How to Hunt Down and Handle Hazards

Howard Sneider,
CRB

February 21, 2013

ISPE®

Agenda

- Define Hazard
- Review Hazard Identification Techniques
- Review Hazard Mitigation and Elimination

- This presentation is a concise review of these topics!

ISPE

What is a Hazard

A Hazard is an inherent physical or chemical characteristic that has the potential for causing harm to people, the environment, or property.

Center for Chemical Process Safety, "Guidelines for Hazard Evaluation Procedures," 3rd ed., American Institute of Chemical Engineers, New York, NY, and John Wiley & Sons, Inc., Hoboken, NJ (2008).

Why Have Hazards?

- Can't we always identify processes and materials that are non-hazardous

Not exactly….

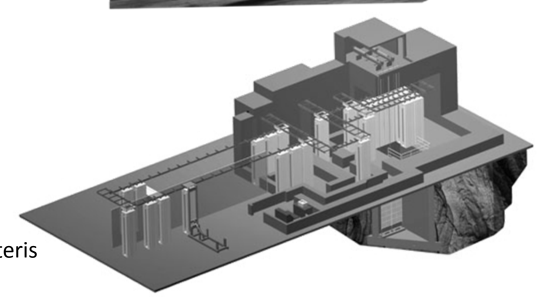
Process Property

- Sterilization
- Hold Vessel

Courtesy of Steris

Material Properties

- Fuel
- Radiation

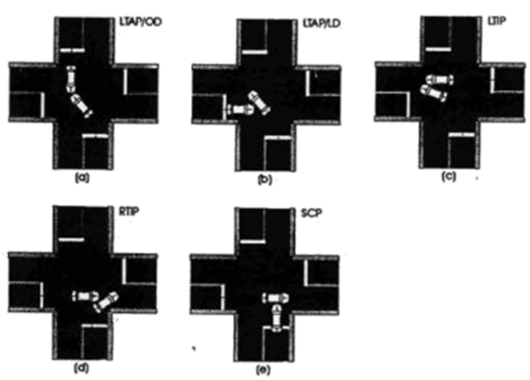


Courtesy of Steris

Hazards are only part of the "Problem"

- A **safety event** causes an **undesirable event** when a **barrier** that is normally in place to control a **hazard** fails.
- When hazard control is lost the **potential outcome** of the undesirable event may be limited and recovery may be hastened by **hazard mitigation.**

What is the Hazard?

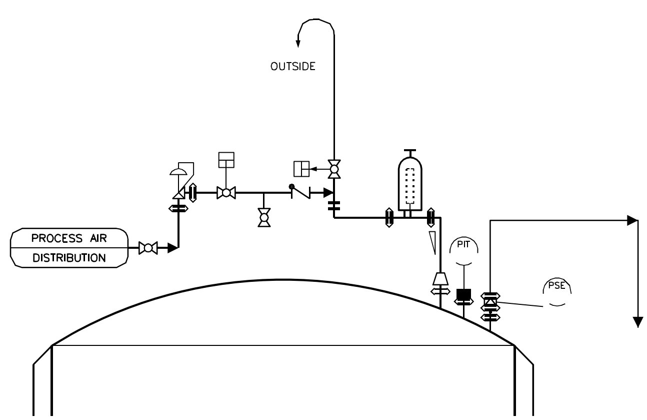


Bellomo-McGee Incorporated. *Intersection Collision Avoidance Study.* September, 2003. Intelligent Transportation Systems Joint Program Office Technical Report No. FHWA-JPO-05-030

Hazards are only part of the "Problem"

- A **failure to stop** causes an **automobile collision** when a **stop sign / attention to surroundings** that is normally in place to control **traffic at an intersection** fails.
- When traffic at an intersection control is lost the **passenger injuries** of the automobile collision may be limited and recovery may be hastened by **air bags and seat belts.**

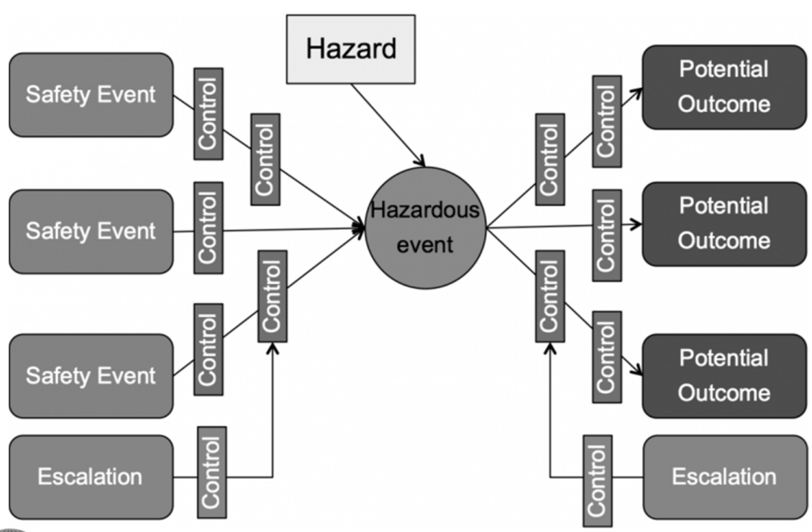
What is the Hazard?



Hazards are only part of the “Problem”

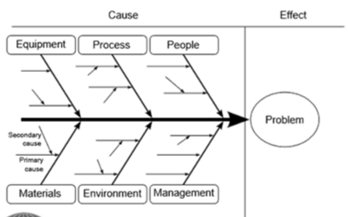
- An **equipment malfunction** causes an **increase in vessel pressure** when a **pressure regulator** that is normally in place to control **overpressure** fails.
- When overpressure control is lost the **vessel damage** of the increase in vessel pressure may be limited and recovery may be hastened by a **rupture disk.**

Hazards are only part of the “Problem”



What are we looking at?

- **System**
  - People
  - Procedures
  - Equipment
  - Area



- **Ishikawa 6 M's**
  - Machine (Technology)
  - Method (Process)
  - Material (Raw Materials and Information)
  - Man/Mind Power
  - Measurement
  - Milieu/Mother Nature (Environment)

How to Identify Hazards

Required Detail / Preparation

- Checklist
- What if?
- HAZOP
- LOPA
- FMEA
- Fault Tree Analysis

PHA
Process
Hazard
Analysis

Checklist

- Lists of known hazards or hazard causes
- May be used in combination with other techniques – Not scenario based
- Sample Section Headings
  - Bio-mechanical and Postural
  - Physical Environment and Workplace Design
  - Mechanical
  - Electrical
  - Chemicals and Toxicity
  - Biological and Human
  - Organizational and Procedural Arrangements
  - Psycho-social Environment and Task Design
  - Natural Environment

What if?

- Purpose is to identify all the hazards which are "inherent in the job"
- Requires multidisciplinary subject matter experts and facilitator. To ask
  - What if…?
  - Could someone…?
  - Has anyone ever…?
- Prioritize
  - Accidents, near-misses, complaints (similar or actual)
  - User and EHS staff concerns
  - Code

HAZOP– HAZard and OPerability

- Evaluates each aspect of the system to determine how it may deviate from normal (safety event or barrier) and lead to an undesirable event
- Evaluation Process:
  - select appropriate **parameters** which apply to the design intention.
  - apply **guide words** to each parameter for each section of the process
    - No or not
    - More
    - Less
    - As well as
    - Part of
    - Reverse (of intent)
    - Other than
    - Early
    - Late
    - Before
    - After

HAZOP– HAZard and OPerability

- **HAZID** - **HAZ**ard **Id**entification
  - What are the possible significant **deviations** from each system aspect?
  - What are the feasible **causes** of each deviation?
  - What are the likely **consequences** of each deviation?
- Evaluating preventive or proactive barriers
  - It can then be decided whether existing, designed safeguards are sufficient, or whether additional actions are necessary to reduce risk to an acceptable level.

LOPA – **L**ayer **O**f **P**rotection **A**nalysis

- Scenario Based – considers one scenario at a time
- Identify all safety events and determine the frequency of each
  - The safety event frequencies should be based on industry-accepted and standards-compliant failure rate data for each device, system, or human.
- Determine the consequence of the hazard scenario – Safety, Environmental, Economic

LOPA – **L**ayer **O**f **P**rotection **A**nalysis

- Use a risk matrix to determine if risk of scenario occurring must be reduced. If so, add IPL(s).
- IPL - **I**ndependent **P**rotection **L**ayer - capable of detecting and preventing or mitigating the consequences of the safety event.
- PFD - **P**robability to **F**ail on **D**emand = SIL - **S**afety **I**ntegrity **L**evel[1]. Will the IPL work?

1. SIL serves as the benchmark for Safety Instrumented System design, operation, and maintenance according to ANSI/ISA 84.01-1996 (2) and IEC 61511 (3).

FMEA - Failure Mode and Effect Analysis

- For each process input, determine the ways in which the input can go wrong (failure mode).
  - A failure mode is the failure state of the system or component
  - Examples of failure modes are fail to start, fail to open, fail to shutdown
- For each failure mode, determine effects. Select a severity level for each effect.
- Identify potential causes of each failure mode. Select an occurrence level for each cause.
- List current controls for each cause. Select a detection level for each cause.

FMEA - Failure Mode and Effect Analysis

SEV = How severe is effect on the customer?

OCC = How frequent is the cause likely to occur?

DET = How probable is detection of cause?

RPN = Risk priority number in order to rank concerns; calculated as SEV x OCC x DET

Process step	Potential failure mode	Potential failure effects	SEV	Potential causes	OCC	Current process controls	DET	RPN
What is the step?	In what ways can the step go wrong?	What is the impact on the customer if the failure mode is not prevented or corrected?	10	What causes the step to go wrong? (i.e., How could the failure mode occur?)	10	What are the existing controls that either prevent the failure mode from occurring or detect it should it occur?	10	**1000**

FMEA - **F**ailure **M**ode and **E**ffect **A**nalysis

E	F	G	H	I	J	K	L

calculated as SEV x OCC x DET

ential uses	OCC	Current process controls	DET	RPN	Actions recommended	Responsibility (target date)	Actions taken
auses the go (i.e., uld the node	10	What are the existing controls that either prevent the failure mode from occurring or detect it should it occur?	10	**1000**	What are the actions for reducing the occurrence of the cause or for improving its detection? You should provide actions on all high RPNs and on severity ratings of 9 or 10.	Who is responsible for the recommended action? What date should it be completed by?	What were the actions implemented? Include completion month/year (then recalculate resulting RPN).

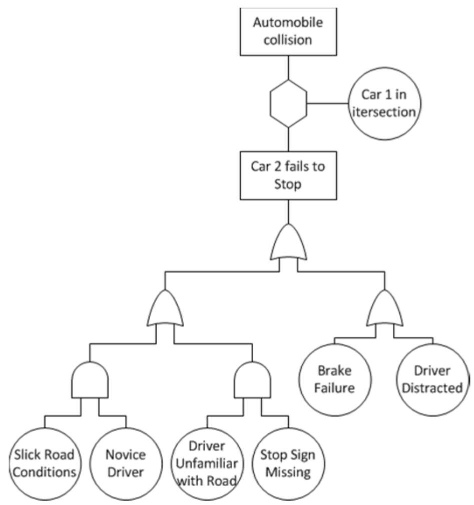
ISPE

Fault Tree Analysis

- Steps:
  - An undesired event is defined
  - The event is resolved into its immediate causes
  - This resolution of events continues until basic causes are identified
  - A logical diagram called a fault tree is constructed showing the logical event relationships

ISPE

Fault Tree Analysis



Options for Eliminating Reducing and Controlling Hazards

- Procedural
  - use operating procedures, safety rules and procedures, operator training, emergency response procedures, and management systems to manage risk.
- Active
  - manage risk using process control systems, SIS, mitigation systems, and other active systems.
- Passive
  - minimize hazards using process or equipment design that reduce the likelihood /consequence of an incident without the active functioning of any device.
- Inherent
  - eliminate hazards by a shift to nonhazardous or much less hazardous materials and conditions.

ISD - Inherently Safer Design

- The most effective approach to process risk management is the elimination of hazards where feasible rather than relying on safety systems and procedures to manage risk.

Center for Chemical Process Safety, “Inherently Safer Chemical Processes: A Life Cycle Approach,” 2nd ed., American Institute of Chemical Engineers, New York, NY, and John Wiley & Sons, Inc., Hoboken, NJ (2009).

Kletz, T. A., and P. Amyotte, “Process Plants: A Handbook for Inherently Safer Design,” 2nd ed., Taylor CRC Press, Boca Raton, FL (2010).

Inherently Safer

- Substitute
  - use less-hazardous materials, chemistry, and processes.
- Minimize
  - use small quantities of hazardous materials; reduce the size of equipment operating under hazardous condition such as high temperature or pressure.
- Moderate
  - reduce hazards by dilution, refrigeration, or process alternatives that operate at less-hazardous conditions.
- Simplify
  - eliminate unnecessary complexity.

Eliminating Reducing and Controlling Hazards in your Process

- Conceptual Design
- Front End Engineering
- Detailed Design
- Procurement Construction
- Operating Process
- Shutdown

- Eraser
- Paper Shredder
- Big Paper Shredder
- Bank Loan/Sledgehammer
- Backhoe
- Backhoe

ISPE

Not always a Best Option

- Intensify Other Hazards
- Create new Hazards
- May shift hazards from plant to environment
- Design decisions must consider all process hazards

ISPE

Hazard Reduction Drivers

- Cost Savings
  - Less protective equipment required.
  - Less training
  - Less Instruments
  - Less maintenance
  - Smaller size

Hazard Reduction Drivers

- Regulatory
  - OSHA's process safety management (PSM)
  - EPA Risk management program (RMP)
  - Toxic Catastrophe Prevention Act (TCPA) Program
  - Industrial Safety Ordinance
- Voluntary
  - OHSAS 18001