METHOD FOR PROMOTING ICT ENGINEERING SAFETY LEARNING FROM CRISIS MANAGEMENT

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

[1]Fujitsu FSAS Inc., Support Administration Group, Hamamatsu-Cho Support Center, 5-1, Hamamatsu-Cho 1-Chome, Minato-ku, Tokyo, 105-0013, 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 target ICT reliability. However, safety is the upper layer of reliability in terms of a system hierarchy. 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 risk management framework to promote a holistic view to manage system failures. An application example of ICT human error exhibits the effectiveness of this methodology.

Keywords: 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 reliability and safety of a system should be dealt with differently. The reliability of components is a part of the safety of systems. Therefore, component reliability does 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 Reliability, Reductionist, and System I. Systems V and I are terms from the viable system model (VSM) (Beer, 1979, 1981). A whole spectrum of viewpoints should be examined in order to solve safety issues. Improving the reliability 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.

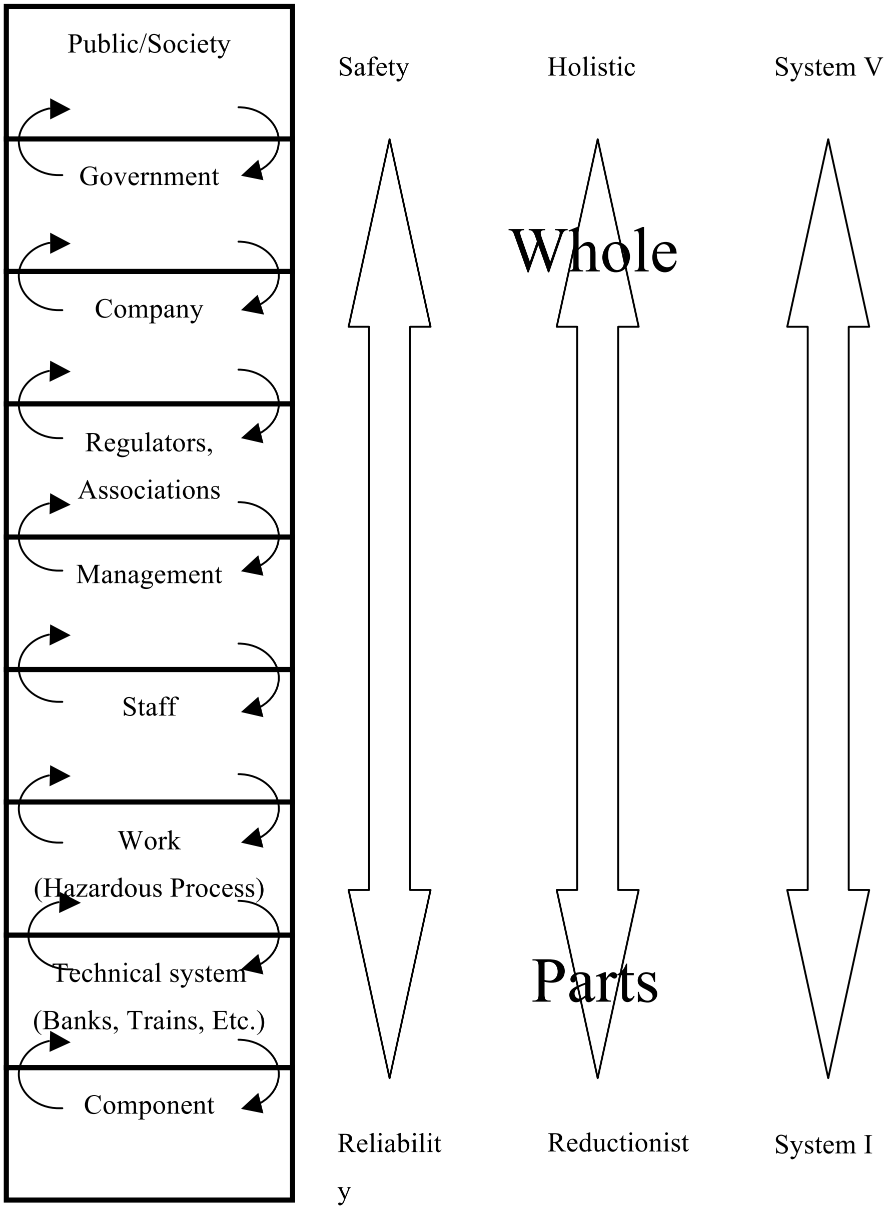


Figure 1 Socio-technical system involved in risk management

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 risk management 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 consideration what is at stake. It seeks to protect all people and assets. ***People come first.***	***Dynamic approach:*** Implement a crisis management plan as a part of an ongoing crisis management initiative. ***The organization is ANTICIPATING/BEING PROACTIVE/REACTING.***

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

Safety is a system problem. Reliability is a component's ability to achieve safety. This suggests that measures to promote reliability itself are not enough to promote safety. Systemic problems, i.e., emergent problems, could not be addressed from the standpoint of reliability. 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.

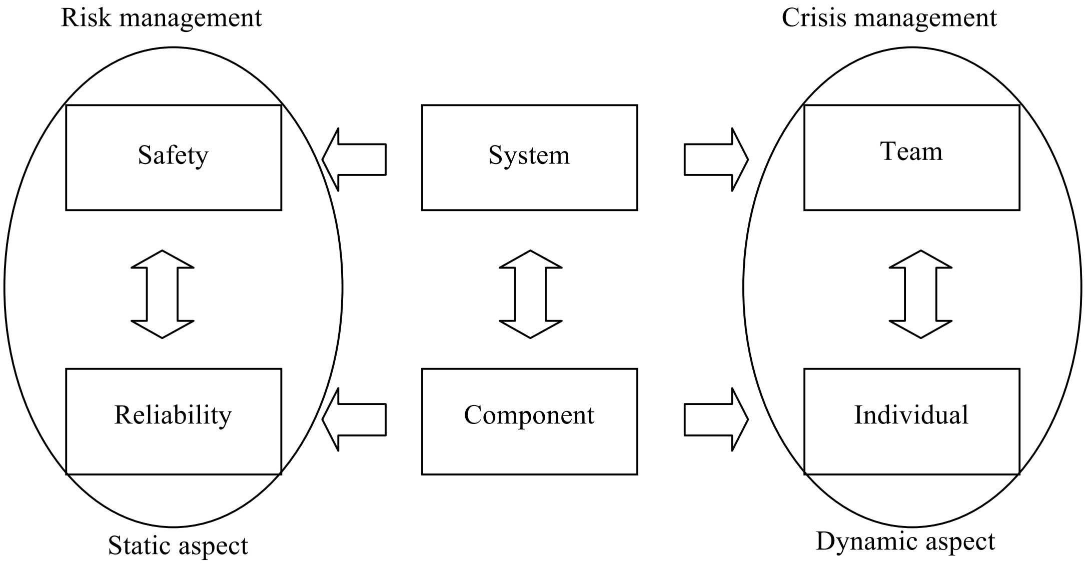


Figure 2 Different views between risk and crisis management

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.

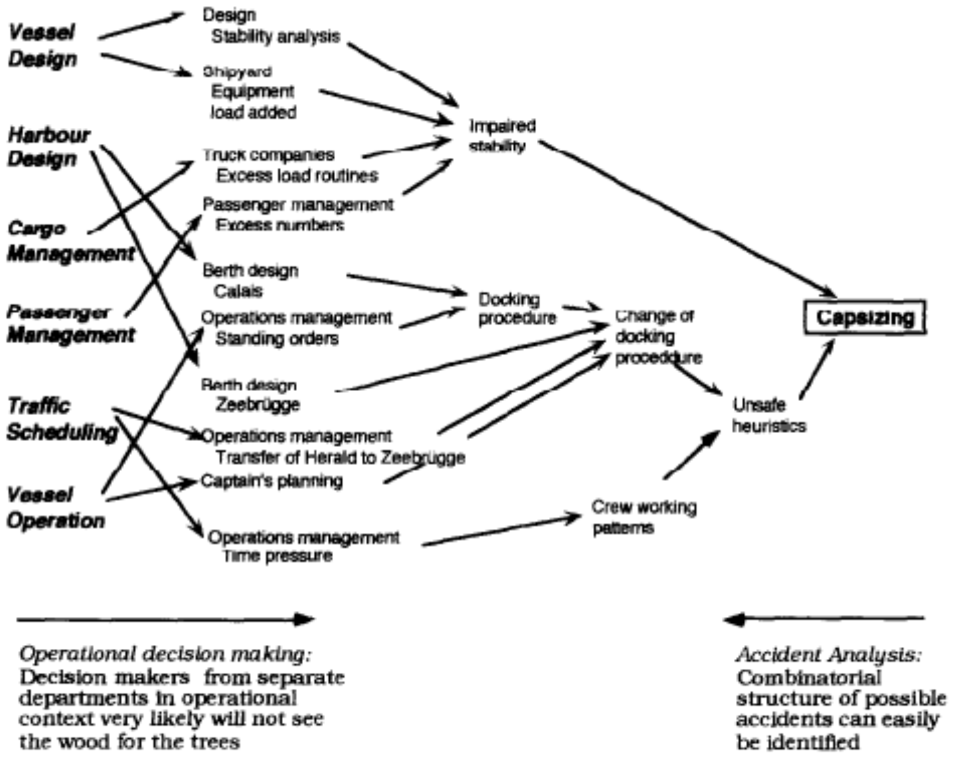

Vessel Design
Harbour Design
Cargo Management
Passenger Management
Traffic Scheduling
Vessel Operation
Design Stability analysis
Shipyard Equipment load added
Truck companies Excess load routines
Passenger management Excess numbers
Berth design Calais
Operations management Standing orders
Berth design Zeebrügge
Operations management Transfer of Herald to Zeebrugge
Captain's planning
Operations management Time pressure
Impaired stability
Docking procedure
Change of docking procedure
Unsafe heuristics
Crew working patterns
Capsizing
Operational decision making: Decision makers from separate departments in operational context very likely will not see the wood for the trees
Accident Analysis: Combinatorial structure of possible accidents can easily be identified

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. The organization theories are not enough to manage the emergent property of systems. 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.

Analytical or Technical

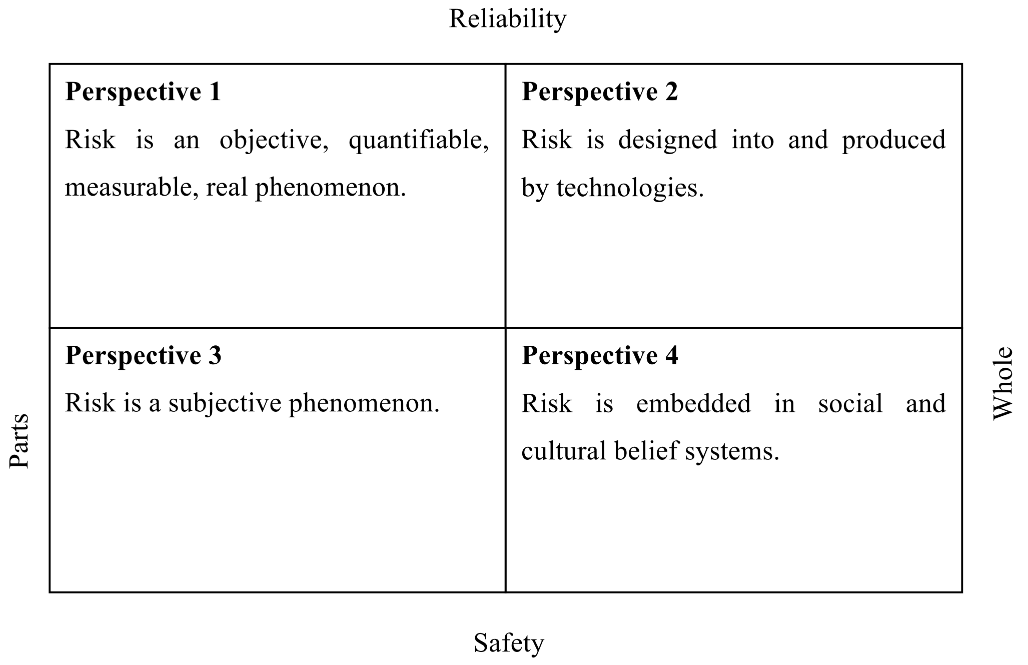
Parts	**Perspective 1** Details, facts, formulas, here and now	**Perspective 2** The big picture, multiple interpretations, systems, future possibilities	Whole
	Perspective 3 Specific individuals, stories, personal values, feelings	**Perspective 4** Communities and the entire planet, governance, social values, politics	

Personal or People

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. Reliability 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.



Perspective 1 Risk is an objective, quantifiable, measurable, real phenomenon.	**Perspective 2** Risk is designed into and produced by technologies.
Perspective 3 Risk is a subjective phenomenon.	**Perspective 4** Risk is embedded in social and cultural belief systems.

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.

Reliability

Individual

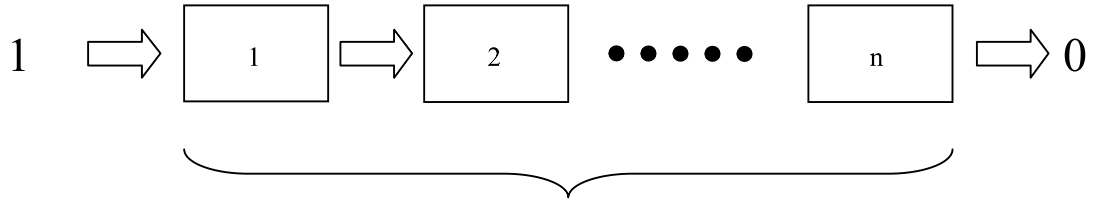
Perspective 1 Human error is an objective, quantifiable, measurable, and real phenomenon. **Slip**	**Perspective 2** Human error is designed into and produced by technologies. **Rule based mistake**
Perspective 3 Human error is a subjective phenomenon. **Lapse**	**Perspective 4** Human error is embedded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

Team

Safety

Figure 6 Human error framework

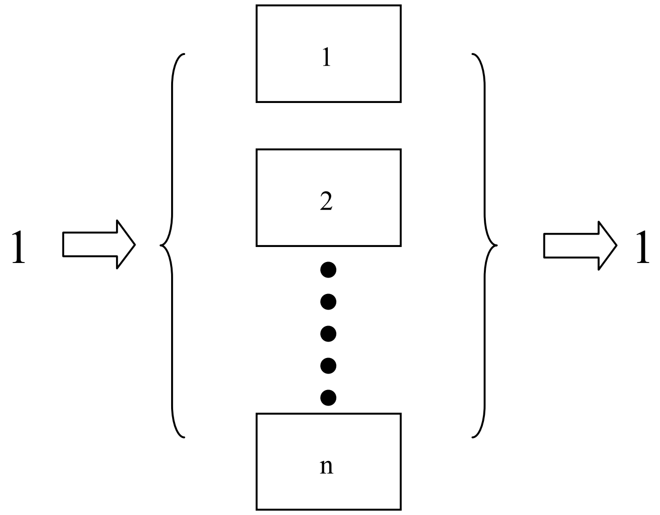
Now, we should further discuss the horizontal dimension in figure 6. To discuss team and individual working processes, which are more reliable or safer, we need a working process model. We introduce two simple models of the working process, i.e., the sequential and parallel models. Figure 7 shows the sequential model. It reduces reliability or 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 □ 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 reliability or safety with a parallel working model. Figure 8 shows this model. It enhances reliability or 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 □ 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 three hypotheses.

1. Safety problems include reliability problems. Therefore, the occurrence ratios of safety problems are greater than those of component problems.
2. Team errors include individual errors. Therefore, the occurrence ratios of team errors are greater than those of individual errors. (Single person or single group work process is more reliable or safer than multiple working processes.)
3. A parallel working process is more reliable or safer than are sequential working processes.

The ferry accident example confirms hypothesis 1. Failures are classified in accordance with the following criteria (Nakamura and Kijima, 2008, 2009ab). The ICT safety research (Nakamura and Kijima, 2009ab) confirms hypothesis 1. The meaning of error types in table 3 are:

Class 1 (failure of deviance): The root cause is within the system boundary, and conventional troubleshooting techniques are applicable and effective, Class 2 (failure of interface): The root cause is outside the system boundary but is predictable in the design phase, and Class 3 (failure of foresight): The root cause is outside the system boundary and is unpredictable in the design phase.

Table 3 Hypothesis 1

	Error type	Occurrence rate
Safety problems	Classes 3, 2, and 1	High
Component problems	Class 1, 2	Low

Table 4 summarizes hypotheses 2 and 3. 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. The next chapter examines hypotheses 2 and 3 in ICT systems.

Table 4 Hypothesis 2 and 3

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

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 9. 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 9 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)

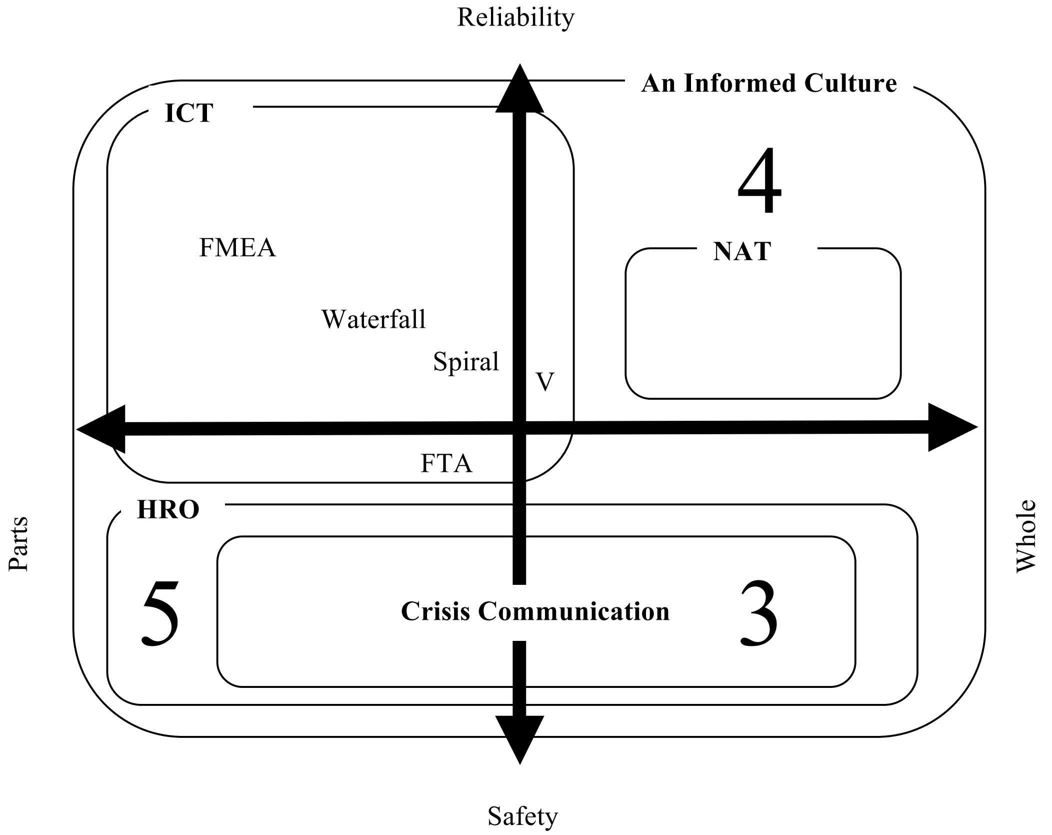


Figure 9 Mapping ICT methodologies onto risk framework

3.1 Human error contribution

Three systems were chosen to confirm the contribution of human error to the systems. They are stock exchange, meteorology, and healthcare systems. They are located in the IC chart (Perrow, 1999) from the Linear-Tight to Complex-Loose domains with the sequence from stock exchange, meteorology, and health care (Nakamura, Kijima, 2011). Figure 10 is the proportion of human error incidents and operator induced incidents. The human error incidents include the operator induced incidents. The incident data are collected from three systems in the year 2010 in table 5. They are sequentially located from Tight-Linear (upper left domain) to Complex-Loose (lower right domain).

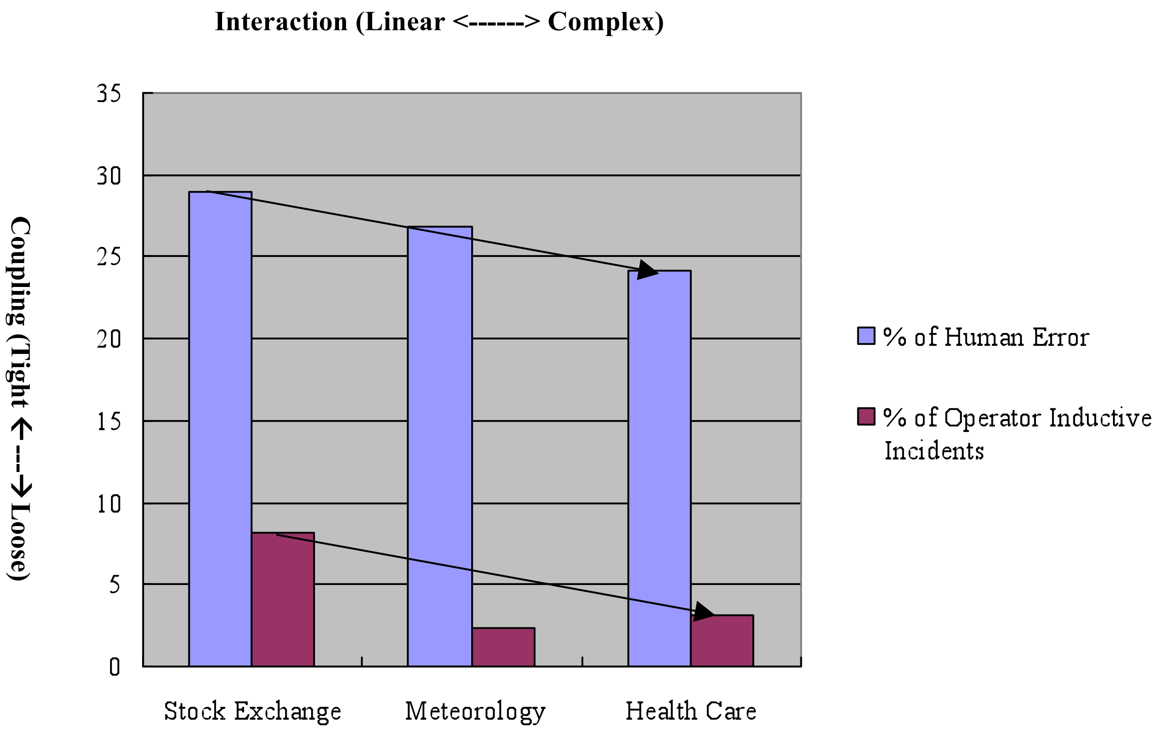


Figure 10 Proportion of human error incidents and operator inductive incidents

Table 5 Data from three systems in 2010

	% of Human Error	% of Human Error Inductive Situation caused by Operator
Stock Exchange	29 (30/145 Incidents)	8.2 (12/145 Incidents)
Meteorology	26.8 (30/123 Incidents)	2.4 (3/123 Incidents)
Health Care	24.2 (255/1207 Incidents)	3.1 (37/1207 Incidents)

Further research was done, and data were collected in February of 2012. To increase sample data, segments were slightly changed from figure 10 in the year 2010. The stock exchange was extended to the banking system, and meteorology was extended to the government. Also, human errors were classified by individual and team errors. As can be seen in figure 11, the overall trend did not change from that of figure 10. The errors are sequentially located from banking, government, and health care systems, the same as in figure 10 for the year 2010. In figure 12, human errors are classified into individual and team errors. Figures 13 and 14 further focus on the nature of work, namely incident and planned work, respectively. Incident work means corrective maintenance work, and planned work is scheduled maintenance work. Tables 6, 7, 8, and 9 are the detailed data for figures 11, 12, 13, and 14, respectively. Figures 12, 13, and 14 show that team contributed human errors more than did individual. The only exceptional case is in the banking system in figure 14. This could be due to the effect of improving safety procedure checks after having several human errors in this segment. However, the sequences of the three categories for team error are slightly different from those of individual error. The government sector was the highest human error ratio, followed by banking and health care in figure 12. The planned work errors of government were significantly higher than those of banking and health care in figure 14. The reason is discussed in the next chapter.

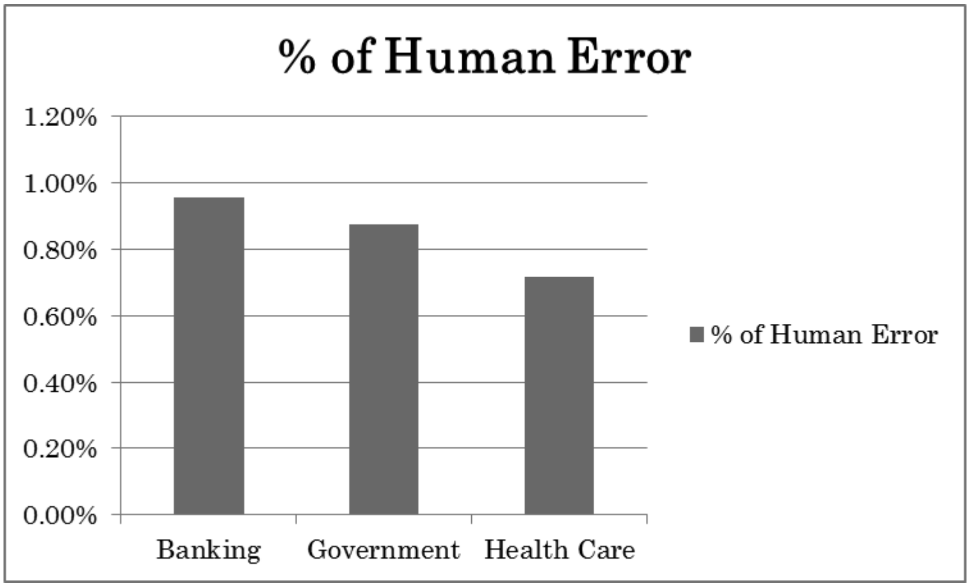


Figure 11 Proportion of human error

Table 6 Total human error data from three systems in February 2012

	Total	Human Error	% of Human Error
Banking	16875	161	0.95%
Government	3429	30	0.87%
Health Care	3905	28	0.72%

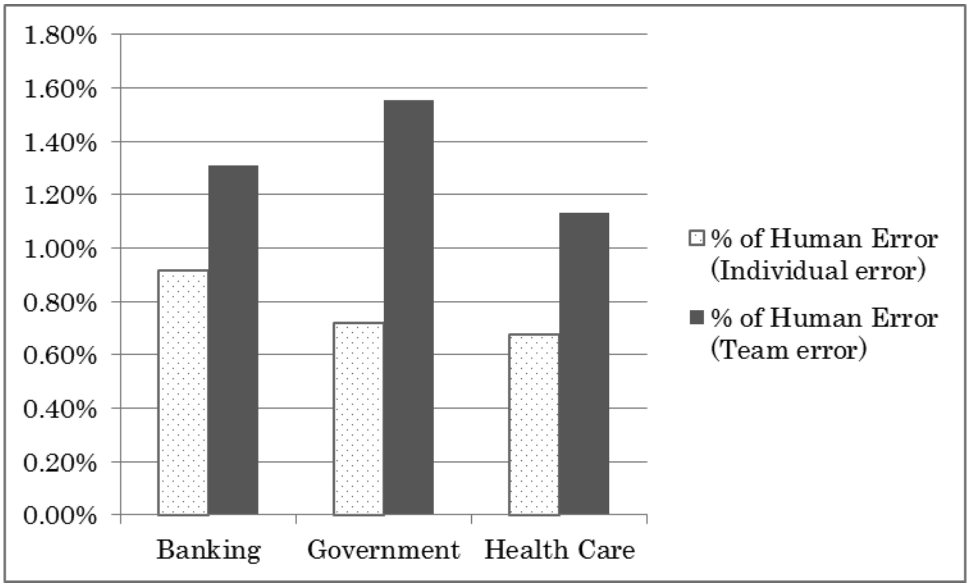


Figure 12 Proportion of human error (classified by individual and team errors)

Table 7 Classified by individual and team errors in February 2012

	Total (Individual)	Human Error (Individual error)	% of Human Error (Individual error)	Total (Team)	Human Error	% of Human Error (Team error)
Banking	15270	140	0.92%	1605	21	1.31%
Government	2785	20	0.72%	644	10	1.55%
Health Care	3552	24	0.68%	353	4	1.13%

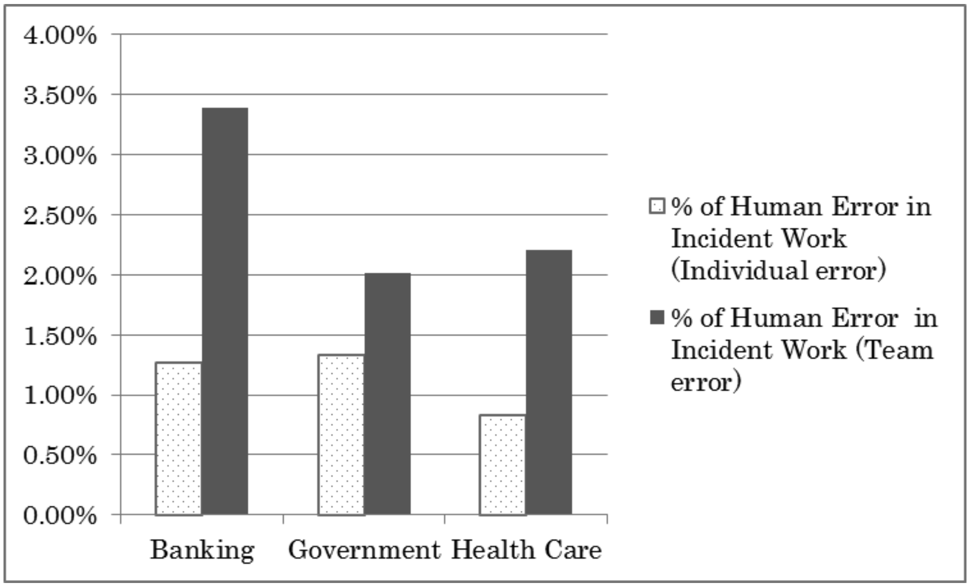


Figure 13 Proportion of human error in incident work (classified by individual and team errors)

Table 8 Classified by individual and team errors in incident work in February 2012

	Total Incident Work (Individual)	Human Error	% of Human Error in Incident Work (Individual error)	Total Incident Work (Team)	Human Error	% of Human Error in Incident Work (Team error)
Banking	9042	115	1.27%	560	19	3.39%
Government	1350	18	1.33%	298	6	2.01%
Health Care	2784	23	0.83%	136	3	2.21%

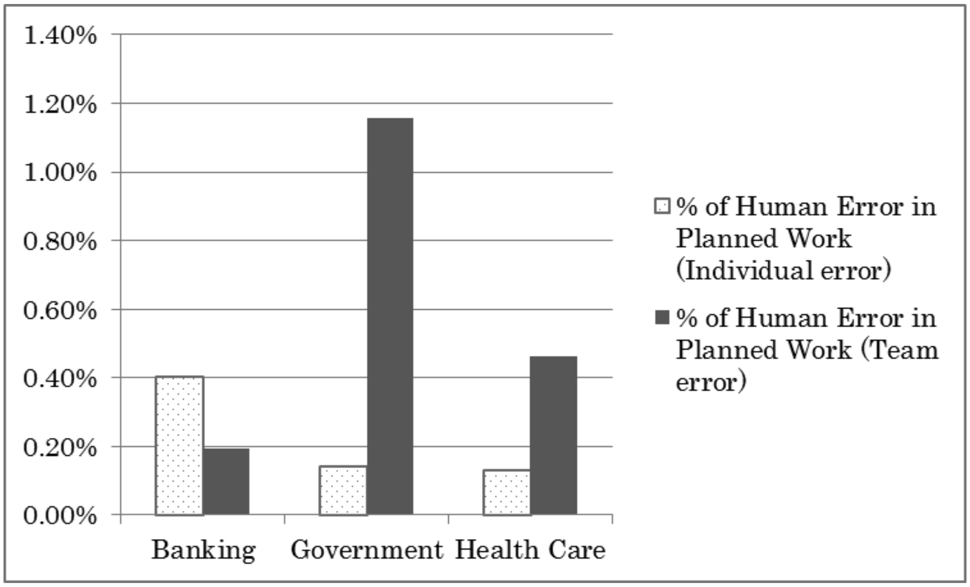


Figure 14 Proportion of human error in planned work (classified by individual and team errors)

Table 9 Classified by individual and team errors in planned work in February 2012

	Total Planned Work (Individual)	Human Error	% of Human Error in Planned Work (Individual error)	Total Planned Work (Team)	Planned Work	% of Human Error in Planned Work (Team error)
Banking	6228	25	0.40%	1045	2	0.19%
Government	1435	2	0.14%	346	4	1.16%
Health Care	768	1	0.13%	217	1	0.46%

CONCLUSIONS

We obtained several findings by applying our method to several ICT systems. The proportion of human error in system failures is relatively high in the Linear-Tight domain. Also, the ratio of human error induced by an operator in system failures tends to be high in the domain in figure 10. This trend suggests that having different viewpoints is necessary in a complex domain such as in healthcare systems rather than in IT system operator education, i.e., Perspective 1, in the Linear-Tight domain. Figure 12 shows that the human error (team error) occurrence ratios were greater than those of the human error (individual error) in all three segments. The results of applying the method confirmed hypothesis 2, introduced in section 2.6.

[Hypothesis 2] Team errors include individual errors. Therefore, the occurrence ratios of team errors are greater than those of individual errors. (Individual working process is more reliable or safer than are team working processes.)

In comparison, hypothesis 3 was not as obvious as hypothesis 2.

[Hypothesis 3] A parallel working process is more reliable or safer than are sequential working processes.

We apply an analogy between the Linear-Tight domain and sequential process (between the Complex-Loose domain and parallel process), and we assume the nature of operations in the Linear-Tight domain (Sequential process) to be rule based operation and that of the Complex-Loose domain (Parallel process) to be skill based operation. Thus, the Linear-Tight domain (Sequential process) should have more rule based operations than skill based operations. In comparison, the Complex-Loose domain (Parallel process) should have more skill based operations than rule based operations. To verify hypothesis 3, we should confirm the following three points. 1) Rule based operations are the dominant factor for contributing human errors in the Linear-Tight domain. 2) Skill based operations are the dominant factor for contributing human errors in the Complex-Loose domain. 3) The team error occurrence ratio in the Linear-Tight domain is greater than that in the Complex-Loose domain. Therefore, hypothesis 3 can be refined as in Table 10.

Table 10 Refinement of hypothesis 3

	Rule based operations	Skill based operations	Human error ratio
Linear-tight domain Sequential process	Majority (Perspective 2)	Minority (Perspective 1)	High
Complex-loose domain Parallel process	Minority (Perspective 3)	Majority (Perspective 4)	Low

The team error sequence shows that the government sector is followed by banking and health care in figure 12. This sequence is different from that of the individual error, i.e., banking followed by government sector and health care. The main cause of this trend was that the number of planned work errors in government was higher than that in banking and health care in figure 14. On the contrary, team error in incident work in figure 13 did not have a significant trend in figure 14. Therefore, in the government sector, human error in planning work is the main cause aggravating reliability and safety. According to table 10, this could be the result of immature skill based processes in the Complex-Loose domain (parallel working processes), especially in the government sector. We may need to use perspective 4's measure to tackle the domain. 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. Table 11 is the guiding principle obtained by this research.

Table 11 Guiding principle to improve human errors

	Dominant error	Rule based operations	Skill based operations
Linear-tight domain Sequential process	Lapse, Slip (Execution Error)	Operator education (Perspective 2)	
Complex-loose domain Parallel process	Mistake (Decision Error)		Front liner education Rule building (Perspective 4)

To confirm hypothesis 3 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 three 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

Heinrich, H.W., Petersen, D., and Roos, N. 1989. Industrial Accident Prevention: A Safety Management Approach. 5th ed. McGraw-Hill: New York.

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.

Nakamura, T. and Kijima, K. (2008). Failure of Foresight: Learning from System Failures through Dynamic Model. Proceedings of the 52nd Annual Meeting of the ISSS in Madison (Jul. 2008).

Nakamura, T. and Kijima, K. (2009a). System of system failures: Meta methodology for IT engineering safety. Systems Research and Behavioral Science Vol. 26, Issue 1, January/February 2009: 29–47.

Nakamura, T. and Kijima, K. (2009b). A methodology to prolong system lifespan and its application to IT systems. Proceeding of the 53rd Annual Meeting of the ISSS in Brisbane (Jul. 2009).

Nakamura, T. and Kijima, K. (2011). Method for visualizing risk factors of system failures and its application to ICT systems. Proceeding of the 55th Annual Meeting of ISSS in Hull (Jul. 2011).

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.