UNIT- IV

Safety, Responsibilities and Rights

***Syllabus*:** Safety Definition, Safety and Risk, Risk Analysis, Assessment of Safety and Risk, Conflict of Interests, Occupational Crime, Human Rights, Employee Rights, Whistle Blowing, Intellectual Property Rights

Definition of Safety: The condition of being protected from or unlikely to cause danger, risk, or injury.

Definition of Risk: Risk is the likelihood of an undesirable outcome or the potential for harm.

Safety and Risk: There is an interconnection between safety and risk. In fact, both the concepts are relational. Risk is the possibility of harm or loss, while safety is the freedom from risk or exposure to danger. Essentially, safety aims to mitigate or eliminate risks.

Safety measures involve implementing procedures, practices, and technologies to reduce the likelihood and impact of potential risks. For example, Wearing sterilized hand gloves during surgeries or wound caring reduces the risk of possible infection. Wearing a seatbelt while driving is a safety measure that reduces the risk of injury in an accident.

Risks can be classified based on their severity, likelihood, and the nature of the threat (e.g., environmental, financial, health & safety). It can arise from various factors, both internal and external, controllable and uncontrollable. For example, the risk of a traffic accident includes the potential for injury or property damage.

So far if we think of the relationship between the two, we find that safety and risk have an inverse relationship; as one increases, the other decreases.

Since, risk shows the probability of the outcome/consequence, hence effective risk management is crucial for improving safety by identifying, assessing, and mitigating potential hazards. Therefore, a healthy balance between taking risks and ensuring safety is important in various contexts, including investment, business, and professional & personal decisions.

Summarizing the above, we can say safety is the result of proactive measures taken to address and minimize risks, aiming to create a protected and secure environment.

Categories of Risks

Voluntary and involuntary risk: Voluntary risk is a situation wherein the people choose willingly and involve in risk Whereas Involuntary risk is taken by people unwillingly or by compulsion.

Many consider something safer if they knowingly take on the risk, but would find it unsafe if forced to do so. If the property values are low enough, some people will be tempted to buy a house near a plant that emits low levels of a toxic waste into the air. They are willing to assume the risk for the benefit of cheap housing. However, if a person already living near a plant finds that toxic fumes are emitted by the plant and he wasn't informed, the risk will appear to be larger, since it was not voluntarily assumed.

Short term and long-term consequences: Something that might cause a short-lived illness or disability seems safer than something that will result in permanent disability. An activity for which there is a risk of getting a fractured leg will appear much less risky than an activity with a risk of a spinal fracture, since a broken leg will be painful and disabling for a few months, but generally full recovery is the norm. Spinal fractures, however, can lead to permanent disability.

Reversible effects: Something will seem less risky if the bad effects are ultimately reversible. This concept is similar to long term and short-term risk.

Expected Probability: Many might find a one-in-a-million chance of a severe injury to be an acceptable risk, whereas a 50: 50 chances of a fairly minor injury might be unacceptable.

Threshold level of risk: Something that is risky only at fairly high exposure will seem safer than something with a uniform exposure to risk. Studies have shown that low levels of nuclear radiation actually have beneficial effects on human health, while only at higher levels of exposure are there severe health problems or death. If there is a threshold for the effects, generally there will be a greater tolerance for risk.

Delayed Risk and Immediate Risk: The activity that will cause harm in future seems less risky and is called delayed risk. Example: Mobile radiation, Fast food and alcohol. Any activity that results is immediate harm or risk is immediate risk. Example: fall due to slippery floor, electric shock, fall from ladder and explosion will put risk for engineers immediately.

Analysis and Assessment of Risk and Safety

Discuss analytical methods adopted in testing for safety of a product/project or Risk analysis?

Scenario Analysis

It is a technique used in risk management to understand how different future events could affect an organization's objectives. It provides insight into potential risks and opportunities that may arise from uncertain situations, allowing companies to make informed decisions. This method involves considering different scenarios or hypothetical situations that may occur and assessing the potential outcomes of each scenario. The scenarios can be based on various factors such as economic conditions, regulatory changes, natural disasters, or industry developments.

Steps for Risk Assessment

- What can go wrong that could lead to an outcome of hazard exposure? **(Identification and characterization of risk**)
- How likely is this to happen? (**Quantification of risk, likelihood, and magnitude**)
- If it happens, what are the consequences? Scenarios are constructed and the **ways and means of facing the consequences are designed.**

Example: Consider three loss scenarios facing the company which is transporting various cargoes, some hazardous. The three scenarios involve the legal liability arising from use of company vehicles on public roads.

- **Scenario A:** It has a probability of occurrences of 0.001 and a loss potential of 50 million. It is deemed sufficiently "possible" and significant so as to be unequivocally classified as "risky".
- **Scenario B**: It represents the company's liability for an accident involving bodily injury and property damage from relatively "ordinary" road hazards. No spill or disruption of cargo is involved.
- Finally, **Scenario C** identifies a situation involving multiple simultaneous catastrophes to the company fleet.

Scenario A has probability of occurrence of 0.001 and a loss potential of 50 million. It is deemed sufficiently "possible" and significant so as to be unequivocally classified as "risky".

Scenario B, on the other hand, while more probable than A, involves losses that this firm considers "affordable". As such, it is rated not risky with confidence.

Not so easy to classify scenario C. while the probability of multiple catastrophes is not strictly zero, it is rare (10^{-6}, or chance in a million). So, while the loss potential is great, the chance of occurrence is "virtually impossible". Scenario C, nonetheless, resides in that gray area of risk that result in considerable anxiety over its classification.

Methods of Assessment of Safety and Risk

Failure Mode and Effect Analysis (*FEMA*)

Failure Mode and Effects Analysis (FMEA) is a structured approach to discovering potential failures that may exist within the design of a product or process. Failure modes are the ways in which a process can fail. Effects are the ways that these failures can lead to waste, defects or harmful outcomes for the customer. Failure Mode and Effects Analysis is designed to identify, prioritize and limit these failure modes.

Types of FMEAs

- Design
    - Analyzes product design before release to production, with a focus on product function
    - Analyzes systems and subsystems in early concept and design stages
- Process
    - Used to analyze manufacturing and assembly processes after they are implemented

When to Conduct an FMEA

- Early in the process improvement investigation
- When new systems, products, and processes are being designed
- When existing designs or processes are being changed
- When carry-over designs are used in new applications

- After system, product, or process functions are defined, but before specific hardware is selected or released to manufacturing

FMEA Procedure

1. For each process input (start with high value inputs), determine the ways in which the input can go wrong (failure mode)
2. For each failure mode, determine effects
    - Select a severity level for each effect
3. Identify potential causes of each failure mode
    - Select an occurrence level for each cause
4. List current controls for each cause
    - Select a detection level for each cause
5. Calculate the Risk Priority Number (RPN)
6. Develop recommended actions, assign responsible persons, and take actions
    - Give priority to high RPNs
    - MUST look at severities rated a 10
7. Assign the predicted severity, occurrence, and detection levels and compare RPNs

What is Severity, Occurrence, and Detection in FMEA

- Severity: Importance of the effect on customer requirements
- Occurrence: Frequency with which a given cause occurs and creates failure modes (obtain from past data if possible)
- Detection: The ability of the current control scheme to detect (then prevent) a given cause (may be difficult to estimate early in process operations).

Rating Scales

- Severity: 1 = Not Severe, 10 = Very Severe
- Occurrence: 1 = Not Likely, 10 = Very Likely
- Detection: 1 = Easy to Detect, 10 = Not easy to Detect

Risk Priority Number (RPN)

RPN is the product of the severity, occurrence, and detection scores.

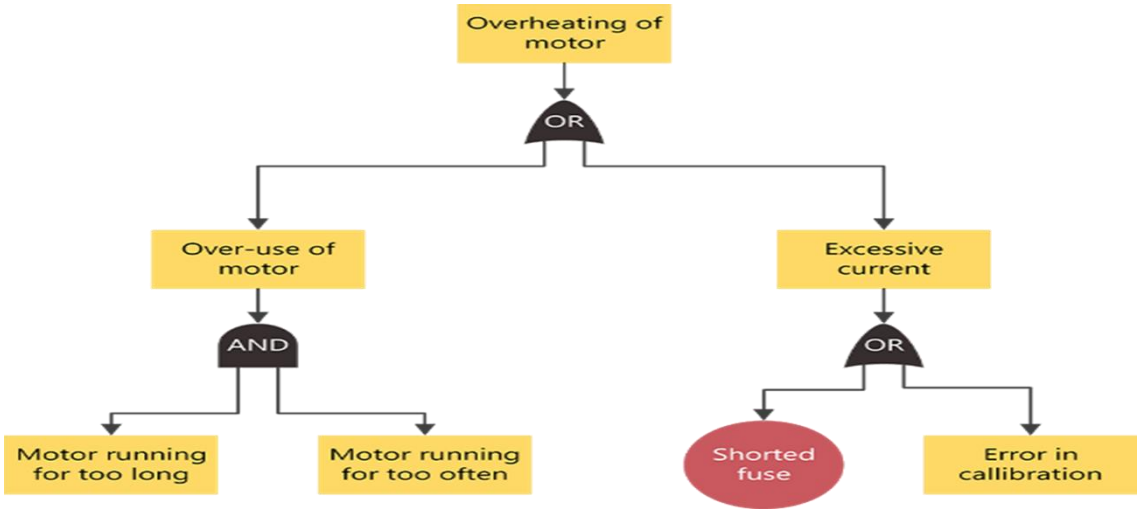
Severity x Occurrence x Detection = RPN

Example of FMEA for Manufacturing Process

Process Step	Potential Failure Mode	Potential Effects of Failure	Severity (S)	Occurrence (O)	Detection (D)	Risk Priority Number (RPN)	Actions Taken
Material Inspection	Incorrect material received	Assembled products may fail to meet specifications	8	3	5	120	Improved supplier communication, additional inspection checks
Cutting Process	Machine blade wear	Inconsistent part dimensions	6	4	6	144	Regular maintenance schedule, blade replacement protocol
Welding Operation	Inadequate weld strength	Structural failure of components	9	2	4	72	Stricter quality checks, regular equipment maintenance
Assembly	Incorrect assembly sequence	Product malfunctions, safety risks	7	3	7	147	Enhanced training for assembly line workers, visual aids
Quality Inspection	Incomplete inspection	Defective products shipped to customers	7	3	7	147	Training and certification for quality inspectors, process audit
Packaging	Incorrect labeling	Misidentification of products	5	4	8	160	Automated labeling systems, additional visual

Fault Tree Analysis (FTA)

FTA focuses on identifying potential failures or faults within a system that could lead to an undesired event or outcome. It starts with the top event, which is the undesired outcome, and then systematically breaks down the event into its component parts, such as system failures, human errors, equipment malfunctions, or external events. Example:



Breakdown of the Fault Tree Analysis:

1. *Top Event (Primary Failure):*
    - The **Overheating of Motor** is the top-level failure event that needs to be analyzed.
2. *Contributing Factors (Intermediate Events):*
    - The overheating of the motor can be caused by **Overuse of the motor** or **Excessive current** (connected via an OR gate).
3. *Basic Causes (Root Causes):*
    - *Overuse of the Motor*:
        - This happens when both **Motor running for too long** and **Motor running too often** occur together (AND gate).
    - *Excessive Current:*
        - This can be caused by either **Shorted fuse** or **Error in calibration** (OR gate).

Logical Analysis:

- If **either** excessive current or overuse of the motor occurs, overheating can happen.
- For overuse of the motor to occur, **both** conditions (motor running for too long and too often) must be met.
- Excessive current can occur due to **either** a shorted fuse or an error in calibration.

Application in Risk Assessment:

- FTA helps in **identifying critical failure points** and their dependencies.
- It allows engineers to **prioritize risk mitigation strategies** by addressing root causes.

- By analyzing the logic gates, one can determine the **probability of system failure** and implement preventive measures.

Event Tree Analysis (ETA)

ETA, on the other hand, focuses on analyzing the possible sequences of events that may occur following an initiating event, leading to various outcomes or consequences. It begins with an initiating event, such as an accident or failure, and then models the potential subsequent events and their probabilities, often branching out into different scenarios based on different conditions or responses. Example:

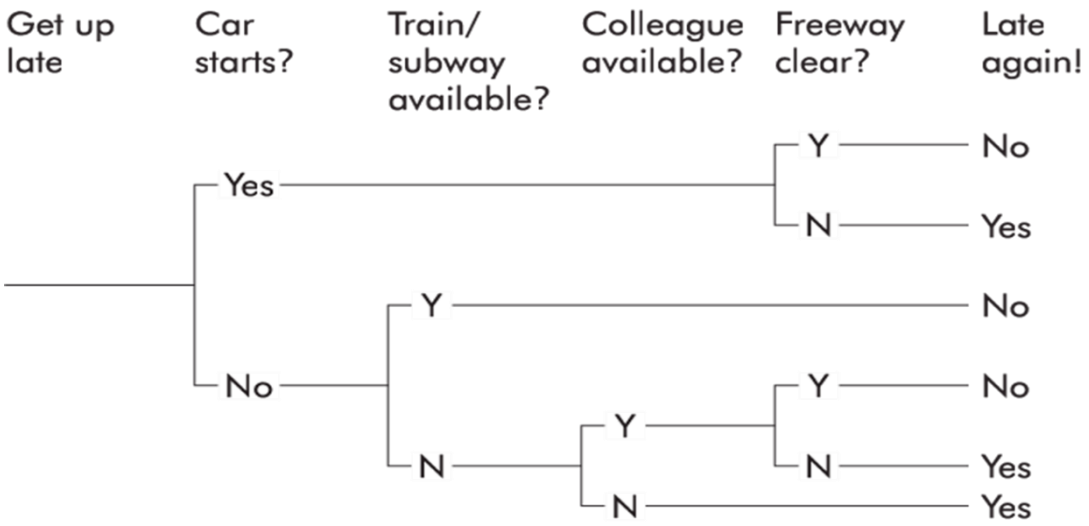


Figure: Event Tree Analysis

Whistleblowing

Whistle-blowing refers to the phenomenon when someone comes out with the information that something unethical has happened or is happening. Whistle-blowing in general has the following five attributes:

Disclosure: A person discloses information about an unethical happening. The unethical act is serious enough to warrant such disclosure and concerns public safety.

Whistle-blower: the whistle-blower is the person disclosing the information. In a narrow sense of the term, the person disclosing the information is an employee or former employee. In a wider sense, it can be anyone who has the knowledge and proof of the unethical acts.

Mode: when a person discloses information of some unethical acts, he/she does not follow the approved or regular channels to convey information. There can be

many reasons for this: the person is under pressure from the organization not to disclose such information; or the person finds that the immediate supervisors who form the normal channels of communication do not listen to what he/she considers legitimate complaints.

Motive: the motive of the whistleblower is important. He / she would reveal information that the organization considers confidential, with a noble motive to bring to the public notice or authorities, something unethical going on, that could significantly affect public safety or morality.

Audience: When a whistle-blower passes information about something unethical happening, he/she has to report the same to someone or some entity with the authority to take appropriate action to prevent or punish those who have done that act.

Types of Whistleblowing

- **External whistle-blowing**: This occurs when an employee gives out information about unethical acts to agencies outside the organization, he/she works for.
- **Internal whistle- blowing**: This is when the employee discloses the information within the organization to a superior entity bypassing the normal channels of communication.
- **Open Whistle-blowing**: this is when the person disclosing the information does not hide his/her identity.
- **Anonymous whistle-blowing**: This is when the person disclosing the information does not disclose his/her identity. Anonymous whistle-blowing is generally not taken seriously.

Intellectual Property rights

Intellectual property may be defined as the information and original expression that derives its original value from creative ideas, and is with a commercial value. I.P rights permit people to have fully independent ownership for their innovations and creativity, like that of own physical property. This encourages the IP owners towards innovation and benefit to the society. It is an asset that can be bought or sold, licensed, and exchanged.

Types and norms of intellectual properties

1. **Patents**: Patent is a contract between the individual (inventor) and the society (all others). Patents protect legally the specific products from being manufactured or sold by others, without permission of the patent holder. Patent holder has the legally-protected monopoly power as one's own property. The validity is 20 years from the date filing the application for the patent. Patent is given to a product or a process, provided

it is entirely new, involving an inventive method and suitable for industrial application. While applying for a patent, it is essential to submit the documents in detail regarding the problem addressed, its solution, extent of novelty or innovation, typical applications, particulars of the inventor, and the resources utilized. Inventions are patentable and the discoveries are not.

Types of patents:

a. **Utility Patents**: The utility patent is granted to anyone who invents or discovers any new and useful process, machine, manufacture or chemical composition of any manner or any new and useful improvement thereof. The utility time is 20 years.

b. **Industrial Design Patents**: The industrial design patent is an idea or conception regarding features of shape, configuration, pattern, ornamental with lines or colours applied to any article, two or three dimensional, made by any industrial process and is judged by the eye or a product. For example, the design of a tea cup must have a hollow receptacle for holding tea and a handle to hold the cup. These are functional features that cannot be registered. But a fancy shape or ornamentation on it would be registerable. The design patent has a term of 14 years from the date of filing the application. It is covered under Design Act 2000.

2. **Copyright**: The copyright is a specific and exclusive right, describing rights given to creators for their literary and artistic works. This protects literary material, aesthetic material, music, film, sound recording, broadcasting, software, multimedia, paintings, sculptures, and drawings including maps, diagrams, engravings or photographs. The life of the copyright protection is the life of the inventor or author plus 60 years. Copyrights give protection to particular expression and not for the idea. Copyright is effective in a) preventing others from copying or reproducing or storing the work, b) publishing and selling the copies, c) performing the work in public, commercially (d) to make translation of the work and (e) to make any adaptation of the work.
3. **Trademark**: Trademark is a wide identity of specific goods and services, permitting differences to be made among different trades. It is a territorial right, which needs registration. Registration is valid initially for 10 years, and renewable. The trademark or service mark may be registered in the form of a device, a heading, a label, a ticket, a letter, a word or words, a numeral or any combination of these, logos, designs, sounds, and symbols. Trademark should not be mistaken for a design, e.g., the shape of a bottle in which a product is marketed, cannot be registered as a trademark.
4. **Trade Secret**: A trade secret is the information which is kept confidential as a secret. This information is not accessed by any other(competitor) than the owner and this gives a commercial advantage over the competitors. The trade secrets are not registered but only kept confidential. These are given limited legal protection, against abuse by the employee or contractor, by keeping confidentiality and trust. The trade secrets may be formulae, or methods, or programs, or processes or test results or data collected, analysed, and synthesized.

Occupational Crimes

A. An Industrial Espionage:

The term industrial espionage refers to the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. This activity is a covert practice often done by an insider or an employee who gains employment for the express purpose of spying and stealing information for a competitor. Industrial espionage is conducted by companies for commercial purposes rather than by governments for national security purposes.

Types of industrial espionage

Industrial espionage and corporate spying are conducted through a variety of channels and for various purposes. Some espionage is conducted through legal channels and some is conducted illegally. The following are examples of some common types of industrial espionage.

IP theft. This type of espionage comes in many different forms. For example, it can be a theft of engineering designs from an automobile or aerospace company; a formula for a new drug from a pharmaceutical company; a recipe from a food and beverage or vitamin supplement company; new robotic manufacturing processes from a high-tech manufacturer; or even pricing sheets and customer lists. These items may be stolen by outsider perpetrators or foreign governments, or by employee insiders who are disgruntled or see a way to get hired or compensated by a competitor for the theft.

Property trespass. Breaking into physical premises or files to obtain company information is another form of industrial espionage. A surprising number of critical corporate assets are still in physical form and may be obtained by insider employees or by outsiders who gain access to the premises.

Hiring away employees. Competitors frequently try to hire away employees from companies to gain access to information the employees have acquired on the job. Most of the time, the knowledge employees obtain on the job is part of the trade and is legitimately transferrable, but there also are times when employees leave with valuable trade secrets and formulas in their heads that they can put to work for their new companies.

Wiretapping or eavesdropping on a competitor. Those desiring information from a company can set up portable devices that listen in or record certain conversations, such as a confidential board meeting. In some cases, this wiretapping may be legal and authorized, but in others, it is illegal listening for the purpose of economic or strategic gain.

Cyber-attacks and malware. Whether it is through a distributed denial-of-service attack or an infusion of malware that corrupts a company's network, companies, governments and organizations also seek to disrupt each other by sabotaging daily operations and disabling their ability to work.

B. Bootlegging

Bootlegging, as an occupational crime, refers to the illegal manufacturing, transportation, distribution, or sale of prohibited goods, particularly alcohol during Prohibition, or the illegal reproduction and distribution of copyrighted material today.

What is Bootlegging?

- *Historical Context*:

During the Prohibition era (1920-1933) in the United States, bootlegging involved the illegal production, smuggling, and distribution of alcoholic beverages, which was forbidden under the 18th Amendment to the U.S. Constitution.

- *Modern Usage*:

The term "bootlegging" can also refer to the illegal copying and distribution of copyrighted materials, such as movies, music, or software.

- *Origin of the Term*:

The term "bootlegging" originated from the practice of concealing flasks of illicit liquor in the leg of a high boot.

Examples of Bootlegging as an Occupational Crime

- During Prohibition:
    - Manufacturing Illegal Alcohol: Bootleggers would set up illegal distilleries (like moonshine stills) to produce alcohol, often in rural areas or hidden locations.
    - Smuggling Alcohol: They would smuggle alcohol across state lines or international borders, using various methods to evade law enforcement, like using speedboats to outrun Coast Guard patrols.
    - Supplying Speakeasies: Bootleggers would supply illegal bars (speakeasies) with alcohol, which became social hubs during the Prohibition era.
- Modern Examples:
    - Pirated Movies and Music: Bootlegging can involve the illegal recording and distribution of movies or music, often through unauthorized online platforms.
    - Software Piracy: The illegal copying and distribution of software is another form of modern bootlegging.
    - Counterfeit Goods: Bootlegging can also involve the production and distribution of counterfeit goods, like clothing or electronics.

C. *Grease Payments*

A grease payment is a small payment or favour offered to a minor official or functionary to expedite a routine service or process that the recipient is already obligated to perform by law or regulation.

Grease Payment vs. Bribe

The key difference between a grease payment and a bribe lies in the intent and the outcome. A grease payment aims to expedite a routine process, not necessarily change the outcome. A bribe, on the other hand, is intended to influence a decision in the giver's favor, potentially involving something they are not entitled to by law. The legality of grease payments can be a grey area. In some jurisdictions, they might be considered a minor offense, while others might view them as a form of bribery.

D. *Moonlighting*

Moonlighting is a practice in which the employees take up another job or do freelance work in addition to their regular full-time job during off hours.

Different cultures have different outlooks on moonlighting. For instance, in India, this is usually not encouraged by companies as this leads to many issues like a decrease in productivity, conflict of interest, and even breach of employment contracts. However, it is normalized in western economies. In fact, the percentage of U.S. workers who hold more than one job has been increasing during the past 20 years.

There are four different kinds of moonlighting, based on the nature of motivation and circumstances

1. **Quarter Moonlighting:** In this, employees undertake part-time jobs to supplement the poor pay that they receive. For example, the workers might undertake freelancing as a supplement for their inadequately remunerated principal source of income.
2. **Half Moonlighting:** Employees devote half of their time to a side hustle to build a future financial reserve or support a luxurious life. For example, a marketing professional might run an online retail business during their free hours.
3. **Full Moonlighting:** This happens when employees take up a second job or start a business that requires substantial time and effort, often compromising with their full-time role. An example could be an engineer launching a startup while working full-time at an IT firm.
4. **Blue Moonlighting:** Blue Moonlighting occurs when employees take on a second job despite financial satisfaction, driven by dissatisfaction in their primary role. For example, a financial analyst freelancing as a graphic designer to explore a new career option.

E. Occupational Hazards

An "occupational hazard" is a risk or danger inherent in a specific job or workplace environment that can lead to injury, illness, or death.

- **Definition:**

An occupational hazard is any condition or situation in a workplace that has the potential to cause harm to employees.

- **Examples:**

These hazards can include physical, chemical, biological, or psychological factors, such as exposure to toxic substances, loud noises, repetitive motions, or workplace stress.

- **Categories:**

Occupational hazards can be broadly categorized as:

- **Physical hazards:** These include things like noise, temperature extremes, radiation, and vibration.
- **Chemical hazards:** These involve exposure to chemicals, gases, and vapors.
- **Biological hazards:** These include risks from bacteria, viruses, and other biological agents.
- **Psychosocial hazards:** These involve workplace stress, bullying, and other factors that can negatively impact mental health.
- **Ergonomic hazards:** These relate to how a job is designed and can cause musculoskeletal injuries.

F. Price Fixing

Price fixing is an agreement between competitors or businesses in a market to set the price of goods and services. This agreement involves direct or indirect communication, resulting in prices being set at levels higher than competitive market conditions would otherwise dictate. One example is if two companies who are major producers of a particular product collude to raise the price of their product above what competitive market forces would otherwise dictate.

Example of Price Fixing

In a small town, there are only two gas stations. The two gas stations are engaged in a tough competition with each other, undercutting prices to attract the most customers.

One day, the manager at one of the gas stations decides to schedule a meeting with the manager at the other gas station. He says: “Over the past few months, our profits have declined because we have been decreasing our prices to drive traffic away from each other – why don’t we both agree on a price to charge customers so we can extract more profits from them?”

The other manager agrees, and the gas stations collectively decide to raise prices from $100 to $200. Given no other options, consumers are forced to pump gas at $200.

G. What is an example of paternalism?

Paternalism refers to a person or institution of authority restricting the freedom of choice of a person or persons because they believe it is in their best interest. An example might be a doctor ordering surgery for a patient without informing them of other available options.

Paternalism Definition

Autonomy is the right of a person to make decisions on their own. When a person or institution of authority limits the autonomy of a person or a group of people, supposedly for their own good, the practice is referred to as paternalism. A paternalistic system acts on the premise that certain people are not capable of acting in their own interests and require the supervision of

those in authority. The word paternalism is from the Latin word for fatherly and suggests a parent-child relationship.

The undesired effects of paternalism include the denial of freedom to make decisions for oneself and being in a position of perceived inferiority. Groups that are likely to experience paternalism include the elderly, disabled, or terminally ill.

H. Insider Information

Insider trading, which involves using non-public information for financial gain, is a form of occupational crime, often categorized as white-collar crime, where individuals misuse their position for personal benefit.

- **Insider Trading as an Example:**

Insider trading, where someone trades securities based on non-public, material information, is a classic example of occupational crime.

- **Who is Involved?**

Individuals with access to sensitive, non-public information, such as company employees, directors, or service providers, can be involved in insider trading.

- **Why it's Illegal:**

Trading on insider information creates an unfair advantage in the market, potentially harming other investors and undermining market integrity.

.