Systems Safety
— Introduction and Definitions —

Kazuo FURUTA (RERC)

RESILIENCE ENGINEERING
THE UNIVERSITY OF TOKYO

Dangers in our society (1)

- Natural disaster
  - Earthquake, storm, flooding, thunder, ・・・
- Facility accident
  - Accident, fire, explosion, air crash ・・・
- Occupational accident
  - Fall, electrification, crash, trapping, ・・・
- Health risk
  - Disease, pandemic, medical accident, ・・・
- Environmental destruction
  - Contamination, extinction, climate change, ・・・

Dangers in our society (1)

- Economic risk
  - Bankruptcy, market crash, scandal, ・・・
- Information risk
  - Cracking, internet leak, data alteration, ・・・
- Security risk
  - Crime, terrorism, riot, warfare, ・・・
- Social risk
  - Aging, bullying, uninterest in politics, ・・・

What is safety ?

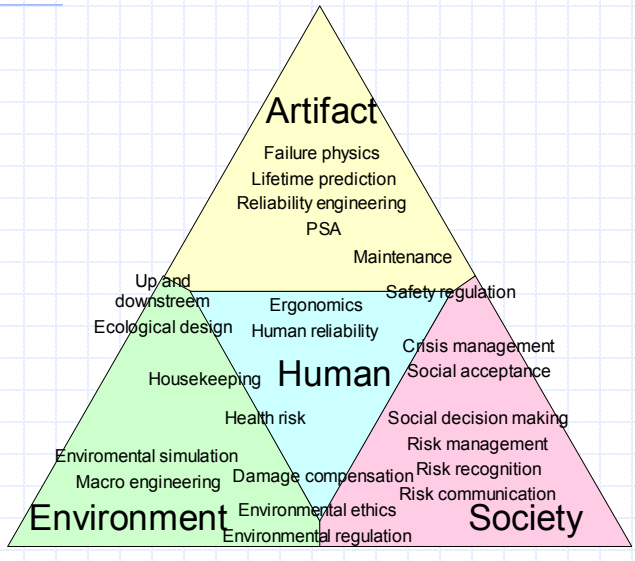
Safe : Protected from any danger or harm
Solid : Having no holes or spaces inside

- The state that the potential of harm to humans or damage to materials is kept below some allowable limit (JISZ8115)
- The state of being free from unallowable risk (JISC0508)

Safety studies

- Safety studies
  - Since safety depends on people's sense of valuation, it exceeds the scope of science, which should be value-free. The academic area therefore for teleological decision and proposition is to be called safety studies. (Yoichiro Murakami, 1998)
- Safety engineering
  - Metaphysical engineering on theories and methodologies for practical management of safety that have developed in separate domains of engineering

Perspective of safety



Hazard and risk

- Hazard
  - An act or phenomena that has the potential to produce harm or other undesirable consequences to humans or what they value. (USNRC, 1996)
- Risk
  - A concept used to give meaning to things, forces, or circumstances that pose danger to people or to what they value. Descriptions of risk are typically stated in terms of the likelihood of harm or loss from a hazard. (USNRC, 1996)

Examples of hazard

- Matters and objects
  - Chemicals, pressurized gas, beasts, cars, water, humans, ・・・
- Human activities
  - Warfare, street crossing, playing sports, taking a bath, sleeping, ・・・
- Phenomena
  - Earthquake, meteorological phenomena, combustion, disease, economic cycle, ・・・

※ Nothing exists that cannot be a hazard.

Different concept of risk

- The unexpected variability or volatility of returns (Finance)
- Root cause events such as accidents and disasters that make harm to the life or health of people (Sociology)
- Combination of the probability of event occurring and the scale of its consequent losses (Technology)

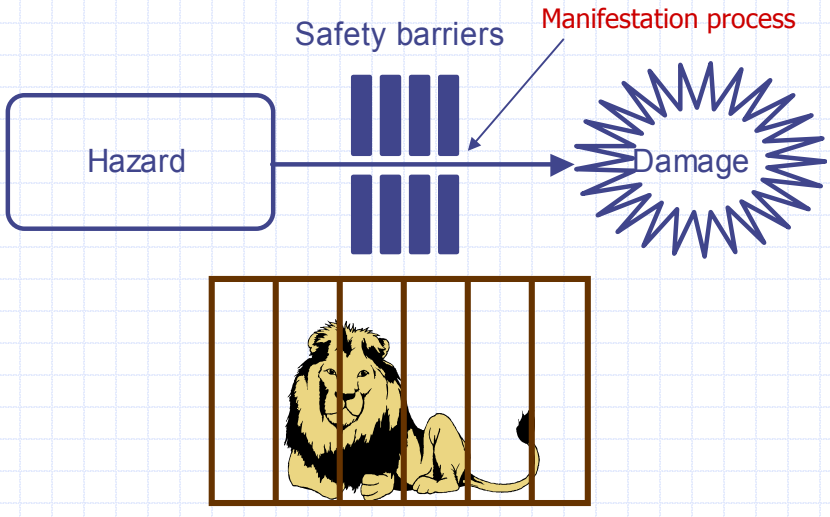
Safety in this lecture

- Safety depends heavily on what people value.
- In this lecture, we will focus just on a technological aspect of safety that is determined based on the technological concept of risk.

Usefulness of technological concept of risk

- Safety cannot be free from uncertainty, because it is related to what may happen in the future.
- Some quantitative measure is essential for making a clear decision for maintaining safety.
- A concept of risk that is defined as a combination of the probability of event occurring and the scale of consequent losses is useful, as far as specialists use it for risk management.
- Social consensus is required, however, to define risk, since it depends of what people value.

Safety barrier



Various safety barriers (1)

- Physical barrier
  - Physically prevent an unsafe actions or phenomena from initiating or progressing
    - Fence, firewall, facility site, containment, key, ···
- Functional barrier
  - Actively intervene the process of unsafe actions or phenomena to stop them
    - Fire alarm, brakes, password protection, ···

Various safety barriers (2)

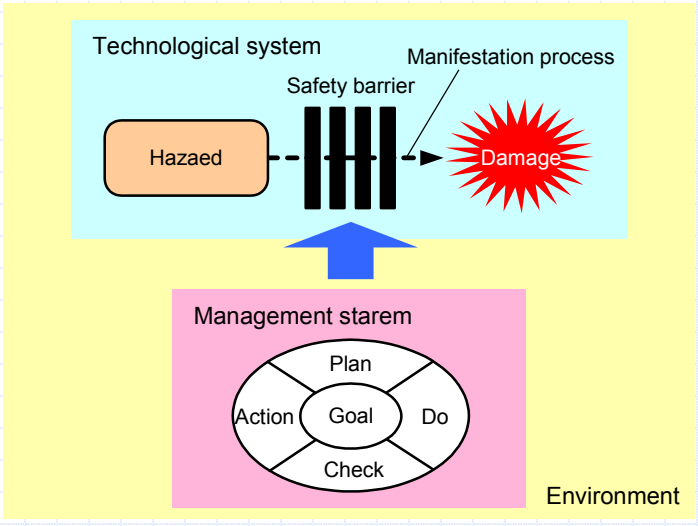
- Symbolic barrier
  - Prohibit unsafe actions by presenting some physical symbols to people
    - Sign, traffic lights, guard rail, ···
- Conceptual (non-physical) barrier
  - Prohibit unsafe actions by the conceptual meaning or knowledge
    - Law, rule, restriction, procedure, training, ···

Importance of management system

- Physical, functional, and symbolic barriers work only if they are properly designed, implemented, and maintained.
  - Although a tall fence is installed around a house but left broken, it does not work for security.
- Design, implementation, and maintenance of these barriers are performed by human activities.

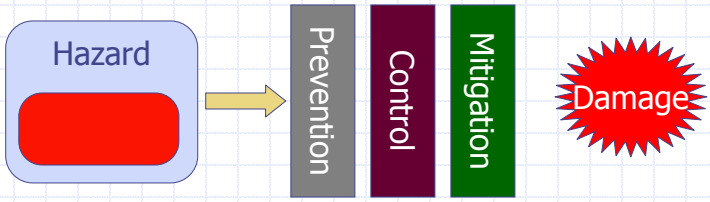
➔ Management system

Technological system and management system



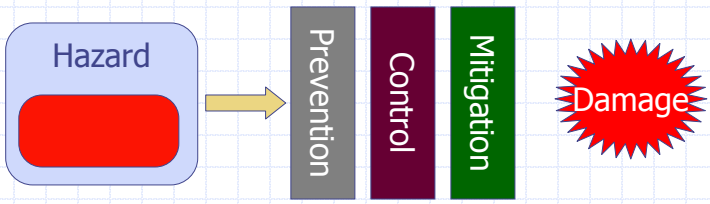
Defense in depth principle

- Practically used in industries with high potential risks
- Assurance of safety by implementing multiple safety barriers
- Conservative approach by neglecting preceding barriers



Depth of safety barriers

- Prevention of abnormal operation and failure
- Control of abnormal condition to avoid progression to an accident
- Mitigation of the consequence of an accident



Texts

安全学入門

古田一雄・長崎晋也
日科技連

http://www.cse.sys.t.u-tokyo.ac.jp/furuta/teaching/safety/index.html