Assignment

Submitted by: **MUHAMMAD WAQAR KHAN**
ID: **13571**
DISCIPLINE: **MS CE**

Question # 1: What is the difference between hazards and threats? Provide examples.

Answer: **Difference between Hazards and Threats:**

To understand the difference between hazards and threats, first we need to clearly grasp the concepts of hazards and threats.

Hazard:

Hazard is something with the potential to cause harm. A hazard can take many forms. It could be a substance, an energy source or an existing work practice or process. In Safety management, a Hazard is defined as a condition that poses danger to an organization, and can lead to an accident, incident, or other mishap if not mitigates.

Examples of hazards could such thing as Substances e.g. chemicals, Energy Sources e.g. machinery with moving parts, Work Practices e.g. working at height from a ladder or moving materials with a forklift truck.

A hazard satisfies all of the following conditions:

- Hazard is a dangerous condition, such as an object, situation, circumstance, that poses an unacceptable level of danger;
- Occurs once in the safety mishap lifecycle;
- Can lead directly to risk occurrence (i.e., safety mishap, accident, etc.) if not mitigated; and
- Arise from hazard mechanisms, such as initiating actions and hazardous sources.

Threat:

Threat is a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.

Threat can be anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. Moreover, any potential cause of an incident can be considered a threat

A threat is what we're trying to protect against.

Threat agent: A person, organization, thing, or entity that acts, or has the power to act, to cause, carry, transmit, or support a threat

Examples of threat in construction industry could be anything from inclement weather to quarantine (a recent addition to the list) to economical factors.

Types of Threats:

There are two types of threats that are used differently in different contexts. They are:

- General threats: the amount danger in a given circumstance; and
- Specific threats: a specific object, situation, behavior, etc., that corresponds to a rising level of danger within a given context.

Difference between hazards and threats:

A threat is a hazard, but a hazard need not be a threat.

A **hazard** occurs ("actualized") when ones operations interact with hazard sources. On the other hand, a **threat** is simply a generic way to describe danger, whether the danger has actualized or not.

The difference between hazard and threat can be best understood from the following example:

A water cooler on the shop floor has a leak. This has created a puddle on the floor which is now a slip hazard. If we do not do anything to remove or control this hazard, there is a significant threat that someone could slip and injure themselves.

On the other hand, if we had identified the potential for harm (hazard) and put suitable and simple control measures in place, such as barriers. The chances of someone coming to harm (threat) would now be low. So although the hazard still exists, the actual risk would be reduced to an acceptable level.

Sometimes, hazard and threat might be used interchangeably. Consider the example of a flock of birds flying close to an aircraft. This flock is both a hazard and a threat.

However, because the concept of a threat is vaguer than the concept of a hazard, a threat is not always a hazard. Consider the example of:

- Migrating birds, which are a hazardous source but not an actual hazard, or
- Fatigue, which is a contributing factor.

Therefore, a threat is a generic way to describe danger, whether the danger has actualized or not. In contrast, a hazard has a potential to cause harm and actualizes when come in contact with hazard source.

Question # 2: Define risk and provide a classification of risk based on its sources. Provide an example for each risk source.

Answer:

RISK:

Risk is exposure to the possibility of economic or financial loss or gain, physical damage or injury, or delay, as a consequence of the uncertainty associated with pursuing a particular course of action.

Risk is not the present problem which should be immediately addressed, but it is considered as future issues that can be avoided or mitigated. Risk is considered as a situation which may lead to negative consequences. Generally, six major categories of risk can be identified as the most important concerns for the majority. They are:

- Environmental risks, including pollution, radiation, chemicals, floods, fires, dangerous road conditions and so on;
- Lifestyle risks, which related to the consumption of such commodities as food and drugs, engagement in sexual activities, driving practices, stress, leisure and so on;
- Medical risks, which related to experiencing medical care or treatment. Such as drug therapy, surgery, childbirth, reproductive technologies and diagnostic tests;
- Interpersonal risks, related to intimate relationships, social interactions, love sexuality, gender roles, friendship, marriage and parenting;
- Economic risks implicated in unemployment or under-employment, borrowing money, investment bankruptcy, destruction of property, failure of a business and so on; and

Criminal risks are those risks emerging from being a participant in or potential victim of illegal activities.

Continued…

The Concept of Risk in Construction Industry:

The construction industry experienced a wide variety of risks which may occur in financing, designing, constructing and managing facilities of a project. There are different definitions of risk in construction industry. In order to understand the process of risk management, it is important to understand the basic concept of risk in all aspects. Risk is a combination of probability of an event which is occurring and its consequences to project objectives. However, some suggest using a more general concept of uncertainty and argue that risk is considered as threats but not opportunities and when it occurs it affects the project performance. Risks have a negative impact on the project's cost, quality or time in most situations. These definitions have a common feature: they define risk in terms of uncertain events and may have positive or negative impact on a project's objectives.

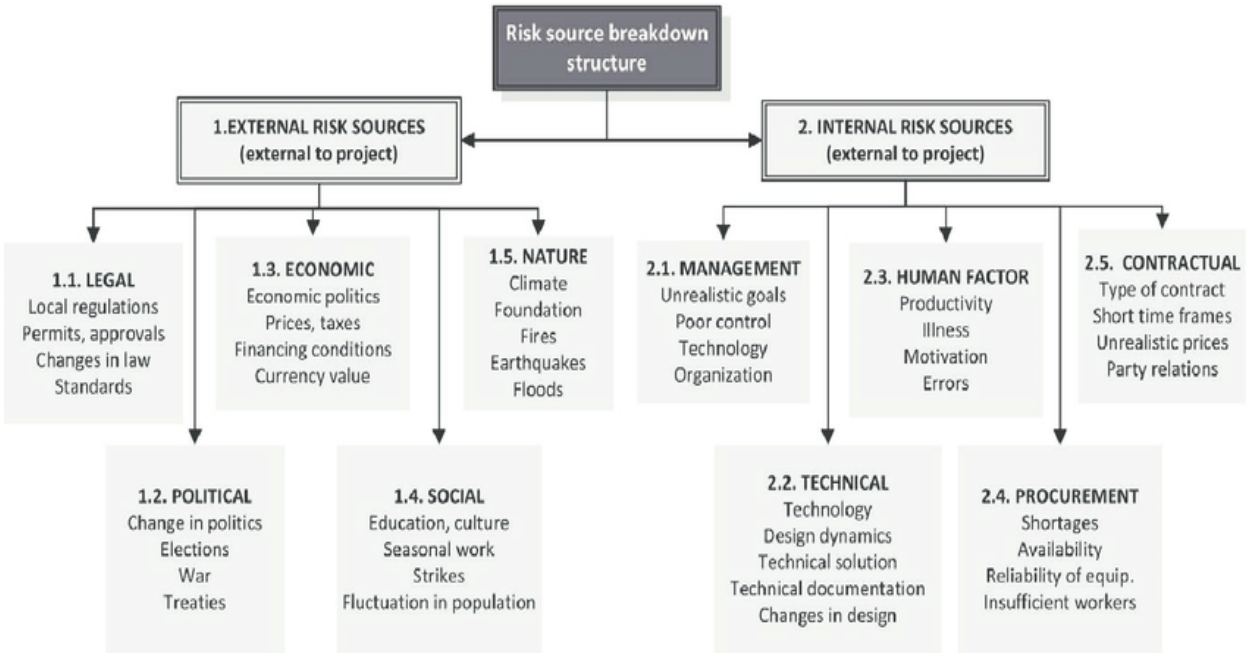
Classification of risk based on its sources:

Many authors who have been studying risk believe that qualitative analysis is most essential. According to them *information about risk source is the first important step*. Risk can be categorized on the bases of sources along with examples in the following categories:

EXTERNAL SOURCES –outside the project		**INTERNAL SOURCES – inside the project**	
LEGISLATIVE	1 - local regulations	**CONTRACT**	1 – unrealistic deadline
	2 – permits and agreements		2 - unrealistic price
	3 – law changes		3 – other contract provisions
	4 – standards	**TECH. DOCUM.**	1 – delay
POLITICAL	1 – policy changes		2 – incompleteness
	2 – elections		3 – imprecision
	3 – war		4 .- new solutions as a consequence of 2 and 3
	4 – existing agreements	**ORGANIZATION**	1 – bad management
ECONOMICAL	1 – economic regulations		2 – bad organization of works
	2 – price rises	**TECHNOLOGY**	1 – poorly chosen tech. solutions
	3 – exchange rates		2 – obsolete technology

	4 – financing conditions	**RESOURCES**	1 – shortage of workers
	5 – economic policy changes		2 – shortage of machinery
SOCIAL	1 – education, culture		3 – machinery breakdowns
	2 – seasonal work		4 – late delivery of materials
	3 – strike	**HUMAN FACTOR**	1 – productivity
	4 – human fluctuation		2 – sick leaves
NATURAL	1 – climate		3 – motivation
	2 – soil		4 - errors and omissions
	3 – subterranean waters		
	4 – natural disasters		

Risk Source breakdown structure is given below:



Question # 3: How would you assess the performance of a transportation system of a city?

Answer:

Assessment of the performance of a transportation system in a city:

Assessment of the performance of a transportation system in a city represents a very useful tool for ensuring continuous increase of the quality of the delivered transit services, and for allocating resources among competing transit agencies.

Transit service quality can be evaluated by *subjective measures* based on passengers' perceptions, and *objective measures* represented by disaggregate performance measures expressed as numerical values, which must be compared with fixed standards or past performances.

Performance Assessment:

Performance measures can be useful also for the allocation of funds but, for this aim, a more thorough understanding of the applicability and appropriateness of performance measures to different types of transit systems is necessary.

There is a variety of performance measures developed for describing different aspects of the transit services. Transit performance measures can refer to the passenger, agency, and/or community's point-of-view. Passenger's viewpoint reflects the passenger's perception of the service. The agency point-of-view reflects transit performance from the perspective of the transit agency as a business. The community's point-of-view measures transit's role in meeting broad community objectives. Measures in this area include measures of the impact of a transit service on different aspects of a community, such as employment, property values, or economic growth. This viewpoint also includes measures of how transit contributes to community mobility and measures of transit's effect on the environment. Perceived performance of a transit service from the passenger's point of view can be defined as quality of service.

Performance of a Transportation System of a City:

Measures of performance of a transportation system in a city falls within the three broad dimensions of effectiveness, reliability, and cost, but there are many more detailed concerns that fall within these principal dimensions.

I would gauge a transportation system on the bases of its effectiveness, reliability, and cost, to assess its performance.

1) Effectiveness of a Transportation System:

Effectiveness of a Transportation System is the ability of the system to provide the services the community expects.

Effectiveness of a system may generally be described in terms of:

- Its capacity and delivery of services
- The quality of services delivered
- The system's compliance with regulatory concerns, and
- The system's broad impact on the community

2) Reliability of a Transportation System:

Reliability is described as the likelihood that infrastructure effectiveness will be maintained over an extended period of time or the probability that service will be available at least at specified levels and times during the design life of the infrastructure system.

Reliability is influenced by planning and implementation decisions as well as inherent uncertainties in the infrastructure system. Construction and operations often extend over periods of many years and affect characteristics of infrastructure elements and their behavior. People make judgments about the value or severity of outcomes of infrastructure-related decisions, also influencing reliability.

3) Cost of a Transportation System:

Measuring infrastructure costs is often a complex financial exercise that goes well beyond simply recording expenditures for facilities construction, operations, and maintenance.

Consideration must generally be given to the initial construction or replacement cost of facilities (also called investment or capital cost) and the recurring expenditures for operations and maintenance that will be required throughout the system's service life.

STANDARDS FOR ASSESSMENT:

Understanding the measures of effectiveness, reliability, and cost in a particular situation is generally accomplished by comparing the measurements to some example or base. The base may be informal and derived from experience.

Analyzing the effectiveness, reliability and cost of a transportation system, I will be in a much better position to assess the performance of a particular transportation system.

Question # 4: Define security vulnerabilities of a university campus.

Answer:

Vulnerability:

The term "vulnerability" is used to explain inborn characteristics of a system. Project vulnerabilities create the potential for harm but are independent from the probability of occurrence of a risk event. Vulnerability indicates the degree to which a project is susceptible to adverse effects of change. It exists within systems independently of external hazards and depends on organization's capability to manage risks, and can be internally created by organizational, social and economic factors.

For a systematic understanding it is necessary to distinguish the following categories of vulnerabilities:

- Structural vulnerability
- Non-structural Vulnerability
- Functional Vulnerability

1) Structural vulnerability:

This category of vulnerability pertains to the structural elements of the buildings, e.g., load bearing walls, columns, beams, floor and roof.

2) Non-structural Vulnerability:

"Nonstructural" usually refers to things that are designed by someone other than the structural engineer; however, nonstructural walls are required to have some strength. For example, interior non-bearing partitions are generally required to be designed to resist a minimum design lateral force. This is intended to provide some resistance to seismic forces perpendicular to the wall and to ensure a minimum stiffness to the walls.

3) Functional Vulnerability:

Functional vulnerability needs to be considered and eliminated for institutions, especially the critical facilities such as hospitals, emergency operation centers, communication centers etc.,

to ensure that the services provided by the facilities would keep on running to meet the demands of the community at the time when these are most needed. Security vulnerability also comes under the umbrella of functional vulnerability.

Security vulnerabilities of a university campus:

There is a wide range of security vulnerabilities that have to be neutralized at the earliest. While assessing security vulnerability, consideration is made of 1) location, accessibility, and distribution of the services within the system, 2) individual services, both medical (equipment and supplies) and non-medical (utilities, transportation and communication), that are vital to the continuous operation, and 3) public services and safety measures

Many physical security vulnerabilities depend on such factors as

- Size of the building
- Number of buildings or sites
- Number of employees
- Location and number of building entrance and exit points
- Placement of the data centers and other confidential information

Literally thousands of possible physical security vulnerabilities exist. Here are some examples of physical security vulnerabilities:

- No receptionist in a building to monitor who's coming and going
- No visitor sign-in or escort required for building access
- Employees trusting visitors because they wear vendor uniforms or say they're in the building to work on the copier or computers
- No access controls on doors or the use of traditional keys that can be duplicated with no accountability
- Doors propped open

- IP-based video, access control, and data center management systems accessible via the network with the default user ID and password
- Publicly accessible computer rooms
- Software and backup media lying around
- Unsecured computer hardware, especially laptops, phones, and tablets
- Sensitive information being thrown away in trash cans rather than being shredded or placed in a shred container
- CDs and DVDs with confidential information in trash cans

When these physical security vulnerabilities are exploited, bad things can happen. All it takes to exploit these weaknesses is an unauthorized individual entering the university campus.