Applying STAMP/STPA to Human Safety System for Four Wheel Drive Power-train

Yasuhiko Kawabe, **Tatsuya Yanagisawa**

UNIVANCE CORPORATION
2418 Washizu, Kosai-city, Shizuoka-Pref., 431-0494 Japan
yasuhiko.kawabe@champ.uvc.co.jp
tatsuya.yanagisawa@champ.uvc.co.jp

Abstract: We have been using FT or FMEA…etc to design our new products till now. In this study, we find that the new vehicle product development can be more efficient if we adopt STAMP/STPA, which shows the complicated relationship between human and machine and feedback the hazard in an early development stage.

1 Background

After the Great East Japan Earthquake happening on March 3rd, 2011, our company kept pressing forward with the evaluation and the preventive measures of Safety Risk. In particular, among the automobile drive parts, there are many parts needing gas carburization and quenching, which requires flammable gas. In order not to cause explosion or fire while the accident happens, we pushed forward the risk assessment and confirmed the effectiveness of using STAMP/STPA method. And we reported our work at the 2014 STAMP Conference. [Mn14]

Taking this occasion, UNIVANCE CORPORATION attempts to apply STAMP/STPA on the 4WD systematic safety planning and embed the safety management in the future products at the developing stage. Here, we are going to introduce how we build the scheme of development in this paper.

UNIVANCE CORPORATION's self-developed transfer case is equipped in the "GTR," which is the flagship 4WD vehicle of NISSAN Motors. Until now, it has also developed the 4WD systems of other vehicle manufacturers.

Different from ISO26262 [ISO11], which regulates the minimum safety of the individual components and became a great issue of concern recently, we adopted the idea of STAMP/STPA, which focuses on the safety of the whole system including the complicated relationship between human and machine.

We focus on the concept of "human factors" within STAMP/STPA method, in order to consider "the way of developing 4WD driving system within the vehicle automatic control function" and "the system safety of product development" at early stage of the development.

2 Applying STAMP/STPA

2.1 The characteristics of STAMP/STPA and this study

The STAMP/STPA is introduced by MIT Professor Nancy Leveson, the writer of " Engineering a Safer World." [Ln11] This methodology proves that even though there is no defect in the individual sub-systems or components, the defect will still occur while the whole system is built up by them.

Under the circumstance of the road traffic network nowadays, to drive the vehicle by automatic control completely is still under study. For the vehicles equipped with 4WD system, times of driving in the natural circumstance are more than the other vehicles. For example, although the high speed 4WD vehicles are supposed to run on the pavement, most drivers expect them to run in the complicated road conditions into which many natural conditions are added into, such as snowy roads or frozen roads…etc. Therefore, we think the product development which includes human recognition is necessary during the early stage of the product planning. And then, we move ahead on our study based on the cases which is related to human factors and were presented at the 2014 STAMP Conference. In this study, we attempt to explore this concept in depth.

First of all, STAMP/STPA has the following characteristics.

- Focusing on the system-level issues: considering the interactions between the controllers, but not only on the malfunctions of the individual components.

- Considering the accident is not caused only by the malfunction of the component, but caused by that the safety constraint toward "Unsafe Control Action" which leads to dangerous status is not practiced.

- Emphasizing that safety constraint should be recognized and embedded in the design, but not only the malfunction countermeasures, such as fault tolerance design.

- The cause of the accidents due to the software or human factors is that the process which the controller's supposition is inconsistent with the actual process.

- The unsafe control actions and the hazard factors can be analyzed by Guide Words.

Among these characteristics of STAMP/STPA method, we focus on the 4th one, and integrated STAMP/STPA into the thinking at the early stage of development.

2.2 Analyzing methodology which integrate the human behavior into the STAMP/STPA

The STAMP/STPA is Practiced according to the following steps.

- Recognition of the hazard and the high-level safety requirement.
- Building the Control Structure Diagram to control the hazard.(Step 0)

- Recognizing the hazard scenario caused by impropriate control action. (Step 1)
- Recognizing the potential cause that leads to hazard scenario. (Step 2)

In this study, in order to add in the human error factors, we refer to the Dr. Jens Rasmussen's "Skills, Rules, Knowledge (SRK) framework" [Rj90] which is mentioned in the presentation of Hoshino from Japan Manned Space Systems Corporation (JAMMS) at the 2014 STAMP/STPA Conference. This model shows the rule or mechanism which works in the process of recognition. It presents the real-life problems with all kinds of factors which correlated to one another complicatedly in the cognitive science.

Rasmussen states that when human practices a certain behavior, from a prospective of consciousness, that behavior is also being automated at the same time. And, the automation will be effected by the following 3 recognition levels.

- Skill-based behavior: Performance is smooth, automated, and consists of highly integrated patterns of behaviour in most skill-based control. [Rj90]
  ⇒it is practiced without intention, and sometimes a reflex movement.
- Rule-based behavior: Characterised by the use of rules and procedures to select a course of action in a familiar work situation. [Rj90]
  ⇒we can also shift this behavior to skill-based behavior by repeating practicing.
- Knowledge-based behavior: By identifying the environment, building up the psychological model and finding the countermeasures from the knowledge which one has already had.
  ⇒needed at complicated and ambiguous environment.

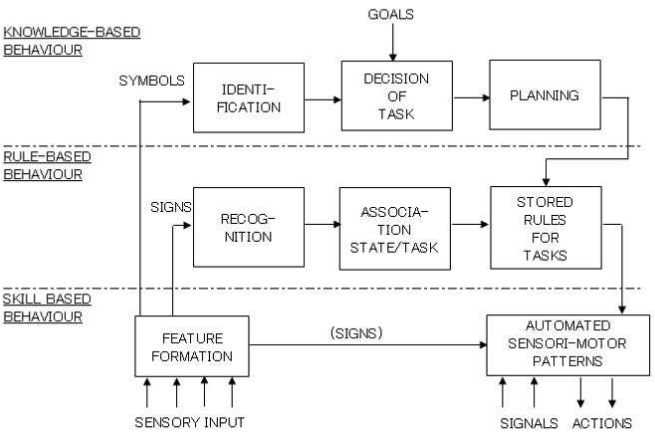

Figure 1 · The relation of the 3 Behavior Layers

The advantage of the model showed in the figure above is that it makes it possible to recognize or realize the interface behavior of the user and to find out the factors which cause human error. And then, it makes it possible to prevent the human error by improving the interface.

According to the statement of Hoshino from JAMSS(Japan Manned Space Systems Corporation), the process of human recognizing behavior can be divided into the following 4 items:

- Detection
- Identification
- Decision
- Action

And then, he divides every error pattern in each level defined by Rasmussen into 4 items.

Table 1 shows how the Human Mental Model analysis is conducted.

Layer	Process			
	①Detection	②Identification	③Decision	④Action
(1)SKILL-BASED BEHAVIOR				
(Ⅱ)RULE-BASED BEHAVIOR				
(Ⅲ)KNOWLEDGE-BASED BEHAVIOR				

Table 1. The idea of Human Mental Model analysis

3 Result of analysis

3.1 Applying to product developing

We suppose that if we can find out the conditions precedent that cause the system of 4WD vehicle to collide with the human behavior, then we will be able to build up a system which can automatically avoid the accident effectively. Under this assumption, we try to find out the collision between human and the system by the following condition which happens in 2 or 3 seconds.

Usually, it is necessary to consider the oncoming vehicle. However, because the purpose of this study is about the product development, we assume that there is no oncoming car. (One way, no car coming from the opposite direction)

① The start point is on a dry pavement. The vehicle can speed-up without difficulty.

② Suddenly, the snowy road with a sharp corner is confirmed.

③ During the corner, it is confirmed that in the front, there is an extremely sharp corner which concaves oppositely.

④ After passing the crowning point (clipping point), cornering out.

⑤ After that, in order to get into the next sharp corner, the driver turns the steering wheel to the end.

We suppose that if the driver is not a professional driver, the movement of the vehicle will spin out because of understeer.

This might be a rear case in US, but it exits in Europe or Asia where it snows. Figure 2 illustrates the situation above.

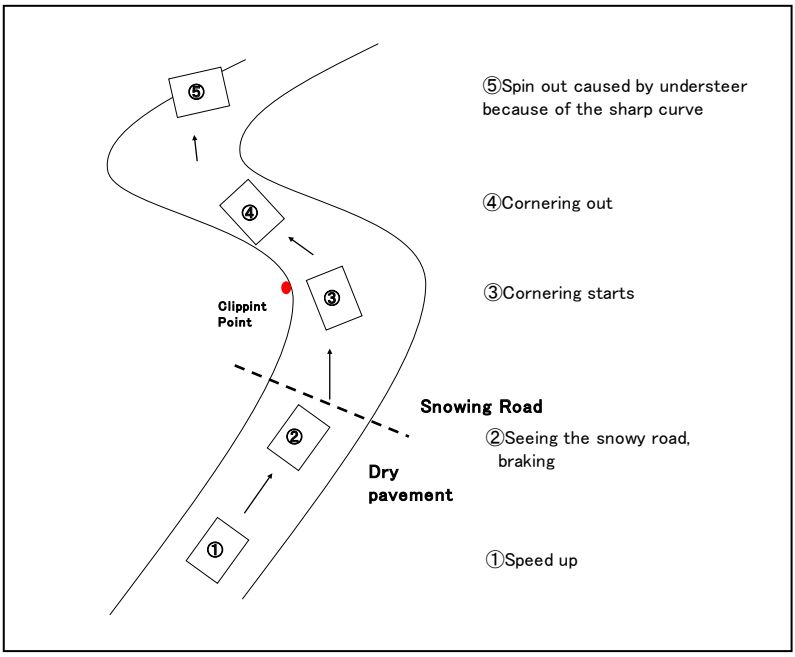

Figure 2 The situation of the road and driving conditions

Under this kind of situation, the following systematic control is necessary.

① Start moving and speed up: 4WD system reaches the fastest situation and the front-back torque distribution is under control.

② Braking: Optimizing the braking force in order to prevent the lock of the wheels.

③ Clipping point: Distributing the front-back torque in order to maximize the steering, acceleration, braking balance, and cornering force of the tires…etc. and increasing the stability.

④ Cornering out: Recovering the distribution of the front-back torque gradually and maintaining the balance of the vihecle.

⑤ Spin out caused by understeer: Entering the sharp curve again, and acting with the same logic as ③.

This kind of systematic control is programmed according to the driving features or experiences of the professional drivers. However, under the situation ⑤, it is too difficult for a normal driver. Therefore, we consider that the collision will occur between the systematic control and the driver's behavior here.

3.2 Analysis by STAMP/STPA

As we have mentioned above, what we want to talk about is "the secon sharp cuver on the snowy road." And we use STAMP/STPA to analyzed this situation.

3.2.1 Step 0 Control Structure

We have made the control structure diagram, considering the datum among the components which are related to the hazards.

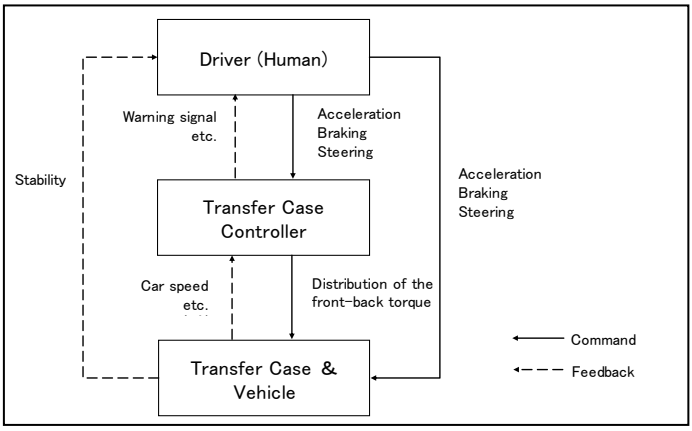

Figure 3 Control Structure Diagram

Here, we take the driver as one component and take the "transfer case controller" and the "transfer case & vehicle" which receive the command from the driver as the other two components. The commands from the driver are acceleration, brake, and steering…etc. While the transfer case controller receive the commands, it will compute the distribution of the front-back torque, and then send it to the transfer case & vehicle. After the transfer case & vehicle receive the commands from the driver and from the transfer case controller, it will practice the acceleration, brake, or turning, and provide the driver stability.

3.2.2 Step 1 Hazard senario analysis based on recognizing unsafe control action

We summarized the the general sequence of every command below.

#	Event / Command	from	to	Description
1	Acceleration	Driver	vehicle	Speed up
2	Acceleration	Driver	Transfer case controller	Compute the front-back torque
3	Steering	Driver	vehicle	Turing
4	Steering	Driver	Transfer case controller	Compute the front-back torque
5	Distributing the front-back torque	Transfer case controller	Transfer case & vehicle	Distributing the torque into front and back, increasing the connering force, in order to optimize the movement

Table 2 The general sequence of every command during a sharp curve

Once receiving the command #1, acceleration, and command #3, steering, the vehicle will speed up and turn in the same time. And, by command #2, acceleration, and command #4, steering, it will reach situation #5, in which the distribution of the front-back torque is worked out so that the "speed up & turning" becomes stable because of the distribution of the torque. Although all the commands are writen sequetially above, all of them happen in just 2 or 3 seconds.

Here, we analyze the unsafe control action of every command by aaplying the 4 guide words.

#	Event/Command	not provided	incorrectly provided	provided too early/late	stopped too soon
1	acceleration to vehicle	No hazard	become unstable, and then spin out (UCA1)	No hazard	No hazard
2	acceleration to controller	cannot compute the torque, but no hazard	cannot compute the torque, but no hazard	No hazard	cannot compute the torque, but no hazard
3	steering to vehicle	cannot steer correctly, and understeer + spin out (UCA2)	cannot steer correctly, and understeer + spin out (UCA2)	cannot steer correctly, and understeer + spin out (UCA2)	cannot steer correctly, and understeer + spin out (UCA2)
4	steering to controller	cannot compute the torque, but no hazard	cannot compute the torque, but no hazard	No hazard	cannot compute the torque, but no hazard
5	distributing the front-back torque	cannot increase the cornering force, and understeer + spin out (UCA3)	cannot increase the cornering force, and understeer + spin out (UCA3)	cannot increase the cornering force, and understeer + spin out (UCA3)	cannot increase the cornering force, and understeer + spin out (UCA3)

Table 3 Unsafe Control Action analysis

As shown in table 3, there are three kinds of unsafe control action.

UCA1: Becoming unstable, and then spin out. When it is time to speed up, if the steering or brake commands are incorrectly provided, the hazard occurs.

UCA2: Cannot steer correctly, and become understeer and spin out. If the adequate command (steering) is not provided at the adequate timing, the hazard occurs.

UCA3: Cannot increase the cornering force, and become understeer and spin out. If the torque of front and back is not distributed at the adequate timing, the hazard occurs.

3.2.3 Step 2 Analyzing the hazard factors by Control Loop

Among the unsafe control actions we have derived, we next focus on the UCA2 and practice the Control Loop analysis, because we want to focus on human behavior in this study.

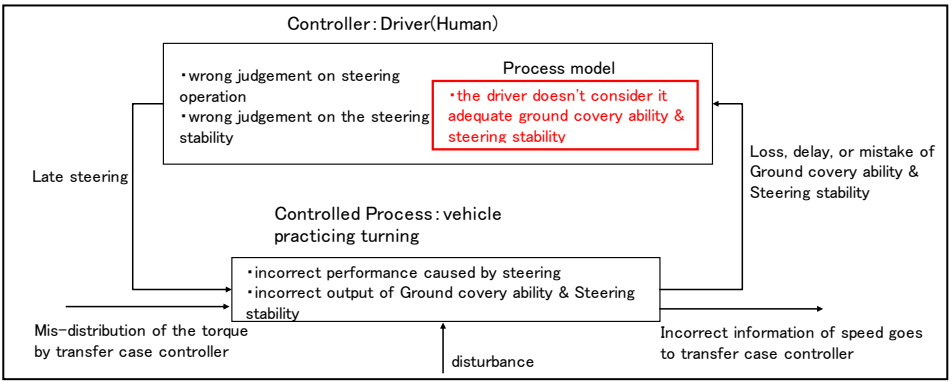

Figure 4 The analysis of hazard factors by control loop diagram

As shown in Figure 4, many hazard factors are found. According to the general process of STAMP/STPA, the safety countermeasures should be made for every hazard factor. However, because we focus on human behavior in this study, we only discuss the part that is relative to the driver(human). That is, we will analyze why the driver doesn't consider it adequate ground covery ability & steering stability.

3.2.4 Human Mental Model analysis

We use the Human Mental Model, which is mentioned in 2.2, to analyze.

Layer	Process			
	①Detection	②Identification	③Decision	④Action
(1)SKILL-BASED BEHAVIOR	(1a)mis-consider it as a gentle curve (1b)cannot judge if it is snow or ice road	N/A	N/A	(4a)speed up incorrectly (4b)fail to turn the steering wheel
(Ⅱ)RULE-BASED BEHAVIOR	(1a)mis-consider it as a gentle curve (1b)cannot judge if it is snow or ice road	(2a)cannot figure out that he should turn the steering wheel to the end and press the acceleratinopedal	(3a)because of fear, the driver judges that he should press the brake pedal and return the steering wheel	(4a)speed up incorrectly (4b)fail to turn the steering wheel
(Ⅲ)KNOWLEDGE-BASED BEHAVIOR	(1a)mis-consider it as a gentle curve (1b)cannot judge if it is snow or ice road	(2b)press the brake pedal because of the snowy road	(3a)because of fear, the driver judges that he should press the brake pedal and return the steering wheel	(4a)speed up incorrectly (4b)fail to turn the steering wheel

Table 4 the result of Human Mental Model analysis

If the driver is not a professional driver, he will take the (Ⅱ) RULE-BASED BEHAVIOR or (Ⅲ) KNOWLEDGE-BASED BEHAVIOR. And the process that may lead to the hazard will fall on Identification or Decision.

Each process which is necessary for the system control is as following.

A. Detection: Recognize there is a sharp curve again.

B. Identification: Identify that he should turn the steering wheel to the extreme and press the acceleration pedal.

C. Decision: Even the speed is high, “B” still works out.

D. Action: Turn the steering wheel to the extreme and press the acceleration pedal.

And then, we try to make the countermeasure for each situation.

ID	Causal Factor	Safety Constraints
(2a)	Cannot figure out that he should turn the steering wheel to the end and press the acceleratinopedal	For general drivers, it is difficult to complete the process in such a short time. Therefore, ESC(Electronic Stability Control) should be equipped.
(2b)	Press the brake pedal because of the snowy road	
(3a)	Because of fear, the driver judges that he should press the brake pedal and return the steering wheel	

Table 5 Countermeasure

For the general drivers, it is difficult to practice the process that the system does. However, due to the safety reason, we cannot just modify the behavior of the driver directly, but should try to prevent the event. Therefore, we decide to equip the vehicle with ESC (Electronic Stability Control) to monitor the yaw rate gyro and ensure the running stability.

Although we conclude with the countermeasure above, we are also considering the “auto-drive” concept that makes everyone be able to carry out the process that the systematic control attempt to pratice.

3.3 Safety countermeasure based on the method in the past

Naturally, the safety countermeasures are adopted in the development of vehicles, including GT-R etc. In the vehicle indutry, QFD (Quality Function Deployment) [IK98] [ONF98], including FT or FMEA, is applied. About the “spin out caused by understeer” issue which we discussed about this time, the safety countermeasure has already been made by the method in the past. Especially, the result of ESC equipment, which is derived from STAMP/STPA, is completely the same to the one which is derived from the method in the past.

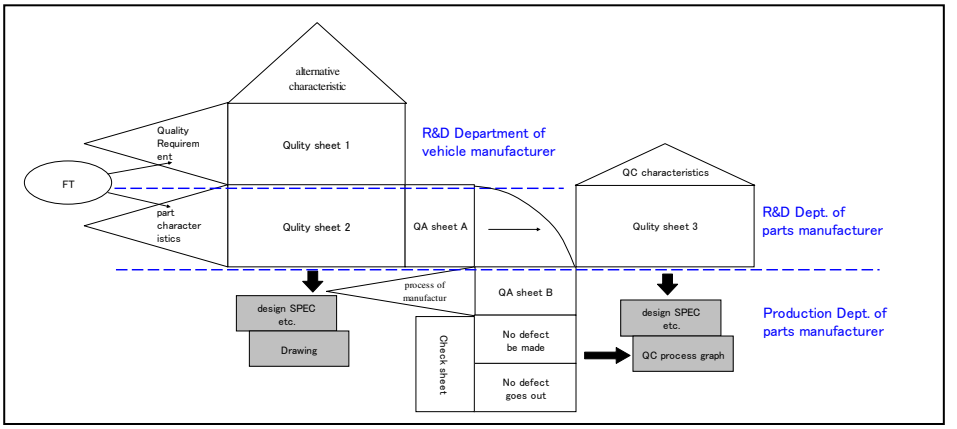

Figure 5 The procedure of QC based on QFD

By adopting the procedure shown in Figure 5, the design department receives the request from the customer and make instructions. Then, the production department or the suppliers receive that instructions and function smoothly to meet the customer's needs. Here, the R&D Dept. of vehicle manufacturer issues the quality sheet 1, and the parts manufacturers make quality sheet 2, and then QA sheet A, QA sheet B…etc. The vehicle's unique sales point, or the safety design concept is defined in the quality sheet 1. Here, we want to focuss on the quality sheet 1 because it acts as the STAMP/STPA analysis we performed in this paper.

Alternative characteristic / Quality required					characteristic	Initial		Durability				Appearance				
								heat		quiet						
						××××	××××	××××	××××	××××	××××	××××	××××	××××		
					value	○○kg	○○kg	○○kg	○○kg	○○kg	○○kg	△△	△△	△△		
product name	function	point (Quality)	Quality required (1)	quality reqired(2) detail		A	A	A	A	A	A	B	B	B		
Part A	To decorate ××	comfort	clean	the WAX powder won't stay on it									○	○		
		safety	hard to get hurt	won't get hurt even touching by hands	A							◎				
				nail won't get caught on when car was	A								○	○		
				clother won't get caught on	A								○	○		

Table 6 Sample of quality sheet 1

Table 6 shows a sample of qulity sheet, which is usually applied on product development, and the designer designs according to the detail value derived from the quality sheet or FT.

About the theme, spin out caused by understeer, the vertical axis should be:

- Characteristic(quality): safety, comfort

- Quality reqired(1): hard to get hurt, easy to drive
- Quality reqired(2): stable when acceleration or braking at the sharp curve

  stable when lane changing at the sharp curve

And the horizontal axis will be ESC and the alternative characteristics of the ECU.

This way, we can still consider the human level factors and conduct the safety design. However, if the person in charge is not well experienced, there may be miss in the FT graph, and it may take much time on breakdown all the detail characteristics.

4 Result and Observation

By STAMP/STPA, which can analyze the system including human behavior, we become able to find out the hazard faster than the methodology in the past. In the future, we attempt to stand on a higher safety point of view as the vehicle manufacturer to develop safest product. And, we also attempt to make people realise the importance of STAMP/STPA and push forward the standardization through these kind of product developing activities.

References

[Mn14] Morishita N.: Applying STAMP/STPA to Analyze the Cause of the Unexpected Fire Happening at the Heat Treatment Process, 2014 STAMP Workshop, 2014.

[ISO11] ISO26262-1:2011(en) Road vehicles-Functional Safety, ISO, 2011

[Ln11] Leveson, N.: Engineering a Safer World, Massachusetts Institute of Technology, 2011.

[Rj90] Rasmussen J.: Mental models and the control of action in complex environments. In D. Ackermann, D. & M.J. Tauber (Eds.). Mental Models and Human-Computer Interaction 1 (pp. 41-46). North-Holland: Elsevier Science Publishers. ISBN 0-444-88453-X

[IK98] Isobe, T.; Katagiri, S.: Quality Function Development concept for quality assurance, Advanced QFD Technology for Value Creation, Union of Japanese Scientists and Engineers, JUSE, 1998

[ONF98] Ooishi, T.; Negishi, M.; Furukawa, M.: Applied to the transmission of automotive and industrial vehicles, Advanced QFD Technology for Value Creation, Union of Japanese Scientists and Engineers, JUSE, 1998