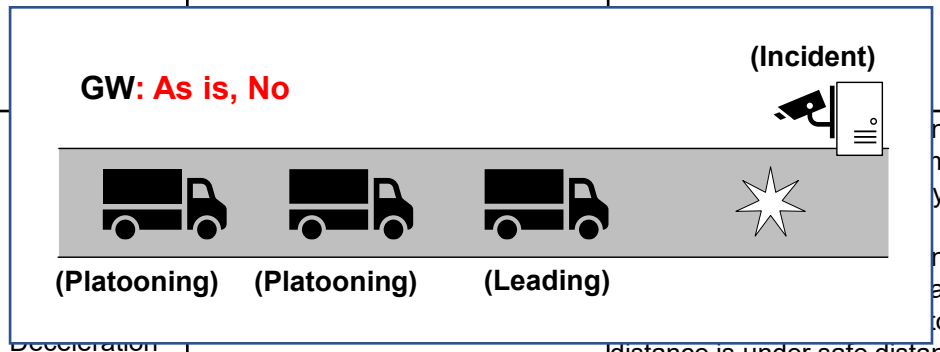
Hazard

1. Violation of safety distance in platoon
2. incorrect/confused platoon composition

STPA results

- A part of UCA tables

Control Action	Not providing causes hazard	Providing causes hazard	Too late, Too soon, Out of order	Stopped too soon, Applied too long
Lane change	[UCA1]Leader mode platoon controller does not provide a lane change command to followers when leader changes the driving lane	[UCA2]Leader mode platoon controller provides a lane change command to followers when leader drives with maintaining lanes	[UCA3]Leader mode platoon controller provides a lane change command to followers too late when leader changes the lane	
			[UCA4]Leader mode platoon controller provides a lane change command too soon **when leaving and merging function has not been completed (Fig. 8 (b) + Late)**	
Deceleration		n controller nand to y situation n controller and to o-vehicle distance is under safe distance	[UCA8]Leader mode platoon controller provides deceleration command to followers tool ate when the leader decelerate under emergency situation	[UCA9]Leader mode platoon controller stop the deceleration command too soon when the follower did not decelerate enough
	[UCA10]Leader mode platoon controller does not provides deceleration command to followers **while AIDS fails to operate its behavior under incidents (Fig. 8 (a) + No (Fail)**	[UCA11]Leader mode platoon controller provides deceleration command to followers **while a non-platooning (external) vehicle is driving in cut-in the platoon (Fig. 8 (C) + as is)**		[UCA12]Leader mode platoon controller stop the deceleration command too soon **while AIDS is under an incident state (Fig. 8 (a) + as is)**
Merge	[UCA13]Leader mode platoon controller does not provide merge command to the other leader when desired	[UCA14]Leader mode platoon controller provides merge command to unrelated platoon	[UCA15]Leader mode platoon controller provides merge command to the other leader too late than requested	



Case Study Results

- The combination of captured structures and GWs **can help** analysts **consider** **the hazards under such circumstances** additionally and thoroughly.
  - They are not easy to elicit in typical hazard analysis process thoroughly.
  - The proposed approach can also provide **additional** thinking for hazard analysis of cooperative aspect.
    - E.g. "*Platoon does not merge with other platoon when this is desired ([17])*" can also be combined with our circumstances
- We also have several issues and limitations need to be considered.
  - **Complexity** of the VIUM
  - *Several issues about* ***dynamic*** in safety analysis
    - E.g. by *monitoring*

Conclusion & Future Works

- This paper proposes an approach for hazard analysis of cooperative systems
  - with considering dynamic configuration uncertainty
  - It can contribute to find various hazardous scenarios under multiple/various circumstances for hazard analysis of cooperative systems

- Future Work
  - Developing a (semi-)automatic and more systematic method for using VIUM
    - Also with a CASE tool
  - Creating VIUM efficiently
    - like generating the model from traceability analysis results automatically

THANK YOU

Q & A

Sejin Jung
Konkuk University
jsjj0728@konkuk.ac.kr