CPE/EE 322
Engineering Design VI
Lesson 9: Failure Analysis and Hazard Analysis

Kevin W. Lu

2023-04-03

Outline

1. Failures in Engineering
2. Three levels of failure
3. Dealing with hazards
4. Hazard analysis
5. Hazard avoidance

Objectives

G. Voland, Engineering by Design, Chapter 9

- Explain the three levels of failure: physical features, errors in process, and errors in perspective or attitudes
- Distinguish among such product hazards as entrapment, impact, ejection, and entanglement
- Apply hazard and operability study (HAZOP), hazards analysis (HAZAN), fault tree analysis (FTA), failure modes and effects analysis (FMEA), and Ishikawa diagrams to engineering design analysis
- Describe how exposure to hazards can be reduced through the use of guards, interlocks, and sensors, or via safety factors, quality assurance, or intentional redundancy

Lab 9 — YANG

- Study the GitHub repository Lesson 9
- Install pyang and PlantUML
- copy ~/iot/lesson9/intrusiondetection.yang to ~/demo
- Run pyang to generate intrusiondetection.yin and intrusiondetection.uml
- Run PlantUML to generate intrusiondetection.png

Assignment 9 — Failure and Hazard Analysis

Provide solutions to eliminate hazards identified in Assignment 8
9.1. Ethical issues, e.g., foreseeable misuses
9.2. Product liability, e.g., changes that may occur during the useful lifetime
9.3. Social impact, e.g., disposal after the useful life has ended

Program Outcome 4: (Ethical and Professional Conduct)
4.2 (Ethics and morals) Students will be able to understand the associated ethical issues.
4.3 (Professionalism) Students will be able to understand the associated professional responsibilities.
Program Outcome 2: (Design)
4.1 (Social issues) Students will be able to explore the non-technical space of social requirements, with a particular concern for the social impacts (both favorable and unfavorable) of their project "product."

Failures and Hazards in Engineering

- Failure analysis is a post-failure forensic or diagnostic evaluation of the factors that led to an actual design failure
- Hazard analysis is a pre-failure or preventive determination of the potentially dangerous aspects of a design that could lead to disaster
- Most potential engineering failures can be avoided if engineers perform work with care, knowledge, precision, and thought
- Engineers should strive to avoid failure and minimize hazards by
  - Expecting the unexpected, i.e., the black swan
  - Responding to warning signals, i.e., the gray rhino
  - Focusing on both the local and global aspects of a design

Failure Analysis

Three Levels of Failure

Level Three	Errors in perspective or attitude
Level Two	Errors in process
Level One	Physical flaws

Physical Flaws

- Metal fatigue
- Corrosion
- Toxicity
- Exposed moving parts
- Excessive noise or vibration
- Electrical faults
- Inadequate structural integrity, leading to collapse

Errors in Process

- The problem may be misunderstood, leading to an incorrect and potentially hazardous design solution
- The design and its implementation are based on invalid assumptions
- Errors in calculation
- Incomplete or improper data collection on which design decisions have been based
- Incorrect or faulty reasoning used to develop an engineering solution
- Miscommunication of essential information, constraints, and/or expectations
- Information overload
- Errors in manufacturing
- Errors in assembly of the final design
- Improper operation or misuse of a product by the user that might have been foreseen and prevented by the design engineer
- Failure to anticipate unexpected operating conditions or other developments
- Improper storage
- Errors in packaging
- Carelessness
- Inadequate training of personnel
- Errors in judgment

Errors in Perspective or Attitude

- Unethical or unprofessional behavior
- Inappropriate priorities, objectives, and values
- Isolation from others affected by one's work
- Lack of motivation
- Indifference and callousness to others' difficulties or needs
- Overconfidence
- Impulsive behavior or decision-making

Five Whys

- Five whys, developed by Sakichi Toyoda 1867—1930, is an iterative interrogative technique used to explore the cause-and-effect relationships underlying a particular problem
- The primary goal of the technique is to determine the root cause of a defect or problem by repeating the question "Why?" and each answer forms the basis of the next question
- The "five" in the name derives from an anecdotal observation on the number of iterations needed to resolve the problem, e.g.,
  - Why? The battery is dead
  - Why? The alternator is not functioning
  - Why? The alternator belt has broken
  - Why? The alternator belt was beyond its useful service life and not replaced
  - Why? The vehicle was not maintained according to the recommended service schedule

Root Cause Analysis (RCA)

- Root cause analysis (RCA) is a method of problem solving used for identifying the root causes of faults or problems in four steps
  - Identify and describe the problem clearly
  - Establish a timeline from the normal situation up to the time the problem occurred
  - Distinguish between the root cause and other causal factors, e.g., using event correlation
  - Establish a causal graph between the root cause and the problem
- RCA generally serves as input to a remediation process whereby corrective actions are taken to prevent the problem from recurring
  - In *Applied Problem Solving* (2014), Ivan Fantin defined the true root cause as the MIN Process that is Missing, Incomplete, or Not followed
  - A poka-yoke is any mechanism in any process that helps an equipment operator avoid (yokeru) mistakes (poka) by Shigeo Shingo 1909—1990 as part of the Toyota Production System

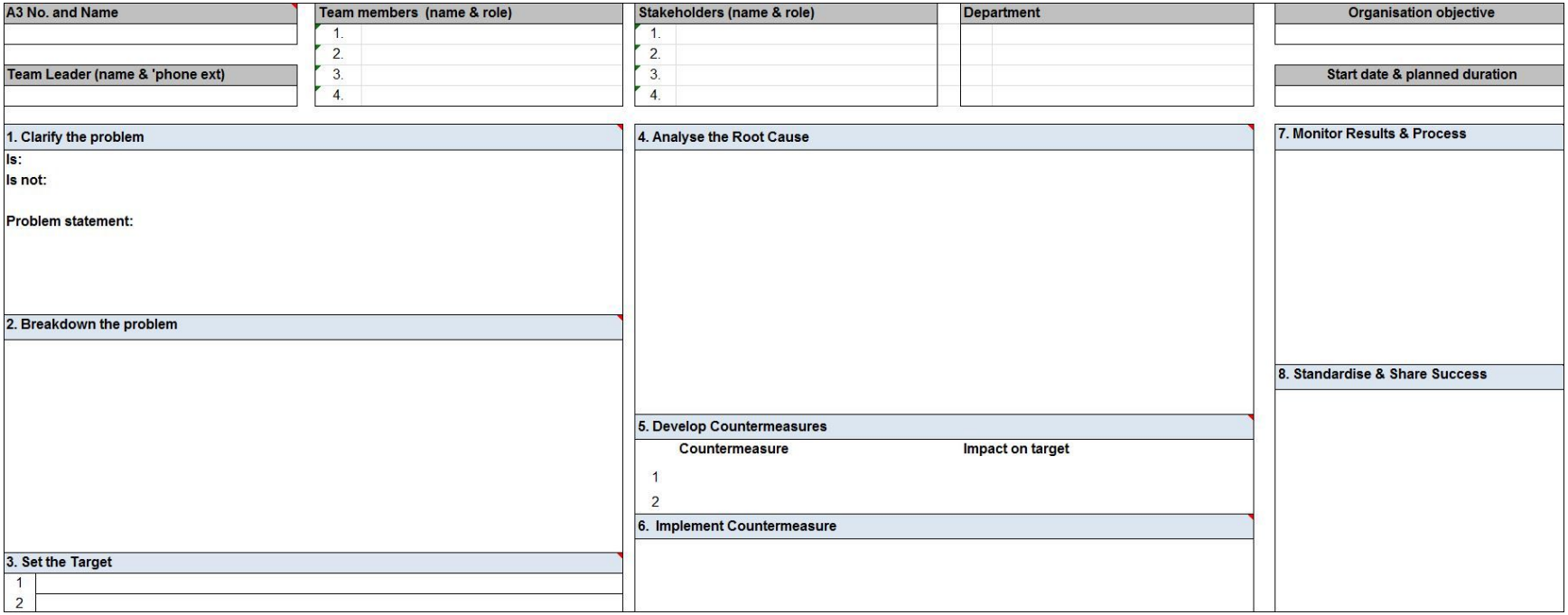
The Toyota Way

The 14 Principles of The Toyota Way in Four Sections

- Long-Term Philosophy
  - Base your management decisions on a long-term philosophy, even at the expense of short-term financial goals
- The Right Process Will Produce the Right Results
  - Create a continuous process flow to bring problems to the surface
  - Use "pull" systems to avoid overproduction
  - Level out the workload (heijunka)
  - Build a culture of stopping to fix problems, to get quality right the first time
  - Standardized tasks and processes are the foundation for continuous improvement (kaizen) and employee empowerment
  - Use visual control so no problems are hidden
  - Use only reliable, thoroughly tested technology that serves your people and processes
- Add Value to the Organization by Developing Your People
  - Grow leaders who thoroughly understand the work, live the philosophy, and teach it to others
  - Develop exceptional people and teams who follow your company's philosophy
  - Respect your extended network of partners and suppliers by challenging them and helping them improve
- Continuously Solving Root Problems Drives Organizational Learning
  - Go and see for yourself to thoroughly understand the situation (Genchi Genbutsu)
  - Make decisions slowly by consensus, thoroughly considering all options; implement decisions rapidly (nemawashi)
  - Become a learning organization through relentless reflection (hansei) and continuous improvement (kaizen)

A3 Problem Solving

A3 problem solving is a structured problem-solving and continuous-improvement approach, first employed at Toyota and typically used by lean manufacturing practitioners in a single sheet of ISO A3-size paper



Fault Tree Analysis (FTA)

	Combination event	Event (often a fault) due to a combination of more fundamental or basic component faults
	Basic fault	Component fault (usually with assignable probability of occurrence)
	Undetermined fault	Fault of undetermined causes (causes remain undetermined because of a lack of data, limited time, or lack of necessity)
	Normal event	Event that is expected to occur
	Reference key	Continuation key to another part of fault tree
	AND-gate	All input events must occur for output event to occur
	OR-gate	Any one (or more) input event(s) is sufficient to trigger output event

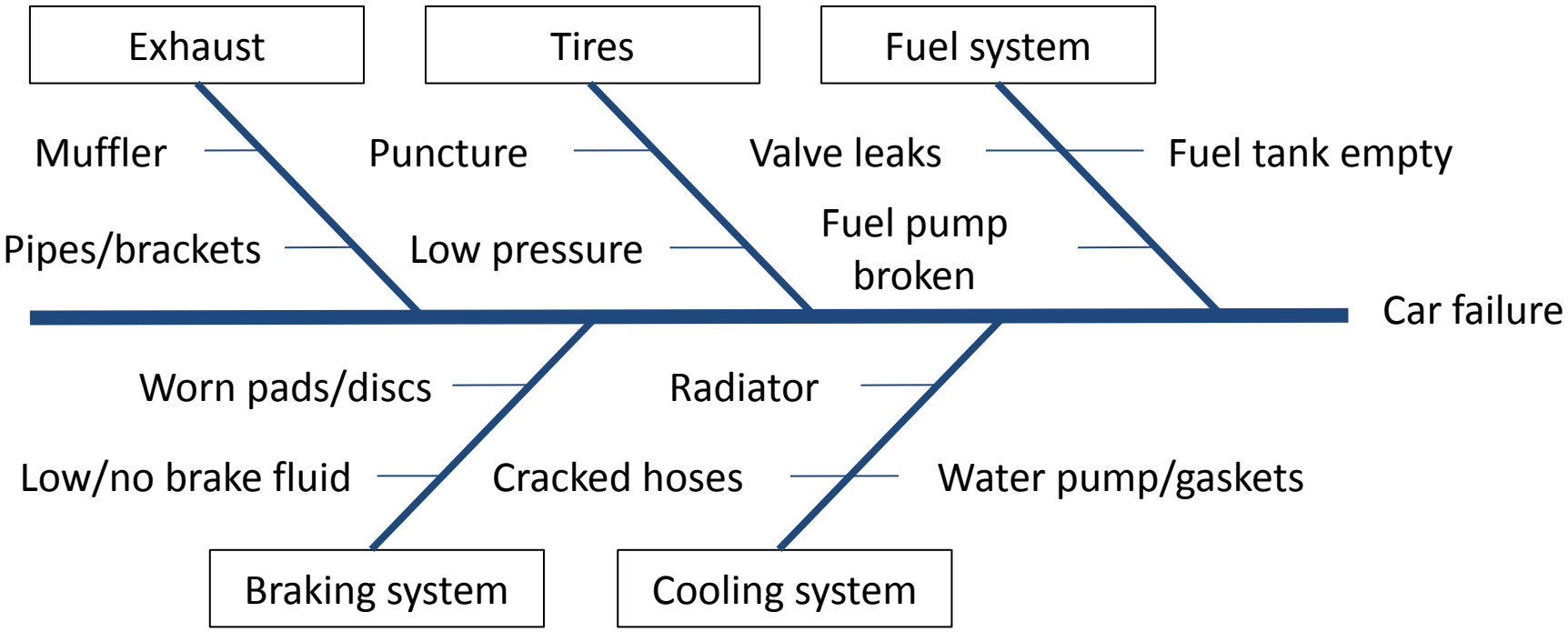
Failure Modes and Effects Analysis (FMEA)

- A combination of FTA top-down approach and FMEA bottom-up approach can be most beneficial
- For simplicity, the values for severity, frequency of occurrence, and imperilment (SFI) are not included

Part Number	Part Name	Failure Mode	Failure Cause	Identification Method	Backup Protection	Effect/ Hazard	SFI	Notes
949	Filter	Fails to control flow of coolant	Jams	System overheats	None	Fire, engine stops, Damage	—	Need warning signal and automatic
872	Rachet	Slips	Loose	Load slips	None	Supported load slips or released	—	Need backup lock/ support

Ishikawa (Fishbone) Diagnostic Diagram

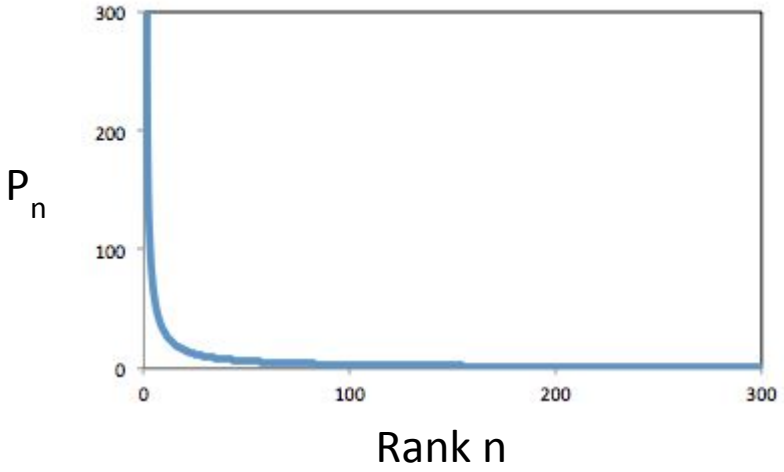
Ishikawa diagrams break down (in successive layers of detail) root causes that potentially contribute to a particular effect

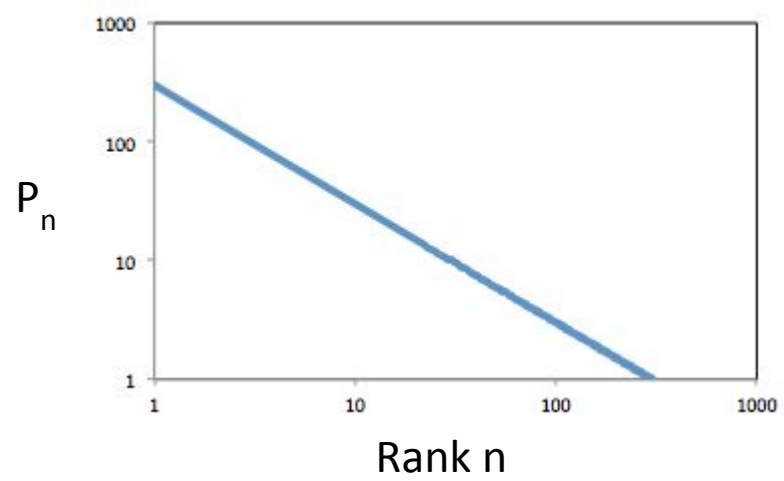


Fault Tolerance

- Fault tolerance enables a system to continue operating properly in the event of the failure of some of its components
- A Byzantine fault (from the Byzantine Generals Problem) is a condition of a computer system, particularly distributed computing systems, where components must agree on a single strategy to avoid complete failure, but some of the components are unreliable and disseminating false information
- A system with Byzantine fault tolerance (BFT) is able to resist the Byzantine faults
- Examples of BFT systems include
  - The Archistar software framework
  - The Bitcoin Proof of Work (PoW) consensus algorithm
  - The Boeing 777 Aircraft Information Management System (AIMS)
  - The SpaceX Dragon

Zipf's Law (1935)





George Kingsley Zipf 1902–1950

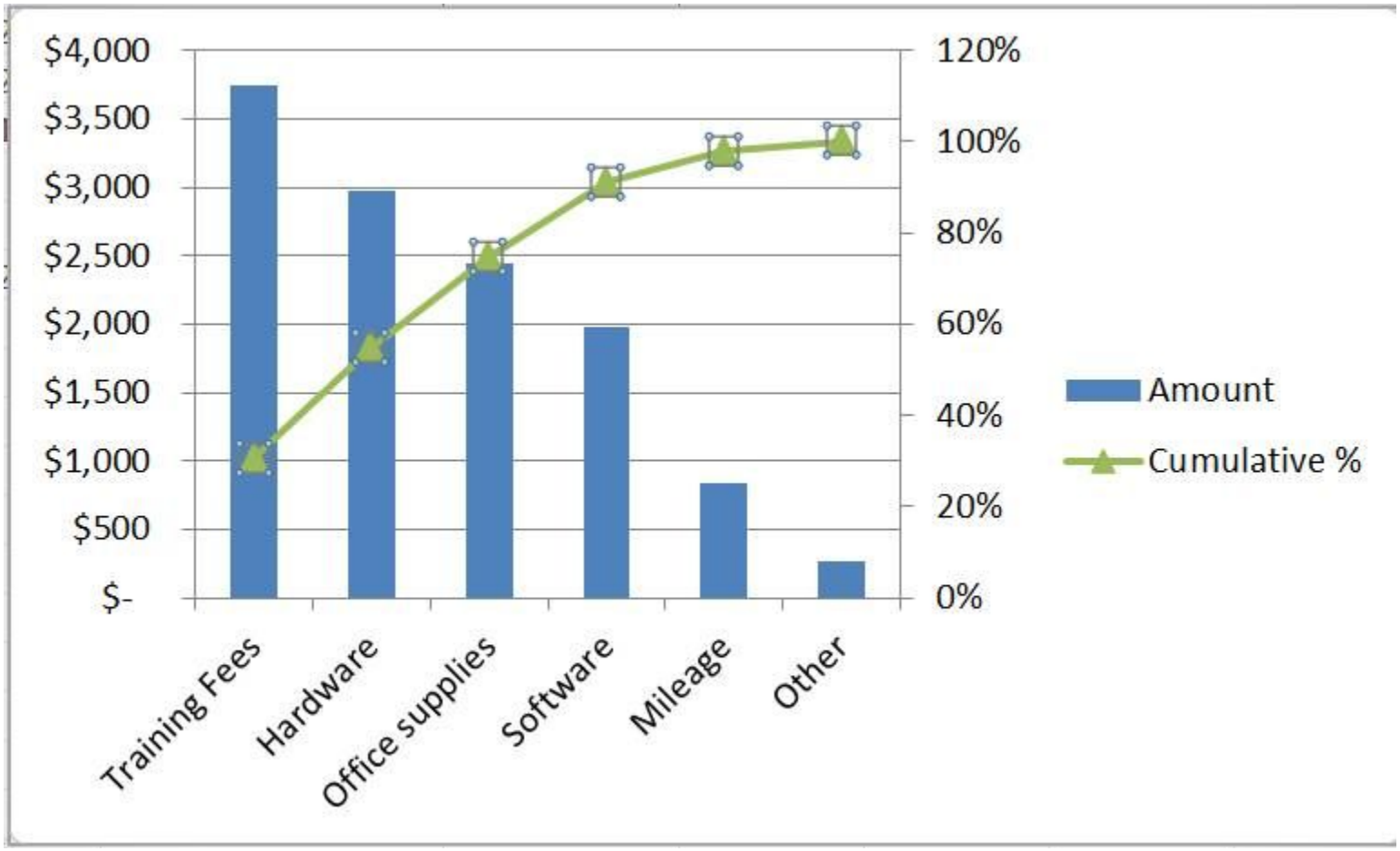
Word frequency $P_n \sim 1/n^a$, $a \sim 1$

Also called discrete Pareto distribution

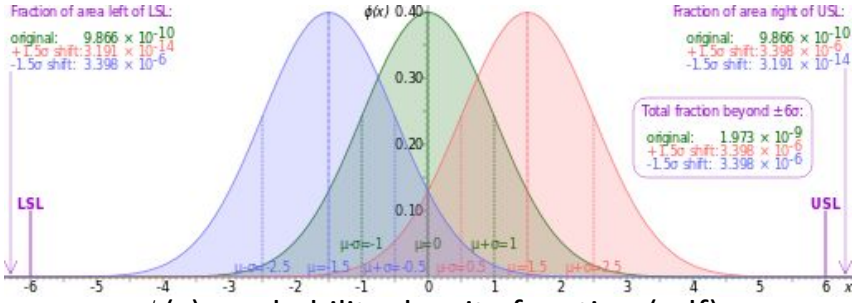
Vilfredo Pareto 1848—1923

- Vilfredo Pareto was an Italian civil engineer and economist who helped develop the field of microeconomics
- He discovered that income follows a Pareto distribution, which is a power law probability distribution
- The Pareto principle named after him, now also known for the 80/20 rule, was built on his observations such as 80% of the land in Italy owned by about 20% of the population
- The Pareto chart is a special type of histogram, used to view causes of a problem in order of severity from largest to smallest

Pareto Chart



Six Sigma



ϕ(x): probability density function (pdf)
Φ(x): cumulative distribution function (cdf)

σ	$\sigma - 1.5$	$\Phi(\sigma - 1.5)$	DPMO
1	−0.5	0.308537539	691462
2	0.5	0.691462461	308538
3	1.5	0.933192799	66807
4	2.5	0.993790335	6210
5	3.5	0.999767371	233
6	4.5	0.999996602	3.4

- SIX SIGMA® is a registered trademark and service mark of Motorola (1993)
- In Six Sigma process improvement efforts, defects per million opportunities (DPMO) is $1{,}000{,}000 \times (1 - \Phi(\sigma - 1.5))$ where Φ(x) is the process cumulative distribution function of the standard normal distribution with mean μ=0 and standard deviation σ=1
- The upper and lower specification limits (USL and LSL) are at a distance of 6σ from the mean
- Even if the mean were to move left or right by 1.5σ in the future, there is still a good safety cushion

Six Sigma Methodologies

DMAIC for improving existing business processes

- Define
- Measure
- Analyze
- Improve
- Control

DMADV for creating new product or process designs

- Define
- Measure
- Analyze
- Design
- Verify

Capability Maturity Model Integration

Level	Maturity	Characteristics
5	Optimizing	Focus on process improvement
4	Quantitatively managed	Processes measured and controlled
3	Defined	Processes characterized for the organization and is proactive
2	Managed	Processes characterized for projects and is often reactive
1	Initial	Processes unpredictable, poorly controlled and reactive

- Capability Maturity Model Integration or CMMI® is a process level improvement training and appraisal program developed at Carnegie Mellon University (CMU) and administered by the CMMI Institute, a subsidiary of ISACA (Information Systems Audit and Control Association)
- CMMI is required by many U.S. Government contracts, especially in software development
- CMMI can be used to guide process improvement across a project, division, or an entire organization for development, acquisition, or services

Hazard Analysis

Types of Hazards

Entrapment	Part of all of a person's body may be pinched or crushed as machine parts move together
Contact/Tactile	Hot surfaces, sharp edges, electrically charged elements
Impact	A person strikes a portion of an object, or a part of the device strikes the person
Ejection	Bits of material from a workpiece or loose components from a machine strike a person
Entanglement	A person's clothing or hair can become entangled in a device
Noise and vibration	Can cause loss of hearing, tactile sense, or fatigue

Dealing With Hazards

Step 1	Review existing standards
Step 2	Identify known hazards
Step 3	Identify unknown hazards
Step 4	Determine characteristics of hazards
Step 5	Eliminate or minimize hazards

Hazard and Operability (HAZOP) Study

Hazard and operability study is a qualitative yet systematic approach

- Consider any deviations from the desired system performance that may occur
  - What if there is more waste from the process than is acceptable?
  - What if there is less deceleration than necessary?
  - What if there is no power output?
  - What if there is behavior exhibited by the system other than what is expected?
- Identify consequences of such deviations
  - Will someone be harmed? Who? In what way? How severely?
  - Will the product's performance be reduced? In what way? How severely? What will be the effect of such a reduction in performance?
  - Will costs increase? By how much?
  - Could there be a cascading effect in which this one deviation leads to another? What, specifically, is this cascading effect?
- Identify causes for such deviations
- Develop specific actions to eliminate or minimize the deviations

Hazard Analysis (HAZAN)

- Hazard analysis is quantitative in nature
- Identify the most effective way in reducing the threat of hazards within a design
- Estimate the frequency and severity of each threat and develop an appropriate response to these threats
  - How often?
  - How big?
  - So what?
- Severity scale or severity-frequency-imperilment (SFI)
  - Level 1: Minor repairs necessary, no injuries or property loss
  - Level 2: Major repairs necessary, no injuries or property loss
  - Level 3: Some property loss, no injuries
  - Level 4: Minor injuries and/or large property loss
  - Level 5: Major injuries
  - Level 6: Death or multiple major injuries
  - Level 7: Multiple deaths

Hazard Avoidance

It is always preferable to eliminate the hazard from the design if possible; otherwise, reduce the exposure of the user to the hazard by

- Using appropriate guards, sensors, interlocks, and other mechanisms to distance the user from the hazard
  - Avoid malware from opening infectious links or attachments
- Increasing the safety factor for the design
  - Safety factors are used to ensure that engineering designs will be able to withstand expected loads when in operation
- Using quality assurance efforts, including appropriate tests, to minimize the number of defective units that enter the marketplace
- Incorporating redundancy into the design
  - Routinely test backups for operability and data integrity
- The use of warnings that is the least effective approach to hazard reduction and should be used only as a last resort or in combination with other approaches
  - Non-traffic safety signs as opposed to traffic warning signs

Marine Safety Code

- Continued disasters and high loss of life prompted congressional action through the passage of the Act of February 28, 1871 applied to all steam vessels and sought to protect their crews as well as their passengers
- It retained the useful functions of the Act of 1838 and the Steamboat Act of May 30, 1852, and added new requirements that provided a comprehensive Marine Safety Code, which forms the basis of the present marine safety code
- The Act of 1871 created the Steamboat Inspection Service that was merged with the Bureau of Navigation in 1932 to form the Bureau of Navigation and Steamboat Inspection, reorganized into the Bureau of Marine Inspection and Navigation in 1936, temporarily transferred to the US Coast Guard in 1942, and permanently transferred to the Coast Guard in 1946
- It established a Supervisory Inspector General directly responsible to the US Secretary of the Treasury, extended licensing requirements to all masters and chief mates, provided for the revocation of licenses, authorized periodic inspection, and gave the Board of Supervisory Inspectors the authority to prescribe nautical rules of the road

Automotive Safety Integrity Level

- Automotive Safety Integrity Level (ASIL) is a risk classification scheme defined by the ISO 26262 - Functional Safety for Road Vehicles standard
- ASIL is an adaptation of the Safety Integrity Level (SIL) used in IEC 61508 for the automotive industry
- ASIL is established by performing a risk analysis of a potential hazard by looking at the severity, exposure, and controllability of the vehicle operating scenario
- There are four ASILs identified by the standard: ASIL A, ASIL B, ASIL C, and ASIL D
- ASIL D dictates the highest integrity requirements on the product and ASIL A the lowest

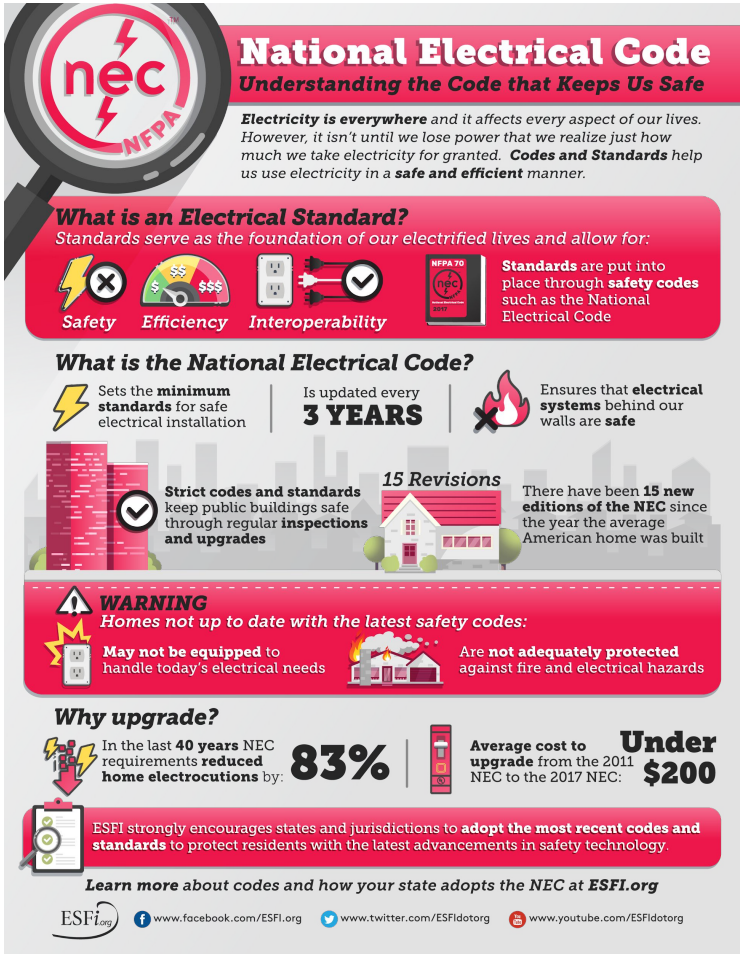
  Risk=(*expected loss in case of the accident*)×(*probability of the accident occurring*)

  ASIL=*Severity* × (*Exposure* × *Controllability*)
- The level QM (quality measurement) means that risk associated with a hazardous event is not unreasonable and does not therefore require safety measures in accordance with ISO 26262

International Building Code

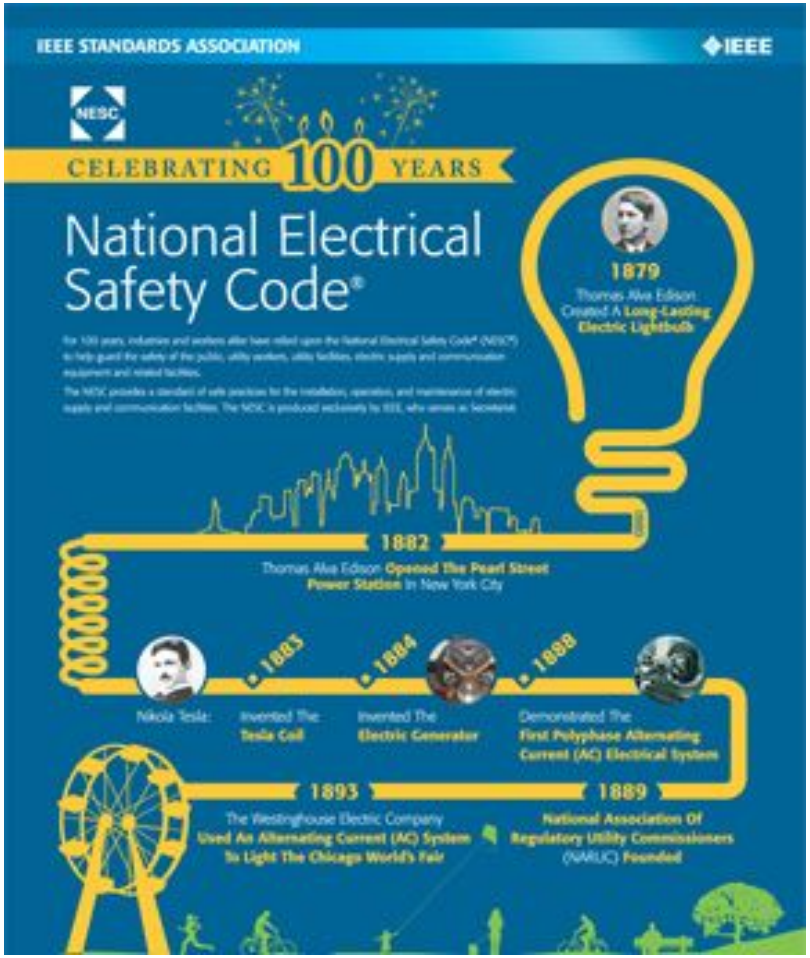
- The International Building Code (IBC) establishes minimum requirements for building systems using prescriptive and performance-related provisions
- It is founded on broad-based principles that make possible the use of new materials and new building designs
- The International Code Council (ICC) promulgates a new International Building Code every three years through the ICC Code Development Process
- The current version of the IBC is the 2021 edition, also known as ICC IBC-2021 (cf. 2018 edition) that is fully compatible with all of the International Codes (I-Codes) published by the International Code Council (ICC)
- The I-Codes are used in a variety of ways in both the public and private sectors
- Most industry professionals are familiar with the I-Codes as the basis of laws and regulations in communities across the U.S. and in other countries

National Electrical Code



- First published in 1897, the National Electrical Code (NEC), or NFPA 70, is a regionally adoptable standard for the safe installation of electrical wiring and equipment in the U.S.
- It is part of the National Fire Code series published by the National Fire Protection Association (NFPA)
- A ground fault circuit interrupter (GFCI) is required for all receptacles in wet locations defined in the Code
- As of 1962, the NEC required that new 120 Volt household receptacle outlets, for general purpose use, be both grounded and polarized — NEMA connectors implement these requirements

National Electrical Safety Code



- The National Electrical Safety Code (NESC) or ANSI Standard C2 is published by the IEEE since August 1914, currently on a 5-year cycle
- It's a United States standard of the safe installation, operation, and maintenance of electric power and communication utility systems including power substations, power and communication overhead lines, and power and communication underground lines
- Urgent safety matters that require a change in between code editions are handled through a Tentative Interim Amendment (TIA) process

Motor Vehicle Safety Standards

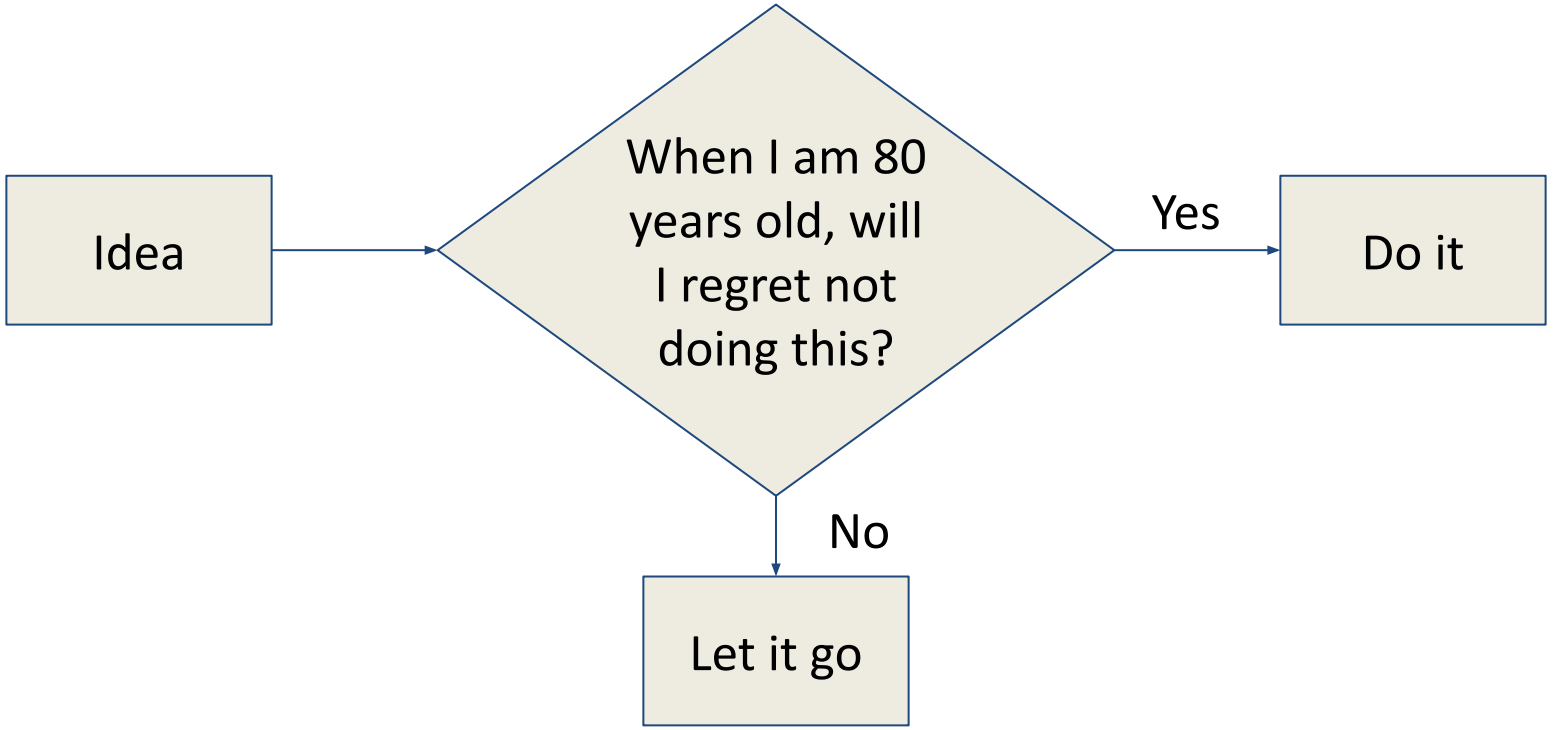
- The U.S. National Highway Traffic Safety Administration (NHTSA) develops and enforces the Federal Motor Vehicle Safety Standards (FMVSS) that are the U.S. federal regulations specifying design, construction, performance, and durability requirements for motor vehicles and regulated automobile safety-related components, systems, and design features
- FMVSS are divided into three categories: crash avoidance (100-series), crashworthiness (200-series), and post-crash survivability (300-series)
- The first regulation, FMVSS 209 Seat Belt Assemblies, was adopted on 1967-03-01 and remains in force to date though its requirements have been periodically updated and made more stringent
- NHTSA amended FMVSS 208 Occupant Crash Protection on 1984-07-11 to require cars produced after 1989-04-01 to be equipped with a passive restraint (seat belt, airbag) for the driver
- NHTSA has mandated Anti-lock Braking System (ABS) and Electronic Stability Control (ESC) under the provisions of FMVSS 126 as of 2013-09-01

Regrettable Inventions

- Thomas Midgley Jr. 1889—1944 was an American mechanical engineer and chemist in a team led by Charles F. Kettering 1876—1958 that developed the tetraethyllead (TEL) additive to gasoline and some of the first chlorofluorocarbons (CFCs) as refrigerants, propellants in aerosol applications, and solvents
- These inventions and products led to the release of large quantities of neurotoxic lead in the environment and the ozone-depleting and greenhouse gas effects of CFCs in the atmosphere

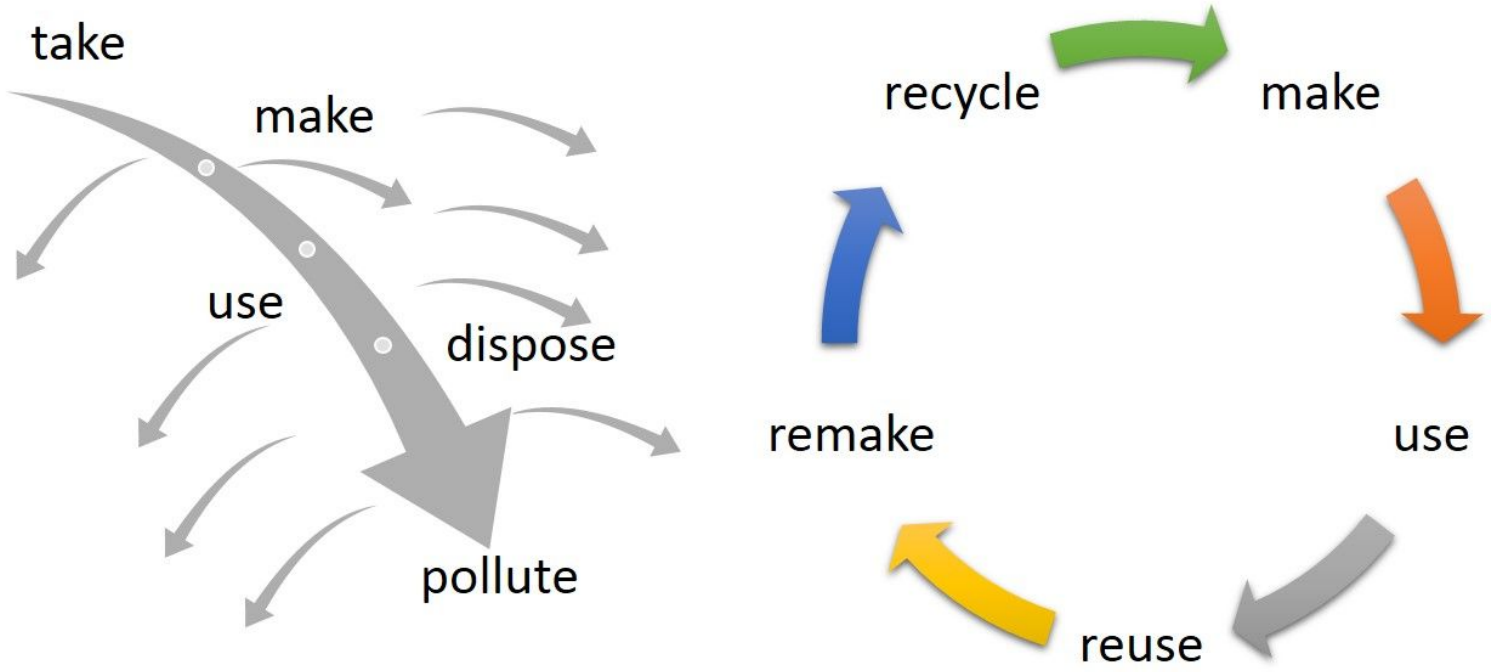
Regret Minimization Framework

Jeff Bezos left D. E. Shaw & Co, L.P. and founded Amazon.com, Inc. on 1994-07-05



Circular Economy

The regenerative approach to a [circular economy] is in contrast to the traditional linear economy, which has a 'take, make, dispose' model of production



A Circular Economy Handbook for Business and Supply Chains: Repair, Remake, Redesign, Rethink [Link]

SecDevOps

- SecDevOps is the process of integrating secure development best practices and methodologies into development and deployment processes

Chaos Engineering

- Chaos engineering is the discipline of experimenting on a software system in production in order to build confidence in the system's capability to withstand turbulent and unexpected conditions
- The Simian Army is a suite of tools developed by Netflix to test the reliability, security, or resiliency of its Amazon Web Services infrastructure, e.g., Chaos Monkey in 2011 to test the resilience of its information technology (IT) infrastructure, and 10-18 Monkey to detect problems with localization and internationalization (l10n-i18n)

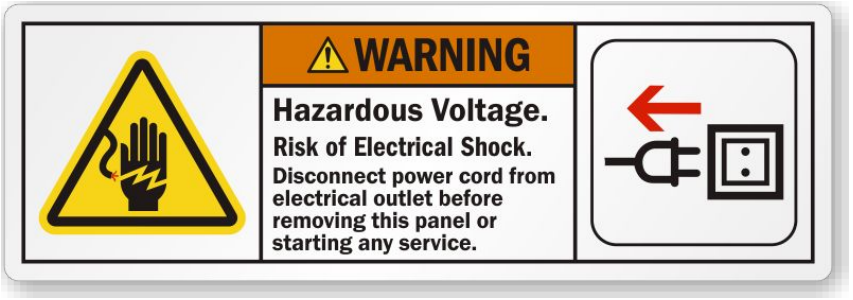
Occupational Safety and Health

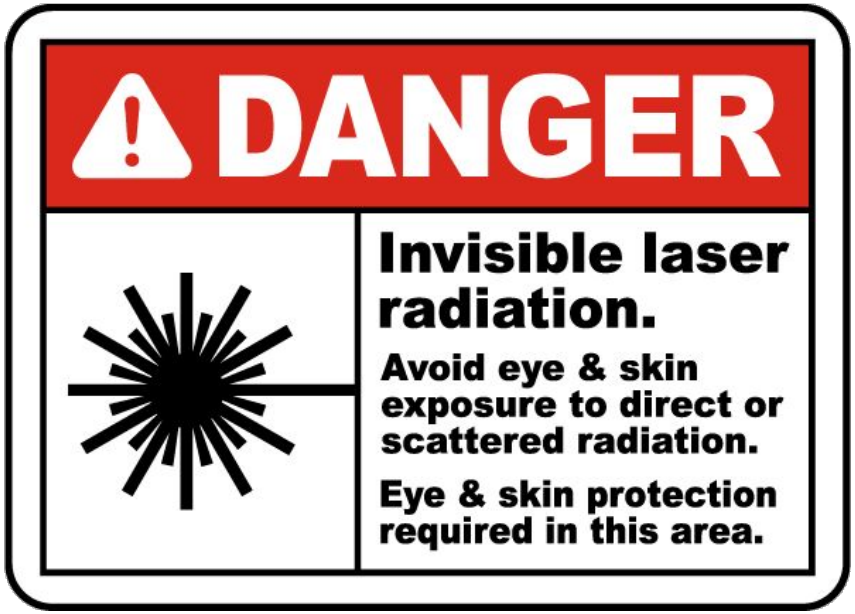
- The goal of occupational safety and health (OSH) programs is to foster a work environment that protects co-workers, family members, and customers
- The Occupational Safety and Health Administration (OSHA) is an agency of the U.S. Department of Labor (DOL) as of 1971-04-28
- The National Institute for Occupational Safety and Health (NIOSH) is part of the Centers for Disease Control and Prevention (CDC) within the U.S. Department of Health and Human Services (HHS) responsible for conducting research and making recommendations for the prevention of work-related injury and illness
- There is continued use of asbestos in some developing countries where asbestos-related disease is expected to continue to be a significant problem
- The World Health Organization (WHO) international electromagnetic fields (EMF) project has been established to assess health and environmental effects of exposure to static and time varying electric and magnetic fields in 0-300 GHz
- Nanotechnology presents a new set of challenges in the near future to rethink contemporary measures to safeguard the health of employees against a nanoparticle that most conventional controls have not been designed to manage

Personal Protective Equipment

- The purpose of personal protective equipment (PPE) is to reduce employee exposure to hazards when engineering controls and administrative controls are not feasible or effective to reduce these risks to acceptable levels
- PPE is needed when there are hazards present, and has the serious limitation that it does not eliminate the hazard at the source and may result in employees being exposed to the hazard if the equipment fails
- PPE is protective clothing, helmets, goggles, or other garments or equipment designed to protect the wearer's body from injury or infection including physical, electrical, heat, chemicals, biohazards, and airborne particulate matter
- Protective equipment may be worn for job-related occupational safety and health purposes, as well as for sports and other recreational activities
    - Protective clothing is applied to traditional categories of clothing
    - Protective gear applies to items such as pads, guards, shields, and masks
    - The severe acute respiratory syndrome-related coronavirus particle is 80-90 nm in size, whereas an N95 respirator blocks at least 95 percent of 300 nm test particles — Reference by the U.S. Food and Drug Administration (FDA)

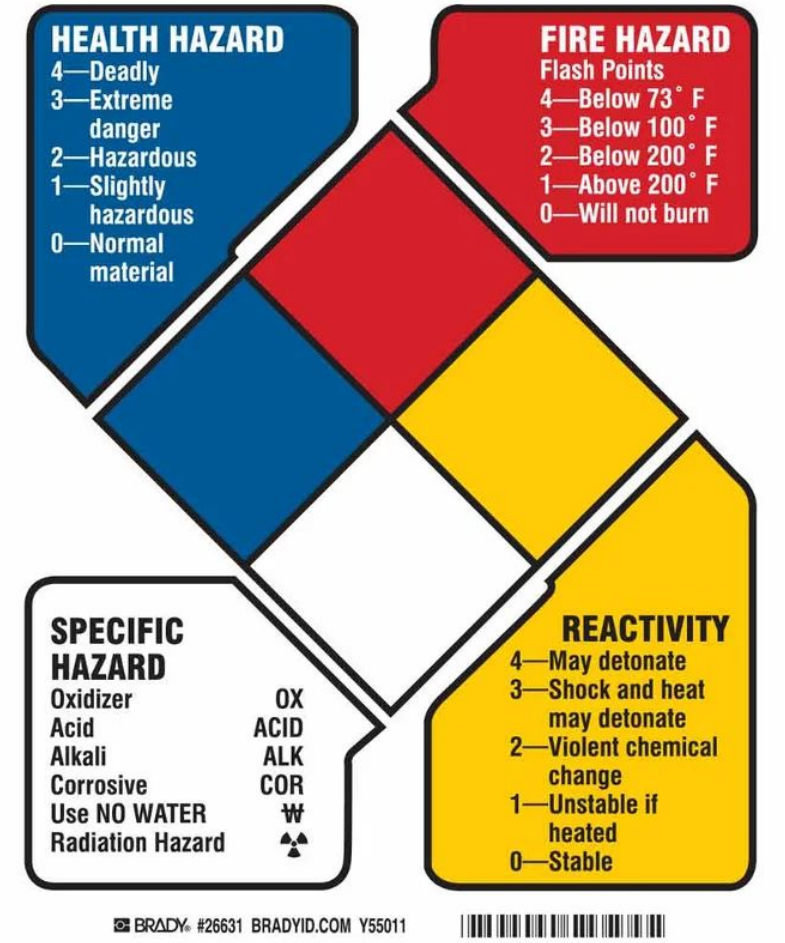
Warnings as a Last Resort



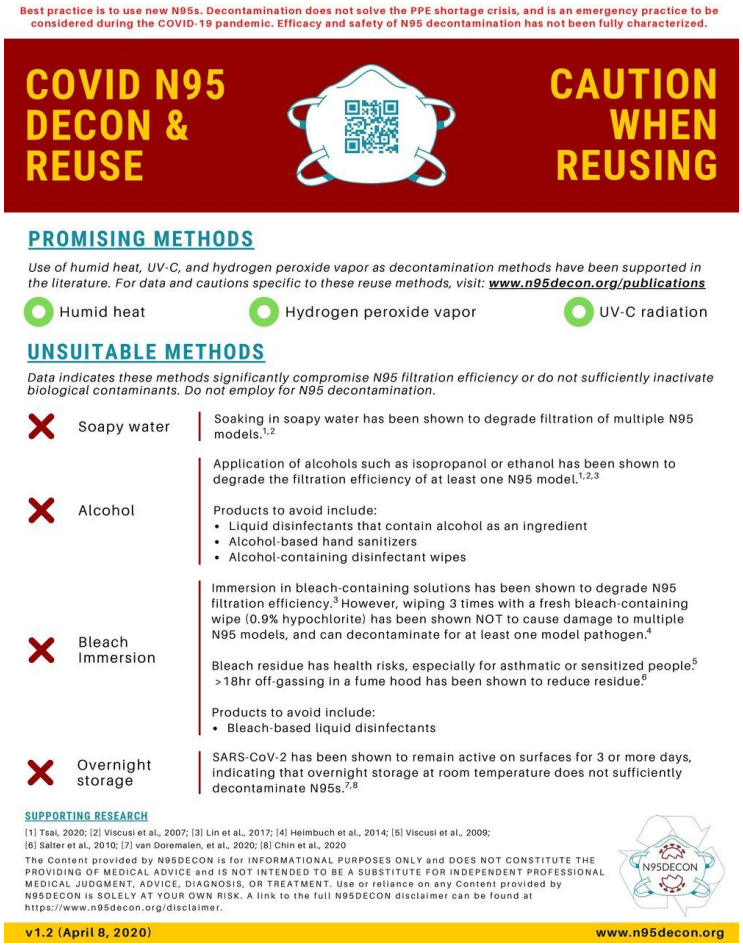


Safety Square or Fire Diamond

NFPA 704, Perfluorooctanoic Acid (PFOA)



Disclaimers



Best practice is to use new N95s. Decontamination does not solve the PPE shortage crisis, and is an emergency practice to be considered during the COVID-19 pandemic. Efficacy and safety of N95 decontamination has not been fully characterized.

COVID N95 DECON & REUSE — **CAUTION WHEN REUSING**

PROMISING METHODS

Use of humid heat, UV-C, and hydrogen peroxide vapor as decontamination methods have been supported in the literature. For data and cautions specific to these reuse methods, visit: www.n95decon.org/publications

- Humid heat
- Hydrogen peroxide vapor
- UV-C radiation

UNSUITABLE METHODS

Data indicates these methods significantly compromise N95 filtration efficiency or do not sufficiently inactivate biological contaminants. Do not employ for N95 decontamination.

- **Soapy water** — Soaking in soapy water has been shown to degrade filtration of multiple N95 models.[1,2]
- **Alcohol** — Application of alcohols such as isopropanol or ethanol has been shown to degrade the filtration efficiency of at least one N95 model.[1,2,3]
  Products to avoid include:
  - Liquid disinfectants that contain alcohol as an ingredient
  - Alcohol-based hand sanitizers
  - Alcohol-containing disinfectant wipes
- **Bleach Immersion** — Immersion in bleach-containing solutions has been shown to degrade N95 filtration efficiency.[3] However, wiping 3 times with a fresh bleach-containing wipe (0.9% hypochlorite) has been shown NOT to cause damage to multiple N95 models, and can decontaminate for at least one model pathogen.[4]
  Bleach residue has health risks, especially for asthmatic or sensitized people.[5]
  >18hr off-gassing in a fume hood has been shown to reduce residue.[6]
  Products to avoid include:
  - Bleach-based liquid disinfectants
- **Overnight storage** — SARS-CoV-2 has been shown to remain active on surfaces for 3 or more days, indicating that overnight storage at room temperature does not sufficiently decontaminate N95s.[7,8]

SUPPORTING RESEARCH

[1] Tsai, 2020; [2] Viscusi et al., 2007; [3] Lin et al., 2017; [4] Heimbuch et al., 2014; [5] Viscusi et al., 2009; [6] Salter et al., 2010; [7] van Doremalen, et al., 2020; [8] Chin et al., 2020

The Content provided by N95DECON is for INFORMATIONAL PURPOSES ONLY and DOES NOT CONSTITUTE THE PROVIDING OF MEDICAL ADVICE and IS NOT INTENDED TO BE A SUBSTITUTE FOR INDEPENDENT PROFESSIONAL MEDICAL JUDGMENT, ADVICE, DIAGNOSIS, OR TREATMENT. Use or reliance on any Content provided by N95DECON is SOLELY AT YOUR OWN RISK. A link to the full N95DECON disclaimer can be found at https://www.n95decon.org/disclaimer.

N95DECON

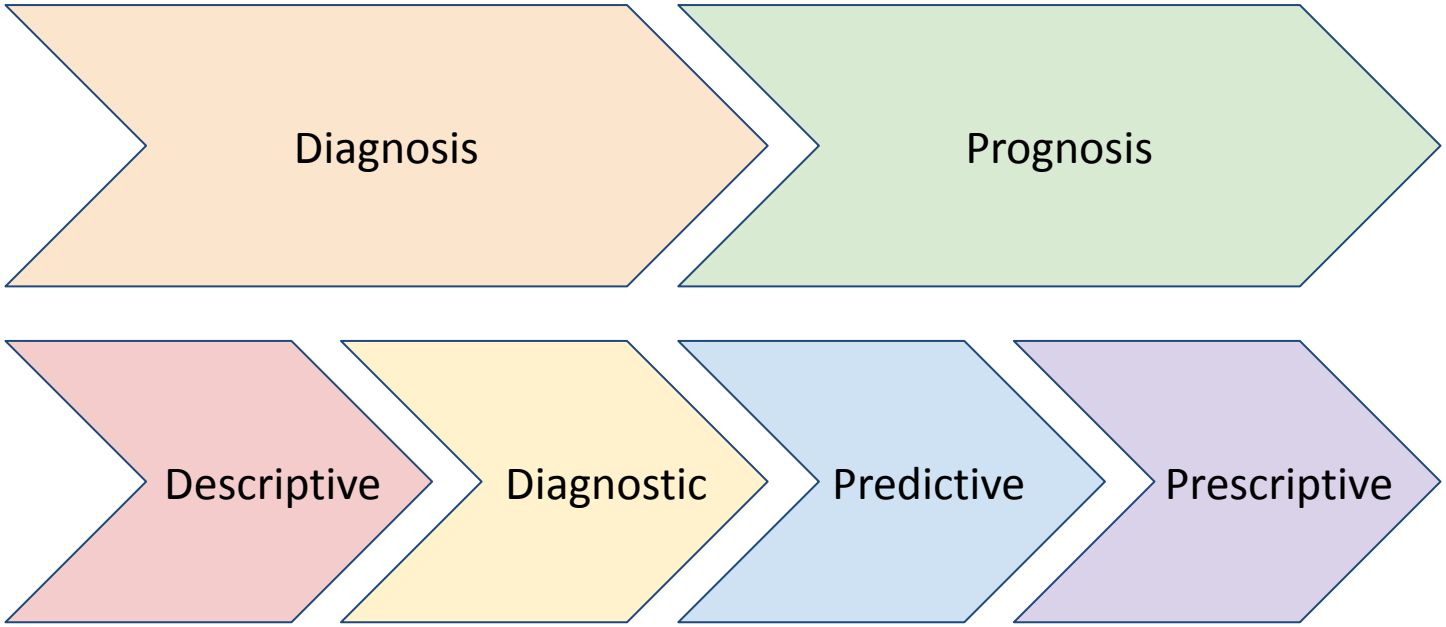
v1.2 (April 8, 2020) www.n95decon.org

- A disclaimer denies responsibility
- N95DECON is scientific consortium for data-driven study of N95 filtering facepiece respirator decontamination
- Best practice is to use new N95s
- Decontamination does not solve the PPE shortage crisis, and is an emergency practice to be considered during the COVID-19 pandemic
- Efficacy and safety of N95 decontamination has not been fully characterized
- Use of humid heat, vaporized hydrogen peroxide (VHP), and ultraviolet germicidal irradiation (UVGI) as decontamination methods have been supported in the literature (see the N95DECON disclaimer)

Lesson 9 Summary

- Commercial products should be evaluated for hazards such as entrapment, contact/tactile, impact, ejection, entanglement, and noise and vibration
- Root cause analysis (RCA), fault tree analysis (FTA), and failure modes and effects analysis (FMEA) can be used to enhance the quality and safety of engineering designs
- It is best to eliminate a hazard if at all possible; otherwise, reduce the exposure of the user to the hazard by
  - Using appropriate guards, sensors, interlocks, and other mechanisms to distance the user from the hazard
  - Increasing the safety factor for the design
  - Using quality assurance efforts, including appropriate tests, to minimize the number of defective units that enter the marketplace
  - Incorporating redundancy into the design
  - The use of warnings that is the least effective approach to hazard reduction and should be used only as a last resort or in combination with other approaches

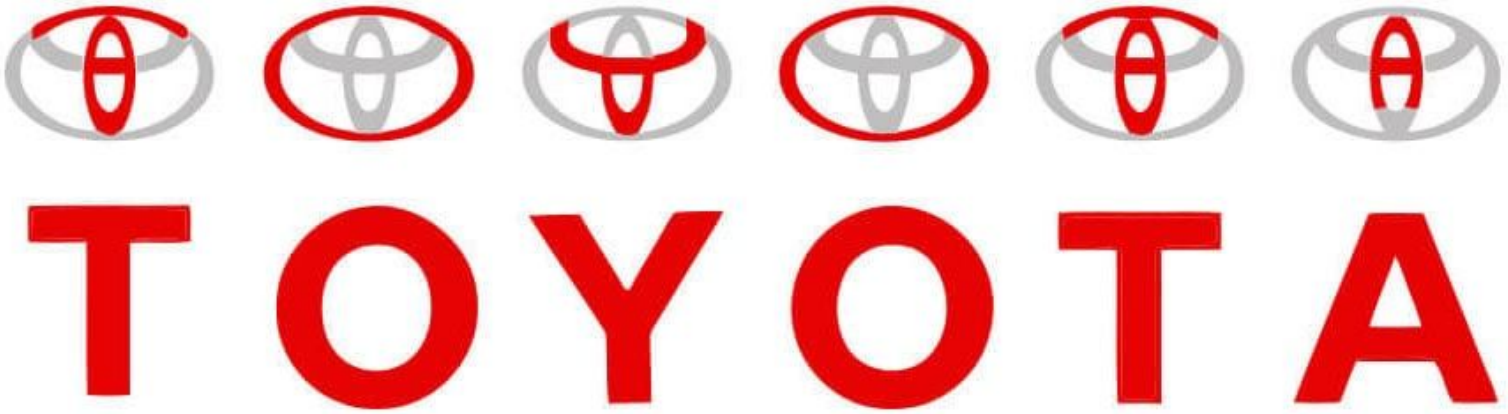
Types of Data Analysis



Hindsight: What has happened?	Insight: Why did it happen?	Foresight: What could happen?	Oversight: What needs to happen?

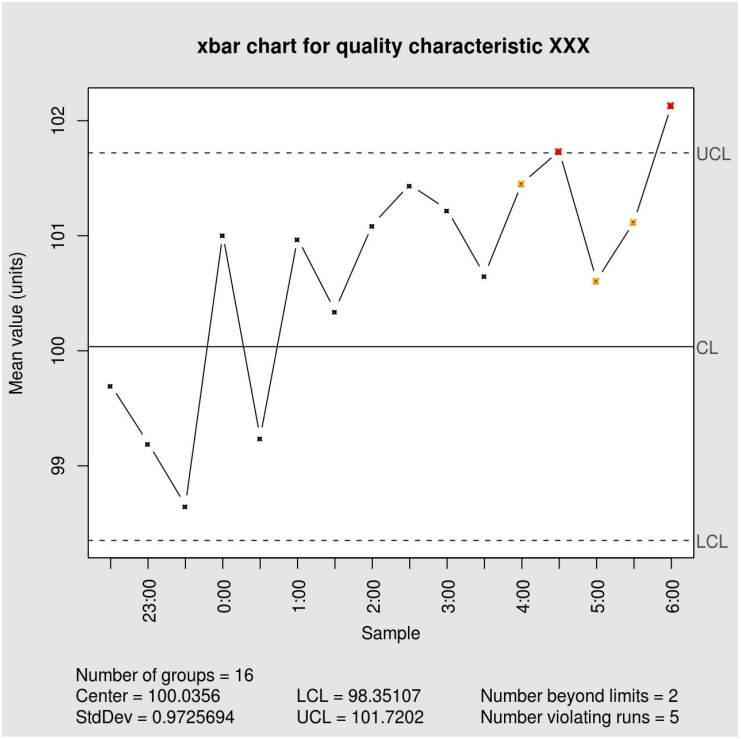
Toyota Logo

- Toyota Motor Corporation was founded in 1937 by Kiichiro Toyoda 1894—1952, as a spinoff to manufacture automobiles from his father's company Toyota Industries, a manufacturer of automatic looms and forklift trucks
- The Toyota logo has two perpendicular ovals inside an outer oval that refer to each letter of the name and offer a lot of meanings to the curious eye
- The stylized image symbolizes the steering wheel of a vehicle and the eye of a needle with a thread passed through it, hinting at the company's origin of producing weaving machines



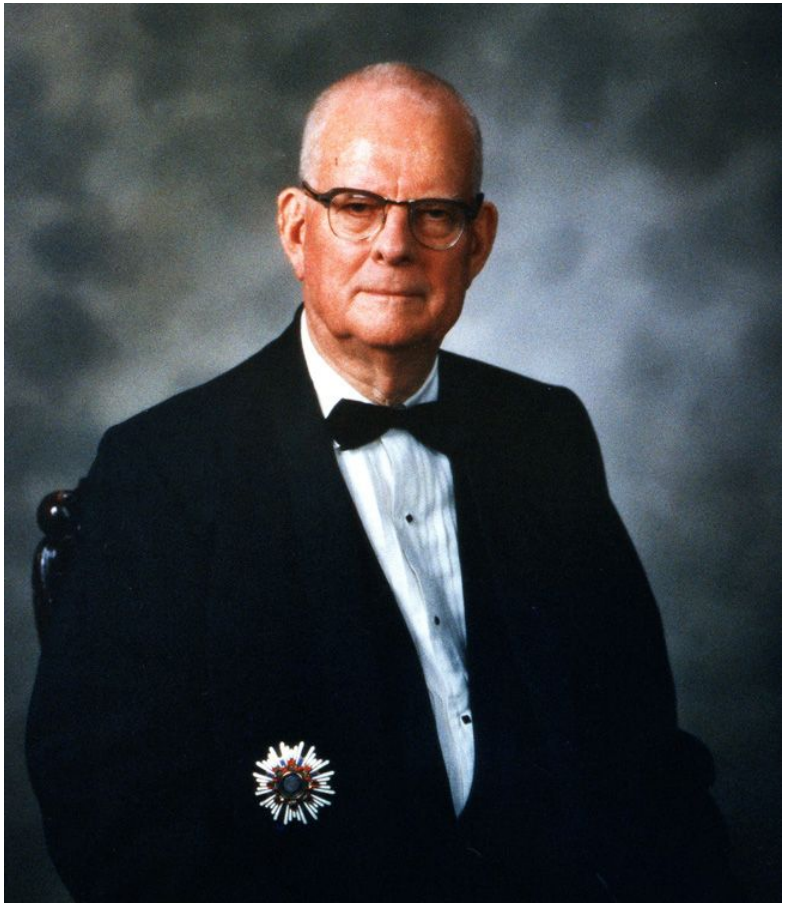
Walter A. Shewhart 1891—1967

At Bell Labs in 1924, Shewhart created the basis for the control chart and the concept of statistical process control



W. Edwards Deming 1900—1993

The W. Edward Deming Institute



In August 1950, Deming delivered a speech on "Statistical Product Quality Administration" at Mt. Hakone Convention Center in Tokyo where Deming presented the ideas that influenced industry leaders, engineers, managers, and scholars:

- Better design of products to improve service
- Higher level of uniform product quality
- Improvement of product testing in the workplace and in research centers
- Greater sales through global markets

"If you can't describe what you are doing as a process, you don't know what you're doing."
"It is not enough to do your best; you must know what to do, and then do your best."

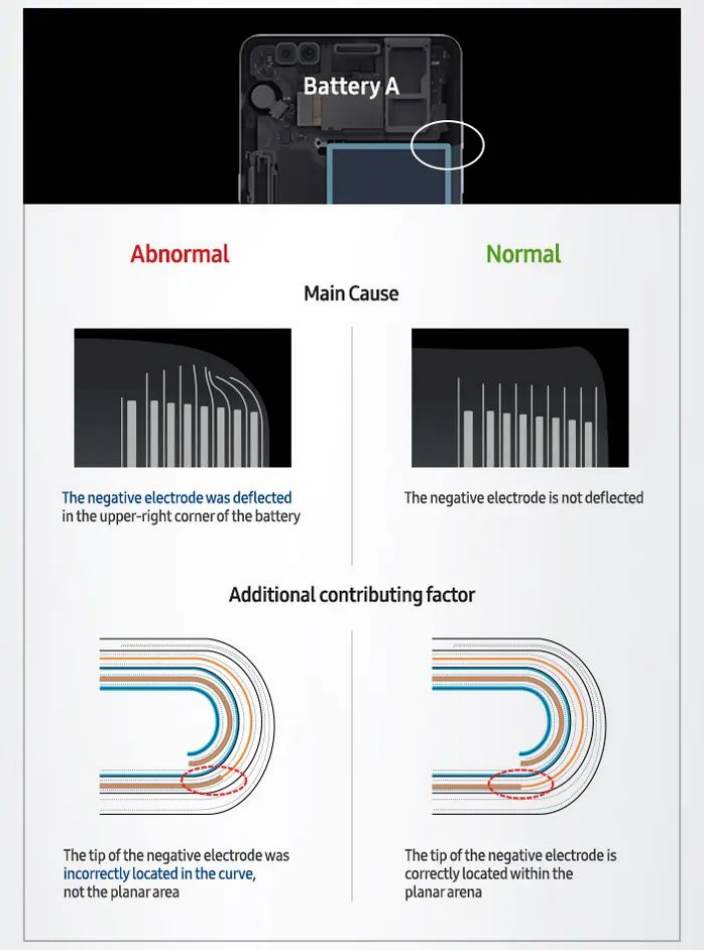
Kaoru Ishikawa 1915—1989

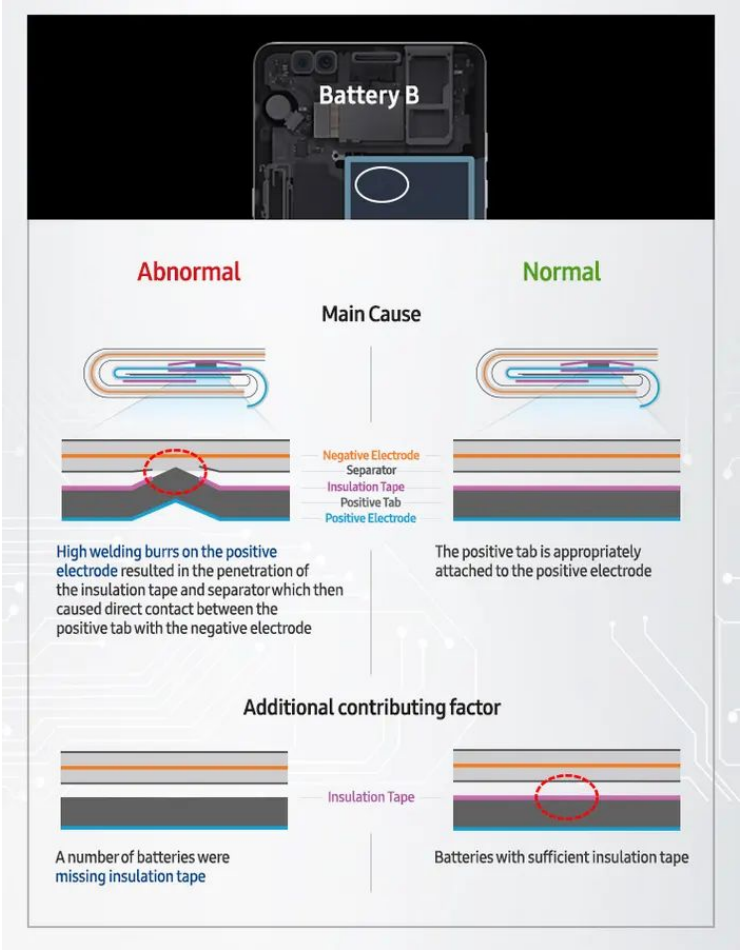
Quality throughout a product's life cycle, not just during production

- Ishikawa expanded W. Edwards Deming's Plan-Do-Check-Act (PDCA) model into the following six steps:
  - Determine goals and targets
  - Determine methods of reaching goals
  - Engage in education and training
  - Implement work
  - Check the effects of implementation
  - Take appropriate action
- Seven basic tools of quality: check sheet, control chart, stratification (alternatively, flowchart or run chart), Pareto chart, histogram, cause-and-effect (fishbone or Ishikawa) diagram, and scatter diagram
- Standards are not the ultimate source of decision making; customer satisfaction is

Battery Failure

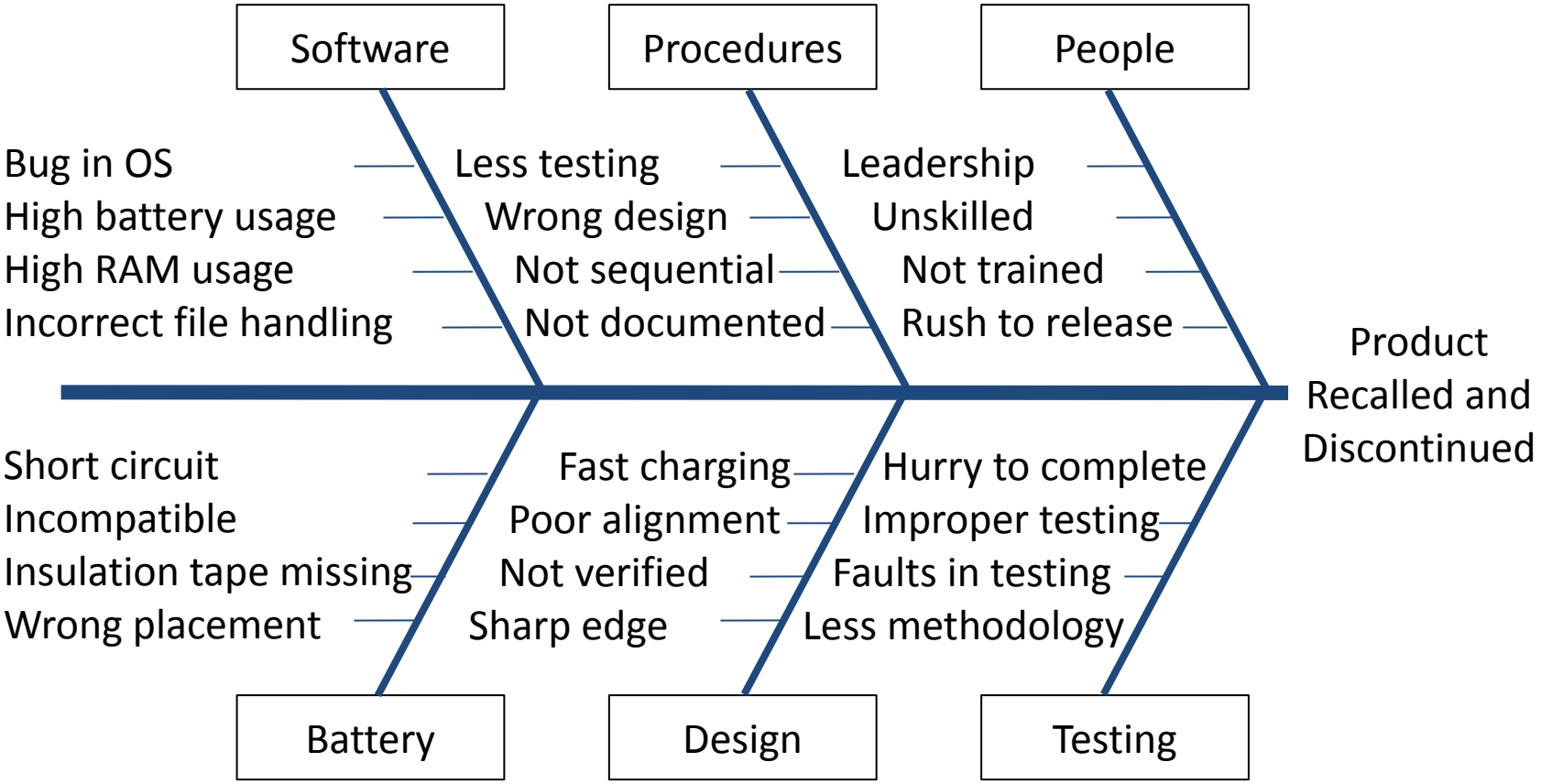
[Samsung Galaxy Note 7]





Product Recall

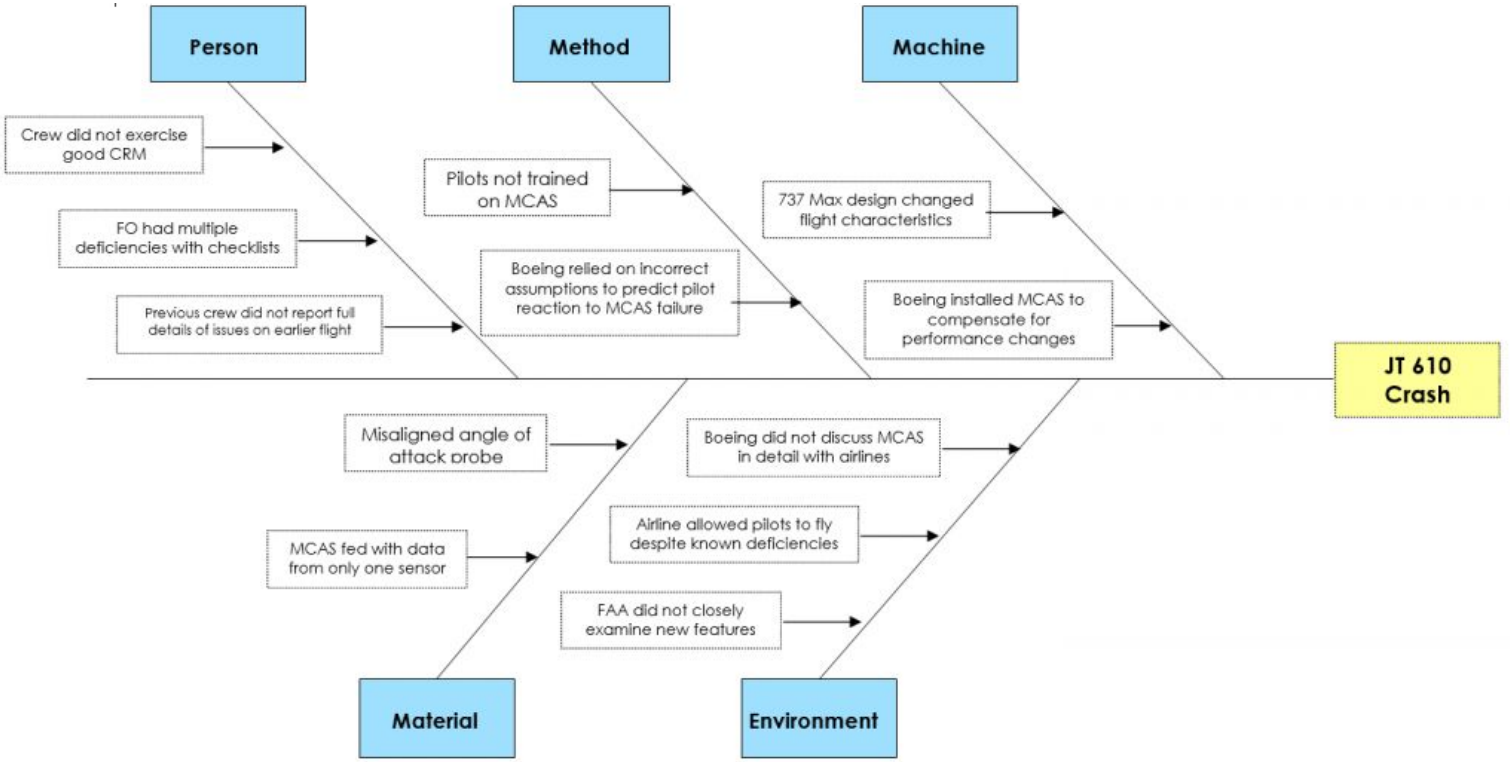
[Samsung Galaxy Note 7 Recall Case Analysis]



Aircraft Crash

The Embry-Riddle Avion Newspaper

On 2018-10-29, a Boeing 737 MAX of the Indonesian airline Lion Air Flight 610 from Jakarta to Pangkal Pinang crashed into the Java Sea 13 minutes after takeoff, killing all 189 passengers and crew



Electric Scooter Geofencing

Scooter Speed Zones

Beginning March 26th, Bird, Jump, Lime, and Lyft will use geofencing to implement a maximum acceleration of 8 mph on their scooters in defined areas of campus

Safety Tips

Wear a helmet and follow other safety guidance

Operate at a low speed in the presence of pedestrians

Ride scooters only where bicycle traffic is allowed

KEY

- City of Austin - 15 mph
- UT Campus - 15 mph
- Under review - proposed 8 mph
- Inner Campus - 8 mph

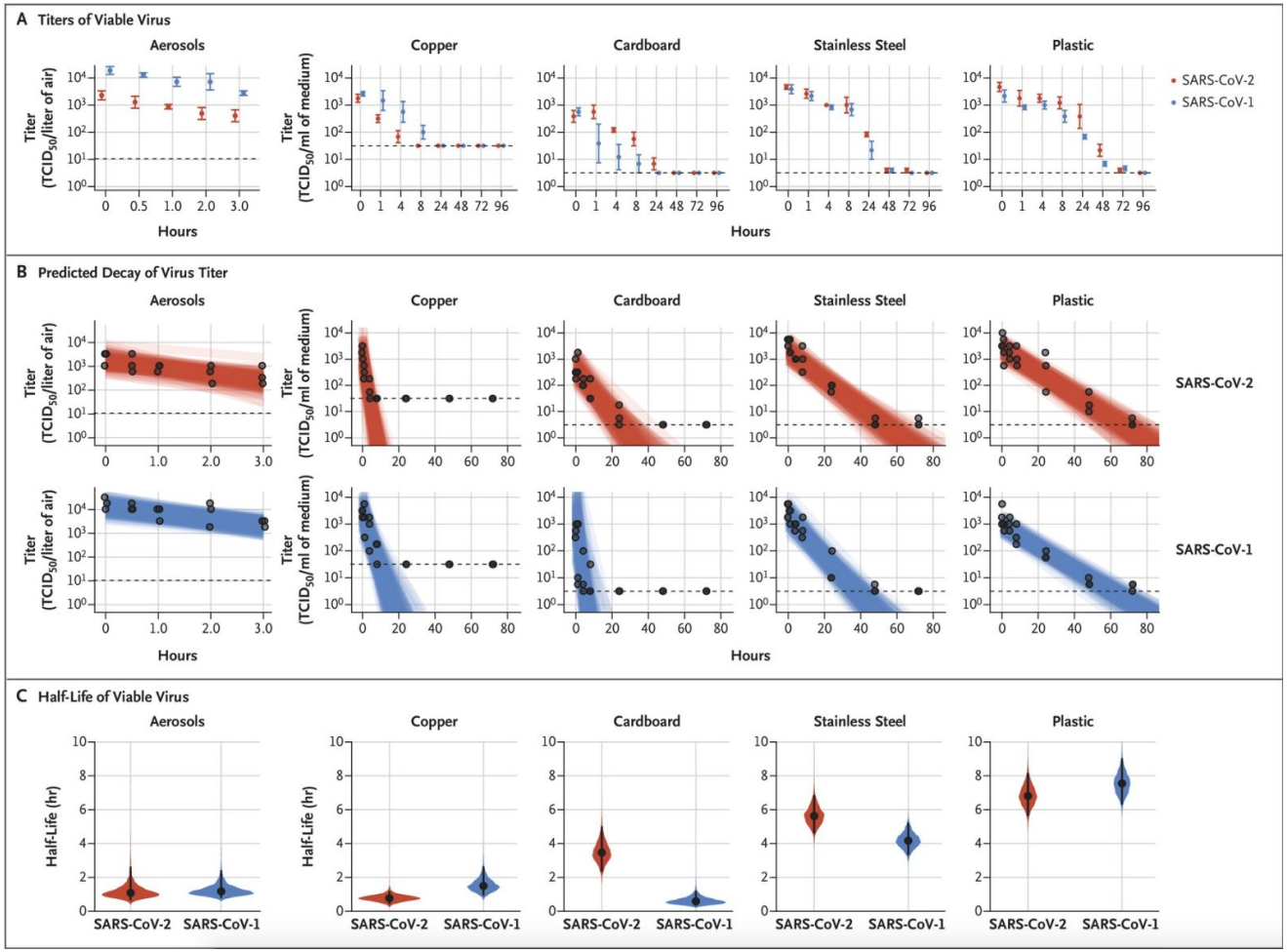
SOURCE: HTTPS://PARKING.UTEXAS.EDU/SCOOTER

Zoombombing

- Zoombombing is the unwanted intrusion into a video conference call by an individual, which causes disruption
- Here are Zoom features to make a video conference call more secure
  - Disabling "join before host"
  - Enabling waiting room
  - Requiring meeting password
  - Locking "Only Host" screen-sharing
  - Disabling participants annotation
  - Using caution when opening links in the chat window
  - Putting a participant on hold
  - Removing a participant
  - Locking meeting
- List of video telecommunication services and product brands
- List of collaborative software

Coronavirus Infectivility

[Aerosol and Surface Stability of SARS-CoV-2 as Compared to SARS-CoV-1]



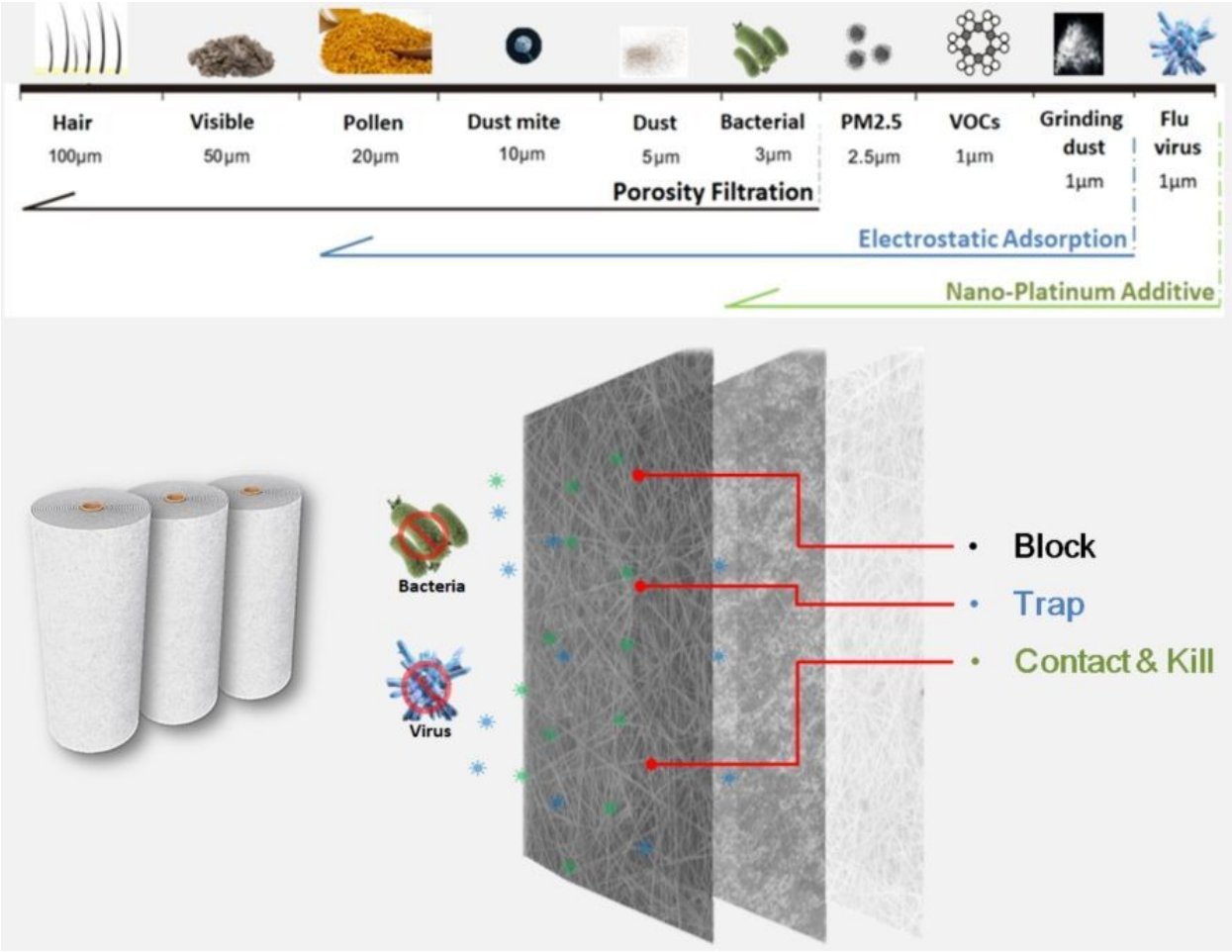
Modeling Aerosol Particles

Aalto University 2020-04-06

Contribution by Stephanie Senkevich, 2020 Spring

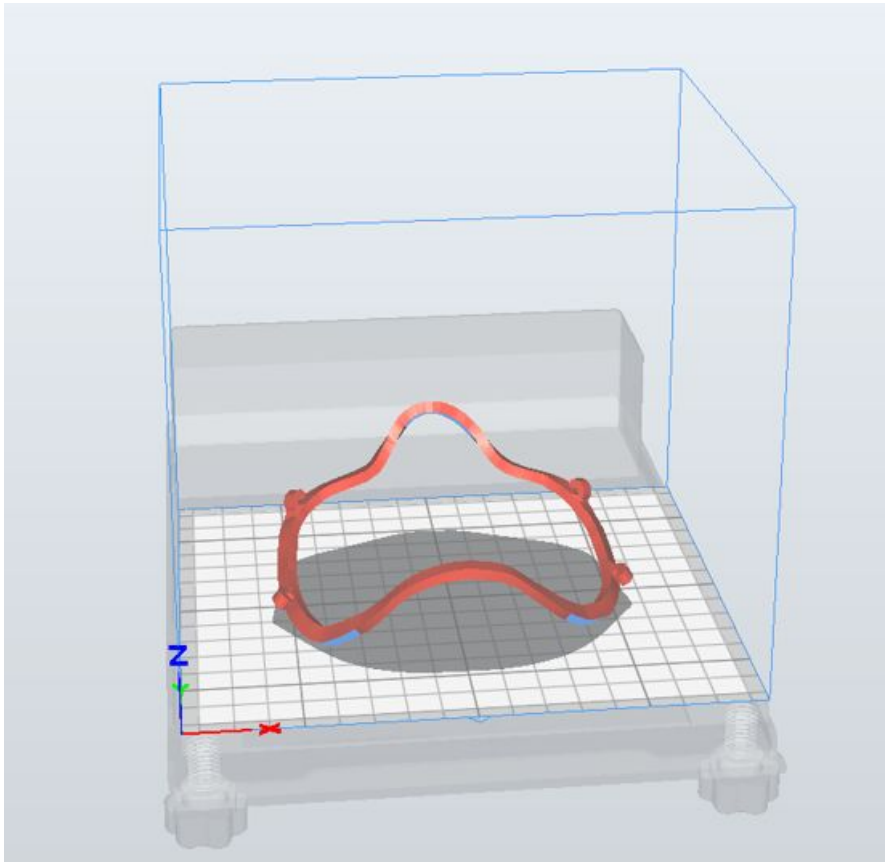
Electrostatic Filtration Material

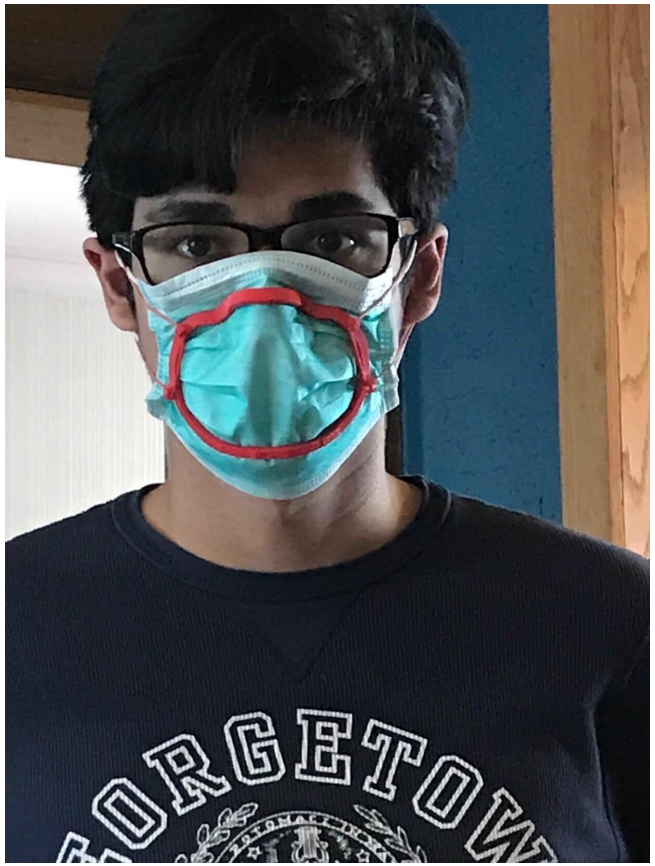
Mytrex Melt-Blown Nonwoven Fabric, Electrostatic Adsorption Particulate Matter (PM), Volatile Organic Compound (VOC)



Face Mask Fitter

Bellus3D, Mobile FaceApp, iOS SDK, Android SDK, NIH 3D Print Exchange





Contribution by Zubin Kremer Guha, 2020 Spring