METHOD FOR PROMOTING ICT ENGINEERING SAFETY

Takafumi Nakamura[1]*, Kyoich Kijima[2]

[1]Fujitsu FSAS Inc., Support Administration Group, G-7 Bldg., 7-16-12, Ginza, Chuo-ku, Tokyo, 104-0061, JAPAN, nakamura.takafu@jp.fujitsu.com

[2]Tokyo Institute of Technology, Graduate School of Decision Science and Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8550, JAPAN, kijima@valdes.titech.ac.jp

*Correspondence to: Takafumi Nakamura

ABSTRACT

In this paper, a method is proposed for promoting ICT engineering safety learning from crisis management. The current majority of methodologies for ICT use reductionist approach (i.e. lack of holistic view). Therefore, we need more holistic methodologies to realize system safety, and system safety should include human factors. In particular, ICT engineering arena human factors play a crucial role in promoting ICT system safety. The Tokyo stock exchange was crushed on 1st of November 2005 by an operation error, which had a severe impact on the global. The human factors (operator error, maintenance engineers' error, etc.) cause severe impact to not only ICT systems but also social systems (nuclear plant systems, transportation systems, etc.). A JR West train derailed and overturned on

25th April 2005 due to driver misconduct caused the loss of 106 passengers' lives at Kyoto in Japan. The progress of ICT technologies (i.e., cloud, virtual and network technology) inevitably shifts ICT systems into complexity with tightly interacting domains. This trend places the human factors above other elements to promote safety more than ever. The emergent property interacting between ICT and human conduct should be dealt with in order to promote system safety. Crisis management treats holistic property over partial component. We introduce a human error framework to promote a holistic view to manage system failures. An application example of ICT human error exhibits the effectiveness of this methodology.

Key words: Risk management; Crisis management; Normal accident theory (NAT); High Reliability Organization (HRO); Information and Communication Technology (ICT)

1. INTRODUCTION

Socio technical-systems are influenced by various environmental stresses. The main environmental stressors are political climate, public awareness, market conditions, financial pressures, competency levels of education, and the fast pace of technological change. The socio-technical system involved in the control of safety is shown in figure 1. In the context of system science, the safety of a system

should be dealt with differently from 4M (i.e. Man, Machine, Media and Management). Accident-causing theory is used to research the causes, process and consequences of accidents. The ‘4M’ theory is the theory summed up accident chain reaction theories, and is widely applied, which attributes accident to the ‘Man factor’, ‘Machine factor’, ‘Media factor’ and ‘Management factor’. For working team, foreman and worker is the main subject of the ‘Man factor’, and the ‘Machine factors’ include equipment, control system, structure, method of operation, ‘Media factors’ are the team's production process in working environment, technology environment, and ‘Management factors’ are mainly embodied in the safety culture, safety management assessment and so on. The components of 4M are a part of the safety of systems. Therefore, components of 4M do not necessarily guarantee the safety of a system. Figure 1 shows the hierarchy of socio-technical systems. The systems should be dealt with by using multiple disciplines to promote system safety. The upper side of figure 1 is the domain of wholeness, and the lower side is the domain of the parts that constitute the whole. The interpretations of wholeness are shown as Safety, Holistic, and System V, and those of the parts are shown as 4M, Reductionist, and System I. Systems V and I are terms from the viable system model (VSM) (Beer, 1979, 1981). A viable system is composed of five interacting subsystems which may be mapped onto aspects of organizational structure. In broad terms Systems I , II and III are concerned with the 'here and now' of the organization's operations, System IV is concerned with the 'there and then' – strategically responses to the effects of external, environmental and future demands on the organization. System V is concerned with balancing the 'here and now' and the 'there and then' to give policy directives which maintain the organization as a viable entity. A whole spectrum of viewpoints should be examined in order to solve safety issues. Improving the 4M of a part by concentrating on that part is not the solution to improving safety. We will explain this by using a Japanese train crash accident.

On April 25, 2005, Japan’s deadliest rail disaster occurred on the West Japan Railway Company’s (JR West) Fukuchiyama Line when a seven-car train derailed and overturned, claiming 107 lives. More than 500 people were injured. “The driver of the commuter train that crashed into a building in Amagasaki, Hyogo Prefecture, in 2005, killing him and 106 passengers, was worried about the conductor's radio call to the control center and applied the brakes too late as the train took a sharp curve too fast, a government panel said in a report released Thursday. The final report on the accident, compiled by the government's Aircraft and Railway Accidents Investigation Commission, also blamed West Japan Railway Co. for the accident, citing its punitive re-education program for train drivers who committed mistakes such as overruns leading to schedule delays. The commission, under the Land, Infrastructure and Transport Ministry, attached an opinion in the report urging JR West to give more practical training to improve drivers' skills and to place priority on safety when setting train schedules” (The Japan Times Online, 2007). According to the final report, there are at least five causes involved in the accident. They are 1.) human (The driver of the train was in a hurry

to make up for the delay caused by an overrun and was worried about possible consequences.), 2.) machine (The train was a lightweight train that would not automatically apply the brakes on the cars even if the train were exceeding the speed limit.), 3.) environment (Preceding the curve, the train ran along a long straight section where train drivers are apt to speed up; this curve was changed to the present 300-meter radius curve to gain a time advantage over its competitors), 4.) duty (The driver was vested with the duty of arriving at each station at a fixed time, observing the on-schedule operation rule.), and 5.) managers (The company executives adhered to a principle of showing little leniency, followed a policy of placing priority on profits, and placed the train diagram at the top of their agenda.). Implementing a driver re-education program is not the solution; instead, the whole spectrum of the five causes should be considered simultaneously in order to improve train safety. To completely understand the cause of accidents and to prevent future ones, the system's hierarchical safety control structure must be examined to determine why control at each level was inadequate at maintaining the constraints on safe behaviour at the level below and why the event occurred. The goal is not blame but to determine why well-meaning people acted in ways that contributed to the losses.

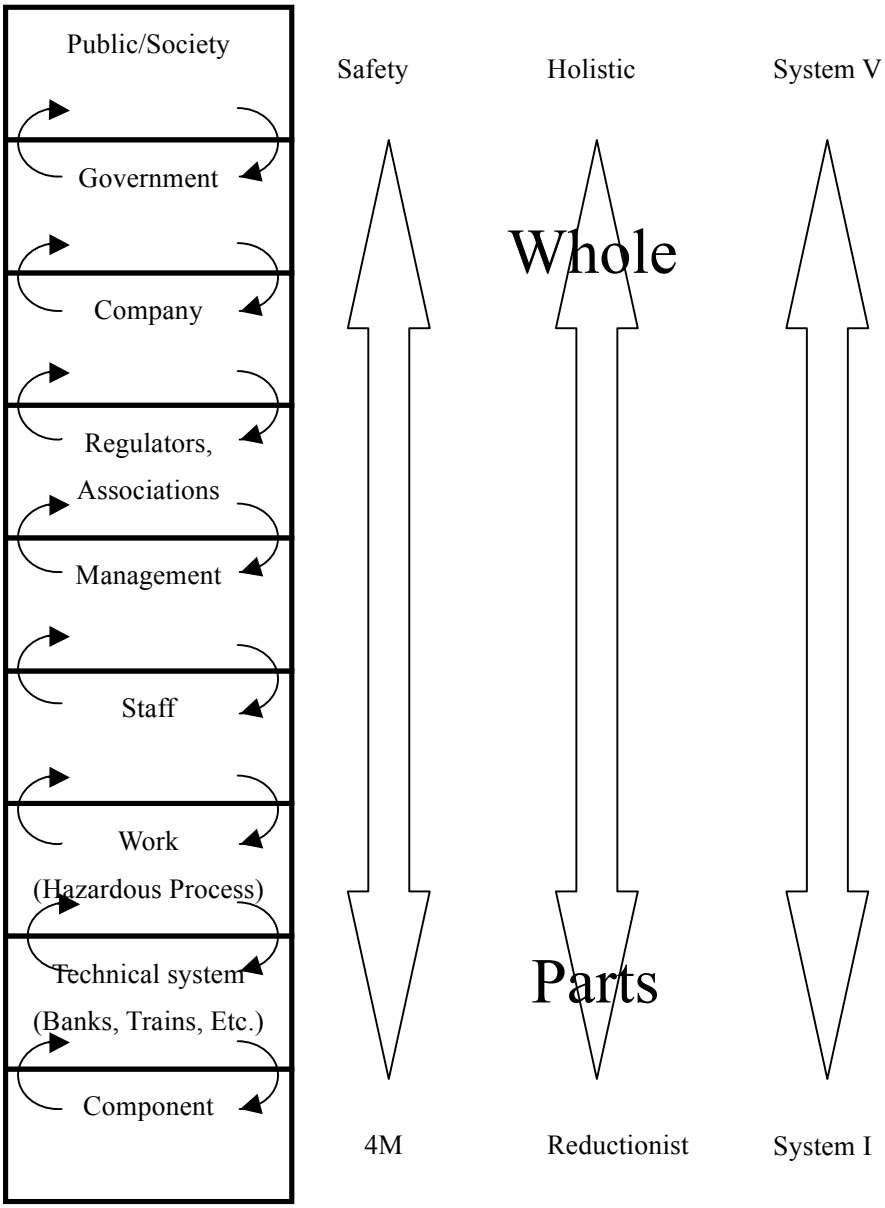


Figure 1 Socio-technical system involved in risk management

In chapter 2, we review risk and crisis management to show that they are approached from different angles in terms of the static and dynamic nature of systems. Risk management is approached from the static nature of system safety, and crisis management is approached from the dynamic nature of human working processes. We review two organization theories for managing system failures. They are the Normal Accident Theory (NAT) (Perrow, 1999) and High Reliability Organization (HRO) (Weick, 1987; Weick and Karlene, 1993; Weick et al., 1999). NAT sees systems with complex interaction and tight coupling as inevitable to fail, i.e., a normal accident. HRO realizes safety with people on the frontline working in a critical situation. As first glance, these two theories contradict

each other (Leveson, 2009). Thus, we introduce a risk management matrix to promote a holistic view. The two organization theories complement each other if we use this matrix. Also, the contribution of human error to system failures is examined, and hypotheses are presented that use parallel and sequential working models. The result of applying the matrix proves that the hypotheses and the human error framework are effective at promoting system safety in the ICT arena.

2. RISK MANAGEMENT VS. CRISIS MANAGEMENT

Risk management is the process of identifying, analyzing, and either accepting or mitigating uncertainty in investment decision-making. Unlike risk management, which involves planning for events that might occur in the future, crisis management involves reacting to an event once it has occurred. Crisis management often requires decisions to be made within a short time frame and often after an event has already taken place. Reflecting upon these definitions, risk management is a proactive notion, and it involves planning, estimation, and decision as preparation. Crisis management, however, is ongoing event management that concentrates on the here and now. If we view a system objectively, it requires a risk management methodology; however, if we view a system subjectively or from the human side, it requires a crisis management methodology. The following table outlines the differences between risk management and crisis management. It clearly shows that crisis management takes a proactive approach to risks and the stakes involved as well as the people concerned and all assets. To promote safety, both approaches are necessary. Table 1 summarizes the difference between risk management and crisis management.

Table 1 Risk management and Crisis management

	Plan	Focus	Approach
Risk management	People are part of the management	This plan addresses the identification of risks and the search for prevention and reaction measures to mitigate the risks. ***Focused on processes and operations.***	***Static approach:*** Take preventive action and implement emergency /contingency measures if an emergency or a disaster occurs. ***The organization is mainly REACTING to a threat.***
Crisis management	People are the main focus	This plan addresses the causes and the impact of risks, taking into	***Dynamic approach:*** Implement a crisis management plan as a part of an ongoing crisis

		consideration what is at stake. It seeks to protect all people and assets. ***People come first.***	management initiative. ***The organization is ANTICIPATING/BEING PROACTIVE/REACTING.***

2.1 Static view, i.e., Safety vs. 4M, and dynamic view, i.e., Individual vs. Team

Safety is a system problem. 4M is a component's ability to achieve safety. This suggests that measures to promote 4M itself are not enough to promote safety. Systemic problems, i.e., emergent problems, could not be addressed from the standpoint of 4M. The left hand side of figure 2 shows the view from risk management, i.e., static. We provide a ferry capsizing accident case as the left hand side's example (in figure 2) of systemic failure in the next chapter. The same discussion can be had for the human side. Team error is a system problem. Individual error is a component error within team error. This suggests that measures to prevent individual errors are not enough to prevent team errors. Systemic problems, i.e., emergent problems, could not be addressed from the standpoint of individual error prevention. The right hand side of figure 2 shows the view from crisis management, i.e., dynamic. The JR West derailment accident example of systemic failure provided in the introduction is the right hand side's example in figure 2.

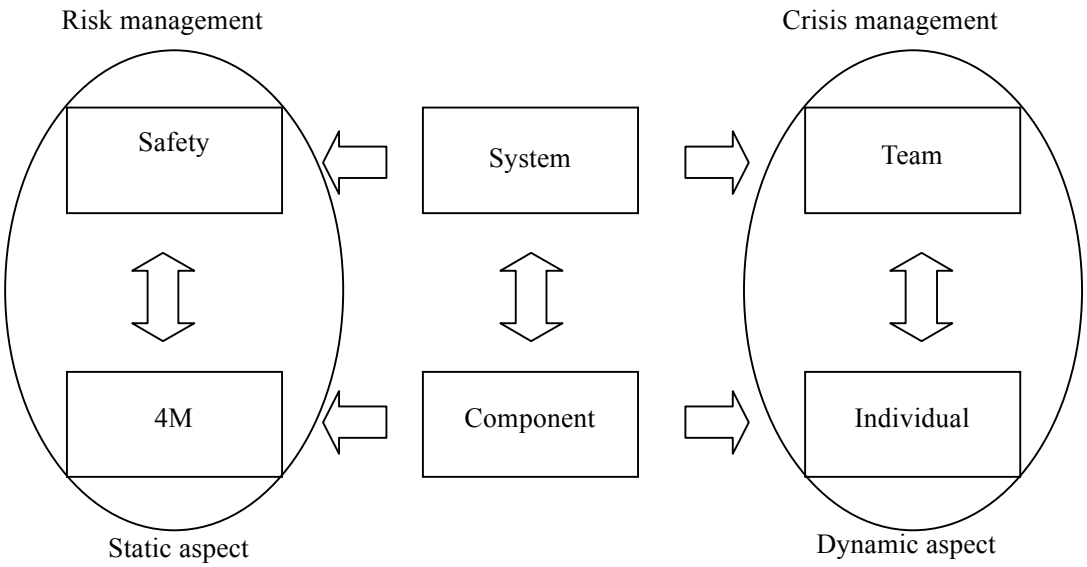


Figure 2 Different views between risk and crisis management

2.2 Safety is a system problem

The safety phenomenon occurs at the organizational and social levels above the physical system as illustrated by Rasmussen's analysis of the Zeebrugge ferry mishap (Rasmussen, 1997) shown in figure 3. In this accident, those independently making decisions about vessel design, harbour design,

cargo management, passenger management, traffic scheduling, and vessel operation (shown at the left of the figure) were unaware of how their design decisions might interact with decisions made by others, which lead to the ferry accident. Each local decision may be "correct" (and "reliable," whatever that might mean in the context of decisions) within the limited context within which it was made but can lead to an accident when the independent decisions and organizational behaviours interact in dysfunctional ways (portrayed by the intersecting rightward arrows in the figure). As the interactive complexity grows in the systems we build, accidents caused by dysfunctional interactions among components become more likely. Safety is a system property, not a component property, and must be controlled at the system level rather than at the component level. In this situation, modelling activity in terms of task sequences and errors is not very effective for understanding behaviour, so we have to dig deeper to understand the basic behaviour shaping mechanisms. In the next chapter, two major organization theories are reviewed, followed by an introduction of a framework for understanding and revealing a basic behaviour shaping mechanism.

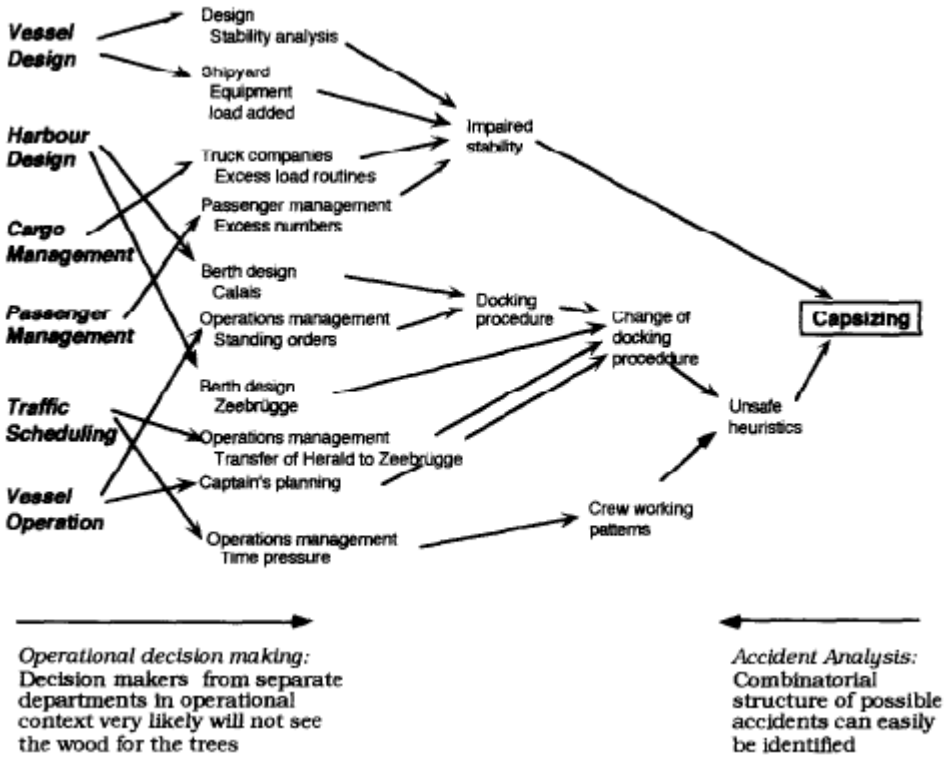


Figure 3 Complex pattern of the Zeebrugge accident

2.3 The two major organization theories (NAT vs. HRO)

As mentioned above, there are two major organization theories. One is the Normal Accident Theory (NAT), and the other is High Reliable Organization (HRO). Charles Perrow initially formulated what

has become known as NAT after the Three Mile Island nuclear power plant accident. His basic argument is that the interactive complexity and tight coupling in some technological systems, such as nuclear power plants, leads to the unpredictability of interactions, and hence, system accidents that are inevitable or "normal" (Perrow, 1999) for these technologies. In an optimistic rejoinder to Perrow's pessimism, Todd Laporte (LaPorte, Consolini, 1991) and Karlene Roberts (1990a) characterized some organizations as "highly reliable" because they had a record of consistent safety over long periods of time. By studying examples such as air traffic control and aircraft carrier operations, they identified features that they considered the hallmark of HROs, including technical expertise, stable technical processes, a high priority placed on safety, attention to problems, and a learning orientation. Weick et.al. (1999) later offered five characteristics of an HRO: preoccupation with failure, reluctance to simplify interpretations, sensitivity to operations, commitment to resilience, and deference to experience. In short, the HRO researchers asserted that organizations can become highly reliable and avoid system accidents by creating the appropriate behaviours and attitudes (Weick and Karlene, 1993). In particular, bureaucratic rules are seen as stifling expert knowledge; according to HRO theory, safety has to be enacted on the frontlines by workers who know the details of the technology being used in the respective situation and who may have to invent new actions or circumvent "foolish" rules in order to maintain safety, especially during a crisis. NAT theory focuses on the nature of the system, and HRO focuses on the human side, especially the frontlines. Both theories view systems from different perspectives in this sense they do not contradict but rather complement each other.

2.4 The general perspective for crises

Partial solutions are not enough to promote safety, as explained in the ferry accident example in the previous section. To solve the safety issue, we need a holistic perspective. The Briggs Myers matrix is a matrix for helping to identify the standpoints of methodologies, solutions, and perspectives (Mitroff, 2011). It consists of two basic dimensions: the horizontal, which pertains to the scope or size of a problem or situation that a person is inherently (instinctually) comfortable in dealing with, and the vertical, which pertains to the kind of decision-making processes that a person inherently (instinctually) brings to bear on a problem or situation. The framework is important because it shows that, for the how and why on any issue or problem of importance, there are at least four very different attitudes or stances with regards to the issue or problem. None of them is more important or right, so we need to check all perspectives intentionally in order to overcome psychological blind spots. Figure 4 shows the general framework.

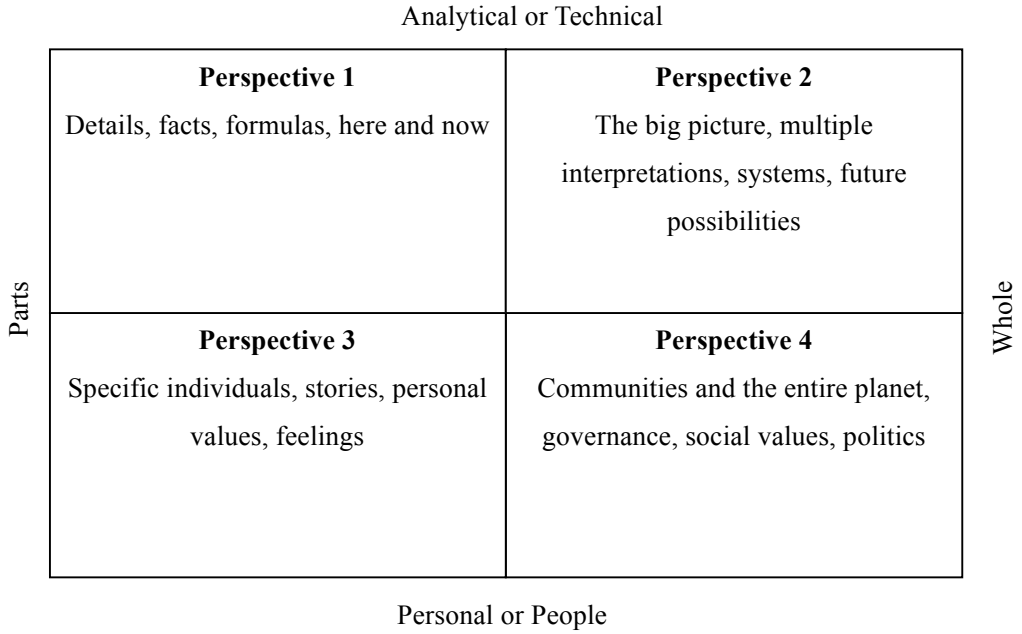


Figure 4 General framework

Figure 5 is the risk framework derived from the general frame work. The vertical dimension is the scope of the view of risk issues, and the horizontal dimension is the same as the general framework. 4M is more analytical and technical than is safety, which is more personal and social. In hindsight, the ferry accident is derived from perspective 2, i.e., a lack of multiple perspectives. According to the two organization theories discussed above, NAT is located in perspective 2, and HRO (including crisis communication) is located in perspectives 3 and 4. An informed culture, claimed by Reason (1997) to manage the risks of organizational accidents, requires free exchange of information, which requires a culture that is just, reporting, able to learn from itself, and flexible . An informed culture theory covers entire perspectives.

The risk framework is also useful for preventing problems by implementing various counter measures in a proactive manner. If current existing methodologies are mapped onto the risk framework, it is useful to identify vulnerable areas in the current state-of-the-art methodologies. Indeed, each position or stance picks up a basic sense or meaning of an important issue or problem that the others might either ignore or dismiss altogether.

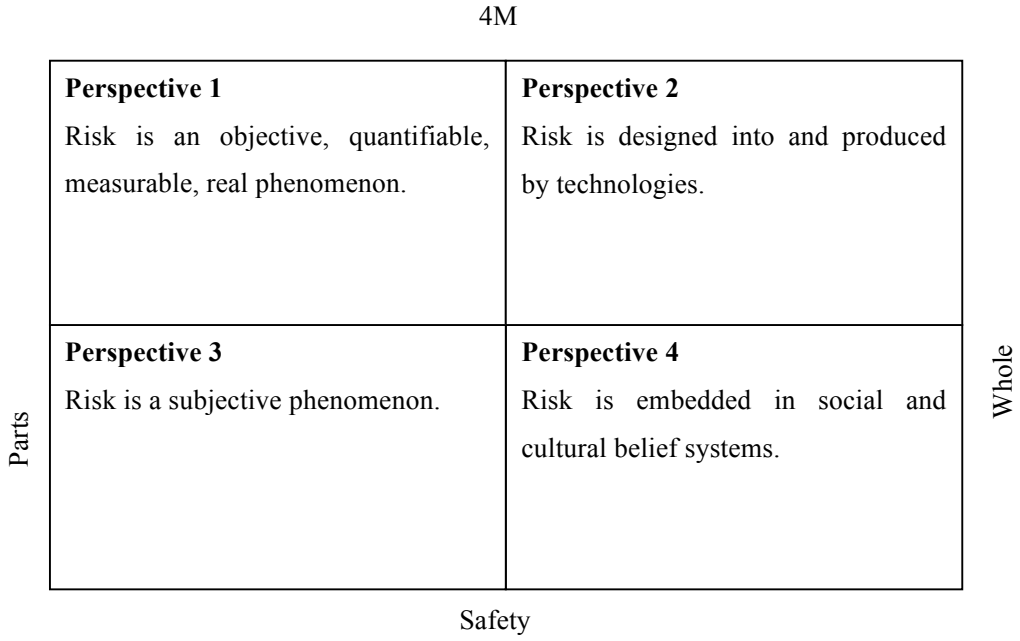


Figure 5 Risk framework

2.5 Human error contribution (Team error vs. Individual error)

Reason (1990) categorized human errors into three types: mistakes, lapses, and slips. Mistakes occur when an intended outcome is not achieved even though there was adherence to the steps in the plan. This is usually a case in which the original plan was wrong, was followed, and resulted in an unintended outcome. Mistakes are decision-making failures. The two main types of mistakes are rule-based mistakes and knowledge-based mistakes. They arise when we do the wrong thing, believing it to be right. Lapses are generally not observable events. They involve "Forgetting to do something, or losing your place midway through a task." Slips are generally externalized, observable actions that are not in accordance with a plan, that is "Not doing what you're meant to do." Table 2 summarizes human error types and typical examples to reduce errors.

Table 2 Classification of human error types

Error type	Occurring phase	How to reduce
Rule based mistake	Planning Decision making	■ Increase worker situational awareness of high-risk tasks on site and provide procedures for predictable non-routine, high-risk tasks.
Knowledge based mistake		■ Ensure proper supervision for inexperienced workers and provide job aids and diagrams to explain procedures.
Lapse	Execution	■ Make all workers aware that slips and lapses do happen, ■ use checklists to help confirm that all actions have been completed, ■ include in your procedures the setting out of equipment, site layout, and methods of work to ensure there is a logical sequence, ■ make sure checks are in place for complicated tasks, and ■ try to ensure distractions and interruptions are minimized, e.g., mobile phone policy.
Slip		

If we categorize the four human errors (table 2) onto the risk framework, we obtain figure 6. The vertical dimension has been modified from Parts-Whole to Individual-Team. When using this framework (figure 6), it is important to review current measures or management processes to check whether all perspectives are considered in order to have a holistic view. The JR West train accident example explained in the introduction can be applied to the human error framework. According to the example, there are at least five causes that were involved in the accident. They are 1.) human (Perspective 1), 2.) machine (Perspective 2), 3.) environment (Perspective 3), 4.) duty (Perspective 4), and 5.) managers (Perspective 4). Only giving more practical training to improve drivers' skills (to implement perspective 1's view) is not the solution in this case. Placing a priority on safety when

setting train schedules (managing perspective 4) should also addressed as The Japan Times Online (2007) indicated. The whole spectrum of the five causes should be considered simultaneously to achieve train safety.

4M

Perspective 1 Human error is an objective, quantifiable, measurable, and real phenomenon. **Slip**	**Perspective 2** Human error is designed into and produced by technologies. **Rule based mistake**
Perspective 3 Human error is a subjective phenomenon. **Lapse**	**Perspective 4** Human error is embedded in social and cultural belief systems. **Knowledge based mistake**

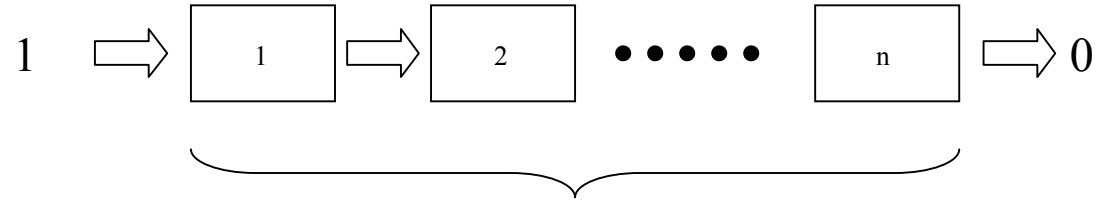
Individual

Team

Safety

Figure 6 Human error framework

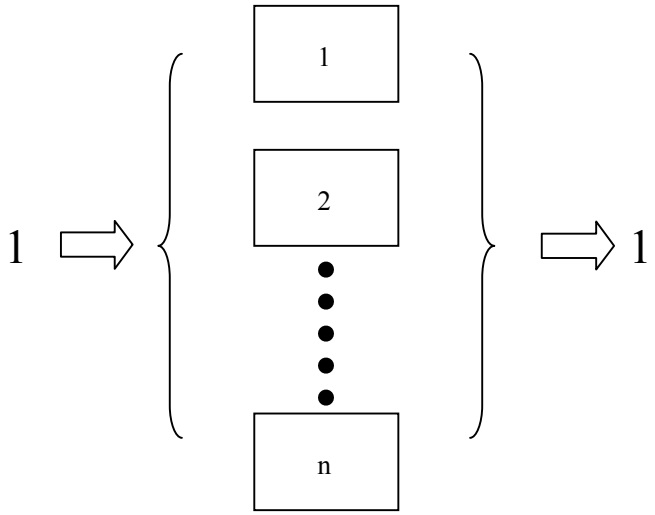
Now, we should further discuss the horizontal dimension in figure 6. To discuss team and individual working processes, which are more safer, we need a working process model. We introduce two simple models of the working process, i.e., the sequential and parallel models. Figure 7 shows the sequential model. It reduces safety depending upon the number of sequences of persons or groups. Each box represents one person who has an error ratio greater than 0%, i.e., all humans are not perfect. Then, theoretically, if persons are sequentially connected infinitely, the success ratio eventually becomes 0, i.e., 100% failure. S_i in figure 7 is the probability of success for i's person or group ($0 \leqq S_i < 1$).



$$\lim_{n\to\infty} \prod_{i=1}^{n} s_i^n \to 0$$

Figure 7 Sequential process model

To overcome this shortfall of the sequential model, it is natural to promote safety with a parallel working model. Figure 8 shows this model. It enhances safety with duplicating processes depending upon the number of duplicate persons or groups. Then, theoretically, if a person is duplicated infinitely, the success ratio eventually becomes 1, i.e., 100% success. f_i in figure 8 is the probability of failure for i's person or group ($0 \leqq f_i < 1$).



$$\lim_{n\to\infty}(1-\prod_{i=1}^{n} f_i^n) \to 1$$

Figure 8 Parallel process model

2.6 Hypotheses

According to the discussion above, we can derive two hypotheses.

1. Tight coupling area is less safer than loose coupling area.
2. A team working process (parallel) is more safer than is individual working process.

Table 4 summarizes hypothesis 2. The meaning of the error types in table 4 are explained in table 2. The meaning of the process types are explained in figures 7 and 8. Figure 9 shows the sequence of human error occurrence. The parallel team working is the lowest occurrence ratio followed by individual working process. And the sequential team working process is the highest occurrence ratio. The next chapter examines hypotheses in ICT systems.

Table 4 Hypothesis 2

	Error type	Process type	Occurrence ratio
Team errors	Mistake, Lapse, and Slip	Parallel	Low
		Sequential	High
Individual errors	Mistake, Lapse, and Slip	Single	Medium

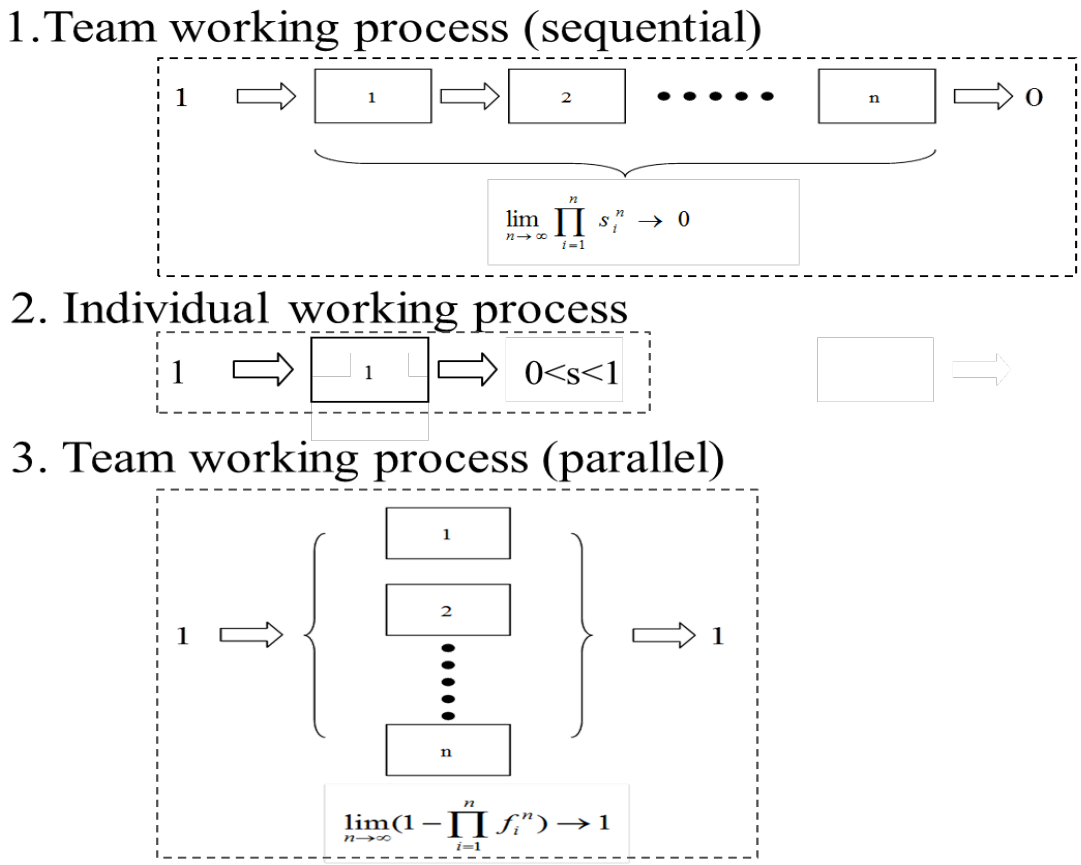


Figure 9 the sequence of human error occurrence ratio

3. APPLICATION TO ICT SYSTEMS

Computing systems are characterized by five fundamental properties: functionality, usability, performance, cost, and dependability (Avizienis et al., 2001). The dependability of a computing system is the ability to deliver service that can justifiably be trusted (Laprie, 1992). This property integrates the following basic attributes: reliability, availability, safety, confidentiality, integrity, and

maintainability. Conventional development models, either for hardware or for software, do not explicitly incorporate all the activities needed for the production of dependable systems. Indeed, while hardware development models (e.g., BSI, 1985) traditionally incorporate reliability evaluation, verification, and fault tolerance, traditional software development models (Waterfall: Royce, W. W., 1970, Spiral: Boehm, B. W., 1986, V: Forsberg, K. and Mooz, H., 1991, et al.) incorporate only verification and validation activities but do not mention reliability evaluation or fault tolerance. Several models are proposed (Kaniche et al., 2002) that are explicitly incorporated in a development model focused on the production of dependable systems. Comparatively, the failure analysis methodologies in computing systems are relatively few compared with dependability development. The major risk analysis techniques are explained in (Bell, 1989, pp. 24-27; Wang, J. X. et al., 2000, Chapter 4; Beroggi et al., 1994). Most failure analyses and studies are based on either failure mode effect analysis (FMEA: IEC 60812) or fault-tree analysis (FTA: IEC 61025). FMEA and FTA are rarely both performed, though, and when both are done, they will be separate activities executed one after the other without significant intertwining. FMEA deals with single-point failures by taking a bottom-up approach; it is presented as a rule in the form of tables. In contrast, FTA analyzes combinations of failures in a top-down manner, and the results are visually presented as a logic diagram. Both methodologies are used mainly in the design phase. However, they depend heavily on personal experience and knowledge. FTA in particular has a tendency to miss some failure modes in failure mode combinations, especially emergent failures. Current methodologies tend to lose the holistic view of the root causes of system failures. The majority of them stay as perspective 1 in the risk framework in figure 10. This suggests that, in order to promote safety, it is imperative to broaden the perspective to the other perspectives. Numbers 3, 4, and 5 in figure 10 are the number of key concepts and behaviours necessary for attaining high reliability.

3- Respectful interaction: trust, honesty, and self-respect (Campbell, 1990)

4- An informed culture: just, reporting, learning, and flexible culture (Reason 1997)

5-Hallmarks of HRO: preoccupation with failure, reluctance to simplify, sensitivity to operation, commitment to resilience, and deference to expertise (Weick et al. 1999)

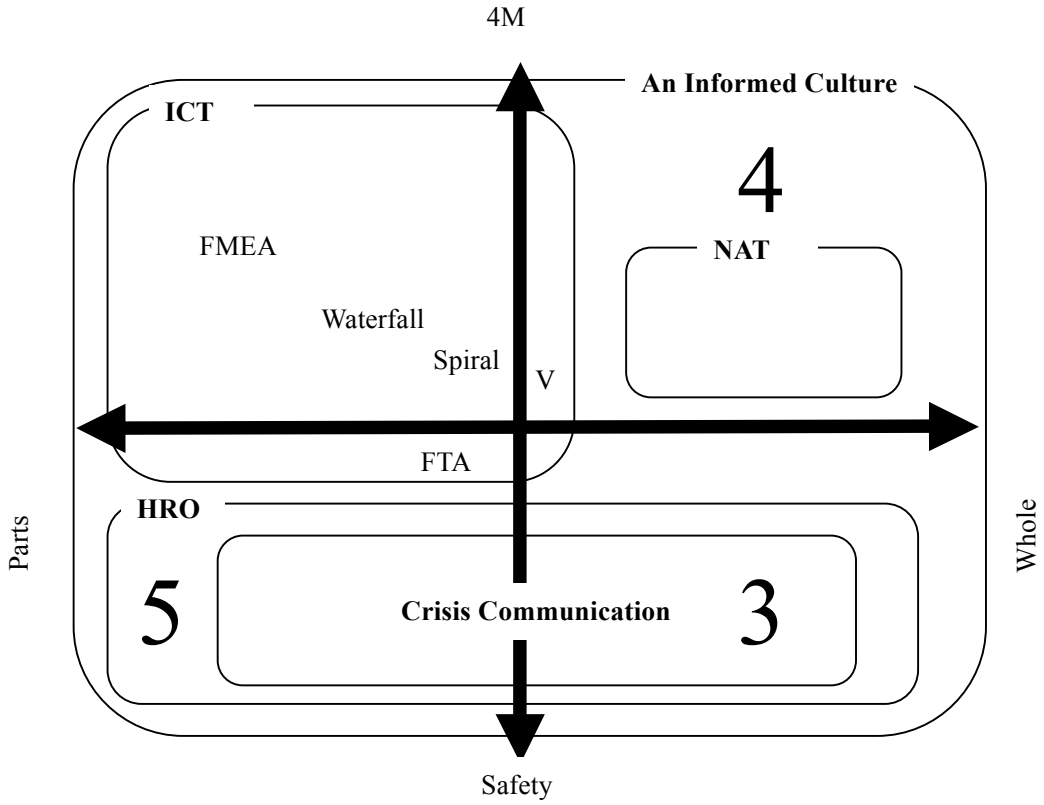


Figure 10 Mapping ICT methodologies onto risk framework

3.1 Human error contribution

Four systems were chosen to confirm the contribution of human error to the systems. They are banking, electricity and gas, manufacturing, and education systems. They are located in the IC chart (Perrow, 1999) from the Linear-Tight to Complex-Loose domains with the sequence from banking, electricity and gas, manufacturing and education systems. Figure 11 is the sequence of incident, human error and near miss. They are sequentially located from Tight-Linear (upper left domain) to Complex-Loose (lower right domain). Also liner interaction systems are prone to human error than complex interaction systems. The incident data are collected from four systems in the year 2012, 2013 and 2014 in table 5, table 6 and Table 7. Table 8, table 9 and table 10 are Incident per user occurrence ratio, human error per user occurrence ratio and near miss per user occurrence ratio respectively.

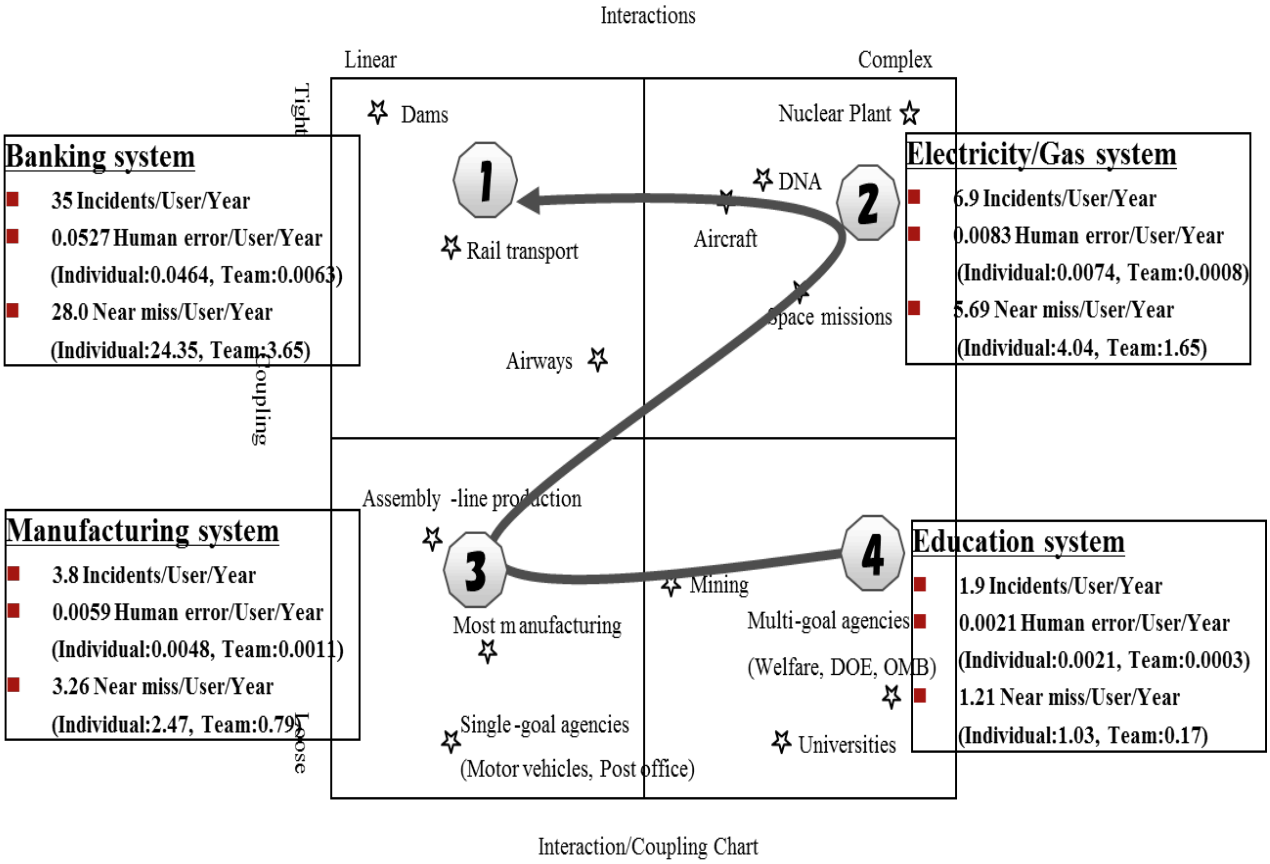


Figure 11 the sequence of Incident and Human error

Table 5 Human error and Incident data in 2012

		Banking	Manufacturing	Electricity&Gas	Education
2012	Human Error	338	169	8	20
	(Severity A)		2	1	1
	(Severity B)	11	5		1
	(Severity C)	327	162	7	18
	Incident	103307	43065	2727	7164
	User	2657	11778	404	4220
	Incident/User	38.9	3.7	6.8	1.7
	Human Error/Incident	0.3%	0.4%	0.3%	0.3%
	Human Error/User	12.7%	1.4%	2.0%	0.5%
	Human Error/Incident/User	0.00012%	0.00003%	0.00073%	0.00007%
	Severity A/Incidnt	0.00000%	0.00464%	0.03667%	0.01396%
	Severity B/Incidnt	0.01065%	0.01161%	0.00000%	0.01396%
	Severity C/Incidnt	0.31653%	0.37618%	0.25669%	0.25126%
	Severity A/Incidnt/User	0.00000%	0.00000%	0.00009%	0.00000%
	Severity B/Incidnt/User	0.00000%	0.00000%	0.00000%	0.00000%
	Severity C/Incidnt/User	0.00012%	0.00003%	0.00064%	0.00006%

Table 6 Human error and Incident data in 2013

		Banking	Manufacturing	Electricity&Gas	Education
2013	Human Error	53	25	1	8
	(Severity A)	2	1		1
	(Severity B)	1			
	(Severity C)	50	24	1	7
	Incident	94235	39918	2838	6155
	User	2657	11778	404	4220
	Incident/User	35.5	3.4	7.0	1.5
	Human Error/Incident	0.1%	0.1%	0.0%	0.1%
	Human Error/User	2.0%	0.2%	0.2%	0.2%
	Human Error/Incident/User	0.00002%	0.00001%	0.00009%	0.00003%
	Severity A/Incidnt	0.00212%	0.00251%	0.00000%	0.01625%
	Severity B/Incidnt	0.00106%	0.00000%	0.00000%	0.00000%
	Severity C/Incidnt	0.05306%	0.06012%	0.03524%	0.11373%
	Severity A/Incidnt/User	0.00000%	0.00000%	0.00000%	0.00000%
	Severity B/Incidnt/User	0.00000%	0.00000%	0.00000%	0.00000%
	Severity C/Incidnt/User	0.00002%	0.00001%	0.00009%	0.00003%

Table 7 Human error and Incident data in 2014

		Banking	Manufacturing	Electricity&Gas	Education
2014	Human Error	29	13	1	2
	(Severity A)	2			
	(Severity B)	2	1		
	(Severity C)	25	12	1	2
	Incident	81332	35755	2483	4843
	User	2657	11778	404	4220
	Incident/User	30.6	3.0	6.1	1.1
	Human Error/Incident	0.0%	0.0%	0.0%	0.0%
	Human Error/User	1.1%	0.1%	0.2%	0.0%
	Human Error/Incident/User	0.00001%	0.00000%	0.00010%	0.00001%
	Severity A/Incidnt	0.00246%	0.00000%	0.00000%	0.00000%
	Severity B/Incidnt	0.00246%	0.00280%	0.00000%	0.00000%
	Severity C/Incidnt	0.03074%	0.03356%	0.04027%	0.04130%
	Severity A/Incidnt/User	0.00000%	0.00000%	0.00000%	0.00000%
	Severity B/Incidnt/User	0.00000%	0.00000%	0.00000%	0.00000%
	Severity C/Incidnt/User	0.00001%	0.00000%	0.00010%	0.00001%

Table 8 Incident per user occurrence ratio

Incident/User	Banking	Manufacturing	Electricity&Gas	Education
2012	38.9	3.7	6.8	1.7
2013	35.5	3.4	7.0	1.5
2014	30.6	3.0	6.1	1.1
Total	35.0	3.8	6.9	1.9

Table 9 Human error per user occurrence ratio

Human Error/User	Banking	Manufacturing	Electricity&Gas	Education
2012	12.72%	1.43%	1.98%	0.47%
2013	1.99%	0.21%	0.25%	0.19%
2014	1.09%	0.11%	0.25%	0.05%
Total	5.27%	0.59%	0.83%	0.24%

Table 10 Near miss per user occurrence ratio

Near miss/User	Banking	Manufacturing	Electricity&Gas	Education
2012	23.52%	3.20%	5.94%	1.47%
2013	28.98%	3.53%	5.69%	1.18%
2014	31.50%	3.04%	5.45%	0.97%
Total	28.00%	3.26%	5.69%	1.21%

Further research was done, human errors were classified by unknown caused human. As can be seen in figure 12 and table 11, the errors are sequentially located from electricity and gas, banking, manufacturing and education systems.

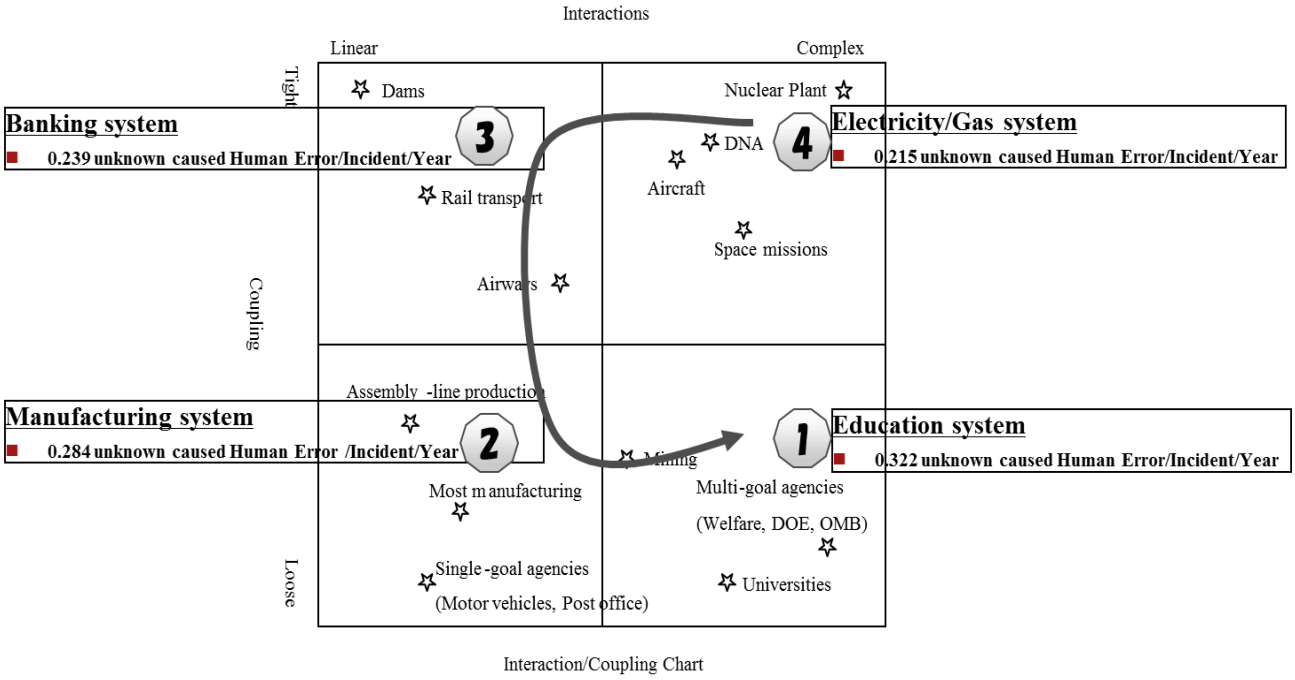


Figure 12 Unknown caused human errorratio

Table 11 Unknown caused human error per incident

2012~2014	Banking	anufacturi	ectricity&G	Education
User number	2657	11778	404	186
Mistake	615	308	19	41
Unknown	635	386	17	60
Lapse&Slip	814	343	26	45
Others	588	321	17	40
Total	2652	1358	79	186
Unknown Caused Human error/Incident	0.239442	0.284242	0.21519	0.322581

And furthermore, human errors were classified by individual and team errors. As can be seen in figure 13, table 12 and table 13, Banking system as well as Electricity and gas system in Figures 13,table 12 and table 13 show that individual contributed human errors more than did team. This suggests that the team working process might be sequential rather than parallel based upon table 4. But this should be confirmed further. And banking system (i.e. Linear interaction domain) have greater human error than Electricity and gas system (i.e. Complex interaction domain). This confirms hypothesis 1.

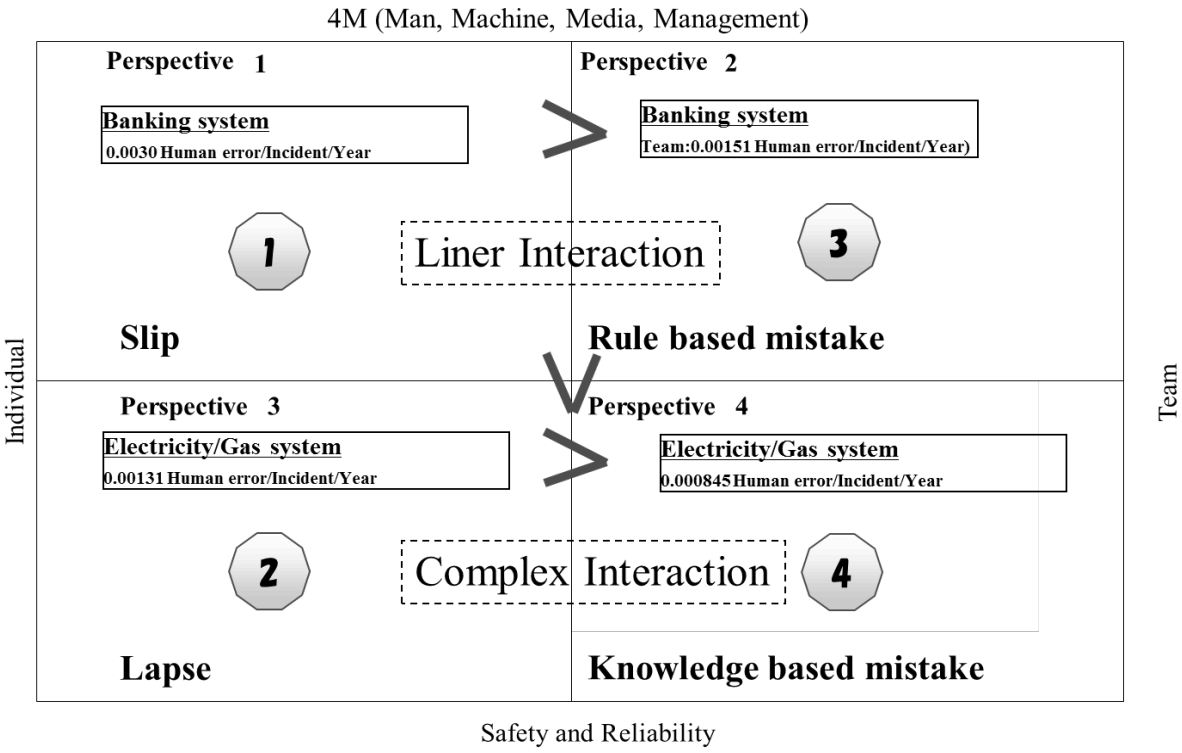


Figure 13 Human error occurrence ratio comparisons between individual and team work

Table 12 Human error per incident for individual work

Human Error/Incident	Banking	Electricity&Gas
2012	0.00%	0.29%
2013	0.06%	0.04%
2014	0.04%	0.05%
Total	0.030%	0.131%

Table 13 Human error per incident for team work

Human Error/Incident	Banking	Electricity&Gas
2012	0.34%	0.33%
2013	0.05%	0.00%
2014	0.02%	0.00%
Total	0.151%	0.085%

4. CONCLUSION

We obtained several findings by applying human error framework in several ICT systems. The proportion of human error in system failures is relatively high in the tight domain.

(1) Tight domain have greater error ratio than loose domain. This data support NAT.

(2) Loose domain has greater unknown caused human error and incident ratio.

These findings are obtained by the data form figure 11, figure 12 and figure 13. Figure 14 shows incident versus unknown caused distribution between four systems.

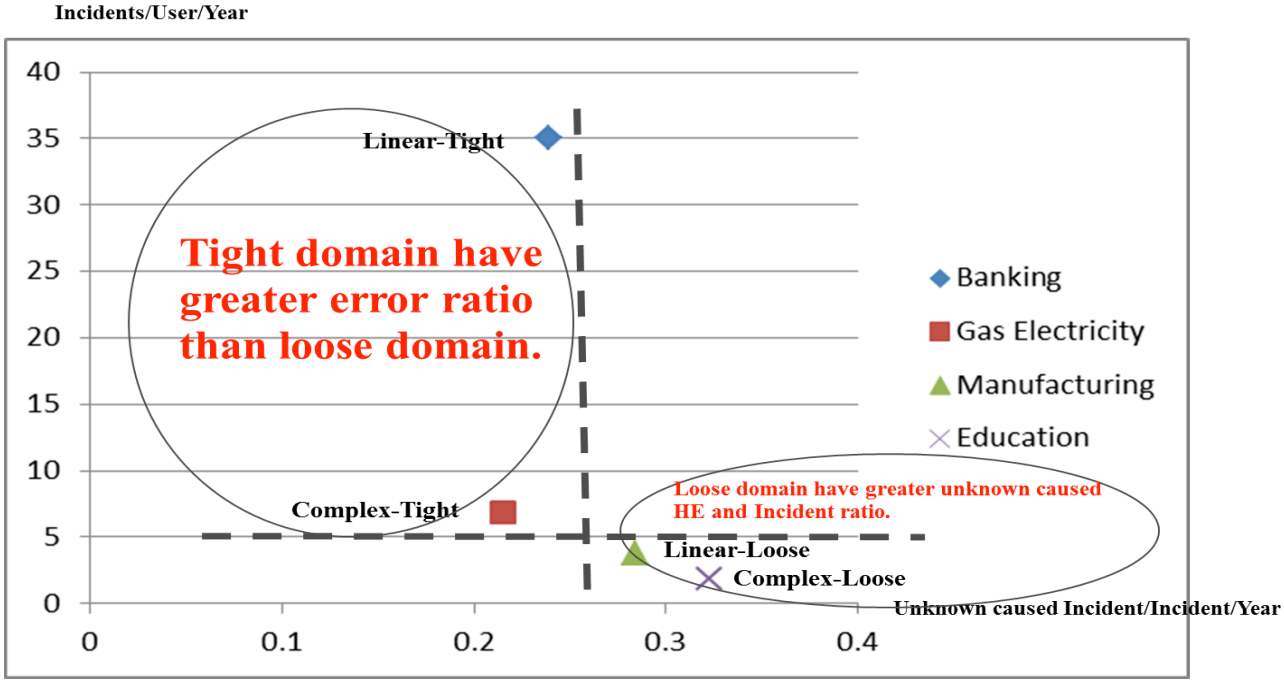
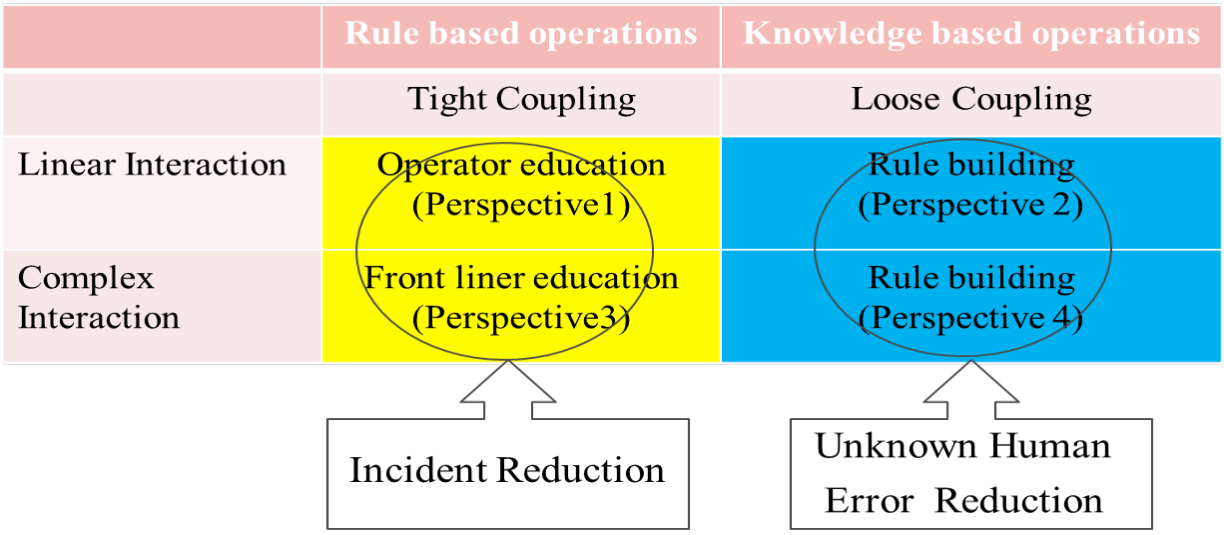


Figure 14 incident and unknown caused distribution between four systems

(3) Individual work have greater human error ratio than Team work in banking system and electric gas systems. Also liner interaction systems are prone to human error than complex interaction systems. These data suggests working process types (i.e. parallel or sequential) should be confirmed in those systems to see if parallel working processes are less human error ratio than sequential processes. This finding is obtained by the data form figure 13.

Table 14 is the guiding principle obtained by this research. Tight coupling area should have incident reduction measures putting emphasis on operator education in linear interaction area and front liner (i.e. not only operator but also other engineers who work at front line) education in complex interaction area. Loose coupling area should have unknown human error reduction measures putting emphasis on analytic (i.e. perspective 2) measure in linear interaction area and socio-technical (i.e. perspective 4) measure in complex interaction area. According to the discussion of HRO in section 2.3, the counter measures should educate front liners by creating the appropriate behaviours and attitudes (Weick and Karlene, 1993). However, this is not enough. Creating mature rule based operations from immature skill based operations to avoid decision errors (i.e. mistake error type in table 2) is also indispensable.



To confirm hypothesis 2 fully, further research should be done to collect more detailed data for human errors, both skill and rule based operation error cases, and compare them between the four sectors. However, the proposed method for promoting ICT engineering safety is effective because it complements the shortcomings of the static nature of risk management. In particular, the risk framework (human error framework) is effective at ensuring countermeasures holistically. The dynamic nature of human processes should be monitored periodically to see if the number of skill

based errors remains high. This would enable us to objectively compare various systems in terms of crisis management and assure that countermeasures will be introduced to mitigate risk and to migrate toward the ideal domains.

REFERENCES

Avizienis,A., Laprie,J.C. and Randell,B. (2001). Fundamental Concepts of Dependability (LAAS-CNRS Report No. 01145).

Beer, S. (1979). The Heart of Enterprise. John Wiley & Sons: London and New York.

Beer, S. (1981). Brain of the Firm, 2nd edition. John Wiley & Sons: London and New York.

Bell, T.E., ed. (1989). 'Special Report: Managing Murphy's law: engineering a minimum-risk system,' IEEE Spectrum, June, pp 24-57

Beroggi, G.E.G. and Wallace, W.A. (1994). 'Operational Risk Management: A New Paradigm for Decision Making,' IEEE Transactions on Systems, Man and Cybernetics, Vol.24, No.10, October, pp.1450-1457

Boehm, B.W. (1986). A Spiral Model of Software Development and Enhancement, ACM SIGSOFT Software Engineering Notes, ACM, 11(4): pp.14-24

BSI, 1985. Reliability of Constructed or Manufactured Products, Systems, Equipment and Components, Part 1. Guide to Reliability and Maintainability Programme Management (Report No. BS 5760). British Standard Institution.

Campbell, D. T., (1990). In Asch's moral epistemology for socially shared knowledge. In Irwin Rock (Ed). The legacy of Solomon Asch: essays in cognition and social psychology: 39-52. Hillddale, NJ: Erlbaum.

Forsberg, K. and Mooz, H. (1991), The Relationship of System Engineering to the Project Cycle, Proceedings of the First Annual Symposium of National Council on System Engineering, pp.57–65

IEC 60812 (2006). Procedure for failure mode and effect analysis (FMEA)

IEC 61025 (2006). Fault tree analysis (FTA)

JR, train driver faulted in final report on crash. 2007-06-29. Retrieved May 3, 2013 from http://info.japantimes.co.jp/text/nn20070629a5.html

Kaniche,M., Laprie,J.C. and Blanquart, J.P. (2002) A frame-work for dependability engineering of critical computing systems, Safety Science, Elsevier, Issue 9, Vol.40, pp.731-752

Laprie,J.C. (1992). Dependability: basic concepts and terminology, dependable computing and fault-tolerant systems. Springer Verlag, Wien-New York.

Leveson, N., Dulac, N., Marais, K. and Carroll, J. (2009). Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems. (J.

Carroll, Ed.)Organization Studies, 30(2-3), 227-249. EGOS.

La Porte, T. R. and Consolini, P. (1991). Working in practice but not in theory: Theoretical challenges of High-Reliability Organizations. Journal of Public Administration Research and Theory 1: 19–47.

Mitroff, I.I. (2011). Swans, Swine, and Swindlers: Coping With The Growing Threat of Mega Crises and Mega Messes. With Can M. Alpaslan. Stanford Business Press.

Perrow, C. (1999). Normal Accidents: Living with High-Risk Technologies. Princeton Paperbacks: New York.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem Safety Science, 27 (2-3), 183-213

Reason, J. (1990). Human Error. Cambridge University Press. Cambridge

Reason, J. (1997). Managing the Risk of Organizational Accident. Ashgate Pub Ltd

Karlene, H. R. (1990a). Managing high reliability organizations. California Management Review 32(4): 101–114.

Royce, W.W. (1970). Managing the Development of Large Software Systems, Proceedings, IEEE WESCON, August 1970, pages 1-9.

Wang, J.X. and Roush, M.L. (2000). WHAT EVERY ENGINEER SHOULD KNOW ABOUT RISK ENGINEERING AND MANAGEMENT. Marcel Dekker, Inc.

Weick, K. E. (1987). Organizational culture as a source of high reliability. California Management Review 29(2): 112–127, Winter.

Weick, K. E. and Karlene, H. R. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *A*dministrative Science Quarterly 38(3): 357–381, September.

Weick, K. E., K. Sutcliffe and D. Obstfeld. (1999). Organizing for high reliability. Research in Organizational Behavior, 21: 81–123.