World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:10, No:8, 2016

The Framework of System Safety for Multi Human-in-The-Loop System

Hideyuki Shintani, Ichiro Koshijima

***Abstract*—**In Cyber Physical System (CPS), if there are a large number of persons in the process, a role of person in CPS might be different comparing with the one-man system. It is also necessary to consider how Human-in-The-Loop Cyber Physical Systems (HiTLCPS) ensure safety of each person in the loop process. In this paper, the authors discuss a system safety framework with an illustrative example with STAMP model to clarify what point for safety should be considered and what role of person in the should have.

***Keywords*—**Cyber Physical System, Human-in-The-Loop, Safety, STAMP model.

I. Introduction

IN these days, Internet of Things (IoT) and CPS become popular as trend words. IoT is put forward by Kevin Asthon as a concept "to connect discernible everything to Internet" [1]. CPS means integrations of computation, networking, and physical processes, by which embedded computers and networks monitor and control the physical processes, with feedback loops where the physical processes affect the computations and vice versa. CPS is formed with the following three important components.

1) Sensor: A thing that collects data from target things.
2) Controller: A thing that controls and decides things based on information from the sensor so as to prepare an appropriate situation.
3) Actuator: A thing that acts things based on commands from controller so as to realize the appropriate situation.

These three components of CPS are shown in a diagram of Fig. 1.

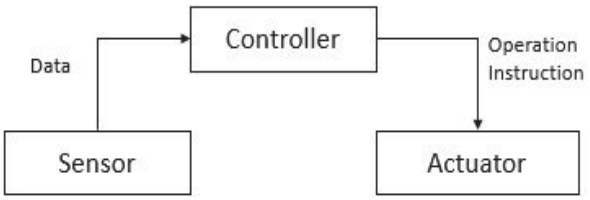

Fig. 1 CPS

Recent researchers for IoT and CPS focus not only things but a human [2], [3]. Typically, there is a research for Human-in-The-Loop (also referred to as HiTL) where at least one human is incorporated as a part of a process system. HiTL would be a key theory in expansion of CPS.

A. Review of Previous Researches

John A. Stankovic mentioned HiTL system that incorporates at least one human in IoT system [2]. He said one of the problems people should solve is that the need for comprehensive understanding of the spectrum of types of HiTL, and the applications of HiTL can be classified into the following four categories.

1) Applications where the human directly controls the system
2) Applications where the system passively monitors the human and takes appropriate actions
3) Applications where physiological parameters of the human are modeled
4) Hybrids of 1), 2), and 3)

The following control modes are carried out in the applications of the categories 1), 2) and 3).

- In applications of category 1), the system usually acts autonomously but the human operates the system only when it is necessary under supervisory control.
- In applications of category 2), behavior of the human is observed so that interventions are controlled to improve his/her quality of life.
- In applications of category 3), the process accepts a command, carries out the command autonomously, reports the results and waits for further commands to be received from the human.

Further, David et al. mentioned HiTLCPS [3]. This system is based on not only IoT but CPS, considering human interactions through the means of the applications of these four categories in [2]. And, they also stated about categories of HiTLCPS applications. Fig. 2 shows the categories of the applications of HiTLCPS for explaining management techniques.

In a management technique of Human Control of left side circle in Fig. 2, Direct Control is provided for a manner where a human manipulates directly a system. In this manner, the human will join a management of the system only when needed. On the other hand, Supervisory Control is provided for a manner where the human instructs throughout a process more directly than in a case of Direct Control. In Supervisory Control, a relationship between one who gives instructions and one who receives instructions is clearly understood.

In another management technique called as "people-centric sensing" by David et al. [3], of Human Monitoring in the right side circle of Fig. 2, two categories, namely Open Loop and Closed Loop. In Open loop, a system monitors human information whereas in Closed system, a system uses collected data and processing results in order to make a human contribute to a specific goal.

H. Shintani is a master student of Department of Architecture, Civil Engineering and Industrial System Management, Nagoya Institute of Technology (phone: +81 52-735-7177; e-mail: h.shintanni.406@nitech.jp).
I. Koshijima is a professor of Nagoya Institute of Technology (e-mail: koshijima.ichiro@nitech.jp).

Hybrids formed by overlapping Human Control and Human Monitoring is provided for a management system that incorporates these two methods.

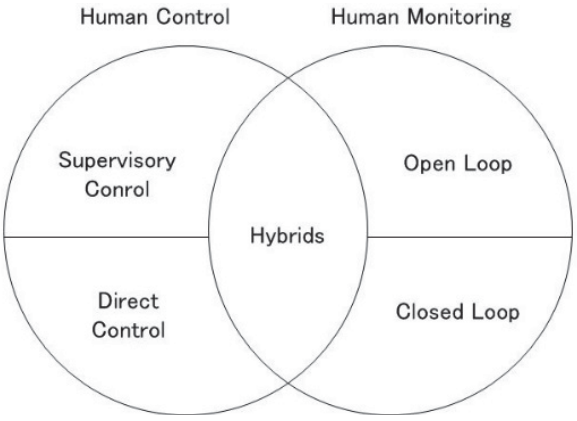

Fig. 2 Taxonomy of human-in-the-loop applications

B. Problem Statement

Although researches as to HiTLCPS which is based on the concept of CPS have already been made, a HiTLCPS for a large number of persons might be different from a case of HiTLCPS for a single person. In HiTLCPS for a large number of people, feedback of the process loop should be connected to the individual person correspondingly. Thus, in light of the difference in treatment of human, it is necessary to study HiTLCPS for the large number of persons.

In structuring and conducting a management system based on IoT and CPS, a security system has been studied for protecting the system against different attacks such as a cyberattack on network or directed to devices and the like. Additionally, in HiTLCPS where humans are incorporated as a part of the system, "safety" for the humans must be also considered. Precisely, a desired system should be protected against the attacks and more importantly, in the desired system, the safety of the person is ensured in the first place. However, since such safety has not been studied sufficiently, it should be considered deeply how to ensure the safety in HiTLCPS incorporating one person or a large number of persons. In this paper, therefore, frameworks for defining the following two issues are discussed.

1) HiTLCPS intended for a large number of persons
2) The safety for HiTLCPS

II. Safety Framework of Multi Human-in-The-Loop CPS

A. HiTLCPS Intended for A Large Number of Persons

As stated before, CPS is composed of the three units, the sensor, the controller, and the actuator. Among the three units, those operated by these persons are part of the sensor and that of the actuator. As studied in previous researches, role of the controller is undertaken by two types of control; namely, system control by these persons and automatic control by the system. When the large number of persons are charged in the role of the controller, there is a possibility that difference in decision-making is caused depending on a person. Due to such situation, control loop of HiTLCPS would fall in the unstable system. Thus, if a system incorporates humans as controllers, instead of placing them depressively, it is desirable to configure a system in which one person is charged so as to perform a centralized management. Therefore, when the large number of persons are incorporated in HiTLCPS as the sensor and the actuator, not only how to incorporate them but how to control the humans charged in the sensor and the actuators are discussed in this section.

1) Human as the Sensor

When CPS incorporates humans as sensor into part of process, the data to be collected are the character that contains the abilities each person owns and the status on what condition each person is. In recent years, because of the development of sensor technology, it becomes possible to collect various data. Therefore, by passing the things to be a sensor, the sensor can collect data as numerical value for the state of the human, and collected data that was not be measured until now by communicating over a network

Even the system obtains data from individual human in the crowd, it becomes essential to manage a tag-set with obtained data as shown in Fig. 3. And, it must also be made to the controller to be a receptacle of the data of the tagging from the sensor. In addition, to collect accurate information of capacity and features with the individual person, it is necessary for HiTLCPS to perform a feedback of the appropriate information against the person who provides the data.

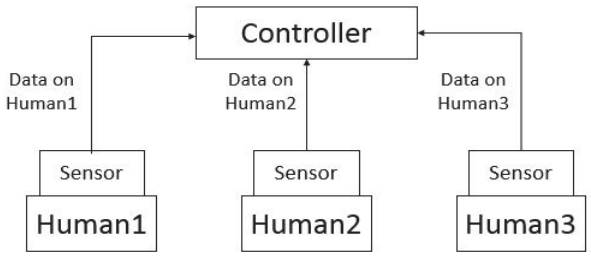

Fig. 3 HiTLCPS that human act as sensor

2) Human as the Actuator

An actuator performs an operation in order to realize the optimum condition derived in the controller. In conventional thinking, it is considered that the things as an object operate as the actuator, and things perform the provision of information to the person. However, under the situation a large number of people exist, it is difficult for the things to realize the all environment derived by the controller. Furthermore, system must provide information to human quickly at the real time in some circumstances. Therefore, it must be considered that the thing acting as the actuator is not only the thing of the object but humans. That is, by incorporating humans into CPS as the actuator, it is important to think about the system doing feedback of information directly having humans act like Fig. 4.

Unlike the conventional thinking, by performing feedback information to human directly for decision making that person moves, it is possible to change the role to do final decision making that perform decision making of actuator from

controller to actuator, especially human. Furthermore, it is possible to construct a flexible system to respond to changes in the environment dynamically. If system finally attempt to make the human as an actuator decision-making, it must be considered to think about the kind of information to be given.

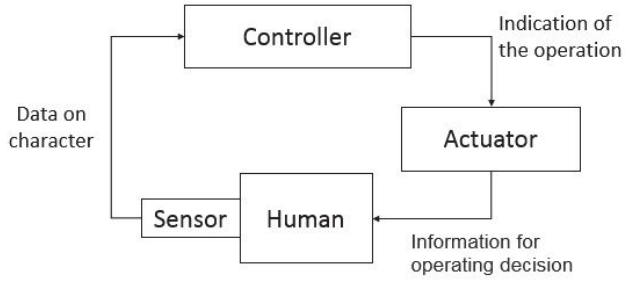

Fig. 4 HiTLCPS

Because continuing to impart extra information result in impairing for decision making, and there is the fear that prevent the make accurate judgment, it is essential that also performs selection of the type of information to be imparted according to the situation.

3) Controller in HiTLCPS

The control method to provide accurate information to human as controlled process based on the data sent from the sensor at real time is model predictive control. Model predictive control is a framework to continue to intelligence of the system by responding to changes in the situation by updating every moment the optimal control.

As shown in Fig. 5, the mathematical models to predict the response of a critical control object and the evaluation function to measure desirability of response are made separately from the controller for optimum control. And, after making, the model and function are added to controller to perform optimal control.

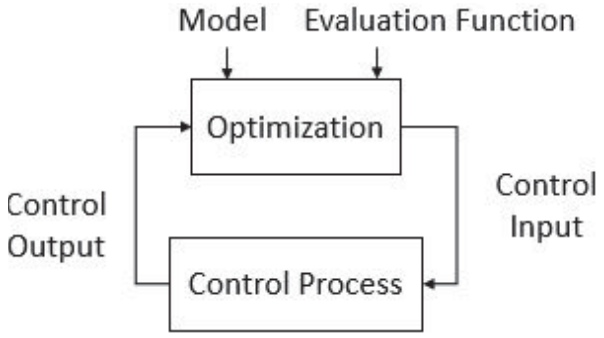

Fig. 5 Optimal control system

In the conventional model predictive control, it has been performed in a form that continue to add to the control system while disconnecting the calculation part of optimization in control from the control system. However, it takes time to achieve the optimal state in this form. Therefore, in recent years there is a form of performing optimum control by the controller of the control system. The system is shown in Fig. 5. By using this form of system, it is possible to calculate at high speed, so system can do optimal control in a short time. However, by expanding IoT increasingly, it is possible to collect big data, to use the technique for analyzing the data at high speed and even to construct mathematical model and the evaluation function for the model predictive control inside the controller. By realizing this, the optimization in control system becomes more high speed while controller constructs process model based on input data according to circumstances. Therefore, as a function should have the controller in HiTLCPS include the function of the following three points (see Fig. 6).

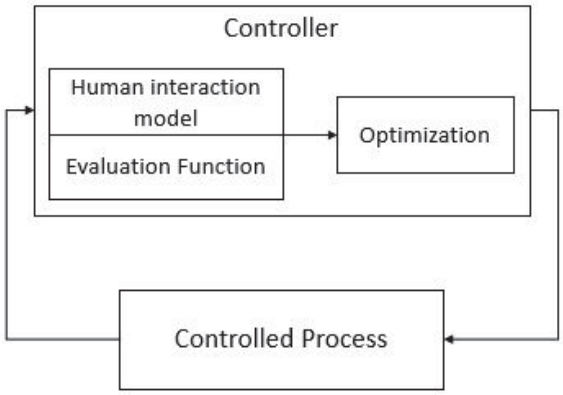

Fig. 6 Controller in HiTLCPS

1) Function to build human behavior models and evaluation functions (Human behavior model is the model which predicts the control output that indicates what kind of action target of humans move with respect to the control input)
2) Function for optimum control using human behavior model based on input data from the sensor
3) Function of performing feedback control for humans to be controlled a result of the optimization

If these three functions are built on a single controller, very hard load would be applied on the controller. Therefore, it is desirable to use cloud computing (below Cloud) as the controller because cloud computing can collect and analyze the enormous amount of data and withstand a large load as a controller.

B. HiTLCPS Considering Safety

In the conventional IoT systems and CPS, since for exchanging data via a network, discussions have been made about the system in a secure plane to protect the safety system from attacks such as cyberattacks and the Physical Attacks. However, in HiTLCPS, we should think not only safety that protects from system attack but also the safety of HiTLCPS which ensures the safety for human at all time.

Safety required in HiTLCPS is considered to have the following two profiles.

1) Functional safety
2) System Safety

Functional safety shows that the device involved in the system works normally, that is, it is required for device to work

stably and continuously in the IoT system without any harmful actions. The requirement for device is also to keep exchange data stably even under changing environment. However, IoT system is not composed of only the device, and performs an operation while working together with various things over the network. In recent years, the system configuration has become more complicated, and HiTLCPS involves not only things but humans. So, to considering the safety on HiTLCPS, the system must fulfill the functional safety at first. And, after ensuring the functional safety, the system should be considered about the system safety that ensures the safety of the entire system. Therefore, accidents caused in HiTLCPS include the factor that can be limited to one component, that is, the factor also according to the interaction of multiple elements. In addition, it must be considered not only interaction inside machines but the interaction between human and machine. So, as a model of accident that can occur in a complex configuration system is produced, in this paper the STAMP (Systems-Theoretic Accident Model and Process) theory is used (See Fig. 7).

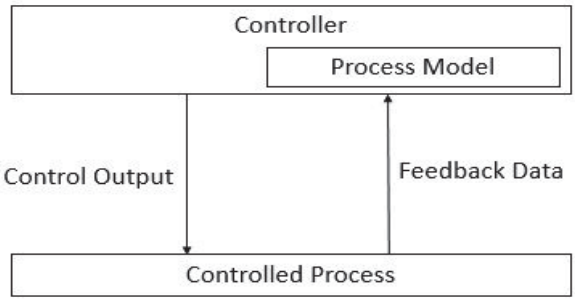

Fig. 7 STAMP model

STAMP is the accident model that has been proposed by Leveson professor in 2012. STAMP states that safety of systems are intended to be emergent from the interrelation of components, and many modern system accidents are caused by not working interaction properly between the controller that controls for safety and the controlled process that is controlled element [4].

In particular, the main cause of the accident would be the condition that the Controlled Action (direction from Controller to Controlled Process) is not provided properly. Then, as a factor inappropriate control actions is given, actual behavior model and Controlled Process behavioral models included in the controller do not match. In the STAMP model, safety is ensured that interaction of the Controller and Controlled Process works properly. The figure representing the STAMP model is shown in Fig. 8 [5] where human and system are incorporated as a controller.

Controlled Process in HiTLCPS is a human. Subject who must ensure safe at the very beginning in HiTLCPS is a human, especially human life. One of the factors that does not ensure safety for human in HiTLCPS is that the appropriate operation instruction is not granted from the controller. The reason why this occurs is where the interaction of people and the controller does not work properly.

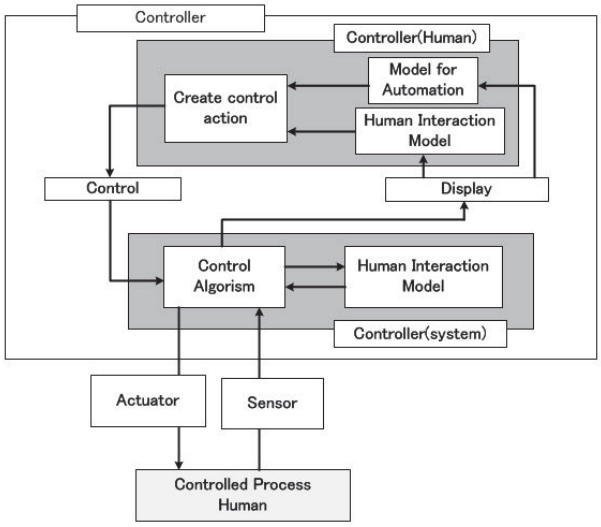

Fig. 8 HiTLCPS fitted to the STAMP model

Here, what is considered as a factor in the accident that interferes with the safety system of in HiTLCPS fitted to the STAMP model occurs are the following two points.

1) Human interaction model controller should recognize cannot reproduce the human behavior in the real world faithfully
2) Controller cannot provide the accurate control instructions reliably to human as controlled process

The first factor is in question of the controller. Specifically, when controller controls with the collected data, it is impossible to derive optimal information to feed back to human if controller does not include the human interactive model reproducing the human behavior in the real world. Modeling how human act properly and making the model the basis of control algorism would be the important factor of control performed by the controller.

The second factor is to deliver certainly information to be fed back to human derived by the controller. If the information would not be delivered certainly, human has possibility of performing high risk decision in the condition there are insufficient information for human to make decision. Therefore, in order to avoid decision making in lack of information state, it is essential for HiTLCPS to provide the information at the right time to protect human.

Previously, the accident factor using STAMP model in terms of the interaction of the system was described. However, STAMP model is merely accident model, STAMP is not the theory for analyzing whether system is safe. Further, in constructing a specific system based on HiTLCPS, it is also necessary to analyze whether the system is safe for humans in the design phase of the system. Thus, when analyzing the security of the system, the analyzed method is not only STAMP model but also STPA (System Theoretic Process Analysis) which is the safety analysis method which is based on STAMP model.

III. Illustrative Example

In this section, the framework discussed in the previous section is illustrated by using a HiTLCPS for evacuation system.

When the disaster has occurred, it must be made a priority evacuation to ensure the safety. However, people who carry out the evacuation cannot make the appropriate assessment under the emergency situation because they would be so panic that they cannot keep the normal state of mind of trying to act in top priority to safety. Not only that, while evacuation routes have been specified in advance in a normal, the evacuation route available would also will change by changing the damage status for the disaster. Considering these situation, it is necessary to provide appropriate information to the human in order to realize rapid evacuation. In evacuation system, giving accurate information to human more real-time is required, and to ensure the safety for human at all time is also required because human life is involved. In this case, considering that human is incorporated as part of the process in the evacuation system, go forth about what should be any system.

At first, people in HiTLCPS should act as sensors. The data to be collected at the time of incorporation of the "Human as the Sensor" to the system is data on a specific feature with each person. But, although it may be desirable to collect accurate information on the human outgoing, it is not possible to guarantee the certainty that things work accurately at the time of emergency. Therefore, in order to incorporate the Human as sensor, we should do approach in not only transmitting information from thing humans have, or using another technique, such as Human Monitoring using setting camera, which said that where there are people and how many people are. In this system, a smartphone each human may has is expected as the thing to collect data related to individual human. Through an application that takes into smartphone, it sends the information about the environment of the characters, the information around the current position, and information on smartphone holders to the cloud.

If HiTLCPS incorporate the humans as actuator, the point to be careful is that human who placed under special circumstances may not be able to make a calm decision. So, we must think about the way to provide the information that aid of decision-making to perform a calm judgment against the person. And concrete examples, the way is that show the way to go on the wall and floor existing in front of the eye. As a result, HiTLCPS must be a loop structure like putting out the instructions on a case-by-case basis after having collected the evacuation routes and information of people. To realize these requirement, things on walls and floors must also be kept connected to the network. In addition, it would be required for the whole building to be managed by the network.

Next, the controller in evacuation system should be defined. The resource for use in performing analysis of the collected data at controller is Cloud computing (below Cloud). Cloud collect and control the data sent from the smartphone and the camera in the building. The control method in the cloud is model predictive control. Control performed in the cloud is a model predictive control, model showing the human behavior which to be basis of the control are created on the cloud based on the collected data. Model will be changed in line with the change in the value of the data. Then, when performing optimal control in the cloud system, it performs optimum control using the data coming into the cloud as an input value of the control. After that, when performing control while monitoring the system by human on cloud, human corrects the control result while observing the control output derived in the cloud system.

In the evacuation system, since the system must perform the feedback of information to the Human more in real time, performing the data management and analysis in the cloud leads to increasing time all through the network until the feedback. Therefore, since it is possible to prevent data over-concentration for the cloud to be used as the Controller by using the Fog Computing placing things having another processing function between the device side and the cloud side, it should be considered that how the system analyzes the data when constructing the system in fact.

Based on the above, diagram of the evacuation system representing HiTLCPS based on STAMP model is shown in Fig. 9.

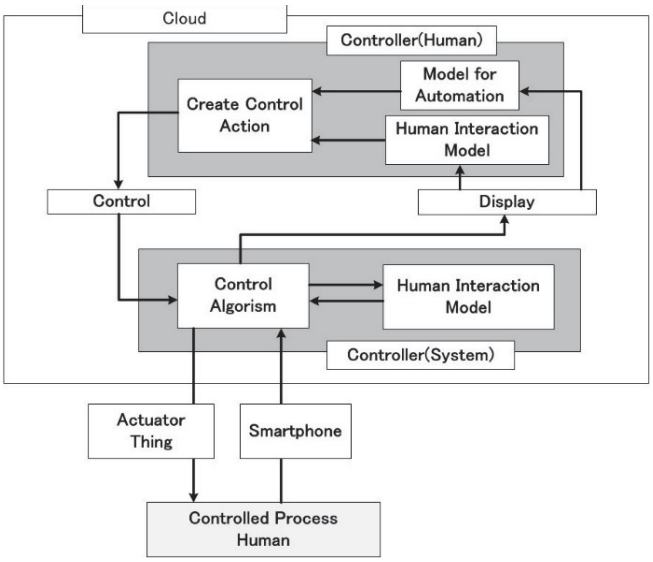

Fig. 9 Evacuation system based on STAMP model

The evacuation system should be performed as a safe HiTLCPS with reference to Fig. 9. What is the most important is to remain the safety of people in the system priority. For this purpose, it is essential that the network connecting the goods like the phone or in a building comprising a sensor and cloud operates stably. This condition is a functional safety feature among the safety required for the system, and system safety in a system device and humans each other involved in helping must be considered after filling functional safety.

For evacuation system, the system safety by using the STAMP model should be stated that the main cause of the accident would be the condition the Controlled Action (direction from Controller to Controlled Process) is not provided properly. In this concrete system, the Controlled Action is not given from the Cloud as controller to human as

controlled process.

As the factors that cannot be given the appropriate information, the timing of feedback the control algorithms may not be appropriate. The solution that timing of the control algorithms and feedback is not appropriate must be considered in the model predictive control. It is required to carry out experiences assumed a variety of environments in the process of building because to predict how much ahead of timing of the control lead to the acquisition interval of data collection. And, the accuracy of the human behavior model that becomes the base of the model predictive control also can be a factor of the system accident. For the improvement of model accuracy is, it is necessary only to collect only the minimum necessary data but to collect a variety of information. Therefore, data should be collected not only data as an input control and it must also include data collected only for model building. As before, it should be specifically considered that what information is collected and fed back actually in the course of building a system.

It has been described the safety of the evacuation system with a STAMP model as above, but on going to build actual systems, it must be done that analysis on system accident that can occur in the given conditions. This is cited as future challenges.

IV. Conclusion

The authors describe HiTLCPS incorporating human in the part of the system of the process based on the IoT and the CPS in this paper. Among them, HiTLCPS for crowded people and its safety are stated.

As the future of research, it is believed to carry out the implementation of a prototype system of a system using the HiTLCPS. While the implementation of this prototype system, it will be believed to specifically discuss what should be not only the safety of HiTLCPS but security.

Acknowledgment

This research was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (A), No.16H01837 (2016), and Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), “Cyber-Security for Critical Infrastructure” (funding agency: NEDO).

References

[1] MCPC M2M/IoT Committee, Shuichi Inada: “M2M/IoT TEXTBOOK” (in Japanese), 2015
[2] John A. Stankovic, Life Fellow, IEEE: ”Research Directions for the Internet of Things”
[3] Cabinet Office PFI Promotion David Sousa Nunes, Pei Zhang, and Jorge Sá Silva: “A Survey on Human-in-the-Loop Applications Towards an Internet of All”, IEEE Communication Surveys & Tutorials, vol. 17, no. 2, Second Quarter 2015Department, Action Plan for the Drastic Reform of PPP/PFI, 2013
[4] Information-technology Promotion Agency: For the first time of STAMP/STPA (in Japanese), Ver.1.0, 2016
[5] Nancy G. Leveson: ”Engineering a Safer World -Systems Thinking Applied to Safety-“ , The MIT Press,2011