A five-layer model for analyses of complex socio-technical systems

Tomoko Kaneko [1][0000-0001-5033-2861] and Nobukazu Yoshioka [2][0000-0002-1986-5675]

[1] National Institute of Informatics, Tokyo, Japan
t-kaneko@nii.ac.jp and nobukazu@nii.ac.jp

ABSTRACT

Current systems , which connect things and people through computer systems, have had a considerable effect on society. Not only are things connected, but systems, the people who use them, and organizations have a complex relationship. In order to model a complex system, we propose to use a layers pattern to describe the control structure diagram using five layers according to the lifecycle of software and system requirements. This model applies several techniques such as safety, security, risk, and incident analysis. We extend the System Theoretic Accident Model and Process (STAMP) model proposed by Nancy Leveson to produce the System Theoretic Architecture Model and Process (STAMP S&S). The reason for the term Architecture rather than Accident is that it extends STAMP with a five-layer hierarchical pattern and a process, necessary for various analyses. Based on the STAMP S&S （five-layer model), a way to perform analysis in each layer and to generate specifications and standards ensuring safety and security or other qualities is demonstrated.

KEYWORDS

Keywords: STAMP, STAMP S&S, Socio-technical System, Layer Pattern, Modeling, Analysis, Safety, Security

1. Introduction

Current systems, which connect things and people through computer systems, have had a considerable effect on society. Not only are things connected, but systems, the people who use them, and organizations have a complex relationship[1]. Although the evolution of Artificial Intelligence (AI) is rapidly becoming commercialized, it is challenging to ensure the safety and reliability of machine learning systems, including mission-critical systems such as automatic driving.

To ensure safety and reliability in complex systems, it is necessary to first understand the entire target system, and the effects of its components on each other, model them clearly and deal with its risks. However, it is difficult to model a complex system as a whole when its implementation has not been established. Currently, the

lifecycle model standards for systems and software specify the requirements for "what" is to be implemented during the planning, development, operation, and maintenance processes. However, the problem is that "this lifecycle does not specify how to build each stage." That objective requires the use of a development methodology and there are several of them to build secure systems using patterns [2]; however, there are no methodologies to build systems combining several quality factors.

Leveson proposed the System Theory Accident Model and Process (STAMP) methodology [3] and its analysis methods, such as System Theory Process Analysis (STPA) [4]. STAMP uses specifications, safety guide design, design principles, system engineering, risk management, management principles, and regulation of organizational design to analyze safety aspects. Our objectives are to extend the use of STAMP not only as an accident model but also as a model that can analyze the impact of complex systems on society. For that purpose, we will apply the Layers pattern [5] to separate the different system concerns in the form of a five-layer model. This pattern illustrates components and their interactions as components of a society and analyzes flawed control actions which are unsafe or insecure. Improvements in control actions are reflected in the output of the analysis in system service stakeholders in society. Their impact can be measured when they are reflected in the specifications and standards. This pattern's users are system engineers and analysts who are working on systems that require complex and diverse considerations, including human and social aspects, such as autonomous driving and smart cities, and want to know how to build them. As a first step toward solving this problem, the authors aim to "model complex systems, analyze them to ensure quality such as safety and security, and establish ways to standardize the results." Traditionally, the use of a single device, a component of a complex system, has been analyzed as much as possible. However, this method has its limitations for the analysis of a complex system as a whole. It is desirable that the modeling is in accordance with development standards.

In this paper, a model using a five-layer pattern and processes using a control structure for complex socio-technical systems are shown. Related work is introduced in Section 2, the proposed model is explained in Chapter 3, and the model is illustrated in Section 4 using several case studies, such as a railroad crossing system, a Phasor Measurement Unit, and Autonomous driving. Section 5 presents some conclusions.

2.Related Work

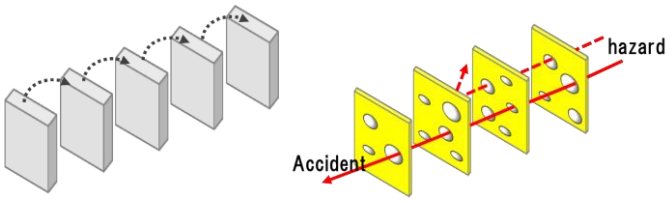
2.1. Traditional safety model and analysis

Traditional Safety models are the Domino model and slices model in the Fig.1. The series of cause and effect (the following causes) is called the Domino model. If you hold your hand somewhere in this domino defeat, you can avoid the accident. Each technique of the accident analysis, which is said the root cause analysis stands in this idea.

The defense wall and the leak is like the hole of the cheese. It is called the Swiss cheese slices model. It becomes an accident when the hole overlaps, and it foresees.

This is dealt with by blocking individual holes.

It underlies traditional safety analysis techniques (such as Fault Tree Analysis, Event Tree Analysis, HAZOP, FMECA, and HFACS) just as the traditional analysis methods are constructed on the assumptions about why accidents occur in a chain-of-failure-events model. The STAMP model is a new safety model that replaces the Domino model and the Swiss cheese model.



Domino model Swiss cheese slices model

Fig.1. The Domino model and the Swiss cheese model

2.2. STAMP model and its related methods

Modern embedded systems are becoming gradually larger and more complexed due to the interaction among connected elements in addition to the advanced functionality of each component. Traditional safety analysis techniques (such as Fault Tree Analysis [6], FMEA [7], and HAZOP [8]) are based on accident chain event models. However, since this model seeks causal relationships between individual events, it cannot capture a complex system as a whole. Therefore, to ensure the safety of these complex systems, Leveson proposed the System Theory Accident Model and Process (STAMP) [3]and its analysis methods, like System Theory Process Analysis (STPA) [4]. The STAMP model is proposed as an improved model of the conventional safety model such as the Domino model and the Swiss cheese model. The mechanism of STAMP is explained by focusing on the element (component) and the interaction (Control action) in the Fig.2. Many of the system accidents are not

only caused by the failure of the components, but also by the interaction of the control elements (control element and the controlled element) for safety in the system. As a process, STAMP use specifications, safety guide design, design principles, system engineering, risk management, management principles, and regulation of organizational design. However, STAMP is originally an accident model for safety, not for security or relaibilty either. It has not been established as a method for analyzing the impact of computer systems on society.

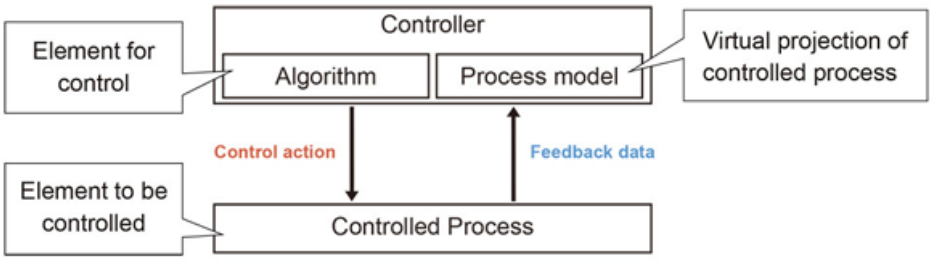


Fig.2. Control and controlled component in STAMP [5]

2.3. Traditional Methods of Security Analysis and development

Security analysis includes two aspects: 1) threat modeling and enumeration, 2) security evaluation.

Threat modeling and enumeration requires modeling how a threat is performed and several models have been proposed such as attack trees [9], misuse cases [10], and STRIDE [11]. Some HAZOP-based security analysis methods have also been proposed [12]. Security evaluation implies estimating the degree of security reached by a system; there are no widely accepted methods for this purpose.

There are also several methodologies to build secure systems. A group of these is based on building secure code and includes Microsoft Security Development Life Cycle (SDL) [13]. SDL analyzes threats using STRIDE. A more effective group of methodologies uses model-driven engineering (MDE) [2]. MDE is necessary to deal with complex systems because it applies abstraction.

However, compared with traditional standardized safety analysis methods such as FTA and FMEA, no security analysis or development methodology has been standardized and of widespread use.

2.4. Socio-technical Systems and Software Engineering

The system, which includes nontechnical elements such as people, processes, and regulations, as well as technical components such as computers, software, and other

hardware, is called Socio-technical System[14].

A socio-technical system includes hardware, software, people, and organizations. Socio-technical systems are so complex that it is impossible to understand them as a whole.

Therefore, you have to view them as layers. The socio-technical systems stack is shown in Fig.3. Software systems are not isolated systems but are part of more extensive systems that have a human, social, or organizational purpose. Therefore software engineering is not an isolated activity but is an intrinsic part of systems engineering. Also, as shown in Fig. 3, software engineering includes business processes, application systems, communication and data management, and operating system layers, and system engineering covers organization and equipment(hardware) in addition to them. But society alone is not included in either. The social layer is not included in software engineering and systems engineering[14]. In addition, although a complex system requires modeling based on such a hierarchy, the socio-technical systems stack does not show how to analyze it.

Fig.3.The socio-technical systems stack[9]

2.5. Layers pattern

The Layers pattern is a common architecture pattern, used in many applications, e.g., the ISO standard for communication networks uses a 7-layer decomposition. Its main objectives are separation of concerns and decoupling of the system functions so they can evolve independently [5].

A variant is the Secure Layers pattern [15], where the layers hide sensitive parts of a system. Another important variant is the N-tier pattern, which is a business architecture describing the typical layers of IT systems [16]. This pattern is the de facto standard for most Java EE applications and therefore is widely known by most architects, designers, and developers.

Components within the layered architecture patterns are organized into horizontal layers, each layer performing a specific role within the application (e.g., presentation logic or business logic). The layered architecture pattern does not specify the number and types of layers that must exist in the pattern.

The Layers pattern is more general and also includes other systems decomposed in layers to separate concerns; for example, the ISO standard for communication networks uses a 7-layer decomposition. The Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard communication protocols. The model partitions a communication system into abstraction layers.

The N-tier pattern is a business architecture describing the typical layers of IT systems regarding software[16]. This pattern is the de facto standard for most Java EE applications and therefore is widely known by most architects, designers, and developers. The layered architecture pattern closely matches the traditional IT communication and organizational structures found in most companies, making it a natural choice for most business application development efforts.

Components within the layered architecture pattern are organized into horizontal layers, each layer performing a specific role within the application (e.g., presentation logic or business logic). Although the layered architecture pattern does not specify the number and types of layers that must exist in the pattern, most layered architectures consist of four standard layers: presentation, business, persistence, and database.

3. A five-layer modeling and analysis process for complex socio-technical systems

3.1 Motivation

Systems are becoming more and more complex with the introduction of the Internet and technologies such as AI and blockchain. There is a great need to develop safe, and secure systems that meet the needs of society.

3.2 Problem

Complex systems cause safety and security problems, and accidents and incidents occur. We try to develop complex systems which are safe and secure but it is difficult to develop such systems. Traditional models that capture accidents are models that consider isolated objects, such as the Swiss cheese and domino models. Also, the hierarchical systems engineering model (Fig.3.) captures the system itself, but not the society layer.

Forces are shown below.

A) Complex systems cannot be captured as a whole.
B) Computer systems affect not only systems but also various objects, but the objects are various and complicated, such as people and organizations, in addition to the included software.
C) The analysis that captures the entire system, including people and organizations, is performed using the STAMP model, but it is not defined how the model is divided into layers for detailed analysis.
D) A method for analyzing the influence of a computer system on society has not been established.
E) Existing analysis methods vary depending on the attributes and targets such as safety, security, business, risk, and accident.
F) Even if there is a suitable model, quality factor analysis cannot be done unless the analysis process is decided.

3.3 Solution

A solution to this problem is to define a modeling and analysis process with a 5-layer control structure diagram. This solution is called STAMP S&S five-layer modeling, which tries to capture different interacting elements, different perspectives, and needs [17] [18]. In order to do this, STAMP's Control Structure(CS) diagram, which is based on system theory, is a good choice. However, STAMP's CS diagram is mainly used as a base for hazard analysis in a system layer, so it is necessary to devise a way to capture the interaction in a more hierarchical manner. Clarifying the hierarchy enables us to capture the characteristics of each layer and to conduct detailed analysis within each layer, which enables us to capture the whole system more accurately. In addition, STAMP S&S is analysis methods of STAMP in the safety & security engineering methodology for AI/IoT called CC-Case [19] [20].

Solutions to forces are shown below.

A) Use STAMP methodology that captures a complicated system as a whole as an accident model based on system theory.
B) Model a complicated system hierarchically.
C) Divide the software layer, system layer, service layer, and stakeholder layer.
D) Determine the process of analyzing interactions and create a method that can include the social layer, which is not included in software and systems engineering, to analyze.
E) Analyze by focusing on the interaction of various components.
F) Make a model with a process of analysis.

Therefore, we propose to use a five-layer model. To show the pattern is a complete solution constrained by the forces, the five layers consist the hierarchical model solution and the analysis process solution in detail, as shown below.

3.3.1 The hierarchical model solution

A model that captures complex systems as a whole is needed. This is because of the high-quality development of complex systems requires capturing various elements in interaction, different perspectives, and needs.

In order to do this, STAMP's Control Structure(CS) diagram, which is based on system theory, is a good choice. However, STAMP's CS diagram is mainly used as a base for hazard analysis in a system layer, so it is necessary to devise a way to capture the interaction in a more hierarchical manner. Clarifying the hierarchy enables us to capture the characteristics of each layer and to conduct detailed analysis within each layer, which enables us to capture the whole system more accurately.

Therefore, we propose a five-layer model. These five layers consist of Society, Stakeholder, Service, System, and Software, which we call the STAMP S&S five-layer model. Software is a concept, and systems are physical. Services are are provided to people., stakeholders are businesses, and society does not have a representative entity, but can be captured by features that include the environment. Also, these five layers are in an inclusive relationship where the upper layers include the lower. This five-layer model uses a control structure diagram that shows the interaction between the components in terms of control actions and feedback. This CS diagram is a different graphical representation from UML, which is commonly used in software models; the elements of the CS diagram have been presented as interactions of control relations, i.e., what is controlled and what is done. However, the authors view this as an interaction of connections, rather than control, for use in modeling for software-like cyber contents.

3.3.2 The analysis process solution

The process of analysis defines the goals that are aimed at and model the interactions between the components involved in those goals. A component is an element of the 5-tier model. Then, the factors that meet or hinder the goal are derived in the interaction, and scenario analysis is carried out to deal with them. A scenario is a knowledge representation used in a predefined sequence of events to determine the outcome of interactions between known entities. Various analyses, such as safety, security, reliability, risk, and accident, are conducted on a scenario basis.
The output of analysis at each layer of software, systems, services, and stakeholders is the "specification." There is a standard as the output of analysis in the social layer.

3.4 Stages of the process model

The process model should define the activities in each lifecycle stage. For example, the requirements and analysis stage should enumerate the threats and hazards for the system under design. This is the stage where the 5-layer model is necessary.

3.4.1 Implementation of the hierarchical model

The specific contents of each layer are shown in Table1. The social layer refers to the laws and regulations of society that govern the operation of the system. It also includes human social life (rules, standards, customs) and its external environment (natural environment such as weather). The stakeholder layer includes the organizational business processes, which make use of the software system, higher-level strategic processes as well as business rules, policies. It is a unit in which a business or organization has a responsibility as a stakeholder. The service layer includes actions performed by people, services, and services provided by people and organizations. The system layer includes a computer system, hardware, communication equipment, semiconductor chip. The software layer includes Programs (application software, OS, and other software), cyber information, data, and AI.

Table1. Specific contents of each layer

Layer	Contents
Society	Human social life (rules, standards, customs) and its external environment (natural environment such as weather)
Stakeholder	Individual or organization having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations such as business
Service	Actions performed by people, and services provided by people and organizations
System	Combination of interacting elements organized to achieve one or more stated purposes. e.g.Hardware, which describes the physical aspects of a computer, communication equipment, semiconductor chip
Software	Set of instructions, data or programs used to operate computers and execute specific tasks. e.g.Programs (application software, OS, and other software), cyber information, data, and AI.

3.4.2 Implementation of the analysis process

The following is an overview of the scenario analysis process.

(1) Take the event to be analyzed as a goal and determine the scope of analysis.

(2) Find the loss or achievement conditions for the goal.

(3) Determine the components in each layer and diagram the control relationship.

-The control component issues control actions to the controlled component.

-The control component issues control actions to the controlled component, and the controlled component returns feedback to the control action.

-Each component has its own algorithm and process model.

-Each component has its own algorithm and process model.

-If the component is a person, the process model is a mental model.

If the component is a person, the process model is a mental model - The process model or mental model is aware of what the process (state) of the component under control is.

(4) Scenario-based state and cause analysis is performed on control actions.

-Problematic conditions occur when there is a flaw in the perception of the process model or mental model.

-Perform analysis to find and address this problematic state.

-It cannot only find the problematic state but also analyze the requirements of the achievement conditions.

5) The extracted requirements are reflected in specifications and standards and improved interactively.

* Depending on the attributes of the target, this can be safety analysis, security analysis, reliability analysis, privacy analysis, or maintainability analysis.

In summary, scenario-based analysis is conducted by modeling what the goal and the state of affairs in a five-level CS diagram to determine the scope of the analysis and then focusing on the control actions is.

3.4.3 Significance of layered modeling of complex systems

The authors extend the use of conventional STAMP not only as an accident model but also as a model that can analyze the impact of complex systems on society. The STAMP model has been shown to adapt to social technology systems, but the structure is not specified in five layers, such as STAMP S&S. In addition, the STAMP model has been mainly subject to analysis of the system layer, service layer, and stakeholder layer presented by STAMP S&S. However, the STAMP model does not make the software layer and the social layer a detailed analysis object.

Although the STAMP model has many advantages, such as the ability to analyze the interaction of multiple components such as people and organizations, we are not only interested in accident models, but also for modeling complex system requirements and risk analysis. The work is proposed as STAMP S & S. S & S is the abbreviation of System, Software, Service, Stakeholder, Society, Specification, Standard, Scenario, Safety, and Security. This paper discusses the five layers of S: systems, software, services, stakeholders, and society. The remaining five S evaluate the impact of various events on a scenario basis for safety and security analysis and show that they will be made into specifications and standards. The relationship between ten S is scheduled to be described separately.

One of the reasons for adding these abbreviations is not only the various devices and systems but also the extended use of STAMP in this article is to model the interaction at the software, system, service, stakeholder and society layers. Its purpose is

to build a framework for hierarchical modeling and analysis of complex systems in an AI / IoT society.

Fig.4 shows the STAMP S&S Five-Layer model. In the STAMP S & S hierarchy, the business is called the stakeholder layer, and the operations are called the service layer. Systems and software layers are used as they are.

This model indicates that, as the development progresses, the corresponding processes usually progress in the order of the layers. However, STAMP S & S's analysis is not a waterfall type of analysis like this. It performs incremental analysis to stay resilient to changing requirements. Also, from the concept stage of development, we intend to conduct an analysis that considers the elements of each of these layers. Furthermore, it is intended to carry out a detailed analysis for each layer while considering the interaction. This allows many people to perform various analyses based on one structure.

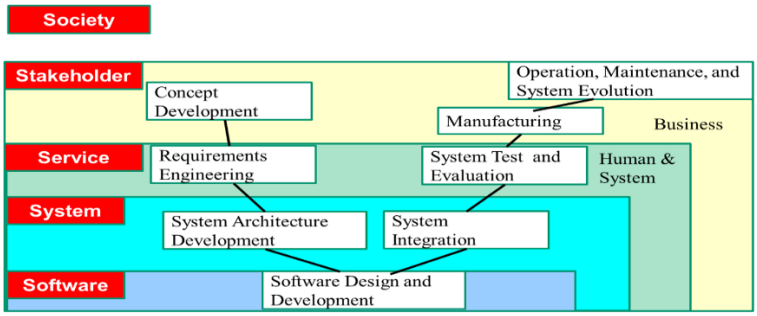


Fig.4. Five-layer model

Scenario means a knowledge representation used in a predefined sequence of events to determine the outcome of interactions between known entities. STAMP S & S performs scenario-based analysis, and specification is the output of analysis at each layer of software, system, service, and stakeholder. Standard is the output of analysis in the social layer, as shown in Fig**. 5.**

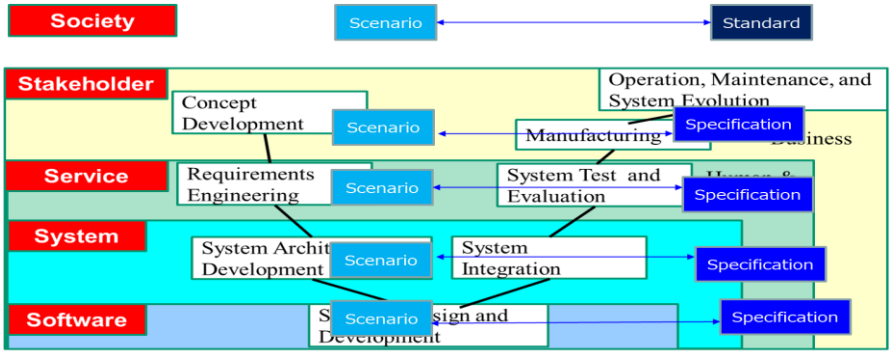


Fig.5. Relationship of Scenario, Specification, and Standard

3.5 Consequences:

The answer of the forces was presented in the problem section.

A) A complex system was modeled, as shown in figures in chapter4.
B) It was possible to model with layers.
C) The layered model allows us to perform various analyses based on one structure.
D) Components of the social layer were also presented and could be analyzed for interaction.
E) The analysis can be conducted with various emergent properties. (Various quality attributes).
F) Analyze various objects and conditions, such as risk analysis, accident analysis, business process analysis, and social needs analysis. Analyze by focusing on the interaction of various components.

By applying the five-layer model, it can be viewed as an interaction between a five-layer perspective: society, business, people, subsystems and devices, and software.

This interaction can be used to analyze by looking for non-secure states of control actions, as well as to analyze various quality requirements such as security, privacy, maintainability. The CS diagram of STAMP S&S should be an architectural model that captures the functional requirements of the entire system. However, it is a challenge to present concrete examples of application to these functional requirements in the future.

Although special structure and process for analysis have not been defined in the layer or Layer N, STAMP S&S has five layers for analyses of complex socio-technical and can analyze various emergent properties such as safety, security, reliability.

3.6 Rationale:

By structuring STMP S&S as a five-layer architecture, you can make it more flexible and can now analyze quality factors in a larger variety of complex systems, which need more layers to be described properly. To show the correspondence between problems, policies, and solutions, and to show the reason why it was effective in satisfying functional and non-functional requirements in Fig.6.

1) Five -layered model to clearly show the hierarchy of the system so that the features of each layer can be analyzed, and the detailed analysis within the layers can be performed to more accurately capture the entire system.

2) The elements of each layer are considered as an interaction of connections, and the relationships are also modeled in the CS diagram.

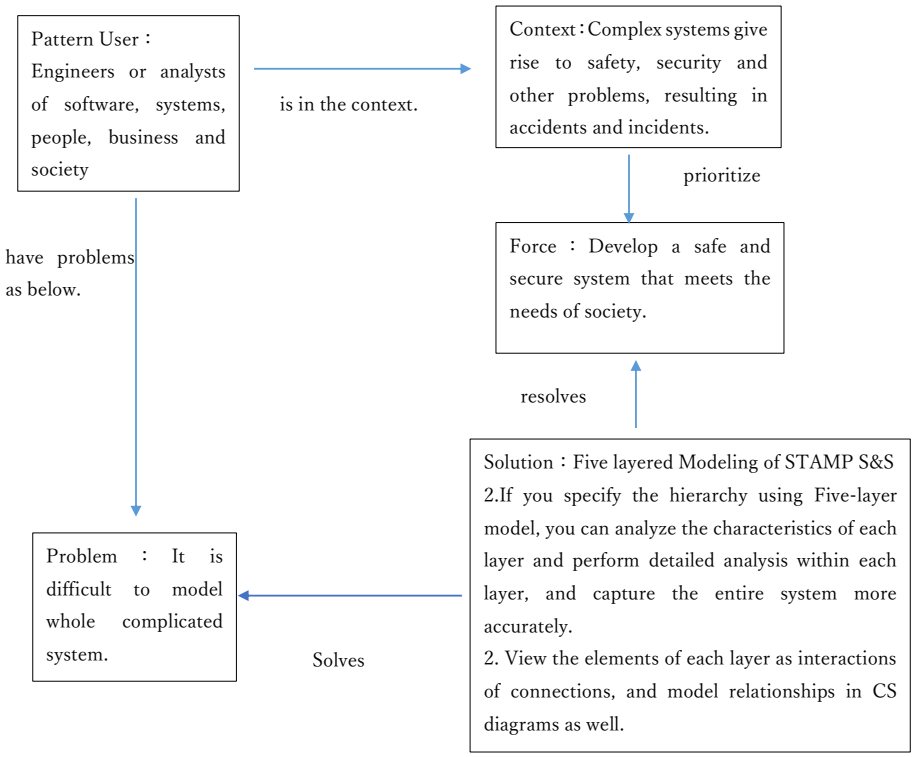


Fig.6. Relationship of the pattern

In order to implement the system quality, it is necessary to accurately grasp the factors of everything. The CS describes the interaction between the control component and the controlled component as a whole.

This component can be almost anything: equipment, system, people, organization, and so on. Components include algorithms and processes. In the case of humans, the algorithm is regarded as a mental model.

Factors common to all life(entity) is divided into the following ten categories, such as "the appearance, nature, entity, power, influence, internal cause, relation, latent effect, manifest effect, and their consistency from beginning to end" in Buddhism philosophy [21]. The CS diagram includes all these factors precisely. In terms of 10 factors common to all life, the component of the object is the entity, and it is divided into its appearance and nature.

In addition, each component is modeled to be exchanged by control action and feedback. In terms of control engineering, an actuator that amplifies force and a

sensor that collects information is also added. In terms of 10 factors, the control action is regarded as power and feedback as a function.

Furthermore, the process can analyze the causes, the hazards that triggered them, and the results. The process can be said to analyze the cause and relation (condition) and effect, which are the ties between them, for each power.

In addition, the manifest effect (reward) is considered an accident, or a goal to prevent the accident.

The CS diagram takes these components into systems thinking and captures that everything is connected and interacting with each other. That is the same idea as that "consistency from beginning to end" unifies factors.

The overall view is that a wide range of systems and devices are connected, like the IoT, from a highly abstract layer that broadly perceives society itself as one system and the environment, and people are also aware of one layer and AI. It can be handled hierarchically from one system and individual device layer, each component in the device, and the function in the software, and the relationship from the layer with high abstraction. It can be captured so that it can be tracked.

4. Case studies of Five-Layer Model and processes

In this case study, we introduce case examples of various industries to which five-layer modeling is applied, and we can see from what perspective the system should be overlooked by these five-layer patterns. In addition, it is clear that the STAMP model clarifies the interaction by simply describing the image diagram and the STAMP model. Each section presents examples in a different domain. It explains how the overall pattern was applied in each application domain.

4.1 Case 1: Railroad crossing system

The case study of a railway is presented. This case shows a system layer only model, which has been central to the traditional analysis of safety in the system layer only.

The control structure consists only of the system layer. This is the most basic layer. Traditional safety analysis methods have mainly targeted mechanical parts. However, the control structure of the STAMP is characterized by analyzing the interactions between each component. Therefore, the interaction of each component of the system layer is represented by the CS, even in the following cases.

The actual railroad crossing system is closed by lowering the bar in Figure 7, flashing the signal, and sounding an alarm. It is using the control structure shown in Fig.8, whether or not the railroad crossing control system will function safely in the event of abnormal train operation or component failure is analyzed using hazard techniques such as STPA. The following figure is for the STAMP model. The configuration of this case is only for the device and communication, so it consists of only the system layer.

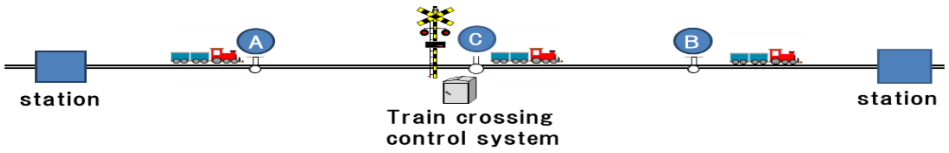


Fig.7: Image Figure of Railroad crossing system (on a single line) [22]

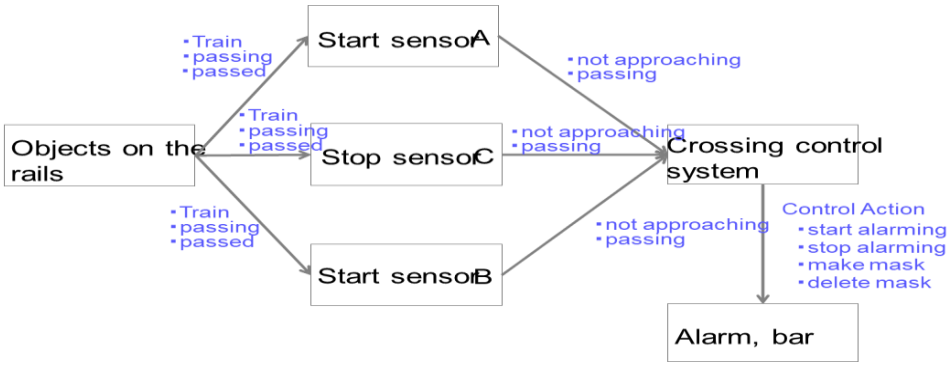


Fig.8: Control Structure (System Layer) of Railroad crossing system on a single line

Table2. Unsafe control action of Safety(Hazard) Analysis

#	Control action	Not Providing	Providing	Too early/too late Wrong order	Stopping too soon Applying too long
1	Start the alarm	(UCA1) Crossing is open while train is passing	Crossing is blowing the alarm even when no train is approaching	(UCA2) Crossing is still open even when train is approaching	(UCA3) Crossing open while train is passing
2	Stop the alarm	Crossing is still blowing the alarm even after the train passed	(UCA3) Crossing is open while train is passing	(UCA3) Crossing is open while train is passing	(UCA2) Crossing stops the alarm and opens while train is passing
3	Start masking	Crossing starts the alarm again when train reaches the opposite sensor	(UCA4) Crossing does not start the alarm when train is approaching from the masked side	Crossing starts the alarm again when train reaches the opposite sensor	(UCA6) Crossing does not start the alarm even when the next train is approaching from the opposite side
4	Stop masking	(UCA5) Crossing does not start the alarm even when train is approaching from the opposite side	Crossing starts the alarm again when train reaches the opposite sensor	(UCA5) Crossing does not start the alarm even when train is approaching from the opposite side	Crossing starts the alarm again when train reaches the opposite sensor

4.2 Case 2: Phasor Measurement Unit (PMU)

The case study of a PMU is presented. This case study also presents a system-layer only model, which was central to the analysis of traditional safety.

A generator set is operated synchronously with the main grid while in islanding mode. A Phasor Measurement Unit (PMU) at a remote, secure location in the main grid communicates with a local controller. A second PMU measures the power metrics on the island. The controller compares the measurements from the two PMUs and controls the generator(Fig.9). This can be figured by STAMP modeling of only the system layer in Fig 10. After making the control structure of STAMP, each control action is analyzed to be safe or not. As a supplement, The authors have pointed out the drawbacks of STPA-SafeSec[23] in which this case is published that threat analysis is not performed only by vulnerability analysis[24]

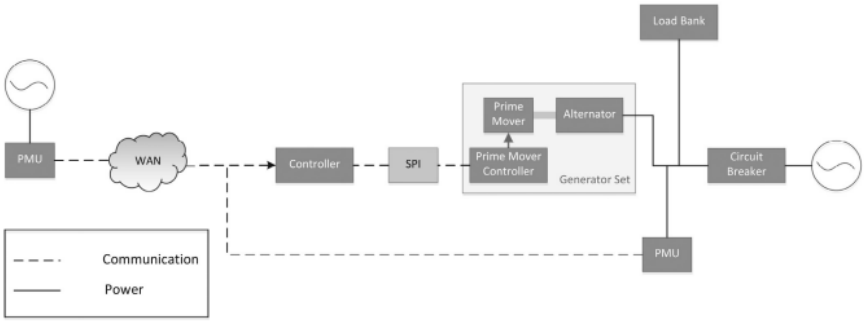


Fig.9: Image Figure of a Phasor Measurement Unit (PMU)[23]

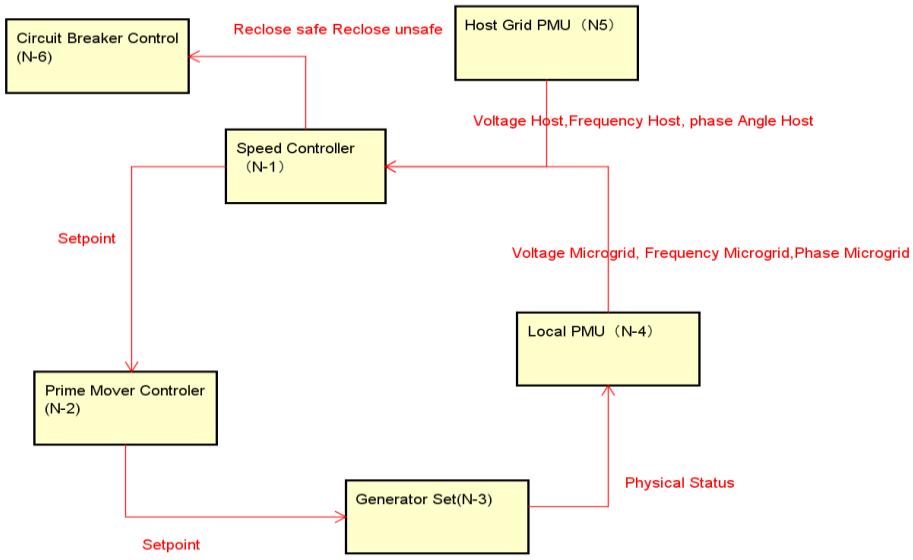


Fig.10: Control Structure(System Layer) of Power Grid

- **Step 0 Preperation1:** System Engineering Foundations

Define the frame safety and security problem.
Assure a safe and secure power operation. Today, threats of cyberattacks are increasing in power grid operation, including maintenance. There can be many attack elements, including terrorism.

Identify losses or accidents following A1-A4 in Table 3. STPA-SafeSec can also be used in the same manner.

Next, identify hazards (H1-H7) and threats (T1-T3) in Table 4. In our opinion, not only hazards but also threats must be identified in this step because safety hazards represent security threats.

- **Step1:** Identify Unsafe or Unsecure Control Actions

Table 3. Identify losses or accidents

ID	Accidents/Losses
A1	Injury to humans
A2	Damage to power equipment
A3	Damage to end-user equipment
A4	Interruption of power supply to consumer loads

Table 4. Identify hazards (H1-H7) and threats (T1-T3)

ID	Hazard
H-1	Out-of-sync reclosure
H-2	Operation of power equipment outside of operational limits
H-3	Violation of power quality metrics
H-4	Inability to achieve synchronization
H-5	Inability to meet local demand
ID	**Threat**
T-1	Power equipment is destroyed
T-2	Operation of power equipment is deprived of authority
T-3	Control information of the device is stolen

Unsafe or Unsecure control action from the speed controller is shown in Fig. 10 in red. In this case, instructing the prime mover controller to set the value outside the operation range not only leads to the hazard (H-2) but also threatens (T-1, T-2). Hence, this control action is unsafe and insecure. Table 5. shows four types of unsafe and insecure status for each control action (CA).

Table 5. The unsafe or unsecured control action

No	CA	From	To	Not Providing	Providing causes hazard	Too early or too late	Stopping too soon or applying too long
1	Reclose safe Reclose unsafely	Speed Controller (N-1)	Circuit Breaker Control(N-6)		The speed controller wrongfully assumes that synchronization is achieved. It would then indicate that the reclosure of the circuit breaker is safe when it is not. (H1)	The speed controller assumes that synchronization is achieved. It would then indicate that the reclosure of the circuit breaker is safe while it is too early or too late. (H1)	
2	Setpoint	Speed Controller (N-1)	Prime Mover Controller (N-2)	When the breaker is in the released state, set values within the operating range are instructed to the prime mover controller with Not (In other words, the setting value is not updated)(H-3, H-4, H-5)	Instructs the prime mover controller to set the value outside the operation range(H-2, T-1, T-2)	When the breaker is in the released state, set values within the operating range are sent as instructions to the prime mover controller with Too late. (In other words, the setting value is not updated) (H-3,H-4,H-5)	
3	Voltage Host, Frequency Host, Phase Angle Host	Host Grid PMU (N5)	Speed Controller (N-1)	Host Grid PMU does not report measured voltage Host, Frequency Host, or Phase angle Host. (H-3, T-3)	Host Grid PMU reports incorrect measured voltage Host, Frequency Host, or Phase angle Host. (H-3,T-1)		
4	Voltage Microgrid, Frequency Microgrid, Phase Microgrid	Local PMU (N-4)	Speed Controller (N-1)	Host Grid PMU does not report measured voltage Host, Frequency Host, Phase angle Host. (H-3, T-3)	Local PMU reports incorrectly measured voltage Host, Frequency Host, or Phase angle Host. (H-3,T-1)		

* PMU: Phasor Measurement Unit

Table 6. SCF of N1, Threat Scenarios, and Countermeasures for the Speed Controller (in the System Layer)

STRIDE	Required Properties	SCF of N1	Expected threat scenarios	Example of measures
Spoofing identity	Authentication	No correct authentication is made for N1-1 (Speed controller) (N1-S)	Host PMU impersonates the local PMU	Use an IC chip with an authentication function
Tampering	Integrity	Incorrect FB signal is inserted into N1 (Speed controller) (N1-T)	Some or all of the software running on the speed control is replaced by an attacker	Message authentication code (MAC), tamper-proof mechanism applied to speed controller
Information Disclosure	Confidentiality	The FB signal of N1-1 (Speed controller) is leaked (N1-I)	If the software running on the speed controller has been modified, the modified software might disclose the plaintext to an unauthorized person.	Implemented anti-malware, Secure Key Management
Denial of Service	Availability	N1 (Speed controller) is destroyed (N1-D)	• The speed controller is exposed to the threat of DoS in the form of constantly waiting for the network for incoming and unsolicited datagrams. • An attacker can open a large number of connections at the same time and take an extremely long time to process. In some cases, one-sided traffic can undermine the speed controller's ability to handle it. In both cases, the speed controller is virtually a malfunction in the network. -The function of the speed controller stops or cannot communicate by interference or cable cutting.	Limit the number of accesses from an attacker or the same IP. Create a speed controller that can withstand large-scale traffic
Elevation of Privilege	Authorization	（N1-E）	Limit the number of accesses from an attacker or the same IP. Create a speed controller that can withstand large-scale traffic	Access control of the speed controller. Establish an authorization scheme.

Table 7. SCF of N1-1, Expected scenario, and measures of Raspberry Pi (in the Software layer)

STRIDE	Required Properties	SCF of N1-1	Expected scenarios	Example of measures
Spoofing identity	Authentication	No correct authentication is made to N1-1 (Speed controller CPU) (N1-1-S)	-If the operating system user settings are not set properly, attackers might spoof them	Set the password appropriately: SSH Login with a private key
Tampering	Integrity	Incorrect FB signal is inserted into N1-1 (Speed controller CPU) (N1-1-T)	If an illegal program has access to a cryptographic key or an encryption mechanism that holds the cryptographic key, the software replaced will misuse the real ID of the speed controller. An attacker can use the extracted cryptographic keys to intercept, block, and replace data from the speed controller with false data and pass authentication with a stolen cryptographic key.	MAC Applying a tamper-proof mechanism to the speed controller
Repudiation	Accountability	(N1-1-R)	If the Raspberry Pi user does not have a log of the communication, it is likely to negate the fact of the operation that the user performed improperly	Acquisition and maintenance of various logs
Information Disclosure	Confidentiality	The FB signal of N1-1 (Speed controller CPU) is leaked (N1-1-I)	The attacker exploits the encrypted key and obtains the encryption key and decryption key between the speed controller and The Controller (the field gateway or the Cloud gateway), thereby allowing the attacker to get the cleartext.	Implemented Anti-malware, Secure Key Management
Denial of Service	Availability	N1-1 (Speed controller CPU) is destroyed (N1-1-D)	The function might be stopped if unauthorized access is performed over a WAN or Ethernet, or when a large amount of data is received.	Apply response limit
Elevation of Privilege	Authorization	(N1-1-E)	If the administrator setting of the OS is not appropriate, the user who does not have administrator rights of the OS originally has administrator privileges, and execution with administrator authority might be used illegally	"Run as Administrator" or "Restrict users who can get administrator rights."

4.5 Case5: Autonoumous driving

A case study of autonomous driving is presented. In this case study, the five layers (software, system, service, stakeholder, and social layer) require a social perspective, such as the environment. Fig.11 is an Image Figure of Autonomous driving. Fig.12 is a control structure that includes software, system, service, stakeholder, and society layers. This is a five-layered model.

Autonomous driving is a technology that has a significant impact on society. The control action in the case of the automatic driving level 3 is shown in Fig.12. In this figure, five layers of STAMP S & S are shown on the left side bylines, and the components of the layers are shown on the right side. In this case, CS shows the interaction between the system layer braking and the control of both the service layer driver and the software layer automatic driving AI. In this way, the hierarchical modeling of STAMP S & S itself is divided into layers and presenting their mutual relations. Also, there are several control actions in this CS diagram, and among them, using the deceleration command to the brake system by the artificial intelligence module, it is explained that the five layers of STAMP S & S influence each other.

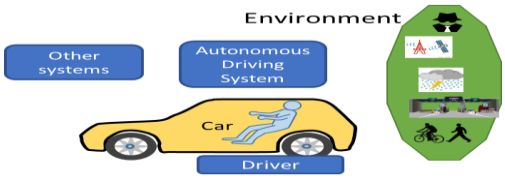


Fig.11: Image Figure of Autonomous driving

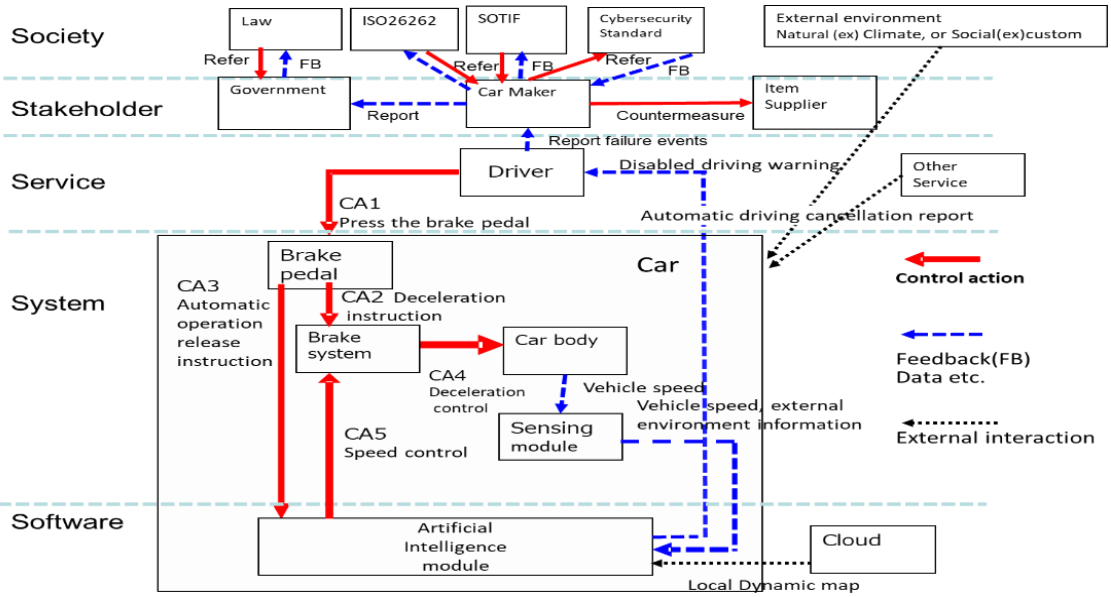


Figure 12: Five-layered modeling for autonomous driving

Autonomous driving is a technology that has a significant impact on society, and Table 8 shows the level of achievement. Fig. 13 shows the traditional STPA procedure and the STAMP S & S safety and security analysis procedure. When safety and security are specified instead of STAMPS & S, they are shown in blue, and new concepts are shown in red.STAMP S & S is goal-oriented, and for accidents (LOSS in a broad sense) that you want to analyze.

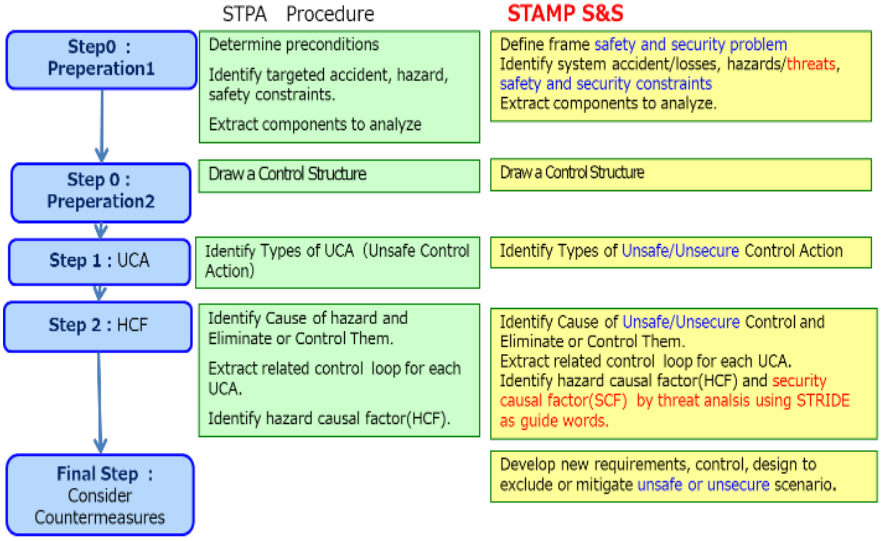


Fig 13. Analysis procedure of STAMP S&S

Table 8. Accidents, hazards, constraints

Accident	Hazard	Safety Constraints
(A1) The car collides/contacts with the external environment (pedestrian /other cars /surroundings)	(H1-1) Even if the car brakes, you cannot stop in front of the external environment (the distance to the external environment and the relative speed cannot be controlled)	(SC1-1)Braking the car so that it does not collide with the external environment (controlling the distance to the environment and relative speed)
	(H1-2) The brake does not work.	(SC1-2) The brake works.

Table 9.Extracting unsafe control actions in CA5

No	CA	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
5	Deceleration command to brake system by artificial intelligence module	(UCA5-N) If artificial intelligence does not issue a deceleration command during automatic driving, it will collide with the external environment.[SC1]	(UCA5-P) Unnecessarily strong deceleration command is issued, and rear-end collision occurs[SC3]	(UCA5-T) If the deceleration command is delayed, a collision cannot be maintained with the appropriate distance to the external environment ahead[SC1]	(UCA5-D) The deceleration command ends before sufficient deceleration is performed, and a collision cannot be maintained with the appropriate distance to the external environment[SC1] Continues to issue deceleration command after required deceleration is completed, making acceleration difficult

Table 10. Hazard causal factor analysis for UCA5-D

UCAS	Missing or wrong control input or external information	Inconsistent, incomplete, and inaccurate process models	Inadequate or missing feedback, delayed feedback	Conflicting control actions	Tampering	Denial of Service
(UCA5-D)	Unintentional automatic operation release instruction is input from the driver during deceleration	A situation that does not exist in the artificial intelligence learning data has occurred	Speed measured slower than it actually is ・The external environment could not be recognized due to bad weather	When the driver senses danger and performs a sudden braking operation, the judgment of artificial intelligence takes precedence	The automatic operation release instruction has been tampered with, and the automatic operation ends during deceleration.	The local dynamic map is attacked by a DOS attack, and map reference becomes impossible

5.Conclusions

In this paper, software, systems, services, stakeholders, and societies are modeled and layered as an instance. Instances could be divided into system layer only, system and service layer, system service, stakeholder layer, software, system service, stakeholder layer, software, system service, stakeholder, and social layer. It has been shown as an example that it can be used as a basis for safety and security analysis of complex systems.

References

1. Information Promotion Agency (IPA), "IoT Safety/Security Development Guidelines (Second Edition)" Important Points to be understood by Software Developers toward the Smart-society https://www.ipa.go.jp/english/sec/reports/20160729-02.html.
2. Anton V. Uzunov, Eduardo B. Fernandez, Katrina Falkner, "Securing distributed systems using patterns: A survey", Computers & Security, 31(5), 2012, 681 - 703. doi:10.1016/j.cose.2012.04.005
3. Nancy G Leveson, 2012. *Engineering a Safer World*, MIT Press
4. "STPA handbook," http://psas.scripts.mit.edu/home/
5. F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, M. Stal. Pattern-Oriented Software Architecture: A System of Patterns, Vol. 1. J. Wiley, 1996.
6. IEC 61025:2006 Fault Tree Analysis(FTA), https://webstore.iec.ch/publication/4311
7. United States Military Procedure, "Procedure for performing a failure mode effect and criticality analysis," November 9, 1949, MIL-P-1629
8. IEC 61882:2001 Hazard and operability studies (HAZOP studies) - Application guide. http://www.iec.ch
9. Schneier, Bruce. "Attack Trees," *Dr. Dobb's Journal of Software Tools*, 24(12), (1999), 21–29.
10. Sindre, Guttorm; Opdahl, L. Andreas. "Eliciting security requirements with misuse cases," *Requirements Engineering*, Vol.10, No. 1, pp. 34–44 (2005).
11. Lipner, Steve; Howard, Michael. "The Trustworthy Computing Security Development Lifecycle," https://msdn.microsoft.com/en-us/library/ms995349.aspx.
12. Jingxuan Wei, Yutaka Matsubara,Hiroaki Takada,"HAZOP-Based Security Analysis for Embedded Systems: Case Study of Open Source Immobilizer Protocol Stack.", Recent Advances in Systems Safety and Security pp 79-96 2016
13. Shostack, Adam. "Threat Modeling: Designing for Security," Wiley., 2014.
14. Ian Sommerville, " Software Engineering-10ed", Pearson Education Limited (2016)
15. E.B.Fernandez, Security patterns in practice: Building secure architectures using software patterns, Wiley Series on Software Design Patterns, 2013
16. https://www.oreilly.com/library/view/software-architecture-patterns/9781491971437/ch01.html
17. Tomoko Kaneko, Nobukazu Yoshioka, "STAMP S&S: Layered Modeling for the complexed system in the society of AI/IoT," JCKBSE2020
18. Tomoko Kaneko, Nobukazu Yoshioka, Ryouichi Sasaki, "STAMP S&S: Safety & Security Scenario for Specification and Standard in the society of AI/IoT," The 2020 IEEE International Workshop on Cyber Forensics in Software Engineering (CFSE)
19. Tomoko Kaneko, Nobukazu Yoshioka, "CC-Case: Safety & Security Engineering Methodology for AI/IoT", 1st chapter of "A Closer Look at Safety and Security", 2020
20. Tomoko Kaneko, Shuichiro Yamamoto, Hidehiko Tanaka," CC-Case as an Integrated Method of Security Analysis and Assurance over Life-cycle Process", International Journal of Cyber-Security and Digital Forensics 3(1) 49 - 62 2014
21. Soka Gakkai English Buddhist Dictionary Committee. (2002). "Ten factors of life," in The Soka Gakkai Dictionary of Buddhism. Tōkyō: Soka Gakkai. ISBN 978-4-412-01205-9. Archived from the original on 2016-02-26
22. IPA, First STAMP / STPA -New safety analysis method based on systems thinking-,2016(in Japanese)

23. Ivo Friedberg, Kieran, Paul Smith, David Laverty, and Sakir Sezer. STPA-SafeSec: Safety and security analysis for cyber-physical systems, Journal of Information Security and Applications, Volume 34, Part 2, pp.183-196 （2017）
24. Tomoko Kaneko, Yuji Takahashi, Takao Okubo, Ryoichi Sasaki, "Threat analysis using STRIDE with STAMP/STPA," The International Workshop on Evidence-based Security and Privacy in the Wild (APSEC2018Workshop)