# The 2nd Japanese STAMP Workshop Abstracts

## Nov.27 (Monday)

（1）Integration of Security into CAST ; Zurich University of Applied Sciences Christoph Senn, Carmen Frischknecht, Benjamin Contreras, Sven Krauss

（2）A Brief Survey of STAMP-based Hazard Analysis Tools ; National Institute of Technology, Sendai College. Keishi Okamoto

（3）IPA/SEC will provide a STAMP based hazard analysis tool i-STAMP(code name)

## Nov. 28 (Tuesday)

（4）Applying STAMP/STPA to project management focusing on motivation; University of Nagasaki, Shigeru Kusakabe

（5）Using STAMP/STPA focusing on “freedom from interference” ; University of Nagasaki, Shigeru Kusakabe

（6）Review of STAMP/STPA case studies and explanation support of STPA process using GSN ; Nihon University. Taito Akiyama,

（7）Risk analysis of autonomous driving system using STAMP/STPA - confluence on highway ; Aichi Institute of Technology. Masatoshi Hori

（8）Risk Analysis of multi-purpose batch plants using STAMP/STPA ; Nagoya Institute of Technology. Shun Kondo

（9）STAMP/STPA Application Guide for Automotive ～From JASPAR Functional Safety WG Activity Result～ ; JASPAR. Yoshihiro Miyazaki

(10) STAMP/STPA with using system model ; Hitachi Industry & Control Solutions, Ltd. Takeo Hashimoto

(11) Prospect for availability of STAMP/STPA as safety analysis in international safety standards ; TOSHIBA CORPORATION. Hisashi Yomiya

(12) Safety Assessment of Closed-Loop Level Crossing Control Systems by Means of Systems-Theoretic Accident Model and Processes (STAMP) ; Kyosan Electric Mfg.Co.,LTD. Tetsuya Takata

(13) Application and extension of STAMP/STPA to Railway Signalling System ; East Japan Railway Company. Yusuke Takano

(14) A Proposal of The Refinement STPA Guide Words on Human Factor of Supervisory Control Systems for Safety (Security) Analysis of Automated Vehicles ; Hitachi, Ltd. Yasuhiko Nagai

(15) Safety analysis of level crossing obstruction detecting system using STAMP/STPA method ; East Japan Railway Company. Satoru Kitamura

(16) Safety requirement analysis of level crossing control system using STAMP/STPA method ; East Japan Railway Company. Takashi Kunifuji

(17) Hazard analysis for power assist bicycle/Comparison of STAMP/STPA and numerical simulation analysis ; The university of Aizu. Shigeru Kanemoto

(18) The STAMP/STPA method of intentions and requirements description level ; JFP Inc. Hiroshi Nakamura

(19) A Proposal to identify unsafe control actions in STAMP/STPA by simulation using State Transition Specification of Control Structure and guide word ; Osaka Institute of Technology. Yasuko Fukazawa

## Nov.29 (Wednesday)

(20) An idea how to derive Process Models based on Extending STPA ; Nihon Unisys Ltd. Yuko Fukushima

(21) A Study on STAMP and HAZOP in IoT and deep learning application ; Nagoya Municipal Industrial Research Institute. Kiyoshi Ogawa

(22) Verification of Cyber-Physical Systems Using STAMP / STPA ; Nihon Unisys, Ltd. Yoshitaka Aoki

(23) Suggestion of Risk Management Framework by using STAMP/STPA ; Information Services International-Dentsu, Ltd. Hoonhee Kim

(24) A rubber “STAMP” was analyzed using “STAMP” based Process Analysis ; OMRON Automotive Electronics Co.Ltd. Hajime Tamanaha

## (1) Title

Integration of Security into CAST

## Speaker, Authors

Zurich University of Applied Sciences  Christoph Senn, Carmen Frischknecht, Benjamin Contreras, Sven Krauss

## Abstract

Due to increasingly complex systems, the demand for safety and security has grown, while their realization has become even more difficult. Even though both fields, safety, and security, aim to create safe, reliable and secure systems, they are treated as different domains. Thus, the positive effect on systems created when methodologies of both domains are applied is completely underestimated.

The main objective of this work is to integrate security aspects into the STAMP methodology. Therefore, the incident from Dallas in spring 2017, in which a signal spoof attack set off the city's emergency sirens, is used as a case study to evaluate if CAST can be applied for security incident analysis. We are also analyzing the issue with the security vulnerabilities of modern cars applying a CAST analysis, a security-based analysis and a combination of both on the Jeep Cherokee model. Based on the results we want to show the feasibility of combining safety and security analyses in a methodical way. Adopting the WannaCry ransomware attack, which affected over 150 countries and infected more than 230'000 devices in May 2017, with special attention on the National Health Service(NHS) in the UK is used as a verification and feasibility example of our modulated methodology.

In parallel with the case studies, the methodology to integrate security into CAST is developed.

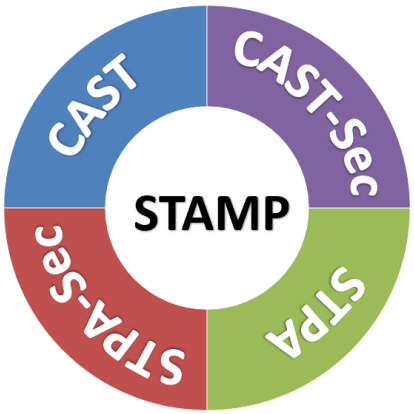



Figure 1 Cast-Sec as extension to the existing methodologies STPA, STPA-Sec and CAST.

## Keywords

(1) Security

(2) STPA

(3) CAST

## (2) Title

A Brief Survey of STAMP-based Hazard Analysis Tools

## Speaker, Authors

National Institute of Technology, Sendai College. Keishi OKAMOTO

## Abstract

STAMP(Systems-Theoretic Accident Model and Processes) is a new accident model, and STPA(System Theoretic Process. Analysis) is a STAMP-based hazard analysis method.

STPA is a systematic hazard analysis method. But it requires simple and tedious tasks. It is necessary to use a STAMP dependent data structures, e.g., a control action is assigned to a connection between components and a

process model is defined in a controller. It is also necessary to associate a control action in the control structure diagram with a control action to be analyzed in Step 1. By achieving these simple and tedious tasks manually, it is possible to conduct STPA using a generic drawing tool and a spreadsheet tool. However, by using a STAMP-based tool to support simple tasks, analysts can concentrate on essential analysis, thus some STAMP-based tools are developed.

In this presentation we give a brief survey of existing STAMP base-hazard analysis tools.

## Keywords

(1) STAMP/STPA

(2) STAMP- based Hazard Analysis Tools

(3) i-STAMP

## (3) Title

IPA/SEC will provide a STAMP based hazard analysis tool i-STAMP(code name)

## Speaker, Authors

IPA/SEC Shogo Ishii

## Abstract

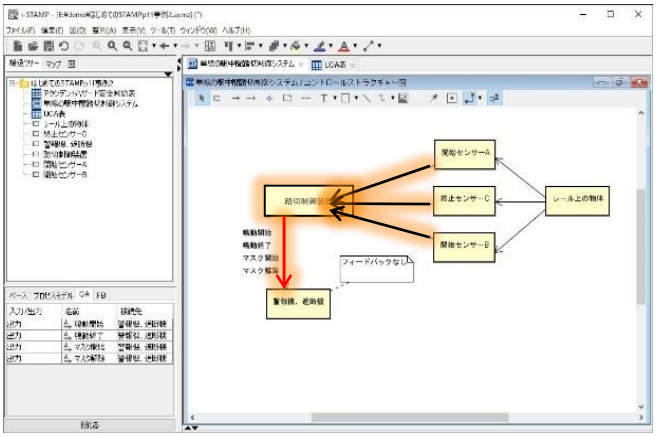
STAMP (Systems-Theoretic Accident Model and Processes) is the new concept that an accident occurs by the Emergent Properties of the system, and STPA (System Theoretic Process Analysis) is based on the STAMP and is the new hazard analytical method which focuses on the mutual interaction during components and specifies a hazard causal factor.

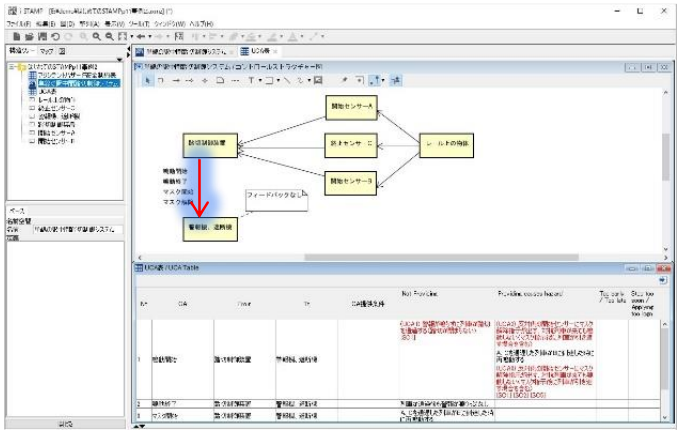
STAMP and STPA are a new concept and a new method. Therefore, the engineer who works on application of STAMP/STPA for the first time must research a STPA procedure in detail of what to do and how to do, and is annoyed to understand the essence of STPA procedure.
STAMP/STPA is the method to get free idea in an analysis. While analyzing, so the engineer perceives something new idea, and return to previous Step and often continue the analysis. That's a desirable thing to improve the comprehensiveness. On the other hand, it's necessary to renew tables/diagrams which were made at previous Step and analyze, and work of tables/diagrams renewal takes time and effort. That makes the efficiency of the analysis work fall. Thought will be stopped by tables/diagrams renewal work. It’s a big problem.

* It takes much time to understand analysis details of work and a procedure. Much experience is needed to analyze efficiently.

* Tables/diagrams creation and edit work are troublesome, and engineer can't concentrate on thought.

IPA thought these are hindrance of the STAMP spread, and thought STAMP support tool utilization was effective as the countermeasure for hindrance. Several STAMP support tools are also proposed overseas so far, and software of these tools are released as open source, and it can be used freely. But when IPA tried those tools out, it was difficult to say that the tool with which an analysis is supported. And it seems that these are tool to make a fair copy of an analyzed result, and the assumption user of these tools are the advanced level engineer about an analysis by STAMP or STAMP researchers. So IPA decided to develop an STAMP support tool which really support STAMP analysis and is useful even for the engineer of the beginner's course level who will try to introduce STAMP. We call this tool as i-STAMP (i-STAMP is a development codename). Engineer can enjoy the effect of the tool utilization, too. IPA will release software of i-STAMP as open source in March, 2018. Now We're advancing development of i-STAMP.





## Keywords

**(1) STAMP/STPA**

**(2) STAMP support tool**

**(3) IPA/SEC**

**(4) STPA step navigation**

**(5) Improving STPA work efficiency**

## (4) Title

Applying STAMP/STPA to project management focusing on motivation

## Speaker, Authors

University of Nagasaki, Shigeru Kusakabe

## Abstract

This is a report of application of STAMP/STPA to a case of project management. STAMP/STPA allows us to define an accident, undesired and unplanned event resulting in a loss, in a broad sense such as a failure of a project, as well as more narrow ones involving death of humans. In managing a project, we need to identify the dependencies among various stakeholders and workproducts, and keep required constraints for the project on the control structure reflecting the dependencies. One of the problems in project management involving human natures, the fifth pattern of unsafe control action, the control action is issued but not followed. As one of the example case of this pattern, we discuss the case of the PSP (Personal Software Process) training course in a software-process education project at Kyushu Institute of Technology. One of the problems of the class is low completion rate and professors have been trying to resolve the situation. They think the problem is motivation and formalized the motivation process of the PSP course trainees by using state transition modelling based on the Organizational Expectancy Model. The latest model, Practical-STM, treats an individual trainee of the PSP course as a state machine, and formalizes the motivation process of a trainee using the state, values of the factors regarding the trainee's motivation and a set of operations from the course instructors. Theoretically, instructors can decide effective actions for the trainees based on the assumption on the state and the corresponding state transition function of the trainees. However, it is difficult to develop and analyze the instructor scenarios, series of instructions during the PSP course, by considering the trainee's motivation. We use STAMP/STPA make an educational guideline architecture to manage the situations during the course in a top-down manner based on the Practical-STM.

## Keywords

(1) Project management

(2) Motivation process

## (5) Title

Using STAMP/STPA focusing on “freedom from interference”

## Speaker, Authors

University of Nagasaki, Shigeru Kusakabe

## Abstract

In the software architecture field, there exists a claim that proper usage of "views and perspectives" is useful in describing and analyzing architecture. Likewise, the author proposes usage of some useful phases to facilitate better application of STAMP/STPA. The author considers FFI, “Freedom From Interference” is one of such a useful phase.  FFI is mentioned in ISO 26262, Part 1, Definition 1.49, as "Absence of cascading failures between two or more elements that could lead to the violation of a safety requirement". While FFI is strongly related to partitioning in an ISO 26262 context, the phase can be useful in more general context. For example, we can correlate the description and analysis of EMV2 (Error Model annex version 2) for AADL(Architecture Analysis & Design Language) with the modeling and analysis of STAMP/STPA. Moreover, the we facilitate modeling and analysis of more general cases such as a case of project management with the phrase in STAMP/STPA.

## Keywords

(1) Freedom from interference
(2) Architecute description and analysis
(3) Perspective
(4) ISO26262

## (6) Title

Review of STAMP/STPA case studies and explanation support of STPA process using GSN

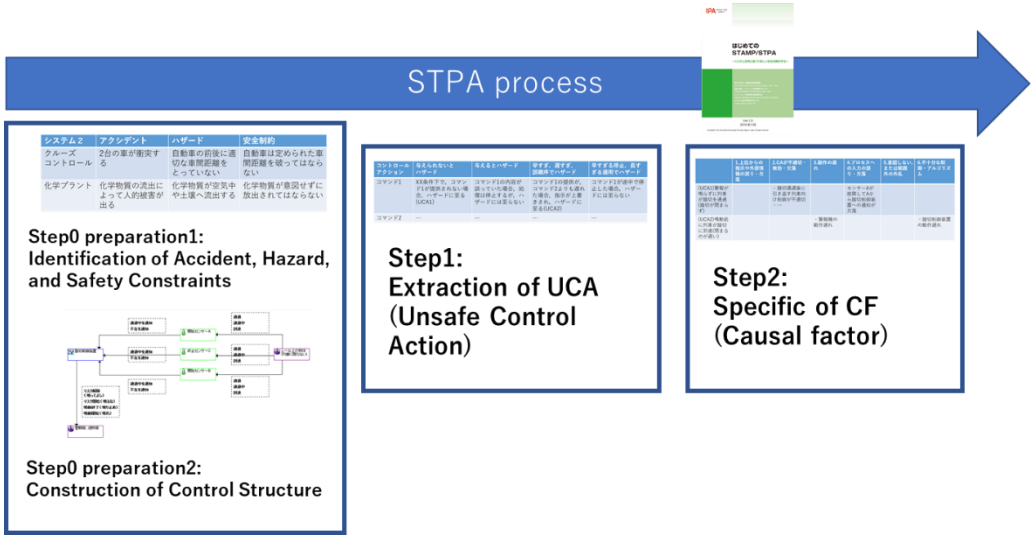
## Speaker, Authors

College of science and technology, Nihon university. Taito Akiyama, National Institute of Technology, Sendai College. Keisi Okamoto, College of science and technology , Nihon university. Yutaka Matsuno

## Abstract

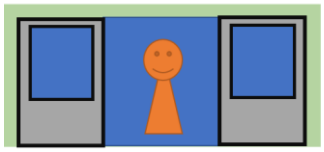
STAMP/STPA method was also tried in Japan in recent years, and a STAMP workshop was held at Kyushu University the first time last year. But much, a point different from a conventional risk analytical method (FTA,FMEA) has just started with sharing of know-how for the implementation.

I'll look back to an announced case by the STAMP workshop the first time by this publication and report the moot point for putting STAMP/STPA into effect, and regaining consciousness. The GSN pattern why to do do those accidents, a hazard and the explanation support of whether a control structure was set using GSN (Goal Structuring Notation) is proposed about the point which becomes a problem in each step of STAMP/STPA (for example, accident, setting of a hazard and setting of control build).




I don't sometimes know for example why the hazard is important in setting of a hazard in a procedure of STAMP. At that time, the explanation, it's supplemented in GSN.

**Step0 preparation1:**
**Identification of Accident, Hazard, and Safety Constraints**

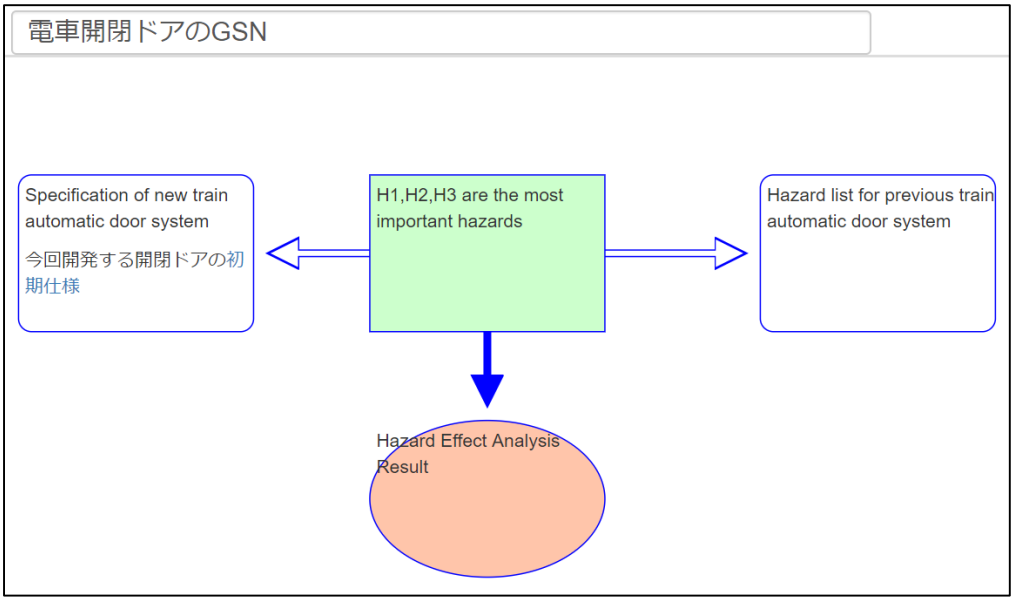


The system that a door on the train opens and shuts

Why were these 3 hazards established?
D-Case (It's possible to think GSN to click.)

| Accident | Hazard | Safety Constraints |
|---|---|---|
| A passenger is injured. | It closes for time when a passenger is between the door.(H1) | When a passenger is between the door, a door is always open. |
| | When a train stops besides the platform with moving time, a door is open.(H2) | When a train stops besides the platform with moving time, all except for emergency is always closed for a door. |
| | Emergency and a door are closed, and a passenger can't go outside.(H3) | A door holds emergency certainly. |

GSN where a hazard above-mentioned indicates a chosen reason is indicated.





## Keywords

(1) STAMP/STPA

(2) Review

(3) Explanation support

(4) GSN

## (7) Title

Risk analysis of autonomous driving system using STAMP/STPA - confluence on highway -

## Speaker, Authors

Aichi Institute of Technology. Masatoshi Hori, MITSUBISHI ELECTRIC ENGINEERING COMPANY LIMITED. Nobuyuki Ito,

Aichi Institute of Technology. Katsuhiko Kaji, Katsuhiro Naito, Tadanori Mizuno, Naoya chujo

## Abstract

In recent years, autonomous driving systems have been actively researched and developed because of social demands for safety, economical and environmental problems. Particularly, with regard to expressways, some systems which realized some functions of SAE Level 3 have been launched.

In Level 3, the autonomous driving systems have to cooperate with the driver's operation. If the autonomous driving system and the driver cannot communicate properly, there are some risks which lead to traffic accidents. However, to the best of the author's knowledge, these risks and their mitigation have not been sufficiently analyzed.

Therefore, we focus on the cooperation between this autonomous driving system and the driver and try to analyze the risk using STAMP/STPA. In this research, we focus on the confluence of expressway and analyze their risks.

As a result of the analysis so far, we found that the risk of rapid approach from the rear was increased by applying a manual brake operation, if the driver is not accustomed to merging onto the expressway (Fig. 1). It could be avoided by providing information about other vehicles around the autonomous driving vehicle by using road-to-vehicle communication.

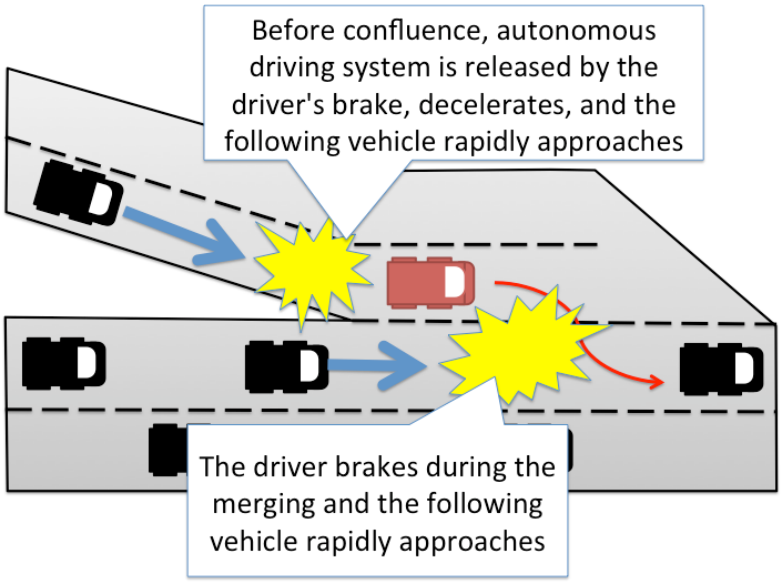



Figure 2: Risks at confluence on highway

## Keywords

(1) Autonomous Driving

(2) Driving Assistant System

(3) Driver Collaboration

(4) Expressway

(5) Confluence point

## (8) Title

Risk Analysis of multi-purpose batch plants using STAMP/STPA

## Speaker, Authors

Nagoya Institute of Technology. Shun KONDO, Takashi HAMAGUCHI, Yoshihiro HASHIMOTO

## Abstract

In the chemical industry, product life is getting shorter and shorter, and early introduction into the market is more important as competitiveness than production efficiency. For this reason, a system is required that not only constructs a dedicated plant, but also realizes new manufacturing by mastering general-purpose equipment, and also continues to manufacture conventional products. Therefore, flexible operation of multi-purpose/multi-batch is required, but problems arise due to contamination and handling of multiple products. Therefore, it is necessary to analyze the risk for operation, and addition of recipes must also be considered. However, HAZOP study is common as a risk analysis method in continuous plants, but development of a method to identify the risk of a batch plant on the premise of multi-purpose/multi-batch operation has not progressed. This is due to the difficult handling of changing piping structure and product quality, as well as by free operation methods. It is also the reason why measures to avoid risk are wide ranging such as top policies. Therefore, when considering risk analysis for batch plants, we need not only pay attention to ‘objects’ such as plant structures, but also new frameworks that expand analysis targets to software related to operations and human systems are necessary.

For the reasons stated above, we focus on STAMP/STPA which can deal with accidents caused by software and can be analyzed even to human systems and organizations. In this presentation, we will discuss the application of STAMP/STPA to batch plant in conjunction with cyber-attack which is a threat of control system in recent years.

## Keywords

(1) Batch Process

(2) Risk Analysis

(3) Cyber Security

## (9) Title

STAMP/STPA Application Guide for Automotive ～From JASPAR Functional Safety WG Activity Result～

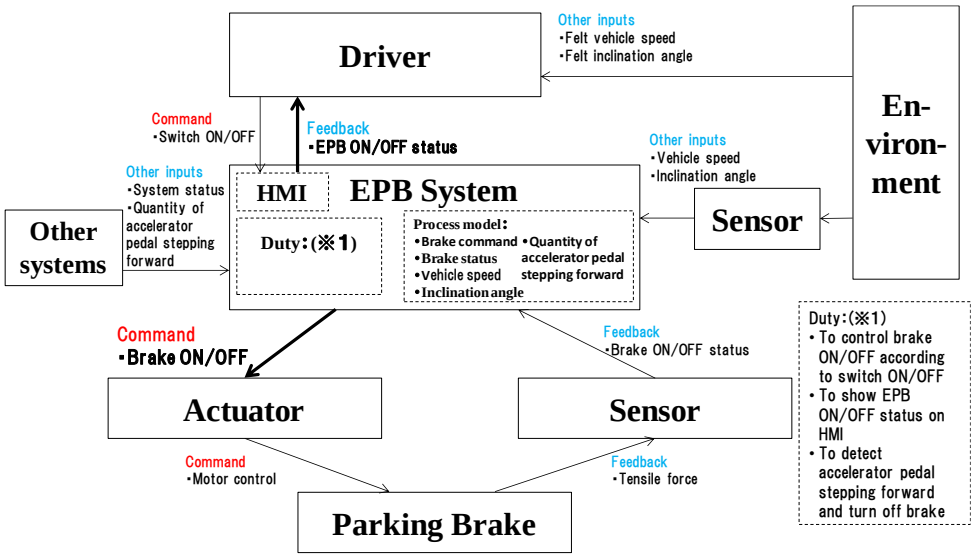
## Speaker, Authors

JASPAR. Yoshihiro Miyazaki, Manabu Okada

## Abstract

Automotive electronic control technology advancement is critical in the drive toward autonomous driving. Significant improvement in the safety, quality and efficiency for design and verification is required for automotive in-vehicle electronic control systems development. Automotive functional safety standard ISO 26262 was established in 2011, and the product application advanced, too. However, in case of autonomous driving, it becomes huge and complicated system that plural systems cooperate. It is thought that applying only conventional safety analysis method (FTA, FMEA) may derive risk of oversight and that applying STAMP/STPA additionally will be effective. Because STAMP/STPA performs hazard analysis and safety analysis by accident model that pays its attention to the interactions between each component in the system. JASPAR Functional Safety WG considered how to apply STAMP/STPA efficiently and effectively at development sites, and gathered it up as an application guide for development sites. The main contents are (1) Difference analysis against hazard analysis and safety analysis of ISO 26262 which is already operated, (2) Trial of STAMP/STPA on assumed EPB (electric parking brake) system as an example and extraction of its effect, (3) Standardization proposals of control structure diagram and analysis process description in order to operate efficiently and effectively between car manufacturers and suppliers.

Control Structure Diagram of Assumed EPB System




## Keywords

(1) STAMP/STPA

(2) Electric Parking Brake

(3) Hazard analysis

(4) Safety analysis

(5) Control Structure Diagram

## (10) Title

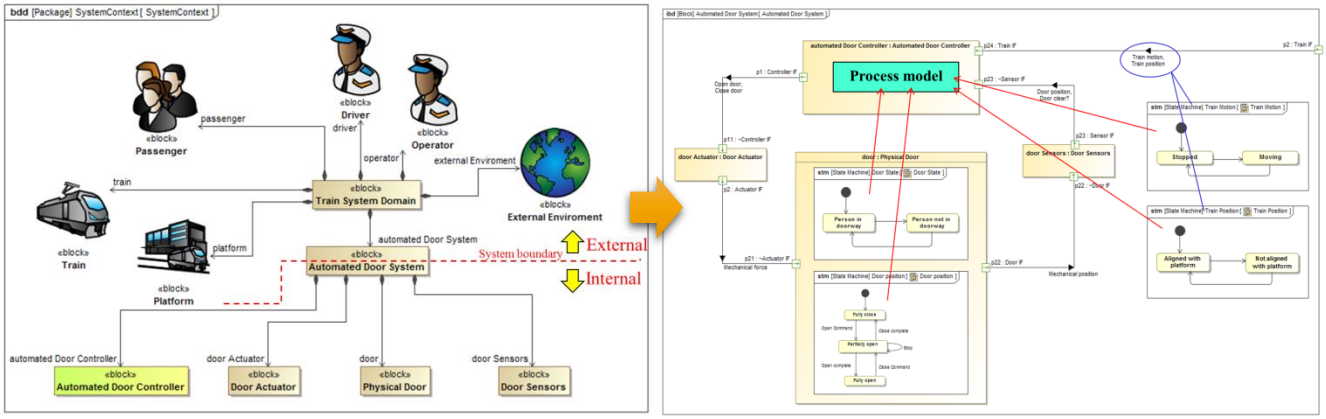
STAMP/STPA with using system model

## Speaker, Authors

Hitachi Industry & Control Solutions, Ltd. Takeo Hashimoto

## Abstract

STAMP/STPA is said that it can be used for analyzing not only the system malfunction but also the cause of accidents which were caused from the interaction between the components such as multiple systems, humans, and environments. One of the differences between STAMP/STPA approach and conventional safety analysis approaches is that STAMP/STPA approach can be used for safety analyzing even at a concept design phase (before defining system elements). STAMP/STPA also has an aspect of as a method to generate ideas easily, we could get the variety of analysis results depend on analysts.  But without the analysis process, it is difficult to judge the coverage and validity of the analysis result. Therefore we think visualizing and recording the thinking process of analysis are a key solution for this issue, and we introduce the STAMP/STPA trial result with specific examples by using system models which were made by system engineering approach. We used international standard SysML (Systems Modeling Language, ISO/IEC 19514:2017) to visualize “Control structure “and “analysis process”. For example, we made “Control structure(right figure)” depend on the analysis result of “System context(left figure)” , “Sequence diagram”, and so on. (Not shown all process)  Visualizing the thinking process of analysis enables us to get new findings such as the lack of actors or new consideration points.




## Keywords

(1) Systems Engineering
(2) Unexpcted event
(3) Visualizing the analysing process
(4) SysML
(5) Traceability

## (11) Title

Prospect for availability of STAMP/STPA as safety analysis in international safety standards

## Speaker, Authors

TOSHIBA CORPORATION. Hisashi YOMIYA, JFP, Inc. Hiroshi NAKAMURA

## Abstract

In international safety standards such as IEC 61508 and ISO 26262, safety analyses are conducted multiple times according to the product development phases.

These standards give recommended analysis methods, but traditional methods such as FMEA, FTA and HAZOP are used in many actual developments.

This presentation represent following (1), (2) and so on.

(1) Characteristics and differences between traditional analysis methods and STAMP/STPA,

(2) Availability of STAMP/STPA according to purpose and procedure of safety analysis in standards.

We present these analyses are mutually complementary such as STAMP/STPA is the most suitable for the conceptual design in uppermost development phase and traditional analyses can be fully used in lower development phases.

In addition, we present STAMP/STPA can be useful as a method to expand the scope of safety analysis in standards and to enhance safety of products through intent of the standards and the results of surveys from some public information.

This presentation includes outline and aspect of safety analysis in standards such as IEC 61508, ISO 26262, ISO 14121, ISO 12100 and so on, but it does not include detailed explanation of STAMP/STPA and international safety standard, and case example.

## Keywords

(1) STAMP/STPA

(2) Safety Analysis

(3) International Safety Standards

(4) ISO 26262

(5) Development Phase

## (12) Title

Safety Assessment of Closed-Loop Level Crossing Control Systems by Means of Systems-Theoretic Accident Model and Processes (STAMP)

## Speaker, Authors

Kyosan Electric Mfg.Co.,LTD.  Development Center. Tetsuya TAKATA

## Abstract

There have been a large number of accidents at level crossings of railways and this has been considered to be a significant issue to be solved for the realization of safe and stable railway transport. Conventional level crossing control equipment consists of two types of level crossing controllers; one detects a train approaching to a level crossing section and the other then detects the train having left the level crossing. By contrast, closed-circuit level crossing control systems in which level crossing controllers and train-borne equipment communicate with each other have been advocated and are expected to serve as an effective solution to the abovementioned issue. This paper describes the following three types of closed-circuit level crossing control systems: decentralized control system, fully-centralized control system and semi-centralized train-based sequential control system. This paper then assesses the safety of these systems in comparison to the conventional level crossing control equipment. For the purpose of the assessment of their safety, a new accident analysis model called STAMP (Systems Theoretic Accident Model and Processes) that is suitable for software intensive systems is used to clarify the advantage of the proposed three types of level crossing control systems in terms of safety.

## Keywords

(1) Level crossing control
(2) Railway signaling
(3) closed loop control method
(4) safety assessment
(5) STAMP

## (13) Title

Application and extension of STAMP/STPA to Railway Signalling System

## Speaker, Authors

East Japan Railway Company. Yusuke Takano, Hiroshi Sasaki, Yuichi Morita, Koji Sugiura, Takashi Kawano

## Abstract

STAMP/STPA is currently gaining attention as a new safety analysis method for complex systems. Here, the complex systems include complex human/machine interactions, internet communications or advanced software. The conventional safety analysis methods based on reliability engineering are not always applied to them, and, STAMP/STPA is expected as a top down safety analysis tool. The concept of STAMP/STPA includes an important paradigm shift in the conventional safety design process. It is important to understand the benefit of this paradigm shift through the concrete case study.

One of the advantages of STAMP / STPA is that even engineers who are not domain experts can analyze complex systems. On the other hand, the railway signallig system has been examined by domain experts based on accidents and defects so far, and the current safety is being built up. In railway signalling system, not only safety but also reliability are important factors. Therefore, STAMP / STPA is also extended for reliability, and we evaluate accidents and defects so far in the railway signal system.

## Keywords

(1) STAMP/STPA

(2) Railway signalling system

(3) Safety

(4) Reliability

## (14) Title

A Proposal of The Refinement STPA Guide Words on Human Factor of Supervisory Control Systems for Safety (Security) Analysis of Automated Vehicles

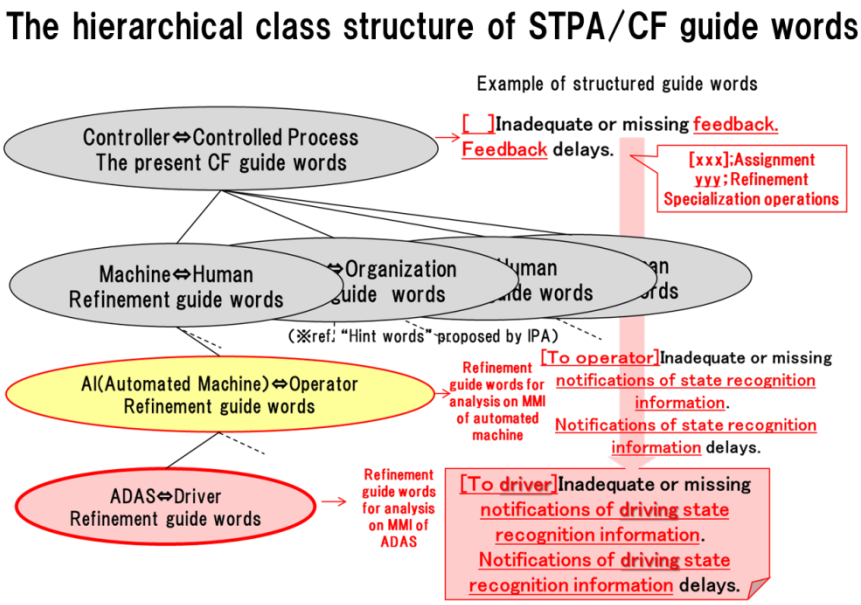
## Speaker, Authors

Hitachi, Ltd. Service Platform Business Division Group Security Business Division. Yasuhiko NAGAI

## Abstract

The new system safety (security) analysis technique “STAMP/STPA” begins to be attention with technique suitable for analysis of system which became complicated in the IoT/CPS age. Because by using the technique, we can identify the abnormality about system characteristics such as software abnormality or interaction abnormality between system components. Particularly in future, I think that STPA is an effective means for analysis on the human factor problem with MMI (Man-Machine Interaction) of SVC (SuperVisory Control system) applying automation technologies such as AI. However, it is difficult in the present CF (Casual Factor) guide words that a general engineer extracts the issue of human factor of SVC appropriately and systematically.

Therefore, this subject propose the refinement guide words to be able to extract the issue of SVC human factor easily by defining the class structure of guide words such as the following figure for SVC analysis and using the knowledge from previous studies on SVC human factor of aeronautical fields, and then reports a simple example of analysis result using the proposed guide words on the security attack application to an automatic driving car.




## Keywords

(1) STAMP/STPA

(2) system safety (security) analysis

(3) supervisory control system

(4) man-machine interaction

(5) human factor

## (15) Title

Safety analysis of level crossing obstruction detecting system using STAMP/STPA method

## Speaker, Authors

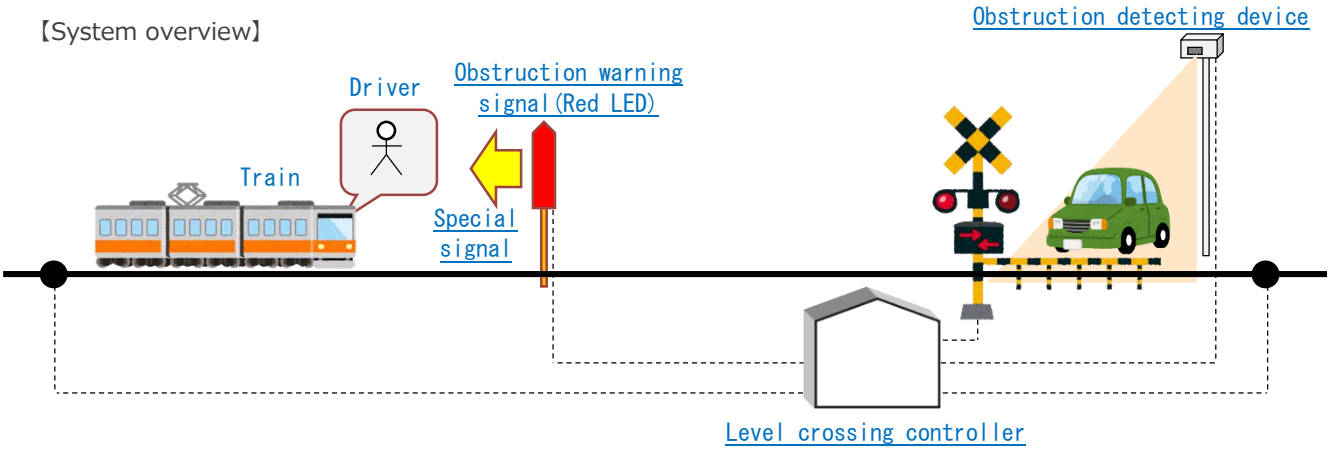
East Japan Railway Company. Satoru KITAMURA

## Abstract

For railway operators, the importance of ensuring safety at level crossings is increasing.

As one of measures to ensure safety at level crossings, East Japan Railway Company (JR-East) has "obstruction detecting devices" that detect obstacles such as automobiles in a level crossing, and "obstruction warning signals" that emit special signal light (flashing red LED light, etc.) to the train approaching to a level crossing on detection of obstacles at the level crossing. Through the functions of these devices, we are trying to prevent collision accidents between trains and obstacles at level crossings (these series of equipments are referred to as "level crossing obstacle detection systems" in this presentation). Also, the level crossing obstacle detection system exchanges the information with the level crossing controller which detects an approach of a train to the level crossing and controls the operation of warning lights and barrier machines. In addition, the train driver who recognized a special signal light emission is supposed to stop the train promptly.

In this study, we analyzed JR-East's level crossing obstacle detection system using the STAMP/STPA method, identified hazard causal factors (HCF), and extracted design safety constraints for eliminating HCF. This shows an example of safety analysis in the system where machines and human beings cooperate, but also how the railway-specific safety design is reflected in the control structure was considered.




## Keywords

(1) Level crossing

(2) Obstruction detecting device

(3) Obstruction warning signal

(4) Special signal

## (16)Title

Safety requirement analysis of level crossing control system using STAMP/STPA method

## Speaker, Authors

East Japan Railway Company . Takashi KUNIFUJI

## Abstract

In recent years, with the development of the information communication technology on which the railway signalling system is based, advancement and complication of both hardware and software are progressing. Coupled with its expertise in the railway signalling system, there are special circumstances such as high safety requirements, large order-made elements, ambiguous responsibility boundaries between operators and suppliers, and these exist in railway signalling systems making it even more complicated. Under such circumstances, as one of the technological development leading to the reduction of the development cost of the railway signalling system and the improvement of the safety, we are working on verifying validity through the safety analysis of software and control logic itself.

In this research, we tried to apply the STAMP / STPA method to the risk analysis carried out in the upstream process of development, with the theme of the level crossing control system in the station yard made in the past. In this trial, it was possible to efficiently extract general safety requirements for level crossing control, and confirmed that the STAMP / STPA method is effective for a railway signalling system which is one of event driven system. On the other hand, it was also found that there is still a problem that securing comprehensiveness of risk analysis has a large dependence on experiences of the target system owned by the analyst. Based on these, we also present future prospects for more effective use of the STAMP method.

## Keywords

(3) Level crossing
(4) Railway signalling system
(5) Safety
(6) STAMP/STPA
(7) STAMP/CAST

## (17)Title

Hazard analysis for power assist bicycle/Comparison of STAMP/STPA and numerical simulation analysis

## Speaker, Authors

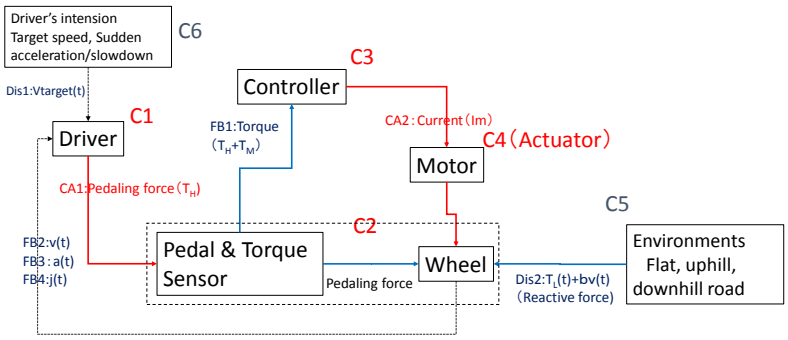
The university of Aizu.  Shigeru Kanemoto

## Abstract

STAMP/STPA is currently gaining attention as a new safety analysis method for complex systems.  Here, the complex systems include complex human/machine interactions, internet communications or advanced software.  The conventional safety analysis methods based on reliability engineering are not always applied to them, and, STAMP/STPA is expected as a top down safety analysis tool.  The concept of STAMP/STPA includes an important paradigm shift in the conventional safety design process.  It is important to understand the benefit of this paradigm shift through the concrete case study.

In the present paper, we apply STAMP/STPA to the hazard analysis of power assist bicycle which would be a typical example of human cooperative system.  Furthermore, we compare the results with those of numerical simulation like SIMULINK, and, discuss how STAMP/STPA is useful for the hazard analysis of the system including human.  The following figures indicate the control structure diagram of power assist bicycle and the definition of accident, hazard and safety constraints.  Here, two control actions (Pedaling force and assist force) and several feedback information are defined.  Also, driver's intention and road conditions are defined as disturbances.  Especially, to evaluate human actions, we made STPA analysis for three typical contexts (start, stop and normal travelling phases).  Also, numerical simulation of hazardous behavior will be made and compared  with STPA results.

Control structure diagram of power assist bicycle




- Accident
  - self-inflicted accident by falling or collision
- Hazard
  - Unbalancing state (Unintentional sudden acceleration or slowdown)
  - Over speed leading to falling or collision
- Safety constraints
  - Power assist to prevent unintentional sudden acceleration or slowdown
  - To prevent the assist for over speed
- Contexts
  - Analyze the hazards for Start, Stop, Normal travelling phases
  - Consider road conditions such as step of road or uphill or downhill (Downhill and freezing roads are omitted here)

## Keywords

(1) STAMP/STPA

(2) Power assist bycicle

(3) Numerical simulation

(4) Human-machine system

(5) Hazard analysis

## (18)Title

The STAMP/STPA method of intentions and requirements description level

## Speaker, Authors

JFP,Inc. Hiroshi　Nakamura

## Abstract

The working group for specifying safety in Japan Embedded Systems Technology Association is studying “Safety-guided design” as a process model of specifying safety-related requirements. The safety-guided design features to describe development intentions and system specifications, analyze those descriptions and repeat those describing according to the safety analysis, and aims at "If write intentions, safety increases". Virtual electric assist bicycle development was chosen as a trial case, and safety analysis was put into effect using the STAMP/STPA method.

When the STPA method was applied to safety analysis, a control structure was drawn as follows based on the requirements which reflect intentions about product development:

1) components are picked out from a System Context diagram

2) human-machine interactions are identified from a Use Case diagram

3) interactions inside the machine are identified from the intentions and requirements descriptions

I thought unsafe control actions depend on operation conditions of a bicycle, picked context variables as follows and tried to identify unsafe control actions every context :

1) feedback data

2) the data which shows outcomes of control actions

As a result, it was possible to identify several hazard scenarios, and it was possible to derive a recommendation measure which suits realization of the intentions from the identified measures. I think the STPA method is suitable for the safety-guided design and so I'd like to analyze development intentions by STPA, and to enhance safety and soundness of products.

## Keywords

(1) development intention

(2) safety analysis

(3) electric assist bicycle

(4) context variable

## (19)Title

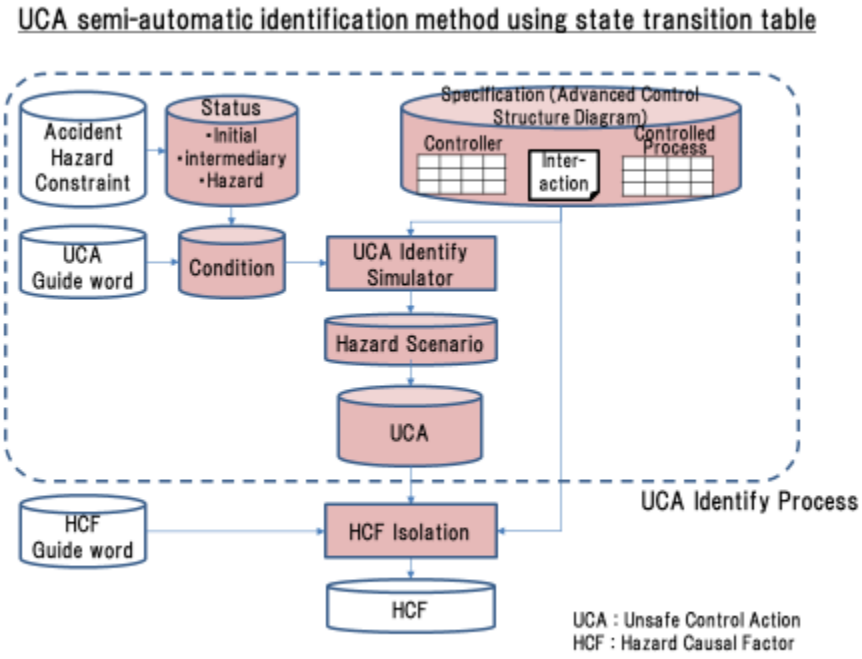
A Proposal to identify unsafe control actions in STAMP/STPA by simulation using State Transition Specification of Control Structure and guide word

## Speaker, Authors

Osaka Institute of Technology. Yasuko FUKUZAWA

## Abstract

“STAMP/STPA” is useful method for safety and security analysis of complicated system such as Internet of Things and Cyber-Physical System. By using this method, software abnormality and interaction abnormality between components on system are identified. This method consists of two steps. [Step 1] Identify unsafe control actions (UCA) leading to a hazard in accordance with a guide word from a control structure showing an intersystem configuration. [Step 2] Identify a hazard causal factor for each UCA according to a guide word. It is difficult to analyze cyclopaedically with the guide word. So to reduce the analysist's load of UCA identification, we propose the following method to identify UCA leading to hazards by using state transition specification and simulation. The specifications of the controller and controlled target in the control structure are represented by state transition tables. Then the UCA is identified by simulating the reachability to the hazard state on the state transition tables according to the guide word for CA. We report the effectiveness and approach of the method to identify UCA using state transition tables and simulation.




## Keywords

(1) system safety (security) analysis

(2) STAMP/STPA

(3) finite state machine

(4) state transition table

(5) reachability analysis

## (20)Title

An idea how to derive Process Models based on Extending STPA

## Speaker, Authors

Nihon Unisys Ltd. Yuko Fukushima

## Abstract

In STAMP / STPA, one of the common causes of accidents is that the "unsafe control action" (UCA) is executed when the process model does not match the system. While the process model is important, the method by which to derive the process model is not presented. Therefore, analysts should derive it ad hoc.

To solve this issue, Dr. Thomas of MIT introduced a technique called Extending STPA. In this method, analysts can take high-level context from a hazard and understand the refined process models. Then, identify the UCA by combining the process models.

Although Extending STPA is an effective method, the process models may be overlooked while refining the hazard context in process model hierarchy. Therefore, we can apply the viewpoints of 6W3H while UCA identification broadly captures the context.

The presentation will explain the issue of STAMP/STPA, outline Extending STPA and its issue, and explore the idea of applying 6W3H to identify the context and results of the trial.

## Keywords

(1) Extending STPA

(2) Process Model

(3) Context

(4) UCA

(5) 6W3H

## (21)Title

A Study on STAMP and HAZOP in IoT and deep learning application.

## Speaker, Authors

Nagoya Municipal Industrial Research Institute. DR. Kiyoshi Ogawa, ICS CO., LTD. Kazunori Ishizu, DENSO CREATE INC. Kazuo Kashiwabara, A&D Company, Limited. Masaru Sato

## Abstract

Since it came to Panel with Nancy in 2006 WOCS, we've been associating Nancy's method with international standards. The international standard on the method is to define an abstract common part or to facilitate the understanding of the differences of other methods by showing one example of the method. In particular, in 2011, invited Nancy at WOCS, after receiving Safeware's lecture, I focused on STAMP and explained the relation with HAZOP method. Currently we are planning to introduce IoT to industrial machinery, and show the correspondence relation in the study. Although HAZOP can be used at each stage of planning, designing, shipping and operation, since STAMP is mainly design-centered, the content of consideration includes analysis of the existing system. In addition, there are many organizations that combine many methods, such as JAXA published in the process improvement navigation guide issued by IPA in 2004, and relations with other methods such as FRAM are also organized.

## Keywords

(1) STAMP
(2) FRAM
(3) HAZOP
(4) ISO/IEC guide 50
(5) Design Review

## (22)Title

Verification of Cyber-Physical Systems Using STAMP / STPA

## Speaker, Authors

Nihon Unisys, Ltd. Yoshitaka Aoki, Shinshu University. Shinpei Ogata, Osaka University. Hiroyuki Nakagawa

## Abstract

CPS (Cyber Physical System) is used in various fields. Many systems will include CPS in the future. CPS connects cyber world and physical world. Therefore, it is influenced by the fluctuation of the external environment. Thus, CPS has uncertainty in the behavior of system and it is difficult to verify the safety.

STAMP / STPA is a method of safety analysis of complex systems. STAMP/STPA is based on Systems-Theoretic Accident model. Hazard analysis is performed by finding unsafe interactions among components. STAMP / STPA can also include a dynamic external environment in the accident model. Therefore, it is suitable for analysis of CPS system which is greatly affected by external environment. However, since CPS operates competingly for multiple devices, it is assumed that the control structure becomes complicated and analysis becomes difficult.

In this presentation, we propose a method of arranging complicated control structures and a method of verifying the stable state of the control loop using model checking. In this paper, we analyze the safety of traffic control system using Vehicle-to-Device (V2D) system as case study. The combination of STAMP / STPA and this proposal is useful for verifying the safety of a CPS system which is difficult to predict behavior.

## Keywords

(1) STAMP/STPA

(2) Cyeber-Physical Systems

(3) Model Checking

## (23)Title

Suggestion of Risk Management Framework by using STAMP/STPA.

## Speaker, Authors

Information Services International-Dentsu, Ltd. Hoonhee KIM, Motoki ANO, Naohiko SAKAI

## Abstract

In manufacturing industries including automobiles, FTA, FMEA, DRBFM, etc. are broadly used as a risk extraction and management tools. In this presentation, I would like to explain that by applying STAMP / STPA to a risk management method, we can extract and manage hazards and risks not only from mechanical point of view but also control point of view. In addition, here we suggest a framework which is enable us to manage not only technical risk but also schedule risk by visualizing the causes / measures / task progress / schedule of each risk and hazard together.

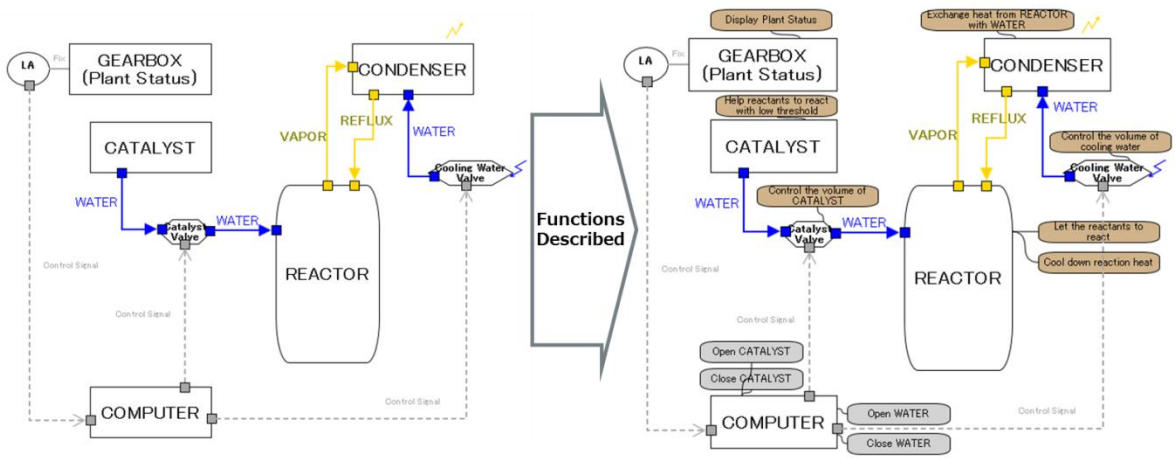



Figure 3 Function of each component is described on Control Structure Diagram

Figure 1 is a Control Structure Diagram introduced from “STAMP / STPA Intermediate Tutorial”. In addition to the control command (Open / Close WATER / CATALYST) to the controller (COMPUTER), the function of each component is also specified.

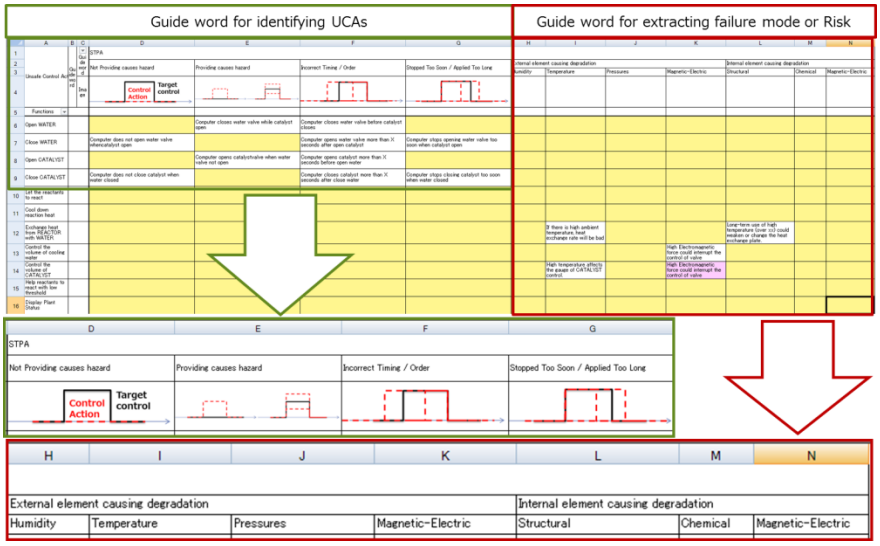



Figure 4 In reference to guide word, UCAs and risks are extracted from control command and function respectively.

In Figure 2, the UCA for each control command is extracted (green) using the guide word of STPA and the risk (red) of each function is extracted from the physical viewpoint (stress from the environment, component aging / deterioration) . In Figure 3, the extracted UCAs are applied to the FMEA format, and the impact analysis (RPN), causes, measures, tasks are arranged.

| Component | Function Control | UCA / Risk (Effect - RPN) | Cause･Countermeasure･Task |
|---|---|---|---|

| | Component | | Function | Guide word | Unsafe Control Action / Risk Details | RPN | Hazard / Risk Causal Factor | Safe Constraint / Countermeasure | Countermeasure task Task details | Person in charge | Due date | Progress |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | System | GEARBOX (Plant Status) | Display Plant Status | | | | | | | | | |
| 2 | | CATALYST | Help reactants to react with low threshold | | | | | | | | | |
| 3 | | REACTOR | Let the reactants to react | | | | | | | | | |
| 4 | | | Cool down reaction heat | | | | | | | | | |
| 5 | | CONDENSER | Exchange heat from REACTOR with WATER | Temperature | If there is high ambient temperature, heat exchange rate will be bad | 200 | Low heat exhaust | Generate blow to heated components to evacuate | Function Evaluation (Experiment or CAE) | Nakajima Myu | 9/29 | 0 % |
| 6 | | | | Structural | Long-term use of high temperature (over xx) could weaken or change the heat exchange plate. | 100 | | | | | | |
| 7 | | COMPUTER | Open WATER | Providing causes hazard | Computer closes water valve while catalyst open | 150 | Because ... | Computermust not close water valve while catalyst valve open | | | | |
| 8 | | | | Incorrect Timing / Order | Computer closes water valve before catalyst closes | 150 | Because ... | Computermust not close water valve before catalyst valve closes | | | | |
| 9 | | | Close WATER | Not Providing causes hazard | Computer does not open water valve whencatalyst open | 120 | Because ... | Computer must open water valve whenever catalyst valve is open | | | | |
| 10 | | | | Incorrect Timing / Order | Computer opens water valve more than X seconds after open catalyst | 100 | Because ... | Computermust open water valve within X seconds of catalyst valve open | | | | |
| 11 | | | | Stopped Too Soon / Applied Too Long | Computer stops opening water valve too soon when catalyst open | 80 | Because ... | Computer must open catalyst valve after a certain time passed. | | | | |
| 12 | | | Open CATALYST | Providing causes hazard | Computer opens catalystvalve when water valve not open | 60 | Because ... | Computermust not open catalyst valve when water valve not open | | | | |
| 13 | | | | Incorrect Timing / Order | Computer opens catalyst more than X seconds before open water | 20 | Because ... | .. | | | | |
| 14 | | | Close CATALYST | Not Providing causes hazard | Computer does not close catalyst when water closed | 20 | Because ... | .. | | | | |
| 15 | | | | Incorrect Timing / Order | Computer closes catalyst more than X seconds after close water | 20 | Because ... | .. | | | | |
| 16 | | | | Stopped Too Soon / Applied Too Long | Computer stops closing catalyst too soon when water closed | 20 | Because ... | .. | | | | |
| 17 | | LA | | | | | | | | | | |
| 18 | | Catalyst Valve | Control the volume of CATALYST | Temperature | High temperature affects the gauge of CATALYST control. | 250 | Because gauge is exposed to the external heat. | Block from external environment by placing air gap between gauge and environment | New Task | Nakajima Myu | 9/22 | 0 % |
| 19 | | | | Magnetic-Electric | High Electromagnetic force could interrupt the control of valve | 400 | There is no shield from external EM field. | Make the metal cabinet surrounding the valve | New Task | Nakajima Myu | 9/26 | 0 % |
| 20 | | Cooling Water Valve | Control the volume of cooling water | Magnetic-Electric | High Electromagnetic force could interrupt the control of valve | 400 | There is no shield from external EM field. | Make the metal cabinet surrounding the valve | New Task | Nakajima Myu | 9/26 | 0 % |

Figure 5 FMEA Table with STAMP/STPA applied

Countermeasures are taken against risks that are heavily influenced by the FMEA table and broken down to specific work tasks. By visualizing and managing the tasks with the person in charge, the deadline, and the progress (Figure 4), it is possible to manage risks “certainly” at the development site while balancing other schedules.

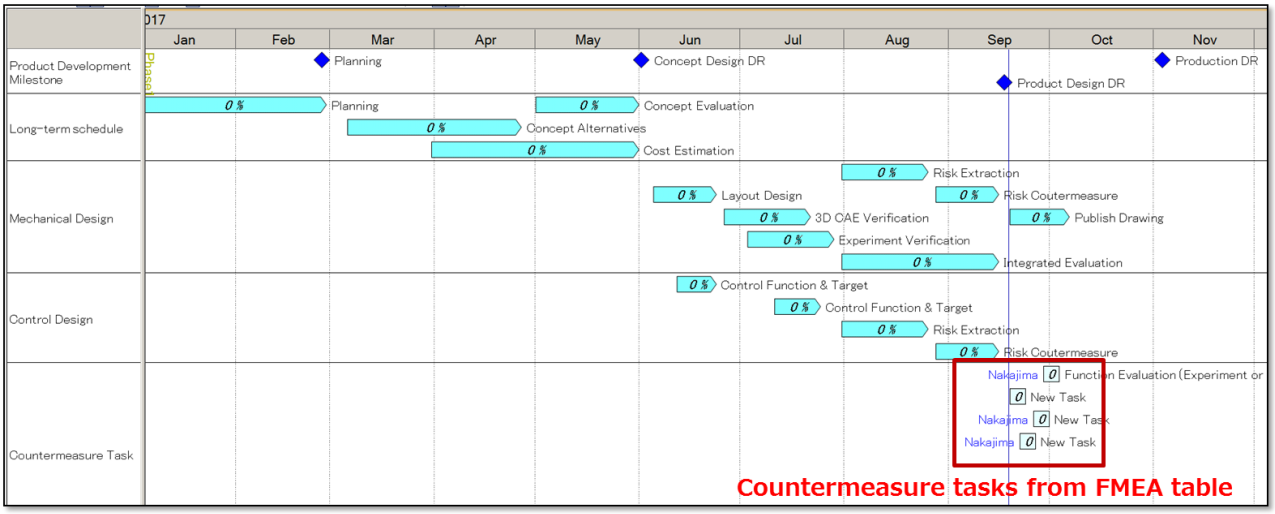



Figure 6 Visualizing of countermeasure tasks on the whole development schedule

## Keywords

(1) STAMP/STPA

(2) FMEA

(3) Risk Management

(4) Block Diagram

## (24)Title

A rubber “STAMP” was analyzed using “STAMP” based Process Analysis.

## Speaker, Authors

OMRON Automotive Electronics Co.Ltd. Hajime Tamanaha

## Abstract

STAMP/STPA which has been propounded by Prof. Nancy Leveson at MIT is a new safety analysis technique based on systems theory and a technique which is focused on interaction between elements of composing a system. In the IoT age arrival, a human, a machine and a system that social infrastructure link complicatedly, and a complicated and large-scale system is going to be organized. In such a system, it is extremely difficult to do analysis of safety using a traditional technique, i.e. a deductive analysis or an inductive analysis such as FTA or FMEA, which is focused on a failure of a part in reliability engineering: it increases in an analyzed element of composing a system explosively. Thus, STAMP/STPA is the analysis technique which is based on systems theory, i.e. it's regarded as the whole system that components of a system are abstracted to subsystems and subsystems interact with one another, and indeed proper analysis method in the IoT age.

On the other hand, as this technique is different from a traditional technique in the way of thinking of an analysis, it is the case that the technique’s challenge level is high.

Thus, IPA/SEC published a booklet titled “HAJIMETENO STAMP/STPA”, and the contents of the booklet are easy to understand, so companies which uses this safety analysis technique are also gradually increasing in Japan.

In the present paper, I made a hazard analysis of a rubber stamp, e.g. commemoration stamp in many sightseeing spots, using the technique and explained the results of analysis.

Table. Example : Identify accidents, hazards and safety Constraints

| Accident | Hazard | Safety Constraints |
|---|---|---|
| (A1)A seal impression wasn’t solid | (H1-1)A stamp face wasn’t flat | (SC1-1)Shall make a stamp face flatly |
| | (H1-2)Didn’t put ink a stamp face evenly | (SC1-2)Shall put ink a stamp face evenly |
| | (H1-3)A stamp mat wasn’t flat | (SC1-3)Shall make a stamp mat flatly |
| (A2)A seal impression was slanted or upside down | (H2-1)A direction of a seal wasn’t easy to understand | (SC2-1)Shall make a direction of a seal easy to understand |
| (A3)A seal impression was out of position | (H3-1)A position of a seal impression wasn’t easy to understand | (SC3-1)Shall make a position of a seal impression easy to understand |

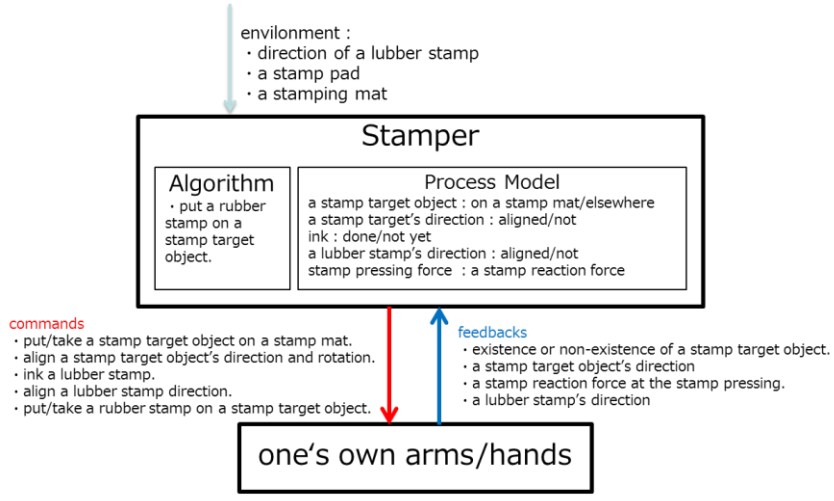



Fig. Example : control structure

## Keywords

(1) STAMP/STPA

(2) a rubber stamp

(3) biginner