Survey on Risk Management Based on Information Security Psychology

Yasuko Fukuzawa[1(✉)], Masaki Samejima[2], and Hiroshi Ujita[3]

[1] Yokohama Research Laboratory, Hitachi, Ltd., Yokohama, Japan
yasuko.fukuzawa.pd@hitachi.com

[2] Graduate School of Information Science and Technology, Osaka University, Suita, Japan
samejima@ist.osaka-u.ac.jp

[3] The Canon Institute for Global Studies, Tokyo, Japan
ujita.hiroshi@canon-igs.org

Abstract. In developing Cyber Physical Systems, such as smart grid and smart cities, risk management technologies play an important role to provide safe and secure services. In this paper, focusing on changes of recent threats represented by Social engineering, a survey shows that the information security psychology is valuable for the risk management of the Cyber Physical Systems. Through surveying, we outline the risk management framework for Cyber Physical Systems.

Keywords: Security · Cyber physical systems · Risk management · Information security psychology

1 Introduction

Cyber-Physical Systems (CPS) [17, 18], such as smart grid and smart cities, lets Control Systems cooperate with Cyber Systems strongly. CPS are integrations of computation, networking, and physical processes. Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa.

So far, in each of control systems and information systems, a technique to manage risk has been developed, e.g. the operational techniques such as hazard analysis and threat analysis, design of security systems architecture, the abnormal detection and diagnosis technology and so on. The techniques have been already used by various systems. However, malicious actions for systems are changing. The social engineering which used the psychological weakness of the person becoming a victim increases these days. "Advanced Persistent Threat" is known as a representative attack. Therefore, a framework of risk management that paid its attention to the psychology of an assailant and the victim is demanded.

The outline of this paper is as follows. In Sect. 2, we explain the risk of Cyber Physical Systems and introduce the Committee of this field. In Sect. 3, we discuss the framework of risk management based on information security psychology. In Sect. 4,

M. Kurosu (Ed.): Human-Computer Interaction, Part III, HCII 2015, LNCS 9171, pp. 396–408, 2015.
DOI: 10.1007/978-3-319-21006-3_38

we give information about trend of the information security psychology. In Sect. 5 concludes the paper.

2 Trend of IT Systems and IT Risk Management

This section shows the trend of IT systems, and the need of the risk management based on Information Security Psychology.

2.1 Cyber Physical Systems and IT Risks

Cyber Physical Systems (CPS), such as smart grid and smart cities, have critical assets, so risk management technologies plays an important role on providing safe and secure services. And CPS consists of not only various devices but also various human such as operators and general users. Because human is a main factor of risks, IT risks on CPS depend on human.

Figure 1 shows a constitution model of CPS. The control object of CPS is a system of the real world to show to a retainer of Fig. 1. The information of the real world is collected with plural sensors, and that is handed by a controller through a network. The user of CPS makes the analysis of gleanings and decision making of the necessary control using a controller and inputs control contents into a controller. The control contents are handed by an actuator through a network, and the actuator controls it for the real world. Therefore it is said that CPS is a system letting real world cooperate with the cyber world as an information processing environment. Considering a smart grid as one of CPU, we collect domestic power consumption and quantity of home generation of electricity with a sensor and control the power transmission.

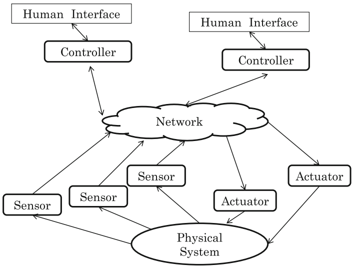


Fig. 1. Model of cyber physical system

Conventionally, there are a lot of systems controlling an object based on sensor information. However, CPS include a tight coupling of cyber world and real world, which is quite different from conventional systems. Based on the fact that consumers join as power suppliers that are unstable in a smart grid, we contribute to avoid blackout and improve the reliability. On the other hand, not only profit but also risk will happen due to the difference from the conventional systems. For example, a service stops by wrong information from the real world, which makes damage the real world. Risks of CPS also have been considered in the existing system, but the evaluation level of the risks may become larger than ever before.

The factors to decide a risk evaluation level are “Value of assets”, “threats”, and “Weakness (vulnerability)”. Therefore, it is important how you control these factors to reduce a risk level.

In addition, a risk in CPS is different from a risk in the existing system from the viewpoint of “Value of Asset”, “Threats”, and “Weakness (vulnerability)”. A large number of components cooperate complicatedly in CPS, which increases a risk level of CPS.

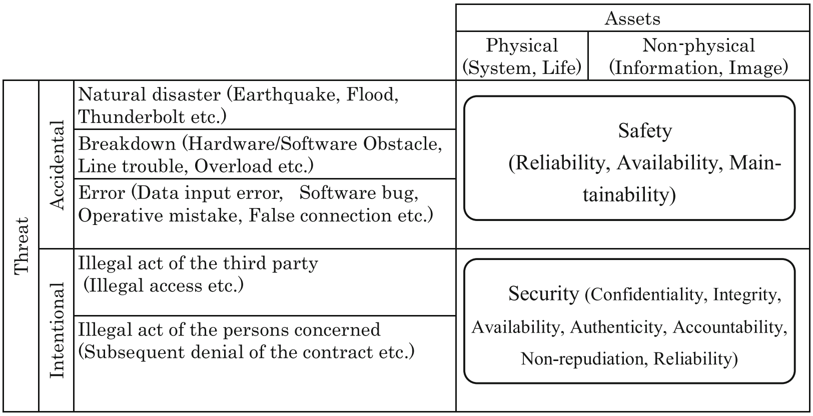
- An influence range by the attack spreads out. In other words, the value of assets is high.
- An attack point and assailants increase. For example, CPS includes not only an operator but also a general user, and the outbreak frequency of the attack increases.
- Conventionally, a vulnerable device is used in a system. This makes the system more vulnerable.

Based upon the foregoing, it is thought that the evaluation level of the risk in CPS is higher than an existing system, and sufficient risk management is necessary for CPS in the introduction.

2.2 Security and Safety

Table 1 shows a concept of “Security” and “Safety”. The threat about IT System is classified into two types. One type is Safety and the other is Security [1].

Table 1. Safety and security



			Assets	
			Physical (System, Life)	Non-physical (Information, Image)
Threat	Accidental	Natural disaster (Earthquake, Flood, Thunderbolt etc.)	Safety (Reliability, Availability, Maintainability)	
		Breakdown (Hardware/Software Obstacle, Line trouble, Overload etc.)		
		Error (Data input error, Software bug, Operative mistake, False connection etc.)		
	Intentional	Illegal act of the third party (Illegal access etc.)	Security (Confidentiality, Integrity, Availability, Authenticity, Accountability, Non-repudiation, Reliability)	
		Illegal act of the persons concerned (Subsequent denial of the contract etc.)		

Safety: It is a concept against an accidental threat (danger) that is in human, organization, and resources. It mainly points to the possibility that reliability, availability, and Maintainability of the information are lost. Examples include Natural disaster (Earthquake, Flood, Thunderbolt etc.), Breakdown (Hardware/Software Obstacle, Line trouble, Overload etc.), and Error (Data input error, Software bug, Operative mistake, False connection etc.).

Security: It is a concept against an intentional threat (danger) that is in human, organization, and resources. It mainly points to the possibility of the value loss. The value is asset's Confidentiality, Integrity, Availability, Authenticity, Accountability, Non-repudiation and Reliability. Examples include Illegal act of the third party and Illegal act of the persons concerned.

"Safety" means the protection from "Human Error", and "Security" means the protection from "Human Illegal Act". Threats are often caused by human factors. Therefore as well as technical measures, it is thought that legal and ethical measures are necessary to manage the risk that a malicious user produces intentionally.

The information security psychology is positioning working on from the psychological side of the relational person (an assailant and a victim) about the risk management of the IT system [2].

2.3 Need of the Risk Management by the Information Security Psychology

In risk management, it is extremely complicated but important to consider the psychological side. So, we organized a committee for survey of risk management based on information security psychology in The Institute of Electrical Engineers of Japan. The mission of the committee is as follows:

1. Investigation into need and trend of the information security from a psychological aspect in IT systems.
2. Investigation and analyses of information security psychology, information security economics, the risk evaluation technology.
3. Consideration and proposal which are based on (1) (2) for realizing resilient system.

The following shows the risk management framework based on the information security psychology by this activity [1].

3 Risk Management Framework

This section shows the framework of the risk management based on Information Security Psychology. The framework is considered by the action of the person concerned with an IT system to clarify the positioning.

3.1 Classification of Unsecured Act

The actions of the person whom a system may plunge into an undesirable state are known to be classified like Fig. 2 [4]. As for the unsecured acts, it is classified in having intention or not.

A conventional accident model is the domino model, in which causes of troubles and errors are analyzed and measures are taken. In the model, slip, lapse, and mistake are used which are the classification of the unsafe act to occur by on-site work. These are categorized as the basic error types, while violation which is intentional act violating rule has become increased recently and considered as social accident.

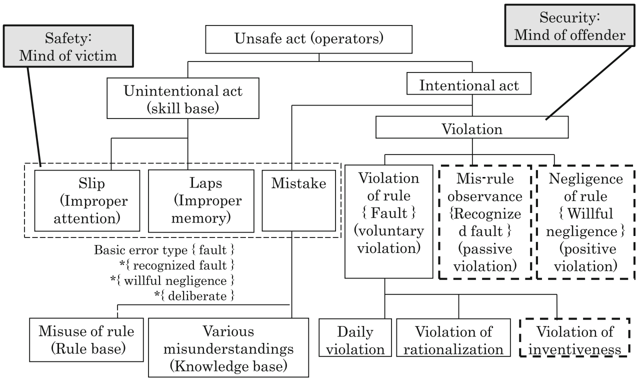


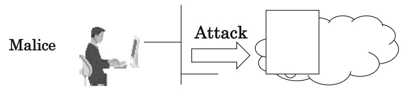
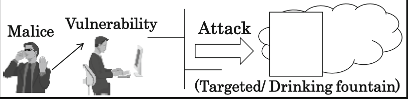
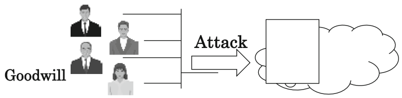
Fig. 2. Classification of unsecured act (modified Reason.J)

3.2 Model of Attack

Table 2 shows the classification of the attack model.

- Type1: Type1 is a direct attack type. This is the crime action that a system operator and an internal person and third party cause directly with malice. Type1 is human violation itself.

Table 2. Model of attacks

Direct Model	
Indirect Model (Social Engineering)	 Malice Vulnerability Attack (Targeted/ Drinking fountain)
Cluster Model (Accumulation of goodwill acts becomes malice: Recognized fault, or Willful negligence)	

- Type2: This is the indirect attack model that an assailant lets the operators such as operators cause human error. For example, there is increasing “advanced persistent threat” these days, this is so-called social engineering [3]. The assailant takes advantage of the weakness of a psychology and the action of the person becoming a victim. And a victim carries out the invasions to the facilities and a system, does the acquisition, the manipulation and the destruction of the information. For example, a link in the email text guides to the malice site that transmits a virus to PCs. The information in the PC is destroyed, and are sent to other PCs is known. As for such attack, the sender of the email pretends to be a manager and a reliable person and the distinction of a genuine article or the imitation is difficult and is hard to notice an attack. The act of the assailant is human violation, and the action of the victim is human error.
- Type3: This is a group model. It has no ill will for a personal action. However, it is taken an in total malicious action when they organize the group (willful negligence/fault of recognition). The authors analyzed the origin of an event in the use of the smart grid using Fault Tree. The event is that “Electricity consumption increased, and the administrator requested each section to save Electricity, but the member did not follow it, and, as a result, a blackout occurred” (See Fig. 3). According to the analysis, it is assumed that, “you will not need to cooperate with power saving because it is lost power and became last time” or “oneself will not need to cooperate because everybody will cooperate with power saving” causes a blackout. The psychology such as the optimistic fantasies in the group acts here. “Group thinking” consists of the following three categories [5].

- Overestimations of the group (Illusions of invulnerability creating excessive optimism and encouraging risk taking, Unquestioned belief in the morality of the group, causing members to ignore the consequences of their actions)
- Closed-Mindedness (Rationalizing warnings that might challenge the group’s assumptions, Stereotyping those who are opposed to the group as weak, evil, biased, spiteful, impotent, or stupid)
- Pressure Toward Uniformity (Self-censorship of ideas that deviate from the apparent group consensus, Illusions of unanimity among group members, silence is viewed as agreement, Direct pressure to conform placed on any member who questions the group, couched in terms of “disloyalty”, Mind guards : self-appointed members who shield the group from dissenting information)

The result of the analysis of Fig. 3 is explained by “Group thinking”. The action of the person depends on a personal characteristic and both environment and situation. The action in the group is known to regard a different action (including the social promotion, social loafing) as the action in the one.

From the viewpoint of Information Security Psychology, a victim becomes the weakness of the system and a victim causes human error. Studies on the state of the psychology of an assailant are not sufficient, but supported by criminal psychology research in the sociology.

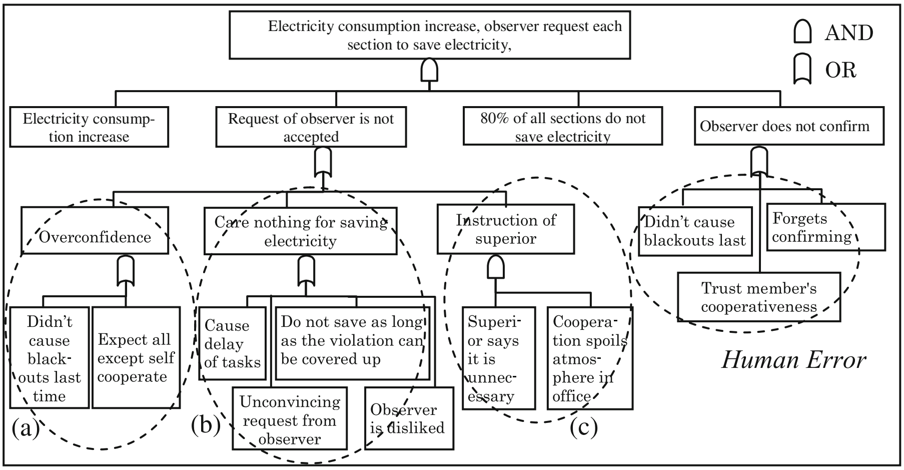

Electricity consumption increase, observer request each section to save electricity,
AND
OR
Electricity consump- tion increase
Request of observer is not accepted
80% of all sections do not save electricity
Observer does not confirm
Overconfidence
Care nothing for saving electricity
Instruction of superior
Didn't cause blackouts last
Forgets confirming
Trust member's cooperativeness
Didn't cause black- outs last time
Expect all except self cooperate
Cause delay of tasks
Do not save as long as the violation can be covered up
Unconvincing request from observer
Observer is disliked
Superi- or says it is unnec- essary
Coopera- tion spoils atmos- phere in office
Human Error
(a)
(b)
(c)

Fig. 3. Factor analysis of power failure outbreak

3.3 Situation

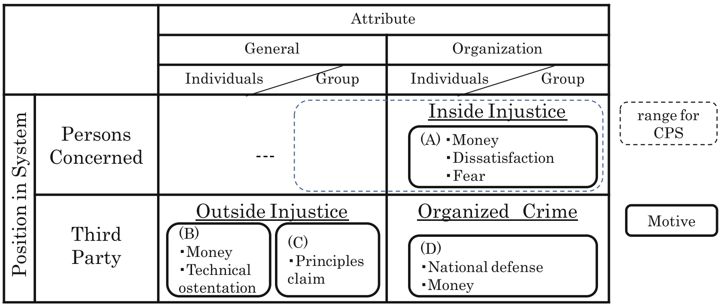
The action of the person depends on a personal characteristic and both environment and situation

- Position in System: An Illegal actor is the third party or the persons concerned. The case of the third party includes "outside injustice". The case of the persons concerned is "inside injustice".
- Attribute: The difference between a person in organization and a general publics are responsibility and regulation. Therefore, person in organization and general publics may do different acts on the same situation. In addition, the action in the group is known to regard a different action. For example, the collaboration performance per person in the group decreases with increase of the number of people in a group. This phenomenon is free rider or social loafing. Or work efficiency only costs because a large number of human beings perform the same work in a group. The social restraint that work efficiency decreases by social promotion and work contents or a motive produces a thing.
- Motive: Malicious mind causes "Human violation". The following is the malicious motives.

  – Intellectual play and mischief.
  – The money(profit) acquisition.
  – Political claim by hacktivist, or dissatisfaction
    And, on insider has another one.
  – Fear, uneasiness by the pressure from the neighborhood

On the Other Hand, Human Error Does not Have Motives. the Human Error Without the Intention Is Unconsciousness and Carelessness, and the Human Error with the Intention Namely the Mistake Is Misunderstood

Table 3. Injustice in IT systems



		Attribute	
		General	Organization
		Individuals / Group	Individuals / Group
Position in System	Persons Concerned	---	Inside Injustice (A) ・Money ・Dissatisfaction ・Fear
	Third Party	Outside Injustice (B) ・Money ・Technical ostentation (C) ・Principles claim	Organized Crime (D) ・National defense ・Money

range for CPS
Motive

Table 3 shows that the classified crimes in the IT system by based on (a)-(c).

- Internal Injustice: It is a crime caused by the person in the organization. The main motive is the acquisition of money and the result, pressure from dissatisfaction or the person concerned on organization (A).
- Outside Injustice: There are two groups. One group is hacktivist whose motive is Principles claim (C). The other group's purpose is intellectual play (offender for pleasure) and money acquisition (D).
- Organized Crime: This Crime is done by various groups (including Nation and Mafia) with organized intention (D).

A national security domain is the sky, the sea, the land, the space, and Cyberspace. Defense from (C), (D) in Cyberspace is very important. However, (C), (D) have the strong will and compelling force more than feeling, and it is difficult to treat it by information security psychology. (C), (D) are out of scope in this paper.

In addition, in CPS, person in organization may be mixed with a general publics. For example, certain person is consumer of the electricity at the same time as an electricity supplier in the smart grid. Of course, this is insider.

3.4 Risk Management Framework

Figure 4 shows the framework of the risk management based on Information Security Psychology. The risks in IT System are defined by Assets, Threat, and Vulnerability in the system, then goal of risks management is the controlling them. Not only the technical aspect but also the legal side and the ethical side are necessary to prevent the malice of the user from leading to a risk. It is necessary to utilize knowledge on various human factor cultivated in psychology and criminology. In the human factor utilization, there are two important points, one is person in organization and a general publics, and the other is human error and human violation.

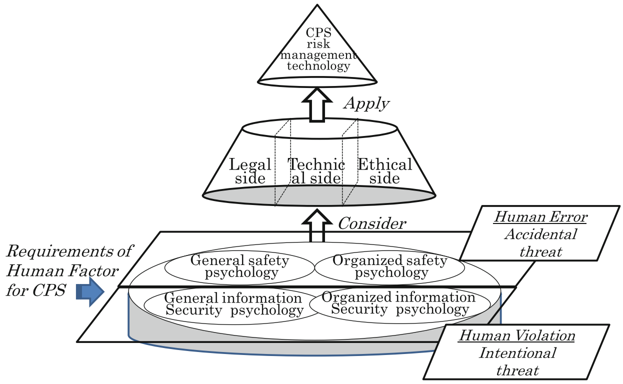

CPS risk management technology
Apply
Legal side
Technical side
Ethical side
Consider
Human Error
Accidental threat
Requirements of Human Factor for CPS
General safety psychology
Organized safety psychology
General information Security psychology
Organized information Security psychology
Human Violation
Intentional threat

Fig. 4. Framework of the risk management based on information security psychology

4 Risk Management Based on Information Security Psychology

The information security psychology is a stage arranging a systematic theory and frame based on an individual risk on a system. Based on this, the information security psychology for the risk of the IT system is described. In addition, the future directions of the risk management are described.

4.1 Inside Injustice

"Inside Injustice" is done by an Illegal actor who is the persons concerned.

One of the works about the "Internal Injustice" is MERIT (Management and Education of Risks of Insider Threat) [6]. This models the action of the internal unjust person using "Systems Dynamics" and analyzes the characteristic tendency and factor of the internal unjust person. "Systems Dynamics" is a technique to model the behavior of systems changing dynamically such as the time.

In addition, the countermeasure of the internal injustice is considered by using the criminal psychology knowledge. Requirements of the crime establishment are that "a crime attempter" meets at "opportunity of the crime". Specifically, the "crime opportunity theory" and "crime cause theory" are used. The "crime cause theory" is a way of thinking for preventing a criminal by removing the social cause of a criminal. On the other hand, "crime opportunity theory" is thought to prevent a crime by not giving a criminal the opportunity of the crime.

"Situational Crime Prevention" is based on "crime opportunity theory" [7, 8]. In this, "The environment of the place that a crime produces" is the main factor of the crime outbreak, and the environment factor should be removed. Based on "Situational Crime Prevention", five points of view to control internal injustice are arranged. The five points of view are "Increase the Effort", "Increase the Risks", "Reduce the Rewards", "Reduce Provocations", and "Remove Excuses". In conformity with this framework, examined measure concretely for the internal crime is reported [9]. In this report, individual about attack type1, 2, or 3; is not considered. By methodology cultivated in criminology, the examination of measures is accomplished generally. In this report, it is mentioned that the measures from the legal side and the ethical side are necessary.

In addition, according to the framework of the "Situational Crime Prevention", not only the real world but also the examination that is going to apply to the field of information security is accomplished [10]. In addition, there are working papers [11] and the guidelines [12] about the injustice on internal person.

4.2 Outside Injustice

An Illegal actor is the third party is "outside injustice".

Requirements of the crime establishment are that "a crime attempter" meets at "the opportunity of the crime". However, factors to make a certain person in the whole general public "a crime attempter" are various, and it is difficult to identify it. So the removal of the factor is difficult. Therefore, for the injustice by the third party, examination from the information security psychology is not enough regardless of type difference (type1, 2, 3) in attack.

About the outside injustice by the third party, intelligence to lead to outbreak is expected in future. For example, the relationship of the action of the user who is easy to encounter the damage of PC operation and cyber attacks such as an email or the Web is studied [13].

In the situation on the victim side of attack type2, there is examination to the example bass of the social engineering. A human characteristic (reciprocation characteristics, a commitment and consistency, social proof, goodwill, authority, rarity) causing the social engineering is pointed out [2, 3].

4.3 Risk Management by Model

It is not so easy to perceive risks appropriately, *e.g.* the risk that makes a huge loss and happens rarely has a tendency of being overestimated. Modeling humans and systems allows us to manage the risks.

Considering the importance of psychological aspects of using the system, we focus on modeling humans with considering psychological factors. *Trust* [14] is one of psychological factors that have an influence on human behaviors to risks. *Trust* indicates whether a user of a system can trust the system or not. Through researches on *Trust* in areas of social science, psychology, and economics, *Trust* is regarded as a composite concept of security, reliability, availability and privacy. Even though people use the same system that has the same risk, people who trust the system with underestimating the risks. On the other hand, people who do not trust the system with overestimating the risks. This makes people use the system more carefully. In other words, *Trust* gives users a sense of security. The sense of security may make users risky operations on systems. In general, users' behaviors to a system can be modeled by users' motivation and knowledge on the system when both of motivation and knowledge are good enough to use the system. When either of motivation and knowledge is insufficient, *Trust* is a useful factor to model human behaviors.

For constructing meta-models, it is necessary to consider a risk management framework based on a standardized guideline. For example, SGIS Toolbox [15] has been proposed as a risk management framework for SG. Based on existing guidelines [16] that are related to security, SGIS Toolbox makes it possible to relate the guidelines to components of systems. Figure 5 shows a flow of using SGIS Toolbox. For developing new services that are related to SG, the guideline requires that we define use cases of the services, identify components of Zones (Market, Company, etc.), Domains (Power generation, Power Transmission, etc.), and Interoperation (Business, Function, etc.) of the use cases, and refer guideline that are related to the components. If the use cases do not satisfy requirements in the referred guideline, the use case is regarded to have risks. The requirements are based on a range of power failure, importance of information assets and so on. Because CPS is used by not only expert operators of the system but also a lot of public users, a risk management model with psychological factors plays an important role on risk management. An example of a risk is conflict of interest among public users, which is related to group psychology. In order to mitigate the risks, it is necessary to extend attack models for CPS and to use approaches of crime opportunity theory and psychological theories of crime as indicated in information security psychology. In addition, approaches from aspects of low and morals are necessary, but we should not make lows to punish seriously people that damage systems without malice. In order to prevent the public users without malice from damaging systems, instead of punishing users, activities for improving IT literacy are also effective.

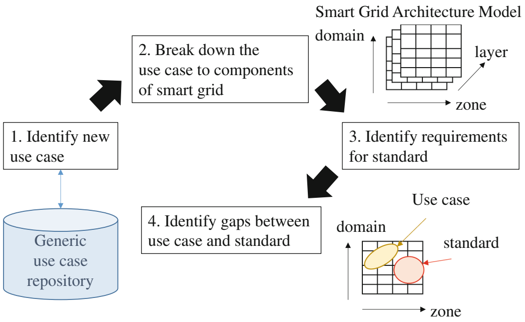

Smart Grid Architecture Model
domain
layer
zone
2. Break down the use case to components of smart grid
1. Identify new use case
3. Identify requirements for standard
Generic use case repository
4. Identify gaps between use case and standard
Use case
domain
standard
zone

Fig. 5. Flow of using SGIS toolbox

5 Conclusion

In this paper, focusing on changes of recent threats like Social engineering, the survey shows that the information security psychology is valuable for the risk management of the Cyber Physical Systems. Through surveying, the outline of the risk management framework for Cyber Physical Systems was described.

The outline was considered the situation of the psychological side. Examination about the internal crime is advances, because its knowledge is in the field of the human error field. However, the human violation and background in the outside crime have not been analyzed yet.

Based on this result, a new committee "the information security psychology investigation for IT system management technologies" was set up in The Institute of Electrical Engineers of Japan. In this committee, the discussion is continued.

Acknowledgement. This work was supported in part by the member of the committee for survey of risk management based on information security psychology in The Institute of Electrical Engineers of Japan.

References

1. Fukuzawa, Y., Samejima, M.: An approach to risks in cyber physical systems based on information security psychology. Inst. Electr. Eng. Jpn. Trans. Electron. Inf. Syst. **134**(6), 756–759 (2014) (in Japanese)
2. Uchida, K.: Information security psychology-information security from the human and psychology sides. J. Inf. Sci. Technol. Assoc. (Johono Kagaku to Gijutsu), **62**(8), 336–341 (2012) (in Japanese)
3. Hadnagy, C.: Social Engineering : The Art of Human Hacking. Wiley, Indianapolis (2010)
4. Yuhara, N., Inagaki, T., Furukawa, Y.: Human Error and Mechanical Systems Design. Kodansha, Tokyo (2012) (in Japanese)
5. Irving, J.: Groupthink: Psychological Studies of Policy Decisions and Fiascoes. Houghton Mifflin Company, Boston (1982)
6. Cappelli, D., Desai, A.G., Moore, A.P., Shimeall, T.J., Weaver, E.A., Willke, B.J.: Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers'Information, Systems, or Networks (2007). http://www.sei.cmu.edu/reports/06tn041.pdf
7. Smith, M.J., Conishi, D.B. (eds.): Theory For Practice in Situational Crime Prevention. Crime Prevention Studies, vol. 16. Criminal Justice Press, Monsey (2003)
8. Conish, D.B., Clarke, R.V.: Opportunities, precipitators and criminal decisions: a reply to wortley's critique of situational crime preventions (2003)
9. Amari, Y., Arai, S., Uchida, J.: Security Jitugen no Genten karamita Naibuyouin jiko youkuseishuhou. pp. 3–29. JNSA Press, Special Column (in Japanese)
10. Uchida, K.: Research of the application of situational crime prevention to information security (2010) (in Japanese). http://www.uchidak.com/InfoSecPsycho/20100922_uchidak01.pdf
11. Information-technology Promotion Agency, Japan: SoshikiNaibusha no Huseikoui ni yoru incident chousa (2012). http://www.ipa.go.jp/files/000014169.pdf

12. Information-technology Promotion Agency, Japan: Soshiki ni okeru NaibuFuseiBoushi guidelines (2013). http://www.ipa.go.jp/files/000027284.pdf'
13. Fujitsu Develops Industry's First Technology That Identifies Users Vulnerable to Cyber Attack Based on Behavioral and Psychological Characteristics. http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0119-01.html
14. Riegelsberger, J., Sasse, M.A., McCarthy, J.D.: The mechanics of trust: a framework for research and design. Int. J. Hum. Comput. Stud. **62**, 381–422 (2005)
15. CEN-CENELEC-ETSI: Smart Grid Coordination Group Investigate standards for information security and data privacy (2012)
16. Shimada, T.: Trends in standardization of smart grid cyber security. Inst. Electr. Eng. Jpn. Trans. Electron. Inf. Syst. **133**(3), 558–561 (2013) (in Japanese)
17. Lee, E.A.: Cyber physical systems: design challenges. In: Proceedings of 2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC), pp. 363–369 (2008)
18. Poovendran, R.: Cyber-physical systems: close encounters between two parallel worlds [point of view]. Proc. IEEE **98**(8), 1363–1366 (2010)