Requirement on Personnel and Organization for Safety and Security Improvement by Accident and Error Model

Hiroshi Ujita

Institute for Environmental and Safety Studies  
38-7 Takamatsu 2-chome, Toshima-ku, Tokyo 171-0042, JAPAN

[kanan@insess.com](mailto:kanan@insess.com)

**Abstract.** As a sequel to the technology systems becoming huge, complex and sophisticated, safety issues are shifted to the problem of organization from human, and further from hardware, such socialization is occurring in every technical field. For this reason, the analytical methods, as well as type and social perceptions of error or accident, are changing with the times also. Human error and Domino accident model had initially appeared, are then has been changing to system error and Swiss cheese accident model, and recently move to safety culture degradation and the organizational accident. Whereas the direction which discusses the safety from the accident analysis, a new trend of analytical methods such as resilience engineering, high reliability organization, or risk literacy research, which analyze the various events by focusing on the good practices, are becoming popular. To further, as the center of the information security field, the social engineering research has just begun as the recent research theme, to consider as the way to induce to a certain behavior of the person, by utilizing the essential weakness with the human, and its measures.

**Keywords:** Accident Model, Human Model, Social Model, Domino Model, Swiss Cheese Accident Model, Resilience Engineering, Bounded Rationality, Social Engineering

1. Introduction

Here, requirement on personnel and organization for safety and security improvement is discussed by using accident model and error model. As a sequel to the technology systems becoming huge, complex and sophisticated, safety issues are shifted to the problem of organization from human, and further from hardware, such socialization is occurring in every technical field. On the other hand, there is no science and technology that does not include risk, but it is also the fact that it has been accepted so far because it has utility beyond risk.

Whereas the direction which discusses the safety from the accident analysis, a new trend of analytical methods such as resilience engineering, high reliability organization, or risk literacy research, which analyze the various events by focusing on the good practices, are becoming popular. To further, as the center of the information security field, the social engineering research has just begun as the recent research theme, to consider as the way to induce to a certain behavior of the person, by utilizing the essential weakness with the human, and its measures.

The relationship between safety issues and security problems is summarized. In security problems, there is a difference from safety that it is necessary to think separately on the standpoint of perpetrators and victims. In the field of engineering such as information systems, attacks called "social engineering" that use psychological weak points of general users are on the rise, and it is difficult to ensure reliability only with technical measures such as information security. Human characteristics on security and its countermeasures are also dicussed.

1. History of Accident and human error type

The history of accident and human error type trend is shown in Fig. 1. In the era when the plant system was not so complicated as in the present age, it was thought that technical defects are the source of the problem and accidents can be prevented by technical correspondence. As the system became more complex, it came to the limit of human ability to operate it, accidents caused by human error occurred. Its typical accident happened at Three Mile Island (TMI) nuclear power plant in 1979. For this reason, individuals committing errors are considered to be the source of the problem, improvement of personnel capacity by appropriate selection and training of personnel, and proper design of interface design are considered effective for error prevention.

Thereafter, accidents caused by complicated interrelationships of elements such as technology, human, society, management, organization and so on occurred, and then the problem was interaction between society and technology. Furthermore, not only within the plant and enterprises but also accidents where the relationship failure with external stakeholders and organizations is a source of the problem becomes noticeable, and a framework for comprehensive problem solving including inter-organizational relationship has become to be necessary. A recent accident is a so-called organizational accident in which the form of an accident is caused by a complex factor and its influence reaches a social scale [1].

For this reason, the analytical methods, as well as type and social perceptions of error or accident, are changing with the times also. Human error and Domino accident model had initially appeared, are then has been changing to system error and Swiss cheese accident model, and recently move to safety culture degradation and the organizational accident.

1. Bounded Rationality in Context vs. Judge by God

In the field of cognitive science and the cognitive system engineering, the human being is considered as to think and judge something reasonably along the context while there are information and time limitations. Sometimes the decision may be judged as an error by the outside later. It is called "bounded rationality in the context" vs. “judge by God”. The absurd action of the organization had been often explained in human illogicality conventionally, while the approach has recently come out to think that the human being rationality was the cause.

There are three approaches proposed from Organizational (Behavioral) Economics as shown in Table 1 [2], business cost theory (reluctant to do), agency theory (information gap), and proprietary rights theory (selfishness). Business cost theory analyses action of opportunity principles and sunk cost, agency theory, moral hazard and adverse selection (lemon market), and proprietary rights theory, cost externality. The common supposition is "the bounded rationality and the utility maximization".

It is necessary to find the social context that the error is easy to occur, in the engineering for human being hereafter. In other words, a way of thinking has changed in the direction to analyzing the social context that is easy to cause an error, from analyzing direct cause of the error. Because this direction is beyond the range of conventional ergonomic treating the contents of the error, it is very difficult. However, we should recognize it now, if we do not analyze an error from the viewpoint of the relationship between safety and security with the environmental element surrounding human being, we can not to lead to measures. The measures should be matched with human rational characteristics.

Countermeasure on Business cost theory is business cost saving system which changes organizational style from group organization, via. centralization of power type organization, and to decentralization of power type organization, agency theory, agency cost reduction system based on mutual exchange of the information, and proprietary rights theory, internalization of the system externality based on proprietary rights distribution.

1. Accident model and Error model

As a result, that the technology systems become huge, complex and sophisticated, safety issues are shifted to the problem of organization from human, and further from hardware, such socialization is occurring in every technical field. For this reason, the analytical methods, as well as type and social perceptions of error or accident, are changing with the times also. Table 2 shows trends of the accident model and error model [3]. Human error and Domino accident model had initially appeared, are then changing to system error and Swiss cheese accident model, and recently move to safety culture degradation and the organizational accident.

A conventional accident model is the Domino model, in which the causation of trouble and the error is 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 type, while violation which is intentional act violating rule has become increased recently and considered as cause of social accident.

Design philosophy of the defense in depths has been established, and the accident to occur recently is caused by the excellence of the error of a variety of systems. The analysis of the organization blunder is necessary for the analysis by the Swiss cheese accident model in addition to conventional error analysis.

An organization accident is a problem inside the organizations, which reaches earthshaking event for the organization as a result by the accumulation of the best intentions basically. It is an act of the good will, but becomes the error. As for the organization accident, the interdependence inside of the organization or between the organizations is accumulated by fallacy in the defense in depths, and it becomes a problem of the deterioration of the safety culture in its turn. The organizational management based on the organization analyses such as behavioral sciences will be necessary for these measures.

Swiss Cheese Model proposed by Reason, J indicates operational problem other than design problem [1]. Fallacy of the defense in depth has frequently occurred recently because plant system is safe enough as operators becomes easily not to consider system safety. And then safety culture degradation would be happened, whose incident will easily become organizational accident. Such situation requires final barrier that is Crisis Management.

Concept of “Soft Barrier” has been proposed here [3]. There are two types of safety barriers, one is Hard Barrier that is simply represented by Defense in Depth. The other is Soft Barrier, which maintains the hard barrier as expected condition, makes it perform as expected function. Even when the Hard Barrier does not perform its function, human activity to prevent hazardous effect and its support functions, such as manuals, rules, laws, organization, social system, etc. Soft Barrier can be further divided to two measures; one is “Software for design”, such as Common mode failure treatment, Safety logic, Usability, etc. The other is “Humanware for operation”, such as operator or maintenance personnel actions, Emergency Procedure, organization, management, Safety Culture, etc. Following the safety design principle of “Defense in Depth”, three level safety functions should be considered for the hardware. Those are, the usual normal system, usual safety system, and emergency system including external support function. On the other hand, software for design including common mode failure treatment, safety logic, and usability should be improved together with the humanware for operation including personnel actions, emergency procedure, organization, management, and safety culture.

1. The methodology on Resilience Engineering, High Reliability Organization, and Risk Literacy

Whereas the direction which discusses the safety from the accident analysis, a new trend of analytical methods such as resilience engineering, high reliability organization, or risk literacy research, which analyze the various events by focusing on the good practices, are becoming popular.

The resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions. A practice of Resilience Engineering / Proactive Safety Management requires that all levels of the organization are able to [4]:

* Monitor
* Learn from past events
* Respond
* Anticipate

Organizational process defined by the High Reliability Organization is listed as follows [5]. There are 5 powers in 2 situations.

* Preparedness for Emergency Situation in Ordinal Time:
* Carefulness (Confirmation),
* Honesty (Report),
* Sensitivity (Observation),
* Emergency Response in Emergency Situation:
* Alert (Concentration),
* Flexibility (Response),

Ability of Risk Literacy is also defined by followings, which is largely divided to 3 powers and further classified to 8 sub-powers [6].

* Analysis power
* Collection power
* Understanding power
* Predictive power
* Communication power
* Network power
* Influence power
* Practical power
* Crisis Response Power
* Radical Measures Power

1. Relationship between safety issues and security problems

Table 3 summarizes the relationship between safety issues and security problems. In security problems, there is a difference from safety that it is necessary to think separately on the standpoint of perpetrators and victims. First of all, in the safety problem, basically the target is an expert, who is expected to be able to make efforts to ensure system safety based on good intention and ability. However, as individuals, safety consciousness deteriorates during the transition of safety activities for many years. Moreover, in the case of an organization, where the safety design based on the idea of ​​defense in depth is sufficiently realized, safety will be sufficiently kept even if it violates safely even in operation, so that experts would have the confidence in the safety of the system. As a result, eventually a chain occurs, where a defense in depth error that depends on the inherent safety of the system occurs, gradually deteriorating the safety culture, and that leads to an organizational accident. As a countermeasure against this problem, constant safety monitoring of the safety culture can be considered.

Meanwhile, when thinking about security issues, correspondence between perpetrators and victims is totally different, so consider the issues and countermeasures separately for this position. First of all, looking at the victim, the characteristic of the security problem is the need to think about countermeasures for general people as well as experts. If we consider about expert, the safety problem and aspect are exactly the same, and we can rearrange the problem by replacing safety with security. There are issues similar to general users as well as experts, but in addition to that, the lack of security literacy emerges as an important issue. The measures will be thorough security education.

The most difficult task is how to protect systems and users from perpetrators. The perpetrator can also be divided into an attacker from the outside and an internal criminal. In any case as it goes against the maliciously planned crime, the countermeasure is exhaustively and rationally carried out based on the system thinking is required. For internal criminals, it is often the case that the cause is greed or grudge, so it is important to maintain a common but healthy organization. For external attackers, internal measures such as thorough education cannot be used, so it is important not only to thoroughly build diverse barriers based on defense in depth thought, to counter social engineering technology targeting general users. It is essential to fully recognize the importance of psychological measures such as social psychology and criminal psychology.

1. Human characteristics on security and its countermeasures

In the field of engineering such as information systems, attacks called "social engineering" that use psychological weak points of general users are on the rise, and it is difficult to ensure reliability only with technical measures such as information security. The main methods of social engineering are impersonation to gather necessary information by impersonating others, garbage box fishing to acquire the desired information from among the things discarded as garbage, cleaning workers, electric / telephone workers, security impersonate as a member, invades the site into offices, factories, etc., peeping to acquire PC information from the back, and the like.

Social engineering is to induce people to certain actions by using the essential weakness of human beings, but there are also many studies outside the field of information security. One of them is systematization of human weakness in the study of Chardini [7], who gives six tactics as a tactic of guidance induction: "returnability", "commitment and consistency", "social proof", "favor", "authority", "rarity". In social engineering, measures against criminal psychology and others are also being applied, and countermeasures are currently being studied.

In the field of information security in recent years, there is movement to utilize psychology such as game theory and incentive mechanism and economic knowledge. However, due to the problem of subjectivity derived from human beings, difficulty of utilization has been pointed out. From the viewpoint of risk management of the system, it is important not only to reduce the risks derived from psychology and behavior but also to control the change in risk to suppress the fluctuation in the performance of the entire system, such as high resilience system is expected to realize.

1. Conclusion

As a sequel to the technology systems becoming huge, complex and sophisticated, safety issues are shifted to the problem of organization from human, and further from hardware, such socialization is occurring in every technical field. For this reason, the analytical methods, as well as type and social perceptions of error or accident, are changing with the times also. Human error and Domino accident model had initially appeared, are then has been changing to system error and Swiss cheese accident model, and recently move to safety culture degradation and the organizational accident. Whereas the direction which discusses the safety from the accident analysis, a new trend of analytical methods such as resilience engineering, high reliability organization, or risk literacy research, which analyze the various events by focusing on the good practices, are becoming popular. To further, as the center of the information security field, the social engineering research has just begun as the recent research theme, to consider as the way to induce to a certain behavior of the person, by utilizing the essential weakness with the human, and its measures.

To achieve safety and security, it is indispensable to consider not only the values and ethics of people, the behavior style (safety culture), but also the social acceptance and the impact on accidents on society and the environment. On the other hand, there is no science technology that does not include risk, but it is also true that it has been accepted so far because it has utility beyond risk. For that purpose, it is desirable to establish a systematization of safety science that can handle safety issues and security problems in a unified way.

**Acknowledgments.**

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. Reason, J.: ‘Managing the Risks of Organizational Accidents’, Ashgate, 1997.
2. Kikusawa, K.: ‘Absurdity of Organization’, DIAMOND, 2000 (in Japanese).
3. Ujita, H., Yuhara, N.: ‘Systems Safety’, Kaibundo, 2015 (in Japanese).
4. Hollnagel, E.: Safety Culture, Safety Management, and Resilience Engineering, ATEC Aviation Safety Forum, 2009.11.
5. Weick, K. E., Sutcliffe, K. M., ‘Managing the Unexpected’, Jossey-Bass, 2001.
6. Lin, S.: ‘Introduction of Risk Literacy- Lessons Learned from Incidents’, NIKKEI-BP, 2005 (in Japanese).
7. Chardini,R. B.: Influence, Science and Practice, 1991.

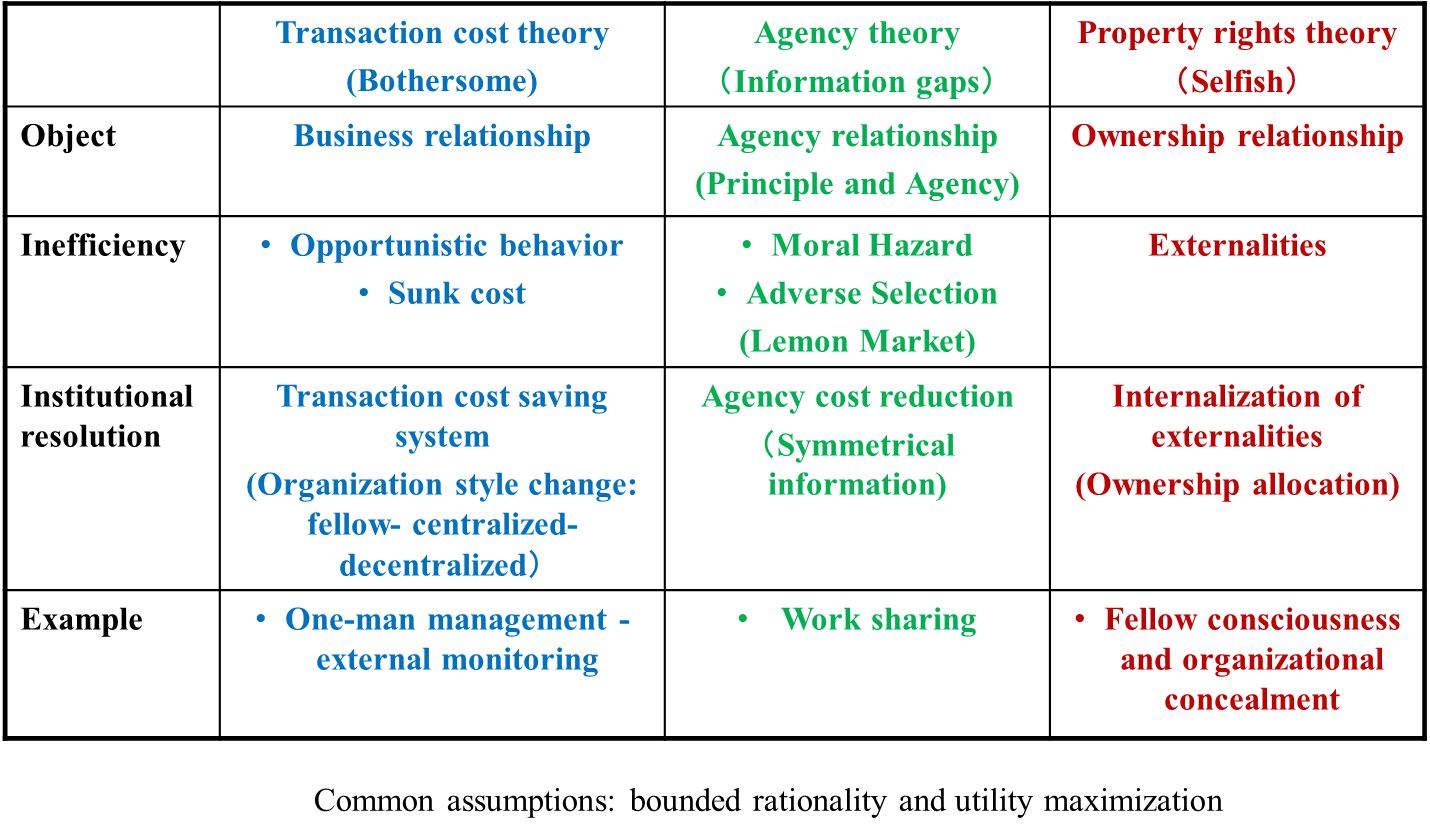
****

**Fig. 1**. Safety Issue Scope (Reason, 1993).

**Table 1**. Accident model and Error model.

****

**Table 2** Three approaches by behavioral economics  
 (The organization fails rationally: Kenshu Kikusawa 2009).

****

**Table 3** Relationship between safety issues and security problems

