2014/08/14

Resilience Engineering and Safety-Ⅱ for Advanced Accident Management

Masaharu Kitamura
Emeritus Professor of Tohoku University
President of Research Institute for Technology Management Strategy

1

OUTLINE

- Introduction
- History
- Safety-Ⅱ
- Essential Capabilities
- Applications
- Concluding Remarks

2

Introduction

- The word "resilience" is gaining popularity in many domains where "safety" is an issue of serious concern.
- The popularity is becoming even higher in Japan after the East Japan Earthquake and the nuclear disaster at the Fukuushima-Daiichi Nuclear Power Station (NPS).
- For example, the prime minister of Japan introduced a new position named minister of national resilience in his cabinet.
- But the method to establish "resilience" is not yet established.

3

Introduction

- Resilience is defined as the intrinsic capability of a system to adjust its functioning prior to, during, or after internal changes or external disturbances, so that the system can continue operations under expected and unexpected conditions.
- When the magnitude of an internal change or external disturbance is extraordinarily large, the resilient system may change its operational mode and become less productive, but can continue its operation without falling into a catastrophic state.

4

Introduction

- The concept of resilience thus covers not only mere safety but sustainability of operation and graceful-degradation as desirable characteristics of socio-technical systems.

5

History

- In 2004, a small group of international experts were invited to participate in a special symposium held in a small town of Söderköping in Sweden.
- The experts discussed about possibilities of overcoming the limitations of existing approaches toward enhancing system safety, and the notion of resilience engineering has been gradually formulated through the discussions
- Hollnagel, E, Woods, D. D. , Leveson, N. (Eds.) (2006), Resilience Engineering: Concepts and Precepts. Aldershot. UK: Ashgate Publishing Co.

6

History

- Since then, a number of research papers has been published, five international meetings named Resilience Engineering Symposium have been held, and several important books have been published.
- Though the methodology of resilience engineering is still young and growing, a wide variety of valuable lessons and observations have been obtained up to present.

7

Pursuit of Safety by Eliminating Causes-1

- Gigantic Seawall : Height 10m, Length 2,400m.
- Located in Iwate prefecture, Town of Tarou

Photos are eliminated.

8

Pursuit of Safety by Eliminating Causes-2

- Disaster Prevention Building Expected to Withstand a Tsunami

Photos are eliminated.

9

Safety- Ⅱ

- The central idea of safety pursued by the adoption of these artifacts is not resilience but robustness.
- Robust design is useful enough as far as the magnitude of external disturbances are lower than the expectations.
- However, if the magnitude exceeds the expected level, the robustness-based safety becomes useless.
- More emphasis must be placed on resilience-based safety.

10

Safety- Ⅱ

- The idea of robustness-based (i.e. conventional) safety is; "The safety of the system will be maintained if potential causes of failures are eliminated in advance".
- This notion of safety is named **Safety- Ⅰ**.
- As far as the safety in this sense is pursued, the main efforts toward safety are focused on reduction of undesirable factors such as a tsunami as shown in the previous slides.

11

Safety- Ⅱ

- The resilience-based safety aims at empowering relevant functions of the system so that the system can continue operation even though the performance might be somewhat degraded.
- The safety pursued in this way is named Safety-Ⅱ. Of course this increase in the number of desirable events will in consequence lead to decrease in the number of undesirable events.
- But the Safety-Ⅱ approach is mode appropriate to safety management of modern socio-technical systems where the number of failures are becoming less and less via various improvements in mechanical and other hardware-related technology, human factors study, organization management techniques, etc

12

Safety- Ⅱ

- The resilience-based safety to empower relevant functions of the system so that the system can continue operation even though the performance might be somewhat degraded.
- The safety pursued in this way is named Safety-Ⅱ. Of course this increase in the number of desirable events will in consequence lead to decrease in the number of undesirable events.
- But the Safety-Ⅱ approach is mode appropriate to safety management of modern socio-technical systems where the number of failures are becoming less and less via various improvements in mechanical and other hardware-related technology, human factors study, organization management techniques, etc

13

Safety- Ⅱ

- If the ratio of failure cases to success cases is as low as 1:10,000 or even less, every failure case tends to be a rare case.
- Efforts of examining the rare case to extract lessons to prevent future accident will be less efficient since the future accident will be caused by other cause(s) often unexpected.
- The improvement of system's capability for performance adjustment via application of resilience engineering will be more beneficial in this context.

14

Safety- Ⅱ

- The pursuit of system safety in the sense of Safety-Ⅱ does not imply to exclude the conventional activities (i.e. high reliability design of hardware components and systems, incorporation of design improvements suggested by human factors principles, standardization of operational procedures, etc.) pursuing safety in the sense of Safety-Ⅰ.
- However, the novel safety methodology based on Safety-Ⅱ is necessary for supplementing the well-established traditional methodology based on Safety-Ⅰ.

15

Essential Capabilities

- The framework of resilience engineering is based on the recognition that systems are always changing either due to internal changes or external disturbances.
  - No system can bee free from these changes.
- A system must be able to adjust its performance.
  - by either a reactive method which takes place after something has happened, or a **proactive** method which takes place before something happens.
  - The latter approach is basically more preferable since it can be used to prevent adverse events to take place.

16

Essential Capabilities

- But the potential benefit provided by the proactive method is limited by the uncertainty of future situations.
- An organization responsible for safety of critically important socio-technical systems such as NPSs must be aware of the fact that higher level of safety can only be attained by paying due attention to the potential benefit of the proactive approach despite the potential sacrifice that might be caused by the intrinsic uncertainty of future situations.

17

Essential Capabilities

- Essential capabilities needed for attaining resilience through appropriate performance adjustment are briefly summarized as follows:
  - Knowing what to do, or being able to respond to regular and irregular changes and disturbances.
  - Knowing what to look for, or being able to monitor that which changes, or may change, so much that it will require a response in the near term.
  - Knowing what to expect, or being able to anticipate changes, threats and opportunities further into the future.
  - Knowing what has happened, or being able to learn from experiences to obtain lessons.

18

Essential Capabilities

- Additional requirements for attaining resilience:
  - Resources are also important in order to be able to respond properly. Even if one knows what to do and how to do it, the work cannot be done without enough time, tools, personnel, funding, and so forth.
  - Another feature of the resilience engineering is in that it pays more attention to success cases.
  - Historically, safety engineering have been paying attention to accidents, trying to find out failures (mechanical as well as human-originated) responsible for the accidents, trying to identify key causes responsible for the failures, and tying to prevent accidents by reducing or eliminate the causes.

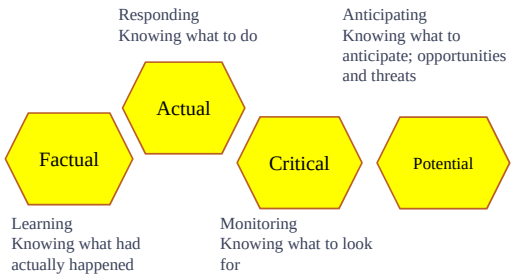
19

Essential Capabilities

- This approach has been useful for relatively simple artifacts, but not so any more for large-scale, complex artifacts in which accident mechanisms cannot be described by simple, cause-consequence relationships (Perrow, 1984).

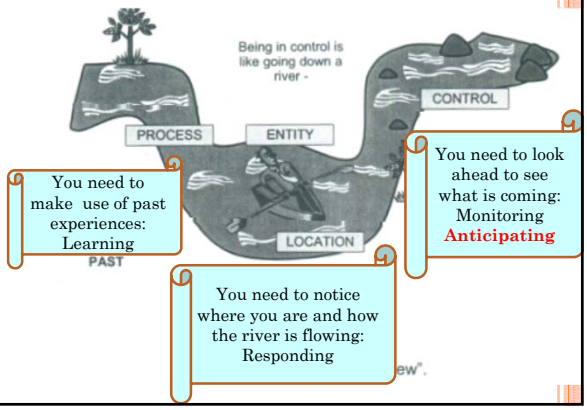
20

Key Capabilities Needed for Resilient Systems



Prepare and allocate appropriate resources.
Pay more attention to success cases rather than failures.

21



Essential Capabilities

- A new paradigm for pursuing safety is definitely needed in current society where a resilient operation of socio-technical systems is critically important for sustainment and development of our society. The endeavor toward establishment of the methodology of resilience engineering summarized as
- the four capabilities, together with the requirements of
  - (1) appropriate resource management and
  - (2) emphasis on learning lessons from success events rather than from failure events
- is a quest for meeting the demand of modern society.

23

Applications

- The resilience engineering methodology has been applied in various domains including airline safety, air traffic control, railway transportation, offshore production, power plant maintenance, financial service systems, patient safety, etc.
- In this panel discussion, one particular application to severe accident investigation is reviewed.
- Most of the activities of Fukushima accident investigation seem to be based on the notion of Safety– Ⅰ.
  - In consequence, tremendous efforts had been paid to identify a large number of cause–consequence relationships that contributed to the onset or development of the accident. After the identification of the causes, recommendations had been formulated to reduce or eliminate the causes.
  - As a natural outcome, the recommendations are large in number and complicated in structure

24

Applications

- It is much promising to restructure and prioritize the large number of recommendations so that countermeasures to prevent recurrence of the disaster can be implemented in more efficient manner.
  - Guidelines derived from resilience engineering have been used to meet the needs.
- Ongoing efforts to improve safety of NPSs are inclined to increase Safety-Ⅰ by hardware systems.
- Lack of capabilities for performance adjustments in diverse situations must be resolved by proper implementation of suggestions derived from resilience engineering.
- Efforts to improve nuclear safety in terms of the Safety-Ⅱ will be imperative for realistic safety management of nuclear facilities.

25

Concluding Remarks

- Resilience engineering is still in its development stage. Further efforts are definitely necessary for attaining higher applicability to target domains.
- However, even at the present stage, the methodology can provide us with rich suggestions and proposals toward enhancing safety of artifacts.
- It is obvious that the nuclear safety community will be highly benefitted by the HT experts if they can develop efficient and dependable tools for "faster-than-real-time simulation" of nuclear accidents.
- One might claim that such a simulation tool is already available.

26

Concluding Remarks

- However, it is absolutely needed that the software tool can cover effects of human interventions causing various changes in plant configuration.
  - Note that the type and timing of the intervention are not specified as initial conditions of the simulation.
- Such a simulation software can be utilized to estimate time margins to core melt and/or release of radioactive materials . Information derived by such tools will be most helpful for operators in a control room of a NPS under severe disturbances.
- Similar simulation can be utilized during design and evaluation phases of countermeasures to be implemented to mitigate severe accidents.

27

Concluding Remarks

- Another future application, highly desirable for nuclear safety, would be the development of techniques for evaluating resilience of the nuclear components and/or systems withstanding beyond-design-specification situations.
- Further applications can be proposed and resolved under close collaborations between nuclear and thermal science experts.

28