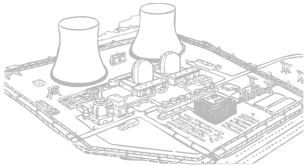
RISK ENGINEERING



# Designing for safety

Eric Marsden

<eric.marsden@risk-engineering.org>

# System safety

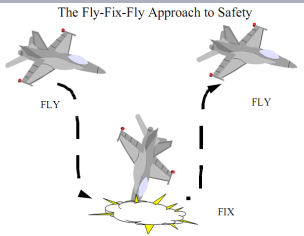
- The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle
- A planned, disciplined and systematic approach to preventing or reducing accidents throughout the lifecycle of a system
- Primary concern is the management of risks:
  - risk identification, evaluation, elimination & control
  - through analysis, design & management

*"A clever person is one who finds a way out of an unpleasant situation into which a wise person would never have got themselves."*

Quote from *Memoirs of a fortunate jew*, D. A. Segre, Grafton Books, 1988.

RISK ENGINEERING

# History of system safety




- ▷ Arose in the 1950s after dissatisfaction with the fly-fix-fly approach to safety
  - early development in US Air Force
  - led to MIL-STD-882 *Standard Practice for System Safety* (v1 1960s)
- ▷ Rather than assigning a safety engineer to demonstrate that a design is safe, integrate safety considerations from the design phase

# Aside: moving from retrofitted fire escapes to a fire code

- Between around 1850 and 1930, large fires killed many people in New York City
- 1867: the Tenement House Act required tenements (medium-rise high-density housing) to have fire escapes
  - fire escapes became an iconic architectural feature of NYC
- Building codes evolved progressively to make buildings safer
  - use non-flammable materials
  - fire-proof stairwells
  - interior fire-proof partitions
  - fire alarms and emergency exits
  - sprinkler systems in higher-risk buildings
- Integrating safety in the design stage is more effective than bolting it on later

RISK ENGINEERING

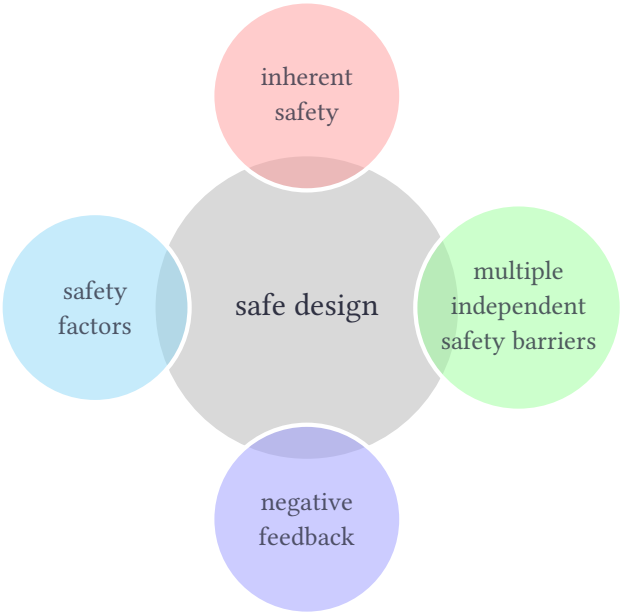
## Founding principles

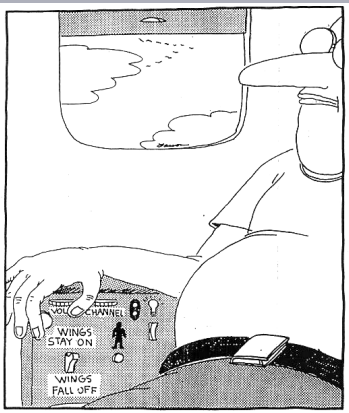
- Safety should be **designed in**
  - Critical reviews of the system design identify hazards that can be controlled by modifying the design
  - Modifications are most readily accepted during the early stages of design, development, and test
  - Previous design deficiencies can be corrected to prevent their recurrence
- Inherent safety requires both **engineering** and **management** techniques to control the hazards of a system
  - A safety program must be planned and implemented such that safety analyses are integrated with other factors that impact management decisions

## Founding principles

- ▷ Safety requirements must be **consistent** with other program or design requirements
  - The evolution of a system design is a series of tradeoffs among competing disciplines to optimize relative contributions
  - Safety competes with other disciplines; it does not override them

# Safe design: main principles




Fumbling for his recline button,
Ted unwittingly instigates a disaster.

RISK ENGINEERING

# Inherently safe design

- **Inherent**: belonging to the very nature of the person/thing (inseparable)
- Recommended first step in safety engineering
- Change the process to eliminate hazards, rather than accepting the hazards and developing add-on features to control them
  - unlike engineered features, inherent safety cannot be compromised
- Minimize inherent dangers as far as possible
  - potential hazards are excluded rather than just enclosed or managed
  - replace dangerous substances or reactions by less dangerous ones (instead of encapsulating the process)
  - use fireproof materials instead of flammable ones (better than using flammable materials but keeping temperatures low)
  - perform reactions at low temperatures & pressures instead of building resistant vessels

*"What you don't have, can't leak."*
*-- Trevor Kletz*

# Inherently safe design


THE MOMENT THE COMPUTERS CONTROLLING OUR NUCLEAR ARSENALS BECAME SENTIENT

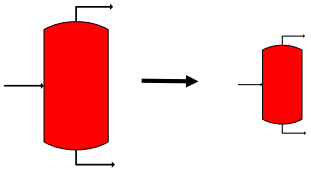
Image source: xkcd.com/1626/, CC BY-NC licence

RISK ENGINEERING

# Inherently safe design

Four main methods:

1. **Minimize**: reducing the amount of hazardous material present at any one time



2. **Substitute**: replacing one material with a less hazardous one
   - Example: cleaning with water and detergent rather than a flammable solvent

3. **Moderate**: reducing the strength of an effect
   - Example: having a cold liquid instead of a gas at high pressure
   - Example: using material in a dilute rather than concentrated form

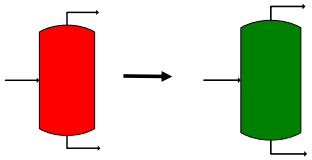
4. **Simplify**: designing out problems rather than adding additional equipment or features to deal with them

RISK ENGINEERING

# Inherently safe design

Four main methods:

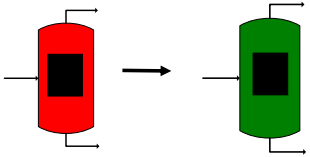
1. **Minimize**: reducing the amount of hazardous material present at any one time
2. **Substitute**: replacing one material with a less hazardous one
   - Example: cleaning with water and detergent rather than a flammable solvent
3. **Moderate**: reducing the strength of an effect
   - Example: having a cold liquid instead of a gas at high pressure
   - Example: using material in a dilute rather than concentrated form
4. **Simplify**: designing out problems rather than adding additional equipment or features to deal with them



# Inherently safe design

Four main methods:

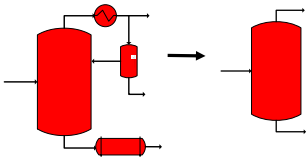
1. **Minimize**: reducing the amount of hazardous material present at any one time
2. **Substitute**: replacing one material with a less hazardous one
   - Example: cleaning with water and detergent rather than a flammable solvent
3. **Moderate**: reducing the strength of an effect
   - Example: having a cold liquid instead of a gas at high pressure
   - Example: using material in a dilute rather than concentrated form
4. **Simplify**: designing out problems rather than adding additional equipment or features to deal with them



# Inherently safe design

Four main methods:

1. **Minimize**: reducing the amount of hazardous material present at any one time
2. **Substitute**: replacing one material with a less hazardous one
   - Example: cleaning with water and detergent rather than a flammable solvent
3. **Moderate**: reducing the strength of an effect
   - Example: having a cold liquid instead of a gas at high pressure
   - Example: using material in a dilute rather than concentrated form
4. **Simplify**: designing out problems rather than adding additional equipment or features to deal with them



RISK ENGINEERING

# Inherently safe design

Two further principles are sometimes cited:

- **error tolerance**: equipment and processes can be designed to be capable of withstanding possible faults or deviations from design
  - example: making piping and joints capable of withstanding the maximum possible pressure if outlets are closed
- **limit effects**: designing and locating equipment so that the worst possible condition gives less danger
  - example: bungalows located away from process areas
  - example: gravity will take a leak to a safe place
  - example: bunds contain leakage

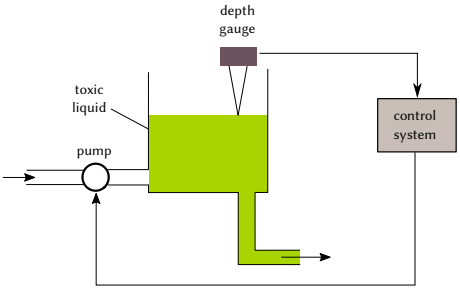
# Related CSB safety video


US CSB safety video *Inherently Safer: The Future of Risk Reduction*, July 2012

Watch the video: `youtu.be/h4ZgvD4FjJ8`

# Example of risk reduction: storage tank

- A storage tank feeds liquid to a chemical process
- Process requires liquid to be supplied at variable pressure
  - achieved by controlling height of liquid within the tank
- A depth sensor measures height of liquid and control system tells pump to move the liquid into tank



# Example of risk reduction: storage tank

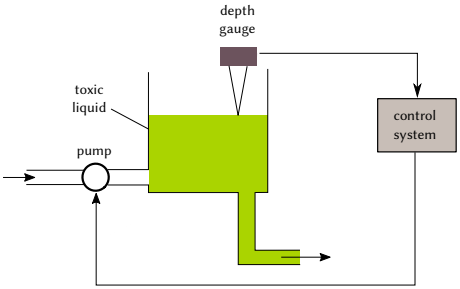
**Hazard**: the toxicity of the liquid.

**Hazardous event** (top event that we wish to prevent): spillage of the toxic liquid.

Possible causes of the hazardous event:

- ▷ depth sensor fails
- ▷ control system fails
- ▷ pump malfunctions (pumps when told to stop)
- ▷ storage tank leaks (corrosion…)

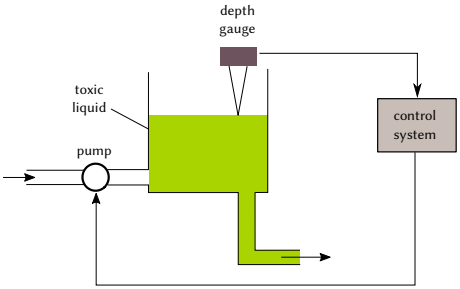
**Question**: how can we reduce the risk of the hazardous event?



# Example of risk reduction: storage tank

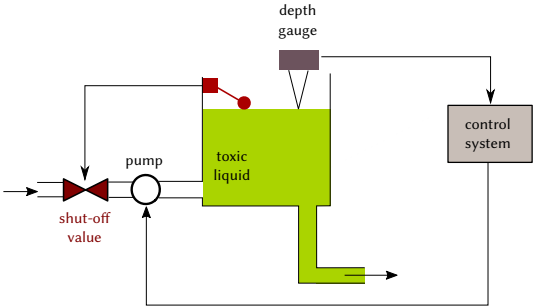
Apply **inherent safety principles**:

- we can **minimize** the impact of the hazardous event by making the tank as small as possible to supply the downstream process
- we may be able to **substitute** a less toxic liquid



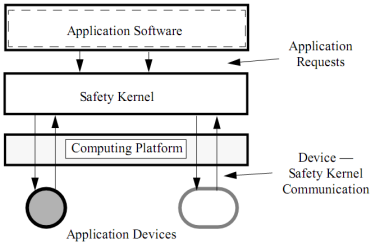
# Example of risk reduction: storage tank

- Use an independent **non-programmable element** to provide additional safety
  - float switch connected to shut-off valve
- What is achieved:
  - even if the depth sensor fails, the tank will not overfill
  - even if the controller erroneously sends safety-violating command to the pump, the tank will not overfill
  - even if the pump continues pumping despite being told to stop, the tank will not overfill
  - the safety-critical area is reduced to float switch and shut-off valve (simple elements)

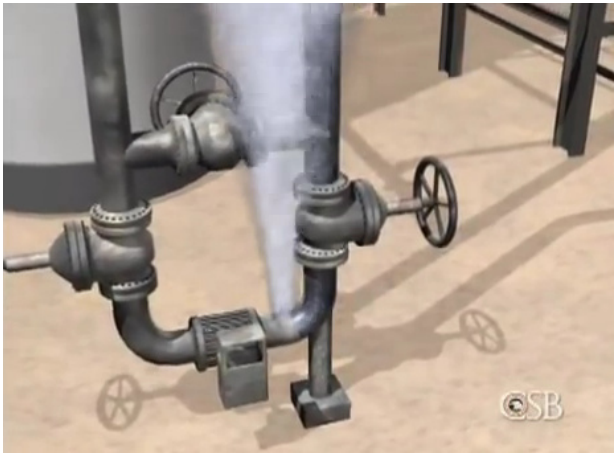


# “Minimize”: the safety kernel concept

- A *safety kernel* is a simple arrangement (*e.g.* combination of hardware and software) that implements a critical set of operations
- Kernel is small and simple so more effort can be applied to verify its trustworthiness
  - is sometimes protected by special hardware techniques
  - decoupled from complexity in other parts of the system
- Similar concept for security: the *trusted computing base*



# Related CSB safety video




US CSB safety video *Fire From Ice*, July 2008

Watch the video: youtu.be/3QKpVnTqngc

# Examples of substitution

- Use bleach in the process (where possible) instead of chlorine gas
- Use simple hardware devices instead of a software-intensive computer system
- Electronic temperature measurement instead of thermometers based on level of mercury
- Reduce dust hazard by using less fine particles, or by treating product in a slurry instead of a powder
- Use an inert gas such as nitrogen instead of an air mixture, to reduce explosion hazards
- The "substitution principle" is part of the EC's REACH regulation and of the Biocidal Products Regulation
  - substitution of harmful chemicals with safer alternatives

ECHA
EUROPEAN CHEMICALS AGENCY

RISK ENGINEERING

# Examples of moderation

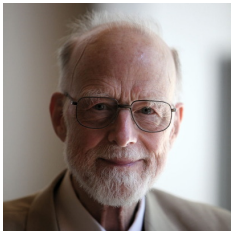
- Reduce mass flowrates to lessen pressure on piping
- Reduce quantities of hazardous materials stored on site
  - and amounts requiring transport by road or rail
- Miniaturize process reactors
- Use proven technology and processes
  - introducing new technology introduces new unknowns, as well as “unknown unknowns”

# Simplification: principles

- A simple design minimizes
  - number of parts
  - functional modes
  - number and complexity of interfaces
- A simple system has a small number of unknowns in the interactions within the system and with its environment
- A system is intellectually unmanageable when the level of interactions reaches a point where they cannot be thoroughly planned, understood, anticipated, guarded against
- “System accidents” occur when systems become intellectually unmanageable

RISK ENGINEERING

# Simplification: principles



> *I conclude that there are two ways of constructing a software design: One way is to make it so simple that there are obviously no deficiencies and the other way is to make it so complicated that there are no obvious deficiencies.*
>
> – C. A. R. Hoare

Emeritus Professor of Computer Science, Cambridge University

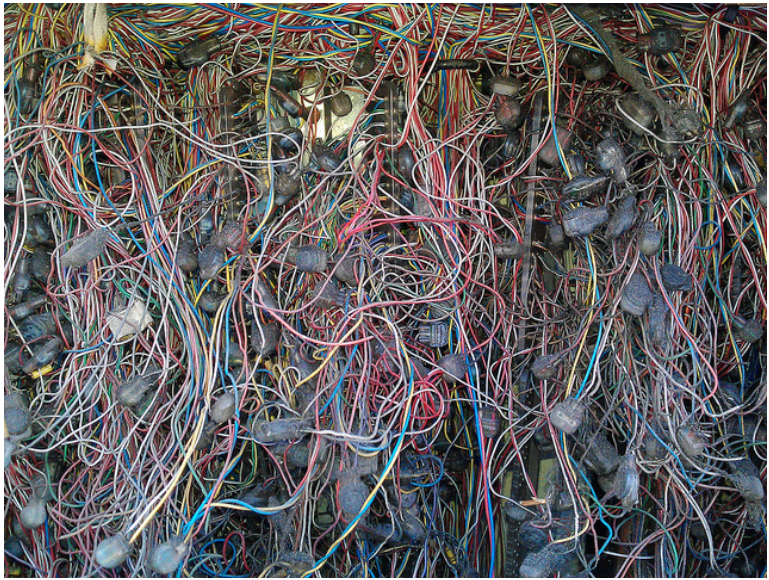
ACM Turing Award, 1980

Image source: Rama via Wikimedia Commons, CC BY-SA licence

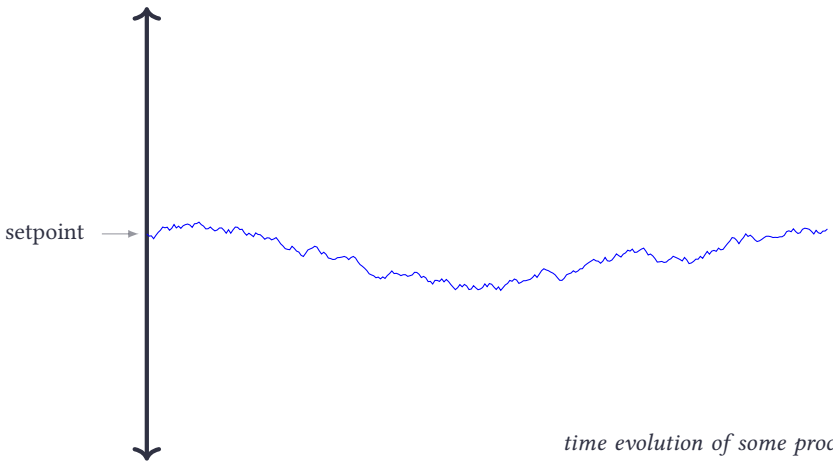
RISK ENGINEERING

# Counter-examples of simplification

# Counter-examples of simplification

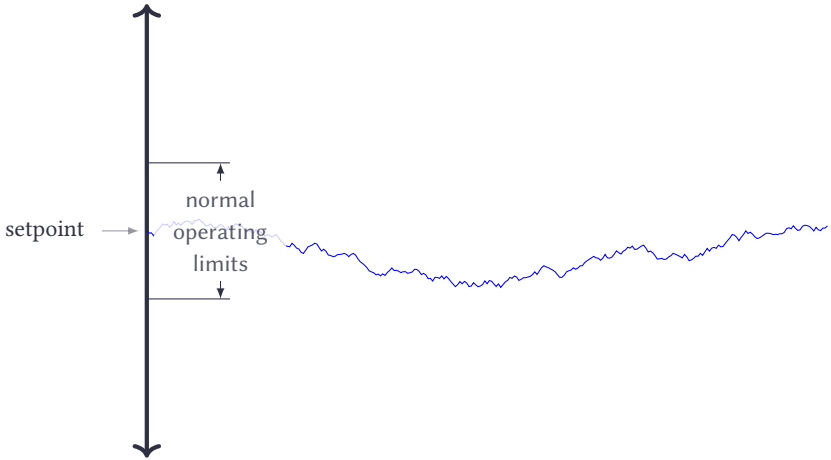


# Principle: tolerate errors

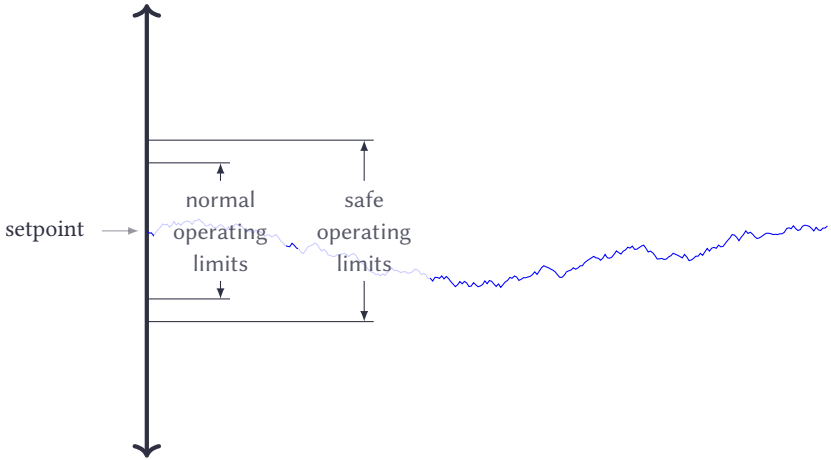



*time evolution of some process parameter (temperature, pressure)*

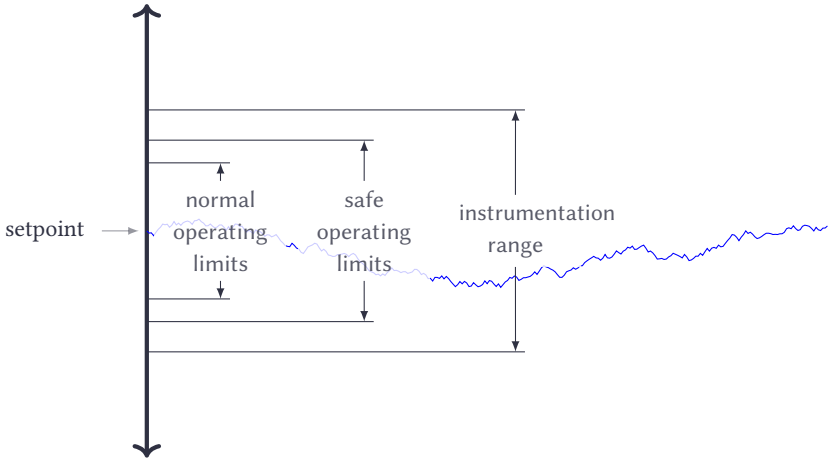
# Principle: tolerate errors



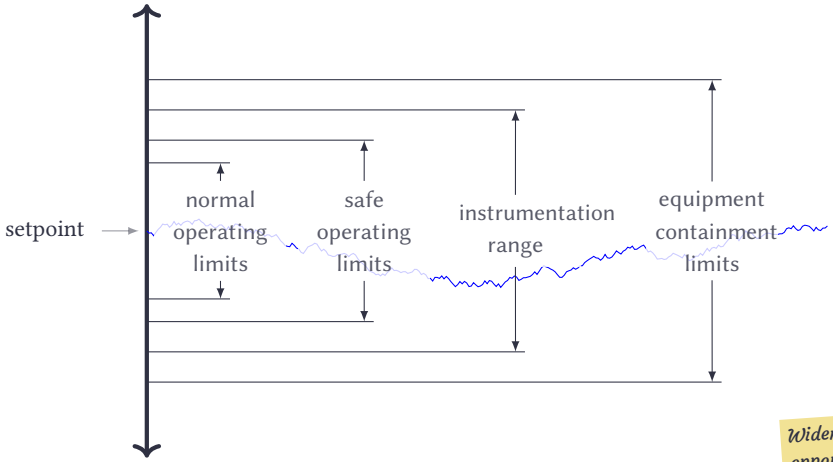
# Principle: tolerate errors



# Principle: tolerate errors



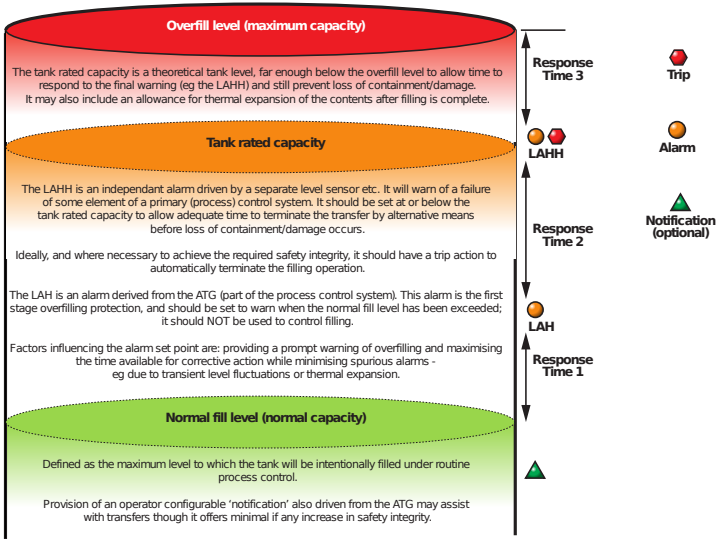
# Principle: tolerate errors




*Wider operating limits → more opportunity for recovery before accident: inherently safer*

RISK ENGINEERING

# Illustration: overfill alarms in fuel tanks




Source: UK HSE report *Safety and environmental standards for fuel storage sites*, 2009

# Illustration of inherent safety principles at Bhopal

- **Elimination**: MIC (methyl isocyanate) would not have been produced if an alternative process route was used to produce the same chemical
- **Minimization**: such a large storage of MIC was unnecessary
  - different reactor design would have cut the inventory of MIC to a few kilograms in the reactor, with no intermediate storage of many tonnes required
- **Substitution**: an alternative route involving phosgene as an intermediate could have been used
- **Attenuation**: MIC could have been stored under refrigerated condition
- **Simplification**: a simpler piping system would have alerted the maintenance crew of necessary action

# Safe design precedence

start here!

## Hazard elimination

- substitution
- simplification
- decoupling
- elimination of human errors
- reduction of hazardous materials or conditions

## Hazard reduction

- design for observability and controllability
- barriers (lockins, lockouts, interlocks)
- failure minimization
- safety factors and margins
- redundancy

## Hazard control

- reducing exposure
- isolation and containment
- fail-safe design

## Damage reduction

- protective barriers

inherently safe systems

probabilistically safe systems

RISK ENGINEERING

# Inherent safety: difficulties

A knife cuts...

# Inherent safety: difficulties


Most medicines
are toxic...



RISK ENGINEERING

# Inherent safety: difficulties


Gasoline is able to store large quantities of energy in a compact form (= very hazardous)...

*Sometimes the very properties for which an object is built are those that make it hazardous...*

RISK ENGINEERING

# Inherent safety: tradeoffs

- CFCs have low toxicity, not flammable, but cause environmental impacts
  - are alternatives propane (flammable) or ammonia (flammable & toxic) inherently safer?
- Increasing the burst-pressure to working-pressure ratio of a tank
  - increases reliability
  - reduces safety (new hazards: tank explosion, new chemical reactions possible at higher pressures)

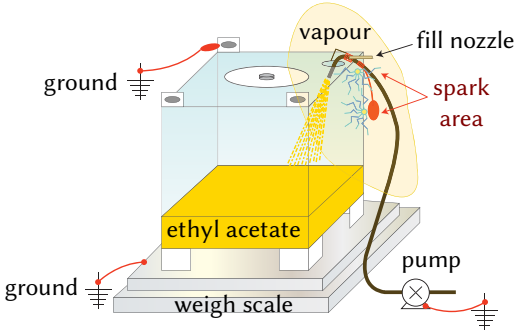
# Passive vs. active protection

- *Passive* safeguards maintain safety by their presence and fail into safe states
- *Active* safeguards require hazard or condition to be detected and corrected
- Tradeoffs:
  - passive methods rely on physical principles
  - active methods depend on less reliable detection and recovery mechanisms
  - passive methods tend to be more restrictive in terms of design freedom
    - not always feasible to implement

# Passive protection: examples

- Permanent grounding and bonding via continuous metal equipment and pipe rather than with removable cables
- Designing high pressure equipment to contain overpressure hazards such as internal deflagration
- Containing hazardous inventories with a dike that has a bottom sloped to a remote impounding area, which is designed to minimize surface area
- Pebble-bed nuclear reactors use “pebbles” of uranium encased in graphite to moderate the reaction: the more heat produced, the more the pebbles expand, causing the reaction to slow down

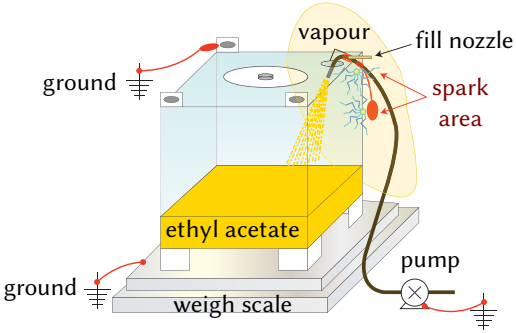
# Passive protection example: filling a tank



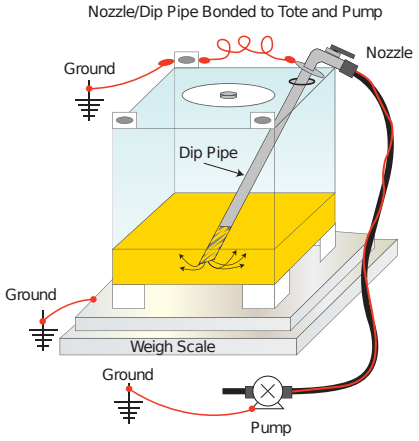

Hazard: ignition of flammable liquid during filling, due to static electricity

Source: *CCPS Process Beacon*, January 2009

# Passive protection example: filling a tank




Hazard: ignition of flammable liquid during filling, due to static electricity



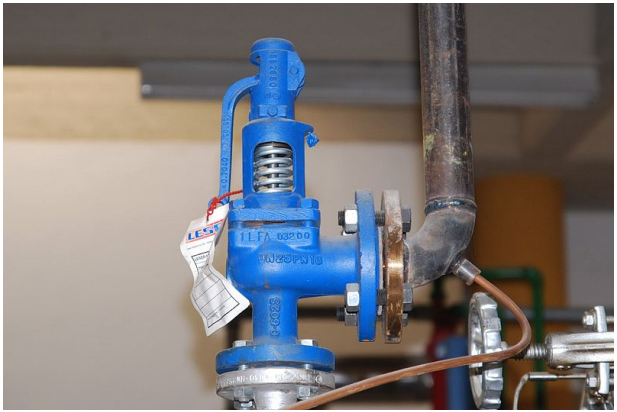

Non-splash filling solution eliminates the hazard

Source: *CCPS Process Beacon*, January 2009

# Active protection mechanisms

- **Active** design solutions require devices to monitor a process variable and function to mitigate a hazard
- Active solutions generally involve a considerable maintenance and procedural component and are therefore typically less reliable than inherently safer or passive solutions
- To achieve necessary reliability, **redundancy** is often used to eliminate conflict between production and safety requirements (such as having to shut down a unit to maintain a relief valve)
- Active solutions are sometimes referred to as *engineering controls*

# Active protection example: safety valve




Safety valve prevents overpressure in a vessel or pipe

Depicted: standard steam boiler safety valve (DN25)

Image source: SV1XV, Wikimedia Commons, CC BY-SA licence

# Active protection example: rupture disk


Rupture disk prevents overpressure in a vessel or pipe

# Active protection example: interlock


Interlocking device to prevent incompatible positions of various switches

Similarly, household microwave ovens have an interlock that disables magnetron if door is open

Image source: Wikimedia Commons, author Audriusa, CC BY-SA licence

RISK ENGINEERING

# A non-standard interlock

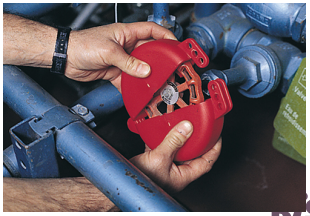

Image source: `@FailsWork` Twitter feed



RISK ENGINEERING

# Active protection example: lockout mechanisms

- Lockout-tagout or lock-and-tag mechanisms ensure equipment cannot be started while maintenance is underway
- Each worker places a lock on the “power” switch for the equipment before intervening on it plus tag with their name
- If another worker arrives to work on same equipment, also puts his lock+tag on same switch
- Power can only be reestablished when all workers have reclaimed their lock
- Essential safety procedure for variety of electrical, mechanical, pneumatic equipment

# Lockout-tagout video by Napo


Watch video: youtu.be/G2ERlrWAmAE

The Napo safety video series, napofilm.net/en/ (EU-OSHA)

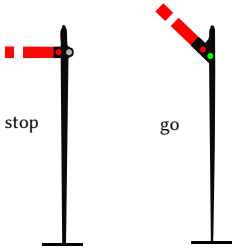
# Lockout-tagout video by SafeQuarry


Watch video: youtu.be/wnFDQSC36Q4

## Fail-safe principle

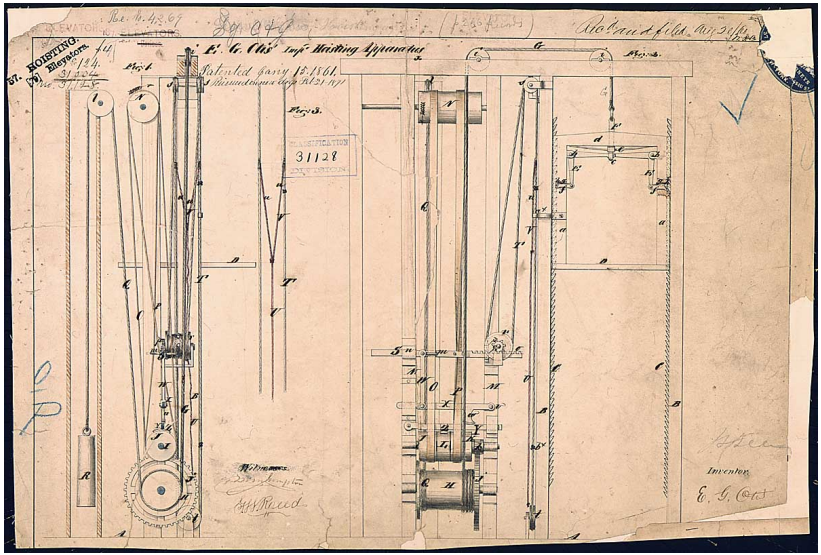
- A system is *fail-safe* if it remains or moves into a **safe state** in case of failure
- Examples:
  - train brakes require energy to be released
  - control rods in a nuclear reactor are suspended by electromagnets; power failure leads to “scramming”
  - traffic light controllers use a *conflict monitor unit* to detect faults or conflicting signals and switch an intersection to a flashing error signal, rather than displaying potentially dangerous conflicting signals

# Illustration: railroad semaphores




- Railroad semaphores are designed so that the vertical position indicates stop/danger
- If the controlling mechanism fails, gravity pulls the arm down to the “stop” position

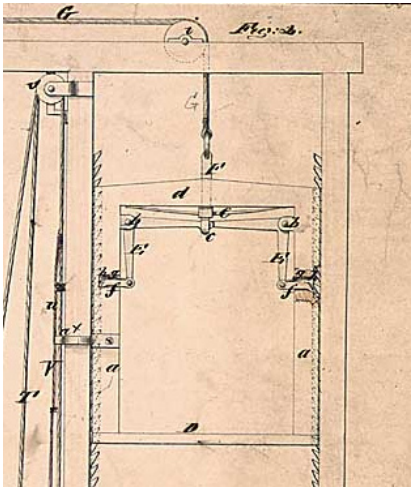
# Illustration: elevator brakes




Source: Elisha Otis's elevator patent drawing, 1861 (via Wikipedia), public domain

RISK ENGINEERING

# Illustration: elevator brakes

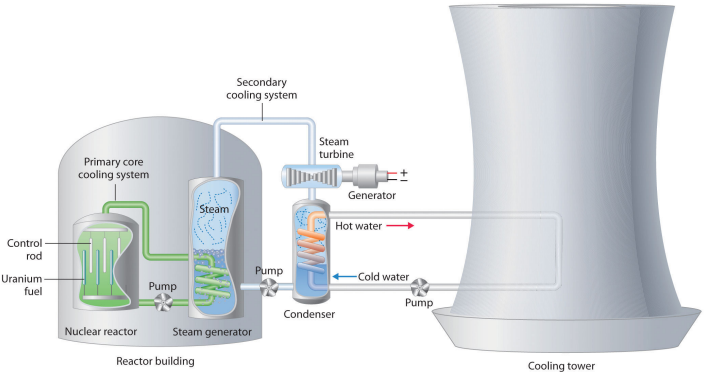


The **safety elevator**, invented by Elisha Otis in 1861.

At the top of the elevator car is a braking mechanism made of spring-loaded arms and pivots. If the main cable breaks, the springs push out two sturdy bars called "pawls" so they lock into vertical racks of upward-pointing teeth on either side. This ratchet-like device clamps the elevator in place.

Modern elevators generally use a **safety governor** which is activated when the elevator moves too quickly. If **centrifugal force** exerts a greater force on hooked flyweights than a spring holding them in place, they lock into ratchets and stop the elevator.

# Illustration: nuclear control rods



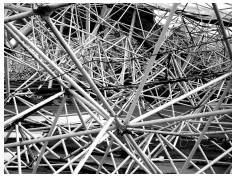

Control rods in a nuclear reactor are suspended by electromagnets. When placed in the reactor vessel, they absorb neutrons and slow down the nuclear reaction.

Power failure leads to "scramming": gravity makes the rods drop into the reactor vessel and progressively shut down the nuclear reaction.

# Fail-silent principle

- Property of a subsystem to remain in or to move to a state in which it does not affect the other subsystems in case of a failure
- Mostly applicable to computer/network systems
- Hypothesis: “silence” is a safe state of the subsystem
- When associated with “watchdog” mechanisms, allows fault detection

# Decoupling



- A tightly coupled system is one that is highly interdependent
  - each part is linked to many other parts
  - failure or unplanned behaviour in one part may rapidly affect status of others
  - processes are time-dependent and cannot wait: little *slack* in the system
  - sequences are invariant
  - only one way to reach the objective
- System accidents are caused by unplanned interactions
- Coupling creates increased number of interfaces and potential interactions

RISK ENGINEERING

# Principle: design for controllability

- Objective: make system easier to control, for humans & for computers
- Use **incremental control**
  - perform critical steps incrementally rather than in one step
  - provide feedback, to test validity of assumptions and models upon which decisions are made; to allow taking corrective action before significant damage is done
  - provide various types of fallback or intermediate states
- Use **negative feedback mechanisms** to achieve automatic shutdown when the operator loses control
  - example: safety value that lets out steam when pressure becomes too high in a steam boiler
  - example: dead man's handle that stops train when driver falls asleep
- Decrease time pressures
- Provide decision aids and monitoring mechanisms

# Procedural design solutions

- Procedural design solutions require a **person** to perform an action to avoid a hazard
  - example: following a standard operating procedure
  - example: responding to an indication of a problem such as an alarm, an instrument reading, a noise, a leak
- Since an individual is involved in performing the corrective action, consideration needs to be given to human factors issues
  - example: over-alarming
  - example: improper allocation of tasks between machine and person
- Because of the human factors involved, procedural solutions are generally the least reliable of the four categories
- Procedural solutions are sometimes referred to as *administrative controls*

# Examples of procedural design solutions

- Following standard operating procedures to keep process operations within established equipment mechanical design limits
- Manually closing a feed isolation valve in response to a high level alarm to avoid tank overfilling
- Executing preventive maintenance procedures to prevent equipment failures
- Manually attaching bonding and grounding systems

RISK ENGINEERING

# Risk treatment: barrier types

| Barriers | Examples |
|---|---|
| 1. Limit the energy (or substitute a safer form) | Low voltage instruments, safer solvents, quantity limitation |
| 2. Prevent build-up | Limit controls, fuses, gas detectors, floor loading |
| 3. Prevent the release | Containment, insulation |
| 4. Provide for slow release | Rupture disc, safety valve, seat belts, shock absorption |
| 5. Channel the release away, that is, separate in time or space | Roping off areas, aisle marking, electrical grounding, lockouts, interlocks |
| 6. Put a barrier on the energy source | Sprinklers, filters, acoustic treatment |
| 7. Put a barrier between the energy source and men or objects | Fire doors, welding shields |
| 8. Put a barrier on the man or object to block or attenuate the energy | Shoes, hard hats, gloves, respirators, heavy protectors |
| 9. Raise the injury or damage threshold | Selection, acclimatization to heat or cold |
| 10. Treat or repair | Emergency showers, transfer to low radiation job, rescue, emergency medical care |
| 11. Rehabilitate | Relaxation, recreation, recuperation |

# Design principle: defence in depth

- Multiple, independent safety barriers organized in chains
  - independence: if one barrier fails, the next is still intact
  - both *functional* and *structural* independence
- Use large design margins to overcome epistemic uncertainty (conservative design)
- Use quality assurance techniques during design and manufacturing
- Operate within predetermined safe design limits
- Continuous testing and inspections to ensure original design margins are maintained
- Complementary principles:
  - high degree of single element integrity
  - no single failure of any active component will disable any barrier

RISK ENGINEERING

# Design principle: defence in depth

| Level | Objective | Essential means |
|---|---|---|
| 1 | Prevention of abnormal operation and failures | Conservative design and high quality in construction and operation |
| 2 | Control of abnormal operation and detection of failures | Control, limiting and protection systems and other surveillance features |
| 3 | Control of accidents within the design basis | Engineering safety features and accident procedures |
| 4 | Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents | Complementary measures and accident management |
| 5 | Mitigation of radiological consequences of significant releases of radioactive materials | Off-site emergency response |

Source: INSAG-10 report *Defence in depth in nuclear safety*, 1996, IAEA

RISK ENGINEERING

# Design principle: defence in depth

- **Hierarchy of safety barriers**:
  - first **preventive** barriers (avoid occurrence of unwanted event)
  - then **protective** barriers (limit consequences of accident)
  - lesson from the Titanic disaster: improvement of preventive barriers (hull divided into watertight compartments) is not a reason for reducing protective barriers (lifeboats)

- Further principles:
  - controls **closest to the hazard** are preferred since they may provide protection to the largest population of potential receptors, including workers and the public
  - controls that are **effective for multiple hazards** are preferred since they can be resource effective

# Hierarchy of controls

Control selection strategy should follow the following standard of preference at all stages of design:

1. minimization of hazardous materials is the first priority
2. safety structures/systems/components are preferred over administrative controls
3. passive structures/systems/components are preferred over active structures/systems/components
4. preventive controls are preferred over mitigative controls
5. facility safety structures/systems/components are preferred over personal protective equipment (PPE)

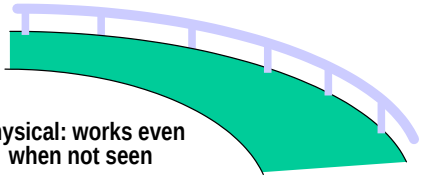
(This wording from DOE-STD-1189-2008)

RISK ENGINEERING

# Barrier types

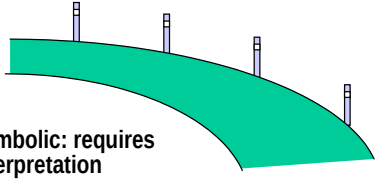
- Physical, material
  - obstructions, hindrances…
- Functional
  - mechanical (interlocks)
  - logical, spatial, temporal
- Symbolic
  - signs & signals
  - procedures
  - interface design
- Immaterial
  - rules, laws, procedures

# Barrier types on the road

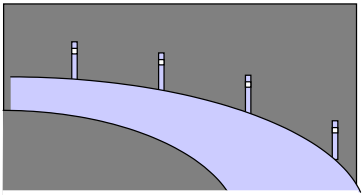


Physical: works even when not seen

Symbolic: requires interpretation



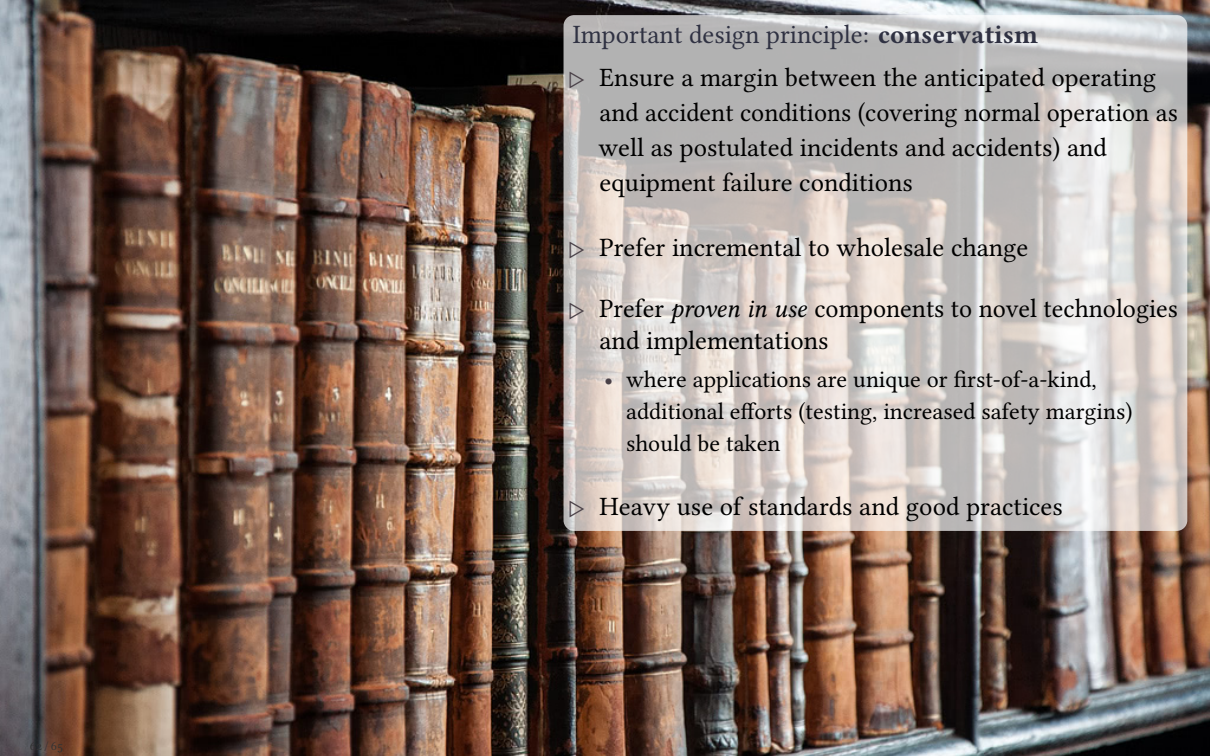
Symbolic: requires interpretation



Symbolic: requires interpretation

## Barrier criteria

- **Effectiveness**: to what extent the barrier is expected to be able to achieve its purpose
- **Latency**: how long it takes for the barrier to become effective, once triggered
- **Robustness**: how resistant the barrier is w.r.t. variability of the environment (working practices, degraded information, unexpected events, *etc.*)
- **Resources required**: cost of building and maintaining the barrier
- **Evaluation**: how easy it is to verify that the barrier works



Important design principle: **conservatism**

- ▷ Ensure a margin between the anticipated operating and accident conditions (covering normal operation as well as postulated incidents and accidents) and equipment failure conditions
- ▷ Prefer incremental to wholesale change
- ▷ Prefer *proven in use* components to novel technologies and implementations
  - where applications are unique or first-of-a-kind, additional efforts (testing, increased safety margins) should be taken
- ▷ Heavy use of standards and good practices

# Image credits


- Fire escapes on slide 4: `flic.kr/p/JQgWqr`, CC BY-NC licence
- Beakers on slide 15: `flic.kr/p/23BSz`, CC BY-NC-SA licence
- Tracks on slide 19: `flic.kr/p/ac7oLB`, CC BY-ND licence
- Wires on slides 20: `flic.kr/p/cFM3cd`, CC BY licence
- Knife on slide 25: `flic.kr/p/4A3oRE`, CC BY-NC licence
- Pills on slide 26: `flic.kr/p/8wbqMi`, CC BY-NC-ND licence
- Petrol cans on slides 27: `flic.kr/p/6BWn2d`, CC BY licence
- Railroad semaphores on slide 40: `flic.kr/p/nP4JbD`, CC BY-NC-SA licence
- Nuclear power plant on slide 43: Online textbook *Principles of General Chemistry*, CC BY-NC-SA licence
- Valve on slide 48: `flic.kr/p/4yixsL`, CC BY-NC-ND licence
- Castle on slide 50: `flic.kr/p/9cKAvr`, CC BY licence
- Books at Trinity College library on slide 57 by Wendy, via `flic.kr/p/fVs7BZ`, CC BY-NC-ND licence

## Further reading

- Book *Engineering a safer world — systems thinking applied to safety* by Nancy Leveson (MIT Press, 2012), ISBN: 978-0262016629
  - can be purchased in hardcover or downloaded in PDF format for free
- UK HSE research report *Improving inherent safety* (OTH 96 521) from 1996
- INSAG-10 report *Defence in Depth in Nuclear Safety*, from IAEA
- US Department of Energy *Nonreactor nuclear safety design guide* (DOE G 420.1-1A 12-4-2012) provides useful generic guidance on designing for safety
- The *International System Safety Society* website at `system-safety.org`

For more free content on risk engineering, visit `risk-engineering.org`

RISK ENGINEERING

# Feedback welcome!



Was some of the content unclear? Which parts were most useful to you? Your comments to `feedback@risk-engineering.org` (email) or `@LearnRiskEng` (Twitter) will help us to improve these materials. Thanks!

`@LearnRiskEng`

`fb.me/RiskEngineering`

For more free content on risk engineering, visit `risk-engineering.org`