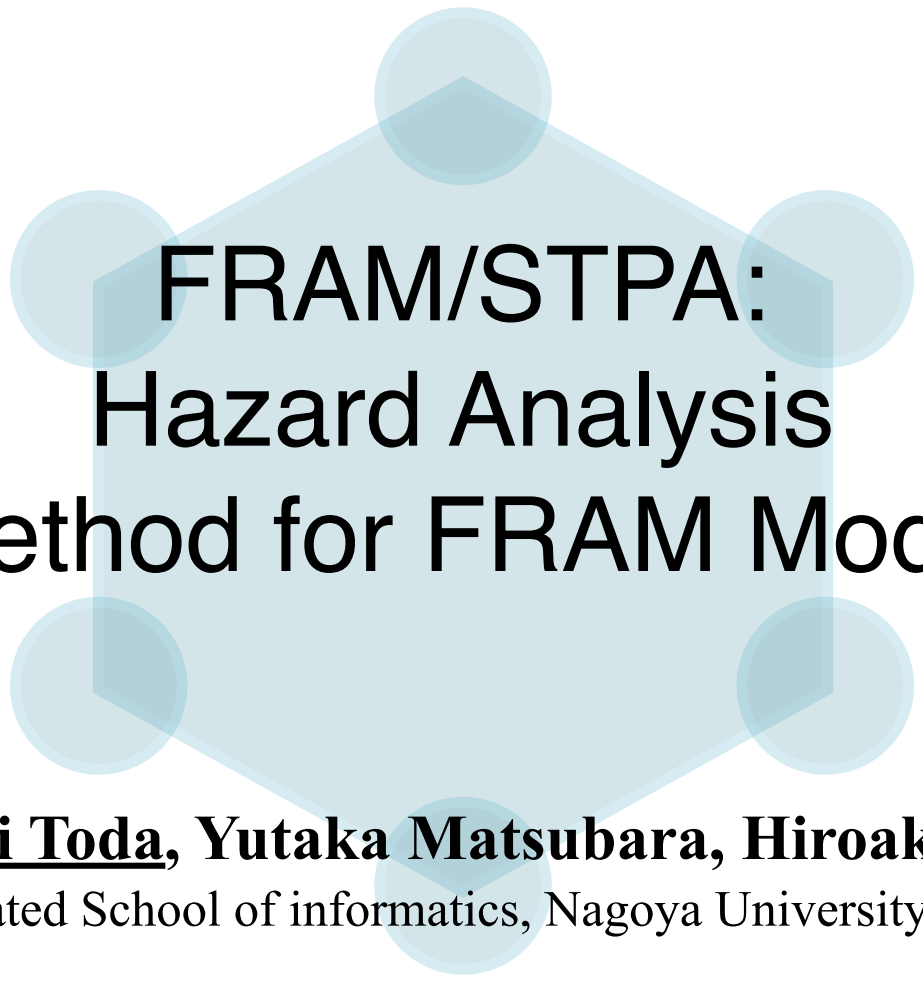


---



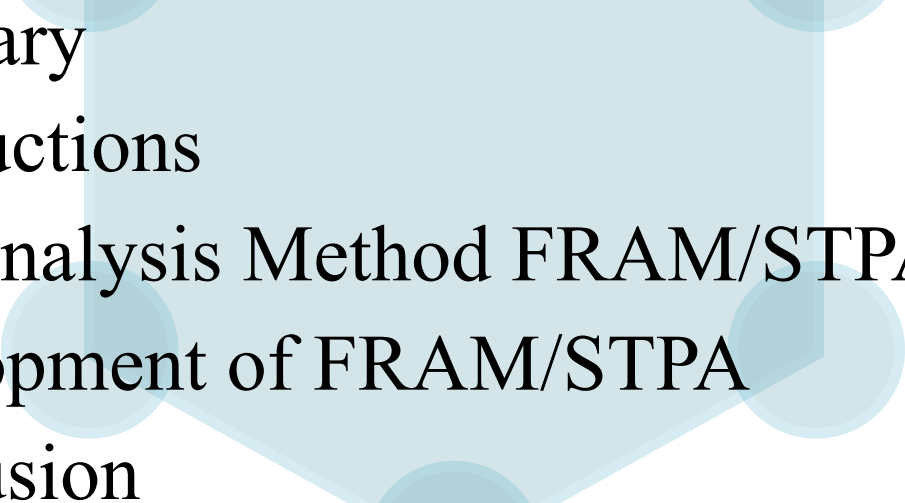
# FRAM/STPA: Hazard Analysis Method for FRAM Model

**Yoshinari Toda, Yutaka Matsubara, Hiroaki Takada**

Graduated School of informatics, Nagoya University, Japan

---

# Outline

- 
1. Summary
  2. Introductions
  3. New Analysis Method FRAM/STPA
  4. Development of FRAM/STPA
  5. Conclusion

# Summary

---

- »New hazard analysis method FRAM/STPA is proposed.
  - »STPA is adapted to models of FRAM.
- »FRAM/STPA analyzed new hazards which were not analyzed in STAMP/STPA.
  - »case study - railroad crossing -
- »New keywords “too much” and “too little” are added to FRAM/STPA.
  - »case study - lane changing -

---

# Introductions

# Hazard Analysis for Autonomous Cars

---

- » Many companies have conducted research and experiments on autonomous cars in various countries.
- » System for autonomous cars need to adapt to various environments.
- » To evaluate risks in such complex control systems, hazard analysis is important.



GM's current automated driving test vehicle "Chevrolet Volt"

# Why Suggest New Analysis Method for FRAM

---

- »FRAM is a modeling language that describes the behavior of a system.
  - »Along with the complexity of the system, it is useful to model by function relationship.
  - »It can be used for systems with varying functions.
    - »Can it be used for autonomous cars?
- »However, hazard analysis methods of FRAM have not been proposed.

# Goals and Contributions

---

## »Goals

- »Propose a hazard analysis method for FRAM model.
- »Propose a method that can analyze fluctuations in FRAM.

## »Contributions

- » We had Proposed new hazard analysis method FRAM/STPA.
- » We had showed the usefulness of FRAM/STPA by comparing STAMP/STPA and FRAM/STPA.
  - »case study -railroad crossing -
- » We had showed that FRAM/STPA is useful for hazard analysis of autonomous cars.
  - »case study - lane changing -

# What is The New Method FRAM/STPA

---

»Propose hazard analysis method of FRAM model by STPA

»Procedure

1. For each aspect of each function of FRAM, hazard analysis is performed according to the four guide words of STPA
2. Express outcomes by **Deviation, Local Influence, Global Influence** and **Severity**

»FRAM and STAMP are different modeling languages.

»Effectiveness of the proposed method is presented through a case study.



# STAMP/STPA

---

- »STAMP(System Theoretic Accident Model and Processes)
  - »Accident model based on system theory
  - »Model based on the relationship between controller and controlled objects
- »STPA(STAMP based Process Analysis)
  - »Hazard analysis with four keywords
  - »Analyze interaction between components(control actions and feedback)

	Not Providing	Providing causes hazard	Too early/Too late	Stop too soon/ Applying too late
Control Action				

NANCY LEVESON and JOHN THOMAS, editors. STPA HANDBOOK. NANCY LEVESON AND JOHN THOMAS, 3 edition, 10 2018.

---

# Analysis Target

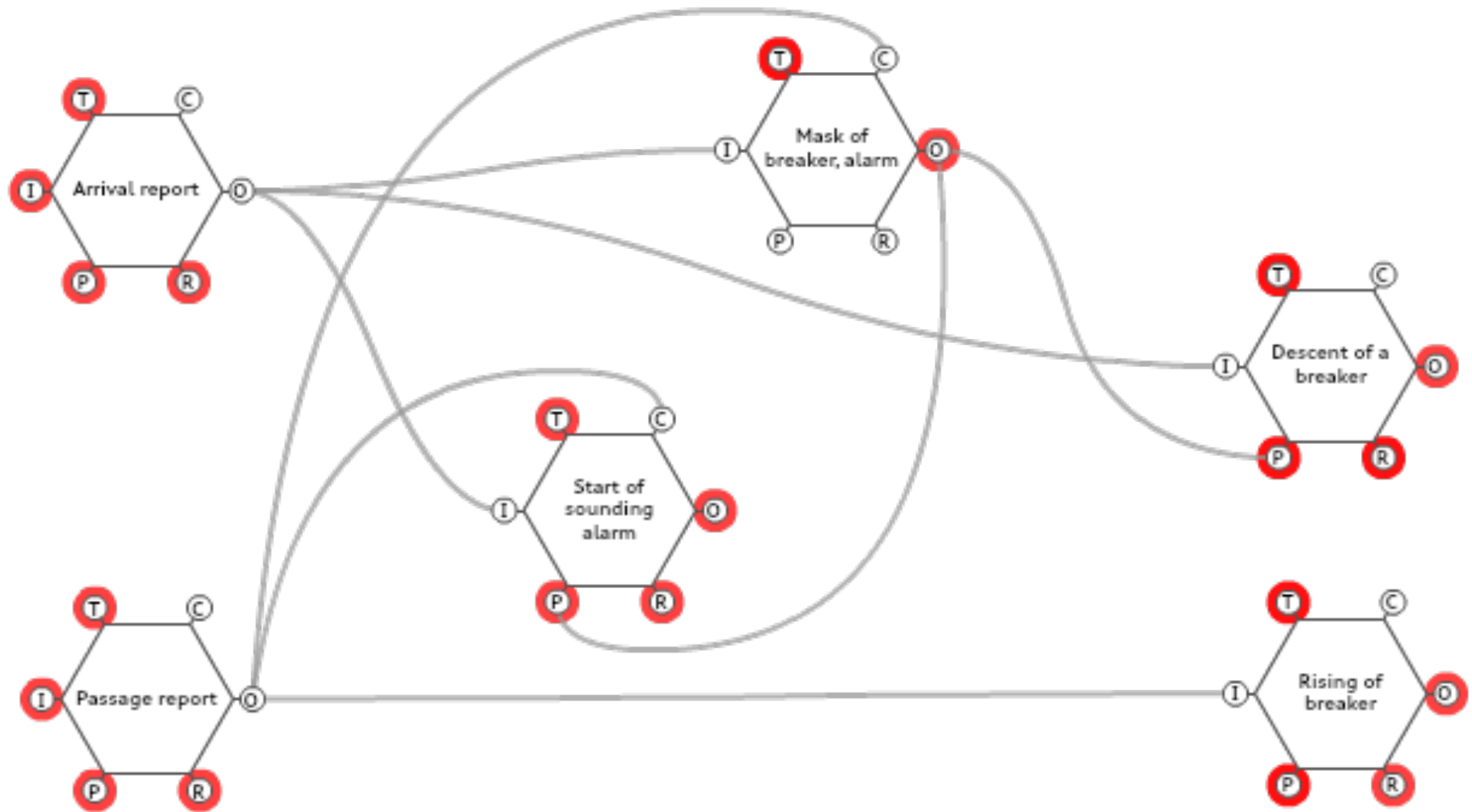
# Railroad Crossing System

- » When a sensor(A or B) detects that the train has approached, it descends the crossing gate and makes the alarm sound.
- » When the sensor(C) detects that the train has passed, it raises the crossing gate and makes the ringing alarm stop.
- » When another train approaches while the crossing gate is descending and the alarm is ringing, the function of masking sensor is activated so that the function does not overlap.



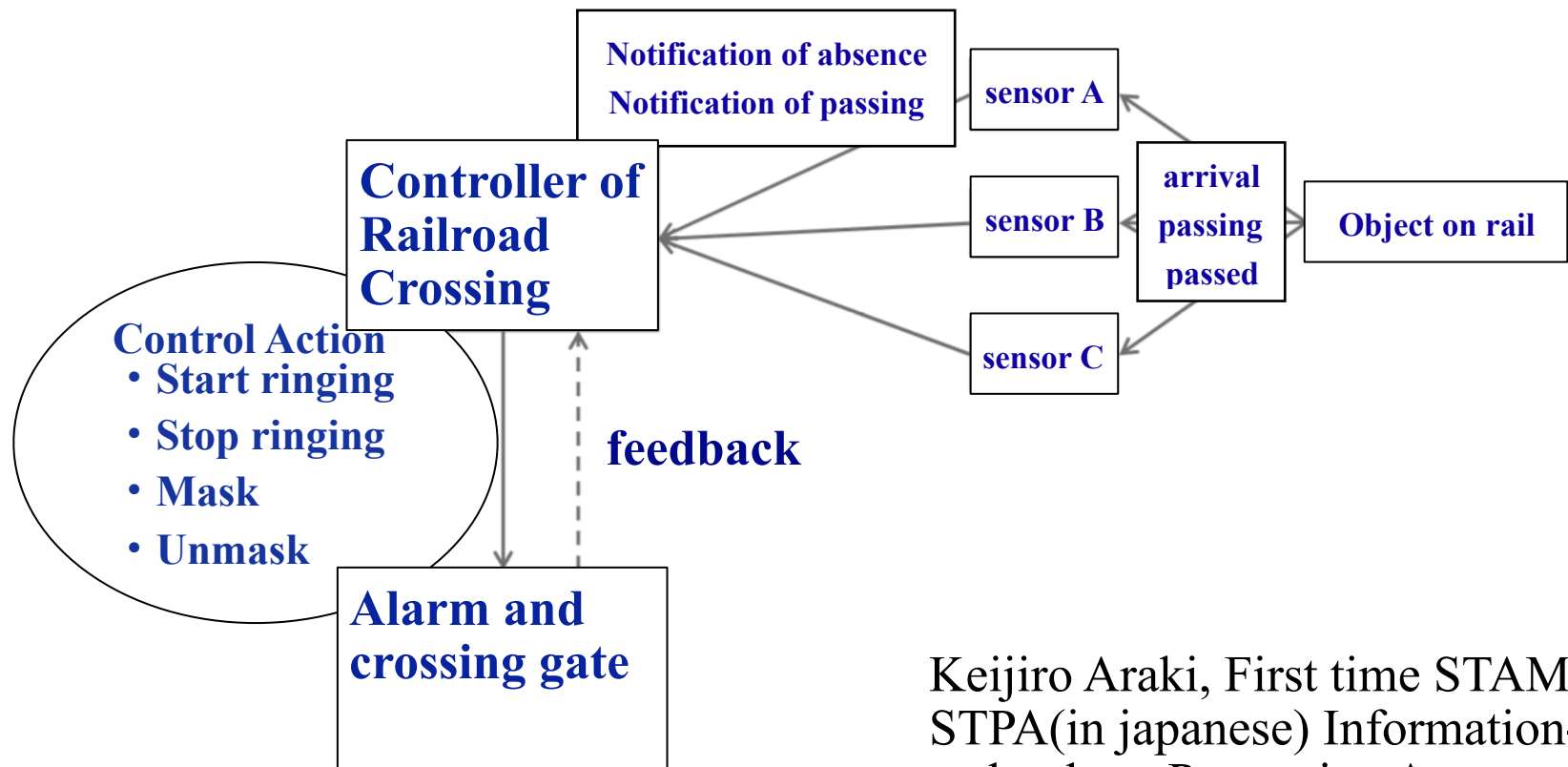
Keijiro Araki, First time STAMP/STPA(in japanese) Information-technology Promotion Agency, Japan, 2017, 10, vol.3

# FRAM Model of Railroad Crossing



# STAMP Model of Railroad Crossing

»STAMP/STPA analyze interaction between controller and controlled components(control action and feedback).



Keijiro Araki, First time STAMP/STPA(in japanese) Information-technology Promotion Agency, Japan, 2017, 10, vol.3

# Comparison between FRAM/STPA and STAMP/STPA

	Total	Severity		
		9	5	1
FRAM/ STPA	87	48	27	12
STAMP/ STPA	16	9	3	4

	New	Similar	Overlook
FRAM/STPA	53	34	2

»FRAM could analyze more hazards than STAMP/STPA.

»14 hazards analyzed by STAMP/STPA are also analyzed by FRAM/STPA.

»Note that ,in FRAM/STPA, same hazards had been analyzed by some aspects.

# New Hazards Analyzed by FRAM/STPA

		Too early/Too late			
		Deviation	Local Influence	Global Influence	Severity
Start of sound-ing alarm	input	Input is too late	Input is late to come	Before the alarm sounds, the train reaches	9
	output	Output is too late	<u>Output is slow</u>		9
	time	Time restriction is too late	<u>Function starts late after receiving input</u>		9

»The hazards(**red characters**) are related to the inside of the component.

»STAMP/STPA couldn't analyze the hazards because they aren't regarding to control actions and feedback between components.

# Hazards not analyzed by FRAM/STPA

---

## STAMP/STPA

	Providing causes hazard
Mask	Mask on <u>different sensors</u> , railroad crossing does not work

»STAMP models the system at **component structure level**.

»FRAM models the system at **functional level**.

»If FRAM models are written in more detail, FRAM/STPA could analyzes hazards related to components.

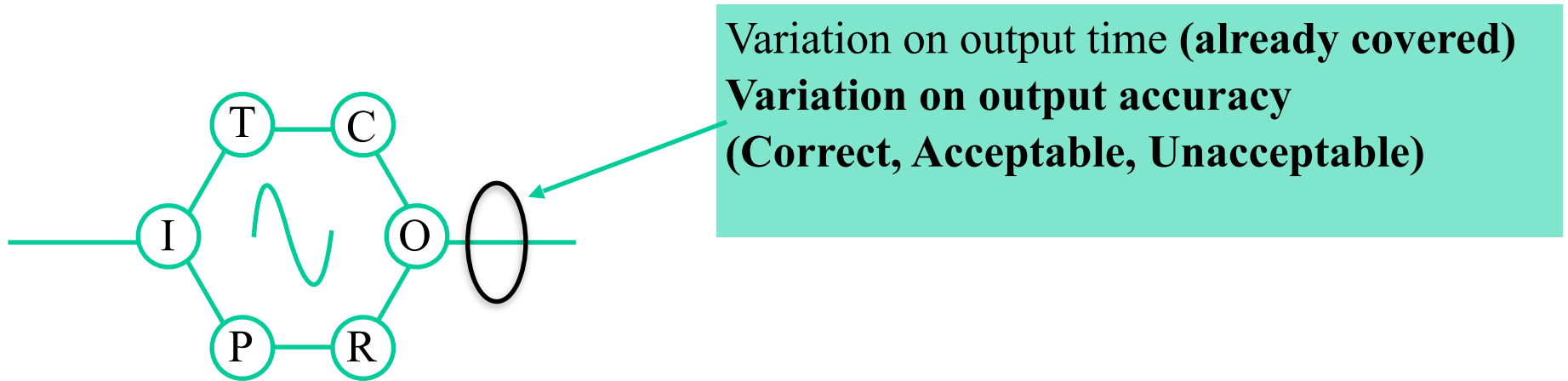
»However, the models become larger.



---

# Development of FRAM/STPA

# Additional keywords to analyze output variability



- » Two added keywords are “Too much” and “Too little”
- » Analyze the output of the function quantitatively
- » e.g. Faster speed, Range is narrower and etc.

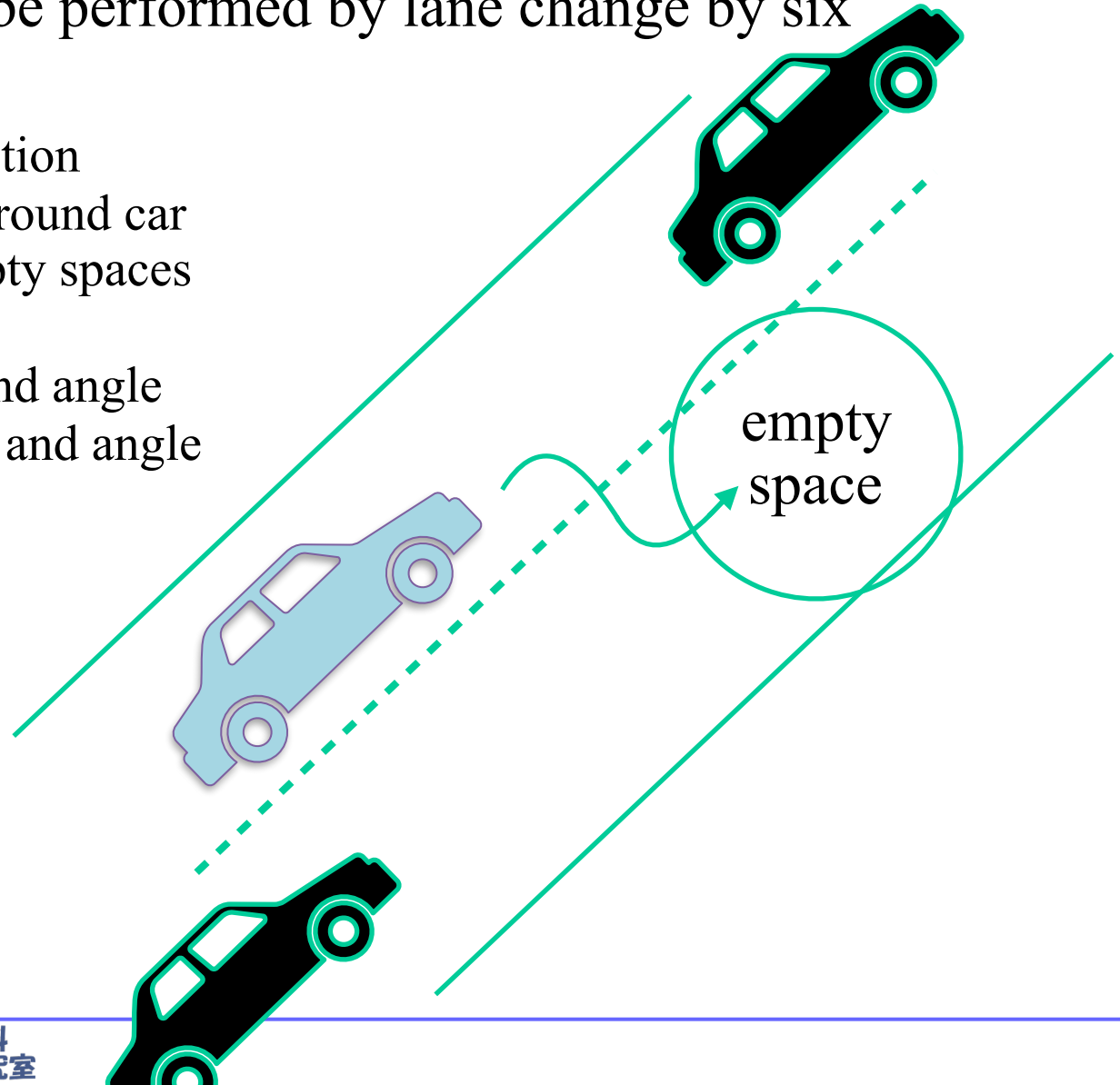
---

# Analyzing Lane Changing (autonomous cars)

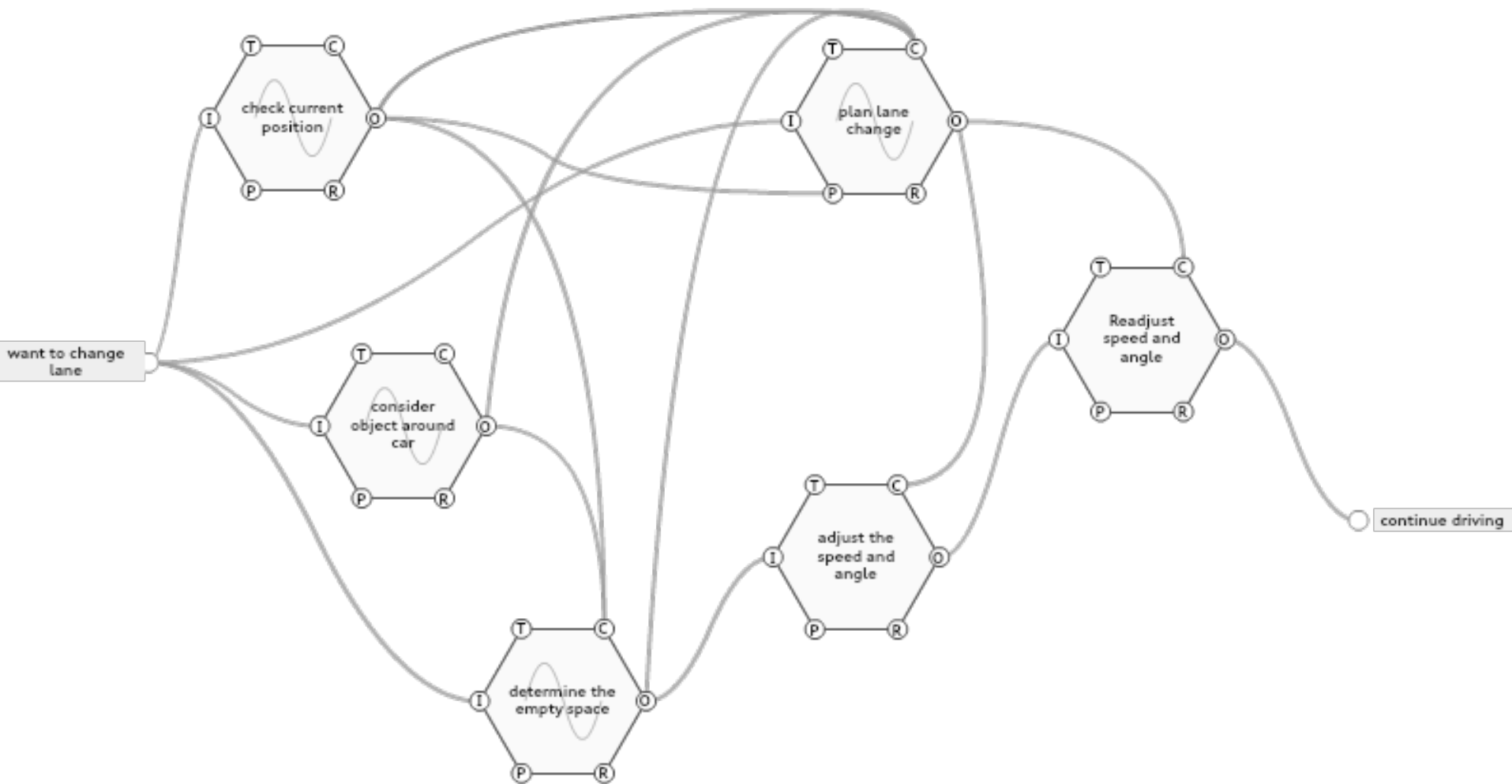
# Analyze Lane Changing (autonomous cars)

» Define actions to be performed by lane change by six functions

- » check current position
- » consider objects around car
- » determine the empty spaces
- » plan lane change
- » adjust the speed and angle
- » readjust the speed and angle



# FRAM Model of Lane Changing



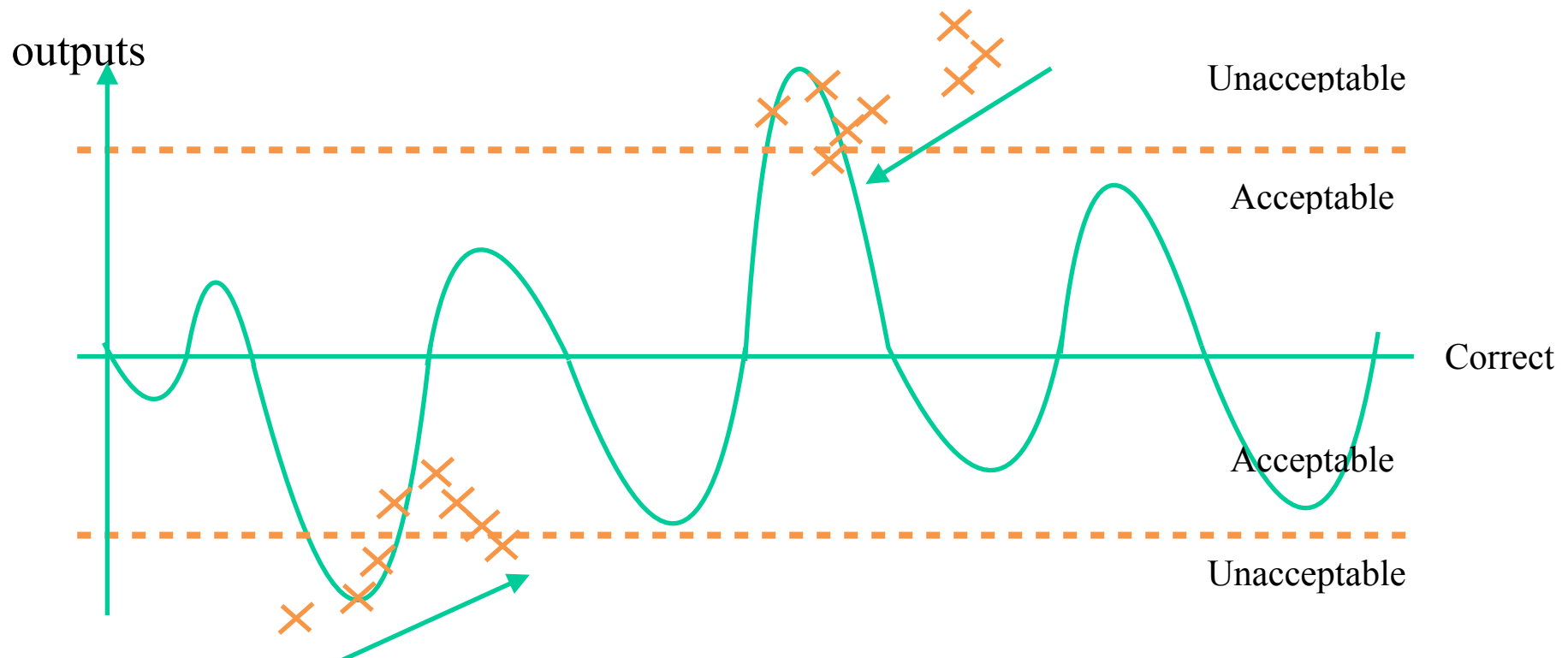
# Results of Hazard Analysis

»Analyzing output fluctuation, FRAM/STPA could analyze hazards related to output fluctuations.

		Too much				Too little			
		Deviation	Local influence	Global Influence	severity	Deviation	Local Influence	Global Influence	Severity
determine the empty space	output	Output range is too wide	Output larger than the value that should actually be output	Space wider than the actual empty space, make dangerous lane change	9	Output is too narrow	Output smaller than the value that should actually be output	It outputs less than the actual empty space, and it becomes impossible to change the lane	5
adjust the speed and angle	output	Output range is too large	Outputs a larger value than the expected output value	Perform a lane change with a speed faster and sharper angle than planned	9	Output range is too small	Outputs a smaller value than the expected output value	Perform a lane change with a speed slower and looser angle than planned	9
readjust speed and angle	output	Output range is too large	Outputs a larger value than the expected output value	Lane change at a speed faster and sharper angle than planned	9	Output range is too small	Outputs a smaller value than the expected output value	Lane change at a speed slower and looser angle than planned,	9

# Consideration

- » Unacceptable situation was analyzed in FRAM/STPA.
- » In order to design a safety function, it is necessary to find a boundary between Acceptable and Unacceptable.
- » There is a need to analyze the fluctuation in stages.



---

# Conclusion



# Conclusion

---

## » Conclusion

- » Conducted a proposal of FRAM/STPA and a comparison with STAMP/STPA.
- » Added new keywords “Too much”, “Too little” and analyzed with them.
  - » Need to make improvements
    - » Several variations
    - » Stepwise variation

## » Future Work

- » Continuation of evaluation of FRAM / STPA
- » Reconsideration of new keywords
- » Development based on FRAM model

---

Thank You for Your Attention

---

# References

# References

---

1. Erik Hollnagel, editor. Safety-I and Safety-II: The Past and Future of Safety Management. Routledge, 1 edition, 28, 5, 2014
2. Keijiro Araki, editor. First time STAMP/STPA(in japanese). Information-technology Pro-motion Agency, Japan, 3 edition, 10 2017.
3. NANCY LEVESON and JOHN THOMAS, editors. STPA HANDBOOK. NANCY LEVESON AND JOHN THOMAS, 3 edition, 10 2018.