

Introduction to Hazard Evaluation

An Online Continuing Education Course for Engineers

Course Number: H-3004

Credit: 3 Hours / 3 PDH / 3 CPD

Introduction to Hazard Evaluation

Introduction

Hazard evaluation is the first step in preventing accidents, injuries and property damage. It is a systematic process of identifying hazards and the failure modes that allow them to be realized. There are five mandatory steps in the process, and an optional sixth step (probability) that may be utilized as the hazards and failure modes are tackled to improve safety. Hazard evaluation should always be followed up with a plan and actions to deal with those hazards in accordance with the tenets of safety engineering.

The six steps are:

- 1) Establish boundaries
- 2) Identify hazards
- 3) Identify failure modes
- 4) Evaluate exposure
- 5) Identify consequences
- 6) Determine probability

There are numerous methods (over 25) of hazard evaluation. Among these are the checklist and what-if methods, which will be emphasized in this course. Several other methods were developed specifically for large-scale hazard evaluations, especially in the process industries, such as chemical plants and refineries.

For a small-scale hazard evaluation, some of these methods are not very practical. The checklist system, the what-if method or the combined checklist/what-if system can work well for small-scale products, such as a home appliance, or for a simple process.

Some hazard evaluation methods combine one or more of the six steps. The following sections give an overview of each step.

Step 1 - Establish Boundaries

The first step in hazard evaluation is setting the boundaries of the system under analysis. The system boundaries should be described in writing or clearly marked on a drawing or process diagram.

Subdividing a large system can make a large hazard evaluation more manageable. Whether a system is subdivided or not, it is important to make sure all interfaces inside and outside the system are accounted for. A hazard evaluation must also account for all the modes or types of operation of a given system or process.

Step 2 - Identify Hazards

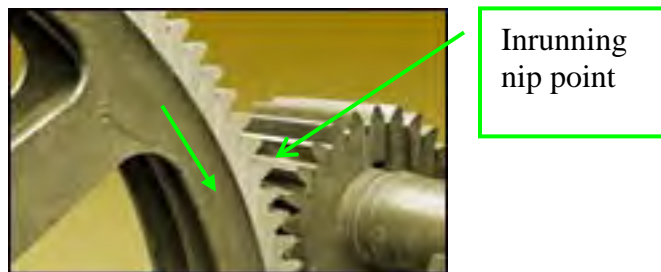
The next step is to identify the hazards within the system boundaries. Hazards cover a wide range, from gravity to high pressure gases to hot surfaces to radiation sources. One definition of a hazard is “a

potential for doing harm” (Roland and Moriarity, 1983).

Many common hazards have been identified in the literature on hazard evaluation. A checklist of some hazards is given later.

One class of hazards is the mechanical hazards: nip points, shear points, pinch points and snags. The photo below shows an inrunning nip point between two meshing gears.

There are also thermal hazards, chemical hazards, fire and explosion hazards, ergonomic hazards, electrical hazards, radiation hazards and more. Chemical hazards can be reactive, poisonous, mutagenic, teratogenic, carcinogenic, and/or cause a fire or explosion. Electrical hazards include high voltage and electrocution, as well as arch flash and short circuits.



Inrunning nip point between meshing gears

Step 3 - Identify Failure Modes

Failure modes are specific occurrences that allow a hazard to be realized into an injury or property damage. To describe failure modes, consider the specific example of a high pressure gas pipeline. The gas inside the pipeline is hazardous, but as long as it is safely inside the pipe, the hazard is not realized. If the gas gets outside the pipe, devastation can be the result.

Therefore, one set of failure modes for this hazard would be unintentional release of gas from the pipeline. One failure mode might be internal corrosion that allows the pipeline to fracture. This was the cause of a gas pipeline explosion near Carlsbad, New Mexico in 2000 that caused 12 fatalities.

Step 4 – Evaluate Exposure

The exposure of a hazard is the individuals or property that can be injured or damaged by the realization of the hazard. For example, the person likely to be harmed by a point of operation hazard on a press is the operator, if the problem occurs in normal production. Sometimes a bystander is injured in addition to the person operating the machine.

A whole population outside the plant can be affected by the right kind of hazard. The poisonous gas cloud that drifted out from the Union Carbide plant in Bhopal, India in 1984 killed several thousand individuals and severely injured many more.

Step 5 – Identify Consequences

The consequences are the types of injury or property damage that occurs if the hazard is realized through a failure mode. Most hazards or failure modes have a range of possible consequences. It is not necessary to identify every possible consequence, just the most damaging reasonably possible injury or property damage scenario. For example, a fall from a 20-foot ladder could result in a sprained ankle, a broken elbow or even death. The only consequence that needs to be retained is death, as it is the worst reasonably possible outcome.

Step 6 – Determine Probability (Optional)

The sixth step is determining the probability of a hazard being realized and is optional.

The probability information may be used to prioritize the subsequent steps of determining how to correct hazards. The overall risk should be evaluated when setting priorities.

Determining probability is not an exact science. It involves the judgment of the hazard evaluation team.

Detailed Discussion of Hazard Evaluation Steps

Step 1 – Establish Boundaries

Establishing the boundaries of the system to be analyzed is the first step in hazard evaluation. The system boundaries should be unambiguous, and described in writing or clearly marked on a drawing or process diagram so they are easily understood.

A large hazard evaluation can be made more manageable by splitting it up. Large systems can be broken down along different types of boundaries, such as physical boundaries, or arbitrary boundaries. Whether a system is subdivided or not, all interfaces inside and outside the system must be taken into account.

For example, consider a 5-axis CNC milling machine which is loaded by a robot removing parts from one conveyor and unloaded by the same robot placing the finished parts on another conveyor. If the system includes the milling machine and the robot, the hazard evaluation would include the interaction of the robot with the CNC mill (internal interface) and both conveyors (external interfaces).

Each type of function, process or mode that each unit has must also be covered. A machine tool might have a normal production function, a fully automated function and a maintenance mode. Other functions or modes might include set-up, jam clearing, replenishment or restocking, part loading and unloading, die-setting, tool changing, diagnostic mode, service mode, system upsets, start-up, transients, normal mode, steady-state, shutdown procedures, forward, reverse, inch, stop, emergency stop, backwash, adjustment, manual mode, partial revolution, flameout, overpressure, underpressure, backwash, self-clean, defrost, and so forth.

A product or process cannot be analyzed in a vacuum. The system must include its environment and the operators or users. Since users and operators are people, that means foreseeable misuse and abuse is another mode that must be considered in a hazard evaluation.

Operators and users do not always follow all instructions; in fact, they can be counted on sooner or

later to not follow an instruction. People are not perfect and will not behave perfectly. The hazard evaluation must include reasonably foreseeable uses and misuses of the product, including non-compliance with warnings and instructions.

In addition to products and equipment, hazard evaluations are also performed on processes, both simple and complex. A typical simple process might be a person performing a specific task in a specific location, such as assembling products on an assembly line. The system in this case would encompass the worker, the work environment, the tools used, the product and parts under assembly, and any material handling equipment or tools. Each different function, mode and process would need to be investigated. A job hazard analysis (JHA) is a specific tool to analyze job tasks. PDHengineer offers an entire course titled “Job Hazard Analysis” based on OSHA 3071.

A process might also be as complex as producing gasoline, diesel fuel and other petroleum products from crude oil, or producing liquid nitrogen and liquid oxygen. There are several methods specifically designed for and/or used for hazard evaluation of large-scale processes. These include Hazard and Operability Analysis (HAZOP), Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis, Event Tree Analysis and Cause-Consequence Analysis.

Space Shuttle Challenger Disaster

The consequences of not checking all the modes of a system are graphically illustrated in the 1986 Challenger space shuttle disaster. There were multiple failures in the decision-making processes leading up to this event, but fundamental was the failure to adequately consider the hazards of a cold temperature launch.

The Challenger shuttle broke up shortly after liftoff on January 28, 1986. The mission, STS 51-L, was going to place a communications satellite and place and retrieve a comet research laboratory, as well as carry the first Teacher-In-Space, Christa McAuliffe.

About 72 seconds into the flight, the right solid rocket booster lower strut came loose and allowed the booster to pivot. The hydrogen fuel tank then failed, followed by the oxygen tank.

All seven aboard the shuttle were killed. It is theorized that they lived until the cabin impacted the ocean after falling for two minutes and 45 seconds from a height of 65,000 feet.

The disaster started after the bottom joint on the right solid rocket booster began leaking, even before the shuttle lifted off the launch pad. The solid rocket, built by Morton Thiokol, was constructed in sections sealed with o-rings. The boosters were reusable and had been used before, which had somewhat changed the dimensions of the pieces.

The o-rings had never been tested in actual use at temperatures below 53° F. In every single previous launch below 61° F, at least one set of o-rings had shown evidence of blow-by of hot gases. In the 21 launches at or above 61° F, there had only been four instances of o-ring blow-by.

The temperature at launch was about 36° F, and overnight temperatures had been as low as 19° F. The Rogers Commission estimated the temperature of the right booster aft joint at 23° – 33° F, far below the temperature of any previous shuttle launch.

Analysis of film from the launch pad showed that puffs of smoke were visible from the o-ring starting at less than 0.7 seconds after ignition of the solid rocket motor. About 59 seconds after ignition, a

tongue of flame was visible from the leaking joint on the right booster. As the flame grew larger it impacted the brace holding the solid rocket booster to the external fuel tank. This eventually failed, leading to the breakup of the shuttle.

A telephone conference had been held the night before between NASA personnel and Morton Thiokol engineers and managers concerning the safety of the launch at cold temperatures. Morton Thiokol engineers were very concerned that the o-rings had never been tested at temperatures that cold and they knew the o-rings didn't seal as well at lower temperatures, due to lower resilience. However, NASA essentially pushed for Thiokol to prove the o-rings weren't safe at the low temperatures. Thiokol managers eventually overrode the Thiokol engineers' concerns and told NASA the o-rings were good to go.

The o-rings are less resilient at low temperatures. When the solid rocket booster would be launched, the joints would experience a temperature drop. This sluggishness would still be on the pad. This burst of pressure would come out of the gap and while the solid rocket joint

It is theorized that during liftoff and a portion of the booster joint

When the solid rocket booster is launched, the joints would experience a temperature drop. This sluggishness would still be on the pad. This burst of pressure would come out of the gap and while the solid rocket joint

for much of the structure during a portion of the solid rocket

To view the remainder of the course material and to take the quiz for PDH credit, you must purchase the course.

Close this window and click "Add to cart" on the product page.

Step 2 - Ide

The next step is to identify pinch points and hazard as "a

Many common hazards will not attempt to produce a cl

Another source of professional hazards is nip points, s

Besides mechanical and ergonomic hazards, there are many types of hazards

hazards, fire and explosion hazards, chemical hazards and more. Some of these classes have many types of hazards. Chemical hazards can be reactive, poisonous, mutagenic, teratogenic, carcinogenic, and/or cause a fire or explosion. Electrical hazards include high voltage and electrocution, as well as arc flash, loose connections that overheat and short circuits. Short circuits can result in unintended disasters. The 1989 in-flight failure of a cargo door on a Boeing 747 was traced to a short circuit powering the latch motor. All eight door latches were opened by the motor, bending the door locks out of the way and allowing the door to blow off the aircraft. Nine passengers were killed when the door caused an explosive decompression that left a 15-foot by 13-foot hole in the fuselage on a United

mut from
ity defined a

his course
ethod of

ety
l hazards