

# FRAM/STPA: Hazard Analysis Method for FRAM Model

Yoshinari Toda, Yutaka Matsubara and Hiroaki Takada  
Graduate School of Informatics, Nagoya University  
Furo-cho, Chikusa-ku, Nagoya, Aichi, Japan

2018/05/15

## Abstract

Few effective methods have been proposed to analyze safety-critical systems using FRAM models. To utilize a FRAM model, we propose a new hazard analysis method, called FRAM/STPA, which derives hazardous event using 4 keywords of STPA (Systems Theoretic Process Analysis) and new keywords for time-variations of functions. The proposed method and several case studies are presented in this paper.

In FRAM/STPA, four keywords, 'Not providing', 'Providing causes hazard', 'Too early/Too late' and 'Stopping too soon/Applying too long causes hazard', are applied to each aspect of each function in a FRAM model. The analysis results include four descriptions, i.e. deviation, local influence, global influence, and severity for each combination of an aspect and a keyword. From our case study, FRAM/STPA could find additional hazards compared to STAMP/STPA. However, the several hazards concerning the components of the system were overlooked.

To improve analysis capability of FRAM/STPA, new keywords suitable for FRAM are proposed to derive hazards due to fluctuation related to the accuracy of output. Both cases where the output value is larger than the expected value and smaller than the expected value were easily analyzed. Then, the new FRAM/STPA found new hazards. Through our case studies, we conclude that FRAM/STPA is effective for the concept phase in the system development where the system structure regarding components of hardware or software has not been fixed yet. Other hazard analysis methods like STAMP/STPA should be also utilized in system design phase.

## 1 Introduction

In the analysis by FRAM, we develop a model of a safety-critical system in functional units and clarify a variability of each function. However, even if we could identify the function with variability, it is not clear how to make the system safe.

Several papers have been published about analysis methods for FRAM model and usage of FRAM. In reference [1], analytical methods have been proposed that qualitatively express the

variability of coupling between functions of FRAM using Monte Carlo simulation. However, it is necessary for the analyst to decide parameters to be used for qualitatively expressing the value of the variability, different analysts will make different evaluations. In [2] and [3], in the medical field and aircraft field, for analyzing the cause of the accident, they compare the model of the assumed work and the model of the work actually done.

In this way, several papers have been published on how to use FRAM, however effective methods have not been clarified yet.

In this paper, we propose a new safety analysis method for FRAM-modeled system. The proposed method is the hazard analysis method FRAM/STPA that applied the hazard detection method STPA to the FRAM model. In this method, hazard analysis is performed according to four keywords for each aspect of each function defined. The four keywords are "not providing", "Providing causes hazard", "too early/too late", "Stop too soon/Applying too late". We add two more keywords "too much" and "too little" to carry out more detailed hazard analysis regarding the variability of the functions.

The contributions of this paper are as follows.

- Propose a concrete hazard analysis method of FRAM,
- Compare the result of FRAM/STPA with the result of STAMP/STPA and
- Add new keywords and analyze output fluctuations.

The structure of this paper is as follows. In the first section, we will explain the description of STPA which is an analysis method of FRAM/STPA and the modeling language STAMP analyzed by STPA. In the second section, we describe the analysis method FRAM/STPA proposed in this paper and its procedure. In the third section, two examples of railway crossing and lane change are shown as an analysis actually using FRAM/STPA. In the next section, we will discuss the consideration obtained from the analysis example and conclude at the end.

## 2 STAMP/STPA

The modeling language STAMP (System-Theoretic Accident Model and Processes) used in STPA analysis will be described. STAMP is the name of a new accident causal relationship model, according to reference [4], which is the basic theory of STPA. STAMP is a modeling language for modeling the interaction between an element (controller) that performs safety control in a system and an element to be controlled (controlled object). Interaction refers to an control action specifically given to the controlled object by the controller and its feedback.

According to [5], STPA (System-Theoretic Process Analysis) is a relatively new hazard analysis method based on the causal relation of the accident. In STPA, accidents are assumed to be caused by non-safe actions of interaction between system components, even if the components are not failing. This is similar to FRAM, and in FRAM failure analysis is carried out under the idea that

accidents occur due to a function variation other than accidents caused by component failure. Incidentally, according to this idea, STPA analyzes the hazard using four keywords for control action in the model. The four keywords are "Not providing", "Providing causes hazard", "Too early/Too late", "Stop too soon/Applying too late".

### **3 Proposal of FRAM/STPA**

We introduced STPA, so we introduce the FRAM/STPA method proposed in this paper.

Firstly, it is the reason why we decided to apply STPA hazard analysis method to FRAM. Of course, we understand that FRAM and STAMP are modeling languages with different concepts. As shown in the Table 1, there are various differences between FRAM and STAMP, such as the purpose of each modeling language, its target, describable elements and so on. At first glance it seems difficult to apply the analysis method used for STAMP to FRAM due to these differences. However, we thought that the keywords used in STPA are similar to those considered in FRAM. In fact, temporal fluctuation of function in FRAM can be analyzed by analyzing keywords "too early/too late" and "not providing" of STPA.

Table 1: Model comparison table

	FRAM	STAMP
Purpose	Explain how things work or should work	A model to show the interaction between the controller and controlled target
Descriptive object	Functions	Separate system components into controller, controlled target
Input	✓	✓
Output	✓	✓
Time	✓	-
Execution order	Depends on precondition	-
Control	✓	✓
Precondition	✓	-
Resource	✓	-
Human Behavior	✓	✓
Function behavior	✓	✓
Safety analysis method	Not well established	STPA
Description of variability	Output timing and accuracy	-

The procedure for actual analysis by FRAM/STPA are explained.

(1) We create an FRAM model of the system to be analyzed. The thing to watch out here is to do functional level modeling without considering concrete components. If you model with specific components and so on, the analysis targets become bigger, so it takes too much time to analyze a target, or hazards are overlooked by concretely doing so. Then, we recommend analysis at functional level.

(2) When modeling is completed, it is finally analyzed. In the analysis, hazard analysis is performed using keywords for each aspect of each function defined. Depending on aspects, there are times when we can not analyze with some keywords, so we do not need to analyze in that case. For example, analysis on keywords such as "not provided" and "Providing causes hazard" on the "time" aspect can not be analyzed, so some frames of the aspects need not be described. In addition, the results of the analysis are divided into four items, Deviation, Local influence, Global influence, and Severity. By doing this, the analysis result is easy to understand and it is easy to

use for reviews.

By using STPA, it is possible to analyze deviations due to time variation in FRAM. In FRAM, another variation on accuracy can be defined. Therefore, I wanted to analyze deviations due to fluctuations in accuracy, and added new keywords. The new keywords are "Too much" and "Too little".

## 4 Case Study

### 4.1 Railroad Crossing - compared with STAMP/STPA -

First case study is a hazard analysis carried out for a railroad-crossing. Note that the keywords of hazard analysis are not included "too much" or "too little" because this analysis was done in the early stages of the study.

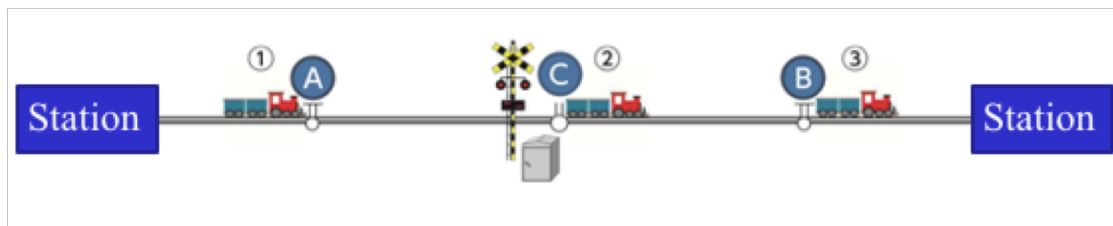


Figure 1: Railroad Crossing

Figure 1 shows the railroad crossing system to be analyzed.

- 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.

The results of modeling the system with FRAM are shown in Figure 2.

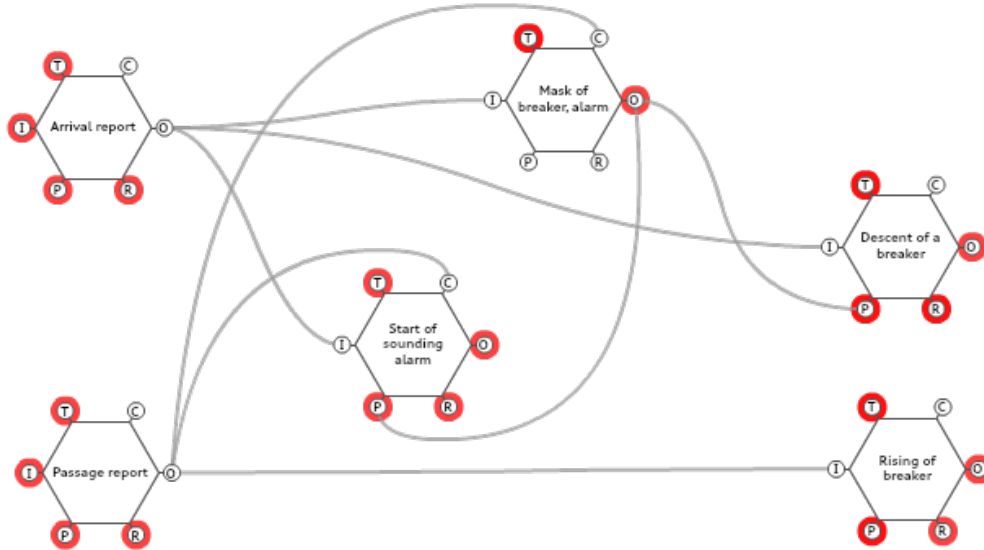


Figure 2: Railload crossing

The results of hazard analysis using keywords for each aspect of each function of this model are Figure 3 to Figure 8. The severity level defines a dangerous condition as 9, an unfavorable condition as 5, and a state as avoidance as 1.

		Not providing				providing causes hazards				too early / too late				stop too soon / Applying too late				
		Deviation	Local influence	Global influence	Severity	Deviation	Local influence	Global influence	Severity	Deviation	Local influence	Global influence	Severity	Deviation	Local influence	Global influence	Severity	
Arrival report	input	There is no input	The function does not start, it does not report arrival	train reaches the railroad crossing with alarm and breaker not functioning	9	Misrecognition as if there is input	Function starts without input	Although the train is not approaching, the railroad crossing starts functioning	5	Input is too late	Function start slow	-/The train reaches before the railroad crossing works	-/9	Input dose not stop	Input dose not stop	Alarm and breaker always function	-/5	
	output	Do not output	Dose not report arrival	train reaches the railroad crossing with alarm and breaker not functioning	9	Output is done arbitrarily	Although the train didn't arrive, the approach notification is done	Although the train is not approaching, the railroad crossing starts functioning	5	Output is too late	Output is slow	The train reaches before the railroad crossing works	-/9	Output dose not stop	Output dose not stop	Alarm and breaker always function	-/5	
	precondition	Precondition are not met	Since the sensor isn't provided, the function does not start	train reaches the railroad crossing with alarm and breaker not functioning	9	It is recognized that the prerequisite is not satisfied, but it is satisfied	It recognizes that the precondition is satisfied though it isn't satisfied, and the function starts	Since this function tries to operate when the sensor is not working, it can't detect the approach of the train	9									
	resource	resource are not provided	Since the sensor does not work, it is impossible to detect the train	The approach of the train can't be detected and it reaches the railway crossing without the railroad crossing working	9	Misrecognition as is there is resource	Since it is recognized that resources exist, the function tries to work but it does not work	The approach of the train can't be detected and it reaches the railway crossing without the railroad crossing working	9	Resource consumption is too early	Resource consumption is fast, it stops functioning/-	The approach of the train can't be detected and it reaches the railway crossing without the railroad crossing working/-	9/-					
	control																	
	time									Time restriction is too early / late	Function starts late after receiving input	The train reaches before the railroad crossing works	-/9					

Figure 3: Arrival report

Passage report	input	There is no input	Function dose not work	The railroad crossing keeps functioning even after passing through the train	5	Misrecognition as if there is input	It detects the passage while there is no input	Before the passage of the train, the railroad crossing will stop	9	Input is too late	Function start slow	It takes time for the railroad crossing to stop after passing the train	-/1	Input dose not stop	Input dose not stop	Since the passage notification is always sent, the railroad crossing stops immediately	-/9	
	output	Do not output	Dose not report passage	The railroad crossing keeps functioning even after passing through the train	5	Output is done arbitrarily	Notify that the train passed though it has not passed	Before the passage of the train, the railroad crossing will stop	9	Output is too late	Output is slow	It takes time for the railroad crossing to stop after passing the train	-/1	Output dose not stop	Output dose not stop	Since the passage notification is always sent, the railroad crossing stops immediately	-/9	
	precondition	Precondition are not met	Since the sensor isn't provided, the function does not start	The railroad crossing keeps functioning even after passing through the train	5	It is recognized that the prerequisite is not satisfied, but it is satisfied	Even though there is no sensor, it is recognized as having a sensor	The railroad crossing keeps moving because the function operates though the sensor does not work	5									
	resource	resource are not provided	Since the sensor does not work, it is impossible to detect the train	The railroad crossing keeps functioning even after passing through the train	5	Misrecognition as is there is resource	It is recognized that resources exist even though there is no resource	The railroad crossing keeps moving because the function operates though the sensor does not work	5	Resource consumption is too early	Resource consumption is fast, it stops functioning	Since passage is not detected, railroad crossing does not stop	5/-					
	control																	
	time									Time restriction is too early / late	Function starts late after receiving input	It takes time for the railroad crossing to stop after passing the train	-/1					

Figure 4: Passage report

Descent of a breaker	input	There is no input	Since the arrival report of the train doesn't arrive, it doesn't work.	The train reaches the railroad crossing without the breaker falling	9	Misrecognition as if there is input	Approach notice arrives even though it is not approaching	Although the train did not arrive, the interrupter has gone down	5	Input is too late	Function start slow	The train reached before the breaker fell down	-/9	Input dose not stop	Input dose not stop	The breaker is always in a state of descending	-/5	
	output	Do not output	Cross breaker does not descend	The train reaches the railroad crossing without the breaker falling	9	Output is done arbitrarily	Output arbitrarily	Although the train did not arrive, the interrupter has gone down	5	Output is too late	Output is slow	Since the start of descent is too late, the train reaches before the breaker falls	-/9	Output dose not stop	Stop before completing output/Continue to output even after completion of output	The train arrived at the railroad crossing without the breaker completing the descent/ Breaker further lowers from lowered position	9/1	
	precondition	Precondition are not met	No interrupter, no controller, so it will not work	The train reaches the railroad crossing without the breaker falling	9	It is recognized that the prerequisite is not satisfied, but it is satisfied	Even though the precondition is not established, it is recognized as establishment and the function operates	It is actually masked and the breaker does not descend	9									
	resource	resource are not provided	Function does not work because resources do not exist	The train reaches the railroad crossing without the breaker falling	9	Misrecognition as is there is resource	Recognizing that there are resources but no resources, the function works	I try to lower the circuit breaker, but the train arrives without the breaker falling	9	Resource consumption is too early	Resource consumption is fast, it stops functioning	The train reached the railway crossing without the breaker falling	9/-					
	control time									Time restriction is too early / late	Function starts late after receiving input	Before the breaker completes its descent, the train reaches the railroad crossing	-/5					

Figure 5: Descent of a crossing gate

Start of sounding alarm	input	There is no input	Since the arrival report of the train doesn't arrive, it doesn't work.	The train reaches the railway crossing without the alarm sounding	9	Misrecognition as if there is input	Approach notice arrives even though it is not approaching	Even when the train does not come, the alarm sounds	5	Input is too late	Function start slow	Before the alarm sounds, the train reaches	-9	Input dose not stop	Input dose not stop	Even if the train does not come, the alarm keeps ringing	-9	
	output	Do not output	The alarm does not sound	The train reaches the railway crossing without the alarm sounding	9	Output is done arbitrarily	Although the train is not approaching, the alarm sounds	Even when the train does not come, the alarm sounds	5	Output is too late	Output is slow	Before the alarm sounds, the train reaches	-9	Output dose not stop	Stop before completing output/Continue to output even after completion of output	Before the train passes, the alarm stops/Even if the train does not come, the alarm keeps ringing	9	
	precondition	Precondition are not met	Prerequisites are not met and do not work	The train reaches the railway crossing without the alarm sounding	9	It is recognized that the prerequisite is not satisfied, but it is satisfied	Even though the precondition is not established, it is recognized as establishment and the function operates	Even if alarm try to ring, it does not ring and the train reaches	9									
	resource	resource are not provided	Function does not work because resources do not exist	The train reaches the railway crossing without the alarm sounding	9	Misrecognition as is there is resource	Recognizing that there are resources but no resources, the function works	Even if alarm try to ring, it does not ring and the train reaches	9	Resource consumption is too early	Resource consumption is fast, it stops functioning	Even if the train comes close, the alarm does not ring	9					
	control	control signal are not provided	Function does not stop because it does not receive passage notification	The alarm does not stop even if the train passes	5	Misrecognition as is there is control signal	Receive passage notification before passing train, stop function	Ring stops even though the train has not passed	9	Control signal is too late	Train passing notification is early/ Since the notification is delayed after passing through the train, the output is delayed	Stop ringing before train passes/After passing for a while, it stops ringing	9	control signal dose not stop	As the passage notification continues, always stop the ringing	Since the passing notification does not stop, the alarm does not sound	-9	
	time									Time restriction is too early / late	Function starts late after receiving input	Before the alarm sounds, the train reaches	-9					

Figure 6: Start of sounding alarm

Rising of breaker	input	There is no input	Since the passage report of the train doesn't arrive, it doesn't work.	Even if the train passes through, the interrupter will not rise	5	Misrecognition as if there is input	Passage notice arrives even though it is not passed	The breaker will rise before passing through the train	9	Input is too late	Function start slow	After a while after passing through the train, the breaker rises	-1	Input dose not stop	Input dose not stop	Continue to recognize passage notifications, breakers are constantly rising	-9	
	output	Do not output	Cross breaker does not rise	Even if the train passes through, the interrupter will not rise	5	Output is done arbitrarily	Output arbitrarily	The breaker will rise before passing through the train	9	Output is too late	Output is slow	After a while after passing through the train, the breaker rises	-1	Output dose not stop	Stop before completing output/Continue to output even after completion of output	After passing through the train, the breaker stops half way up/Despite the rise of the breaker is completed, it does not stop	5	
	precondition	Precondition are not met	No interrupter, no controller, so it will not work	Even if the train passes through, the interrupter will not rise	5	It is recognized that the prerequisite is not satisfied, but it is satisfied	Even though the precondition is not established, it is recognized as establishment and the function operates	After passing through the train, I try to operate the breaker but it does not rise	5									
	resource	resource are not provided	It is recognized that there is no power supply and the breaker can not be raised	Even if the train passes through, the interrupter will not rise	5	Misrecognition as is there is resource	Recognizing that there are resources but no resources, the function works	After passing through the train, I try to operate the breaker but it does not rise	5	Resource consumption is too early	Resource consumption is fast, it stops functioning	Crossing raise can not be done after passing the train	5					
	control																	
	time									Time restriction is too early / late	Late start of function, long until function is completed	After a while after passing through the train, the breaker rises	-1					

Figure 7: Rising of crossing gate

Mask of breaker, alarm	input	There is no input	Since the arrival report of the train doesn't arrive, it doesn't work.	When multiple trains approach each other, overlapping railroad crossings occur	1	Misrecognition as if there is input	Approach notice arrives even though it is not approaching	The train reached the railroad crossing with masked and railroad crossing not working	9	Input is too late	Function start slow	A railroad crossing may function in duplicate when multiple trains come	-/1	Input dose not stop	Approach notifications are continuously made and continue masking	Since the mask is continued, the railroad crossing disappears	-/9	
	output	Do not output	No mask is done	When multiple trains approach each other, overlapping railroad crossings occur	1	Output is done arbitrarily	Output arbitrarily	The train reached the railroad crossing with masked and railroad crossing not working	9	Output is too late	Output is slow	A railroad crossing may function in duplicate when multiple trains come	-/1	Output dose not stop	Mask release is quick, railroad crossings tend to overlap and try to function./ Keep on masking, railroad crossing does not work	A railroad crossing tries to function in duplicate when there are multiple trains/ Railroad crossing does not work if the train arrives again after passing through	1/9	
	precondition																	
	resource																	
	control	control signal are not provided	There is no passing notification, so mask can not be released	Next time the train came, the railroad crossing did not work, the train reached the railroad crossing	9	Misrecognition as is there is control signal	Mask function is canceled arbitrarily, overlapping railroad crossing trying to function	When multiple trains arrive, the railroad crossing tries to function in duplicate	1	Control signal is too late	Passing notification is late, output is slow, function start is late after passage notification	Next time the train came, the railroad crossing did not work, the train reached the railroad crossing	-/9	control signal dose not stop	The passage notification does not stop, mask release continues to be done	Because mask release is done, when multiple trains come, railroad crossings overlap and operate	-/1	
time									Time restriction is too early / late	Mask start too early, masking even the function of railroad crossing starts./The start of masking is late, and overlapping railroad crossing tries to function	A mask was done before the railroad crossing operated, and the train reached the railroad crossing without operating/ A railroad crossing tries to operate in duplicate	9/1						

Figure 8: Mask of crossing gate, alarm

As a result of comparing the results analyzed by FRAM/STPA and those analyzed by STAMP/STPA, FRAM / STPA had overlooked hazards related to some components. The reason why FRAM/STPA overlooked them is because the modeling unit is different. In STAMP / STPA, we modeled each component of the system. In FRAM / STPA, modeling is done for each function, so I overlooked the relevant hazard of the component. The hazard which could not be found specifically is Table 2.

Table 2: New Hazard detected by FRAM/STPA(Figure 6)

		Providing causes hazard			
		Deviation	Local Influence	Global Influence	Severity
Start of sounding alarm	input	Input is too late	Input is late to come	Before the alarm sounds, the train reaches	9
	output	Output is too late	Output is slow		9
	time	Time restriction is too late	Function starts late after receiving input		9

It was possible for FRAM/STPA to detect new hazards that could not be found by STAMP/STPA. Specifically, it is a hazard related to the reaction speed of the function and the processing time. The reason why we detected new hazards is because the object being analyzed is different. In STAMP / STPA, deviations are analyzed only for control actions and feedback, but the analysis procedure of internal behavior of components is not clearly defined. In FRAM, we modeled the behavior of the function, so we were able to discover internal hazards which STAMP/STPA could

not detect. In addition, hazards to aspects such as resources and preconditions were able to be newly detected by FRAM/STPA. Some of the newly discovered hazards are shown in the Table 3.

Table 3: Hazard that FRAM/STPA missed (reference from [4])

	Providing causes hazard
Start of sounding alarm	Mask on different sensors, railroad crossing does not work
Mask release instruction	Unmask the different sensors, overlap railroad crossings and operate

Since it is functional level modeling, we missed component related hazards. We believe that hazard analysis such as component relation is added additionally when components decides, hazards can be analyzed comprehensively by reinforcing it.

## 4.2 Lane Changing - new keywords -

The next analysis example is a scenario for lane changing of a car. In this scenario, the behavior performed when changing the lane on a highway or the like is defined as a function and modeled in FRAM. The functions are the six functions of "consider object around car", "check current position", "determine the empty space", "plan lane change", "adjust the speed and angle" and "readjust speed and angle". In actual operation, although functions will be performed in more detail, modeling was performed with this abstraction degree in consideration of ease of analysis. The modeling results are shown in Figure 9.

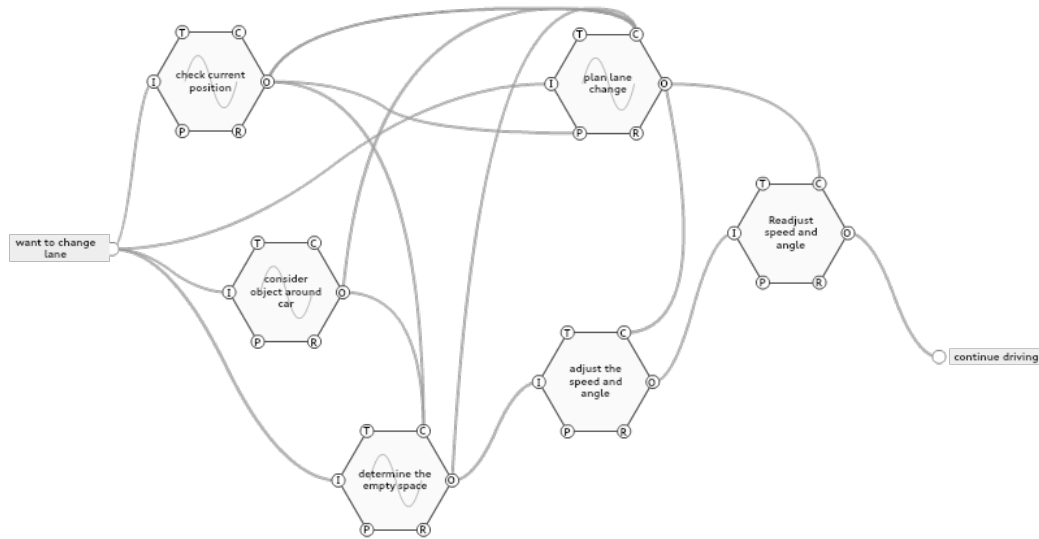


Figure 9: Lane change

The results of hazard analysis using keywords for each aspect of each function of this model are Figure 10 to Figure 14. As in the case of a railroad crossing, the severity level is defined as 9 for dangerous situations, 5 for unfavorable conditions, and 1 for avoidance. In this analysis of FRAM/STPA, hazard analysis using newly added keywords "too much" and "too little" is also carried out.

Lane Change																									
		Not providing				providing causes hazards				too early / too late				stop too soon / Applying too late				Too much				less			
		Deviation	Local Impact	Global Impact	Severity	Deviation	Local Impact	Global Impact	Severity	Deviation	Local Impact	Global Impact	Severity	Deviation	Local Impact	Global Impact	Severity	Deviation	Local Impact	Global Impact	Severity	Deviation	Local Impact	Global Impact	Severity
check current position	input	There is no input	Function dose not work	Can't grasp my position and can't make an accurate plan	5	Misrecognition as if there is input	Function starts without input	I plan to change lanes even where I don't need lane change	7	Input is too late	Function start slow	Late lane change from the beginning	7	Input dose not stop	Input dose not stop	I always check my position and send it	1								
	output	Do not output	Function dose not output	Can't transmit my position and can't make an accurate plan	5	Output is done arbitrarily	Send the location information without permission	I plan to change lanes even where I don't need lane change	7	Output is too late	Output is slow	Late lane change from the beginning	7	Output dose not stop	Output dose not stop	Output is always performed and old information is transmitted	9								
	precondition	Precondition are not met				It is recognized that the prerequisite is not satisfied, but it is satisfied																			
	resource	resource are not provided				Misrecognition as is there is resource					Resource consumption is too early														
	control	control signal are not provided				Misrecognition as is there is control signal					Control signal is too late				control signal dose not stop										
	time										Time restriction is too early / late														
consider object around car	input	There is no input	Do not start surrounding object recognition	I can't plan because there is no information around the car	5	Misrecognition as if there is input	Function starts without input	Send the surrounding information	5	Input is too late	Function start slow	Late lane change from the beginning	7	Input dose not stop	Input dose not stop	I always send the surround information	1								
	output	Do not output	Do not send surrounding information	I can't plan because there is no information around the car	5	Output is done arbitrarily	Send the object information around car without permission	Continue sending old surrounding information	5	Output is too late	Output is slow	Late lane change from the beginning	7	Output dose not stop	Output dose not stop	Continuing to transmit the surrounding situation, even if the surrounding situation changes, and make dangerous lane change	9								
	precondition	Precondition are not met				It is recognized that the prerequisite is not satisfied, but it is satisfied																			
	resource	resource are not provided				Misrecognition as is there is resource					Resource consumption is too early														
	control	control signal are not provided				Misrecognition as is there is control signal					Control signal is too late				control signal dose not stop										
	time										Time restriction is too early / late														

Figure 10: check current position & consider object around car

Lane Change																										
determine the empty space	input	There is no input	Do not start checking empty space	Can't find an empty space and can't make an accurate plan	5	Misrecognition as if there is input	Function starts without input	Recognize the empty space and start unintentional lane change	5	Input is too late	Function start slow	Decision of empty space is delayed, lane change can't be made at the scheduled position	7	Input dose not stop	Input dose not stop	Continue to send empty space	1									
	output	Do not output	Do not send empty space	Can't find an empty space and can't make an accurate plan	5	Output is done arbitrarily	Send the empty space without permission	Recognize the empty space and start unintentional lane change	5	Output is too late	Output is slow	The determined empty space changes before outputting, resulting in a dangerous situation	7	Output dose not stop	Output dose not stop	Continue sending empty space but do send as old information and do dangerous lane change	9	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	
	precondition	Precondition are not met				It is recognized that the prerequisite is not satisfied, but it is satisfied																				
	resource	resource are not provided				Misrecognition as is there is resource																				
	control	control signal are not provided	Information used for functioning is not provided	There is insufficient information to determine the empty space, so planning can't be done	5	Misrecognition as is there is control signal	A control signal is unintentionally provided	Inaccurate information is entered and false recognition of empty space	9	Control signal is too late	The control information required to function is slow, the output becomes slow	Decision of empty space is delayed, lane change can't be made at the scheduled position	7	control signal dose not stop	Continue to receive control signal	Continue sending empty space but do send as old information and do dangerous lane change	9									
	time										Time restriction is too early / late															

Figure 11: determine the empty space





In the hazard analysis of lane change, we found several hazards regarding accuracy. Actual fluctuation has magnitude of fluctuation. The results obtained in this analysis are situations when large fluctuations occurred. However, besides the dangerous situation caused by maximum fluctuations, there is a slight change in situation due to small fluctuations. The future task is how to analyze the small change and change. To analyze how the system will be affected when several fluctuation are combined is also future work.

Finally, as FRAM / STPA analyzes deviations from models describing behavior of ideal functions, measures can be taken that do not deviate, and system updates and improvements are possible. Therefore, this method is considered to be suitable for FRAM usage method.

## 6 Conclusion

The method proposed in this paper FRAM/STPA is a method for performing hazard analysis in the upstream process of system design. In this method, focusing on FRAM's modeling in function units, it is a hazard analysis method that can analyze hazards existing in the system before designing actual structures etc. in designing. In addition, it is possible to discover hazards when fluctuation occurred by analyzing the fluctuation of functions defined in FRAM using several keywords. Also for FRAM/STPA, after the structure of the system has been determined, additional analyzes can be allowed to overlook the risks associated with the structure. After structure determination, it is enough to analyze by focusing on the hazard regarding the structure, so the workload decreases.

In the future, FRAM/STPA will be implemented for more system analysis and we will show the usefulness of this method.

## References

- [1] Riccardo Patriarca, Giulio Di Gravio, and Francesco Costantino. A monte carlo evolution of the functional resonance analysis method (fram) to assess performance variability in complex systems. *Safety Science*, 91:49 – 60, 2017.
- [2] Ditte Caroline Raben Mogensen. Identification of leading indicators in healthcare processes - developing a method. [https://centerforkvalitet.dk/wp-content/uploads/2017/11/Ph.d.-thesis-including-articles\\\_II.pdf](https://centerforkvalitet.dk/wp-content/uploads/2017/11/Ph.d.-thesis-including-articles\_II.pdf).
- [3] Paulo Victor Rodrigues de Carvalho. The use of functional resonance analysis method (fram) in a mid-air collision to understand some characteristics of the air traffic management system resilience. *Reliability Engineering & System Safety*, 96(11):1482 – 1498, 2011.
- [4] Keijiro Araki, editor. *First time STAMP/STPA(in japanese)*. Information-technology Promotion Agency, Japan, 3 edition, 10 2017.

- [5] NANCY LEVESON and JOHN THOMAS, editors. *STPA HANDBOOK*. NANCY LEVESON AND JOHN THOMAS, 3 edition, 10 2018.