Importance of Human Positive Contribution to Safety -Insight from Safety-II Concept-

Professor Makoto Takahashi

Graduate School of Engineering, Tohoku University

Representative Director of CSSC (Control System Security Center)

Outline of Today's Talk

-Introduction to Resilience Engineering(RE)

-Example from 3.11 disaster in Tohoku Area

-Implications for cyber resilience

Complex System?

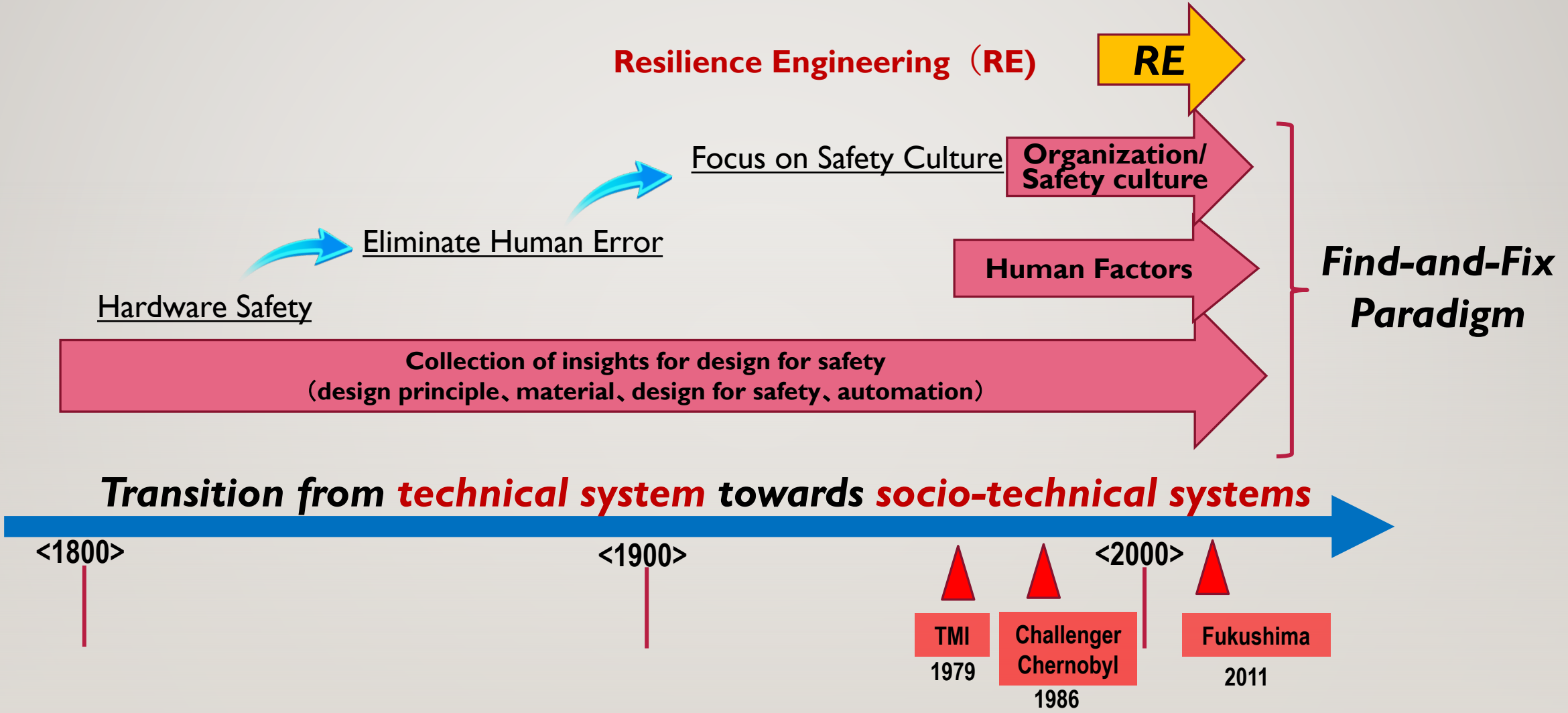
Mechanical System

- ✓ Cause of failure can be identified explicitly.
- ✓ Function of whole system can be described as the collection of each part
- ✓ Reductionism holds.

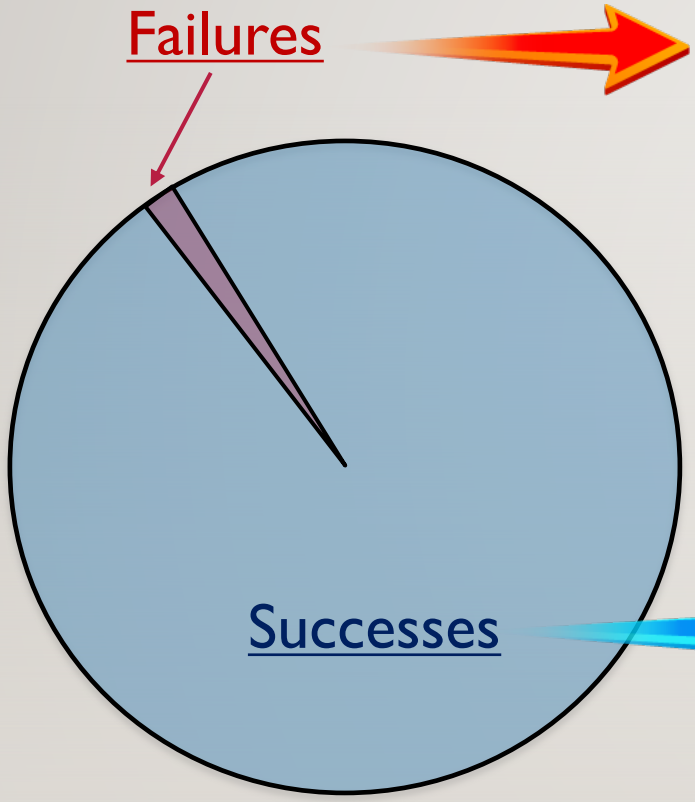
Socio-technical System

?

Historical view of approaches to ensuring safety for technical system



How can we enhance level of safety of the system which has already been highly safe and reliable?



- ✓One failure out of ten thousands success cases is analyzed in detail and lessons are extracted.
- ✓Learning from failure is important but failure tends to be rare case

- ✓Success cases are out of interest
- ✓No lessons learned from these cases ?
- ✓Good practices exist not only in emergency but also in normal functioning

Safety- Ⅱ

Safety-Ⅰ and Safety-Ⅱ(1)

Re-definition of safety

Safety-I: Conventional definition of safety seeking for static state with non-event as safe

- ✓ Characteristics and behavior of each equipment and system structure are fixed and known
- ✓ Expected human behavior are also known in advance as shown in instruction manual

Safety-II: Safety including dynamic failure avoidance and recovery

- ✓ Systems and environments are always changing.
- ✓ Potential for adjustment to deal with change

Typical Examples of Safety-I Approach

- Compliance-based safety approach
  - Require to follow rules and regulations strictly
  - Severe penalty for those violating rules
- Check number of undesirable events (incidents)
  - Based on this performance indicator, level of safety is determined
- Long period of injury-free and incident free performance means higher level of safety. -->> ????
  - Deepwater Horizon in the Gulf of Mexico caused a well blowout, which killed 11people after six years of injury-free performance records.(April 20th,2010)

Ref: SIDNEY DEKKER, "THE SAFETY ANARCHIST"

Limit of Safety-I Approach (1)

- ✓ **Rule inflation**

  More rules sometimes not only create no more safety ; they can also create more risk

- ✓ **Too much resource spent in compliance sector**

  One in eleven working Australians now work in the compliance sector.

- ✓ **Compliance has no relation to safety**

  Research in healthcare also shows a disconnect between rule compliance as evidenced in surveys and how well a hospital is actually doing in keeping its patient safety

- ✓ **Compliance increases risk**

  Compliance with existing rules and regulations cannot deal well with novelty, complexity and uncertainty

Ref: SIDNEY DEKKER, "THE SAFETY ANARCHIST"

Example of "Compliance Increases Risk"

- **Compliance with existing rules and regulations cannot deal well with novelty, complexity and uncertainty**
- **Expert practitioners typically adapt their work so smoothly, so unremarkably, that the existence of these adaptations isn't clear to those who have only a distant or superficial view of the work.**
- **All they might see is deviation.**

<Crash of a large passenger aircraft near Halifax in 1998>

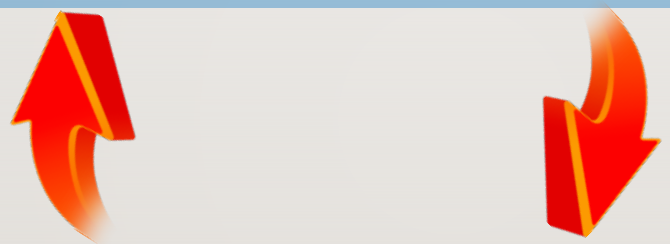
- ✓ *After a departure, a burning smell was detected -> Smoke was reported inside the cockpit*
- ✓ *Co-pilot preferred a rapid descent and suggested dumping fuel early*
- ✓ *But, the captain told the co-pilot not to descend too fast and insisted they comply with applicable procedures(checklists) for dealing with smoke and fire.*
- ✓ *The captain delayed a decision on dumpling fuel.*
- ✓ *With the fire developing, the aircraft uncontrollable and crashed into the sea, taking all 229 lives.*

Ref: SIDNEY DEKKER, "THE SAFETY ANARCHIST"

Limit of Safety-I Approach (2)

✓ **Double Bind**

If rote rule following persists in the face of cues that suggests procedures should be adapted, this may lead to unsafe outcomes. People can get blamed for their inflexibility – their application of rules without sensitivity to context.



If adaptation to unanticipated conditions are attempted without complete knowledge of circumstances or certainty of outcome, unsafe results may occur too. In this case, people get blamed for their deviations – their non-adherence.

Ref: SIDNEY DEKKER, "THE SAFETY ANARCHIST"

Safety-Ⅰ and Safety-Ⅱ(2)

Needs for performance adjustments

- ✓ It is essential to learn from what happens every day - from performance variability and performance adjustments
- ✓ Because this is the reason why things sometimes go wrong, and because this is the most effective way to improve performance.

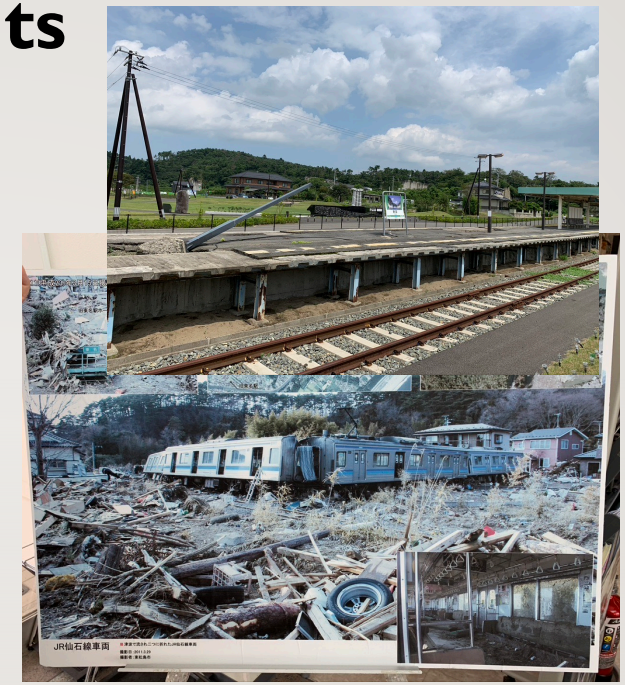
- ✓ Because these performance adjustments work, people quickly come to rely on them - precisely because they work.
- ✓ Indeed, they may be tacitly reinforced in this when things go right but blamed when things go wrong.

Ref: Hollnagel, E. Safety- I and Safety- Ⅱ, The Past and Future of Safety Management. Taylor & Francis, 2014

Difficulty in performance adjustments

Senseki Line(JR Local Line)

- Inbound train bound for Sendai leaved Nobiru-Stn at 14:46. Just after leaving, severe earthquake hit the train. Train driver received instruction to stop the train from operation center. Trained stopped at the position 700m from the station.
- **According to the JR internal rules**, train crew are expected to direct all passengers on board to the nearest designated evacuation location, which was Nobiru elementary school.
- The crew guided all passengers there. Just after they reached the location, tsunami hit the location and several passengers died.



- **It is important to avoid hindsight judgement.**
- **Avoiding just following predefined rules blindly**
- **Anticipate a progress of what is going on**
- **Respond flexibly**

- Outbound train bound for Ishinomaki also stopped just after leaving Nobiru-Stn.
- When train crews gather all 50 passengers into one car and suggested evaluation to Nobiru elementary school **following the rule**, one passenger living this area suggested not to do so.
- He anticipated that "Staying here in the train is safer because we are on a rise". Others followed his suggestion.
- Tsunami stopped just before the train. Surroundings were flooded.

Safety-Ⅰ and Safety-Ⅱ (3)

	Safety-Ⅰ	Safety-Ⅱ
Objectives	Things that go wrong	Things that go right
Basic Principle	Find and fix	Share good practice and apply
Meaning of Safety	Minimization of failure	Maximization of success
Health Analogy	Avoid disease and injury	Seek for better health
Purpose of Accident Investigation	Identification and elimination of failure	Finding lessons for mitigation
Role of human	Follow SOP	Use SOP for reference and seeking for better
Cost for safety measures	Indispensable Cost	Investment for better productivity
Basic recognition	Technology, environment and organizations are definitive and can be described explicitly	Technology, environment and organizations are dynamic and always changing. Uncertainty is unavoidable.

Safety-Ⅰ and Safety-Ⅱ(4)

Relationship of Safety-I and Safety-II

- **While Safety-II represents an approach to safety that in many ways differs from Safety-I, it is important to emphasize that they represent two complementary views of safety rather than two incompatible or conflicting views.**
- **Many of the existing practices can therefore still be used, although possibly with a different emphasis.**
- **Effective performance requires both that people can avoid that things go wrong and that they can ensure that things go right.**

Ref: Hollnagel, E. Safety- I and Safety- Ⅱ , The Past and Future of Safety Management. Taylor & Francis,2014

Concept of Resilience Engineering(1)

- Resilience Engineering is a concept for enhancing safety of socio-technical systems, where human beings play important roles.
- The definition of safety in Resilience Engineering is the "ability to succeed under varying conditions", in contrast to the traditional view of "freedom from unacceptable risk" .
- In Resilience Engineering, emphasis is on **things that go right** than things that go wrong, and stresses on **understanding the normal functioning of socio-technical systems.**

Concept of Resilience Engineering(2)

Underlying principle of Resilience Engineering

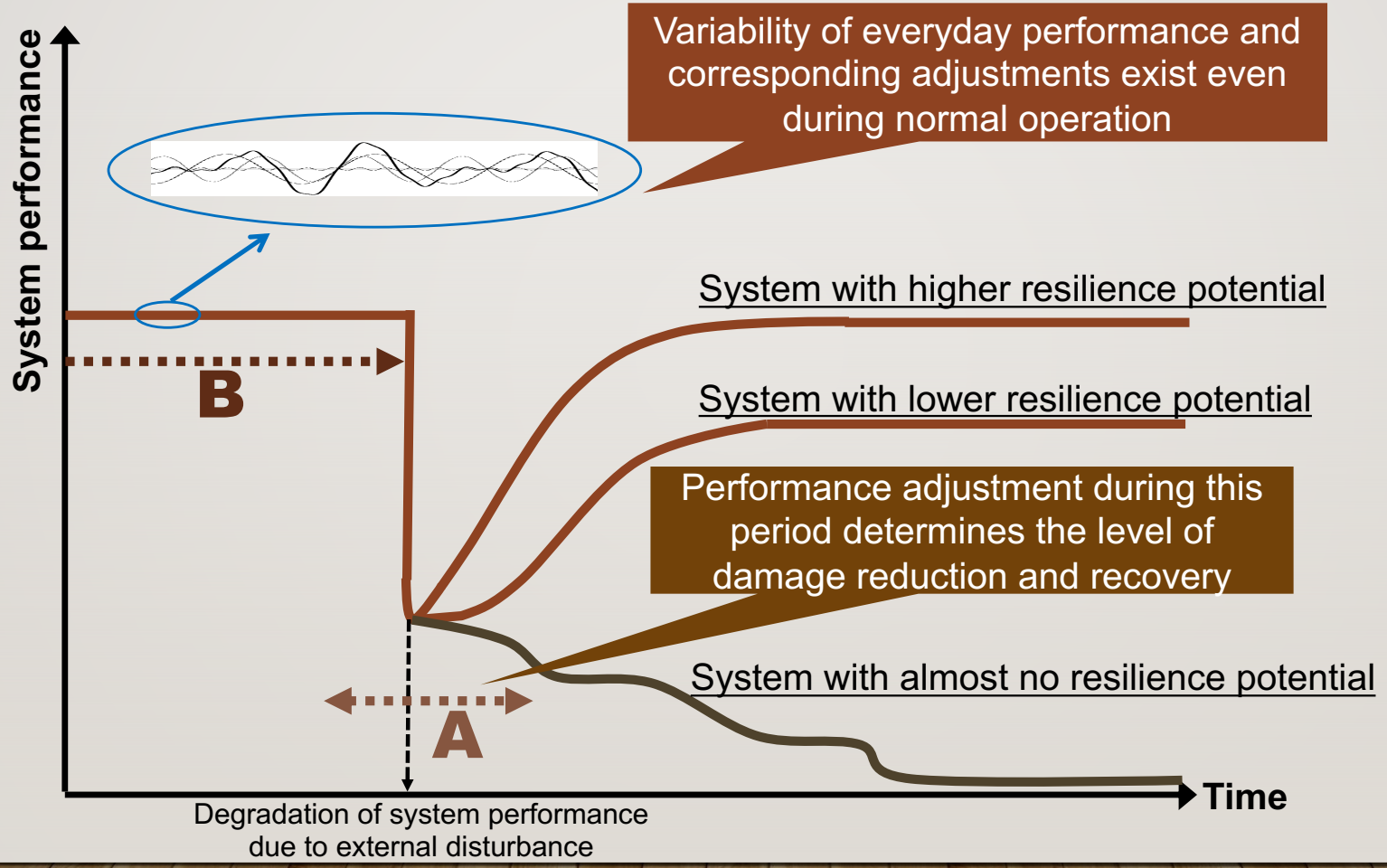
a. Systems and environments are always changing.

b. Important decisions are made based on imperfect information.

c. Systems are required to be beneficial and pursue efficacy, which can result in a "drift to failure", unless special attention is given to maintain safety.

d. Safety is important but it is not the main purpose of a functioning system.

Concept of Resilience Engineering(3)



Concept of Resilience Engineering(4)

Four main potentials for resilience

-Responding (knowing what to do)

Responding is defined as the ability to deal with ongoing changes/disturbances properly. This includes the adjustments of systems behavior or by taking prepared actions.

-Monitoring (knowing what to look for)

Monitoring is defined as the ability to recognize threats to be watched. This also means knowing what to monitor to recognize threats.

-Anticipating (knowing what to expect)

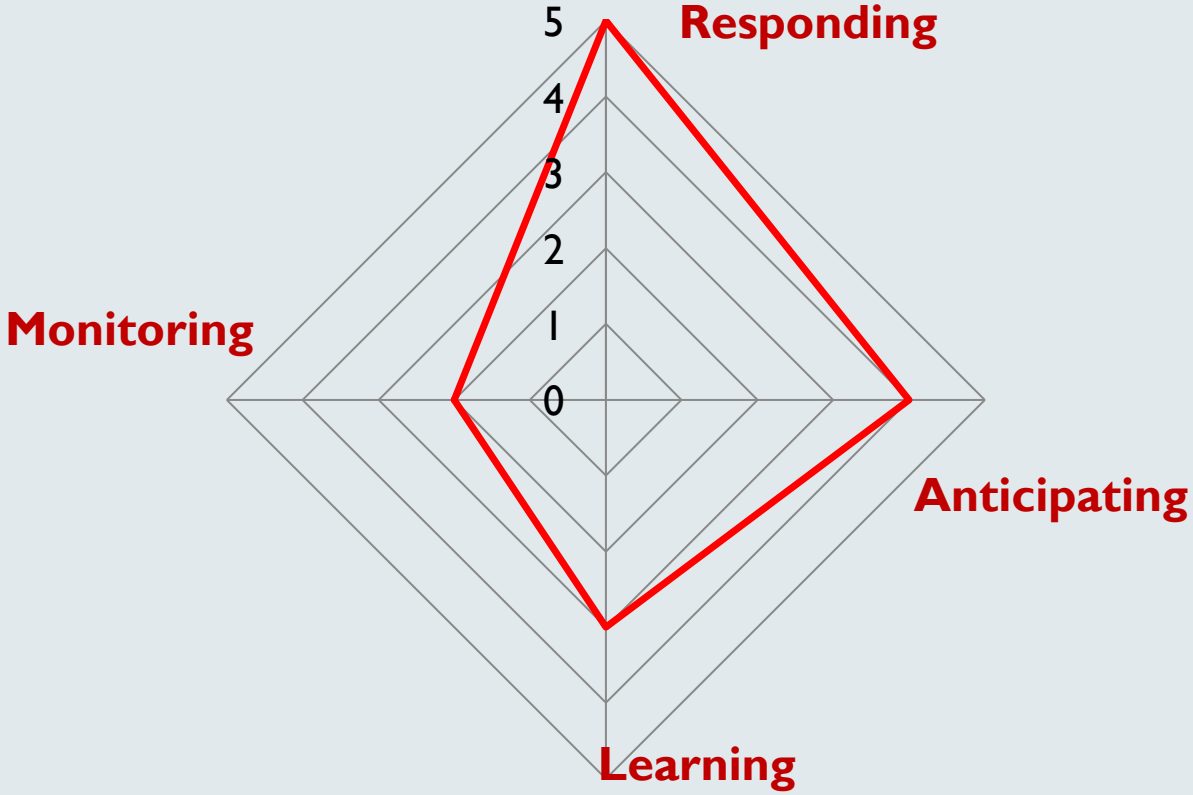
Anticipating is defined as the ability to decide the possibility of developing events, new threats, or good opportunities in a longer timeframe when compared to monitoring.

-Learning (knowing what has happened)

Learning is defined as the ability to improve the above potential to avoid a "drift to failure". For effective learning, the selection of focused events and the methods for deriving lessons from events are necessary.

Assessing the Potentials for Resilient Performance

Resilience Assessment Grid: RAG



https://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf

Example from 3.11 disaster in Tohoku Area

Good examples from the viewpoint of resilience engineering during 3.11 disaster beyond conventional safety approach

- ✓ Japanese Red Cross Ishinomaki Hospital
- ✓ Road network recovery
- ✓ Successful out docking of a tanker at Fukushima Daiichi Nuclear Power Station

Ishinomaki Red Cross Hospital

Ishinomaki Red Cross Hospital (Number of bed:402)

- ✓ All staffs **anticipated** huge damage and sufferers and preparation of triage and medical treatments had been completed soon.
- ✓ Normal operation: 60 emergency patients
- ✓ Two days after disaster: 1251 emergency patients
- ✓ 64 patients were carried by helicopter.
- ✓ Lobby and corridor were packed with patients and accompanying family and relatives.
- ✓ **Responding** by the tentative increase in the number of beds (investigation rooms), which was illegal.
- ✓ Persuaded healthy refugees to leave
- ✓ Provided meals to patients, while staffs could not eat.

Road Network Recovery

Responding actions just after the huge earthquake and tsunami:
Head of Tohoku Regional Development Bureau

- ✓ **Monitoring** of Route 45, Tohoku Express way and important bridge
- ✓ **Anticipation** of large scale disaster and alternation of **Responding** actions from recovery to minimum road opening work.
- ✓ **Responding** with all available resources (Road maintenance office, Civil engineer and construction industries)
- ✓ **Monitoring** aftershock, tsunami and state of ocean,
- ✓ retaining human resources and devices and **responding** to the request for road opening work
- ✓ **Anticipating** the loss of administrative functions, dispatching staffs from Tohoku Regional Development Bureau
- ✓ Realization of **responding** measures to the disaster by tearing down the wall of sectionalism

Emergency out docking of a tanker at Fukushima Daiichi Nuclear Power Station

- A tanker was at the site port and was landing heavy oil when the earthquake occurred.
- Operators followed the emergency procedure to stop landing and made narrow escape from the site port before tsunami came.
- They intentionally cut the oil fence to shorten the time required to escape.
- If they had failed to out dock before tsunami, the ship may have crashed against the reactor building and the leaked oil may have caused uncontrollable fire.

-Why they succeeded?-

- Human resources were available using communication network prepared in advance
- Successful sharing of severity of crisis among related people on board and on land
- They were well trained for emergency escape from port
- Leader decided emergency escape immediately and made task allocation and task priority promptly.

Example: Application of Resilience Engineering to Practical Field(1)

"Using The RAG To Assess International Space Station Organizational Resilience"

The assessment project lead saw the use of resilience engineering as an opportunity to obtain insights into the issue beyond what conventional risk management approaches would normally offer.

- How does ISS handle weak signals that indicate potential safety threats?
- How does ISS balance ongoing resource constraints with production pressures?

Paper presented at 7th International Symposium Liege (Belgium), 26–29, June, 2017

Example: Application of Resilience Engineering to Practical Field(2)

"Trailblazers into Safety- Ⅱ :American Airlines' Learning and Improvement Team (LIT)"

Building LIT's Approach to Safety-II

1. Develop your own language based on your understanding of the how RAG will be used in the cockpit. As the essence of the potential for resilient behavior only has context within the trade space of the work being done, likewise the RAG model should be adapted to meet the unique attributes of the work of piloting commercial airliners.
2. Devise your own data collection. Using data acquired via a data stream anchored in "threats and errors" would be anathema to the appreciative mindset required for a Safety-II approach. The recommendation was to begin the Safety-II program by creating a separate, non-TEM driven data collection and analysis method.

A White Paper Outlining AA's Beginnings of a Safety－Ⅱ Journey

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.

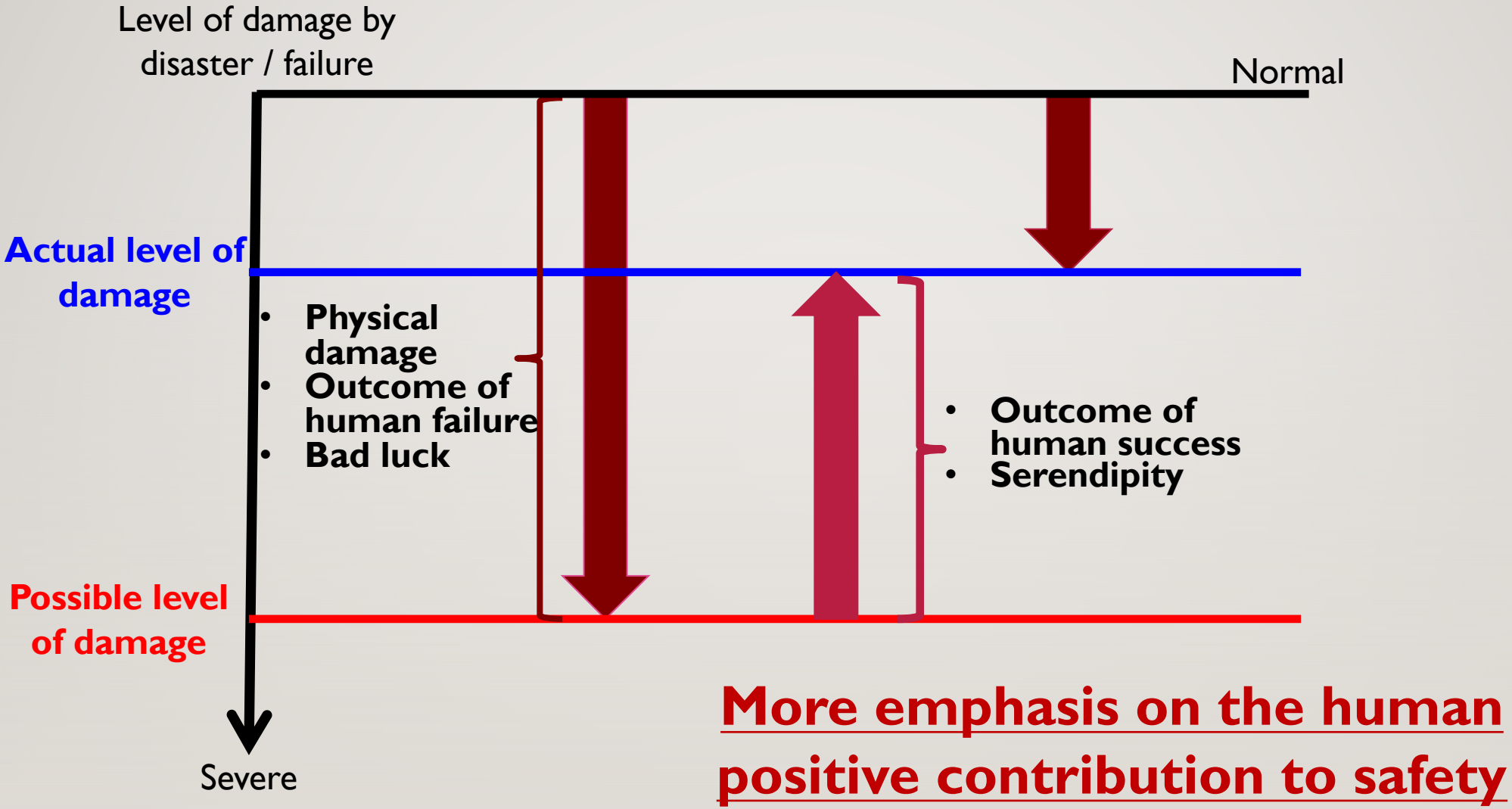
- **Preparing for future threats are crucially important.**
- **Recognition of risk is difficult because of cognitive biases.**
- **State of the whole system is always changing.**

Implications for Cyber Resilience

- Being prepared to be unprepared
- Maintain constant sense of unease
- Be aware of:
  - cognitive bias in recognition of risk
    - that our knowledge is always imperfect
    - that environment is always changing

Concept of resilience engineering can be applied to human organization to mitigate the effect of cyber attack

Insights From Resilience Engineering



More emphasis on the human positive contribution to safety