



engineering

Safety in Design

by

Mark Ludwigson, PE, PMP

**Course 521
3 PDH (3 Hours)**

**PO Box 449
Pewaukee, WI 53072
(888) 564 - 9098
eng-support@edcet.com**

Safety in Design

Course Outline:

- Overview of Safety in Design
- History of Safety Engineering
- Standards and Codes
- Risk Management
- Precedence of Approaches
- Inherent Safety
- Error Tolerance
- Redundancy
- Safety Factors
- Passive versus Active Protection
- Fail-Safe and Decoupling
- Defense in Depth
- HAZOP
- LOPA
- Helpful References
- Examination

Safety in Design

Overview of Safety in Design

Safety can be defined as follows:

- Protection from harm,
- Condition with low probability to experience harm,
- Control of recognized hazards to achieve an acceptable level of health risk.

“Safety in Design” (SiD) refers to engineering principles and techniques that result in designs that prioritize safety. Another phrase for this is “Prevention through Design” (PtD). This course covers high-level SiD/PtD principles that apply to most engineering disciplines and applications. Within each engineering discipline/application there are many more specific techniques for implementing these high-level principles.

Public versus Occupational Safety

Safety considerations are often group as public or occupational:

1. Public Safety

- a. Impacts to visitors, residents, and consumers
- b. Impacts to the general public (planned and unplanned)
- c. Addressed with regulations, codes, and standards

2. Occupational Safety

- a. Impacts to construction workers
- b. Impacts to employees (operators, maintenance staff, inspectors, etc.)
- c. Impacts to hazardous materials (hazmat) workers
- d. Impacts to delivery and transportation staff
- e. Addressed with OSHA regulations

Hierarchy of Controls

Engineers play a critical role in creating safe conditions, including during construction, operations, maintenance, and public use. Considering safety in the design process can have a tremendous impact throughout the lifespan of the improvements. Figure 1 depicts different approaches to preventing injury.

Safety in Design

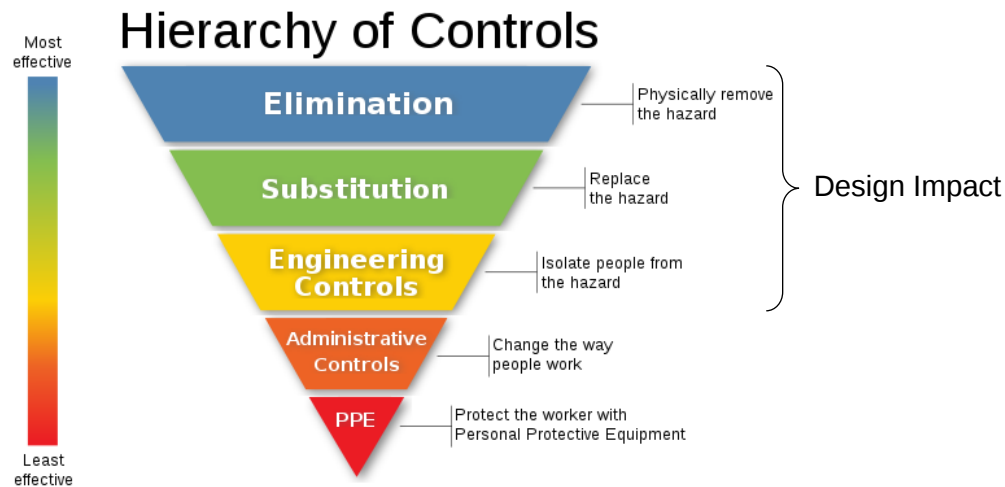


Figure 1: Hierarchy of hazard control triangle. Methods towards the top are generally most effective. Following this hierarchy normally leads to inherently safer systems.

Source: https://en.wikipedia.org/wiki/Hierarchy_of_hazard_controls, p.d.

The three most effective approaches (elimination, substitution, and engineering controls) can often be done in the design stage. The least effective approaches (administrative controls and PPE) involving trying to keep people safe given the design that has already been decided and implemented.

Example Problem 1

Engineer Rob is designing a retaining wall in a yard with the potential for people walking nearby to fall over 6 feet. Help give Rob ideas in each of the five categories in the hazard control triangle. Indicate which are design decisions.

Solution:

1. Elimination: Regrade the yard to avoid a retaining wall and eliminate the hazard.
2. Substitution: Provide a stepped terrace to substitute the hazard.
3. Engineering Controls: Provide a guardrail along the top of the retaining wall.
4. Administrative Controls: Deter people from entering the yard with no trespassing signs and enforcing fines.
5. PPE: Require a fall arrest harness for anyone walking in the yard.

The first three approaches are design decisions.

Safety in Design

Safety and Ethics

Safety is in the first fundamental canon and rule of practice of the NSPE Code of Ethics for Engineers, as highlighted below:



I. Fundamental Canons

Engineers, in the fulfillment of their professional duties, shall:

1. Hold paramount the **safety**, health, and welfare of the public.
2. Perform services only in areas of their competence.
3. Issue public statements only in an objective and truthful manner.
4. Act for each employer or client as faithful agents or trustees.
5. Avoid deceptive acts.
6. Conduct themselves honorably, responsibly, ethically, and lawfully so as to enhance the honor, reputation, and usefulness of the profession.

II. Rules of Practice

1. **Engineers shall hold paramount the **safety**, health, and welfare of the public.**
 - a. If engineers' judgment is overruled under circumstances that endanger life or property, they shall notify their employer or client and such other authority as may be appropriate.

Consideration of safety is an ethical responsibility of every engineer.

Safety in Design

Safety Engineers

There are some situations that call for a specialized “safety engineer” whose primary job responsibility is to perform safety related engineering duties. The following are examples of engineers whose primary focus is on safety.

1. Fire Protection Engineer
2. Automobile Safety Engineer
3. Industrial Safety Engineer
4. Health and Safety Engineer
5. HSE (Health, Safety & Environment) Engineer
6. Product Safety Engineer

Examples of job duties for a safety engineer:

- Create and maintain health and safety policies and procedures.
- Provide safety training.
- Review employee safety programs and recommend improvements.
- Review plans and specifications to ensure they meet safety requirements.
- Perform inspections and identify safety concerns.
- Evaluate industrial control mechanisms for safety standards.
- Perform design modifications to achieve safety goals.
- Review new technologies and innovations for potential safety improvements.
- Investigate accidents and injuries to determine their causes and consider changes to prevent them in the future.

Safety in Design

History of Safety Engineering

Throughout history, engineers have played a pivotal role in the advancement of safety in society. The following are a few examples.

Steam Engines

Scottish engineer James Watt (1736 to 1819) was one of the inventors of the steam engine. He recognized the potential to build high-pressure steam engines for greater efficiency and power but resisted due to the likelihood of explosions and injuries. Watt petitioned Parliament to outlaw the use of high-pressure steam engines.

In the late 1700's and early 1800's, high pressure steam engines resulted in numerous deaths in the United States. For example, the steamboat SS Helen McGregor had an explosion that killed around 50 people.



Figure 2: Photograph of a steam engine boiler explosion in 1878.

Source: [https://commons.wikimedia.org/wiki/File:Wreck_in_Snow_Bank,_Boiler_Explosion,_Engine_-70_\(3739556348\).jpg](https://commons.wikimedia.org/wiki/File:Wreck_in_Snow_Bank,_Boiler_Explosion,_Engine_-70_(3739556348).jpg), p.d.

Engineers worked under a federal government contract to provide recommendations to reduce the number of steam engine explosions and prevent injury and death. Congress used these recommendations to pass bills in 1824 and 1832 that enacted several minimum safety requirements for steam engines. With new regulations in place, steam engines became safer to operate.

Safety in Design

Elevators

Devices for lifting loads go back to Roman times. In the 1st century BCE, Roman engineer Vitruvius documented the details of lifting platforms with pulleys and capstans (called windlasses) operated by people or humans pulling ropes or with waterwheels. In the late 1700's, steam power was applied to lifts. And in the early 1800's, a hydraulic lift was invented which made freight elevators more reliable and powerful. However, the platforms would fall on occasion, and sometimes cause injury or death, so elevators were not used for passengers.

In 1853, American engineer Elisha Graves Otis invented a "safety hoist" which is a type of automatic safety device that prevents an elevator car from falling if the lifting chain or rope broke. This made freight elevators much safer. Also, elevators were deemed safe enough for people to use to get to higher floors. Soon after, buildings were made taller and passenger elevators became commonplace. There were still occasional elevator failures resulting in unacceptable deaths and severe injuries. Over the last 150 years, a multitude of inventors and engineers have added dozens of safety features. See Figure 3 for example patents.

For example, in 1931, two Westinghouse engineers, Luther J. Kinnard and James Dunlop, patented an automatic door reversal safety device. It included two pairs of lights and photoelectric cells, one mounted in the car and one the landings, for detecting people moving in and out of the car, as shown in Figure 3. This prevents the doors from closing on a person and keeps the elevator from moving with something stuck in the doorway.

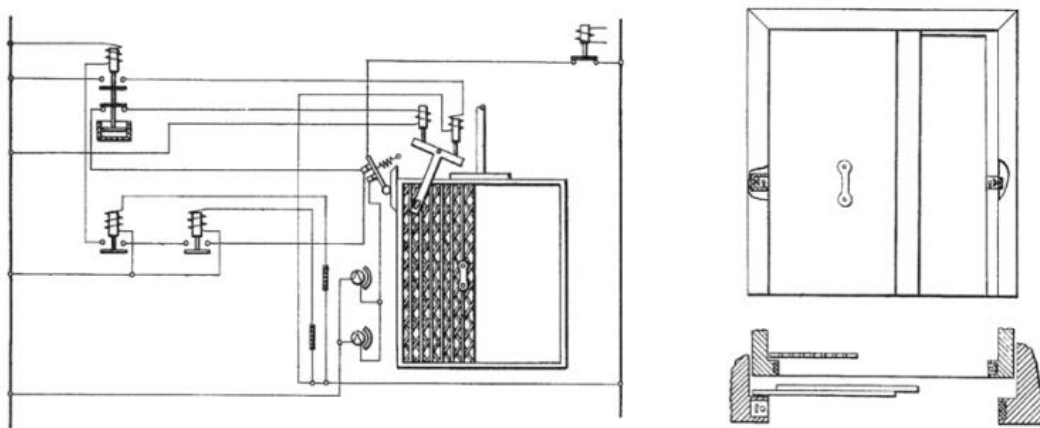


Figure 3: "Automatic door reversal safety device" by Kinnard and Dunlop.

Source: <https://www.uspto.gov/patents/search>, public domain

Safety in Design

Fire Protection

John Ripley Freeman (1855 to 1932) was a civil engineer and hydraulics expert, specializing in the design of dams, locks, aqueducts, and water supply systems. As a young engineer, Freeman saw how water pipes with small holes were first installed on the ceilings of factories for firefighting. Freeman recognized how this development was saving lives, so in 1886 he became an insurance engineer for Factory Mutual and rewarded owners with effective sprinkler systems.

In the 1880's, various types of sprinkler systems become common for new buildings. Scientific research was done to determine the most effective and reliable system. Under Freeman's direction, Factory Mutual promoted the standardization of the sprinkler system that was scientifically proven to automatically start during a fire and provide the greatest coverage on the floor below. Figure 4 shows a modern sprinkler system test.



Figure 4: Testing of Aqueous Film Forming Foam (AFFF) sprinklers.

Source: https://commons.wikimedia.org/wiki/Category:Aqueous_Film_Forming_Foam, p.d.

Freeman created a report that spurred several insurance agencies and communities in the northeast United States to meet in New York City in 1896 and 1897 with the lofty goal of creating national standards of practice for the promotion of safety.

An 1896 meeting on sprinkler systems resulted in the release of a document entitled: "Report of Committee on Automatic Sprinkler Protection", which eventually becoming standard NFPA 13. In 1907, Freeman proudly became an early member of the National Fire Protection Association (NFPA).

Safety in Design

Electricity

Injuries from electrical shocks were common in the early 1900's. Electrical codes were developed which helped prevent fatalities from obviously dangerous human contact. However, electrical injuries were still common and the various scenarios where electricity ends up passing through the body were a mystery.

In the 1950's, engineer Charles Dalziel researched the harmful effects of electric shocks on animals and people. Dalziel published his findings in a book entitled "The Effects of Electric Shock on Man." One breakthrough was to explain how electricity can pass through the body due to "ground faults".

A ground fault occurs when something conductive (like a person) accidentally touches an active circuit (wire) and provides a pathway to the earth (ground). Dalziel invented ground-fault circuit interrupter (GFCI) outlets and breakers to help prevent ground faults. A GFCI is a small circuit breaker designed to stop the flow of electricity in the event of a ground fault within a fraction of a second. The GFCI was so effective that the National Electrical Code (NEC) mandated their use in outdoor receptacles in 1971, bathroom receptacles in 1975, and kitchen receptacles in 1987.



Figure 5: A typical residential GFCI receptacle in North America.
The black button is labeled "test" and the red button is labeled "reset".
The receptacle is labeled "TR" indicating tamper resistance.

Source: https://commons.wikimedia.org/wiki/File:Residential_GFCI_receptacle.jpg, Ben Kurtovic, CC-BY-SA-4.0

Safety in Design

Standards and Codes

Arguably the most successful method to prevent accidental injury and death is to require that designs comply with standards and codes (including regulations) that prioritize safety. The design stage has the greatest potential for creating safe conditions for the lifespan of the improvements, as depicted in the hazard control triangle in Figure 1.

Standards and codes have been developed in most engineering area/fields. Simply following the relevant standards and codes can prevent people from getting hurt.

Here are definitions that apply to engineering:

- Standards are formal engineering documents that establish uniform technical criteria, methods, and practices.
 - *Consensus standards* are typically ratified by committees in recognized organizations.
 - *Non-consensus standards* are issued as good practice but not ratified. Examples include pamphlets, briefs, guides, reports, handbooks, etc.
 - *Internal standards* are accepted within a company or organization.
- Codes, formally called statutes, are laws written and enacted by the legislative branch of government, such as U.S. Congress and state legislators.
- Regulations, also referred to as rules, are written by agencies (for example OSHA or EPA) which have authority granted in laws enacted by the legislature.

Building Codes

In 1625, the first building code in the US, in New Amsterdam, NY, was issued which addressed fire safety and materials for roofs. By the end of the 1800's, various codes were approved in major cities with safety the main motivation. Many engineers were expected to learn and follow local codes for the first time. These early codes addressed natural gas, electricity, steam boilers, explosives, building materials, roofing, chimneys, elevators, and fire protection.

Rather than create unique codes, it is common for local authorities to use “model building codes”, which are national or global codes created by a recognized organization. Model building codes are either adopted (accepted without modifications) or adapted (modified) and then enforced by the local authority. A construction permit is not issued until the local authority is satisfied that the design meets code.

Safety in Design

The most common model building codes are as follows:

- International Building Code (IBC) by the International Code Council (ICC)
- NFPA 1 – Fire Code by the National Fire Protection Association (NFPA)
- NFPA 70 - National Electrical Code (NEC) by the National Fire Protection Association (NFPA)

OSHA Regulations

The Occupational Safety and Health Administration (OSHA) is a U.S. agency devoted to the safety of workers. There are nearly 1,000 OSHA standards, falling under four main categories: Construction, Maritime, Agriculture and General Industry. Construction includes the highest number of individual standards. General Industry addresses safety in most workplaces. OSHA also investigates injuries, performs inspections, and gives citations (see Figure 6).

In general, OSHA requirements do not directly address design. However, the following OSHA topics do impact design:

- Permanent ladders
- Guarding for machinery
- Emergency eyewash and safety showers
- Containment for hazardous materials
- Constructability reviews, construction equipment, scaffolding, etc.



Figure 6: Top 10 OSHA citations in 2022. Design decisions impact if a hazardous condition will exist, which indirectly impacts these citation statistics.

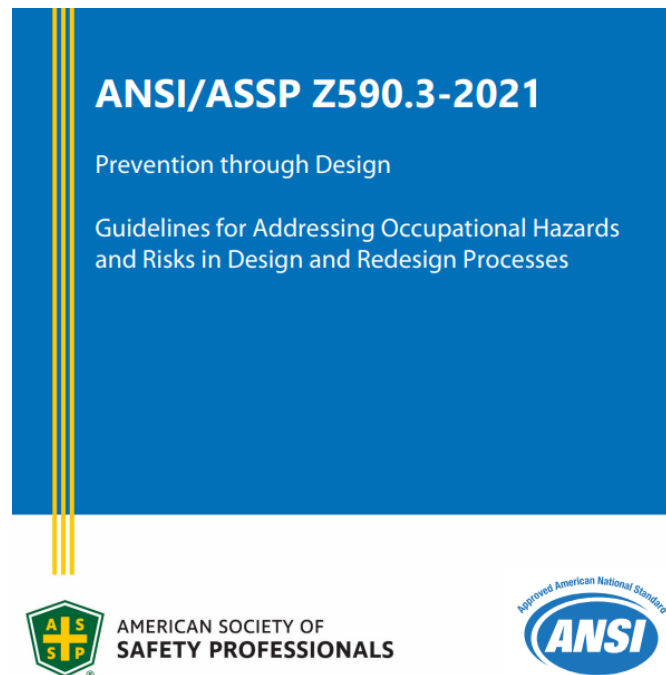
Source: <https://www.osha.gov/top10citedstandards>, public domain

Safety in Design

American Society of Safety Engineers

The American Society of Safety Engineers (ASSE) was founded in 1911 and now has over 30,000 members. ASSE promotes safety in design through education, advocacy, standards development, and collaboration. Annual events include a SafetyFOCUS conference and a Safety Professional Development Conference (PDC).

A relevant standard is ANSI/ASSP Z590.3 entitled "Prevention Through Design". The purpose is to help engineers, safety professionals, and employers incorporate prevention through design (PtD) concepts into decision-making related to the design and redesign of work premises, tools, equipment, machinery, substances, and work processes. Learn to conduct a life-cycle assessment and develop a design model that balances safety and health goals with other objectives over the lifespan of a facility, process, or product.



International System Safety Society

The International System Safety Society (ISSS) is a non-profit organization dedicated to supporting safety professionals, including engineers, in the application of Systems Engineering and Systems Management to the process of hazard, safety and risk analysis. The ISSS was founded in 1964 and draws members throughout the world.

Safety in Design

Risk Management

Safety is often considered an aspect of risk management. Risk management is the process of identifying, assessing, and controlling risks to a project, process, or organization. Types of risks include financial, legal, strategic, security, and safety. Although many design projects do not list safety as an objective, there is no doubt that a poor design that results in an unsafe condition puts the success of the project at risk.

Risks are potential events that would have a negative impact on the project. Risk management involves these activities:

1. Identify risks
2. Prepare for risks
3. Respond to risks

The goal of risk management is to minimize the impact of risks in order to keep on track to meeting project goals.

Risk Register

A risk register is a table with a list of identified risks. Normally, there are columns for risk description, probability (aka likelihood), severity (aka impact or consequence), ranking (aka priority), response, and status. See Figure 7 for an example with safety related risks. Note how for the first two items, priority matches the impact rather than the probability.

ID	Risk	Probability	Impact	Priority
1	Trip hazard from openings in grating	Medium	Low	Low
2	Inadequate clearance between equip.	Medium	Low	Low
3	Truck turn radius too tight	Medium	Medium	Medium
4	Safety shower not visible	Low	High	Medium

Figure 7: Example risk register with safety in design items listed.

There should also be columns on the right for Response and Status.

Source: commons.wikimedia.org/wiki/File:Risk_Register_ID_and_Qual.png, Lapollard, CC-BY-SA-4.0

Safety in Design

The goal is not to list every possible safety risk, but to consider unique aspects of the design that may lead to an unsafe condition, especially if life threatening. If codes already address the issue, then likely it doesn't need to be tracked in the risk register. Also, if the design is a copy of a previous design that has already been constructed and placed in operation, there would be fewer safety concerns. Most safety risks worth tracking are due to unique and inventive arrangements.

For example, placing lighting on the walls instead of the ceiling has a risk of glaring people's eyes and causing an accident. A response could be to only allow lights on the ceiling (if possible) or to specify dim lights designed for wall mounting and require a submittal from the contractor.

Risk Ranking

One way to prioritize risks is to assess the likelihood (aka probability) and severity (aka impact or consequence) of each risk and assign a combined score. See Figure 8 for a plot of severity versus likelihood with resulting risk scores from 1 to 12. This is called a risk matrix. Note how severity is more important than likelihood.

Another approach for risk ranking is to sum the severity and likelihood values (each on the same scale), per this formula:

$$\text{Risk Score} = \text{IF} * \text{Severity Score} + \text{Likelihood Score}$$

IF = Importance factor (often 1.5 to 4.0 for safety)

The higher the importance factor, the more weight is given to severity.

Safety in Design

RISK RATING KEY		LOW	MEDIUM	HIGH	EXTREME
		0 – ACCEPTABLE OK TO PROCEED	1 – ALARP (as low as reasonably practicable) TAKE MITIGATION EFFORTS	2 – GENERALLY UNACCEPTABLE SEEK SUPPORT	3 – INTOLERABLE PLACE EVENT ON HOLD
		SEVERITY			
		ACCEPTABLE LITTLE TO NO EFFECT ON EVENT	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	UNDESIRABLE SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	INTOLERABLE COULD RESULT IN DISASTER
LIKELIHOOD	IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW – 1 –	MEDIUM – 4 –	MEDIUM – 6 –	HIGH – 10 –
	POSSIBLE RISK WILL LIKELY OCCUR	LOW – 2 –	MEDIUM – 5 –	HIGH – 8 –	EXTREME – 11 –
	PROBABLE RISK WILL OCCUR	MEDIUM – 3 –	HIGH – 7 –	HIGH – 9 –	EXTREME – 12 –

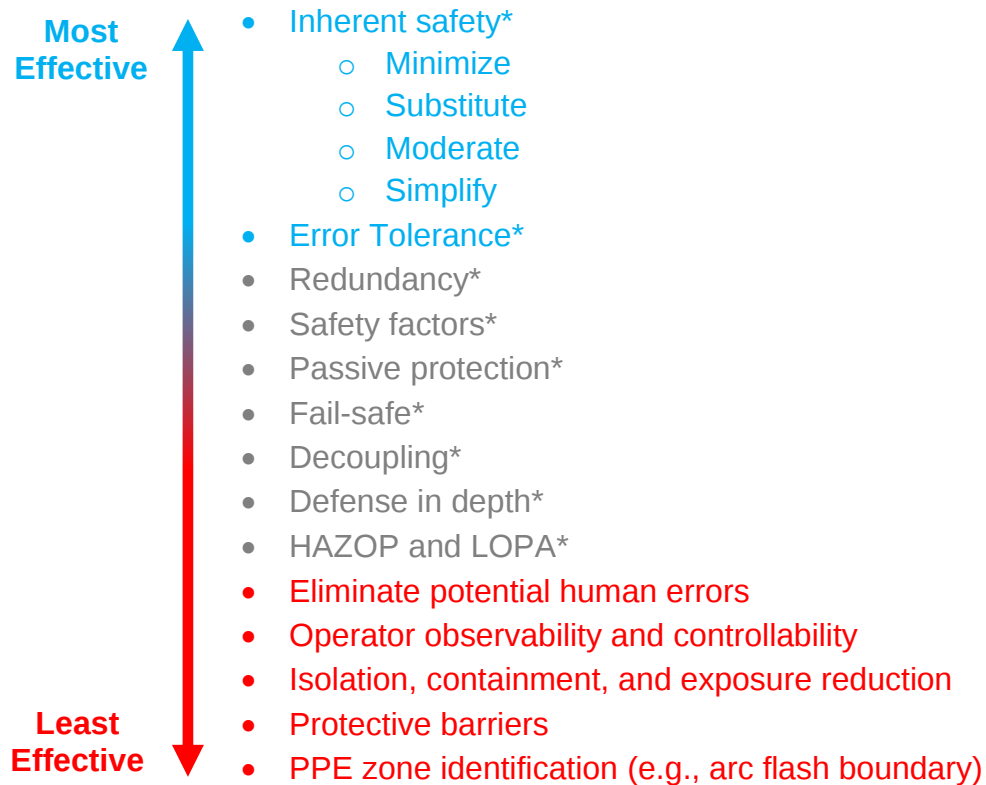
Figure 8: Risk assessment matrix with “severity” resulting in higher scoring.

Source: commons.wikimedia.org/wiki/File:IC-Risk-Assessment-Matrix-Template.jpg, U3115299, CC-BY-SA-4.0

Safety in Design

Precedence of Approaches

The following is a list of safe design approaches, ranked from most effective to least effective. This is a general ranking; actual effectiveness will vary based on the application. Approaches with an asterisk (*) are described in this course.



Safety in Design

Inherent Safety

Inherent safety, also called Inherently Safer Design (ISD), is a design approach where a system configuration is chosen to eliminate or significantly reduce hazards rather than the conventional approach of adding features to control hazards and protect people. The resulting system is inherently safer such that safety cannot be comprised by actions such as low quality construction, inadequate PPE, component failures, or accidents.

Designing for inherent safety often includes these steps:

1. Identify hazards in a design
2. Brainstorm alternatives that eliminate or significantly reduce the severity or likelihood of each hazard
3. Compare alternatives
4. Choose a design with reduced hazards

Table 1 summarizes the four main methods for inherent safety along with examples.

Safety in Design

Table 1: Methods for Inherent Safety

Method	Principle	Examples
Minimize	Reduce the level of hazards present at any one time	• Use smaller quantities of hazardous materials • Eliminate unnecessary equipment • Reduce size of equipment or volumes processed
Substitute	Replace a hazardous component with a less hazardous one	• Use a less hazardous substance • Clean pipes with compressed air instead of natural gas which can ignite • Clean with a detergent rather than a flammable solvent • Use fireproof materials instead of flammable
Moderate	Reduce the strength of a danger	• Reducing the pressure or temperature • Create less hazardous conditions • Spread out, separate, and decouple hazards • Using dilute rather than concentrated chemicals
Simplify	Eliminate potentially dangerous combinations by streamlining and eliminating components	• Eliminate unnecessary complexity • Make operating errors less likely • Use intuitive technology • Rearrange layout to minimize materials and components • Use symmetry • Place operator interfaces in convenient and shared places

Safety in Design

Example Problem 2

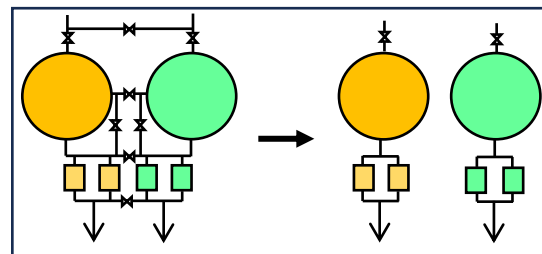
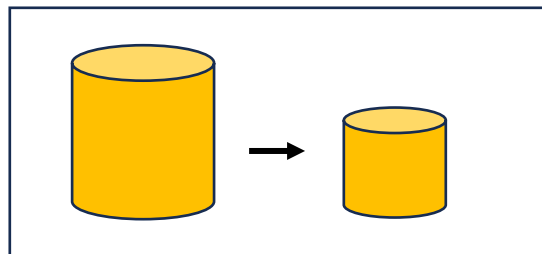
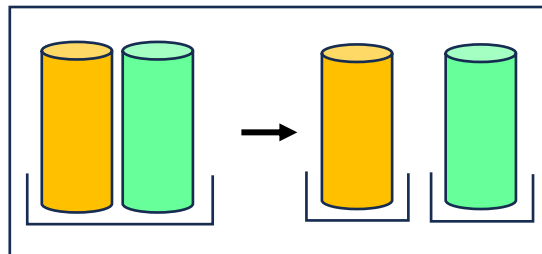
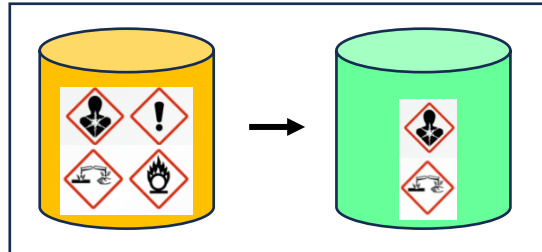
Draw lines to match each inherent safety method (left) with the corresponding image.

Minimize

Substitute

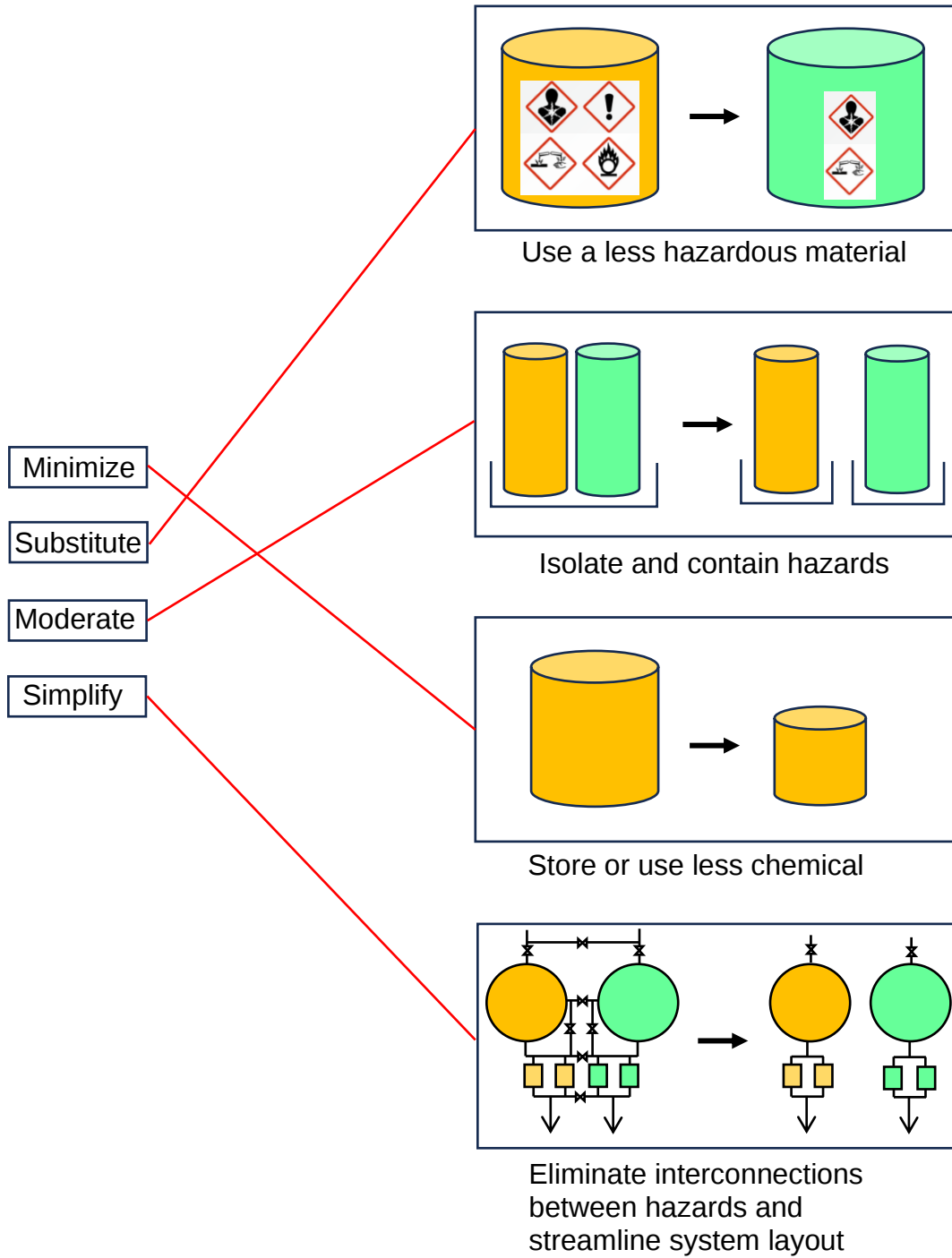
Moderate

Simplify



Safety in Design

Solution:



Safety in Design

Error Tolerance

An effective approach for the design of processes is to specify components with an error (or deviation) tolerance greater than possible conditions. The tolerance can often be expressed as the system design range, instrument range, and containment range, as depicted in Figure 9.

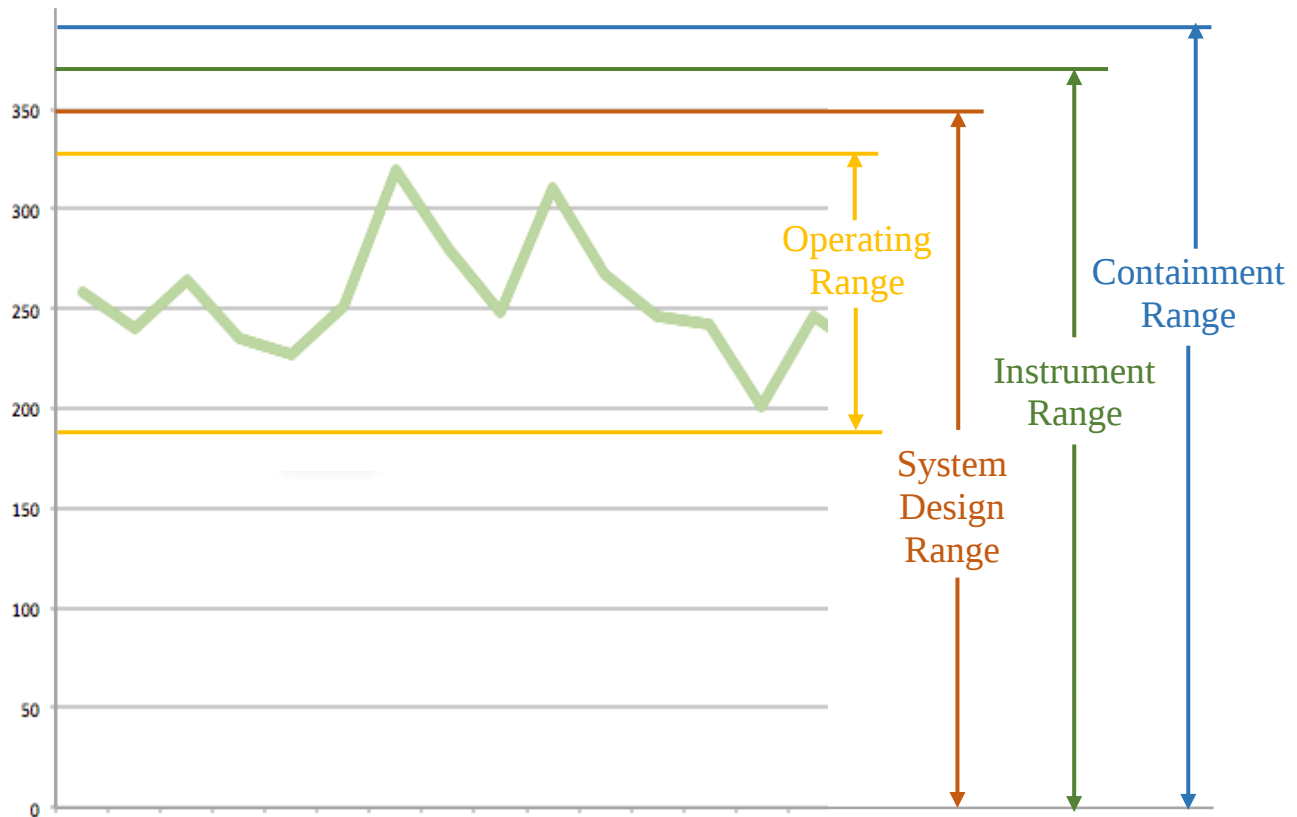


Figure 9: Plot showing design limits for a variable process such as pressure, temperature, level, flow rate, or concentration.

Source: commons.wikimedia.org/wiki/File:Population_graph_of_rochford.png, C.Thomas97, CC-BY-SA-4.0

For example, for selected a pipe thickness/gauge, the working (design) pressure should be greater than any possible operating pressure. After the installed pipe is tested at or above the design pressure, the pipe would be considered safe. If the pipe is subject to corrosion, an additional thickness and coating may be warranted to prevent failure from corrosion. Additional safety factors or other protections may be justified based on the actual conditions.

Safety in Design

Redundancy

Redundancy offers many benefits, including increasing the reliability of a system or process. For example, in a pump station, adding an extra pump (called a standby or installed spare) allows pumping to continue when one of the duty pumps or associated valves goes out of service. See Figure 10 for an example.

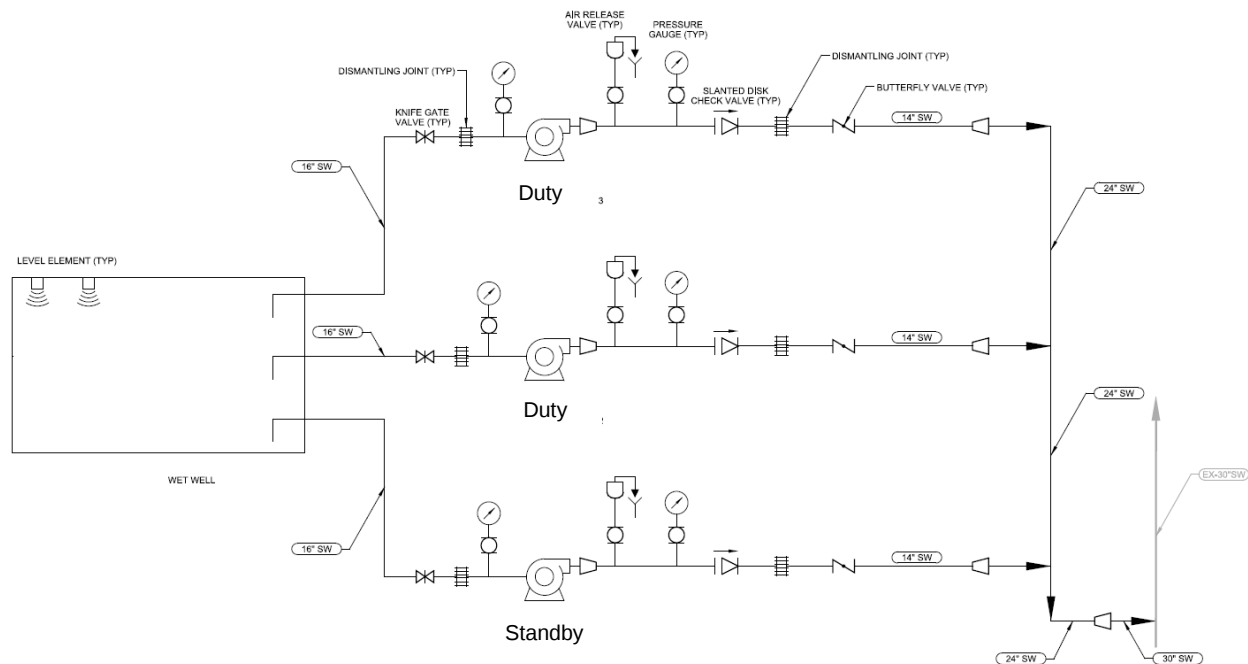


Figure 10: Diagram of a pump station with two duty pumps and one standby pump. There is also a redundant level sensor shown on the left.

Source: Author

Redundancy usually increases the safety of a system for the following reasons:

- Allows operations and maintenance staff to take duty components completely offline while performing work.
- Provides flexibility in operations to avoid potential failures and hazardous conditions.
- Repair work can be scheduled with the correct maintenance staff.
- Safety requirements can be planned prior to repair work.
- Repair work can be done without pressure to complete it quickly.
- Automation can switch to a standby unit upon failure of a duty unit

Safety in Design

Safety Factors

A safety factor (SF), also called factor of safety (FoS), is most commonly defined as the ratio of the maximum capacity divided by the demand or design condition. The formula is as follows as applied to stress:

$$\text{Safety Factor} = \frac{\text{Capacity}}{\text{Demand}} = \frac{\text{Ultimate or Yield Stress}}{\text{Design Stress}}$$

- A beam designed with SF of 1.0 will fail with any load over the design load.
- A beam designed with SF of 2.0 will fail at twice or more than the design load.

Common safety factors are as follows:

- 20 Cast-iron wheels
- 10 Shafts
- 8 Wire ropes, bolts, engine parts, lifting hooks
- 6 Bridge members, rotating turbine parts
- 4 Pressure vessels, boilers, springs
- 3 Automobile chassis, static turbine parts
- 2 Building structural members, airplane parts, pipe stress
- 1.5 Airplane structure, pump hydraulics
- 1.25 Airplane main landing gear
- 1.15 HVAC units, motors
- 1.1 Sprinkler system

FOS - Factors of Safety - Applications	
Applications	Factor of Safety - FOS -
For use with highly reliable materials where loading and environmental conditions are not severe and where weight is an important consideration	1.3 - 1.5
For use with reliable materials where loading and environmental conditions are not severe	1.5 - 2
For use with ordinary materials where loading and environmental conditions are not severe	2 - 2.5
For use with less tried and for brittle materials where loading and environmental conditions are not severe	2.5 - 3
For use with materials where properties are not reliable and where loading and environmental conditions are not severe, or where reliable materials are used under difficult and environmental conditions	3 - 4

Source: The Engineering ToolBox, www.engineeringtoolbox.com/factors-safety-fos-d_1624.html

Safety in Design

Increasing the safety factor typically increases safety but requires more materials and/or more complex configurations. Sometimes there are practical limits to safety factors. For instance, for an airplane, as the safety factor increases, the plane gets heavier and requires more lift and thrust to fly, which means design changes to the wings and engines. At some point, a very high safety factor may actually make the plane less safe.

Example Problem 3

Engineer Howard needs to specify a 316 stainless steel rope to hold a 1 ton load with a safety factor of at least 8. Chose a diameter based on the below 1x7 strand table and calculate the resulting safety factor.

1x7 Strand Galvanized & Stainless Steel Corrosion Resistant					
Diameter (inch)	Galvanized		Stainless Steel		
	Weight (Lbs./ MFT)	EHS	Weight (Lbs./ MFT)	T304	T316
		Minimum Breaking Strength (Lbs.)		Minimum Breaking Strength	
				Lbs.	Lbs.
1/64	-	-	0.55	34.6	30.6
1/32	-	-	2.3	185	165
3/64	-	-	5.5	375	334
1/16	-	-	8.5	500	445
5/64	-	-	14	800	712
3/32	-	-	20	1,200	1,068
1/8	32	1,830	35	2,100	1,869
5/32	51	2,940	55	3,300	2,937
3/16	73	3,990	77	4,700	4,183
7/32	98	5,400	103	6,300	5,607
1/4	121	6,650	135	8,200	7,298
9/32	164	8,950	170	9,952	8,708
5/16	205	11,200	212	12,500	11,125
3/8	273	15,400	282	17,500	15,575
7/16	399	20,800	416	24,083	21,071
1/2	517	26,900	535	30,966	27,094

Solution:

Use the safety factor formula to calculate the minimum capacity/rating for the rope:

$$\text{Capacity}_{\min} = \text{Safety Factor}_{\min} * \text{Demand} = 8 * 1 \text{ ton} = 8 \text{ ton} = 16,000 \text{ lbs}$$

Looking at the catalog table, for T316 in the far right column, the diameter would need to be a minimum of **7/16 inch**, which has a minimum breaking strength of 21,071 lbs.

$$\text{Safety Factor}_{\text{actual}} = \frac{\text{Capacity}_{\text{actual}}}{\text{Demand}} = \frac{21,071 \text{ lb}}{2,000 \text{ lb}} = \mathbf{10.5}$$

Safety in Design

LRFD

For structural design, the traditional method with safety factors is called Allowable Stress Design (ASD). However, there is a growing trend to use the Load and Resistance Factor Design (LRFD) method, which has a safety factor on both sides of the equation, accounting for uncertainty in loads (U) and uncertainty in material strength/construction (Φ). The basic LRFD equation is as follows:

$$\text{Required Strength} \leq \text{Available Strength}$$

$$U \text{ (Service Load)} \leq \Phi(\text{Nominal Strength})$$

Other Factors

Design approaches similar to a safety factor include:

- Design factor (DF) is the inverse of a safety factor. DF is an approach that reduces the material's breaking stress to provide a safe design stress.
- Margin of safety can be defined by any of the following, depending on the use:

$$\text{Margin of safety} = \text{factor of safety} - 1$$

$$\text{Margin of safety} = \frac{\text{failure load}}{\text{design load}} - 1$$

$$\text{Margin of safety} = \frac{\text{failure load}}{\text{design load} \times \text{design safety factor}} - 1$$

$$\text{Margin of safety} = \frac{\text{realized factor of safety}}{\text{design safety factor}} - 1$$

- Reserve factor (RF) is a measure of strength frequently used in Europe:

$$\text{RF} = \frac{\text{proof strength}}{\text{proof load}} \quad \text{RF} = \frac{\text{ultimate strength}}{\text{ultimate load}}$$

Passive versus Active Protection

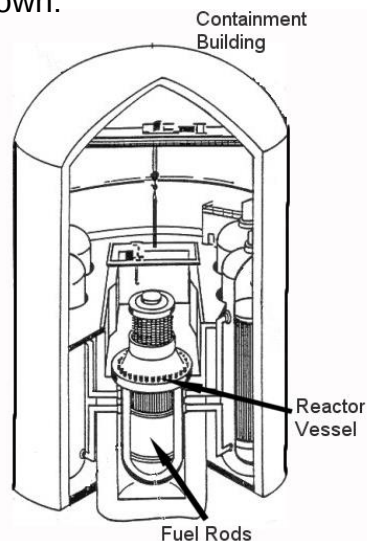
Safeguards are added to protect from potential hazards. They generally fall into the categories of “passive” and “active”. A comparison is below:

Passive Safeguards

- Maintain safety by their presence
- Fail into a safe state
- Rely on physical principles
- Less design freedom
- Not always feasible to implement
- Generally, more reliable

Example:

- A containment building prevents the escape of radioactive material, as shown:



Source: commons.wikimedia.org/wiki/
File:Containment_Building.jpg, public domain

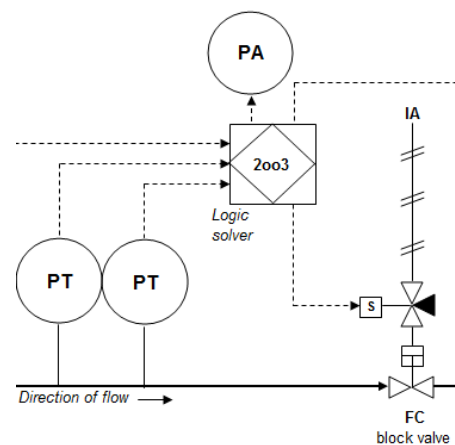
VS

Active Safeguards

- Maintain safety by detection and action
- Usually relies on instruments and controls which need power
- Hazard must be detected
- Can adjust the design to suit the application
- Generally, less reliable

Example:

- A safety instrumented system (SIS) such as a high-integrity pressure protection system (HIPPS) that prevents over-pressurization:



Source: commons.wikimedia.org/wiki/
File:HIPPS.png, public domain

Safety in Design

Fail-Safe and Decoupling

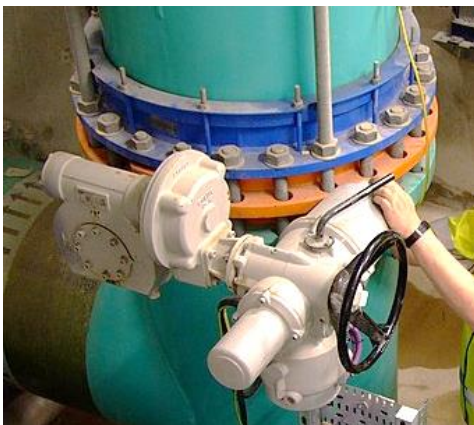
Systems should be designed to fail into a safe mode (fail-safe) that doesn't trigger other systems to be unsafe (decoupled or fail-silent). Here is a comparison of fail-safe and decoupling principals:

Fail-Safe

- Move to or remain in a safe state after a failure
- Can be done with passive or active components

Examples:

- Train brakes require energy to engage
- A trap door that opens and releases excess liquid buildup
- Elevator brakes that engage if a cable breaks or the car exceeds the normal speed
- Control valve with a spring that closes the valve upon power failure:



Source: commons.wikimedia.org/wiki/
File:Rotork_controls.jpg, public domain

VS

Decoupling

- Move to or remain in a state that does not affect other subsystems (fail-silent)
- Decreases the number of interfaces and interactions
- May require more redundancy
- Related to fail-operational, fault-tolerant approaches in which a faulty feature reconfigures itself

Examples:

- In a decoupled programming architecture, software logic has minimal interaction with other services
- Driver assistance with an error will stop displaying the faulty feature while essential driving features continue without impact:



Source: commons.wikimedia.org/wiki/
File:Autonomous-driving-Barcelona.jpg,
Eschenzweig, CC-BY-SA-4.0

Safety in Design

Defense in Depth

A defense in depth approach recognizes that having multiple levels of protection is better than a single level of protection. The design typically includes multiple, independent safeguards (safety barriers) organized in chains. It requires each safeguard be structurally and functionally independent from the others, so if one safeguard fails, the next safeguard remains fully intact.

Safeguard Types

- Physical
 - Blockades, walls, obstructions
 - Hinderances, rumble strips
- Functional
 - Mechanical switches, interlocks
 - Logic, programming
- Symbolic
 - Signs, signals, arrows, reflectors, colors, hazard pictograms
 - Human-machine interface (HMI) elements
- Procedural (non-design)
 - Laws, rules, standard operating procedures, instructions
 - Consequences, rewards, punishments

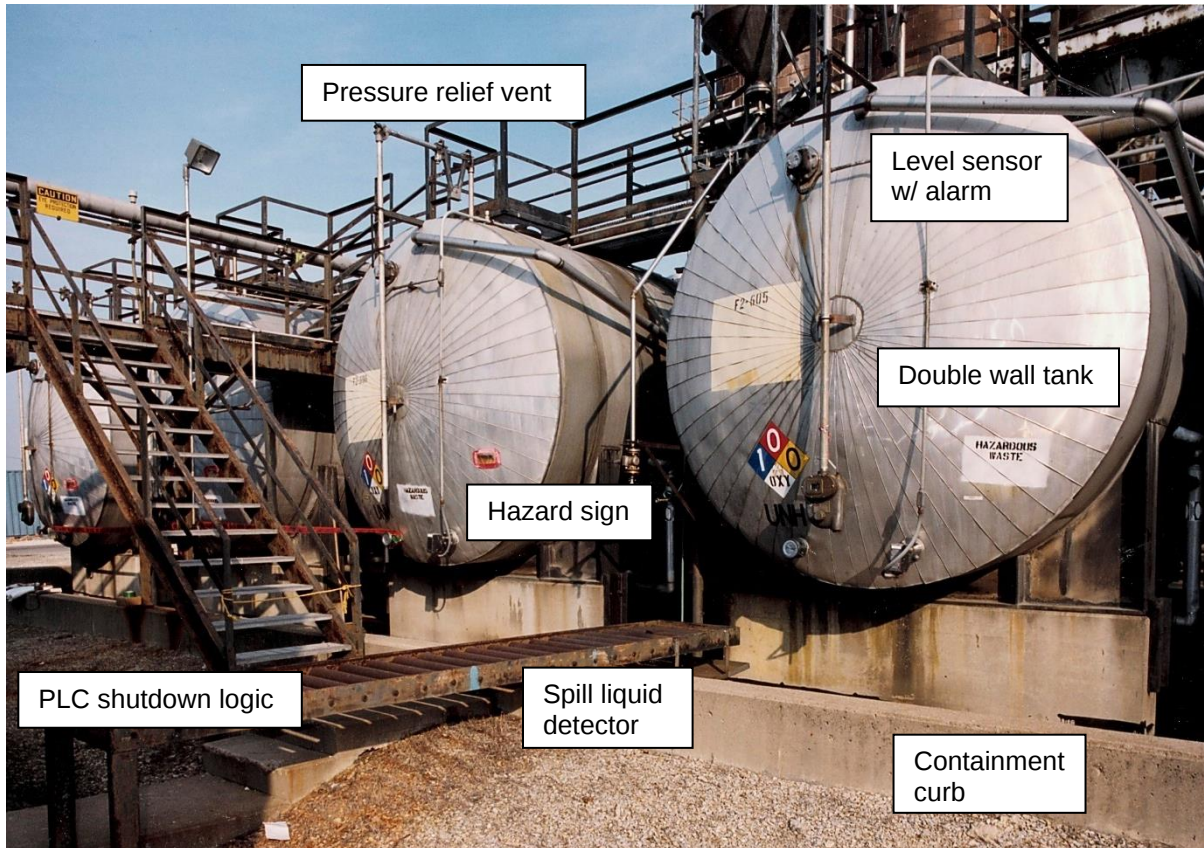
Principles

- A system can be made safer by adding safeguards
- Each safeguard is decoupled from others to avoid a cascading failure
- Use different types of safeguards to prevent a variety of failures
- Review and compare weaknesses of each safeguard so no single failure can surpass all safeguards

Safety in Design

Example Problem 4

Safeguards are labeled in the following picture. Indicate the safeguard type for each.



Solution:

- Physical safeguards:
 - Double wall tank
 - Containment curb
- Functional safeguards:
 - Pressure relief vent
 - Spill liquid detector
 - Level sensor w/ alarm
 - PLC shutdown logic
- Symbolic safeguards:
 - Hazard sign

Safety in Design

HAZOP

A Hazard and Operability Study (HAZOP) is an assessment of a complex system or process facility that identifies potential hazards and operations problems. A HAZOP can be done during design or with an existing system. The goal of a HAZOP during design is to identify all potential failures, their likelihood and consequences, and potential operations inefficiencies based on the design arrangement. A HAZOP breaks down the overall complex design into a number of simpler processes called nodes which are then more easily reviewed.

For a HAZOP during design, the typical approach is as follows:

1. Divide complex processes into a series of simple nodes
2. Review each node for potential failures (called deviations)
3. Create a table with rows for identified deviations
4. Add columns describing the deviation cause and consequences
5. Provided recommendations to address the failures and problems

Table 2: Example HAZOP for a Chemical Feed System				
Node/ Process	Deviation	Cause	Consequences	Recommended Action
1 Storage Tank	High level	Overfilled	Spill out vent	Alarm; Close fill valve
	Low level	Leak in tank	Stop pumping Potential exposure	Alarm; Stop operations
	Low level	Level switch failure	Stop pumping Pumping problems	Alarm; Stop operations
2 Transfer Pumps	Flow too high	Flow meter failure	Overdosing	Alarm; Stop operations
	Flow too low	Blockage in pipe	Pressure buildup in pipe	Add pressure sensor and relief valve; Alarm
	Flow too low	Leak in pipe	Stop pumping Potential Exposure	Double contain; Stop operations

A Hazard Identification Study (HAZID) is a similar approach to identifying hazards. A HAZID is a brainstorming approach that is common for simpler non-process facilities.

Safety in Design

LOPA

Layers of Protection Analysis (LOPA) is an assessment of a process that compares the risk rankings of failures with the robustness of safeguards in place. The goal is to determine if the safeguards are sufficient for each hazard. LOPA uses the defense in depth approach to safety, where additional layers of safeguards are added as needed based on the level of risk.

For a LOPA, the typical approach is as follows:

1. Create a table with a list of potential failures
2. Risk rank each failure based on likelihood and severity
3. Indicate the safeguards currently in place to prevent or contain the failure
4. Compare the robustness of the safeguards to the risk ranking
5. Provide recommendations for additional safeguards or design changes

Table 3: Example LOPA for a Chemical Feed System					
Process	Failure	Risk Ranking	Current Safeguards	Safeguard Robustness	Recommended Additions
Storage Tank	Overflow	High	1. High level alarm 2. Close fill valve 3. Containment curb	High	1. Vent to containment sump
	Leak in tank	High	2. Level change alarm 3. Containment curb	Medium	1. Safe access 2. Leak detection
	Level sensor failure	Medium	1. Redundant sensors 2. Deviation alarm 3. Safe Access	Medium	None
Transfer Pumps	Flow meter failure	Low	1. Alarm 2. Stop pumps w/ interlock 3. Bypass piping	Medium	None
	Blockage in pipe	Low	1. High pressure alarm 2. Relief valve	Medium	None
	Leak in pipe	High	1. Double contained 2. Safe access	Medium	1. Leak detection 2. Stop pumps w/ interlock

Safety in Design

Helpful References

American Society of Safety Engineers (2021) “Prevention Through Design”. ANSI/ASSP Z590.3

Center for Chemical Process Safety (2019) “Inherently Safer Chemical Processes: A Life Cycle Approach” 3rd Ed. Wiley.

Center for Chemical Process Safety (2001) “Layer of Protection Analysis: Simplified Process Risk Assessment”

International Electrotechnical Commission (IEC) (2016). “Hazard and Operability Studies (HAZOP studies) – Application Guide”. International Standard IEC 61882, 2.0 ed.

International Atomic Energy Association (IAEA) (1996) “Defence in Depth in Nuclear Safety”. INSAG-10.

Leveson, Nancy (2012) “Engineering a Safer World — Systems Thinking Applied to Safety”. MIT Press. Reprint Edition.

Marsden, Eric (2014) “Designing for safety”. Risk Engineering. <<https://risk-engineering.org/static/PDF/slides-design-for-safety.pdf>>

Moore, David (2019) “Implementing Inherent Safety” P2SAC Fall 2019 Conference/ Acutech Group, Inc.

Ghavanini, Emad (2021) “Layer of Protection Analysis (Lopa) Building Blocks”. Panaam. <https://panaamconsultants.com/layer-of-protection-analysis-lopa-building-blocks/>

US Department of Energy (2012) “Nonreactor Nuclear Safety Design Guide”. DOE G 420.1-1A 12-4-2012.

US Department of Defense (2012) “System Safety”. DOE Standard Practice MIL-STD-882E.