RESILIENCE

Important issue for ensuring cyber security

Makoto Takahashi
Professor, Tohoku University
Advisor, CSSC-TTHQ

What is Resilience?

- In an increasingly interconnected world - financially, ecologically, politically -, small errors in one place can cascade into broader system failures.
- *Ability to adapt, accommodate and bounce back* is only going to become more important.

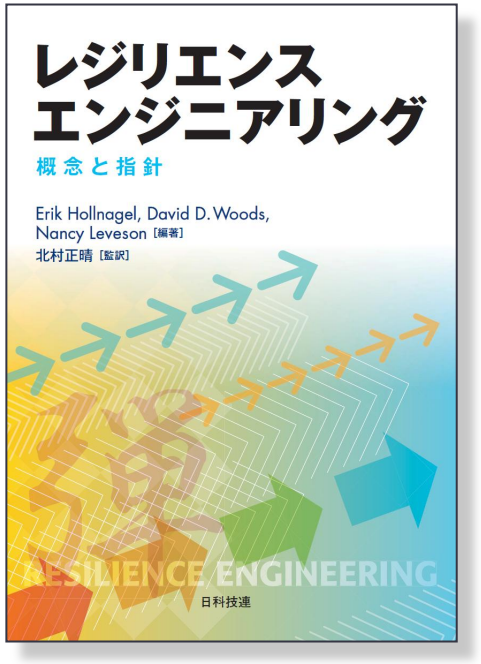
Resilience is the ability of a system to maintain its necessary operations under unexpected as well as expected situations before, during and after the disturbance or changes by adjusting its functions

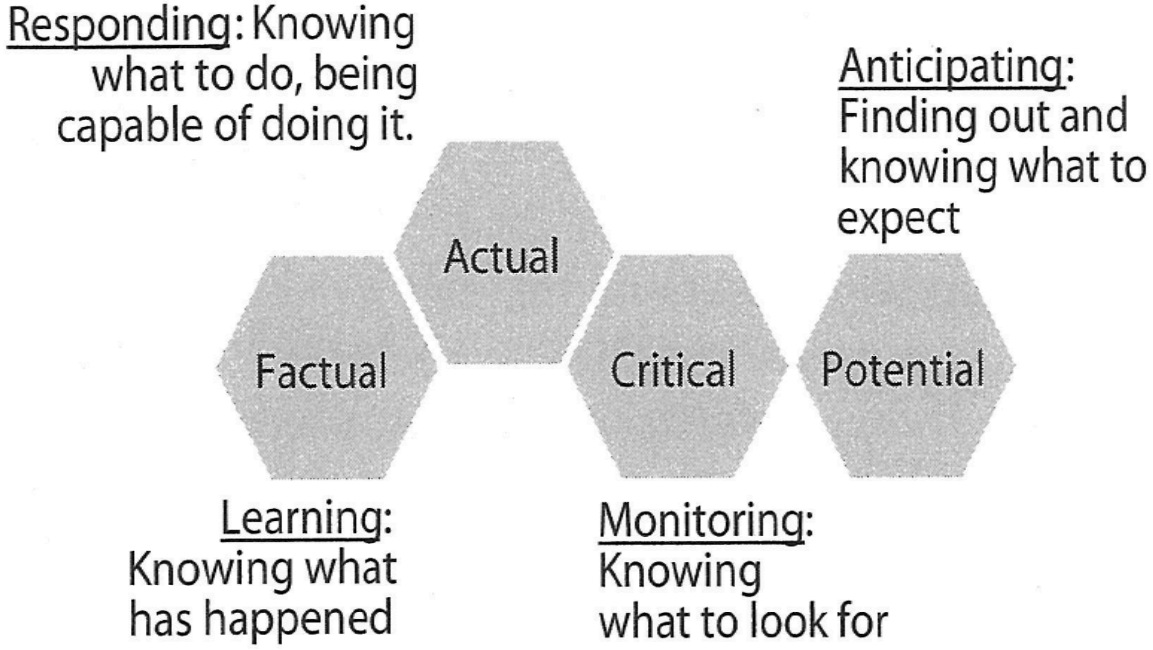
変化や外乱の前、途中、後でシステムが自分の機能を調整し、それによってシステムが想定内、想定外、いずれの状況に対しても必要な動作を維持することができる能力

What is Resilience? (Con’td)

- **Resilience Engineering: Concepts and Precepts**

(Erik Hollnagel, David D. Woods, Nancy Leveson（Ed.）)





Specific features of *cyber security* compared with *organizational safety*

- ***Cyber security:***
  - Cyber attack is intentionally made by malicious human being.
  - Cyber attack would escalate against the activities for protection.
- ***Organizational safety:***
  - Errors would occur unintentionally mainly by human beings under error-prone environments.
  - Safety state of organization would degrade along with time.

However, they both have the following features in common.

- Preparing for future threats are crucially important.
- Recognition of risk is difficult because of cognitive biases.
- State of the whole system is always changing.

What we have learned from Fukushima

- **Learning only from past experiences is not enough to cope with events with ultra low probability.**
- **Accident reports tend to suffer from hindsight / cognitive bias**
- **Focus more on the positive cases, not negative cases.**
- **A constant sense of unease is important.**
- **Sensitivity to failure and to margin to safety boundary is definitely necessary.**

These lessons should be applied to the field of Cyber Security in order prevent disastrous event to happen well in advance.

Importance of human factors (1)

- **From viewpoint of plant operators:**
  - When they first encounter system malfunction:
    - They first consider past experiences and try to interpret current situation within them.
    - If the current situation can not be explained based on the past experiences, they start to consider some hypotheses and check whether the current situation can be interpreted according to any of these hypotheses.
    - As subjective possibility of cyber attack may be very low, hypothesis of cyber attack would not be considered in the beginning.

When cyber attack really happened, it is crucial that the information should be provide to operators to recognize something different from conventional system failure is occurring somewhere in the plant system.

Importance of human factors (2)

- **From viewpoint of board of directors:**
  - The efforts for safety are difficult to be justified.