Chapter 24
Resilience Engineering

A New Horizon of Systems Safety

Kazuo Furuta

Abstract Having experienced natural disasters, accidents, and economic crises, people are getting skeptical about technological approaches to risk management. The conventional approaches have not considered sufficiently how to manage residual risks that spill out of the design basis of a complex socio-technical system. Resilience, which means the ability of a system to absorb changes and disturbances in the environment and to maintain system functionality, is a key concept for resolving the above situation, and resilience engineering is an area where technical methodologies to implement resilience into socio-technical systems are studied. In this chapter, the prehistory of resilience engineering will be described first where the focal point of systems safety has gradually shifted from hardware component failures to the resilience of complex socio-technical systems. Then some relevant topics in resilience engineering will be discussed: how systems resilience can be evaluated and implemented, and the key issues to be resolved in the future.

Keywords Resilience engineering · Socio-technical system · Safety management · Crisis management · Human reliability

24.1 Introduction

We are surrounded by various kinds of dangers including natural disasters, accidents, medical diseases, economic crises, and crime. Prevention of damage and protection of people's safe living are great missions for engineering. Remarkable efforts have been made in conventional safety, reliability, and disaster prevention engineering to assess risks qualitatively or quantitatively, prevent manifestation

K. Furuta (✉)
Resilience Engineering Research Center, Graduate School of Engineering,
The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan
e-mail: furuta@rerc.t.u-tokyo.ac.jp

J. Ahn et al. (eds.), *Reflections on the Fukushima Daiichi Nuclear Accident*,
DOI 10.1007/978-3-319-12090-4_24

of damage, and suppress damage to the minimum extent. Such efforts contributed greatly to making our lives far safer. Risk is a measure for representing the degree of danger as a combination of the scale and the probability that damage will occur. When there is a possibility that disasters or accidents may cause damage to human lives, health, or assets, risk is a very useful measure for achieving safety.

Having experienced unanticipated disasters in this century, however, we have recognized that we need a new framework of systems safety that can cover unanticipated situations that spill out of the scope of conventional risk management.

24.2 Shift in the Focal Point of Systems Safety

24.2.1 Era of Technology

Figure 24.1 shows how the focal point of systems safety has changed in the past decades. Some events that characterize the changes are also indicated in the figure.

When socio-technical systems were not very complex, specialists thought that problems occur for technical reasons, such as failures or malfunctions of hardware components, and that they can prevent accidents and disasters by further advances in technologies. Efforts were made, therefore, to carry out safety design and quality assurance based on understanding of failure mechanisms, and most problems with hardware components were successfully resolved.

The world's first commercial jetliner launched in 1951, de Havilland Comet, crashed repeatedly due to metal fatigue, which is a phenomenon in which a material breaks when great loads are repeatedly applied. The phenomenon itself had been known, but the validation testing method was immature at the time. Following the accidents, many technical improvements and redesigns were made, including improvement of the test method and the structural design method to stop fatigue crack propagation.

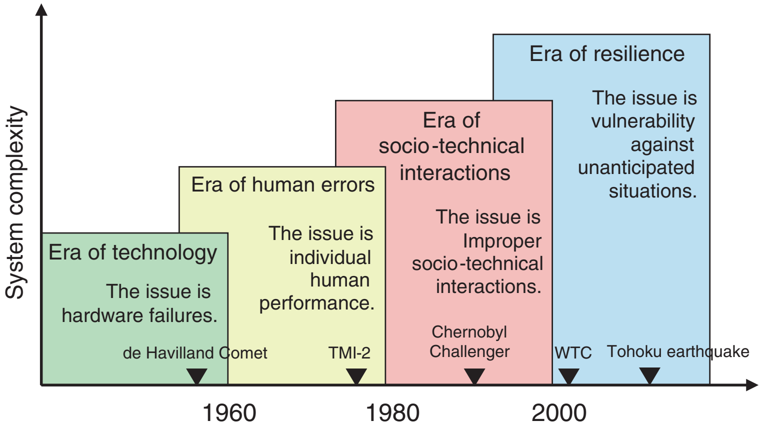

System complexity
Era of technology
The issue is hardware failures.
Era of human errors
The issue is individual human performance.
Era of socio-technical interactions
The issue is Improper socio-technical interactions.
Era of resilience
The issue is vulnerability against unanticipated situations.
de Havilland Comet
TMI-2
Chernobyl
Challenger
WTC
Tohoku earthquake
1960
1980
2000

Fig. 24.1 Shift in the focal point of systems safety

Similar problems occurred in the early introduction stage of nuclear power. Stress Corrosion Cracking (SCC) in the recirculation loop piping of Boiling Water Reactors (BWRs) and wall thinning in the steam generator tubes of Pressurized Water Reactors (PWRs) were serious problems for the industry from the 1950s to 1980s. As technical studies revealed the mechanisms of cracking and degradation, which had not been understood at the beginning, the problems were resolved by substituting the materials with newly designed alloys, improving the management of water chemistry, and improving the method of fabrication.

24.2.2 Era of Human Error

As advanced technologies have been introduced, the complexity of systems exceeded the capacity limits of human operators or users, and many accidents occurred due to human error.

The Three Mile Island, Unit 2 (TMI-2) accident that occurred in 1979 was a typical case in this era. The accident started with a minor malfunction in the secondary loop, but subsequent unfavorable events made the situation worse, finally leading to severe damage of the reactor core. Some of the critical events that caused the accident include operators' human errors. The operators, for example, misjudged that the reactor vessel was full of coolant water, and they tripped manually the Emergency Core Cooling System (ECCS) which had been initiated automatically.

The point where humans interact with human-made equipment is called a human-machine interface. Analysis of the TMI-2 accident revealed that there were improper human-machine interfaces behind the operators' errors. At the beginning, for example, more than 100 alarms were initiated at the same time, and the operators were unable to comprehend what had actually happened in the plant. In addition, the indication of the relief valve position did not reflect the actual valve position. This defect in interface design caused a delay in operators' correctly recognizing the internal state of the reactor vessel.

Individual human factors and prevention of human errors became key issues in this stage [1], and efforts were made to design working conditions and human-machine interfaces appropriate for physical and cognitive human characteristics. Suppression of unimportant alarms based on prioritization of alarms is an example of functions that have been adopted in nuclear power plants after the TMI-2 accident. Since consideration of human factors is nowadays the standard requirement in designing socio-technical systems, the probability that human error may cause a serious accident has been greatly reduced.

24.2.3 Era of Socio-Technical Interactions

In the next stage, socio-technical interactions were the main sources of system failures. Many accidents occurred due to inadequate interactions among technologies, humans, management, organizations, and society. The impact of such accidents often goes beyond the boundary of the organization and cause widespread damage to society. An accident of this type is called "organizational accident [2]."

The accident that occurred at Chernobyl, Unit 4, in 1986 was a typical organizational accident. At the beginning, it was thought that operators' violation of the operation rules for accomplishing a special test at the plant had caused the accident. As investigation by the international community progressed, it was revealed that organizational and social factors characteristic of the Soviet system at the time were the root causes of violation. The operators, for example, were not sufficiently trained in background knowledge of operation rules, technical communication was lacking between different organizations, workers' will to obey the rules was low in comparison with what was needed to accomplish the norm, and so on.

In the same year, the Space Shuttle Challenger disintegrated after launch and killed the entire crew. The direct cause of the accident was failure of O-ring seals of a solid rocket booster due to cold weather. It is said, however, organizational factors of the National Aeronautics and Space Administration (NASA), such as lack of communication and face-saving decision attitudes, were present behind the direct cause.

The notion of safety culture was introduced after these accidents. Safety culture is defined as an assembly of characteristics and attitudes in organizations and individuals which establish that, as an overriding priority, safety issues receive the attention warranted by their significance. Researchers and practitioners made efforts to assess the level of safety culture of a particular organization and then to enhance it. Though remarkable progress has been made, these efforts are still on-going.

24.2.4 Era of Resilience

In this century, we have experienced more shocking events such as the terrorists' attack on the World Trade Center (WTC) in New York and the Great East Japan (Tohoku) Earthquake in Japan. Vulnerability of our socio-technical systems in the face of unanticipated situations was clearly shown in these events. In the conventional approaches of engineering, the design basis is determined beforehand based on some assumptions of severe conditions, and safety design is performed so that the system can fulfill the design basis. An event that exceeds the design basis, however, may happen, and its probability is characterized as residual risks. Since losses are unavoidable in such a case, we have to consider how quickly socio-technical systems can recover from the losses.

The conventional approaches have not considered sufficiently how to manage residual risks that spill out of the design basis of a complex socio-technical system. Having experienced natural disasters, accidents, economic crises, and so on, people are getting skeptical about technological approaches to risk management. Now we need a new framework for the safety of socio-technical systems to manage risks not only within but also beyond the design basis.

From the above background, the concept of "resilience" has lately attracted widespread interest of researchers and practitioners in systems safety [3, 4]. The term means the ability of a socio-technical system to adapt to disturbances from the environment and maintain its normal function. If we want to face up to unanticipated situations like WTC and Tohoku, we need to establish a new academic field, which we can call resilience engineering, to devise resilient socio-technical systems that can quickly recover their functions from damaged conditions.

24.3 Progress in Human Reliability Analysis

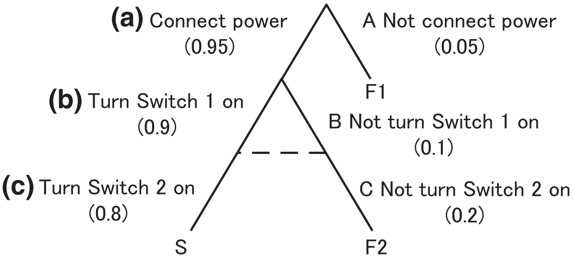
24.3.1 First-Generation HRA

In this section, we will discuss the human reliability analysis method to describe how the primary focus has shifted from a mechanistic view to a systemic view of human performance.

Human Reliability Analysis (HRA) is a method for qualitative or quantitative assessment of the probability (frequency) and the effects of unsafe human acts. In the nuclear sector, HRA had already been an essential step in Probabilistic Risk Assessment (PRA) before the TMI-2 accident, because the probabilities of human errors in plant operations are basic data required for calculating the core damage frequency. In the early stage of development, HRA borrowed primary concepts from reliability analysis of hardware components; human errors were thought of as phenomena similar to hardware component failures. It was assumed, therefore, that operators' tasks can be divided into elementary task units, and the status of each task unit can be described by the binary logic of success versus failure. In addition, a human was dealt with as a black box without considering the internal cognitive mechanism that determines human performance.

Such methods for HRA are often called first-generation HRA. Technique for Human Error Rate Prediction (THERP) [5] is a typical example of first-generation HRA, which was developed early for the first comprehensive PRA of Light Water Reactors, WASH-1400 [6]. In THERP, a human task is modeled using a binary event tree as shown in Fig. 24.2, which shows an example task composed of three steps: (1) connecting power to the equipment, (2) turning Switch 1 on, and (3) turning Switch 2 on. Each branching

Fig. 24.2 Example of THERP event tree with probabilities in parentheses



node corresponds to an elementary task unit and the left and right branches, respectively, show success and failure paths of the task. It is assumed that the basic Human Error Probability (HEP) of an elementary task unit is primarily determined by the class of the task unit and the error mode. Concrete numbers of basic HEPs can be evaluated by looking up the database attached to the THERP handbook [5].

One of the drawbacks of first-generation HRA is its restricted power to describe situations of human performance. It is therefore applicable only to tasks that are well defined as standard operation procedures. Tasks that require complex cognitive processes of judgment are beyond the scope of first-generation HRA. In the TMI-2 accident, the operators misjudged the internal state of the reactor vessel based on the information obtained from the main control panel and stopped ECCS convinced that it was the correct action. Such an error by conviction or an error of commission occurs through an error mechanism very different from simple mishaps. Internal cognitive mechanisms of a human have to be looked into to deal with errors of commission in HRA.

24.3.2 Second-Generation HRA

Towards the end of the 1980s, many researchers of human factors started thinking that some breakthrough was required for HRA methods [7]. It is imperative to take errors of commission into account, because they may defeat multiple safety barriers and put the system into critical conditions. In addition, people cannot readily detect errors of commission by themselves in comparison with errors of omission.

Human modeling is a key technique to consider the cognitive mechanism of human performance for calculating HEPs. Rasmussen's classification of human performance into the three levels of skill, rule, and knowledge is the most popular example of such ideas of human modeling [8]. As research on human modeling and error psychology has progressed, it has become clear that human errors are not causes but consequences of unsafe incidents. Based on the outcomes of this research, methods for second-generation HRA were developed in the 1990s [9, 10].

Figure 24.3 shows the conceptual framework for human performance and human errors that is the basis of second-generation HRA. The context, which is

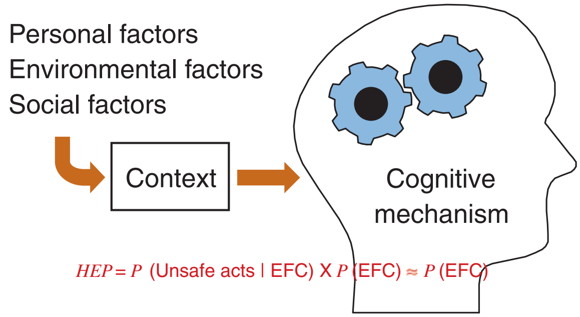


Fig. 24.3 Conceptual framework of human performance and human errors

a set of situational factors and conditions surrounding human performance, is a key concept in second-generation HRA. The context consists of various contextual factors that can be classified into personal, environmental, and social factors. Personal factors include those related to the characteristics of individual personnel such as experience level, skill level, physical and cognitive features, personality traits, and so on. Environmental factors are hardware and software attributes of the workplace such as tools, ambient conditions, design of human-machine interface, available information, and so on. Social factors are attributes of organizational or social institutions such as rules, training programs, workgroup composition, communication systems, and so on.

These factors affect the reliability of human performance through the cognitive mechanism of a human. Since the cognitive mechanism does not differ greatly among individuals, the reliability of human performance does not depend on the functioning of the cognitive mechanism but primarily on the appropriateness of context. A context where humans inevitably commit errors, Error Forcing Context (EFC), should be attended to in particular. EFC is a context in which everybody will commit an error almost certainly; HEP is almost equal to the probability of the appearance of EFC. Since an error of commission will occur under EFC just like a common mode failure of mechanical components, multiple barriers for error prevention can easily be breached. The context of human performance has come to be the target of analysis in second-generation HRA rather than human performance itself. Important contextual factors to be analyzed are chosen based on the consideration of cognitive processes that will produce the expected human performance. This was a great shift of conceptualization from the mechanistic image of human performance behind first-generation HRA.

24.3.3 Cognitive Model of Team Performance

The drawbacks of first-generation HRA are attributable to its basic assumption of the decomposition principle that a human task can be decomposed into elementary task units. It is equivalent to the assumption in the linear system that the whole is the sum of its parts. It will be shown in this subsection that this assumption does not apply to team performance. Since teamwork is used in most business settings, the reliability of team performance must be assessed in PRA, and some model of team performance is required to do so. The simplest approach is to combine multiple models of individual performance and this approach was actually taken in the early stage of development. A team, however, is a nonlinear system so that team performance is greater than the simple sum of individual performance.

The cognitive processes of team performance can be effectively described by the concept of mutual beliefs. Tuomela and Miller introduced a notion of "We-Intentions" to describe the cognitive mechanism in a cooperating team as follows [11]. When a team composed of two members, A and B, intends to do a cooperative task X, the following conditions hold.

(1) A/B intends to do A's/B's own part of X. (intention)
(2) A/B believes that B/A will do B's/A's part of X. (belief)
(3) A/B believes that B/A believes that A/B will do A's/B's own part of X. (belief on belief)

Beliefs like (2) and (3) in the above, which can be recursively defined, are called mutual beliefs. Such an explanation of the cooperation mechanism using one's own cognitive state and a corresponding structure of recursive beliefs can clarify the constitutive meaning of "sharing" intentions by cooperating team members.

Kanno applied the above notion of mutual beliefs not only to team intentions but also to cognitive team processes in general and proposed the Mutual Belief Model (MBM) to represent the team cooperation mechanism [12]. Figure 24.4 shows a recursive structure of cognition and corresponding beliefs of a two-member team. The recursive structure of mutual beliefs can be theoretically defined ad infinitum, but the three layers shown here will be sufficient to describe realistic cooperating situations.

One's own cognition on the state of the external world and oneself is described in the first MBM layer. The beliefs on the partner's cognition are described in the second MBM layer, which is a reflected image of the partner's first layer. The third MBM layer is for describing the beliefs on the partner's beliefs on one's own cognition. It is one's self image through the partner. Since the second and the third MBM layers are nonexistent in the cognitive model of an individual, a model that merely combines individuals will not contain both layers.

Cooperative team performance can be achieved using all of these MBM layers. Cognitive entities on each MBM layer are obtained and related by various types

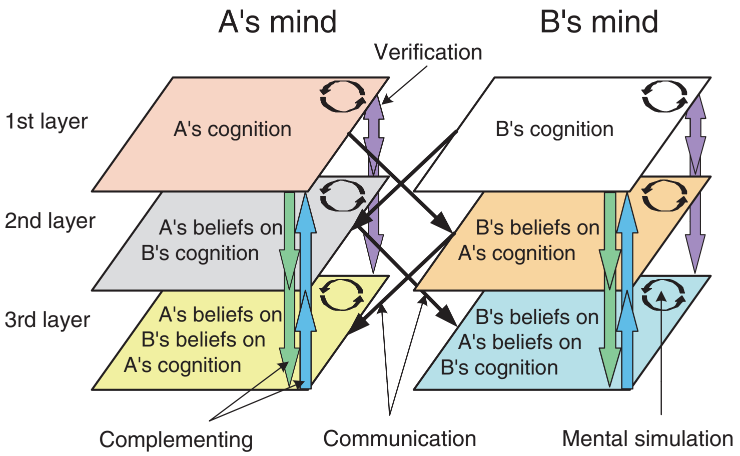

A's mind
B's mind
Verification
1st layer
A's cognition
B's cognition
2nd layer
A's beliefs on B's cognition
B's beliefs on A's cognition
3rd layer
A's beliefs on B's beliefs on A's cognition
B's beliefs on A's beliefs on B's cognition
Complementing
Communication
Mental simulation

Fig. 24.4 Mutual Belief Model and interactions

of interactions within the layer or between different layers. These interactions are classified into four types: verbal communication, mental simulation, complementing, and verification.

Verbal communication is a process to transfer some cognitive entity from one person to another by explicit utterance. Mental simulation is a process to derive new cognitive entities from some others within the same MBM layer by inference using knowledge and manipulating mental models. Mental simulation is a process for interpretation and prediction not only of the state of external world but also of the partner's behavior. In complementing, some cognitive entity will be copied from one MBM layer to another within the same person. One adopts this scheme, for instance, in an occasion where he/she supposes his/her partner believes X because he/she believes X. Such a supposition, however, sometimes results in false presumption. Finally, verification is the comparison of cognitive entities between different MBM layers to check consistency among mutual beliefs.

The cognitive processes mentioned above are nonlinear effects in terms of a combination of individual cognitive processes, and MBM becomes much more complex for a team larger than a dyad. Team cooperation by humans is more than simple division of labor. Accidents often occur with highly automated systems with no hardware failures, because mutual beliefs and cooperating interactions are lacking in systems where a linear human-machine combination is assumed. Consideration of the nonlinear nature of team performance is necessary also for sophisticated human-machine cooperation.

24.3.4 Safety Culture and High Reliability Organization

Safety culture was a new concept in systems safety that was introduced after the Chernobyl accident. As already mentioned, many organizational and social factors were found behind the direct cause of the accident, the operators' violation of the operation rules. This finding led safety specialists to attend to safety culture. Safety culture resides at the basis of the three factors shown in Fig. 24.3 that form the context of human performance. In order to prevent organizational accidents, safety culture has to be implemented and maintained by organizations.

A key question is how we can implement safety culture in organizations and maintain it. Research on organization science, in particular on high reliability organizations, gives us valuable implications to answer this question. A High Reliability Organization (HRO) is an organization where accidents and incidents are suppressed below the standard level of the related industry sector. The idea first came from the pioneering work by a group at the University of California, Berkeley [13]. This group examined behavioral patterns of work groups under high-risk and stressful conditions such as aircraft carriers, air traffic control, and nuclear power plants. From these studies, the characteristics observable in common among various HROs have been revealed, which is represented in a word, mindfulness. Mindfulness consists of the following five elementary characteristics:

- Preoccupation with failure;
- Reluctance to simplify interpretations;
- Sensitivity to operations;
- Commitment to resilience;
- Deference to expertise.

Organizations that incorporate the above characteristics can handle unanticipated situations skillfully and can recover from emergency rapidly.

Safety culture and HROs first drew attention for solving problems in the era of socio-technical interactions: how to establish proper interactions between technologies, organizations, and society, and how to avoid organizational accidents. These concepts, however, are related also to the ability of socio-technical systems to cope with unanticipated situations as suggested in the fourth item of the above list, and they give us implications for the era of resilience. A High Reliability Organization is sometimes characterized as a learning organization, the ability to adapt to changes and disturbances by restructuring itself is an essential requirement of a resilient system [14].

24.4 What Is Resilience?

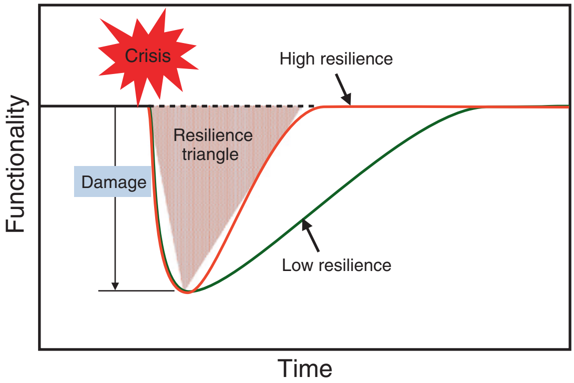
24.4.1 Definition of Resilience

The term resilience has been introduced in different domains, and many researchers have given it somewhat different definitions. Holling [15] first introduced the term in ecology to mean a measure of the persistence of systems and of their ability to absorb changes and disturbances and still maintain the same relationships between populations or state variables.

As for disaster prevention, Bruneau et al. [16] conceptualized seismic resilience as the ability of both physical and social systems to withstand earthquake-generated forces and demands and to cope with earthquake impacts through situation assessment, rapid response, and effective recovery strategies. They pointed out resilience can be defined in terms of the following 4R properties:

- Robustness: strength, or the ability of elements, systems, and other units of analysis to withstand a given level of stress or demand without suffering degradation or loss of function;
- Redundancy: the extent to which elements, systems, or other units of analysis exist that are substitutable, i.e., capable of satisfying functional requirements in the event of disruption, degradation, or loss of functionality;

Fig. 24.5 Resilience triangle



- Resourcefulness: the capacity to identify problems, establish priorities, and mobilize resources when conditions exist that threaten to disrupt some element, system, or other unit of analysis;
- Rapidity: the capacity to meet priorities and achieve goals in a timely manner in order to contain losses and avoid future disruption.

They further proposed a measure of seismic resilience, a resilience triangle, which is shown in Fig. 24.5, where time and system functionality are respectively represented horizontally and vertically. The system functionality degrades after the crisis, but it recovers gradually to return to its level before the crisis in the long run. The recovery will be rapid for a system with a high resilience but slow for that with a low resilience. A resilience triangle is the area of degradation in quality of infrastructure over time just after an earthquake to recovery.

The above definition of seismic resilience provides useful insights for discussion on systems resilience. The scope, however, is too restricted within crisis management after disasters. It focuses just on system responses after a critical event like an earthquake, but does not cover everyday activities of risk management in normal system operations. A more comprehensive view of systems resilience, therefore, is desirable.

Another group who adopted the term around 2,000 is researchers of human factors and cognitive systems engineering [3, 4]. In the early stage of development, they applied a behavioristic view of human performance to assess human error probabilities, but soon faced barriers. Then the mechanism of human cognition was considered to model more precisely the enigma of human performance. In the 1990s, however, they came to recognize that it is almost impossible to model human performance and to assess human reliability based on a mechanistic view of human performance [7].

A complex socio-technical system, which includes humans as system components, shows non-linear interactions among different parts of the system. Such interactions make it difficult to comprehend the system by the decomposition principle, which worked well with mechanical systems in the past. Studies on complex systems have made great progress in the last few decades, and new phenomena characteristic to complex systems with non-linearity have been revealed, e.g., emergence, chaos, fractal, stylized fact, and power law. These works have shown that the probability of highly rare events is much greater than predicted from linear system models and normal distribution. Such an improbable event that exceeds people's imagination is called the Black Swan [17]. Risk management based on the assumption of linear systems and the decomposition principle could not foresee such rare events, and people in non-technological domains often criticized this approach [18].

These findings on complex systems, however, stimulated our investigations into the safety of complex socio-technical systems. Kastenberg [19], for instance, pointed out it is necessary to consider the nonlinear, self-organizing, or chaotic nature of complex systems in risk analysis. Researchers of systems safety are now looking at resilience engineering as a more comprehensive and advanced concept of risk management. This new notion is based on a systemic view of accidents that accidents are caused by a nonlinear combination of performance variability of system functions rather than a linear combination of component failures.

24.4.2 Essential Characteristics of Resilience

From a systemic view, 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. In contrast to resilience in disaster prevention, the systemic notion of resilience will not distinguish between normal and abnormal system conditions. Resilience engineering is a field that studies technical methodologies to implement resilience into socio-technical systems.

While conventional risk management aims at suppressing risks below the allowable limit, risk management in resilience engineering aims at enhancing the ability of a system to suppress performance variability under changes, disturbances, and uncertainties. Resilience, therefore, deals with every system condition: stable operations in normal conditions, prevention of accidents in abnormal conditions, minimization of losses after accidents, and fast recovery from damaged conditions.

Woods pointed out that the focus is on assessing the organization's adaptive capacity relative to challenges to that capacity and that the following are essential characteristics of resilience [20].

- Buffering capacity: the size or kinds of disruptions the system can absorb or adapt to without a fundamental breakdown in performance or in the system's structure;

- Flexibility: the system's ability to restructure itself in response to external changes or pressures;
- Margin: how closely or how precarious the system is currently operating relative to one or another kind of performance boundary;
- Tolerance: how a system behaves near a boundary, whether the system gracefully degrades as stress/pressure increase, or collapses quickly when pressure exceeds adaptive capacity.

Figure 24.6 illustrates the above four characteristics of resilience. The current state of the system in operation is represented as a point in the two-dimensional state space here, and it fluctuates continuously due to performance variability. Safety boundaries that correspond to the constraints for safe system operations determine the area where the system can be operated.

Margin is a distance between the current operating point and the nearest boundary. Sufficient margin must be maintained so that the probability that the system may run out of the safe area will not exceed the design basis. It is the conventional approach to risk management.

In contrast, the other three properties are relatively new in risk management. Buffering capacity is the ability of a system to absorb or resist changes or disturbances. The resilience triangle mentioned in the previous section can be a measure of buffering capacity, which is represented as the speed of recovery from damage. Tolerance represents how gracefully system functionality degrades outside the safety boundaries. In a system with no tolerance the functionality drops immediately outside the boundaries. Flexibility is related to the ability of a system to adapt to changes and disturbances by restructuring itself, redesigning, maintaining, and learning from past experience.

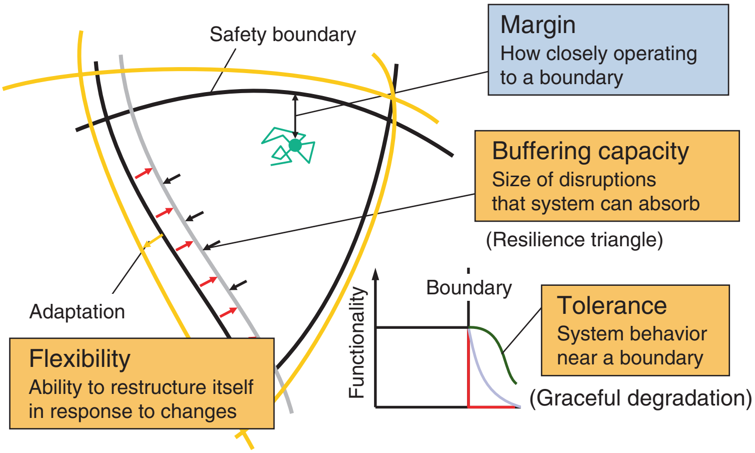

Safety boundary
Margin
How closely operating to a boundary
Buffering capacity
Size of disruptions that system can absorb
(Resilience triangle)
Adaptation
Boundary
Functionality
Tolerance
System behavior near a boundary
(Graceful degradation)
Flexibility
Ability to restructure itself in response to changes

Fig. 24.6 Essential characteristics of resilience

24.5 Social Aspect of Resilience

Assessment of resilience, preferably quantitative assessment, must be the first step to resilience engineering. Since resilience concerns various aspects of system response to changes, there can be multiple measures. The resilience triangle is useful but it cannot be the only measure of resilience.

In addition, we should recognize that resilience is different for different stakeholders. The functionality people expect with a socio-technical system is different for different people, because different people have different interests, sense of values, needs, and so on. In discussing resilience engineering of socio-technical systems, some framework and methodology for resilience assessment that can consider such differences is highly necessary.

Figure 24.7 demonstrates this issue for recovery of infrastructures after the Great East Japan Earthquake. Resilience triangles are drawn here for different stakeholders and for different levels of needs. These results were obtained from the records of activities actually engaged in after the disaster.

Maslow [21] proposed a five-layered hierarchy of human needs, and the levels assessed in this example correspond to the basic three layers in Maslow's hierarchy: physiological, safety, and social needs. Figure 24.7 shows the resilience triangles for physiological and social needs. Physiological needs, which include air, water, food, clothing, and shelter, are the most fundamental needs for survival and they are located at the bottom of the hierarchy. Safety needs are located above physiological needs. They are related to individual safety and freedom from fear, which include personal security, financial security, health, protection against hazards and threats, etc. Social needs, which are located next above safety needs, are desires to be liked by others, to have interpersonal relationships, to belong to community, etc.

The assessment measure of each needs level was divided into more elementary measures until basic data on availability of separate infrastructure services were reached (Table 24.1). The basic data on the recovery rate of infrastructures after the earthquake were collected primarily from Internet web pages.

To consider different stakeholders, the persona method was used. The persona method is an attempt proposed by Cooper [22] in 1980s for reflecting different user needs and characteristics in product design. A persona is an imaginary

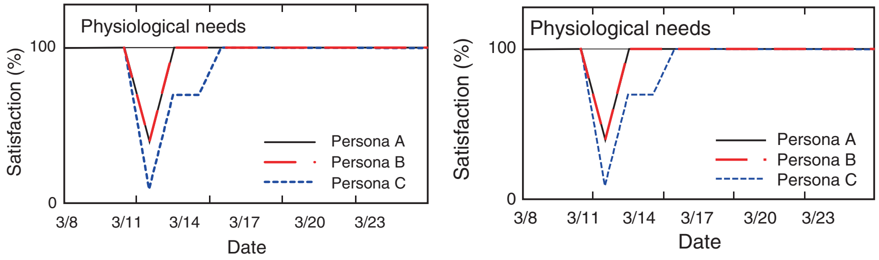


Fig. 24.7 Resilience triangle of utilities after the Great East Japan Earthquake

Table 24.1 Decomposition of assessment measure

Needs level	Item	Basic data
Physiological	Water	Water supply, water wagons
	Food	Shops, distribution
	Dwelling	Home, evacuation centers
	Medical care	Hospitals
	…	…
Safety	Electricity	Electricity grid, generators
	Water	Water supply
	Gas	Gas lines
	Information	Internet, TV, radio
	…	…
Social	Privacy	Home or evacuation center
	Job	Workplace, employer
	Relatives	State of relatives
	Property	House, cars
	…	…

but very specific user model that should be considered in designing products or services. In the persona method, many personas can cover the whole scope of expected users. Three personas of residents in the same town, Kesennuma, but of different features were created and used in this trial referring to opened notes of victims. Persona A is a male employee in his 20s, Persona B is a self-employed businessman in his 40s, and Persona C is a retired male in his 70s. Needs for different infrastructure services were then evaluated for each persona to assess the satisfaction level of physiological, safety, and social needs.

As shown in Fig. 24.7, difference in needs level and stakeholders affect the result of resilience assessment considerably. As for physiological needs, for instance, satisfaction dropped greatly and its recovery delayed for Persona C, because his health condition was poor and healthcare service was relatively critical. As for social needs, recovery of satisfaction was delayed greatly for Persona B, because he could not restart his self-owned business and lost financial independence.

It is a difficult task to establish assessment measures and methods that can cover various aspects of resilience as discussed in the previous section. In addition, however, it is also necessary to consider human perception and human recognition in assessment of resilience as demonstrated in this trial. Otherwise, outcomes of resilience engineering will not match our real needs, and the interests of vulnerable people will be ignored.

24.6 Key Issues in Resilience Engineering

24.6.1 Implementation Process of Resilience

The common characteristics of HROs give us a hint as to how we can incorporate resilience into socio-technical systems. In order to prevent resonance of function variability, the organizations have to repeat the process of four activities: anticipation, monitoring, response, and adaptation. In anticipation, the organization anticipates short-term and long-term threats and changes and gets ready for these threats and changes. In monitoring, the organization monitors operation conditions of the system to detect precursors of unfavorable performance variability that may cause resonance. The organization then takes actions to suppress performance variability so that the system will not go beyond its safety boundaries. Finally, the organization learns from past experience and restructures itself to adapt so that the system can absorb long-term changes.

Most of the base technologies for each step of the above process have already been developed in conventional domains, while more advanced technologies are also expected in the future. Based on these fundamental technologies, the methodologies for synthesizing them, assessing systems resilience, and social installation of the outcomes of research should be pursued. The key issues to be resolved in resilience engineering are as follows.

24.6.2 Assessment of Resilience

Though the resilience triangle shown in Fig. 24.5 is a simple but promising measure for quantitatively assessing systems resilience, the measure for representing system functionality has some arbitrariness. It is also argued that the cost of system recovery should be considered in the resilience measure [23]. The more cost is required, the less resilient the system becomes even if the area of resilience triangle is the same. In addition, the essential characteristics of resilience discussed in Sect. 24.5 should be reflected in the resilience measure. Among these characteristics, safety margin can be represented with risk measures that have been used in the conventional risk management, but the metrics for the other three characteristics have to be established in the future study.

Consideration of different stakeholders as discussed in the previous section is another issue in assessment of resilience. Which function of socio-technical systems is important depends on the situation where a particular stakeholder is placed. As shown in the case of the previous section, the needs for medical services are different between elderly people suffering some health problems and healthy young people. Socially vulnerable groups sometimes have to be taken into account in assessment of resilience rather than considering the average image of the public.

24.6.3 Interdependencies Between Systems

Our society is a complex system of systems that is composed of many systems linked together; it is impossible to understand the behavior of the total system if we look at systems separately. Critical infrastructures, for instance, including the electric power system, the water supply system, the transportation system, and the telecommunication system, are interrelated to each other, and one system depends on the others. The telecommunication system, for instance, does not work without electric power supply, and the electric power system is controlled using the telecommunication system. The breakdown of one system, therefore, sometimes leads to the breakdown of other systems.

A complex system spreads in a physical space and disturbance in one location sometimes propagates to another. It may cause the breakdown of the system over a wide area. The disturbance may propagate further to another system through the interdependencies among different systems. There is a fear that such cascading failures of critical infrastructures might result in serious damage to society.

In order to prevent such cascading failures in case of a devastating natural disaster, terrorist attack, or a crisis of the world market, it is necessary to understand system behavior including the interdependencies and take remedial actions to eliminate vulnerabilities in the system. In order to enhance the resilience of a system of systems, recovery plans must consider the interdependencies among different systems. Technologies allowing for a large-scale simulation are expected to be developed to consider the interdependencies of a system of systems.

24.6.4 Decision Support

In case of a crisis such that the function of a socio-technical system has been severely damaged, some mechanism is highly necessary to collect information on the location, type, and scale of damage, victims' requirements, distribution of resources available for system recovery, and to deliver the information to decision makers. Since fixed sensor-telecommunication networks will be damaged by the disaster, mobile systems that can be deployed over the affected area will be needed. Airborne or satellite sensing systems are often very useful for crisis management.

Collected information has to be delivered in a timely manner to decision makers. The critical information required by the decision makers must be selected from a vast amount of collected information, processed, and presented in a comprehensible manner; technologies such as image processing, data mining, information retrieval, and visualization will be effective for this purpose. While some official information and telecommunication systems were not functioning shortly after the Great East Japan Earthquake, some Social Network Services (SNSs) were very usable. In addition to centralized and specialized information systems, therefore, distributed and general-purpose systems should be focused on.

It should be kept in mind that those who ultimately make decisions are humans. Information is not usable for decision-making, if it does not match the cognitive characteristics or capabilities of a human. Consideration of human factors is still important in designing crisis management systems. In addition, since a group or an organization rather than an individual makes decisions in an emergency, communication, team collaboration, and organizational factors have to be considered.

Decision support is required not only to recognize emergency situations but also for recovery planning in real time, considering interdependencies among different systems. For this purpose, technologies such as disaster simulation, recovery plan optimization, and decision support systems should be developed.

24.6.5 Resilience in Ordinary Situations

Discussions so far have focused primarily on an emergency situation, but resilience is also relevant to safety, reliability, and security of socio-technical systems in ordinary situations. Resilience includes abilities of a system to keep its functionality by maintenance, to renovate itself in response to environmental changes, and to improve itself by learning lessons from past experience. While resilience in an emergency corresponds to recovery from a rapid breakdown of system function, resilience in an ordinary situation corresponds to recovery from a slow degradation of system function.

Maximum efforts are made to detect and eliminate latent flaws in a system in the conventional approach to risk management. It is, however, impossible to operate a complex socio-technical system with no flaws, thus we are forced to accept some latent flaws. Resilience engineering takes the position that function variability in a system is inevitable but that resonance and propagation of function variability have to be damped down to avoid accidents. Flexible response to environmental changes is a key to realizing resilient systems.

Minor incidents will occur frequently in every socio-technical system, but the trends of minor incidents will change following environmental changes. Organizational activities of collecting, analyzing information of such incidents, and renovating the facility, organization, or operations referring to the outcomes of analysis are essential for avoidance of large-scale accidents. Such activities are thought of as organizational learning or system evolution in a larger scale than the conventional activities of accident and incident analysis.

24.6.6 Social Installation

In order to install the outcomes of resilience engineering into society, redesign of social institutions and organizational operations will be necessary. How to motivate people to adopt the outcomes is a key issue here. Side effects, such as people responding to new technologies or new social institutions in an unanticipated manner that cause unfavorable consequences, have to be avoided. Studies on social simulation, organizational management, and project management, will contribute to designing social institutions and organizational operations considering such side effects.

Finally, new technologies must be accepted with consensus among people. When specialists claim that technologies contribute to realizing a better society, they will be asked questions on what are the criteria of social goodness and for whom it will be a better society. These questions should not be answered only by specialist as consensus must be developed among interested people.

24.7 Conclusion

The focal point of systems safety has shifted from technologies to human errors, socio-technical interactions, and now resilience as the scale and complexity of socio-technical systems have increased. Prevention of disasters is the main goal of the conventional approach to risk management, and it is achieved in terms of the design basis that is determined based on certain assumptions. If the reality exceeds these assumptions, losses will occur. Having experienced several disasters, however, like the terrorist attack on WTC and the Great East Japan Earthquake, people have recognized that society has to be ready also for unanticipated situations. Resilience, which is the ability of a socio-technical system to absorb effects of disturbances, maintain its normal function, and recover from damage, is a new frontier in systems safety proposed for answering this issue.

References

1. Dougherty EM, Fragola JR (1988) Human reliability analysis. John Wiley & Sons, New York
2. Reason JT (1977) Managing the risks of organizational accidents. Ashgate, Aldershot, UK
3. Hollnagel E, Rigaud E (eds) (2006) Proc. 2nd Resilience Engineering Symposium
4. Hollnagel E, Woods DD, Leveson N (eds) (2006) Resilience engineering: Concepts and precepts. Ashgate, Aldershot, UK
5. Hall RE, Fragola J, Wreathall J (1982) Post event human decision errors: Operator action tree/time reliability correlation. NUREG/CR-3010, BNL-NUREG-51601
6. US Nuclear Regulatory Commission (1994) Reactor safety study: An assessment of accident risks in U.S. commercial nuclear power plants. WASH-1400 (NUREG-75/014)
7. Dougherty EM (1990) Human reliability analysis—where shouldst thou turn. Reliability Engineering and System Safety 29: 283-299
8. Rasmussen J (1983) Skills, rules, knowledge: signals, signs, and symbols and other distinctions in human performance models. IEEE Trans. Systems, Man, and Cybernetics. MSC-13: 257-267
9. US Nuclear Regulatory Commission (2000) Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA). NUREG-1628
10. Hollnagel E (1998) Cognitive Reliability and Error Analysis Method. Elsevier, Oxford, UK

11. Tuomela R, Miller K (1988) WE-INTENTIONS. Philosophical Studies 53: 367-389
12. Kanno T (2007) The notion of sharedness based on mutual belief. Proc 12th Int. Conf. Human-Computer Interaction. Beijing: 1347-1351
13. Roberts KH (1990) Some characteristics of high-reliability organizations. Organization Science 1: 160-177
14. Senge PM (1990) The fifth discipline: The art & practice of the learning organization. Random House, New York, US
15. Holling CS (1973) Resilience and stability of ecological systems. Annual Review of Ecology and Systematics 4: 1-23
16. Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, Tierney K, Wallace WA, von Winterfeldt D (2003) A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra 19(4): 733-752
17. Taleb NN (2007) The black swan: The impact of the highly improbable. Random House, New York
18. Perrow C (1999) Normal accidents: Living with high-risk technologies. Princeton University Press, Princeton
19. Kastenberg WE (2002) On redefining the culture of risk aanalysis. Proc. 6th Int. Conf. Probabilistic Safety Assessment and Management (PSAM6), San Juan, 2002
20. Woods DD (2006) Essential characteristics of resilience. In Hollnagel E, Woods DD, Leveson N (eds) (2006) Resilience engineering: Concepts and precepts, pp. 21-34. Ashgate, Aldershot, UK
21. Maslow AH (1954) Motivation and personality. Harper & Row, New York
22. Cooper A (1999) The inmates are running the asylum. Macmillan, New York
23. Vugrin ED, Warren DE, Ehlen MA, Camphouse RC (2010) A framework for assessing the resilience of infrastructure and economic systems. In Gopalakrishnan K, Peeta S (eds) (2010) Sustainable and resilient critical infrastructure systems, pp. 77-116. Springer, Heidelberg, Germany