Safety-Reliability-Risk Assessment: Preliminary Hazard Analysis

An Online Continuing Education Course for Engineers

Course Number: M-2057

Credit: 2 Hours / 2 PDH / 2 CPD

Safety-Reliability-Risk Assessment: Preliminary Hazard Analysis

Chelliah Sundararajan, Ph.D.

(Professional development hours = 2)

1. INTRODUCTION

Preliminary hazard analysis (PHA) is conducted at the conceptual design stages of a system (or entire plant) to identify the hazardous elements in the system and to assess their safety implications. The preliminary hazard analysis is a global-type of analysis that looks at the big picture of the system as a whole from a safety point of view. More detailed analyses of components and systems may follow a preliminary hazard analysis; for example, failure modes and effects analysis and/or fault tree analysis may be conducted following a preliminary hazard analysis. Some reliability/risk analysis projects end after the preliminary hazard analysis and no other analysis is carried out; it depends on the scope and purpose of the safety/risk/reliability project.

Findings and recommendations from the analysis are transmitted to the design team and appropriate changes are made in the design to reduce accidents and minimize their consequences. If necessary, another preliminary hazard analysis may be conducted after design changes are made. Preliminary hazard analyses may also be conducted for operating plants if no preliminary hazard analysis was conducted during plant design.

2. ANALYSIS PROCEDURE

A preliminary hazard analysis consists of the following steps.

1. Data collection
2. Identification of hazardous sources
3. Preparation of hazards and effects table

These steps are described below.

2.1 **Data Collection**

The team performing a preliminary hazard analysis should examine all available information about

the hardware, materials, processes, tests and operations relating to the system under study. Since the preliminary hazard analysis is normally performed during conceptual design stages, detailed drawings and data may not be available. System layout drawings showing relative placement of hardware, storage facilities, operator stations and process flows should be examined.

2.2 **Identification of Hazardous Sources**

Any hardware, material, process or operation that could, under certain conditions, cause loss of life, personnel injury or property damage is considered a hazardous source (hazardous element). Under normal conditions, these hazardous sources may be harmless but certain abnormal conditions can trigger the hazardous sources to cause accidents. Consider, for example, a poisonous gas produced as a byproduct of a chemical process. Under normal conditions, plant personnel and the public are protected by containing the gas in a pressure vessel. Here the hazardous element (poisonous gas) does not pose a threat to plant personnel or the public. A triggering event that could set events in progress leading to an accident is a "leak in the pressure vessel" due to corrosion, erosion or crack propagation. A leak in the pressure vessel would release the gas to the environment and affect plant personnel. A more serious triggering event would be an "explosion in the pressure vessel" that could release enormous quantities of the gas, and both plant personnel and the general public in the neighborhood would be at risk.

All hazardous sources, whether they are hardware, material, process or operation, should be identified and listed. A number of hazardous elements are listed below.

1. Explosive charges
2. Flammable materials
3. Excessively high or low pressure
4. Excessively high or low temperature
5. High voltage
6. Radioactive materials
7. Poisonous materials
8. Reciprocating equipment
9. Rotating equipment
10. Spring loaded devices
11. Falling objects

12. Suspended objects

It is important that hazardous elements encountered during operation as well as those encountered during installation, testing, maintenance and decommissioning also be considered.

A particular chemical may not be dangerous as such but it could produce a dangerous situation if it reacts with another chemical. All chemicals and materials should be viewed in such a context and any chemical or material that could produce a safety hazard should be listed. An equipment or component suspended from the ceiling may pose a safety hazard since it could injure people if the suspension system fails. Also, equipment and components fixed at some elevation from the floor level could become a safety hazard if the fixture fails.

Secondary events should also be considered. For example, a high-mounted equipment may be located further away from work places thus posing no hazard to workers. However, should the fixtures fail and the equipment fall on another equipment, say on a toxic chemical storage tank, the latter may fail due to impact of the falling object and release toxic chemical to the environment. This is called a secondary accident. Thus a seemingly harmless equipment, fixed at an elevation, could pose a safety hazard if its location is such that it could interact with other hazardous sources.

The preliminary hazard analysis may be stopped here if no hazardous sources are found.

2.3 **Preparation of Hazards and Effects Tables**

A suggested format for Hazards and Effects Tables is sown in Table 1. There are 11 items to be entered. Some of the items may be omitted or left blank, depending on the scope of the analysis. Each item is explained below. (NOTE: We have listed each item in a row. Some analysts prefer to list them column-wise. Either practice is acceptable.)

1. Hazardous source: The hazardous sources identified in Task 2 (see Section 2.2) are entered in this column one by one.

2. Location and identification of the hazardous source: The identifying name or number of the hazardous source, if any, (as referred in drawings or other documents) and its location are entered here. The location of a hazardous source may be identified by building names, grid number used in drawings, or other means. Location is important because accidents may be reduced or avoided in some cases by locating the hazardous source away from the trigger. If the system is a relatively simple one involving only a few components and is located in a narrow area, this item may be omitted or left blank. If the system contains a large number of components or is spread over a wide area covering a number of rooms or floors, location and identification of the hazardous source will be useful.

3. Trigger mechanisms: As discussed earlier, a hazardous element may not pose a danger under normal conditions. It becomes a safety problem only when some operation, event or process triggers it towards an accident. (More than one trigger mechanism may be needed to trigger an accident in some cases.) A partial list of trigger mechanisms is given below.

1. Chemical reaction
2. Corrosion
3. Explosion
4. Fire
5. Leak
6. Overloading (electrical)
7. Overloading (mechanical)
8. Vibration
9. Material degradation
10. Excessively high voltage
11. Excessively high or low temperature
12. Excessively high or low pressure
13. Mechanical shock
14. Equipment failure
15. Structural failure
16. Power failure
17. Operator error
18. Sabotage

What is a trigger mechanism to one hazardous source may not necessarily be a trigger mechanism in relation to another hazardous source. Also, whether a particular hardware, material or chemical is a trigger may depend on its proximity to the hazardous source and this should be considered in deciding whether a hardware, material or chemical is a trigger. Even if the hazardous source and the trigger are located at a reasonable distance, the Hazards and Effects Table may include a cautionary note that no design changes shall be made to bring the two closer.

In some instances, whether a candidate hardware, material or chemical triggers an accident may

depend on environmental condition (temperature, pressure, etc.). This should be considered and, if appropriate, a cautionary note may be added about temperature and pressure limits.

It is important that not only trigger mechanisms encountered during operation of the system but also those encountered during installation, testing, maintenance and decommissioning be included.

4. Accident: Interaction of the hazardous element with the trigger mechanism results in an accident. For example, corrosion (trigger) in a tank containing poisonous gas (hazardous element) may eventually result in gas leakage (accident). A strong mechanical [illegible] rips equipment located at an elevation (hazardous element) [illegible] t is the accident.

5. E[illegible] property damage. Effe[illegible]

6. W[illegible] ects of the accide[illegible] detectors are examp[illegible] ere. If not, state "none"

7. Safe[illegible] tely eliminate the acci[illegible] e hardware or an opera[illegible] rom triggers is also a

Consider [illegible] may be continual[illegible] nal pressure increases [illegible] valves may be added t[illegible] y of pressure v[illegible]

Consider tl[illegible] nts of the blade will b[illegible] y equipment. [illegible] lades for cracks coul[illegible]

Frequency o[illegible] e system. That is, accident freq[illegible] g operating pressures, operating temperatures [illegible] potential to be triggering mechanisms.

If a safeguard is built into the system, it shall be noted here. If not, state "none". This item is omitted in some Hazards and Effects Tables.

8. Safeguards - Mitigation of effects: Adverse effects of the accident could be mitigated by installing appropriate hardware or through appropriate operating procedures. Fire extinguishers are examples of this kind of safeguard.