Chemical
SAFETY AND SECURITY TRAINING

Hazard and Risk Analysis

Bangkok, Thailand

1 March 2011

SAND No. 2011-0991 C
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

National Nuclear Security Administration

Sandia National Laboratories

Key acronyms

PHA = *process hazard analysis*

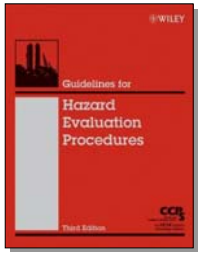
HAZOP = *hazard and operability [study]*

FMEA = *failure modes & effects analysis*

LOPA = *layer of protection analysis*

Hazard and risk analysis resources

CCPS 2008a. Center for Chemical Process Safety, ***Guidelines for Hazard Evaluation Procedures, Third Edition***, NY: American Institute of Chemical Engineers.

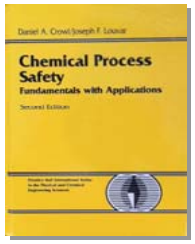


Chapter 4 • Non-Scenario-Based Hazard Evaluation Procedures
4.1 Preliminary Hazard Analysis
4.2 Safety Review
4.3 Relative Ranking
4.4 Checklist Analysis

Chapter 5 • Scenario-Based Hazard Evaluation Procedures
5.1 What-If Analysis
5.2 What-If/Checklist Analysis
5.3 Hazard and Operability Studies
5.4 Failure Modes and Effects Analysis
5.5 Fault Tree Analysis
5.6 Event Tree Analysis
5.7 Cause-Consequence Analysis and Bow-Tie Analysis
5.8 Other Techniques

Hazard and risk analysis resources

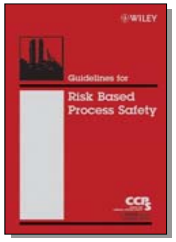
D.A. Crowl and J.F. Louvar 2001. ***Chemical Process Safety: Fundamentals with Applications, 2nd Ed.,*** Upper Saddle River, NJ: Prentice Hall.



Chapter 10 • Hazards Identification
Chapter 11 • Risk Assessment

Hazard and risk analysis resources

CCPS 2007a. Center for Chemical Process Safety, ***Guidelines for Risk Based Process Safety***, NY: American Institute of Chemical Engineers.



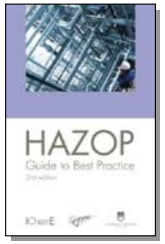
Chapter 9 • Hazard Identification and Risk Analysis
9.1 Element Overview
9.2 Key Principles and Essential Features
9.3 Possible Work Activities
9.4 Examples of Ways to Improve Effectiveness
9.5 Element Metrics
9.6 Management Review

5

Hazard and risk analysis resources

B. Tyler, F. Crawley and M. Preston 2008.

HAZOP: Guide to Best Practice, 2nd Edition, Institution of Chemical Engineers, Rugby, UK.



6

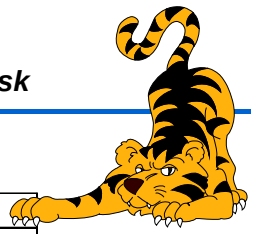
Hazard and Risk Analysis

- Basic risk concepts
- Experience-based vs predictive approaches
- Qualitative methods (What-If, HAZOP, FMEA)
- Order-of-magnitude and quantitative methods
- Analysis of procedure-based operations
- Team meeting logistics
- Documenting hazard and risk analyses
- Implementing findings and recommendations

Hazard and Risk Analysis

- Basic risk concepts

Hazard vs *Risk*



Fundamental definitions:

HAZARD
Presence of a material or condition that has the potential for causing loss or harm

RISK
A combination of the severity of consequences and the likelihood of occurrence of undesired outcomes

Source: R.W. Johnson, "Risk Management by Risk Magnitudes," *Chemical Health & Safety* 5(5), 1998

RISK

Constituents of risk:

- **Likelihood** and
- **Severity**

of Loss Events

$$Risk = f(Likelihood, Severity)$$

RISK

General form of risk equation:

$$Risk = Likelihood \cdot Severity^{n}$$

Most common form:

$$Risk = Likelihood \cdot Severity$$

RISK

Example units of measure:

$$Risk = Likelihood \cdot Severity$$

$$\frac{\text{injuries}}{\text{year}} = \frac{\text{loss events}}{\text{year}} \times \frac{\text{injuries}}{\text{loss event}}$$

$$\frac{\$\ \text{loss}}{\text{year}} = \frac{\text{loss events}}{\text{year}} \times \frac{\$\ \text{loss}}{\text{loss event}}$$

Costs vs *Risks*

Another way of understanding risk is to compare *risks* with *costs*:

Costs	Risks
Near certain; expected	Uncertain; unexpected; probabilistic
Cost estimates are usually available	Risk estimates are usually not available
Higher-precision estimates	Lower-precision estimates, if available
Predictable benefits if cost incurred	Negative consequences if outcome realized
Incurred every year over life of project	Liability incurred only if outcome realized

Source: R.W. Johnson, "Risk Management by Risk Magnitudes," *Chemical Health & Safety* 5(5), 1998

13

Costs + *Risks*

- ***Costs*** **are certain, or expected, liabilities**

  e.g., **30,000 km/year, 10 km/L, $1.00/L = $3,000/year**

- ***Risks*** **are uncertain liabilities**

  e.g., **$10,000 collision, 1/20 year = $500/year**

- **Costs + Risks = Total Liabilities**

  $3,000/year + $500/year = $3,500/year

14

What Is a "Process Hazard Analysis"?

A ***Process Hazard Analysis*** **PHA**

is a structured team review of an operation involving hazardous materials/energies, to

- **identify previously unrecognized hazards,**
- **identify opportunities to make the operation inherently safer,**
- **identify loss event scenarios,**
- **evaluate the scenario risks to identify where existing safeguards may not be adequate, and**
- **document team findings and recommendations.**

15

What Is a "Process Hazard Analysis"?

A ***Process Hazard Analysis*** **PHA**

is a structured team review of an operation involving hazardous materials/energies, to

- **identify previously unrecognized hazards,**
- **identify opportunities to make the operation inherently safer,**

  Already addressed

- **identify loss event scenarios,**
- **evaluate the scenario risks to identify where existing safeguards may not be adequate, and**
- **document team findings and recommendations.**

16

What Is a "Process Hazard Analysis"?

A ***Process Hazard Analysis*** **PHA**

is a structured team review of an operation involving hazardous materials/energies, to

- **identify previously unrecognized hazards,**
- **identify opportunities to make the operation inherently safer,**
- **identify loss event scenarios,**
- **evaluate the scenario risks to identify where existing safeguards may not be adequate, and**
- **document team findings and recommendations.**

Focus of this module

Hazard and Risk Analysis

- Basic risk concepts
- **Experience-based vs predictive approaches**

Experience-based approaches

- **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)**

Experience-based approaches

- **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**

Experience-based approaches

Example experience-based approaches:

- **Safety Review**
- **Checklist Analysis**

Experience-based approaches

Example experience-based approaches:

- Safety Review
- **Checklist Analysis**

Code/Standard/Reg.

1.1 The owner/operator shall …

1.2 The owner/operator shall …

1.3 The owner/operator shall …

→

Checklist

- ☐ Item 1
- ☐ Item 2
- ☐ Item 3
- ☐ Item 4

…

Experience-based approaches

Example experience-based approaches:

- Safety Review
- **Checklist Analysis**
  - Code/standard/regulatory requirements checklist
  - **See Crowl and Louvar 2001, pages 433-436, for a checklist of process safety topics**

Predictive studies

- **Supplement adherence to good practice**
- **Qualitative to quantitative**
- **Able to study adequacy of safeguards against <u>low probability</u> / <u>high severity</u> scenarios**
- **All predictive studies are scenario-based approaches**

Scenario - definition

Scenario:

An unplanned event or incident sequence that results in a loss event and its associated impacts, including the success or failure of safeguards involved in the incident sequence.

- CCPS 2008a

Scenario necessary ingredients:

- **Initiating cause**

  AND

- **Loss event or safe outcome**

Scenario necessary ingredients:

- **Initiating cause**

  AND

- **Loss event or safe outcome**

"Cause - consequence pair"

Example of a simple scenario

While unloading a tankcar into a caustic storage tank, the tank high level alarm sounded due to the person unloading not paying close attention to the operation.

The operator noticed and responded to the alarm right away, stopping the unloading operation. Normal production was then resumed.

- **What is the *initiating cause*?**
- **What is the *consequence*?**

Example of a more complex scenario

A reactor feed line ruptures and spills a flammable feed liquid into a diked area, where it ignites. A fire detection system initiates an automatic fire suppression system, putting the fire out.

The loss of flow to the reactor causes the temperature and pressure in the reactor to rise. The operator does not notice the temperature increase until the relief valve discharges to the relief header and stack. At that point, the emergency shutdown system is activated and the plant is brought to a safe state.

Predictive studies

Objective of scenario-based approaches:

- Identify and analyze <u>all</u> failure scenarios
  - Not generally possible just by inspection
  - Systematic approach needed
  - In reality, many scenarios eliminated by common sense and experience
    - Negligible likelihood (WARNING: Truly negligible?)
    - Unimportant consequence

Predictive studies

Some scenario-based approaches:

- What-If Analysis
- What-If/Checklist Analysis
- Hazard and Operability (HAZOP) Study
- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)

Hazard and Risk Analysis

- Basic risk concepts
- Experience-based vs predictive approaches
- Qualitative methods (What-If, HAZOP, FMEA)

What-If Analysis

What-If Analysis

Concept: **Conduct thorough, systematic examination by asking questions that begin with "What if..."**

- **Usually conducted by a relatively small team (3-5)**
- **Process divided up into "segments" (e.g., unit operations)**
- **Review from input to output of process**
- **Question formulation left up to the team members**

What-If Analysis

- **Question usually suggests an initiating cause.**

  "What if the raw material is in the wrong concentration?"

- **If so, postulated response develops a scenario.**

  "If the concentration of oxidant was doubled, the reaction could not be controlled and a rapid exotherm would result..."

What-If Analysis

Answering each "What if …" question:

1. **Describe potential consequences and impacts**
2. **If a consequence of concern, assess cause likelihood**
3. **Identify and evaluate intervening safeguards**
4. **Determine adequacy of safeguards**
5. **Develop findings and recommendations (as required)**
6. **Raise new questions**

Move to next segment when no more questions are raised.

Adequacy of safeguards

- Determining the adequacy of safeguards is done on a scenario-by-scenario basis
- *Scenario risk* is a function of:
  - Initiating cause frequency
  - Loss event impact
  - Safeguards effectiveness
- If the *scenario risk* is found to be too high, safeguards are considered inadequate
  - Qualitative judgment
  - Risk matrix
  - Risk magnitude

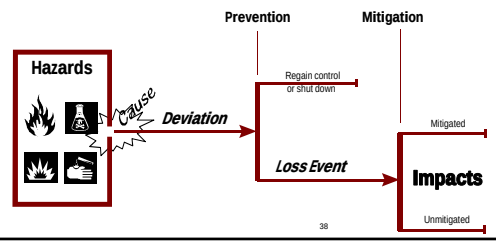
See SVA Overview for matrix and magnitude approaches.

37

Safeguards

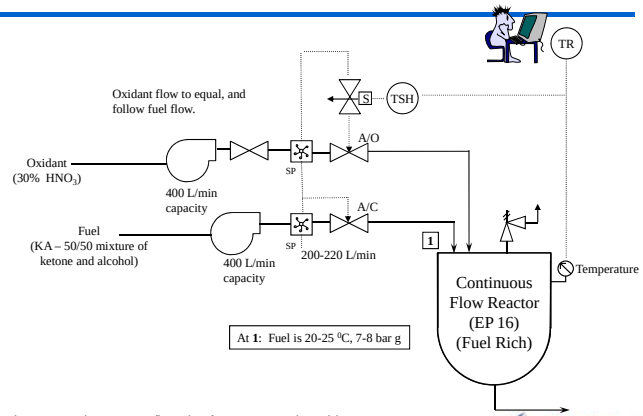
Evaluating the effectiveness of safeguards must take into account:

- *Fast* enough?
- *Effective* for this scenario?
- *Independent*?
- *Reliable* enough?



38

Example: Continuous Process

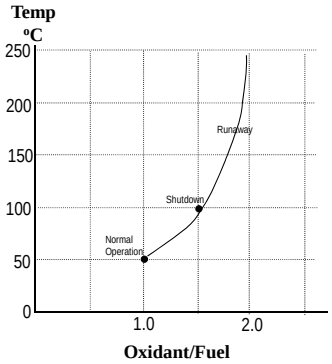


(Not an actual process configuration; for course exercise only)

39

Example: Continuous Process (cont.)

EP 16 produces adipic acid by an exothermic (heat-releasing) reaction of an oxidant (30% nitric acid) and a fuel (mixture of ketone and alcohol). An oxidant-to-fuel ratio greater that 2.0 in the reactor causes the reaction to run away (rapid temperature and pressure build-up). The high temperature shutdown system is intended to protect the reactor by stopping the oxidant flow if the reactor temperature reaches 100 °C. NOTE: RELIEF VALVE CANNOT CONTROL RUNAWAY REACTION.



40

PROCESS SEGMENT:	SCOPE:		What-If Analysis
REVIEW DATE:	INTENT:		
What If …	**Consequences**	**Safeguards**	**Finding/Recommendation** Comments

PROCESS SEGMENT:	SCOPE:		What-If Analysis
REVIEW DATE:	INTENT:		
What If …	**Consequences**	**Safeguards**	**Finding/Recommendation** Comments

PROCESS SEGMENT:	SCOPE:		What-If Analysis
REVIEW DATE:	INTENT:		
What If …	**Consequences**	**Safeguards**	**Finding/Recommendation** Comments

Hazard and Operability Study

HAZOP

CSP

44

Chemical SAFETY AND SECURITY TRAINING

HAZOP Study

- Developed within process industries
- Team-based approach
- Needs well-defined system parameters
- Used as hazard and/or operability study method
  - Safety issues dominate for existing process
  - Operability issues prevail for new designs
  - Many issues relate to both safety and operability

HAZOP Study

Premise:

- No incidents when system operates as intended ("normal operation")
- Failure scenarios occur when system deviates from intended operation ("abnormal situation")

HAZOP sequence

- Establish review scope
- Identify study "nodes"
- Establish Node 1 design/operation intent
- Identify Deviation 1 from Node 1 intent
- Identify causes, loss events, safeguards
- Decide whether action is warranted
- Repeat for every node and deviation

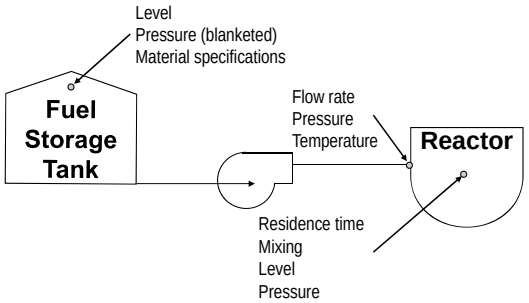
Study nodes

A node is a specific point in a process or procedure where deviations are studied.

Typical study nodes:

- Process vessel
- Transfer line
  - Strictly: Wherever a process parameter changes
  - At end of line (vessel interface)
  - Line may include pump, valves, filter, etc.
- Procedural step

Study nodes



Design/operational INTENT

The **intent** describes the design / operational parameters defining **normal operation**.

- Functions
- Limits
- Compositions
- Procedural steps

It answers one of these questions:

"What is this part of the process designed to do?"

"What is supposed to be done at this point in time?"

Design/operational intent

A complete design/operational intent includes:

- Equipment used
- All functions or operations intended to be achieved in this part of the process
- All intended locations/destinations
- Quantitative limits for all pertinent process parameters
- Intended stream composition limits

Design/operational intent

Example:

The intent of a reaction vessel 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 pressure.

Typical design intents

Storage tank

- **Contain between 40 and 300 cubic meters of 50% caustic at atmospheric pressure and ambient temperature.**

Transfer line

- **Transfer 40 to 45 L/min of [pure] acetone from drum to mixer at room temperature.**

Rotary kiln incinerator design intent

Contain and control the thermal incineration of incoming wastes (up to 4.76 t/h, 33.32 to 66.64 GJ/h heat load) to allow achievement of at least a 99.9% destruction and removal efficiency of organics in the incineration process by providing temperature (1000 to 1400 ^{o}C upstream of the secondary injection air point), residence time (at least 2 s for gases), and oxygen (9 to 13%, measured at the downstream end of the combustion zone) at a slight negative pressure (-100 Pa gage upstream of the secondary air injection point). Additional controlled variables are kiln rotation speed (0.05 to 0.5 rpm) and up to 15% Cl_2, up to 3% S, up to 50% H_2O, and up to 30% inerts entering the kiln.

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

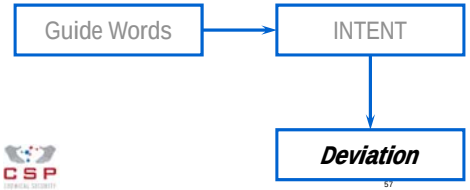
Guide Words → INTENT

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

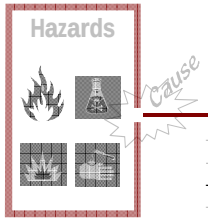
- Do not begin developing deviations until intent is fully described, documented and agreed upon
- List of deviations can be started as soon as intent is established



57

Deviations

A ***deviation*** is an <u>abnormal situation</u>, 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.

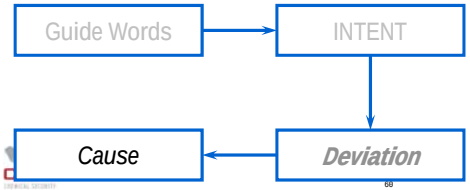
58

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	MORE OF	LESS OF
	Containment lost Procedure step skipped No [function] No transfer No agitation No reaction	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	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	**AS WELL AS**	**REVERSE**	**OTHER THAN**
Part of procedure step skipped Part of [function] achieved Part of [composition] Component missing Phase missing Catalyst deactivated	Extra step performed Extra [function] Transfer from more than one source Transfer to more than one destination Extra [composition] Extra phase present Impurities; dilution	Steps done in wrong order Reverse [function] Reverse flow Reverse mixing	Wrong procedure performed Wrong [function] achieved Transfer from wrong source Transfer to wrong destination Maintenance/test/sampling at wrong time/location

Initiating causes

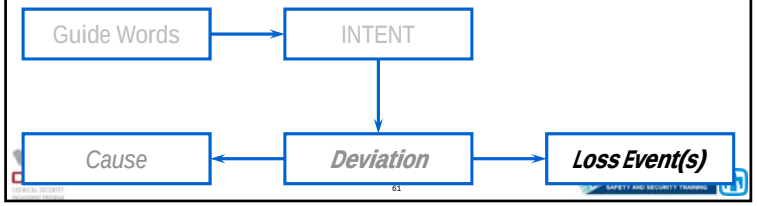
- Identify deviation cause(s)
  - Must look backward in time sequence
  - Only identify <u>local</u> causes (i.e., in current study node)
  - Most deviations have more than one possible cause



60

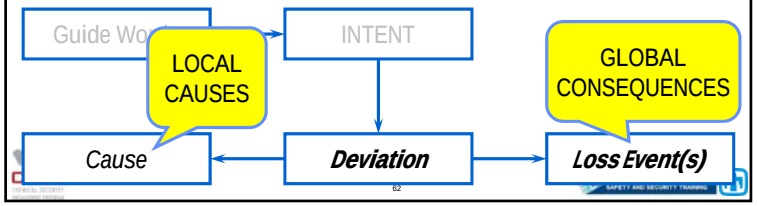
Loss events

- 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



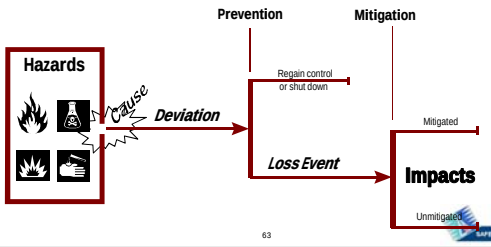
Loss events

- 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 <u>preventive</u> safeguards that intervene between the specific Cause-Consequence pair
- Note that different Consequences are possible, depending on safeguard success or failure *(e.g., PRV)*



	NODE:	HAZOP Study
REVIEW DATE	SCOPE: INTENT:	

Guide Word	Deviation	Cause	Consequences	Safeguards	Finding/Recommendation Comments

REVIEW DATE	NODE: SCOPE: INTENT:	HAZOP Study

Guide Word	Deviation	Cause	Consequences	Safeguards	Finding/Recommendation Comments

REVIEW DATE	NODE: SCOPE: INTENT:	HAZOP Study

Guide Word	Deviation	Cause	Consequences	Safeguards	Finding/Recommendation Comments

REVIEW DATE	NODE: SCOPE: INTENT:	HAZOP Study

Guide Word	Deviation	Cause	Consequences	Safeguards	Finding/Recommendation Comments

Failure Modes and Effects Analysis

FMEA

68

FMEA

- Originally developed for aerospace / military systems
- Good for systems with little human interaction
- Focus is primarily on independent equipment failures and their effects on the larger system

FMEA level of resolution

Level of resolution determines detail in FMEA table:

- Subsystem level
- Equipment (component) level
- Component parts

Equipment failure modes

EXAMPLE OF EQUIPMENT FAILURE MODES FOR FMEA

Equipment Description	Failure Modes
Pump, normally operating	a. Fails on (fails to stop when required) b. Transfers off c. Seal rupture/leak d. Pump casing rupture/leak
Heat exchanger, high pressure on tube side	a. Leak/rupture, tube side to shell side b. Leak/rupture, shell side to external environment c. Tube side, plugged d. Shell side, plugged

DISCUSSION

What are some common failure modes for the following components?

- Safety relief valve
- Check valve
- Float switch
- Agitator

Which of the failure modes are *revealed* and which are *latent*?

Completing the FMEA table

- Complete in deliberate, systematic manner
  - Begin at process boundary (usually input)
  - Evaluate each item in order of flowsheet
  - Complete each item before continuing
- Table entries:
  - Equipment identification
  - Equipment description (type, operation configuration, service characteristics)
  - Failure modes (all are listed)
  - Effects (scenario elements)
  - Safeguards
  - Findings and recommendations

73

REVIEW DATE	System:				FMEA
	P&ID:				
Component ID	Component Description	Failure Mode	Immediate to Ultimate Effects	Safeguards	Finding/Recommendation Comments

REVIEW DATE	System:				FMEA
	P&ID:				
Component ID	Component Description	Failure Mode	Immediate to Ultimate Effects	Safeguards	Finding/Recommendation Comments

Hazard and Risk Analysis

- Basic risk concepts
- Experience-based vs predictive approaches
- Qualitative methods (What-If, HAZOP, FMEA)
- **Order-of-magnitude and quantitative methods**

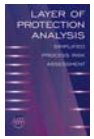
Order-of-magnitude & quantitative methods

- Layer of Protection Analysis (LOPA)
- HAZOP/LOPA
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Human Reliability Analysis (HRA)
- Consequence Analysis
- Others

Layer of Protection Analysis

LOPA

LOPA references



CCPS 2001. Center for Chemical Process Safety, ***Layer of Protection Analysis: Simplified Process Risk Assessment,*** NY: American Institute of Chemical Engineers.

IEC 61511-3, Annex F (Informative), Layer of protection analysis (LOPA)

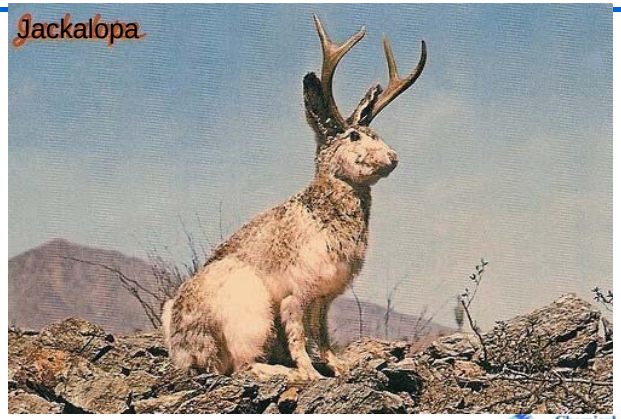
What Is a LOPA?

LOPA

A ***Layer of Protection Analysis***

- is a simplified method of risk assessment,
- intermediate between a qualitative process hazard analysis and a quantitative risk analysis,
- using simplifying rules to evaluate scenario impacts, initiating cause frequency, and independent layers of protection,
- to provide an order-of-magnitude risk estimate.

What Is a LOPA?



81

Impacts

ANALYSIS TYPE	IMPACT MEASURE
Qualitative hazard evaluations	Qualitative impact categories (e.g. L/M/H)
Layer of Protection Analysis (LOPA)	**Order-of-magnitude impact categories**
Quantitative risk analyses (QRAs)	Quantitative total impact assessment

82

What Is a LOPA?

LOPA

A ***Layer of Protection Analysis***

- **is a simplified method of risk assessment,**
- **intermediate between a qualitative process hazard analysis and a quantitative risk analysis,**
- **using simplifying rules to evaluate scenario impacts, initiating cause frequency, and independent layers of protection,**
- **to provide an order-of-magnitude risk estimate.**

83

What is a LOPA?

"LOPA typically uses order-of-magnitude categories

for <u>initiating event frequency</u>,

<u>consequence severity</u>,

and the <u>likelihood of failure of independent protection layers</u> (IPLs)

to approximate the risk of a scenario."

- CCPS 2001, p. 11

84

LOPA scenarios

LOPA scenarios are unique initiating event / loss event (cause-consequence) pairs.

- Scenarios are not identified by the LOPA analyst(s)
- **Scenarios are first identified by other means**
  - HAZOP Study
  - Safety Integrity Level (SIL) determination
  - Incident investigation
  - Management of change
- **Scenarios are then selected for LOPA**
  - Screening of hazard evaluation scenarios
  - Scenario(s) of interest to current situation

Initiating causes

- **"Initiating events" is term usually used in LOPA**
- **Same definition as for HAZOP Studies**
- **One initiating event per scenario**
- **A company may establish default initiating event frequency categories for LOPA usage**
  - **e.g. CCPS 2001, p. 71; see table footnote**
  - **e.g. see next two pages**

Initiating cause frequencies

Example set of initiating event categories for LOPAs:

Frequency*	Example
-1	Pump stops
-1	Sensor or final control element fails
-2	Fail-closed valve fails open
-2	Relief valve opens prematurely
-2	Unloading hose failure
-3	Piping system rupture
-4	Atmospheric tank mechanical failure
-5 to **-6**	Pressure vessel mechanical failure

* Initiating event frequency magnitude

Initiating cause frequencies

Examples given in ANSI/ISA-84.00.01-2004 Part 3:

Frequency*	Description	Examples
> -2	High - Can reasonably be expected to occur within the expected plant lifetime	Process leak Single instrument or valve failure Human error that could result in material release
-2 to **-4**	Medium - Low probability of occurrence within the expected plant lifetime	Single failures of small process lines or fittings
< -4	Low - Very low probability of occurrence within the expected plant lifetime	Spontaneous failure of single tanks or process vessels

* Initiating event frequency magnitude

Loss-of-containment reference

Table 2. Default Equipment Leak Frequencies

Equipment Type	Leak Frequency (per year except as noted)				Notes
	1/8" to 1/2" hole	1/2" to 2" hole	2" to 8" hole	Rupture	
Process piping[a]	3E-6 / (Dp x Dh), where Dp = pipe diam. (in.), Dh = hole diam (in.)				Frequency is per foot of pipe length per year
Pressure vessel	2E-4	1E-4	1E-5	1E-5	
Atmos tank	5E-3	1E-3	1E-4	2E-5	
Pump, centrif.	2E-2	4E-4	--	1E-4	For single seals[b]
Pump, recip.	7E-2	2E-3	--	1E-3	For single seals[c]
Compressor, centrifugal	5E-3	1E-3	--	3E-5	
Compressor, reciprocating or screw	5E-2	3E-3	--	5E-4	For medium-sized compressors[d]
Heat exch., shell	1E-3	2E-4	4E-5	2E-5	
Loading hoses	2E-2	--	--	2E-3	Based on 100 loadings/year per hose[e]

(a). The algorithm includes leaks in the pipe as well as leaks in connections such as welds and flanges in the line. The frequency includes hole sizes a factor of two above and below the hole size input to the equation.
(b). For double sealed pumps divide the ¼" hole frequency by 3
(c). For double sealed pumps divide the ¼" hole frequency by 3
(d). There is a large variation (factor of ~ 30) between small and large reciprocating compressors. Some rates are so large that a plant may have observed enough failures to develop site-specific data that can be used to replace the data above.
(e). For other usages, ratio as follows: Rate = Rate reported above x $[(\#\ \text{loadings/year})/100]^{0.5}$

From M. Moosemiller 2009, "Development of Algorithms for Predicting Ignition Probabilities and Explosion Frequencies," 43rd Annual Loss Prev Symposium.

89

Procedure-based operations

For procedure-based operations where the initiating event is an operational error:

Initiating event frequency

=

Frequency of performing operation

*****

Probability of error per operation

90

PHA EXERCISE

The Upper West Central Midland water treatment plant uses chlorine from 68 kg cylinders.

One cylinder is moved from storage to hookup twice a week.

While transporting a cylinder from storage, a cylinder that does not have its protective cap in place is dropped.

The valve strikes a concrete step and breaks off, resulting in a rocketing cylinder and a Cl_2 release.

What is the initiating event frequency?

91

IPL definition

Independent Protection Layer (IPL):

- A device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence,

  regardless [i.e., independent] of the initiating event or the action of any other protection layer associated with the scenario.

- The effectiveness and independence of an IPL must be auditable.

- CCPS 2001 Glossary

92

Possible IPLs

Use same thinking as for HAZOP Study *safeguards*.

- **BPCS (if criteria met)**
- **Operator response to critical alarm**
- **Safety Instrumented Function (SIF)**
- **Emergency relief system**
- **Mitigative safeguards (sometimes)**

IPL effectiveness

- **Must detect the abnormal situation**
- **Must decide to take the correct protective action (may be done automatically or in software)**
- **Must be capable of bringing the system to a safe state**
- **Must do all of the above quickly enough, before the loss event occurs**
- **All necessary components must work reliably**

Quantification of IPL effectiveness

From ANSI/ISA-84.00.01-2004 Part 3, Annex F:

Typical protection layer PFDs

Protection layer	Probability of failure on demand
Control loop	0.1
Human performance (trained, no stress)	1E-2 to 1E-4
Human performance (under stress)	0.5 to 1.0
Operator response to alarms	0.1
Vessel pressure rating above maximum challenge from internal and external pressure sources	1E-4 or better, if vessel integrity is maintained (i.e., corrosion is understood, inspections and maintenance is performed on schedule)

See also CCPS 2001 Tables 6.3 and 6.4; CCPS 2008a Table 7.4

Quantification of IPL effectiveness

Probability of Failure on Demand (PFD)

$$PFD_{IPL} = PFD_{Sensor} + PFD_{LogicSolver} + PFD_{FinalElement}$$

LOPA calculations

Basic scenario risk equation:

Risk = Scenario Frequency * Scenario Impact

Initiating event frequency * PFD_{IPL1} * PFD_{IPL2} * PFD_{IPL3} ...

Conditional modifiers

Three common *conditional modifiers:*

- **Probability of ignition | release**
- **Probability of person(s) in effect area | loss event**
- **Probability of injury or fatality | person(s) in area**

Conditional modifiers

Three common *conditional modifiers:*

- P_{ign}
- P_{loc}
- P_{inj}
- **These are risk reduction factors but not IPLs**
- **Each factor and its value is scenario-specific**

LOPA calculations

Scenario risk eqn. with conditional modifiers:

Risk = Scenario Frequency * Scenario Impact

IE freq. * PFD_{IPL1} * PFD_{IPL2} * PFD_{IPL3} ... * P_{ign} * P_{loc} * P_{inj}

"Typical spreadsheet that can be used for the LOPA"

#	Impact event descrip-tion	Severity level	Initiating cause	Initiation likelihood	PROTECTION LAYERS: General process design	BPCS	Alarms, etc.	Additional mitigation restricted access	IPL additional mitigation dikes, pressure relief	Inter-mediate event likelihood	SIF integrity level	Mitigated event likelihood	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0.1 / yr	0.1	0.1	0.1	0.1	PRV 01	1E-7 / yr	1E-02	1E-9 / yr	High press. causes column rupture
2	Fire from distillation column rupture	S	Steam control loop failure	0.1 / yr	0.1		0.1	0.1	PRV 01	1E-6 / yr	1E-02	1E-8 / yr	High press. causes column rupture
3	etc.												

ANSI/ISA-84.00.01-2004 Part 3 Report

Risk decisions • Options

Objective: All evaluated scenarios meet level of risk tolerable to the organization.

Approaches:

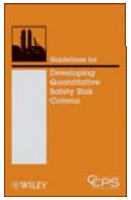
- Comparison with tolerable risk criteria
- Expert judgment *(not recommended by itself)*
- Relative risk reduction of competing alternatives
- Cost-benefit analysis of competing alternatives

Matrix approach - Two risk regions

SCENARIO LIKELIHOOD	MAG.	RISK-REDUCTION PRIORITY				
1 / year Expected to occur occasionally or periodically	0	A	A	A	A	A
1/10 yrs, or 10% per yr Likely to occur more than once during plant lifetime	-1	A	A	A	A	A
1% likelihood per year Might occur once during plant lifetime	-2	C	A	A	A	A
1/1,000 likelihood per yr Unlikely/not expected to occur during plant lifetime	-3	C	C	A	A	A
1/10,000 likelihood per yr Remote likelihood; would be surprising and unexpected	-4	C	C	C	A	A
1/100,000 per yr Not expected to be possible, or almost inconceivable	-5	C	C	C	C	A
		3	4	5	6	7

SEVERITY MAGNITUDE

Risk decisions • Resource



CCPS 2009. Center for Chemical Process Safety, ***Guidelines for Developing Quantitative Safety Risk Criteria***, New York: American Institute of Chemical Engineers.

Who performs LOPAs?

- Hazard evaluation team (HAZOP/LOPA)
- Single LOPA expert, with input
- Dedicated site or corporate LOPA team
- Third party, with input

HAZOP/LOPA

HAZOP/ LOPA

HAZOP/LOPA

- HAZOP Study using order-of-magnitude frequencies, impacts and probabilities
- Conditional modifiers used as risk-reduction factors and documented same as safeguards
- Done by HAZOP Study team
- **Reference:** R.W. Johnson, "Beyond-Compliance Uses of HAZOP/LOPA Studies," *Journal of Loss Prevention in the Process Industries 23*(6), November 2010, 727-733.

HAZOP/LOPA Example

Dev.	Cause	F	Consequences	S	Safeguards	Risk
No C_2H_4 Flow	FCV-1 fails closed	**-1**	Unreacted chlorine to furnace; possible failure of furnace tubes from chlorine contact damage; hot chlorine vapor release from furnace	4	[1] Alarm, shutdown on PT-1 low pressure [2] Detection of loss of ethylene flow by 2/h reactor sampling before furnace tube(s) fail	0

From Johnson 2010

Node 3	Flasher Bottoms Draw-off	HAZOP Study
Review Date:	SCOPE: TK-301 bottom outlet line, PU-301A/B, HE-323, to valve at blowdown tank inlet or valve at aromatics gas header battery limits INTENT: To prevent heavies buildup, transfer liquid heavies (C30's+) to blowdown tank or to aromatics gasoline header at 325-350 °F; suction pressure 8-20 psig, discharge 30-40 psig; 0.5 to 1.5 gpm, to maintain 10-30% level in TK-301	

GuideWord/ Deviation	Cause	Freq	Consequences	Severity On	Severity Off	Severity Bus	Safeguards	Protec Factor	Scenario Freq	Scenario Sev	Scenario Risk	Action Priority	Rec # Comments
NONE No Flow to Blowdown Tank or Header	Line rupture between TK-301 and FV-4113	-3	Release heated crude DCPD, including contents of TK-301	3	3	4	No protection safeguards	0	-3	3.3	**0.3**	C	Prevention: MI tests, inspections Mitigation safeguards: HC detectors
NONE No Flow to Blowdown Tank or Header	Line rupture between TK-301 and FV-4113	-3	Fire	4	3	5	Ignition source control	0.5	-3.5	4.0	**0.5**	B	Mitigation safeguards: HC detectors, fire monitors, Nomex Safeguards considered adequate
NONE No Flow to Blowdown Tank	Line rupture downstream of FV-4113	-3	Release restricted flow of liquid heavies, including backflow from blowdown tank	2	0	4	No protection safeguards	0	-3	2.0	**-1.0**	C	Would likely take longer to detect
NONE No Flow to Blowdown Tank	Line rupture downstream of FV-4113	-3	Fire	3	0	4	Ignition source control	2	-5	3.0	**-2.0**	C	
NONE No Flow to Header	Line rupture downstream of FV-4113	-4	Release restricted flow of liquid heavies, including backflow from header	3	3	4	No protection safeguards	0	-4	3.3	**-0.7**	C	**13** Transfer now goes to blowdown tank
NONE No Flow to Header	Line rupture downstream of FV-4113	-4	Fire	4	3	5	Ignition source control	1	-5	4.0	**-1.0**	C	**13**

Order-of-Magnitude HAZOP Study

Fault Tree Analysis

Fault Tree Analysis

FTA

- **Developed due to FMEA's inadequacy to analyze complex systems**
- **Able to handle concurrent events**
- **Integrates mechanical, human, process, external events**
- **Usually not a team-based approach**

Fault Tree Analysis

FTA

- **Risk analysis "power tool"**
  - **Resource-intensive**
  - **Logic models can get very large**
  - **Quantitative studies can take 3-6 months**
  - **Used in nuclear power risk assessments**
  - **Used for analyzing complex control systems**
- **Deductive, graphical logic modeling method**

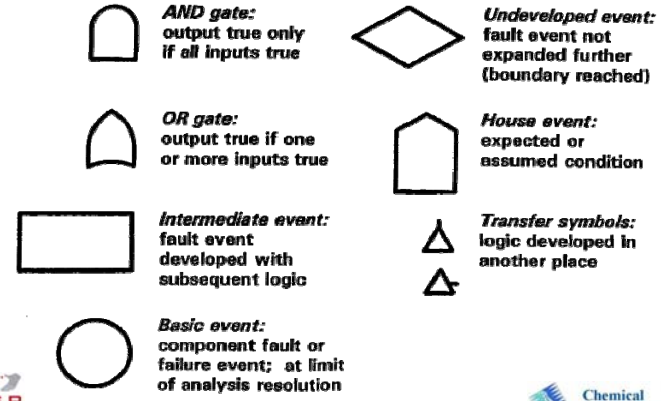
Fault Tree Analysis

"TOP" Event

- Establishes scope of analysis
- Should be a physical, irreversible loss event
  - Example: vessel rupture explosion
- FTA is NOT a system-wide review
  - Only analyzes events contributing to TOP event

113

Fault tree symbols



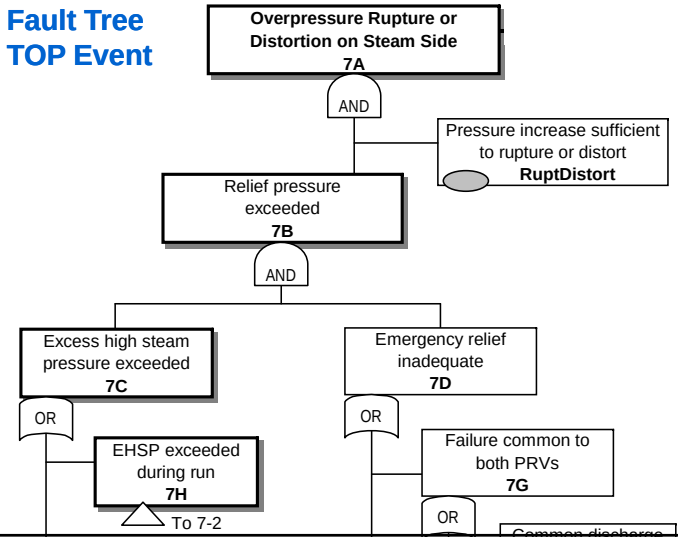
114

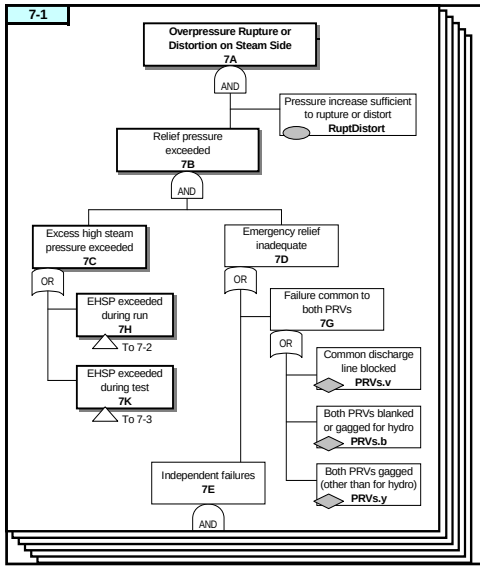
Fault tree construction

- Trace event sequence backwards in time
- No gate-to-gate connections
- Include all necessary and sufficient conditions
- Trace all branches back to basic events or boundaries

115

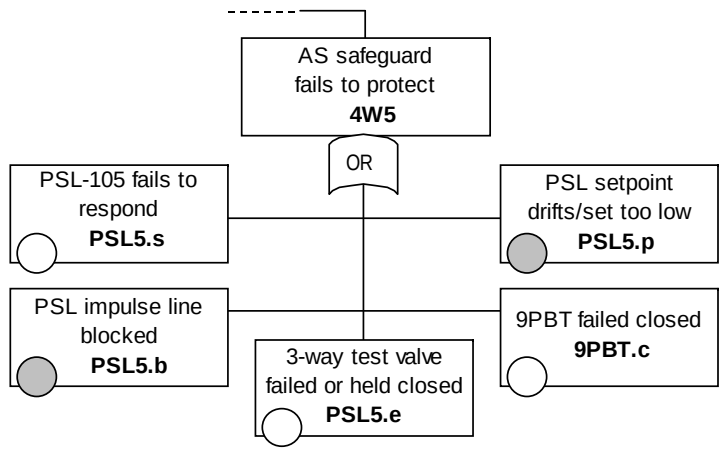
Fault Tree TOP Event





Reference: Kauffman et al., "Combustion Safeguards Test Intervals - Risk Study and Industry Survey," presented at AIChE Loss Prevention Symposium, Houston, April 2001.

Combustion air low pressure switch



Fault tree solution

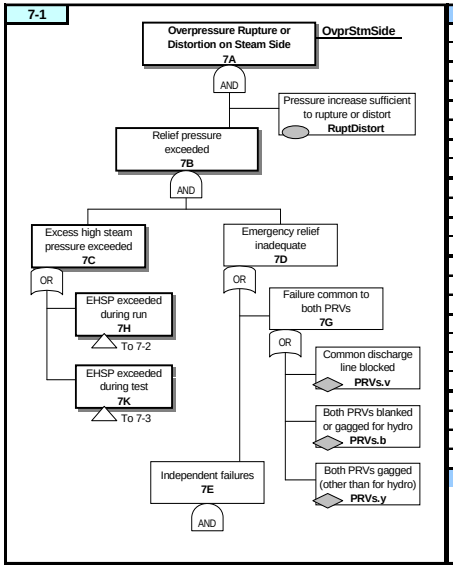
The Fault Tree is a Boolean algebra expression of the system.

Solving the expression yields *minimal cut sets*.

- **Minimal cut sets are all nonredundant scenarios that lead to the TOP event**
- **Common mode failures must have same ID**
- **Solution usually done by computer**

Quantifying basic event frequencies and probabilities yields a TOP event frequency.

119



Type	Name	Freq (/yr)	Dur (h)	Prob
Conseq	OvprStmSide	1.3E-06		
AND	7A	1.3E-06		
	RuptDistort			1
AND	7B	1.3E-06		
OR	7C	0.0071		
OR	7D			0.00018
	7H	0.0006		
	7K	0.0065		
OR	7E			8.E-05
OR	7G			1E-04
OR	7F1			0.0091
OR	7F2			0.0090
	PRVs.v			0
	PRVs.b			0.0001
	PRVs.y			0
	PRV1.v	0.004	4400	0.00201
	PRV1.s	0.009	4400	0.005
	PRV1.b	0.004	4400	0.00201
	PRV1.y			0.0001
	PRV2.v	0.004	4400	0.00201
	PRV2.s	0.009	4400	0.005
	PRV2.b	0.004	4400	0.00201
	PRV2.y			0

Notes:

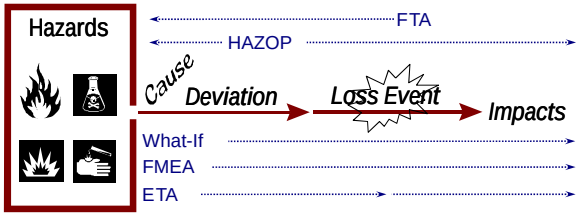
1. hydro = hydrotest
2. PRV settings: PRV1, 180 psig; PRV2, 185 psig
3. PRVs tested once/year, by either bench testing or testing in place

FTA EXERCISE

Draw the next level down for this TOP Event:

Flash fire

Summary of scenario-based approaches



PHA method selection guide

HAZOP	What-If/Checklist	FMEA	FTA	ETA
By deviation	By checklist item	By component	By loss event	By cause
Best for process operations	*Best for relatively standard operations*	*Best for mechanical and electrical systems*	*Best for complex systems/operations*	*Best to study one or only a few causes*
Good for continuous and procedure-based operations	Good for continuous and procedure-based operations	Good for continuous operations	Good for continuous operations; possible for procedure-based	Good to analyze administrative and engineering controls
Higher level of effort	Lower level of effort	Higher level of effort	Highest level of effort	Higher level of effort
Can analyze complex processes with multiple safeguards	*Mostly appropriate for simpler operations*	*Best analyzes processes with single-point failures*	*Can analyze complex processes with multiple safeguards*	*Can analyze complex processes with multiple safeguards*
Distinguishes between causes and safeguards	Does not distinguish between causes and safeguards	Does not distinguish between causes and safeguards	Distinguishes between causes and safeguards	Distinguishes between causes and safeguards
Only looks at causes that could lead to deviations	Only studies causes from checklist and what-if questioning	Looks at all failure modes of all components	Only studies causes and safeguards related to top event	Looks at all safeguards protecting against cause

Hazard and Risk Analysis

- Basic risk concepts
- Experience-based vs predictive approaches
- Qualitative methods (What-If, HAZOP, FMEA)
- Order-of-magnitude and quantitative methods
- **Analysis of procedure-based operations**

Procedure-based operations

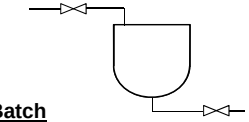
- Batch processes
- Continuous processes:
  - Start-up
  - Shutdown
  - Production changes
- Receipt and unloading of chemicals
- Loading of product
- Sampling
- Maintenance

Why analyze procedure-based operations?

- Typical petrochemical facility time distribution:
  < 10% of the time in "abnormal operations"
- IChemE analysis of 500 process safety incidents:
  53% of the incidents occurred during "abnormal operations" (startup, shutdown, responding to avoid a shutdown)

References:
S.W. Ostrowski and K.Keim, "A HAZOP Methodology for Transient Operations," presented at Mary Kay O'Connor Process Safety Center International Symposium, October 2008
I.M. Duguid, "Analysis of Past Incidents in the Oil, Chemical and Petrochemical Industries," IChemE *Loss Prevention Bulletin 144,* 1999

Batch vs continuous processes



Batch	Continuous
Transient process parameters	Steady-state process parameters
Many operations are time-dependent	Operations do not generally have time-dependencies
Manual operations / control common	Process control is usually automatic
Only part of system in use at any time	Entire system almost always in use

PHA of continuous operations

- Address continuous flows from input to output
- Address startup, shutdown and transient steps as procedure-based operations

PHA of procedure-based operations

Procedures usually follow these general steps:

1. Prepare vessel
2. Charge vessel
3. Reaction with monitor/control
4. Discharge
5. Purge

Which step is most like a continuous operation?

PHA of procedure-based operations

Suggested approach:

- Select study nodes as for continuous process
- Group procedures by nodes
- Conduct procedure-based PHA
- When procedure completed, do equipment-based PHA as for a continuous process

PHA of procedure-based operations

- PHA of procedure-based operation follows order of procedural steps
- All rules of continuous HAZOP Study apply
  - Local causes
  - Global consequences
  - All safeguards pertinent to cause-consequence pairs
- Consequence and safeguards considered at each succeeding step, until consequence occurs

Three approaches

- **What-If Analysis** of each operating step
- **Two-Guide-Word Analysis**
  - OMIT (all or part of the step is not done)
  - INCORRECT (step is performed wrong)
    - Operator does too much or too little of stated task
    - Wrong valve is closed
    - Order of steps is reversed
    - Etc.
- **HAZOP Study** of each step or group of steps
  - All seven guide words used
  - Extra guide word of "MISSING" sometimes used

DISCUSSION

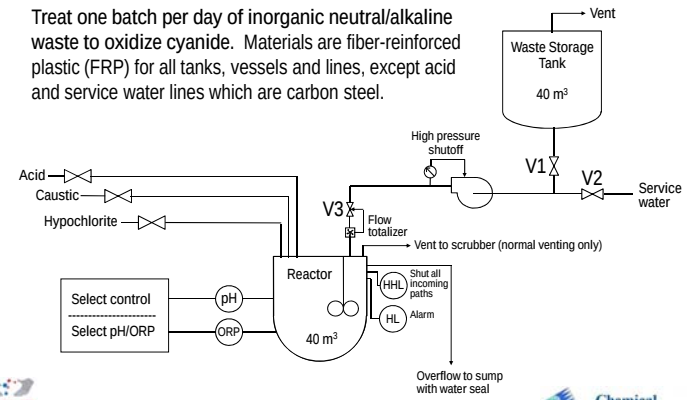
Give one or two examples of a deviation from a procedural step for each HAZOP guide word.

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

133

Example batch process

Treat one batch per day of inorganic neutral/alkaline waste to oxidize cyanide. Materials are fiber-reinforced plastic (FRP) for all tanks, vessels and lines, except acid and service water lines which are carbon steel.



134

Example batch process

Procedure:

1. Charge reactor with 5.3 m^3 of cyanide waste.
2. Add 24.8 m^3 service water to dilute waste to 0.3% (initially at 1.7%).
3. Add caustic (NaOH) on pH control to bring pH to 11.5.
4. Add sodium hypochlorite (NaOCl) on ORP control.
5. React with agitation for 6 hours; caustic and NaOCl to remain on auto-addition to maintain pH and ORP.
6. Send sample of reactor contents to lab to test for cyanide oxidation.
7. If lab approves, continue.
8. Add sulfuric acid (93%) on pH control to bring pH to 2.5.

Potential consequences:

- Concentration > 0.3% releases HCN during oxidation.
- Addition of acid before oxidation is complete releases all available CN^- as HCN.
- Excess NaOCL releases chlorine gas when acid is added.

135

"Actual procedure" for Step 1

1. Charge reactor with 5.3 m^3 of cyanide waste.

1.1 OPEN valve V1 to create path from cyanide waste storage tank to reactor.

Note: Valve V3 automatically opens when a flow totalizer value is set.

1.2 ENTER flow totalizer value of 5.3 via controller keyboard.

1.3 START waste transfer pump.

1.4 VERIFY pump automatically stops when 5.3 m^3 is transferred.

1.5 CLOSE valve V1 at waste storage tank.

136

PHA GROUP EXERCISE

- Divide into teams and conduct PHA of Step 1
- Use one or more of the three procedure-based approaches
- Be prepared to present your most important findings and any problems with, or comments on, your selected approach

137

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

What If …	Consequences	Safeguards	Finding/Recommendation Comments
1. Charge reactor with 5.3 m3 of cyanide waste. 1.1 OPEN valve V1 to create path from cyanide waste storage tank to reactor.			

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

What If …	Consequences	Safeguards	Finding/Recommendation Comments

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

What If …	Consequences	Safeguards	Finding/Recommendation Comments

REVIEW DATE	NODE: SCOPE: INTENT:	HAZOP Study

Guide Word	Deviation	Cause	Consequences	Safeguards	Finding/Recommendation Comments
1. Charge reactor with 5.3 m3 of cyanide waste. 1.1 OPEN valve V1 to create path from cyanide waste storage tank to reactor.					

REVIEW DATE	NODE: SCOPE: INTENT:	HAZOP Study

Guide Word	Deviation	Cause	Consequences	Safeguards	Finding/Recommendation Comments

REVIEW DATE	NODE: SCOPE: INTENT:	HAZOP Study

Guide Word	Deviation	Cause	Consequences	Safeguards	Finding/Recommendation Comments

Hazard and Risk Analysis

- Basic risk concepts
- Experience-based vs predictive approaches
- Qualitative methods (What-If, HAZOP, FMEA)
- Order-of-magnitude and quantitative methods
- Analysis of procedure-based operations
- **Team meeting logistics**

Team meeting logistics

The following are common to all PHA team reviews:

- Team composition
- Preparation
- First team review meeting
- Final team review meeting

PHA team composition

5 to 7 team members optimum

- Team leader (facilitator) – hazard analysis expertise
- Scribe – responsible for PHA documentation
- Key members – should have process/engineering expertise, operating and maintenance experience
- Supporting members – instruments, electrical, mechanical, explosion hazards, etc.

PHA preparation

At initial scheduling of review and designation as team leader:

- ☐Become familiar with the plant's PSM procedures
- ☐Determine exact scope of PHA
- ☐With PSM Coordinator, select one or more PHA methods that are appropriate to the complexity of the process

  (Different techniques can be used for different parts of the process)

PHA preparation

~ 6 weeks before start date of team review:

- ❑Compile process safety information for process to be studied
- ❑Obtain procedures for all modes of operation
- ❑Gather other pertinent information
- ❑Determine missing or out-of-date information
- ❑Make action plan for updating or developing missing information prior to the start of the team reviews

PHA preparation

~ 4 weeks before expected start date:

- ❑Confirm final selection of review team members
- ❑Give copy of PHA Procedures to scribe; emphasize the necessity for thorough documentation
- ❑Estimate the number of review-hours needed to complete PHA team review, or check previous estimate
- ❑Establish an initial schedule of review sessions, coordinated with shift schedules of team members

149

PHA timing

Plan PHA team review in half-day sessions of 3 to 3½ hours duration.

- *Optimum:* 1 session/day, 4 sessions/week
- *Maximum:* 8 sessions/week

- Schedule sessions on a long-term plan
- Schedule at set time on set days
- PHA team reviews usually take one or two days to get started, then ~ ½ day per typical P&ID, unit operation or short procedure

150

PHA preparation

~ 2 to 3 weeks before start date:

- ❑Obtain copies of all incident reports on file related to the process or the highly hazardous materials in the process
- ❑Reserve meeting room
- ❑Arrange for computer hardware and software to be used, if any
- ❑Divide up process into study nodes or segments
- ❑Develop initial design intent for each study node, with the assistance of other review team members as needed

151

PHA preparation

During the week before the start date:

- ❑Select and notify one person to give process overview
- ❑Arrange for walk-around of facility, including any necessary training and PPE
- ❑Secure projector and spare bulb
- ❑Arrange for refreshments and lunches

152

PHA preparation

Immediately before each meeting:

- ❑Check out meeting room and facilities, including heating/air conditioning
- ❑Set up computer and projection equipment
- ❑Lay out or tape up P&IDs and plant layout diagrams

First team review meeting

1 **Attendance**

- Go over emergency exits, alarms and evacuation procedures
- Introduce team members and their background / area of expertise
- Ensure all required team members are present
- Document attendance for each half-day session
- Emphasize need for punctuality and minimal interruptions

First team review meeting

2 **Scope and objectives**

- Go over exact boundaries of system to be studied
- Explain purpose for conducting the PHA

First team review meeting

3 **Methodology**

- Familiarize team members with methodology to be used
- Explain why selected methodology is appropriate for reviewing this particular process

First team review meeting

4 Process safety information

- Review what chemical, process, equipment and procedural information is available to the team
- Ensure all required information is available before proceeding

First team review meeting

5 Process overview

- Prearrange for someone to give brief process overview, covering such details as:
  - Process, controls
  - Equipment, buildings
  - Personnel, shift schedules
  - Hazardous materials, process chemistry
  - Safety systems, emergency equipment
  - Procedures
  - What is in general vicinity of process
- Have plant layout drawings available

First team review meeting

6 Unit tour

- Prearrange for tour through entire facility to be included in team review
- Follow all safety procedures and PPE requirements
- Have team members look for items such as:
  - General plant condition
  - Possible previously unrecognized hazards
  - Human factors (valves, labeling, etc.)
  - Traffic and pedestrian patterns
  - Activities on operator rounds (gauges, etc.)
  - Emergency egress routes

First team review meeting

7 Review previous incidents

- Review all incident and near-miss reports on file for the process being studied
- Also review sister-plant and industry-wide incidents for the type of process being studied
- Identify which incidents had potential for catastrophic on-site or off-site / environmental consequences
- Make sure detailed assessment (e.g., HAZOP Study) covers all previous significant incidents

First team review meeting

8 Review facility siting

- Discuss issues related to whether buildings intended for occupancy are designed and arranged such that people are adequately protected against major incidents
- Various approaches are possible:
  - **API Recommended Practices 752, 753**
  - **Topical review** (e.g., CCPS 2008a page 291)
  - **Checklist review** (e.g., Appendix F of W.L. Frank and D.K. Whittle, *Revalidating Process Hazard Analyses*, NY: American Institute of Chemical Engineers, 2001)

161

First team review meeting

9 Review human factors

- Discuss issues related to designing equipment, operations and work environments so they match human capabilities, limitations and needs
- Human factors are associated with:
  - **Initiating causes** (e.g., operational errors causing process upsets)
  - **Preventive safeguards** (e.g., operator response to deviations)
  - **Mitigative safeguards** (e.g., emergency response actions)

162

First team review meeting

9 Review human factors (continued)

- Various approaches are possible:
  - **Ergonomic studies**
  - **Topical review of positive and negative human factors** (e.g., CCPS 2008a pages 277-279)
  - **Checklist review** (e.g., Appendix G of W.L. Frank and D.K. Whittle, *Revalidating Process Hazard Analyses*, NY: American Institute of Chemical Engineers, 2001)

163

First team review meeting

10 Identify and document process hazards

- See earlier module on Hazards and Potential Consequences
- Also an opportunity to address inherent safety issues

164

Final team review meeting

To do during the final team review meeting:

- Ensure entire scope of review has been covered
- Read through all findings and recommendations to
  - Ensure each finding and recommendation is understandable to those needing to review and implement them
  - Consolidate similar findings
- Ensure all previous significant incidents have been addressed in the PHA scenarios

Hazard and Risk Analysis

- Basic risk concepts
- Experience-based vs predictive approaches
- Qualitative methods (What-If, HAZOP, FMEA)
- Order-of-magnitude and quantitative methods
- Analysis of procedure-based operations
- Team meeting logistics
- **Documenting hazard and risk analyses**

PHA report

<u>Goal</u>: Record the results such that study is understandable, can be easily updated, and supports the team's decisions.

- System studied
- What was done
- By whom
- When
- Findings and recommendations
- PHA worksheets
- Information upon which the PHA was based

Report disposition

- Draft report
  - prepared by scribe
  - reviewed by all team members
  - presented to management, preferably in a face-to-face meeting
- Management input considered by review team
- Final report
  - prepared by scribe
  - reviewed by all team members
  - accepted by management
  - kept in permanent PHA file

Hazard and Risk Analysis

- Basic risk concepts
- Experience-based vs predictive approaches
- Qualitative methods (What-If, HAZOP, FMEA)
- Order-of-magnitude and quantitative methods
- Analysis of procedure-based operations
- Team meeting logistics
- Documenting hazard and risk analyses
- **Implementing findings and recommendations**

Implementing findings & recommendations

What is the most important product of a PHA?

1. **The PHA report**
2. **A deeper understanding gained of the system**
3. **Findings and recommendations from the study**

170

Implementing findings & recommendations

What is the most important product of a PHA?

1. The PHA report
2. A deeper understanding gained of the system
3. **Findings and recommendations from the study**
4. **The actions taken in response to the findings and recommendations from the study**

171

Implementing findings & recommendations

- **Findings and recommendations are developed throughout team review**
  - **Analysis of hazards; inherent safety options**
  - **Facility siting review**
  - **Human factors review**
  - **HAZOP, What-If, etc.**
- **<u>Basis</u> for determining whether finding or recommendation is warranted:**
  - **CHECKLIST REVIEW: Code/standard is violated**
  - **PREDICTIVE ANALYSIS: Scenario risk is too high** (also if code/standard is violated)

172

Implementing findings & recommendations

Wording of findings and recommendations:

- **Be as general as possible in wording of finding, to allow flexibility in how item is resolved**

Install reverse flow protection in Line 112-9 to prevent backflow of raw material to storage	**instead of**	Install a Cagey Model 21R swing check valve in the inlet flange connection to the reactor

- **Describing the concern as part of the finding will help ensure the actual concern is addressed**
- **Use of words such as these warrants follow-up to ensure the team's concern was actually addressed:**
  - **CONSIDER…**
  - **STUDY…**
  - **INVESTIGATE…**
  - **_____…**

173

PHA risk-control actions

Example risk-control actions:

- **Alter physical design or basic process control system**
- **Add new layer of protection or improve existing layers**
- **Change operating method**
- **Change process conditions**
- **Change process materials**
- **Modify inspection/test/maintenance frequency or method**
- **Reduce likely number of people and/or value of property exposed**

174

PHA action item implementation

The employer shall establish a system to promptly address the team's findings and recommendations; assure that the recommendations are resolved in a timely manner and that the resolution is documented; document what actions are to be taken; complete actions as soon as possible; develop a written schedule of when these actions are to be completed; communicate the actions to operating, maintenance and other employees whose work assignments are in the process and who may be affected by the recommendations or actions.

- OSHA PSM Standard, 29 CFR 1910.119(e)(5) and U.S. EPA RMP Rule, 40 CFR 68.67(e)

175

1 - Document findings & recommendations

Example form:

ORIGINAL STUDY FINDING / RECOMMENDATION			
Source: ☐ PHA ☐ Incident Investigation ☐ Compliance Audit ☐ Self-Assessment ☐ Other			
Source Name			
Finding No.		**Risk-Based Priority** *(A, B, C or N/A)*	
Finding / Rec-ommendation			
Date of Study or Date Finding / Recommendation Made			

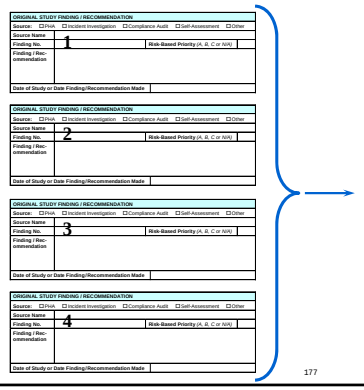
Note that this can also be used for incident investigation and compliance audit findings.

176

2 - Present findings & recommendations

PHA team

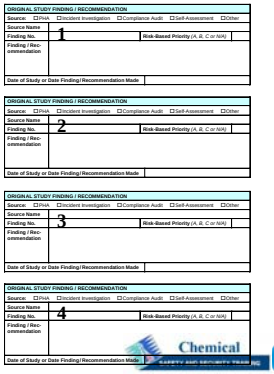
Line management



2 - Present findings & recommendations

PHA team

Line management



3 - Line management response

For each PHA team finding/recommendation:

ACTION COMMITTED TO BY MANAGEMENT		
Specific Action To Be Taken		
To Be Completed By	[date]	*Time extension requires management approval*
Responsible Person	[person or position]	

Suggestions:

- **Use database or spreadsheet**
- **Flag imminent and overdue actions**
- **Periodically report overall status to top management**

Example

ORIGINAL STUDY FINDING / RECOMMENDATION			
Source:	PHA ☐ Incident Investigation ☐ Compliance Audit ☐ Self-Assessment ☐ Other		
Source Name	Formaldehyde Unloading PHA		
Finding No.	PHA-UF-11-01	**Risk-Based Priority** *(A, B, C or N/A)*	B
Finding / Rec-ommendation	*Safeguards against formaldehyde storage tank overfilling are considered to be inadequate due to the signals for the controlling level indication and the high level alarm both being taken off of the same level transmitter. Options for consideration: Take manual level reading before unloading into the tank to cross-check adequate capacity for unloading; add separate high level switch for the high level alarm.*		
Date of Study or Date Finding / Recommendation Made	1 March 2011		
ACTION COMMITTED TO BY MANAGEMENT			
Specific Action To Be Taken	The following steps are to be taken to adopt and implement finding PHA-UF-11-01: (1) Add a separate high level switch on the formaldehyde storage tank, using a different level measurement technology than the controlling level sensor. (2) Add the new level switch, in addition to the high level alarm, to the MI critical equipment list and schedule for regular functional testing. (3) Until the new level switch is installed, implement a temporary procedural change to take manual level readings before unloading into the tank to cross-check adequate capacity for unloading, ensuring proper PPE is specified and used for performing the manual level readings.		
To Be Completed By	1 September 2011	*Time extension requires management approval*	
Responsible Person	I. M. Engineer		

4 - Document final resolution

Document how each action item was implemented.

FINAL RESOLUTION		
Resolution Details *(attach drawings, procedures, etc.)*		
Associated MOC(s)		
DATE COMPLETED		
Date Communicated		
How Communicated		*Attach documentation of the communication(s)*

Communication of actions

Communicate actions taken in response to PHA findings and recommendations.

TO WHOM?

- **To operating, maintenance and other employees whose work assignments are in the process and who may be affected by the recommendations or actions**

Communication of actions

HOW?

- **Train through plant training program when needed**
  - **Use appropriate techniques**
  - **Verify understanding**
- **Otherwise inform, such as by**
  - **Safety meetings**
  - **Beginning-of-shift communications**
  - **E-mail**
- **Document communications**

Communication of actions

WHAT?

- **Physical changes**
- **Personnel or responsibility/accountability updates**
- **Operating/maintenance procedures**
- **Emergency procedures; Emergency Response Plan**
- **Safe work practice procedures**
- **Control limits or practices**

DISCUSSION

WHY?

What are two or more reasons why it is important to communicate PHA action items to affected employees?

-
-
-
-

185

Final word

The task of the PHA team is to <u>identify where action is needed</u>, not to redesign the system.

186