

# Improving Safety Through Detailed Risk Assessment



Presented by

**Scott Genta**

**Safety Management Services, Inc.**

# SMS Personnel

- **Expertise**

- Chemical processing, handling, transportation, and storage
- Propellants and explosives

- **Disciplines**

Chemical engineering

Physics

Mechanical engineering

Process control

Computer technology

Chemistry

Electronics

# SMS Heritage

- **Hercules Aerospace**
  - Hazards Analysis & System Safety Groups
- **Global Environmental Solutions (GES) - Hercules Aerospace & ATK Subsidiary**
  - Demilitarization
  - Environmental Remediation
  - Safety Management Services
- **Safety Management Services, Inc.**

# SMS Capabilities

- **Risk Management and Process Hazards Analysis Methodologies**
  - Qualitative (HAZOP, FMEA, etc.)
  - Quantitative (Fault Tree, Probabilistic Analyses, etc.)
- **Compliance**
  - OSHA PSM, EPA RMP, DOD, VPP
- **Training**
  - Related to Risk Management and Process Hazards Analysis
- **Material Characterization Testing**
  - Sensitivity & Reactivity Testing
  - DOT Classification Testing and Analysis
  - Test Equipment
- **Facility Siting & Design**
  - Quantity Distances, Venting, Barricades, Workstation Protection, etc.
- **Ergonomic Analysis**

# **SMS Experience & Expertise Applied to Various Industries**

- **Commercial & Government Contract Summary**

- Aerospace**

- Air Bag Manufacturers & Suppliers**

- Chemical processing**

- Commercial Explosives Manufacturing**

- Demilitarization**

- DOT Classification**

- Explosives Contaminated Site Remediation**

- Ordnance**

- OSHA Technical Support**

- Petroleum refining**

- Pharmaceuticals**

- Research**

# **Risk Management Heritage**

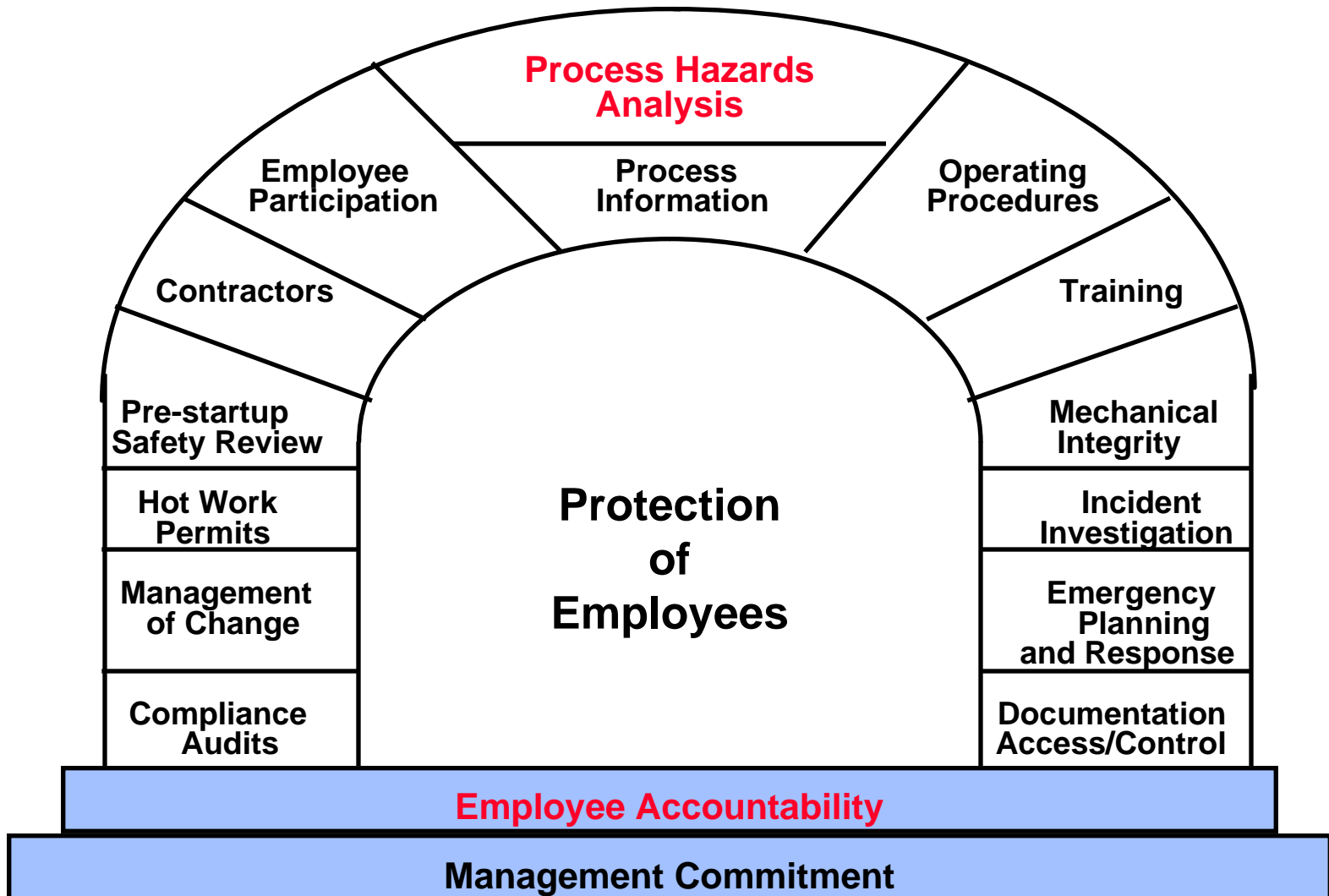
# Explosives Manufacturing Risk Management Heritage



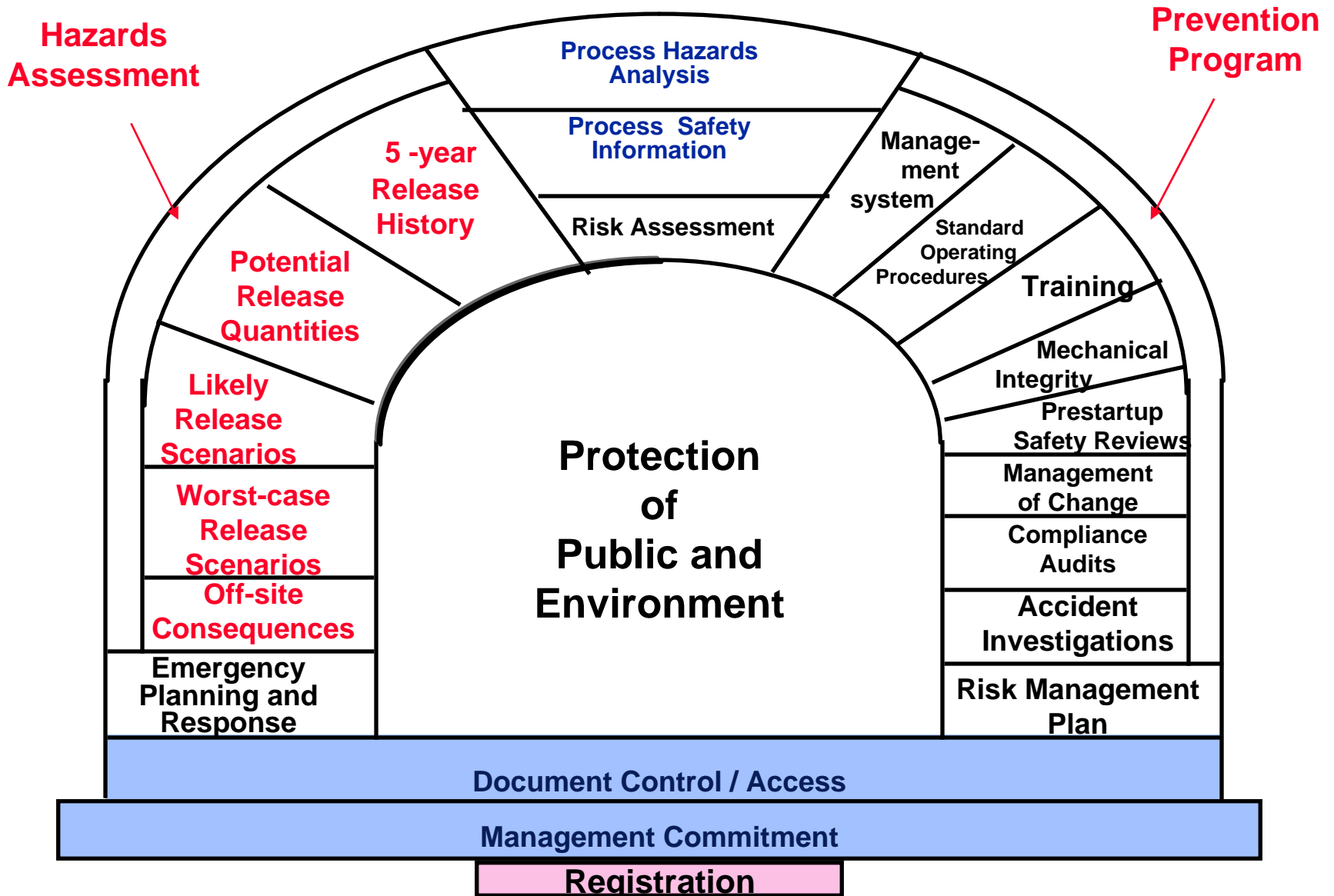
1912		1960	1970	1980	1990	Present
<p>Hercules</p> <p>Dupont</p> <p>Others</p> <p>NG Manufacture</p>		<p>Risk Methods Improved</p> <p>Material character- ization testing</p> <p>Explosives Safety Standards</p>	<p>Fault trees</p> <p>FMEA</p> <p>Probit analysis</p> <p>In-process simulation</p>	<p>Specialized testing &amp; modeling</p>	<p>OSHA 29 CFR 1910.119</p> <p>EPA RMP</p>	

**Video**

# OSHA PSM



# EPA 40 CFR Part 68 Elements



# OSHA's Voluntary Protection Programs Management Guidelines

Work Site Analysis

Baseline  
Hazard Analysis

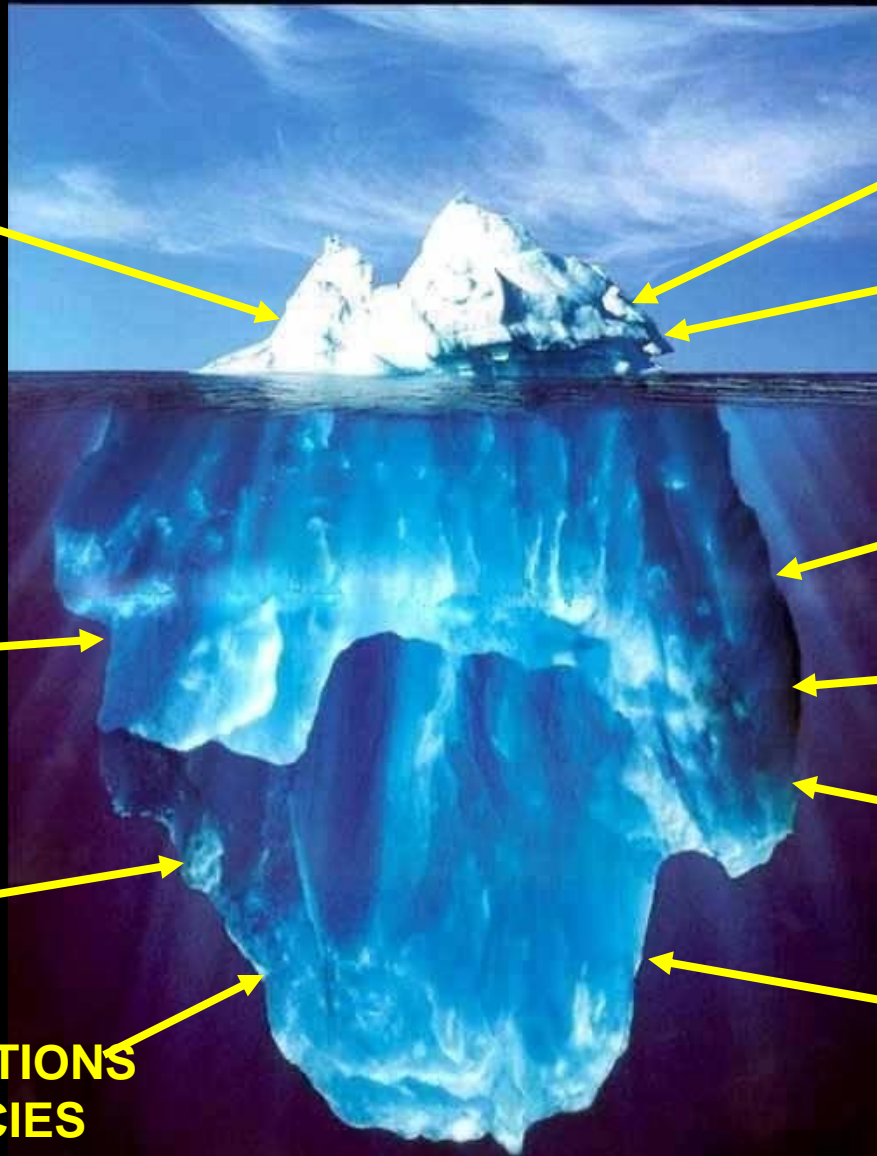


# The Challenge for Many Industries Today

- Operating under downward pricing pressure
- Can companies still perform a detailed risk assessment?



# NOT ALL INCIDENT COSTS ARE EASILY VISIBLE



**PERSONAL  
INJURY/ FATALITY**

**OSHA FINES**

**FACILITY/  
EQUIPMENT  
DAMAGE**

**INCREASED  
INSURANCE  
PREMIUMS/  
DEDUCTIBLES**

**PERSONAL  
SUFFERING**

**LAW SUITS**

**RECURRING  
OSHA INSPECTIONS**

**DAMAGED  
REPUTATION**

**TRIGGER OF INSPECTIONS  
FROM OTHER AGENCIES**

**LOST BUSINESS**

# What Creates the Need for Detailed Systematic Hazard Analysis?

- **Accidents** **cost** company resources, competitive advantage, and profits
- **Management** can be held **criminally liable** for **negligence in safeguarding** employees, community, and the environment
- **Corporation** “**downsizing**” results in limited resources to **focus** on risk reduction

# **Level Setting**

**Fundamental to  
Hazard Analysis and Risk  
Management**

**Operation / Equipment Prioritization**

**Hazard Identification**

**Hazard  
Ranking**

**Failure Scenarios**

**Critical  
Scenarios**

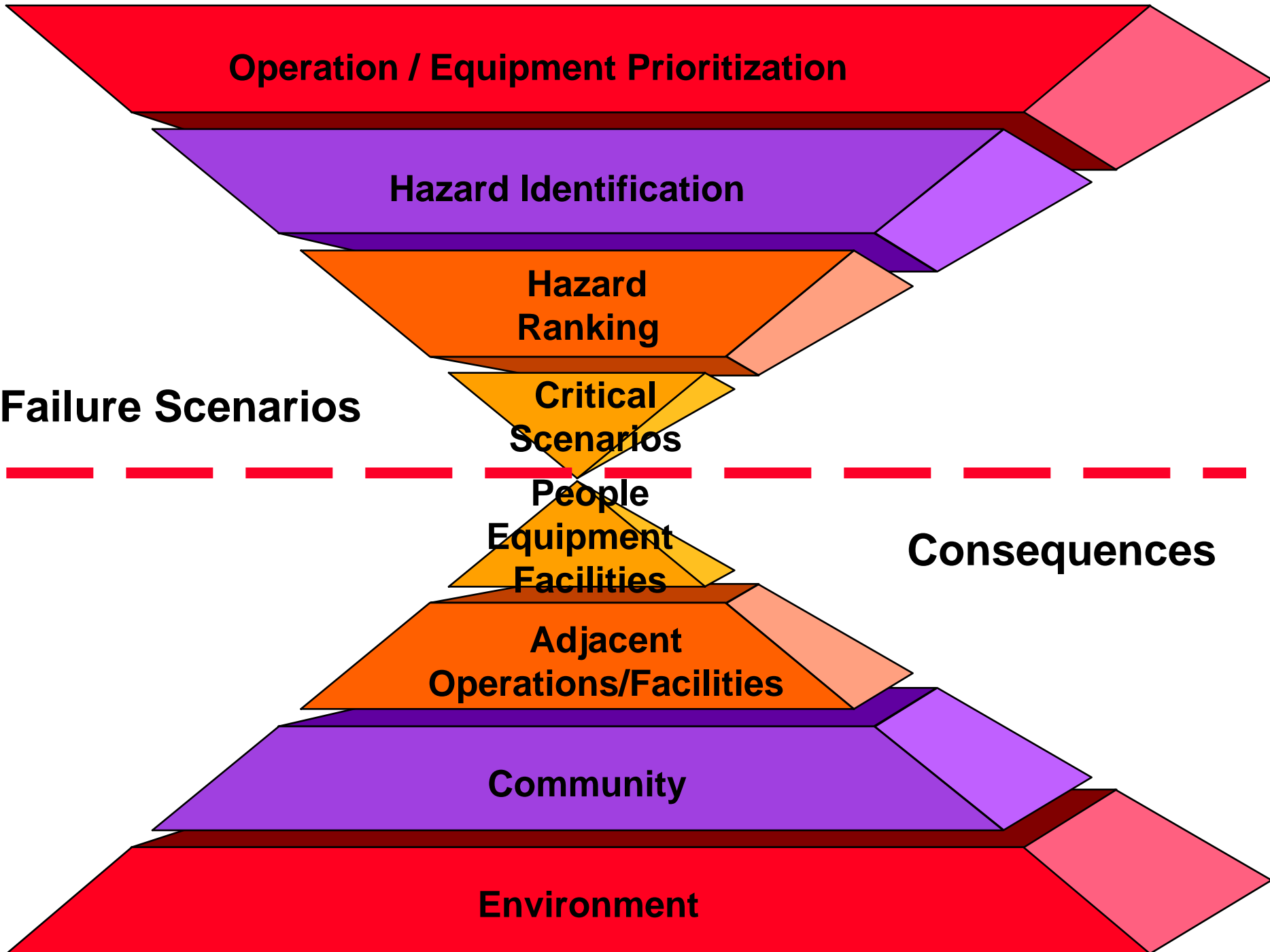
**People  
Equipment  
Facilities**

**Consequences**

**Adjacent  
Operations/Facilities**

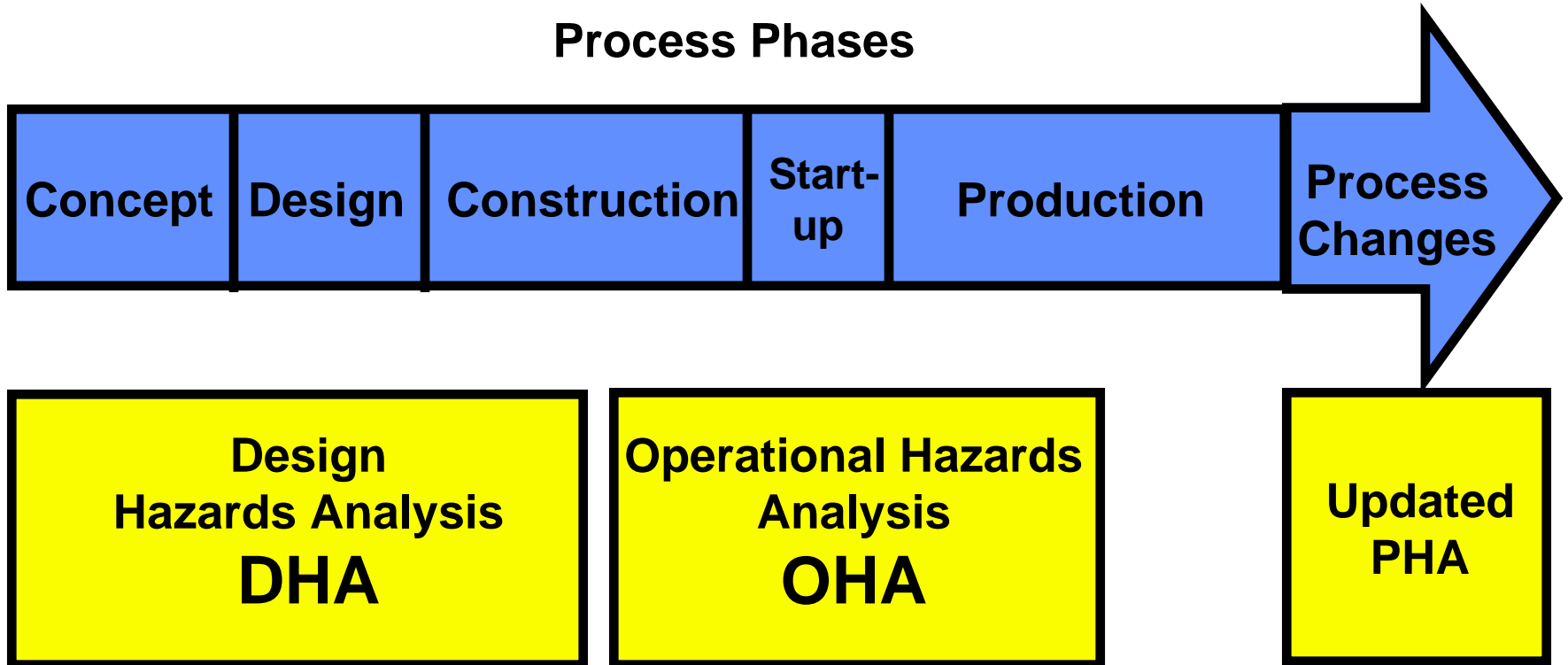
**Community**

**Environment**



# PHA Phases

Process Phases



**DHA + OHA = PHA**

The complexity of the Process Hazards Analysis must reflect the complexity of the process

Applying the correct methodology will efficiently identify critical hazards

# Inductive Approach

- **General characteristics--asks “what-if?”**
  - System broken down into individual components
  - Consider potential failures for each component (what could go wrong?)
  - Effects of each failure defined (What happens if it does go wrong?)
- **Applicability**
  - Systems with relatively few, less interactive components
  - Systems where single point failures are predominant

# Deductive Approach

- **General characteristics**
  - General nature of the hazard has already been identified (Fire, overpressure, etc.)
  - System is reviewed to define the cause of each hazard (how can it happen?)
- **Applicability**
  - All sizes of systems
  - Originally developed for complex systems
  - Designed to identify hazards caused by multiple failures

# PHA Methods

OSHA 29 CFR 1910.119

- Checklist
- What-if
- What-if Checklist
- Hazards and Operability Study (HAZOP)
- Failure Modes and Effects Analysis (FMEA)
- **Fault Tree (Logic diagram)**
- Appropriate equivalent (combination)

# Logic Diagrams

- Logic Diagram to identify potential hazards
  - Level setting
  - Focus analysis on critical paths
- Useful for simple to complex interactive systems
- Define **top undesirable event** for the **specified operation**
  - System
  - Subsystem
- Uses logic symbols to guide thinking and record thought process
- Identify potential “Contributing/Root Causes”

# Logic Diagrams

(continued)

- Inter-relationship between plant process, operations, and equipment
- Help identify potential failures
- Document level of detail of analysis
- **Fault trees can be quantified**

# Guidelines for Organizing the Logic Diagrams

**1<sup>st</sup> Level:** Define top level “undesirable event”

**2<sup>nd</sup> Level:** Identify major operational steps, major process components, or other factors

**3<sup>rd</sup> Level:** Subsets of 2<sup>nd</sup> Level (if appropriate)

**4<sup>th</sup> Level:** Types of energy present

**Subsequent**

**Levels:** Sources/events that could produce the identified energy

# Logic Diagrams (Cont.)

**Step #1: Define Hazardous  
(undesirable) Top Level Event (HTLE)  
for the specified operation**

– **Undesirable Events**

- » Personnel Injury/Death
- » Equipment/Facility Damage/Loss
- » Product Damage/Loss
- » Environmental Damage
- » Manufacturability (rate, labor costs, mat. costs
- » etc.

# Logic Diagrams (Cont.)

**Step #1: Define Hazardous  
(undesirable) Top Level Event (HTLE)  
for the **specified operation****

– Specified Operation(s)

» Handling

» Cleaning

» Maintaining

» Sampling

» Testing

» Mixing, pressing, extruding, casting, etc.

# Logic Diagrams (Cont.)

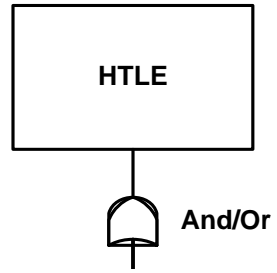
## Step #1: Examples

- Personnel exposure while sampling XYZ chemical stream
- Equipment damage/loss while mixing XYZ propellant
- Facility damage/loss during NG manufacturing
- Product damage/loss during cartridge XYZ loading
- Environmental damage due to release of MEK

### Specific Example:

- Personnel Injury while moving explosive product from production line to storage

Step #1



# Logic Diagrams (Cont.)

**Step #2**: Identify major operational steps, subsystems, etc.

## **Specific Example**:

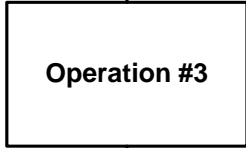
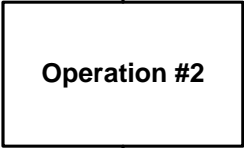
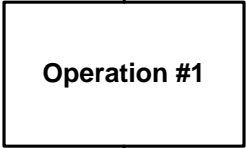
- Personnel injury while moving explosive product from the production line to storage
  - » Packaging/palletizing product
  - » Transporting product to truck dock
  - » Loading truck
  - » Transportation to storage building
  - » Unloading from truck
  - » Transporting into storage building
  - » Product stacking operations

Step #1



And/Or

Step #2



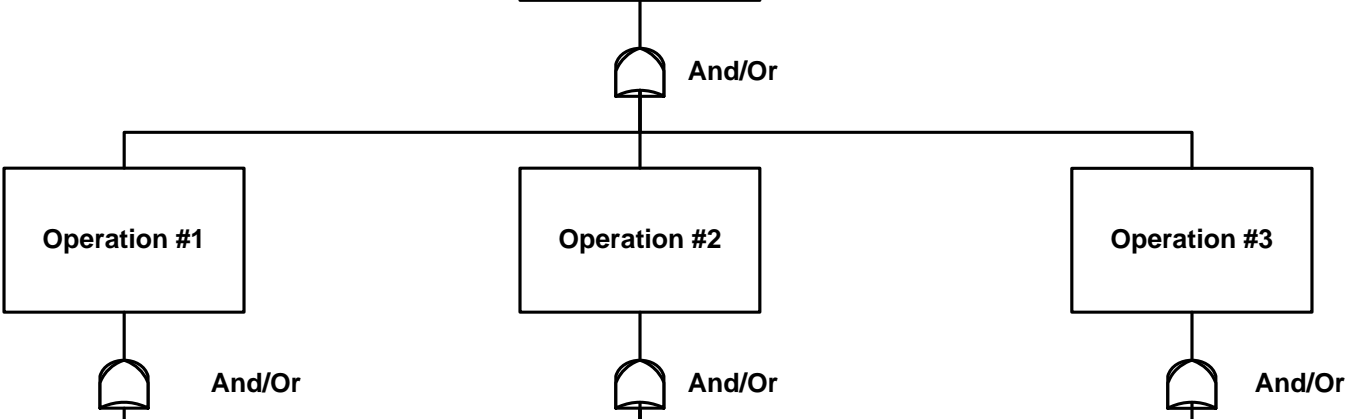
And/Or



And/Or



And/Or



# Logic Diagrams (Cont.)

## Step #3: Identify Subsets of 2<sup>nd</sup> Level (if appropriate)

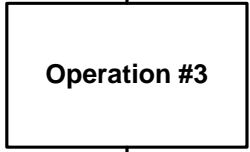
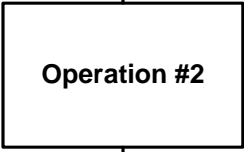
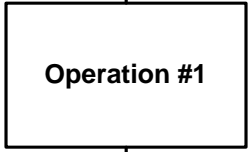
### Specific Example:

- Personnel injury while moving explosive product from production to storage
  - » Packaging/palletizing product
    - Placing items in box
    - Closing the box
    - Wrapping the box
    - Labeling the box
    - etc
  - » Transporting product to truck dock
    - etc.
  - » Transportation to storage building
    - etc.
  - » Unloading from truck
    - etc.

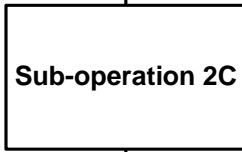
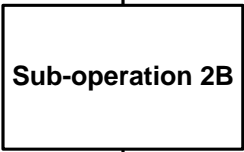
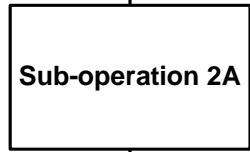
Step #1



Step #2



Step #3



# Root Cause Analysis Using Logic Diagrams (Cont.)

## Step #4:

- Identify Sources of the undesirable event (Hazards/Failure Mode) for the given operations, subsystem, etc.
- **Note: This Step is typically the level where Accident Investigation begins**
- Utilize a “Hazards” Checklist:

# Example: “Hazards” Checklist

- Chemical exposure
- Thermal exposure
- Mechanical energy
  - Pinching
  - Tripping/falling
- Chemicals/explosives ignition energies\*\*
- Thermal, ESD, friction, impact, shock, etc
- etc.

# Types of Energy

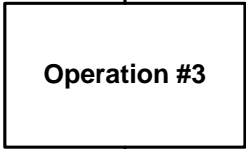
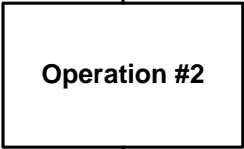
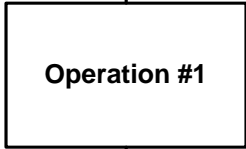
- **Energy**      **Examples**
  - Mechanical      Crushing, pinching, striking
  - Electrical      Electrical shock, short, heating
  - Thermal      Thermal ignition, heating, fire, exposure
  - Chemical      Burn, exposure, toxicity
  - ESD      ESD thin layer, device, human spark, dust cloud
  - Impact      Impact ingredient, component, shock
  - Friction      Friction ingredient, heating
  - Impingement      Impingement component, ingredient
  - Incompatible      Incompatible material(s)
  - Shock      Shock explosive, mechanical
  - Propagation      Propagation fire, explosion, detonation
  - Etc.

Step #1



And/Or

Step #2



And/Or

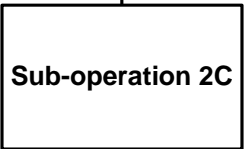
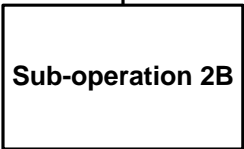
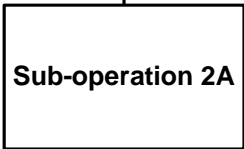


And/Or



And/Or

Step #3



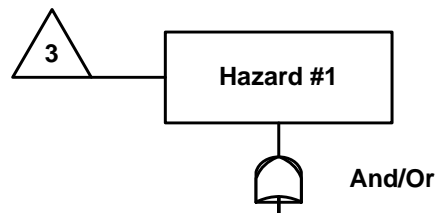
And/Or



Step #4



\*From Hazards Checklist



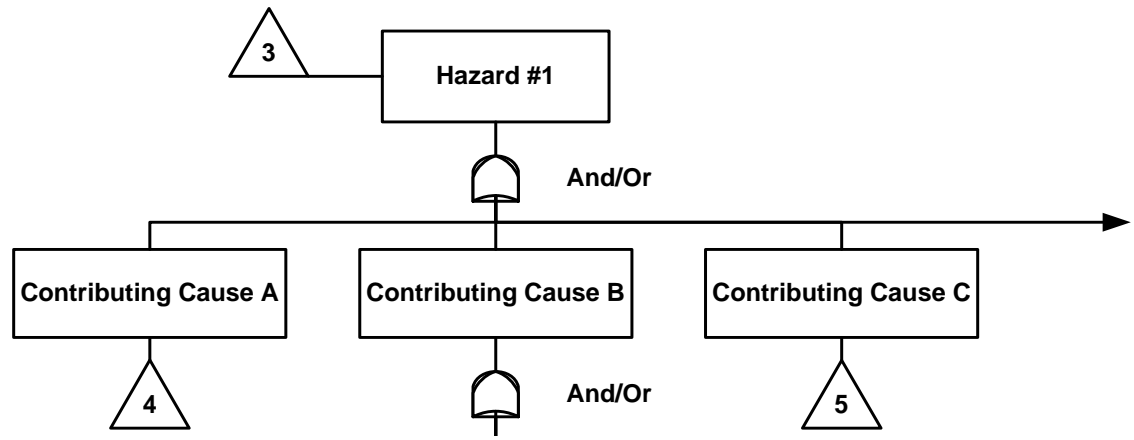
# Root Cause Analysis Using Logic Diagrams (Cont.)

## Step #5:

Identify “contributing causes” that individually or collectively result in the specific Hazard

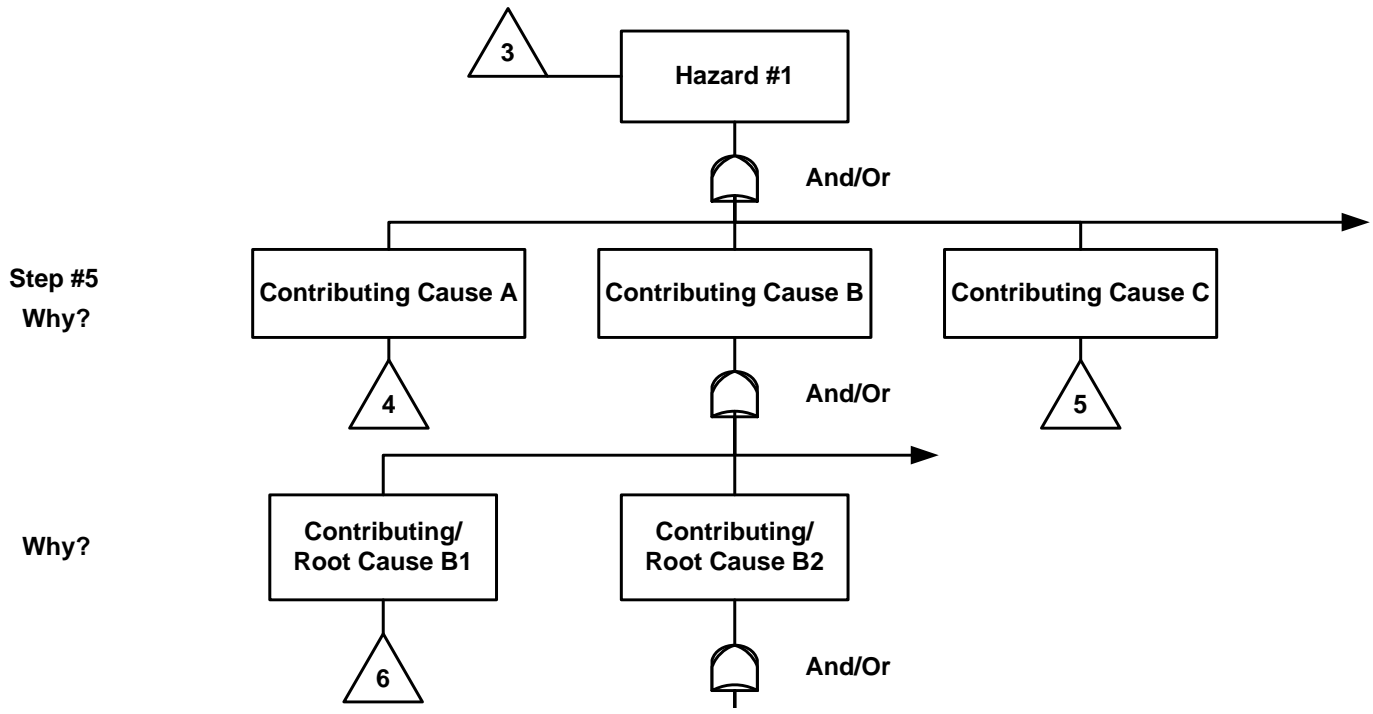
- “**Contributing Cause**” Checklists can be developed to help structure the evaluation.
- “**Contributing/Root Cause**” Checklists can also help structure the evaluation.

Step #5  
Why?



# Example: “**Contributing Cause**” Checklist

- **Equipment**
- **Control Systems**
- **Facility**
- **Environmental**
- **Human Error (Human Factors)**
- **etc.**



# Example: “**Contributing/Root Cause**” **Checklist**

- **Equipment**
  - **Design**
  - **Fabrication error**
    - » **Substitution of Materials of Construction**
    - » **Outside Tolerances ....**
  - **Maintenance**
  - **Process Control/Management of Change**
    - » **Foreign Objects**
    - » **Out of spec. materials ...**
  - **etc.**

# Example: “Contributing/Root Cause” Checklist (Cont.)

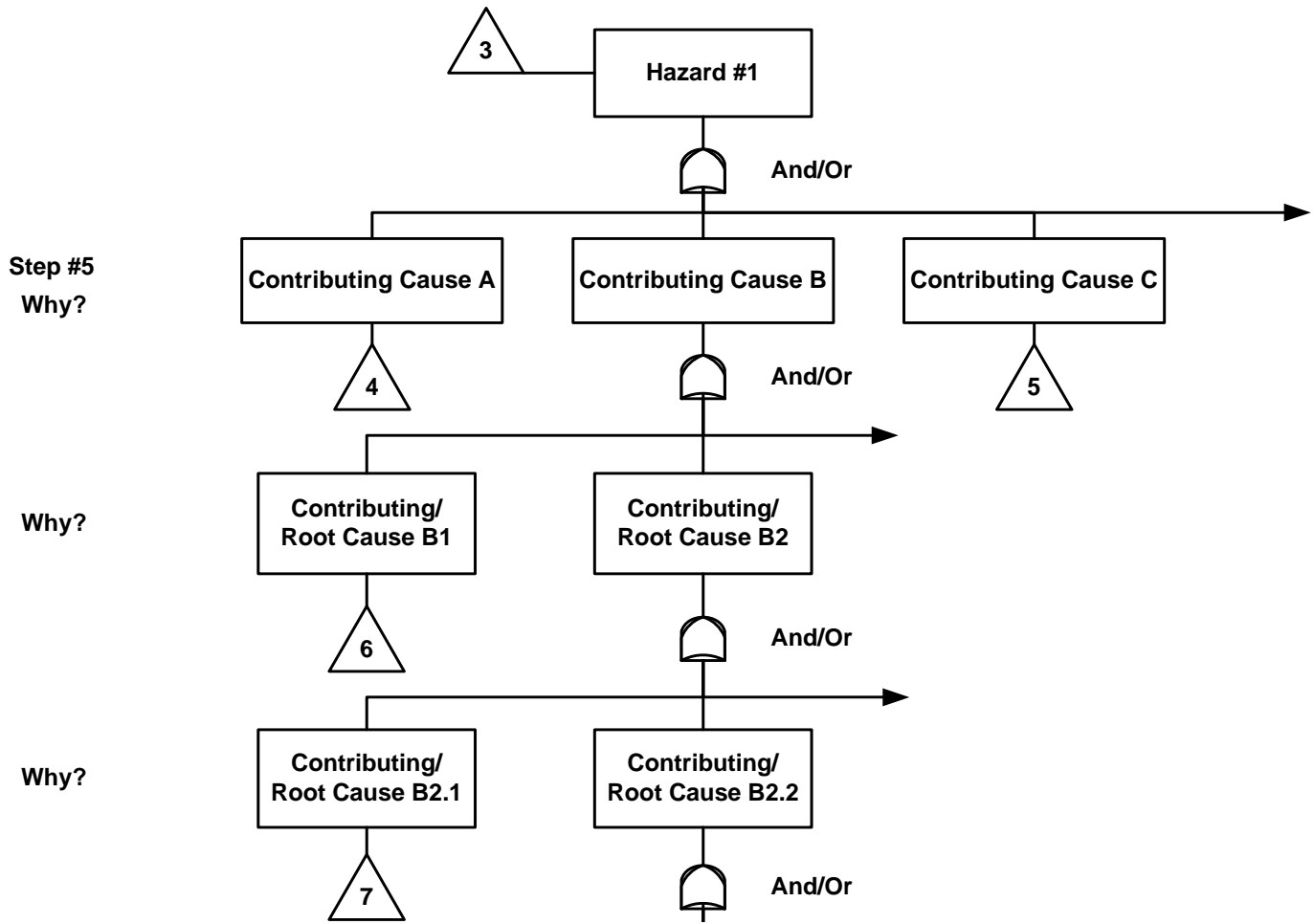
- **Control System Failure**
  - System design error
  - Hard and Software Interlocks
  - Programming error
  - Maintenance/Management of Change/Verification
  - etc.

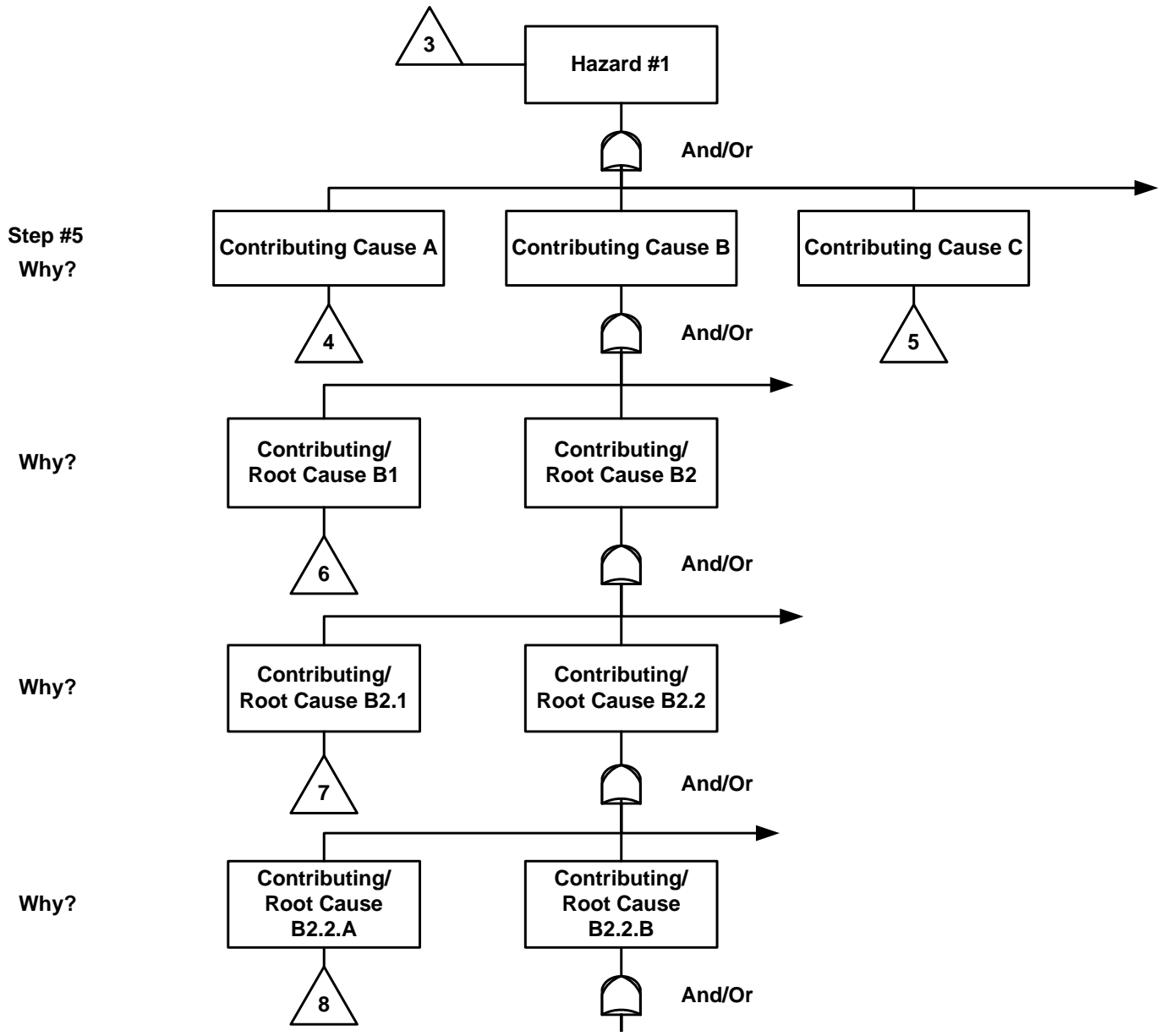
# Example: “**Contributing/Root Cause**” **Checklist (Cont.)**

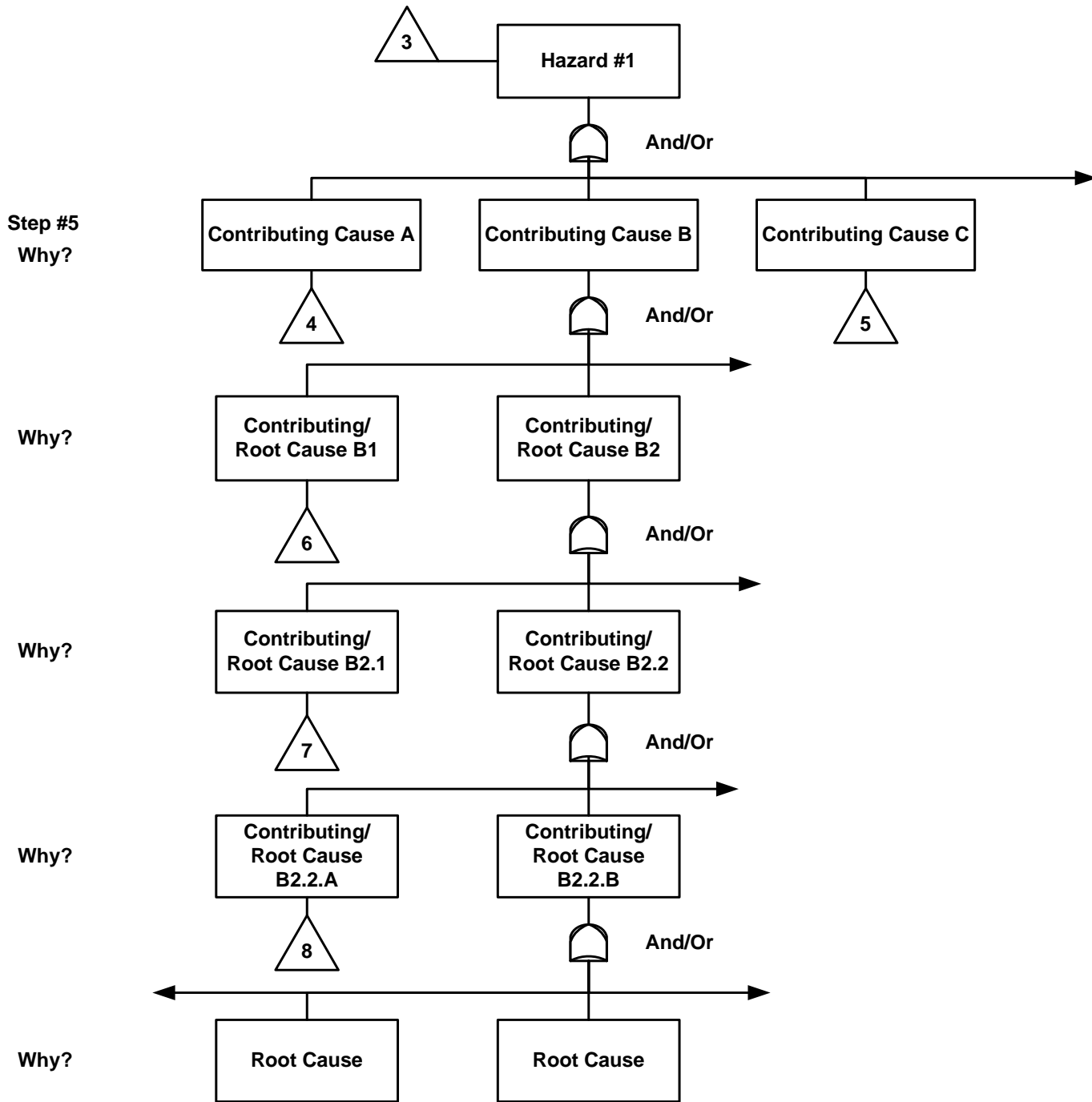
- **Facility**
  - Improper design
  - Configuration (e.g. egress, access, etc.)
  - Material of Construction
  - Maintenance/Housekeeping
  - etc.
- **Environmental Events**
  - Outside and Inside Facility
    - Cold, hot, humidity, etc.
    - Spiders, snakes, etc.

# Example: “Contributing/Root Cause” Checklist (Cont.)

- **Human Error**
  - Inadequate Procedures
  - Inadequate Training
  - Stress
  - Distractions
  - etc.







# Criteria for Terminating Logic Diagrams

- 1) **Sufficient Design Safety in place**
- 2) **Recommendation(s) Sufficient**
- 3) **Component Failure**
- 4) **Non-credible event**

# Logic Diagrams Example

Lee Ball Valve

# Lee Ball Valve

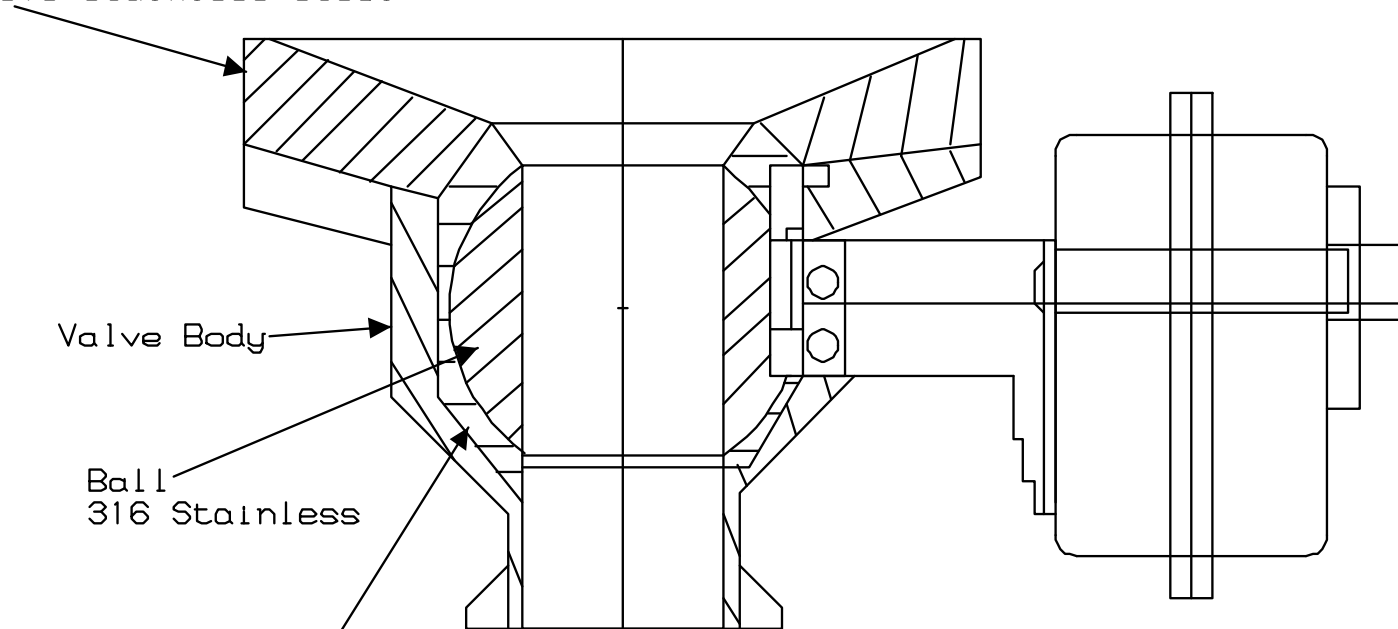
Mounting Flange  
316 stainless steel

Valve Body

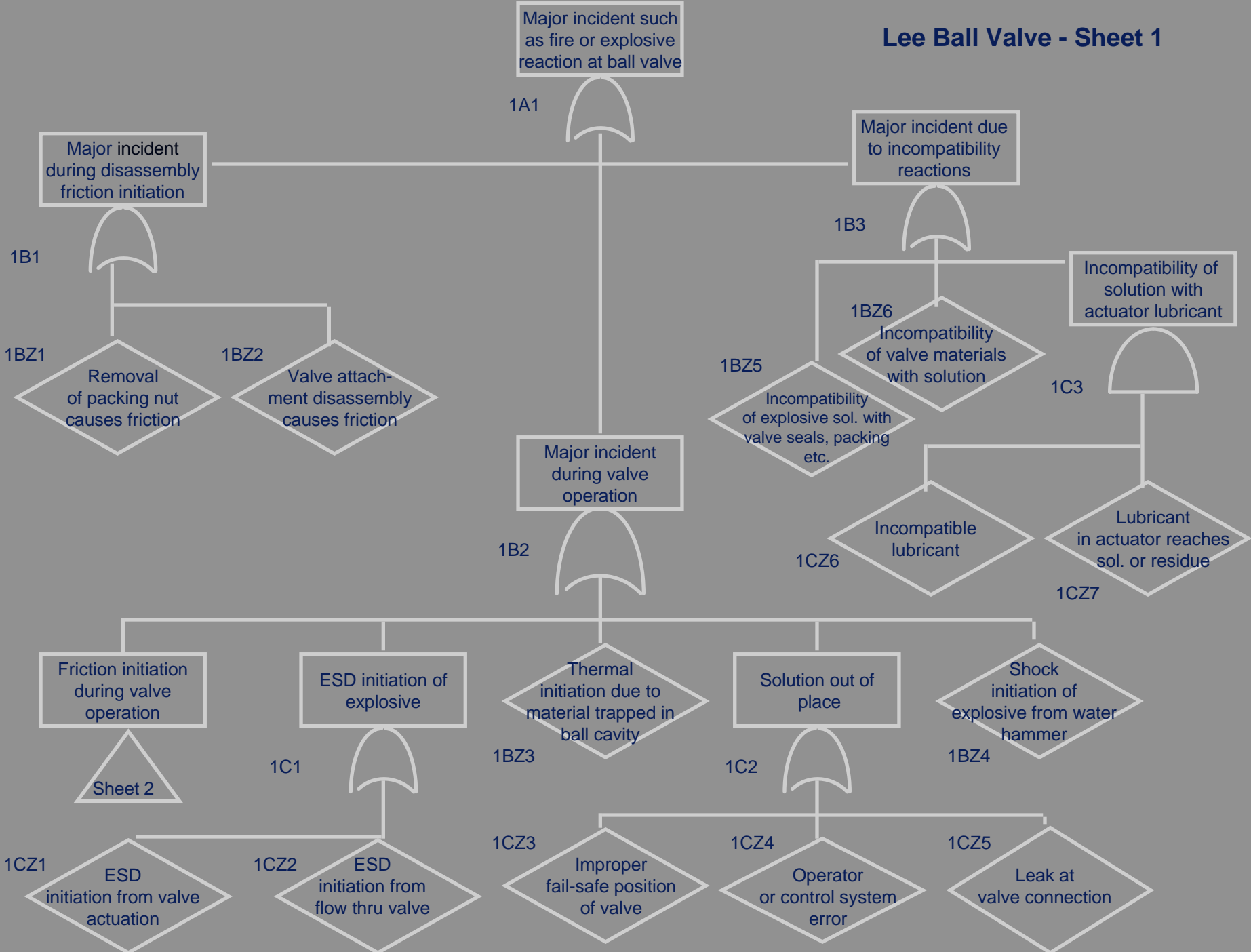
Ball  
316 Stainless

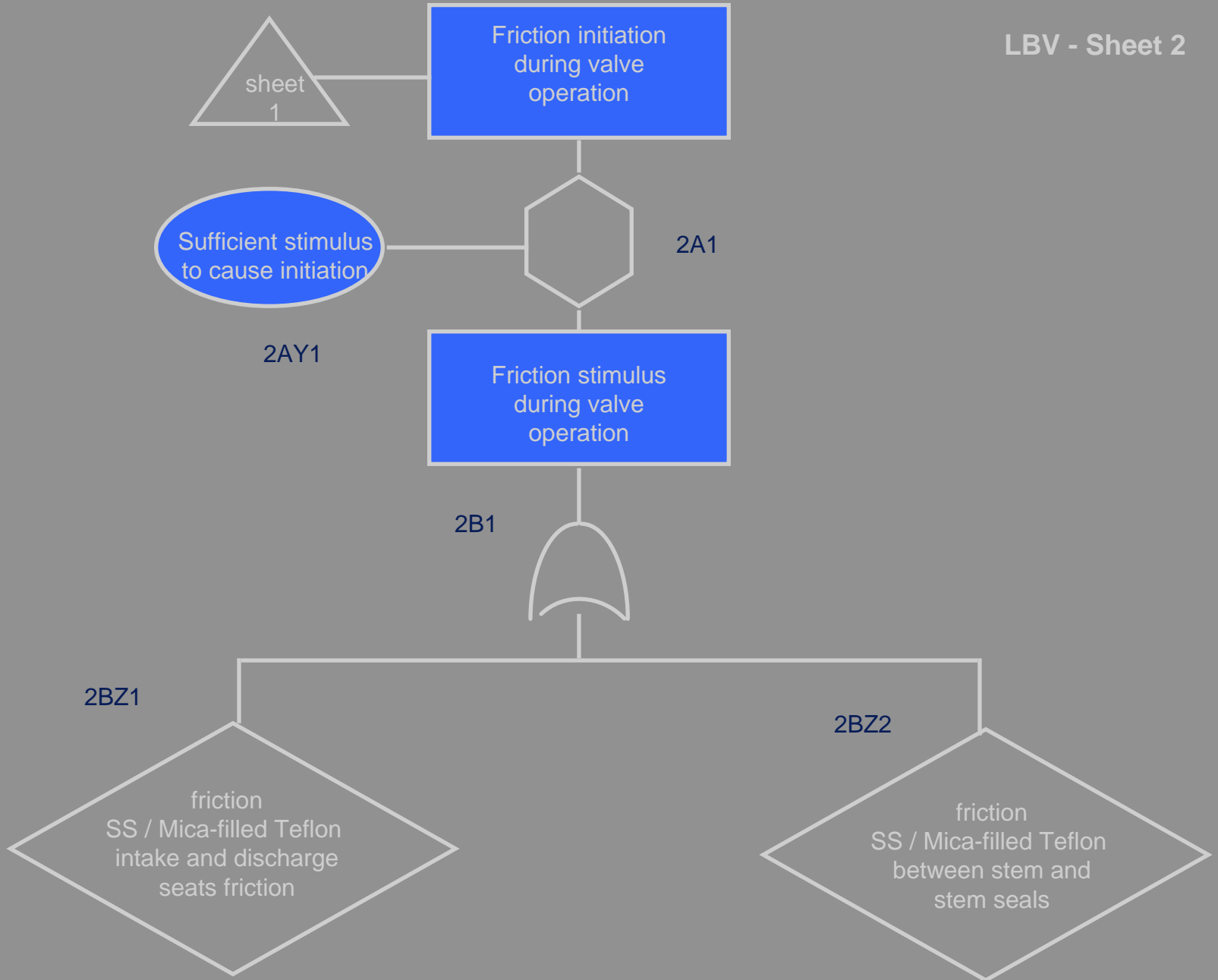
Valve Seals  
(Mica-filled Teflon)

Actuator Assembly



# Lee Ball Valve - Sheet 1





# Quantitative Analysis

- After we have determined critical hazards, by the diagrams, quantitative or engineering analysis may be appropriate
  - Event Probability Calculations
  - Laboratory Work
  - Testing

**In other words “The search for REAL engineering data to support safety decisions”**

**Operation / Equipment Prioritization**

**Hazard Identification**

**Hazard  
Ranking**

**Failure Scenarios**

**Critical  
Scenarios**

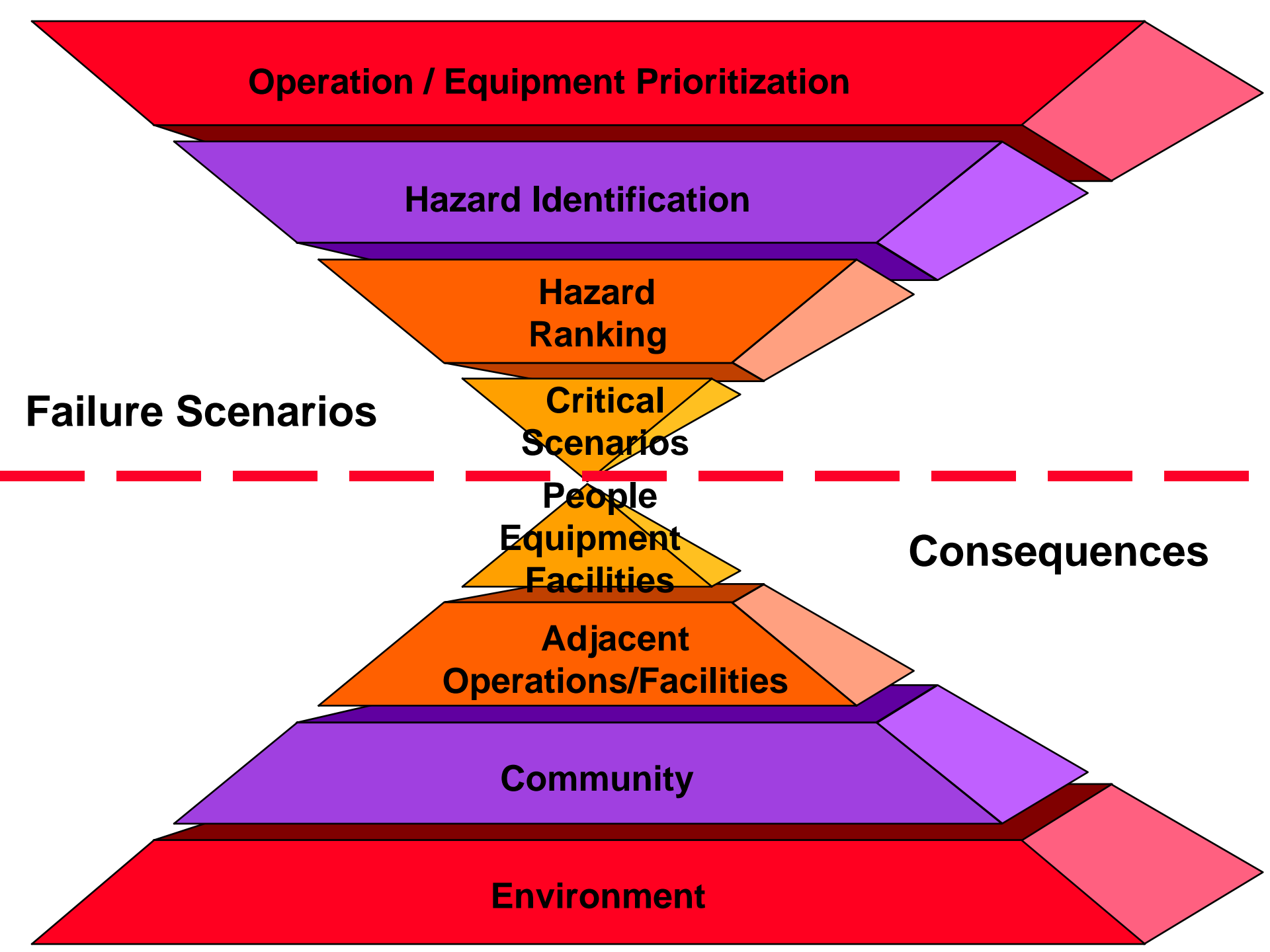
**People  
Equipment  
Facilities**

**Consequences**

**Adjacent  
Operations/Facilities**

**Community**

**Environment**



# Why is Quantitative Risk Assessment Valuable?

- Quantitative Risk Assessment may facilitate greater understanding of actual risks and mitigation benefits

# Event Probabilities

- **Equipment/Component Failure Data**
  - Mechanical
  - Electrical
- **Control System Failure**
- **Natural Phenomenon**
  - Lightning, etc
- **Human Factors**
- **Other**

# **Component Failure Rate Data Sources**

- **Machinery Reliability Assessment; Heinz P. Bloch and Fred K. Geitner**
- **Loss Prevention in the Process Industries, Volume 3, Chapter 14; Frank P. Lees**
- **Government Industry Data Exchange Program (GIDEP)**
- **Vender Data**
- **Engineering Estimates**
- **Life Cycle Calculations**

# Human Error Probabilities

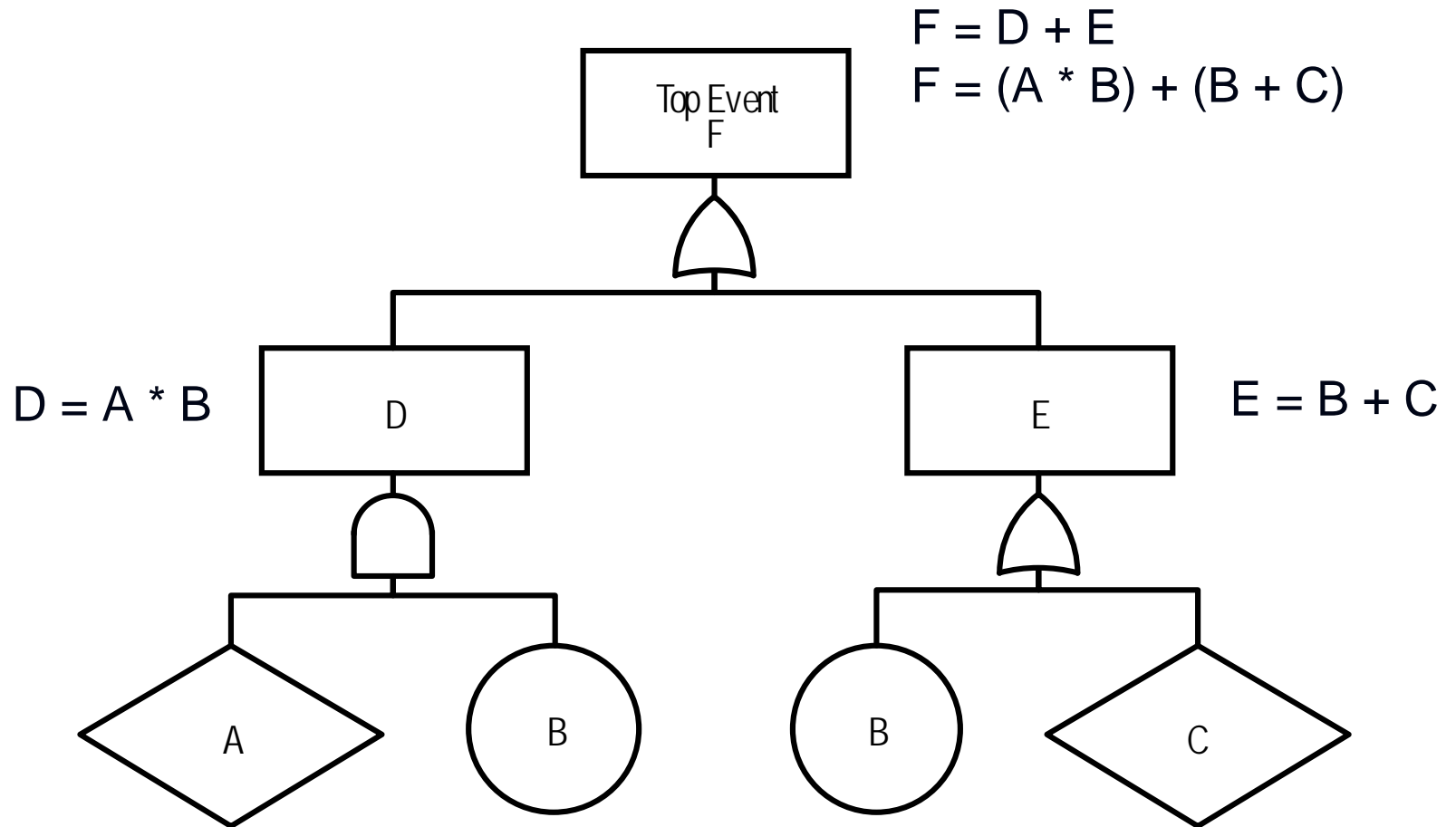
<u>Type</u>	<u>Probability</u>
Error in procedure	$1 \times 10^{-3}$
Item dropped	$1 \times 10^{-4}$
Accidental situations	
Extremely labor intense	$1 \times 10^{-3}$
Moderately labor intense	$1 \times 10^{-4}$
Other accidents	$1 \times 10^{-5}$

# Fatality Statistics

## Non-Industrial Activities

Activity	Risk (Fatalities/8hr. Time Period)
Struck by meteorite	6.9E-14
Struck by lightning	1.1E-10
Staying at home	3.0E-07
Run over by a vehicle	6.9E-08
Traveling by car	5.7E-06
Traveling by motorcycle	5.9E-05
Traveling by canoe	1.0E-04
Rock climbing	3.6E-04

# Fault Tree Quantification



# Boolean Postulates

$$A + B = B + A$$

$$A * B = B * A$$

$$A(B * C) = (A * B)C$$

$$A + (B + C) = (A + B) + C$$

$$A(B + C) = (A * B) + (A * C)$$

$$A + (B * C) = (A + B) * (A + C)$$

$$A * (A + B) = A$$

$$A + 0 = A$$

$$A * 1 = A$$

$$A + A' = 1$$

$$A * A' = 0$$

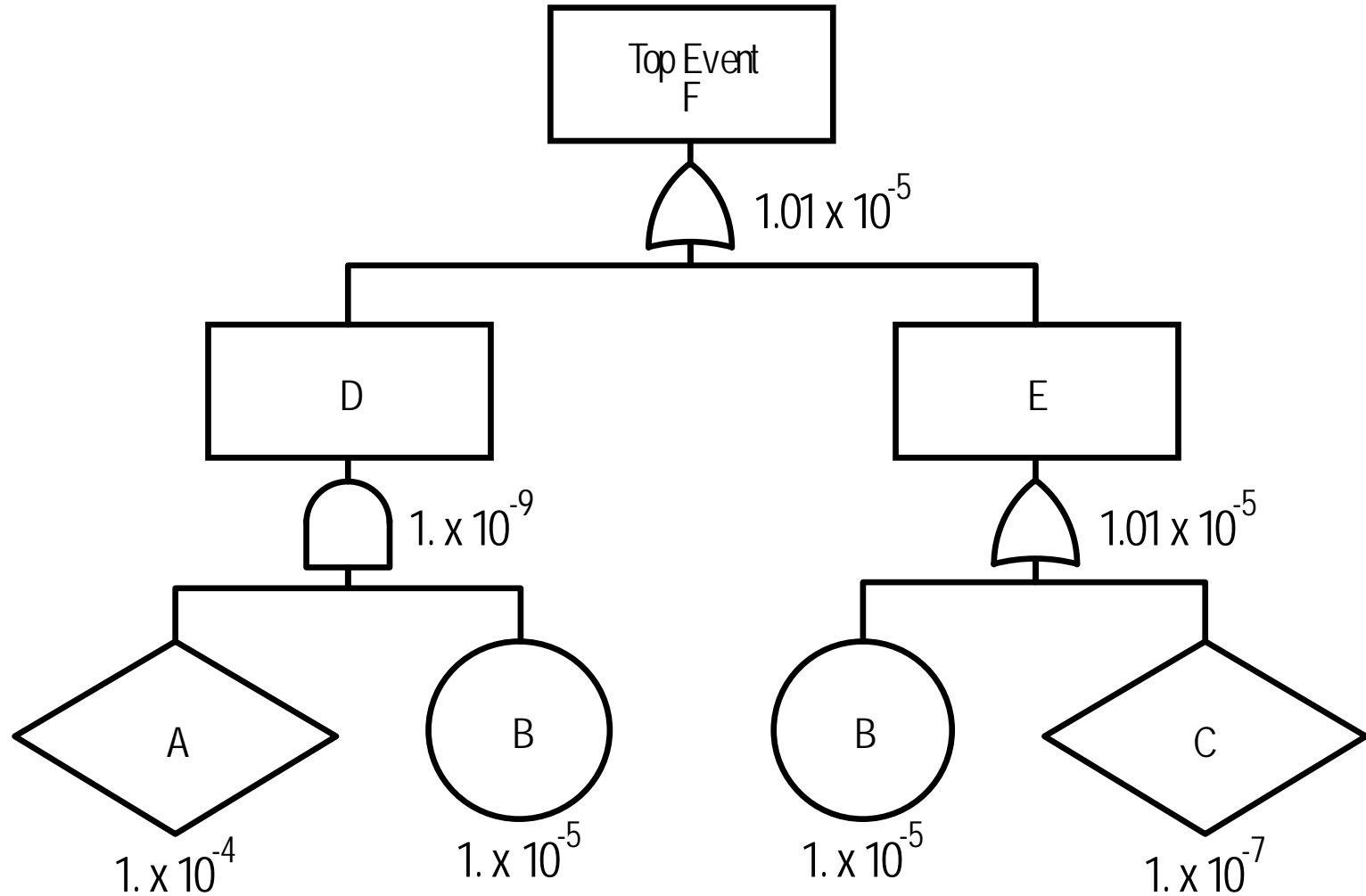
$$A * A = A$$

$$A + A = A$$

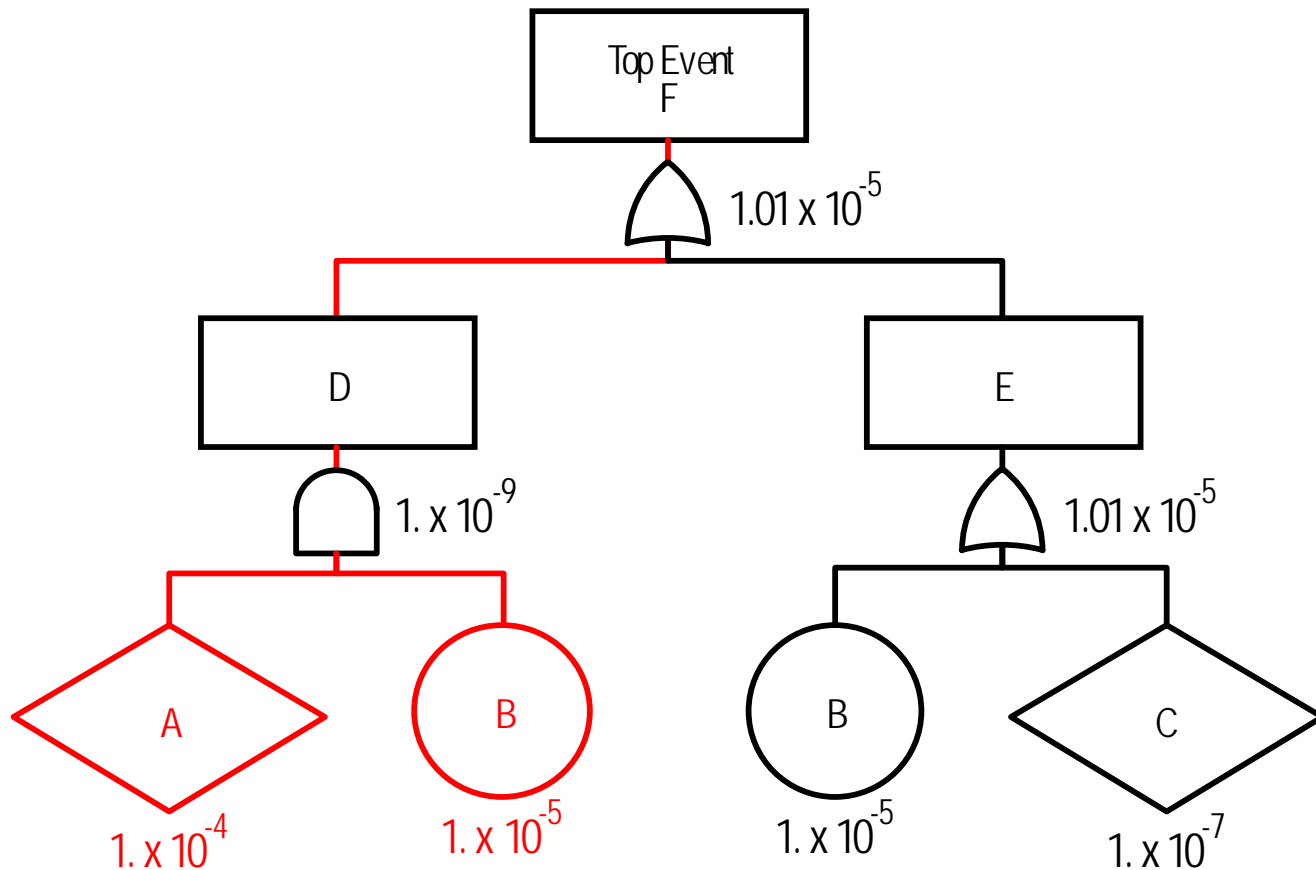
$$A + A * B = A$$

# Top Event Calculation

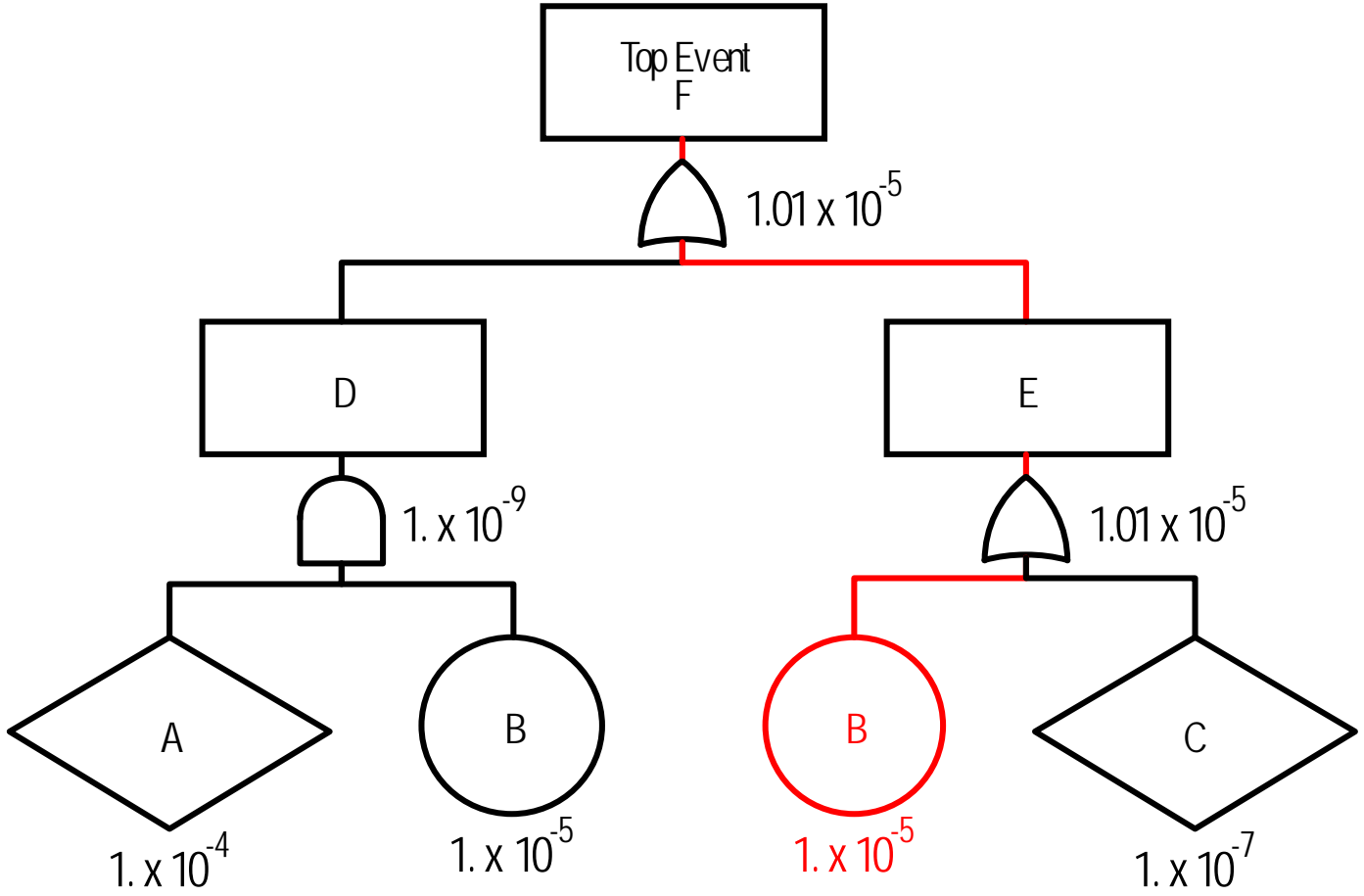
(Using FaultREASE ® software)



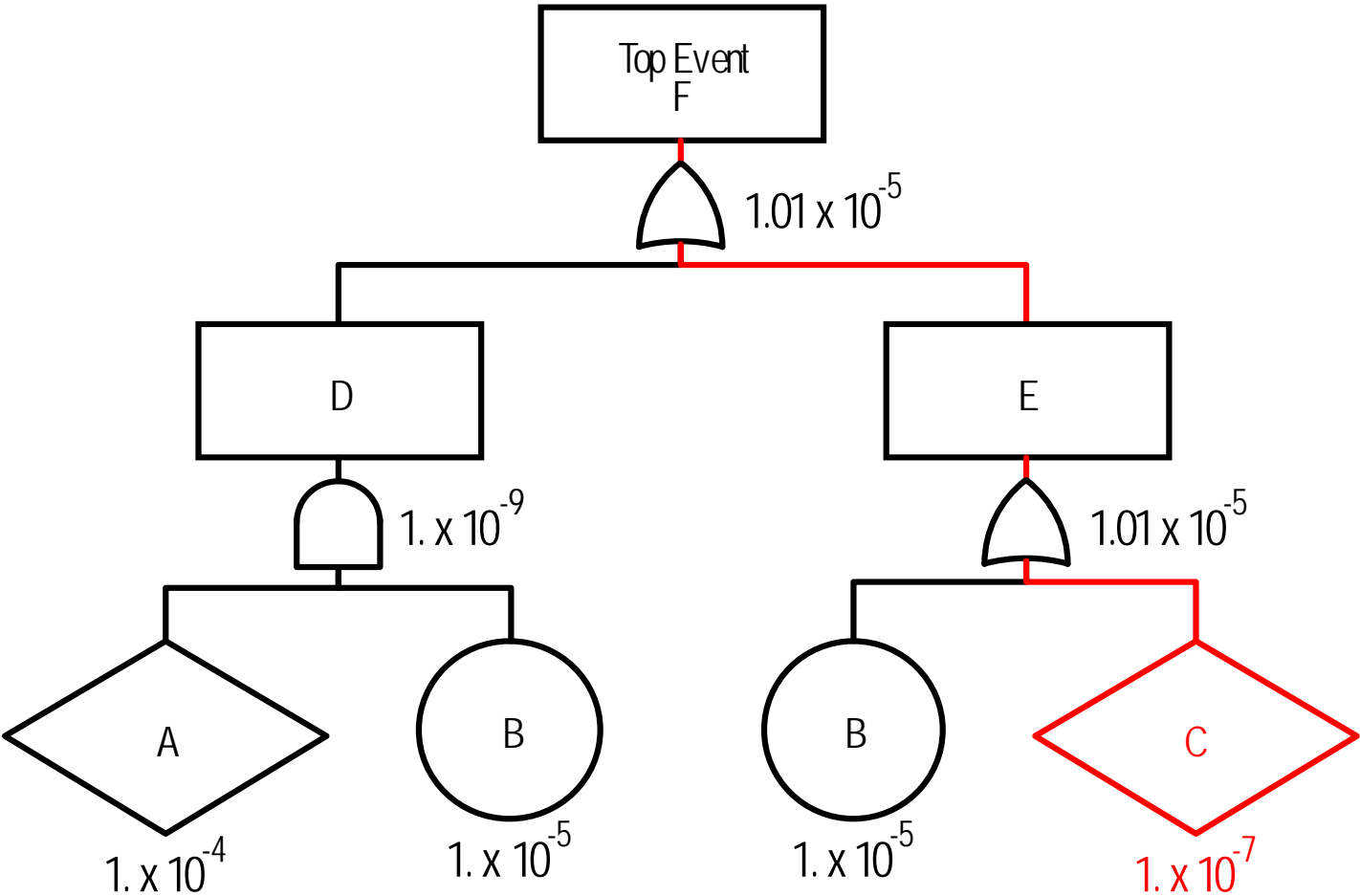
# Cut Set # 1



# Cut Set # 2



# Cut Set # 3

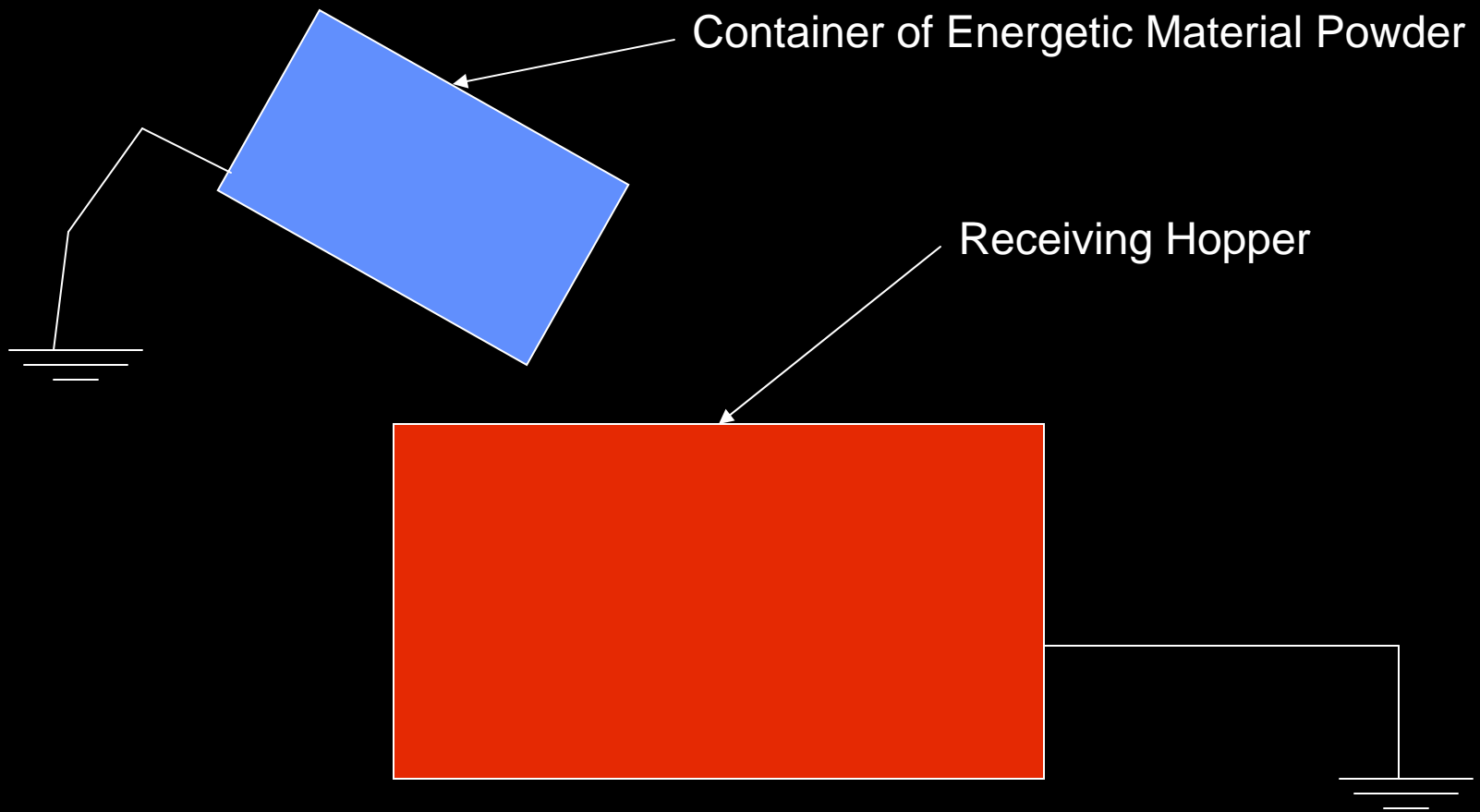




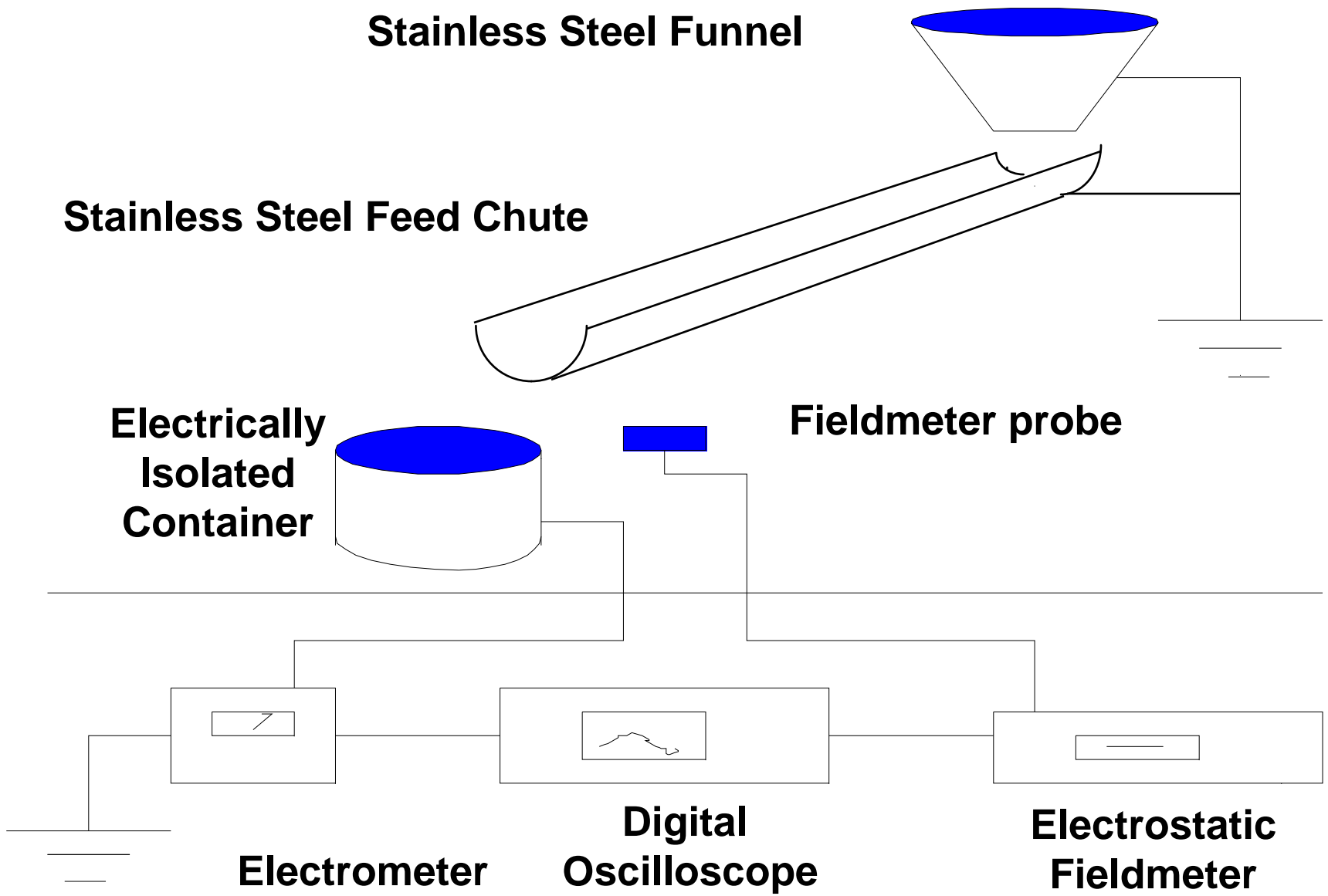
# PHA Identified Hazard

## Electrostatic Discharge Initiation

### Energetic Material Pouring Operation



# Laboratory Inclined Feed Chute



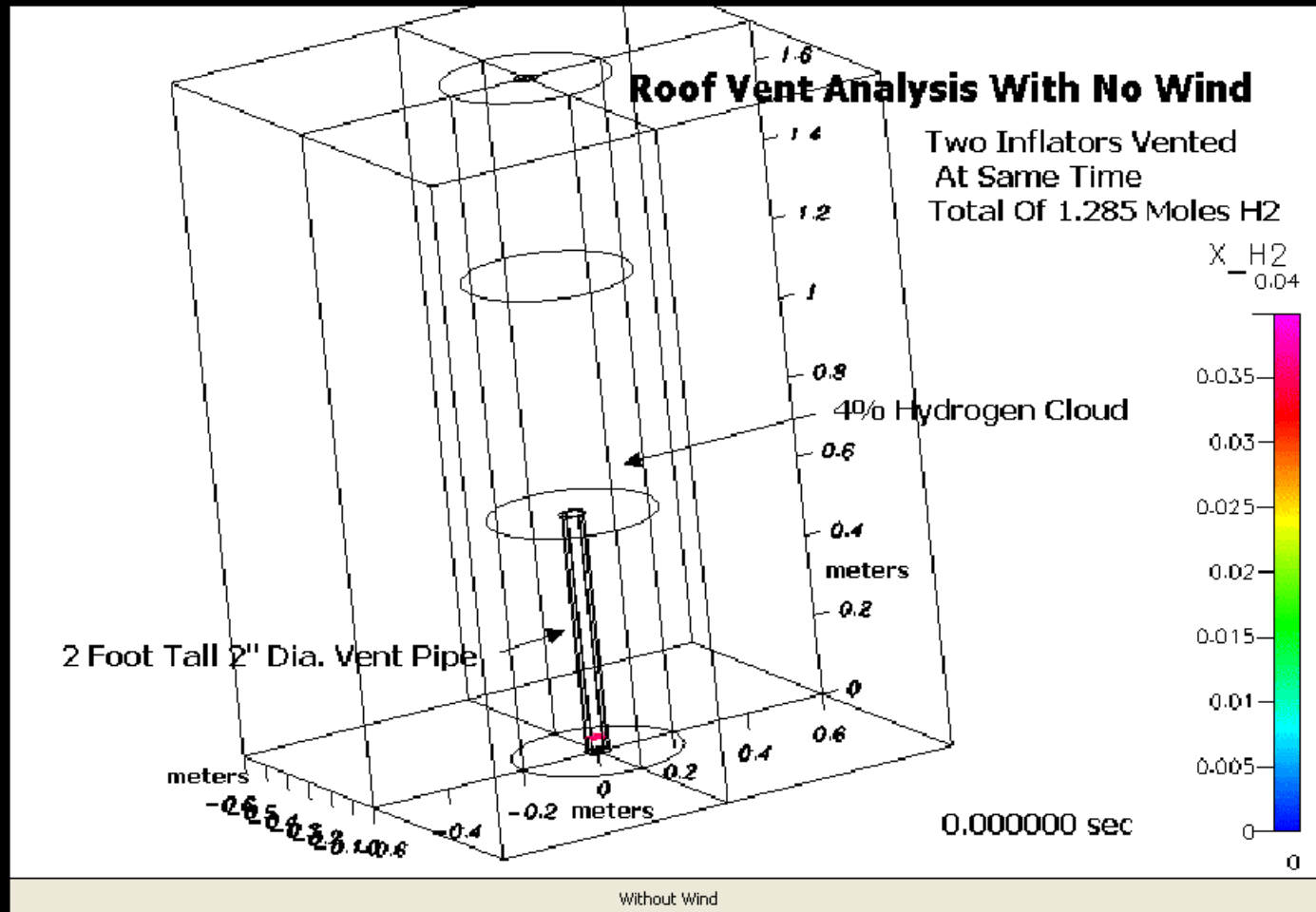
# Transfer System Summary and Conclusions

- Excessive charging is not a problem based on past data, modeling, and full-scale tests.
- Recommendations were made to minimize risks when operating a clean system. Unnecessary cleaning avoided. \$\$\$ Savings
- Laboratory work saved time and limited personnel exposure during full-scale testing. \$\$\$ Savings
- Quantitative analyses and customized testing are sometimes the safest, most **cost-effective** approach to meet regulations and to avoid potential risks.

# Flammable Gas Calculations and Modeling

- Hazards of flammable gasses indentified in the PHA
- Can the hazard be removed?
  - Provide a high level of safety to avoid operating in the flammable range
  - Limit the electrically classified areas

# Flammable Gas Calculations and Modeling of LFL



# Flammable Gas Calculations and Modeling

- **Conservative Calculations and Modeling** were the safest method to determine operating safety margins.
- If the results are sufficient, further expensive lab scale or full scale testing may not be necessary.  
\$\$\$ Savings
- Minimizing the electrically “rated” area based upon sound engineering saved capital and maintenance costs

# **When Testing May be Appropriate:**

- **Sensitivity/Reactivity Testing at Process Conditions**
- **Bulk Material Transfer & Handling**
- **Storage Configuration**
- **Propagation**
- **Facility Siting**
  - **Quantity Distance**
  - **Facility structure (Older Buildings)**
  - **Explosion Control**

# Other Test Examples

# Conclusion

- Level setting is **fundamental to risk Management and Process Hazards Analysis**
- Level setting allows for **resources to be focused** (\$\$ savings)
- Companies can NOT afford to NOT **improve Safety through detailed risk assessment**
- Critical hazards are identified through **detailed risk assessment**
- **Logic diagrams** are simple way to perform detailed risk assessments
- **Calculations, laboratory work, and testing** (sound engineering) can be performed on critical hazard scenarios to determine the appropriate level of **risk reduction** (\$\$ savings)