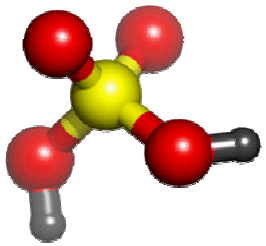
SAND2012-3363C



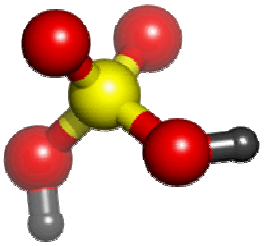
Hazards Identification and Process Hazard Analysis

SAND No. 2010-4653C

Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

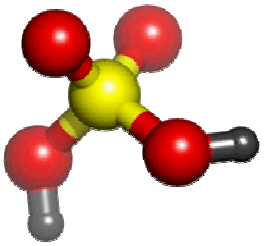
CSP CHEMICAL SECURITY ENGAGEMENT PROGRAM

Sandia National Laboratories



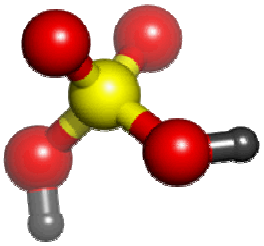
Acronyms

- ETA – Event Tree Analysis
- FMEA – Failure Modes and Effects Analysis
- FTA – Fault Tree Analysis
- HAZOP – Hazards and Operability Study
- MSDS – Material Safety Data Sheets
- P&ID – Piping & Instrument Drawings
- PFD – Process Flow Diagrams
- PHA – Process Hazards Analysis
- RAGAGEP – Recognized And Generally Accepted Good Engineering Practices



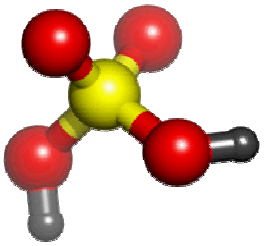
Primary Section Objectives

- Define Process Hazard Analysis
- Detail hazard identification methods
- Practice hazard identification methods



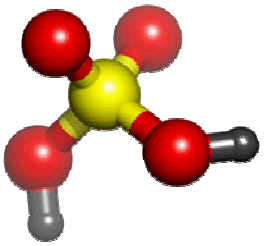
Process Hazard Analysis

- Process Hazard Analysis is a structured team review of an operation involving hazardous materials/energies to:
  a) Identify previously unrecognized hazards
  b) Identify opportunities to make the operation inherently safer
  c) Identify loss event scenarios
  d) Evaluate the scenario risks to identify where existing safeguards may be not adequate
  e) Document team findings and recommendations



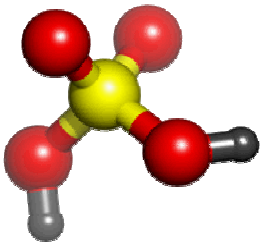
Process Hazard Analysis

- Some PHA methods determine the adequacy of safeguards without assessing scenario risks
- This is done on the basis of collective past experience
- Compare process with recognized and generally accepted good engineering practices (RAGAGEPs)



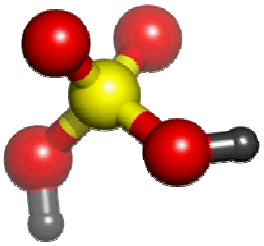
Process Hazard Analysis

- Effective way to take advantage of past experience
- Concentrates on protecting against events expected during lifetime of facility
- Low-probability, high-consequence events not analyzed
- Not good for complex or unique processes

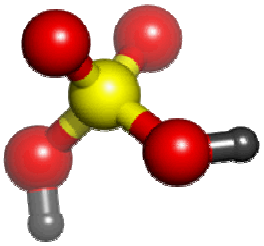


Hazard Identification Methodologies

- What-if
- Checklist (may be combined with other PHA)
- Hazard and operability study (HAZOP)
- Failure mode and effects analysis (FMEA)
- Fault Tree Analysis (FTA primarily covered in Risk Analysis course)
- Event Tree Analysis (ETA primarily covered in Risk Analysis course)
- Appropriate, equivalent methodology

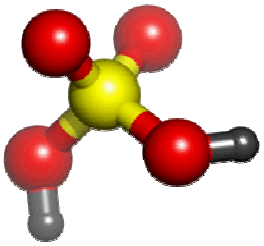


What-if analysis



Hazard Identification Methodologies

- What-if analysis
  - Group of **experienced** people familiar with subject processes ask questions and voice concerns
  - Identify hazards, hazardous situations, event sequences which may lead to undesirable consequences
  - Investigate topics which includes:
    - Electrical safety
    - Fire protection
    - Personnel safety
    - Chemical handling



Hazard Identification Methodologies

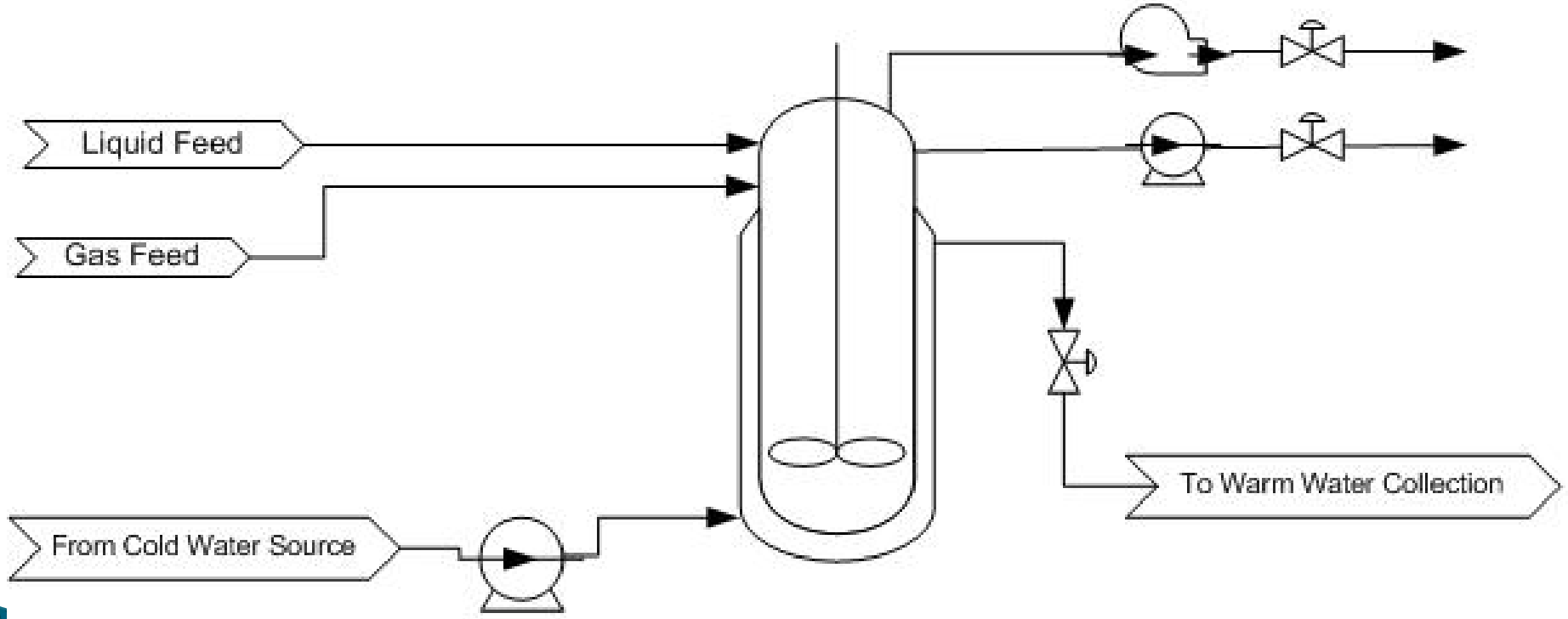
- What-if analysis
  - Start-up, normal operation, maintenance, shift changes
  - Can be performed at any stage of plant life
  - Produces list of questions and answers on processes which may be displayed in a table form

PROCESS SEGMENT:	SCOPE:	**What-If Analysis**
REVIEW DATE:	INTENT:	

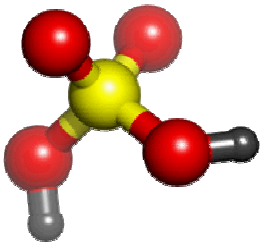
What If …	Consequences	Safeguards	Finding/Recommendation Comments

Hazard Identification Methodologies

- Look at the simply process, identify some what-if questions

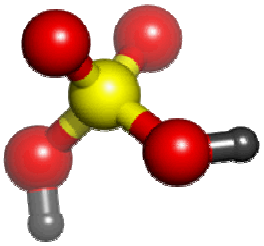


https://controls.engin.umich.edu/wiki/images/0/06/PID.Safety.JPG



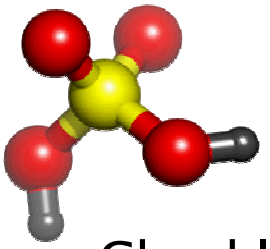
Hazard Identification Methodologies

Checklists



Hazard Identification Methodologies

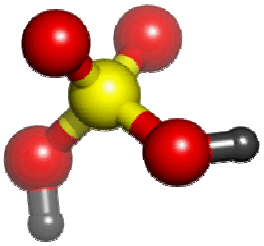
- Checklist
  - Uses a written list of items to verify the status of a system
  - Commonly used in conjunction with another hazard identification method
  - May be used to familiarize inexperienced personnel with a process
  - Common basis for management review
- Addresses material, equipment, and procedures



Hazard Identification Methodologies

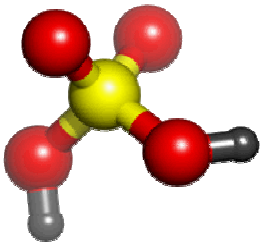
- Checklist Activity – Form small groups and provide very generic questions for a checklist. After, please present your results.

- Materials:
  - 1)
  - 2)
  - 3)
- Equipment:
  - 1)
  - 2)
  - 3)
- Procedures:
  - 1)
  - 2)
  - 3)

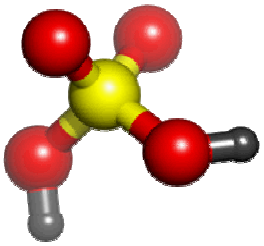


Hazard Identification Methodologies

- Materials:
  - Do raw materials meet documented specifications?
  - Are chemicals tested after being produced?
  - Do staff have material safety data sheets (MSDS)?
- Equipment
  - Has equipment been inspected and replaced as scheduled?
  - Have pressure relief valves and other safety valves been tested?
  - Have fire protection systems been inspected and tested as scheduled?
- Procedures
  - Are there operating procedures for start-up, normal operation, maintenance, and shutdown?
  - Are operators following the written procedures?
  - Are hot work permitting processes and lockout/tagout procedures being implemented?

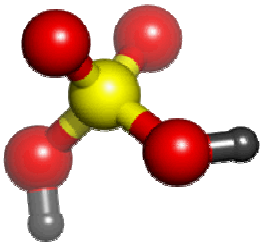


Hazard and Operability Study



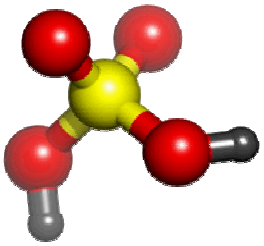
Hazard Identification Methodologies

- Hazards and Operability Study (HAZOP)
  - Team based systematic review of processes and operations
    - Identify and evaluate safety hazards
    - Identify operability problems which could compromise a plant's ability to achieve optimal productivity
  - Mostly used when detailed Process Flow Diagrams (PFD) and Piping & Instrument Diagrams (P&ID) drawings are available



Hazard Identification Methodologies

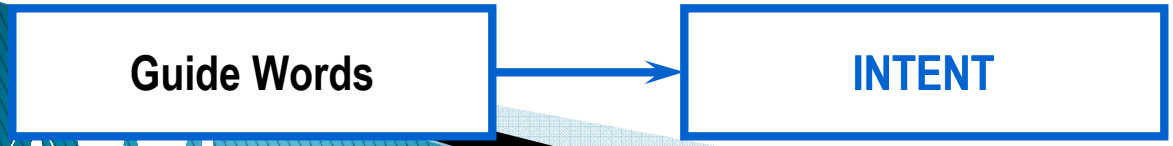
- Hazards and Operability Study (HAZOP)
  - Product results in a table which includes:
    - Items (by equipment such as a storage tank)
    - Deviations from normal operation for the equipment (e.g., high level of liquid chemical)
    - Causes (e.g., failure of components such as a valve)
    - Consequences (e.g., potential release of chemical)
    - Safeguard (e.g., level indicator on storage tank)
    - Action (e.g., none, maintenance schedule)

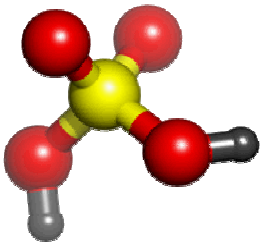


HAZOP Guide Words

Guide Words are applied to the design intent to systematically identify deviations from normal operation.

NONE
MORE OF
LESS OF
PART OF
AS WELL AS
REVERSE
OTHER THAN



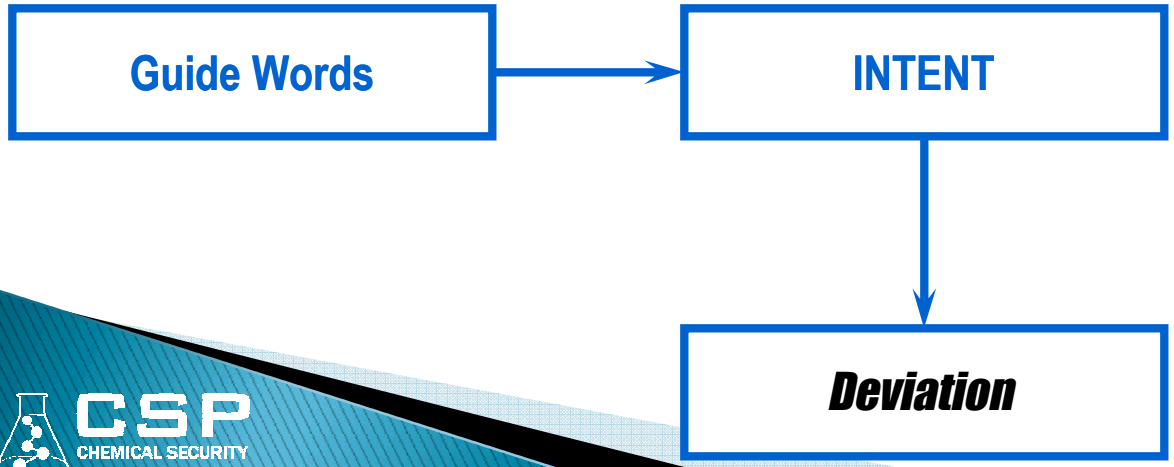


HAZOP Guide Words

Guide Word	Meaning
NONE	Negation of intent
MORE OF	Exceed intended upper limit
LESS OF	Drop below intended lower limit
PART OF	Achieve part of intent
AS WELL AS	Something in addition to intent
REVERSE	Logical opposite of intent occurs
OTHER THAN	Something different from intent

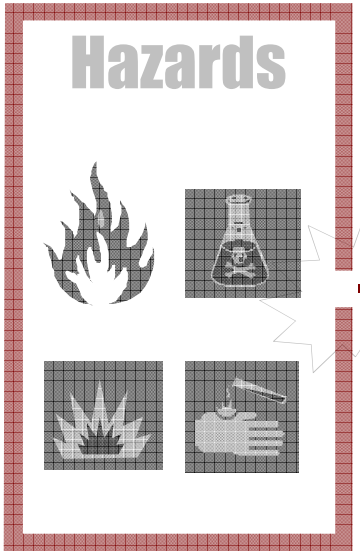
Deviations from Intent

- Do not begin developing deviations until intent is fully described, documented and agreed upon
- List of deviations can be started as soon as intent is established



Deviations

A *deviation* is an abnormal situation, outside defined design or operational parameters.

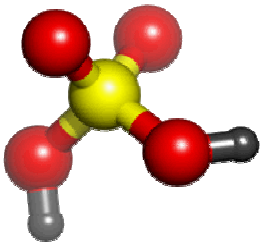


Deviation

- No Flow
- Low Temperature
- **High Pressure** *(exceed upper limit of normal range)*
- Less Material Added
- Excess Impurities
- Transfer to Wrong Tank
- Loss of Containment
- etc.

HAZOP Deviations Guide

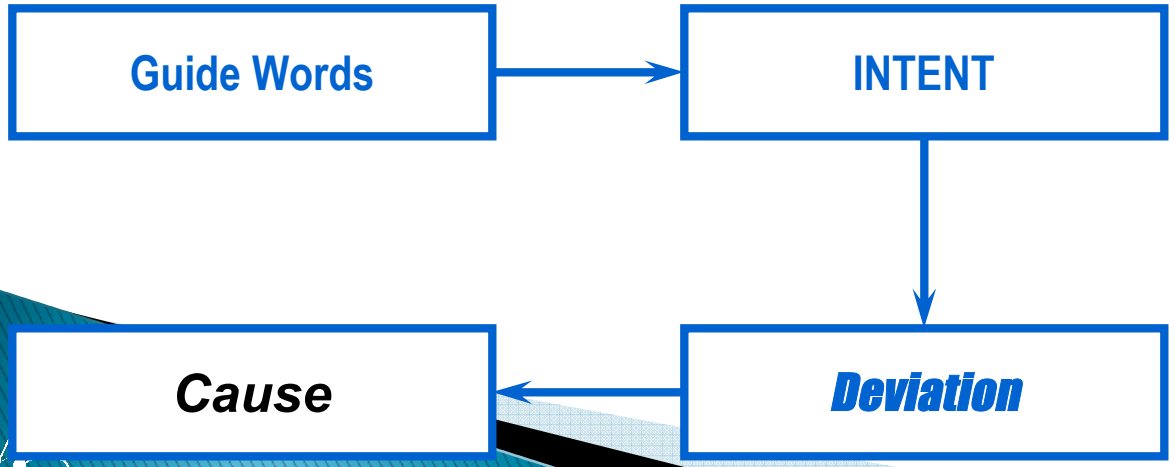
Design Intent *Apply each guide word to intent.* A complete design intent for each line/vessel/node includes: • All functions and locations • Controlled variables' SOCs • Expected compositions • Equipment used E.g., the intent of a reaction step might be to "Contain and control the complete reaction of 1000 kg of 30% A and 750 kg of 98% B in EP-7 by providing mixing and external cooling to maintain 470-500 ºC for 2 hours, while venting off-gases to maintain < 1 bar g"	**NO / NONE** Containment lost Procedure step skipped No [function] No transfer No agitation No reaction	**MORE OF** Procedure started too late Procedure done too long Too much [function] Too much transferred Too much agitation High [controlled variable] High reaction rate High flow rate High pressure High temperature	**LESS OF** Procedure started too soon Procedure stopped too soon Not enough [function] Not enough transferred Not enough agitation Low [controlled variable] Low reaction rate Low flow rate Low pressure Low temperature
PART OF Part of procedure step skipped Part of [function] achieved Part of [composition] Component missing Phase missing Catalyst deactivated	**AS WELL AS** Extra step performed Extra [function] Transfer from more than one source Transfer to more than one destination Extra [composition] Extra phase present Impurities; dilution	**REVERSE** Steps done in wrong order Reverse [function] Reverse flow Reverse mixing	**OTHER THAN** Wrong procedure performed Wrong [function] achieved Transfer from wrong source Transfer to wrong destination Maintenance/test/sampling at wrong time/location

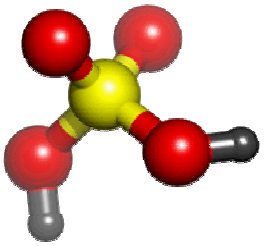


Initiating causes

Identify deviation cause(s).

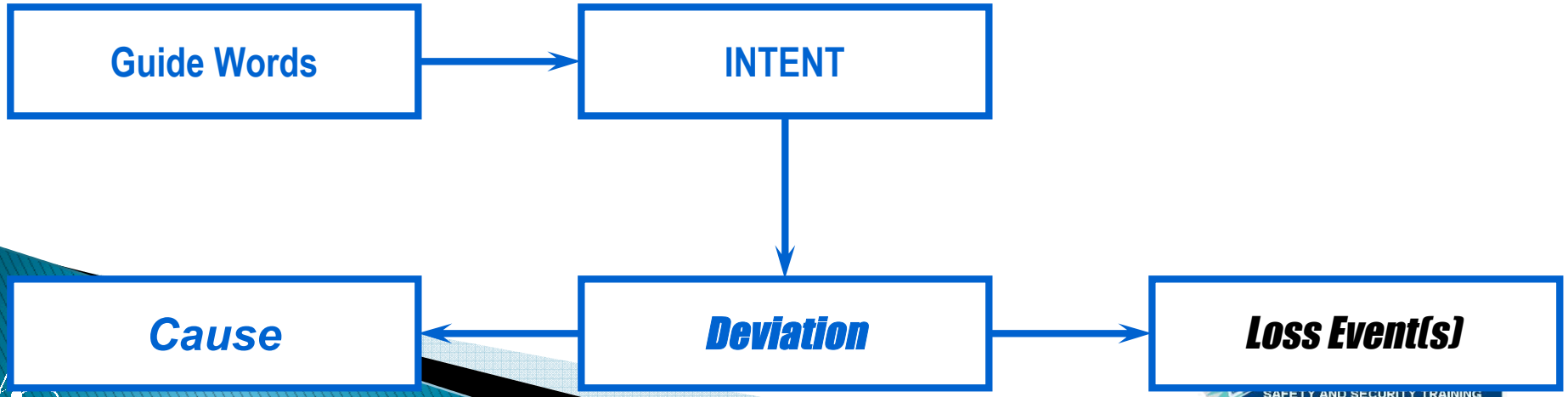
- Must look backward in time sequence
- Only identify local causes (i.e., in current study node)
- Most deviations have more than one possible cause

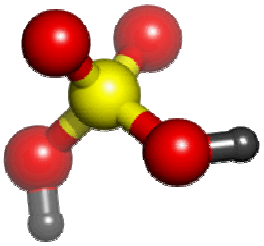




Loss events

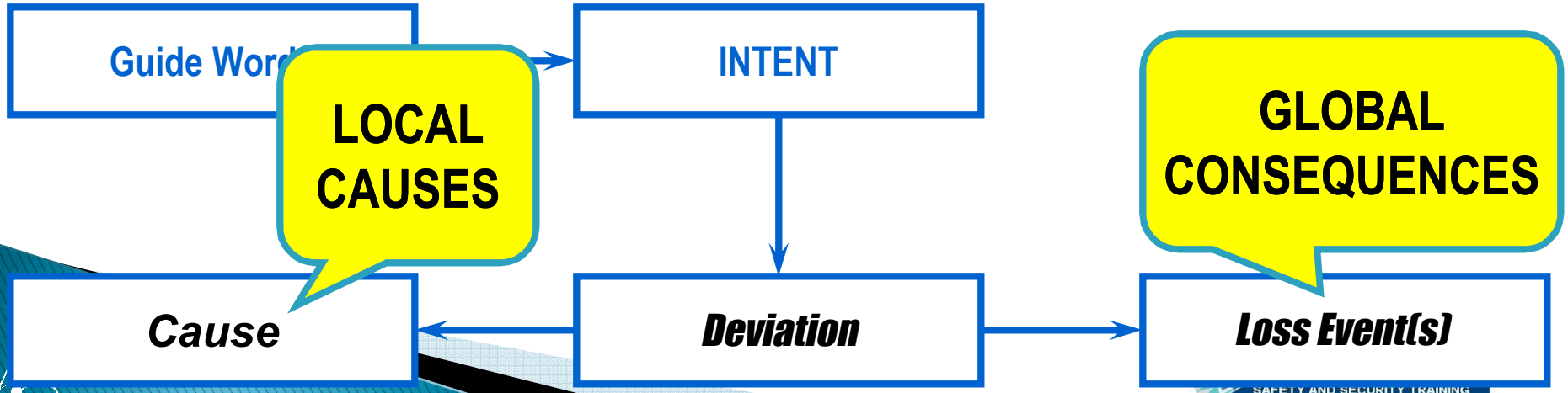
- Determine cause and deviation consequences, assuming failure of protection safeguards.
- Take scenario all the way to a loss event consequence.
- Consequences can be anywhere and anytime.





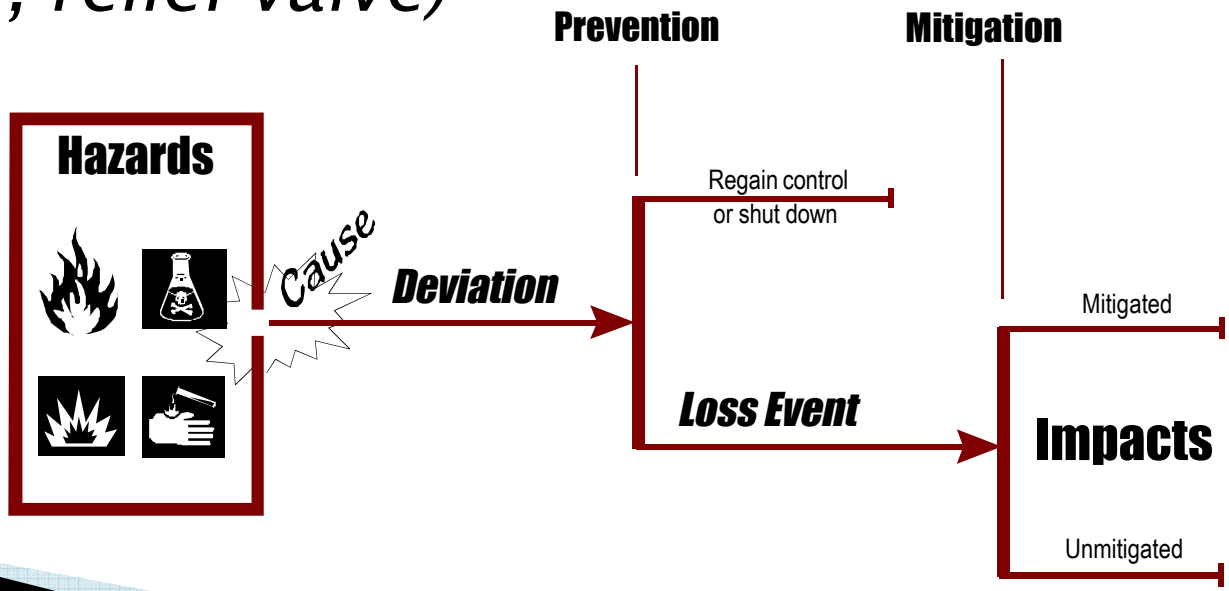
Loss events

- Determine cause and deviation consequences, assuming failure of protection safeguards
- Take scenario all the way to a loss consequence
- Consequences can be anywhere and anytime



Safeguards

- Document preventive safeguards intervening between the specific Cause–Consequence pair
- Note that different Consequences are possible, depending on safeguard success or failure *(e.g., relief valve)*

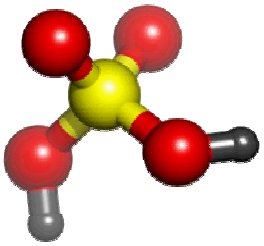


Node 1	Fuel Transfer Line	HAZOP Study
Review Date:	SCOPE: From fuel supply to EP16 inlet, including fuel pump and fuel flow control loop INTENT: Feed fuel (50/50 KA mix) at 50-55 gpm, 20-25 C and 100-120 psig from fuel supply system to reactor EP-16	

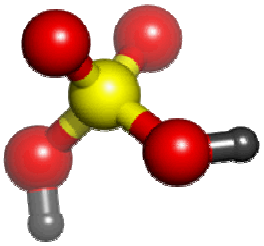
Guide Word, Deviation	Cause	Consequences	Safeguards	Finding/Rec. # Comments
NONE No feed of KA to EP16	Pump stops	High oxidant-to-fuel ratio in reactor; temperature increase in reactor; reaction rate increase; pressure increase in reactor; runaway reaction; vessel rupture explosion, with resulting blast effects causing severe injuries or fatalities to persons nearby and NOx plume drifting off-site	[] Cascade control system stops oxidant flow automatically [] Operator response to high temperature reading (close manual oxidant valve); adequate time to respond, but valve is in same general area as EP16 [] SIL1 high-high temperature trip system shuts off oxidant feed; off same temperature sensor as temperature recorder	1, 2 PRV not designed to relieve runaway reaction
NONE No feed of KA to EP16	Fuel flow control valve fails closed or commanded to close	High oxidant-to-fuel ratio in reactor; temperature increase in reactor; reaction rate increase; pressure increase in reactor; runaway reaction; vessel rupture explosion, with resulting blast effects causing severe injuries or fatalities to persons nearby and NOx plume drifting off-site	[] Operator response to high temperature reading (close manual oxidant valve); adequate time to respond, but valve is in same general area as EP16 [] SIL1 high-high temperature trip system shuts off oxidant feed; off same temperature sensor as temperature recorder	1, 2 PRV not designed to relieve runaway reaction
NONE No feed of KA to EP16	Line blocked upstream of pump	High oxidant-to-fuel ratio in reactor; temperature increase in reactor; reaction rate increase; pressure increase in reactor; runaway reaction; vessel rupture explosion, with resulting blast effects causing severe injuries or fatalities to persons nearby and NOx plume drifting off-site	[] Cascade control system stops oxidant flow automatically [] Operator response to high temperature reading (close manual oxidant valve); adequate time to respond, but valve is in same general area as EP16 [] SIL1 high-high temperature trip system shuts off oxidant feed; off same temperature sensor as temperature recorder	1, 2 PRV not designed to relieve runaway reaction

REVIEW DATE	NODE: SCOPE: INTENT:	**HAZOP Study**

Guide Word	Deviation	Cause	Consequences	Safeguards	Finding/Recommendation Comments

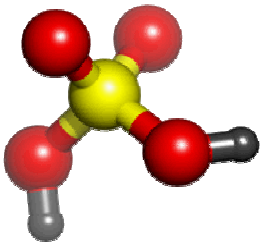


Failure Mode and Effects Analysis



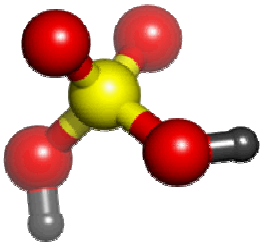
Hazard Identification Methodologies

- Failure Modes and Effects Analysis (FMEA)
  - Purpose is to identify single equipment and system failure mode
    - Valve
    - Chiller System
  - Couple failure mode with potential effect(s) on system or plant
    - Leaking, sticking, rupturing, on, off, open, closed
    - Over-heating, vapor generation
  - General outcome is recommendations to increase equipment reliability, (e.g., maintenance schedule)



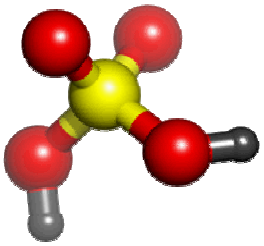
Hazard Identification Methodologies

- Failure Modes and Effects Analysis (FMEA)
  - Necessary resources include to conduct FMEA
    - System or plant equipment list
    - P&ID or PFD
    - Knowledge of equipment or system or plant function and failures
    - Responses of failures
  - FMEA may be done singularly, but should be checked for completeness



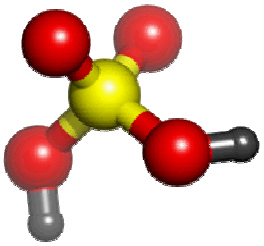
Hazard Identification Methodologies

- Failure Modes and Effects Analysis (FMEA)
  - Each individual failure is considered as independent occurrence with no relation to failures in the system
  - Rarely incorporates damage or frequency of failure
  - FMEA not as efficient as other hazard identification methodologies



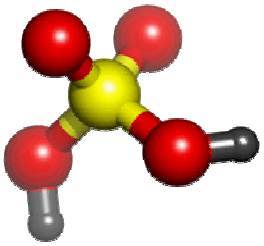
Hazard Identification Methodologies

- Failure Modes and Effects Analysis (FMEA)
  - Human operator error not usually examined directly
  - Human error is examined as it manifests into failure
    - Inadequate design
    - Improper installation/operation
    - Lack of maintenance



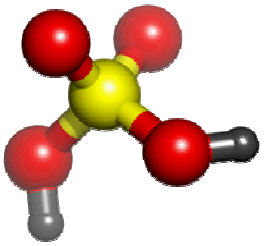
Hazard Identification Methodologies

- Failure Modes and Effects Analysis (FMEA)
  - Three steps to FMEA
    - Defining the study problem
    - Performing the review
    - Documenting the results



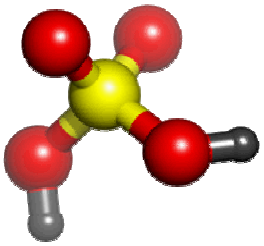
Hazard Identification Methodologies

- Defining the study problem for FMEA
  - Appropriate level of resolution
    - Plant or system level
  - Defining boundary conditions
    - Physical system boundaries
    - Analytical boundaries
    - Collecting current references that identify equipment and relationship to plant



Hazard Identification Methodologies

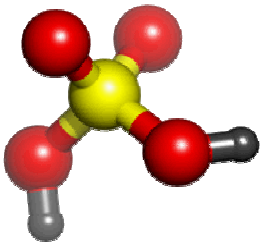
- Performing the review for FMEA
  - Equipment identification
    - Provide a unique identifier for equipment
    - Typically P&ID have unique identification for components
  - Equipment description
    - Type, configuration, service characteristics
  - Failure modes
  - Effects
  - Safeguard
  - Actions
- Document results of FMEA (tabular)



Hazard Identification Methodologies

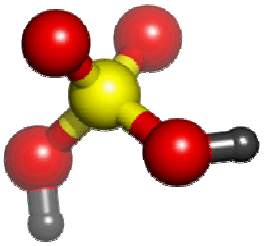
- Brief FMEA activity! With a partner:

1. Define a piece of equipment
2. Provide a type and service characteristics
3. Detail failure modes of equipment
4. Describe the effects of the failure
5. List the safeguards
6. Provide necessary actions

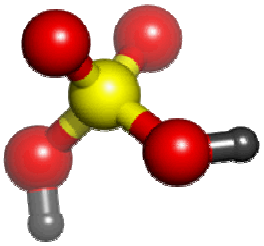


Hazard Identification Methodologies

1. Define a piece of equipment
   - Motor-Operated Valve
2. Provide a type and service characteristics
   - Normally operating at high pressure CO_2
3. Detail a failure mode of equipment
   - Valve body ruptures
4. Describe the effects of failure
   - Release of high pressure CO_2
5. List a safeguard
   - Maintenance schedule on semi-annual cycle
6. Actions
   - Automatically replace valve at five years

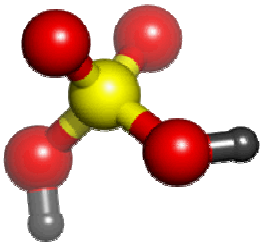


Fault Tree Analysis

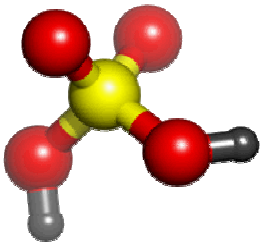


Hazard Identification Methodologies

- Fault Tree Analysis (FTA)
  - Deductive technique that focuses on one particular incident or main system failure
  - Provides a method for determining cause of failure
  - Identifies combinations of equipment failures and human errors that can result in an incident
  - Graphical method that is well suited for highly redundant systems
  - Systems vulnerable to single-failures leading to incidents, use FMEA or HAZOP Study
- Covered more in subsequent course

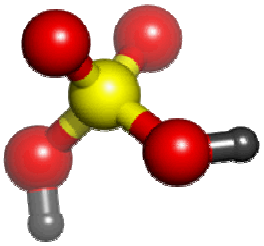


Event Tree Analysis



Hazard Identification Methodologies

- Event Tree Analysis (ETA)
  - Event sequences (failures or errors) that lead to incident
  - All possible outcomes following the success or failure of protective systems given initiating cause
  - Identifies various incidents in complex processes that have several layers of safety systems
  - Graphical event trees represent logical and combinations of events
  - Results input into FTA for qualitative analysis
- Covered more in subsequent course



Section Recap

- Need for Process Hazard Analysis
  a) Identify previously unrecognized hazards
  b) Identify opportunities to make the operation inherently safer
  c) Identify loss event scenarios
  d) Evaluate the scenario risks to identify where existing safeguards may be not adequate
  e) Document team findings and recommendations
- Detail hazard identification methodologies
  - What-if, checklist, HAZOP, FMEA, FTA, ETA
- Practice the various techniques

Questions