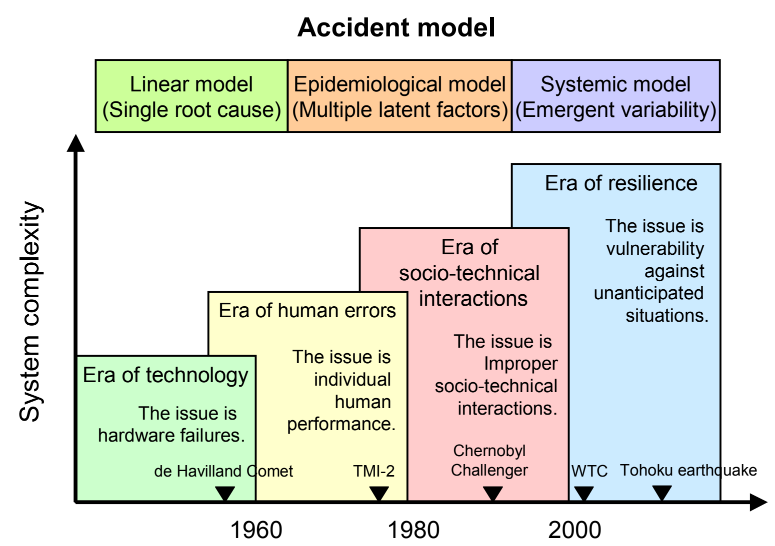
What is Resilience Engineering?

Resilience Engineering Research Center
Kazuo Furuta

Changing focus of system safety



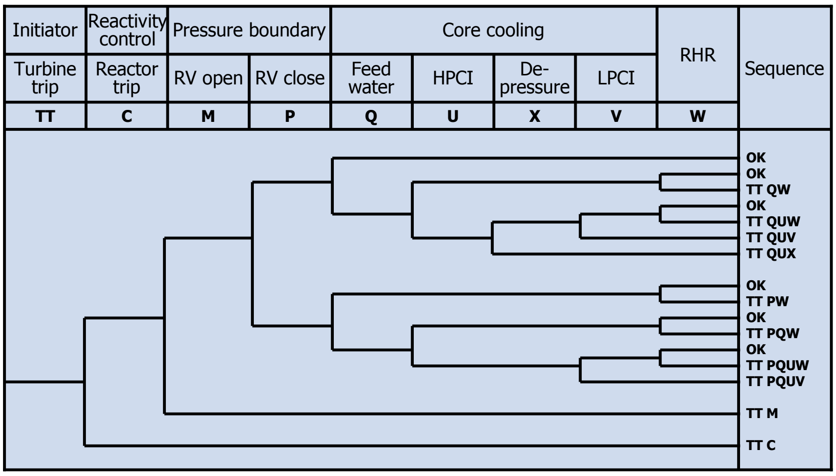
Linear model

- Premise
  - An accident occurs when a series of events occur in a specific order.
- Causes
  - Malfunctions and failures (root causes) of a definite set system components (equipment or humans)
- Countermeasures
  - Eliminate events or situations that may become root causes of an accident

Principles behind linear model

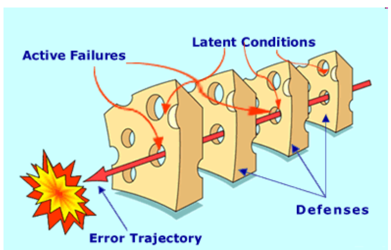
- Decomposition principle
  - Any system is composed of components and understandable by reduction into the components.
- Bimodal state principle
  - Functioning of any system can be described just by two states: normal (success) or abnormal (failure).
- Independence (linear) principle
  - Interactions between system components are definite, and it can be assumed that their functions are independent each other.

Example of linear model



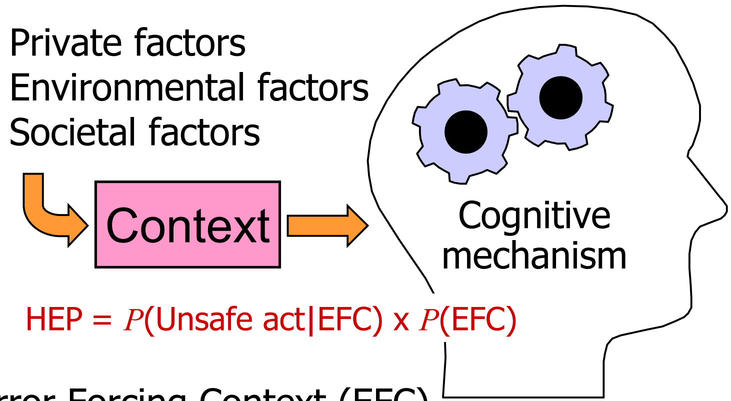
Epidemiological model

- Premise
  - A combination of multiple failures and latent conditions cause an accident.
- Causes
  - Degradation of safety barriers (physical, functional, symbolic, conceptual)
- Countermeasures
  - Detect and repair degradation of safety barriers organizationally



スイスチーズ・モデル

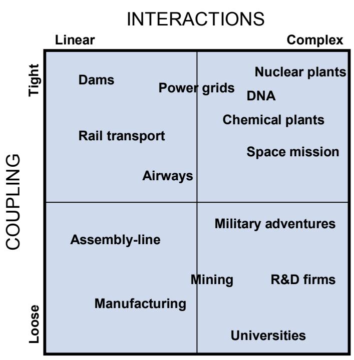
Epidemiological view of human errors



HEP = P(Unsafe act|EFC) x P(EFC)

- Error Forcing Context (EFC)
  Context such that humans inevitably make an error

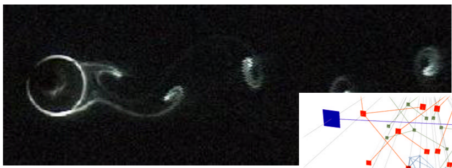
Normal accidents



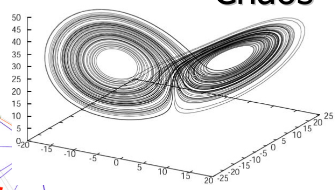
- Charles Perrow (1984)
- Accidents in a huge and complex system are inevitable
  - Unforeseen strong connections between separate parts of system
  - Non-linear system behavior
  - Complexity beyond human understanding
  - Erroneous safety protections
- Acceptance of technologies should not be determined by risk but by potential danger.

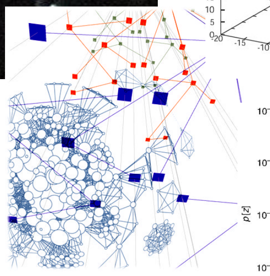
Complex system

Emergent phenomena

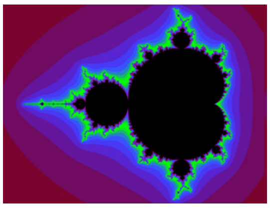


Chaos

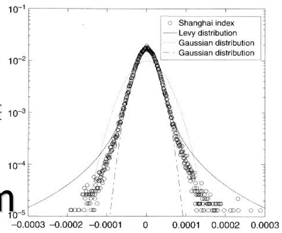




Network system

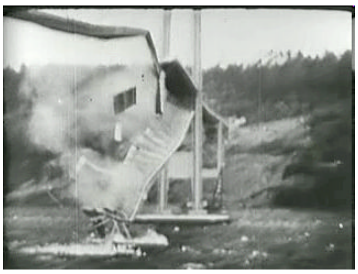


Fractal



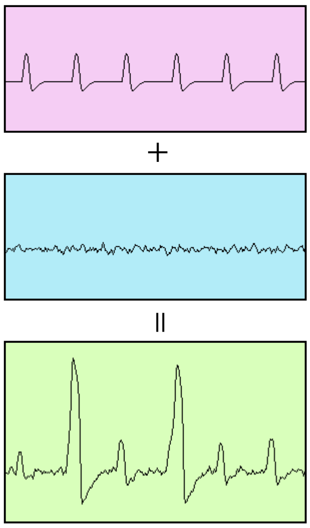
Stylized fact

Non-linear system and resonance



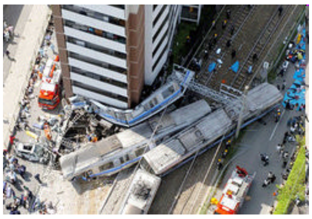
Tacoma Narrows, 1940

- Stochastic resonance
  - A weak periodic signal added to a non-linear system will emerge in the presence of a stochastic noise.



Systemic model

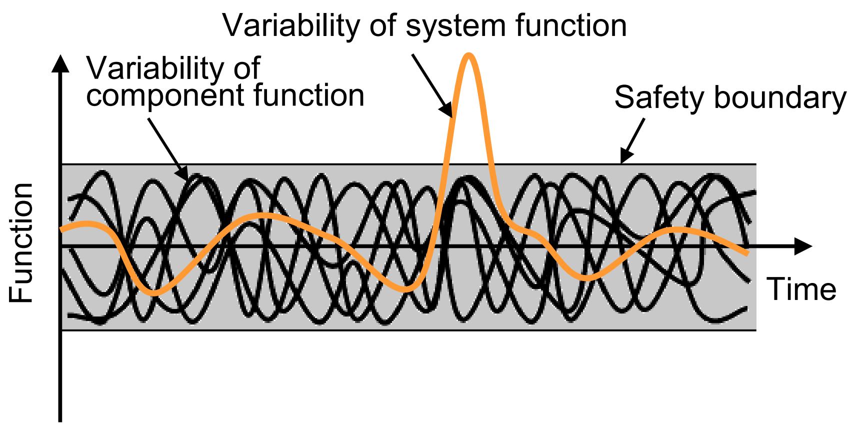
- Premise
  - The performance of system function fluctuates continuously.
- Causes
  - An unexpected combination (resonance) of performance variability causes an accident.
- Countermeasures
  - Monitoring and damping performance variability



Four principles of FRAM
Functional Resonance Accident Model

- Equivalence of success and failure
  - Success and failure derive from essential variability of system function. There are no difference between them.
- Approximate adjustment
  - Adjustment for damping performance variability must be incomplete and approximate due to resource limitations.
- Emergence
  - System behavior emerges from variability of non-linear system functions.
- Functional resonance
  - An accident occurs when variability of system function exceeds a safety limit due to functional resonance.

Functional Resonance Accident Model



What is resilience?

- Ecological resilience (Holling, 1973)
  - 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
- Seismic resilience (Bruneau, 2003)
  - 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

What is resilience?

- Economic resilience
  - The ability to escape from serious economic crises, or to recover from crises by mitigating the influence of external shocks
- Business resilience
  - The ability to respond and adapt quickly to internal or external disturbances of business opportunities, demands, confusions, and threats, to suppress their impacts, and to continue business operations

Resilience engineering

- Resilience from systemic view
  - 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.
- Resilience engineering
  - Design methodology of resilience
  - The objective of risk management is not reduction of risks, but enhancement of the ability to suppress system performance variability under changes, disturbances, and uncertainties.

Proactive risk management

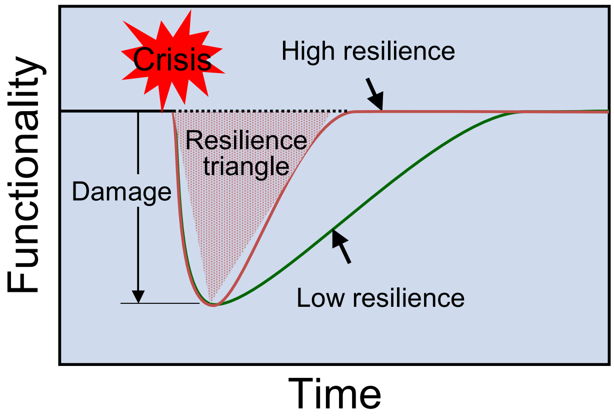
High Reliability Organization (HRO)

- Organization where accident occurring is suppressed below the standard level under severe conditions
  - Aircraft carrier, Air Traffic Control, Nuclear power plants, Emergency Rescue Center
- Vigorously studied around 1990 at UCB
- Features common in HRO
  - Mindfulness
  - Ability to manage unanticipated situations

Implementation process

- Anticipation
  - Get ready for long-term threats and changes
- Monitoring
  - Watch system states and find out clues of threats
- Responding
  - Take immediate actions to regulate function variability
- Learning
  - Learn from good as well as bad consequences

Resilience triangle (Bruneau,2003)



Assessment of resilience

- Key issue in assessing system resilience
  - Different people have different interests, valuations, needs, and so on; resilience is different for different stakeholders.
- Demonstration with recovery of lifeline after Tohoku Earthquake
  - Maslow's five-layered hierarchy of human needs
  - Persona method

Maslow's hierarchy of human needs

- Physiological
  - Freedom from hunger, thirst, sleepiness, fatigue, cold, etc.
- Safety
  - Protection against hazards, threats, fear, and uncertainty.
- Social
  - Desire to be liked by others, to belong to community, etc.
- Esteem
  - Desire to be accepted, respected, and valued by others.
- Self-actualization
  - Desire to become more and more what one is.

Decomposition of assessment measure

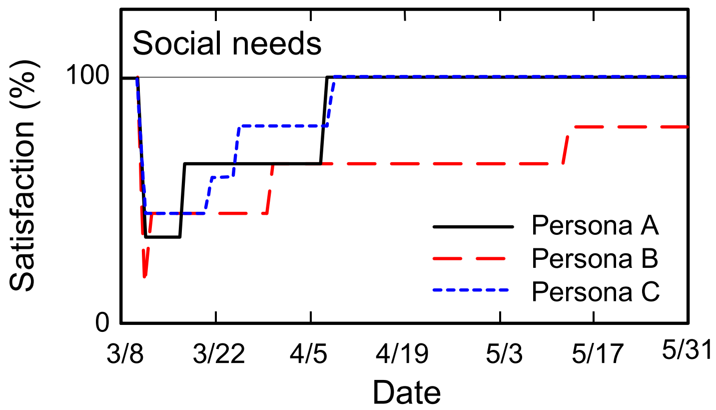
Level	Item	Basic data
Physiological	Water Food Dwelling Medical care	Water supply, water wagons Shops, distribution Home, refugee camps Hospitals
Safety	Electricity Water Gas Information	Electricity grid, generators Water supply Gas lines Internet, TVs, radios
Social	Privacy Job Relatives Property	Home or refugee camp Workplace, employer State of relatives House, cars

Assessment for different stakeholders

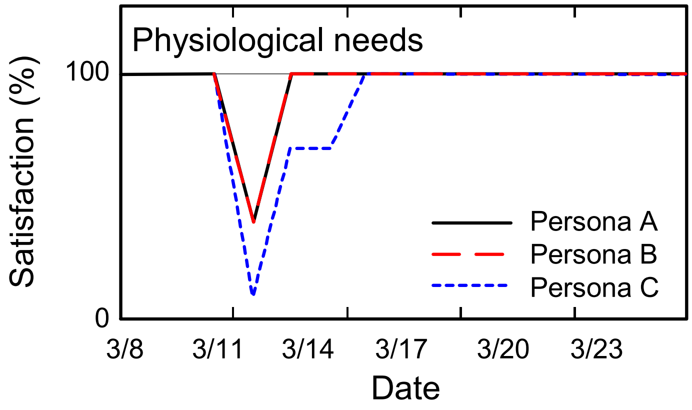
- Persona
  - Imaginary but very specific user model to be considered in designing products or services
  - Not an average user
- Characteristic three personas of earthquake sufferers
  - Based on opened notes of sufferers

【Persona B】
Age: 40s
Sex: male
Residence: Kesen-numa
Family: Wife and 2 sons
Health condition:
Good but blood pressure is a little high
Occupation:
Self-owned shop job

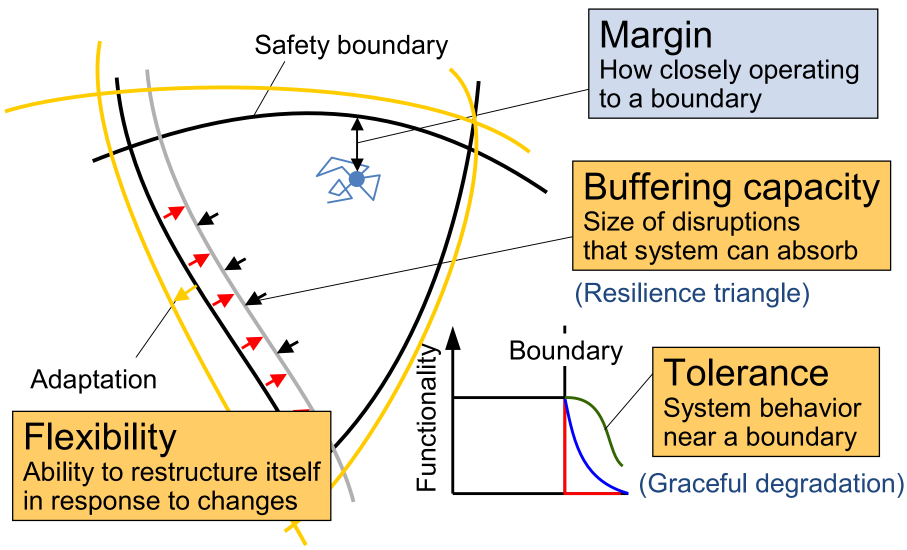
Resilience triangle of utilities after Tohoku Earthquake (2)



Resilience triangle of utilities after Tohoku Earthquake (1)



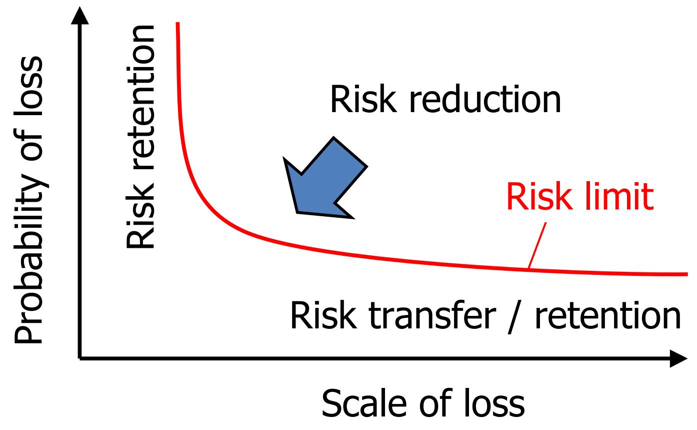
Essential characteristics of resilience



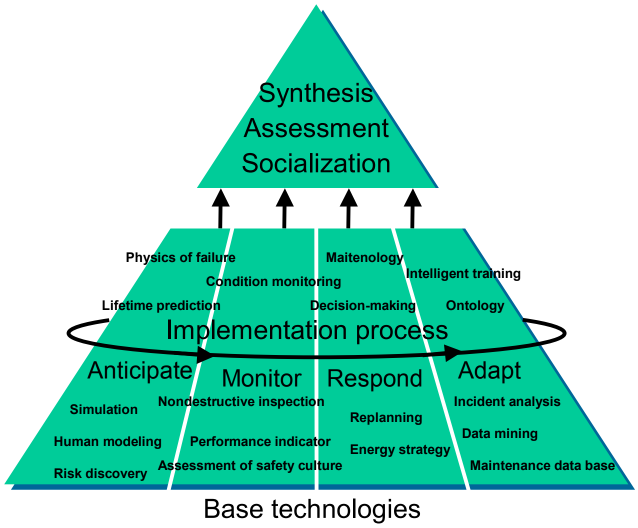
Premises in engineering design

- Systems are to be designed to satisfy specific design bases that are predefined.
- Situations beyond the design bases are not assumed. Functions beyond the design bases are not guaranteed.
- The probability that the system goes beyond the design bases is empirically predictable.
- Where to locate the design bases will not be determined by engineering but by economics and politics.

Safety based on probabilistic risk



Overview of resilience engineering



Super resilience

- Resilience is not restricted to system's response to crisis, but also includes adaptation to slow and long term changes.
  - Resolution of the 3E trilemma (sustainability)
  - Endless innovation under changing global business environment
- Society can get stronger and smarter than the pre-event level by restructuring itself from experience.

Super resilience

Summary

- The conventional approach for risk management does not work often in actual situations. New approaches based on a systemic viewpoint are desired.
- Resilience engineering is a promising idea that can give solution to the above problem based on a concept of complex systems or the systemic model of accident.