Systems Safety
— Hazard Identification —

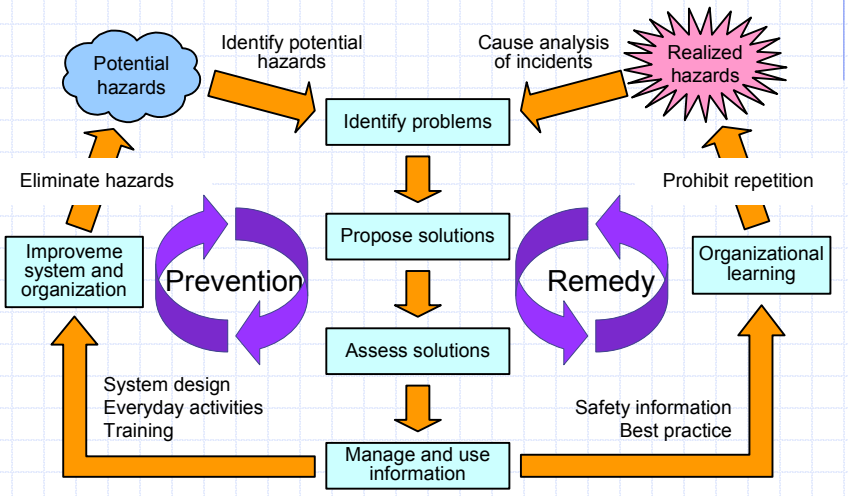
Kazuo FURUTA (RERC)

RESILIENCE ENGINEERING
THE UNIVERSITY OF TOKYO

Risk assessment methods (1)

- Preventive methods
  - Hazards and their impacts are analyzed before the system is put into use to prevent accidents and troubles by installing countermeasures beforehand.
- Remedial methods
  - Causes of accidents and troubles are analyzed after their occurrence to prohibit repetition of similar events.

Prevention and remedy



Yoshimura, 2002

Risk assessment methods (2)

- Qualitative/Quantitative methods
  - Quantitative methods can clearly show the results, but qualitative methods can provide information necessary for proposing countermeasures.
  - In addition, one should not forget that there are implicit assumptions behind the numbers obtained.
- Deterministic/Probabilistic methods
  - Probabilistic methods are required to deal with uncertainties and incompleteness in knowledge, but deterministic methods are useful to be used in practice.

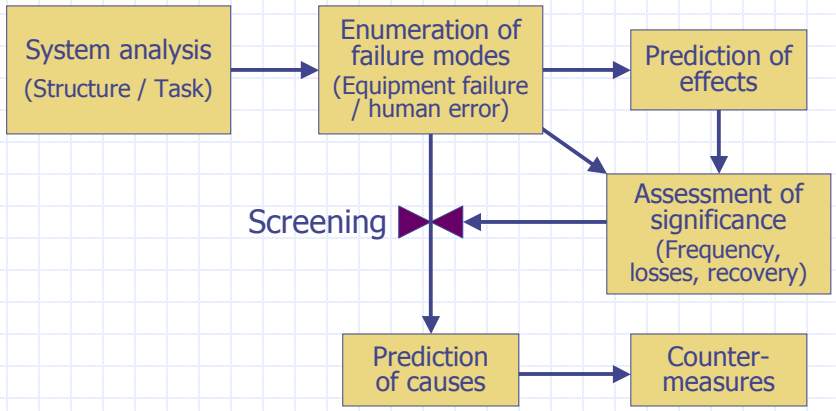
Procedure of risk assessment

1. Definition of objectives, system, and losses
2. Identification of hazards
   what-if analysis, FMEA, HAZOP, ···
3. System modeling
   ETA, FTA, GO, GO-FLOW, DFM, ···
4. Quantification of risks
5. Sensitivity and uncertainty analysis
6. Documentation of results

Failure Mode & Effects Analysis

- Systematic technique for enumerating potential failure modes, assessing their effects on the whole system, and then identifying primary hazards in a bottom up manner
- Developed in 1950s for military industry
- Applicable both to equipment failures and human errors

Procedure of FEMA



FMEA worksheet

Component	Failure mode	Effect	Signifi-cance	Cause	Counter-measure
Coolant pump	Trip	System shutdown	5	Loss of power	Backup power
Manual startup	Delayed start	Delayed production	3	Lack of skill	Training

- Component
  - Decompose technological systems or human tasks into unitary components following the hierarchical structure and enumerate all components

FMEA worksheet

Component	Failure mode	Effect	Signifi-cance	Cause	Counter-measure
Coolant pump	Trip	System shutdown	5	Loss of power	Backup power
Manual startup	Delayed start	Delayed production	3	Lack of skill	Training

- Failure mode
  - Enumerate failure modes (equipment failures or human errors) that probably occur in each hardware component or task

FMEA worksheet

Component	Failure mode	Effect	Signifi-cance	Cause	Counter-measure
Coolant pump	Trip	System shutdown	5	Loss of power	Backup power
Manual startup	Delayed start	Delayed production	3	Lack of skill	Training

- Effect
  - Predict what effects will propagate to the upper systems and finally to the whole system for each failure mode
  - Unnecessary to consider multiple failures

FMEA worksheet

Component	Failure mode	Effect	Signifi-cance	Cause	Counter-measure
Coolant pump	Trip	System shutdown	5	Loss of power	Backup power
Manual startup	Delayed start	Delayed production	3	Lack of skill	Training

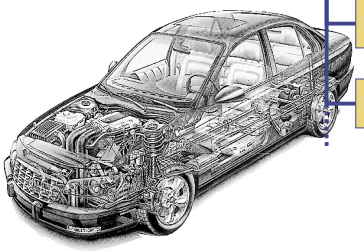
- Significance
  - Assess the significance of failure for each failure mode semi-quantitatively considering some indicators like event frequency, severity of effects, and possibility of recovery

FMEA worksheet

Component	Failure mode	Effect	Signifi-canse	Cause	Counter-measure
Coolant pump	Trip	System shutdown	5	Loss of power	Backup power
Manual startup	Delayed start	Delayed production	3	Lack of skill	Training

- Cause and countermeasure
  - Describe possible cause and then countermeasure to prevent, control, or mitigate failure or its effects

Part-whole hierarchy of technological system

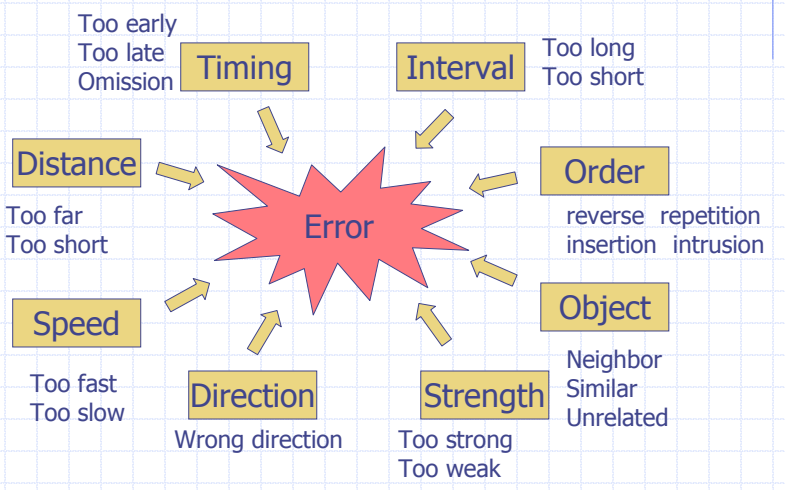


Goal-mean hierarchy of task

Failure modes

- Possible failure modes of equipment can be predicted from the past records of similar equipment.
- Mechanical parts
  - Deformation
  - Break, rupture
  - Wear
  - Erosion, corrosion
  - Sticking
  - Leak
  - Slack, displacement
  - Vibration
- Electrical parts
  - Break, open circuit
  - Short circuit
  - Insufficient insulation
  - No / low outputs
  - Drift
  - Overheat

Error modes (Basic phenotypes)



E.Hollnagel, 1993

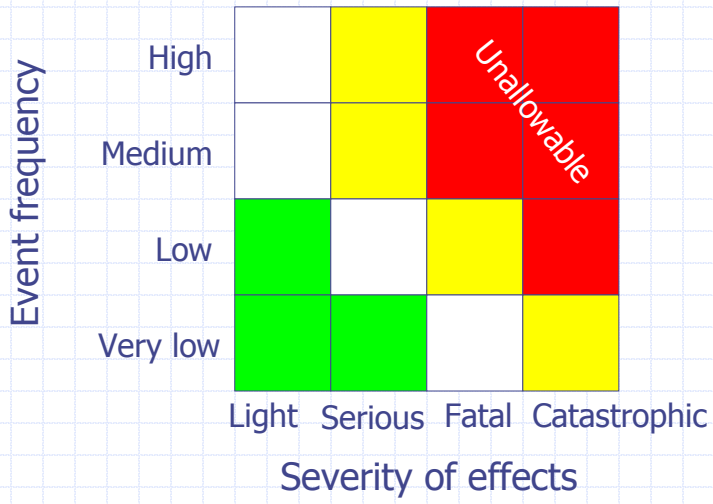
Criteria for event frequency

- Very low
  - Event occurring is negligible during system lifetime.
- Low
  - Event occurring is improbable but possible during system lifetime.
- Medium
  - The event will probably occur a few times during system lifetime.
- High
  - The event will repeat during system operation.

Criteria for consequence severity

- Light
  - System operation is unaffected and fast recovery is possible.
- Serious
  - System operation is disturbed but easily recovered.
- Fatal
  - System shutdown is inevitable and it takes a long time to recover.
- Catastrophic
  - Damages spread beyond the system boundary and recovery is very difficult.

Comprehensive assessment of significance (Risk matrix)



Guide to consider countermeasures

- Prevention
  - Eliminate problematic components
  - Eliminate causation factors of failure
- Control
  - Eliminate propagation paths of failure effects
  - Detect failure and suppress failure effects actively
- Mitigation
  - Suppress consequence of disaster
  - Consider recovery plan

Hazard & Operability Analysis

- While FMEA focuses on system components and their failure modes, HAZOP focuses on process parameters and their deviations.
- Guidewords are prepared for parameters, deviations, and causes to help analysts.
- Developed in 1960s for chemical industry

HAZOP worksheet

Parameter	Deviation	Effect	Signifi-canse	Cause	Counter-measure
Intake flow	No flow	Process shutdown	4	Choke of slag	Install filter
	Decreased flow	Low output	3	Malfunction of valve	Periodical test

- Parameter
  - Enumerate process parameters that determine the state of system such as flow rate, pressure, temperature, and so on

HAZOP worksheet

Parameter	Deviation	Effect	Signifi-canse	Cause	Counter-measure
Intake flow	No flow	Process shutdown	4	Choke of slag	Install filter
	Decreased flow	Low output	3	Malfunction of valve	Periodical test

- Deviation
  - Enumerate the ways how each parameter will deviate from its normative state

Guidewords

- Exhaustive combination of parameters, deviations, and causes
- Customization for a specific domain required

- Flow rate
  - Too high
    - Excessive pumping power
    - Increase of intake pressure
    - Increase of fluid density
    - ……
  - Too low
  - No flow
  - Reversal flow
- Temperature
  - Too high
    - Change of ambient temp.
    - Malfunction of heat exchanger
    - Fire
    - ……
  - Too low
    - Change of ambient temp.
    - Decreased pressure
    - ……