Choosing Appropriate Hazards Analysis Techniques For Your Process

Authors:

Jay L. Potter, Senior Hazards Analyst
Lyman A. Losee, CSP, Senior Hazards Analyst

Global Environmental Solutions

Twenty-Seventh Department of Defense Explosives Safety Seminar
Las Vegas, Nevada
August 21, 1996

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
21 AUG 1996		**00-00-1996 to 00-00-1996**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Choosing Appropriate Hazards Analysis Techniques For Your Process	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Global Environmental Solutions, ,4100 South 8400 West,Magna,UT,84044**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM000767. Proceedings of the Twenty-Seventh DoD Explosives Safety Seminar Held in Las Vegas, NV on 22-26 August 1996.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**22**	

INTRODUCTION

Hazards analysis is one of many important issues for safety professionals. Sometimes we are required to perform Process Hazards Analyses (PHA) within our companies with little or no formal training. Even experienced analysts are sometimes bewildered with the many different techniques available to perform hazards analyses. This presentation is designed to help safety professionals select the right hazards analysis tools to perform a hazards analysis appropriate for the complexity of the process being evaluated. The authors are senior hazards analysts at Global Environmental Solutions (GES) with a total of 60 years experience working with hazardous and explosive materials.

DOES YOUR PROCESS REQUIRE HAZARDS ANALYSIS?

Hazards analysis is a systematic engineering tool for identifying, documenting and resolving process/ system hazards. A complete hazards analysis includes hazard identification, prioritization, risk assessment, risk management, risk/ cost trade-off, and documentation. It is a road map of logical conclusions about safety. It allows safety professionals to easily communicate these conclusions to the management people that make decisions. The hazards analysis alone does not make the plant safe; however, a hazards analysis allows decisions to be made that can prevent accidents before they happen.

We should all now be familiar with the Process Safety Management (PSM) requirements of 29CFR 1910.119. OSHA says that an "appropriate" formal analysis technique shall be used; but it does not require that a specific technique be used[1]:

"The employer shall use one or more of the following methodologies that are appropriate to determine and evaluate the hazards of the process being analyzed.

(I) What-if;
(ii) Checklist;
(iii) What-if/Checklist;
(iv) Hazard and Operability Study (HAZOP);
(v) Failure Mode and Effects Analysis (FMEA);
(vi) Fault Tree Analysis; or
(vii) An appropriate equivalent methodology."

The safety professional has the freedom to select the type, or form of hazards analysis for each project. Selecting the hazards analysis technique (or combination of techniques) that is best for a project is not difficult, but the complexity of the analysis must reflect the complexity of the process. Remember, the main objective of hazards analysis is to manage risk.

WILL HAZARDS ANALYSIS MAKE A DIFFERENCE?

Compliance with PSM will definitely improve plant safety! PSM forces companies to approach safety problems in a proactive manner. Many potential accidents can and will be avoided due to the fact that safety professionals are now looking at ways that things can go wrong. Process design engineers sometimes focus primarily on how a process is supposed to work-- not on how it could fail. Responsible safety professionals through proper application of hazards analysis can make a cost-effective, and perhaps a life saving contribution. It is for this reason that this paper is presented.

AVOIDING ACCIDENTS BEFORE THEY HAPPEN

Until recently, some safety departments existed just to prevent personal injuries like slips, trips, and falls. The days of the old-style "safety glasses and hard hat" industrial safety departments have been replaced with educated, modern, safety professionals. In the past, some safety engineers would be content to wait for an accident to happen; then they would "work like crazy" implementing rules and regulations to prevent the same accident from happening again. The major flaw with this type of reasoning is that a certain number of accidents must be allowed to happen before unsafe behavior can be changed. The goal of modern safety engineering is to prevent accidents before they happen. Hazards analysis is the tool to use to accomplish this goal.

THE COST OF ACCIDENTS VS. THE COST OF HAZARDS ANALYSIS

The cost of doing business in today's world is staggering. The costs of having accidents in the work place is astronomical! The American legal system can evaporate corporate funds in a heartbeat when accidents are allowed to happen.

Management sometimes has great difficulty justifying the "cost of safety". Hazards analysis can be costly up front. However, if the process is accident free (as a result of an appropriate hazards analysis) the hazards analysis is profitable and cost-effective.

WHAT IS PHA?

Process hazards analysis (PHA) is a systematic approach to identify potential hazards and to recommend actions to eliminate (or minimize) hazards in a process. Almost everything we do can be hazardous. Driving to work can be extremely hazardous. We know by observation and experience that automobile accidents are a possibility. It can also be seen that once we identify a hazard, such as an automobile accident, there are various ways to minimize the risk. We minimize automobile hazards by following traffic rules, wearing seat belts, and by having air bags in our cars.

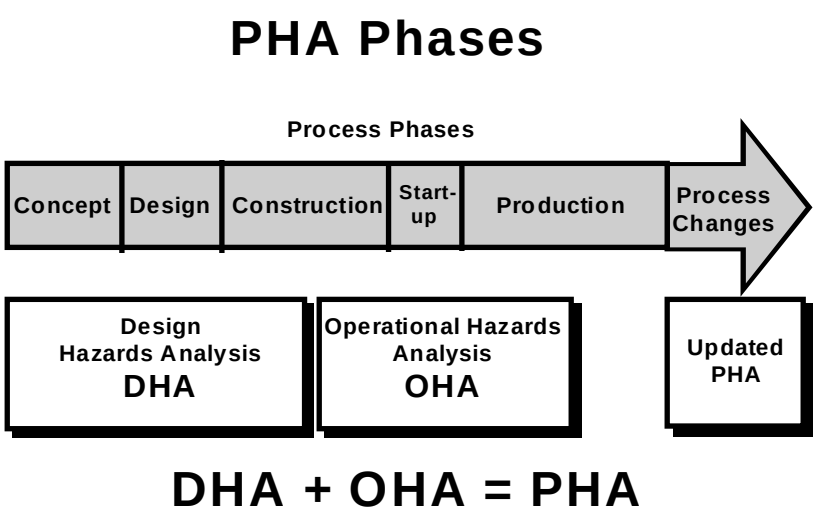
This example shows some of the different philosophies that can be applied to minimize risk--training, operating procedures, safety and warning devices, and design. Training is necessary for all operations but it is not the most fool-proof safety approach. A design improvement such as air bags will automatically reduce the chance of injury to the car occupants without operator action. On the other hand, training, such as in use of seat belts, can be readily accomplished anytime, but some design changes, such as air bags, are most easily and cheaply added early in the design of the car rather than after you purchase it. Time, cost and effectiveness all must be considered.

Process hazards analysis will now be described in more detail. We will show how a PHA has different phases depending on the maturity of the process being analyzed and we will describe the major hazards analysis methodologies available to use in identifying potential hazards in a process. It will be shown that one approach and one technique does not fit all circumstances. PHA must be tailored to most effectively and inexpensively accomplish the goals of identifying hazards and minimizing the risk to personnel, facilities and the environment.

PHA PHASES

The PHA phases in relation to the phases in a process are shown in Figure 1.

Figure 1. A PHA should consist of both design and operational phases



A typical process development will go through many phases from concept to design, construction, start-up, production and then changes as improvements need to be made. The Process Hazards Analysis, if done correctly, will also have phases. During the concept, design and early construction stages of the process a Design Hazards Analysis or DHA is most appropriate. The flowcharts and equipment drawings and discussions with engineers may be the only things that can be evaluated. At this point, however, it is easy and cost effective to correct design problems discovered by the DHA. Safety guidelines can be recommended that will help direct the process design toward a safe and perhaps more economical configuration.

An Operational Hazards Analysis or OHA can be started as equipment is put in place during the construction, start-up, and during the early production phases. An OHA can be done when equipment is in place, when procedures are available and when the operator interface with equipment can be observed. Sometimes the DHA and OHA may overlap if part of the process is still under construction but another part is ready to go into operation.

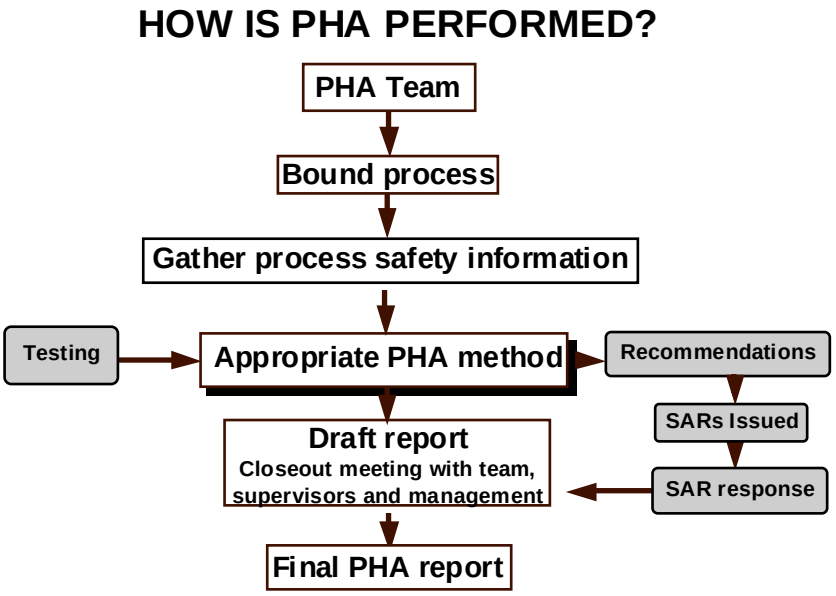
The total Process Hazards Analysis(PHA) consists of both the DHA and the OHA phases. Of course, if the process is an existing process the PHA may consist only of the OHA or maybe include only a small DHA on a part of the process that is being updated.

HOW IS A PHA PERFORMED?

The overall steps in a Process Hazards Analysis whether in the DHA or OHA phases is shown in

Figure 2.

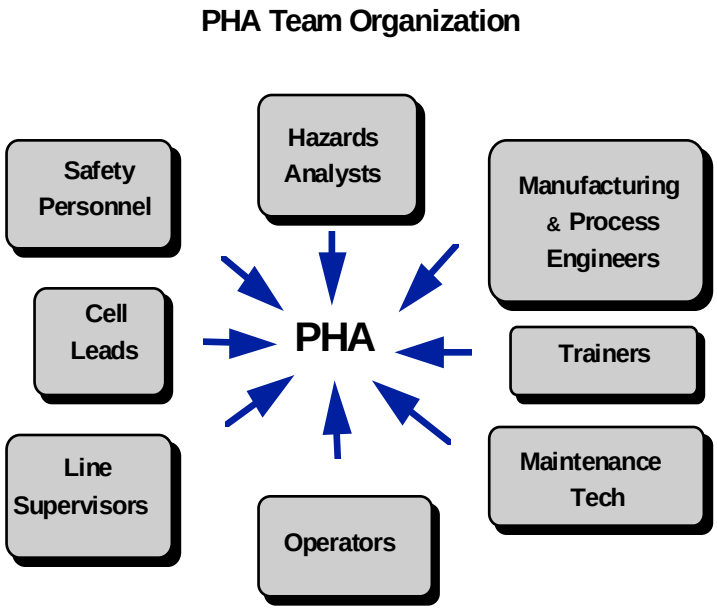
Figure 2. A PHA consists of several important steps including an appropriate PHA methodology



Forming the PHA Team

The initial step in a PHA is formation of an analysis team. Use of the team approach is required by the PSM regulation. The involvement and time spent by the team members will vary depending on the process, the PHA methodology used, and the process and methodology phases. Typical personnel forming a team are shown in Figure 3

Figure 3. All disciplines involved in the process should be represented on the PHA team



The team can vary in size from two people to any reasonable number. The top three team representatives--safety personnel, hazards analysts and manufacturing and process engineers--may be the only ones involved in a DHA team but in an OHA team all representatives should be involved and perhaps others as needed. Note that operators and maintenance personnel play an important part. The team leader, usually the hazards analyst, needs to be fully knowledgeable in the PHA methodology to be used. The other full or part time members provide the expertise in areas such as process technology, process design, instrumentation, maintenance procedures, safety and health, process operation and any other relevant subject that will be helpful to the analyst and the other members of the team. The ideal team will have a working knowledge of the standards, codes, specifications, and regulations applicable to the process being studied or at least know where to go to find this information when questions arise.

Bounding the Process

The next step in the PHA is to bound the process. The hazards analyst needs to define where the analysis begins and ends. The OSHA PSM regulation, the toxicity, or the reactivity of the chemicals involved may help bound the areas to be analyzed. Areas without hazardous material as defined by OSHA may best be evaluated with another technique different from that used for the main process and not requiring a team effort.

Gathering Process Safety Information

Before the analysis can begin, information must be assembled pertaining to hazardous chemicals, process technology, equipment and facility features, and history of previous incidents. The physical and chemical properties of the starting materials, intermediate mixtures and the final product must be determined and material safety data sheets (MSDSs) obtained where possible. If important information is not available tests must be run or the information obtained in some other way. As the analysis progresses it will probably be realized that additional information is needed requiring further information gathering or testing. Process technology information needed are flow diagrams, process chemistry, operating parameters (including credible abnormal conditions) and operating procedures. Equipment and facility details desirable are piping and instrumentation drawings (P&IDs), view drawings, maintenance practices, safety systems (interlocks, venting, and fail-safe conditions), design codes and standards, and information on construction materials.

Selecting the Appropriate PHA Method

A variety of process hazards analysis techniques are available. The methods addressed in this paper are those mentioned in the OSHA PSM regulation 29 CFR 1910.119:

- Checklist
- What-if
- What-if Checklist
- Hazards and Operability Study (HAZOP)
- Fault Tree / Logic Diagram
- Failure Modes and Effects Analysis (FMEA)

The complexity and type of process should be the driving factors in selection the method or combination of methods to use. Unfortunately, many people choose a less desirable methodology just

from lack of knowledge of the choices available or from improperly letting the cost, schedule or resources drive the decision. One of the purposes of this paper is to provide sufficient familiarity with the techniques available and their most appropriate uses to help in this choice. For example, the checklist and what-if methods are more simple than the other methods and are more appropriate for a simple process. The HAZOP has found much use in the petroleum and chemical industries and the fault tree and FMEA techniques have been used in the systematic analysis of complex, interactive systems. One should not be tied to the traditional uses; however, we want to stress using the methodology or combination of methodologies that best fits your process.

PHA Findings, Recommendations, and Documentation

Once the appropriate process hazards analysis methodology has been selected and the PHA process is progressing, documentation of the findings and recommendations must begin. GES uses a closed loop system using Safety Action Requests (SARs) to document recommendations as soon as they arise in the analysis and to start the correction process. You should not wait until the report is finished to alert the plant of important findings and the recommendations to correct them. The SAR form is a one-page document issued by the PHA team to a specific management representative. An example of a SAR is given in Figure 4. The Recommendation and potential hazard are explained. There is a line for management to specify the designated person to address the issue and a section for documentation of the corrective action taken. The status of the action (open, implemented, in-process, or canceled) is noted.

Figure 4. Example of a typical SAR

To: Mr. Chief Engineer

Requester: GNU Process PHA Team

Date: 12-6-95

SAR: GNU - 37

Status: O

Operation/Item: WEIGHING EQUIPMENT

Reference: FMEA Line 42A

Recommendation:
Verify that scale design and wiring is appropriate for use in hazardous area and update as necessary.

Potential Hazard / Safety Benefit:
Propellant initiation from propellant dust in scale or wiring.

Action Assigned to:

Projected Completion Date:

Action Taken:

SIGNATURES:

Completion/Date:	**Verification/Date:**
[Person Assigned Action]	[Action Requester]

Figure 2 shows the loop in the PHA process of recommendations leading to SARs and the SAR being included in the draft report. Many recommendations will be implemented before the report is issued and that would be noted on the SAR to provide closed loop documentation as required by OSHA PSM Regulations.

The PHA Report

The PHA report is very important. It is the main means of communication to management. As such, it must contain the elements needed to make that communication complete. The report should stand alone in that someone reading it will be told enough about the process to understand the importance of the findings and the recommendations. The standard sections we use in our reports are as follows:

- Objectives
- Summary and Conclusions
- Recommendations (Summary)
- Introduction
- Team Members
- Hazards Analysis Methodology (Brief description)
- Process Description
- Discussion (Discuss important findings and recommendations)
- References
- Recommendation Table (Lists recommendations, potential hazard, PHA work sheet reference such a HAZOP or FMEA tables, and SAR status)
- Analysis tables and work sheets (HAZOP, FMEA, fault tree/logic diagram, what-if table etc.)
- Appendix (table heading explanations, logic symbol definitions, etc.)
- Safety Action Requests (SAR status at time of report publication)

PHA TECHNIQUES AND EXAMPLES OF THEIR USE

Selection of the proper PHA methodology for a process should be made on the basis of which technique lends itself to the type and complexity of the process being analyzed. To be able to make a wise choice, the advantages, disadvantages and differences of the various techniques must be known. Most techniques are easily learned. Companies like GES are available to help if necessary and cost effective. Each of the major PHA techniques suggested by the OSHA PSM regulation will be briefly explained and some examples of each will be given.

Checklist

Checklist Analysis consists of listing critical safety items or procedural steps to be done before the process is performed. This type of analysis meets requirements of PSM, and is easy to complete. It can be done at any stage in the life of a project. The major benefit of this type of hazards analysis is that it very cost effective. It usually can be completed within days (sometimes hours), and can be easily understood by non-safety-oriented personnel.

A serious drawback to checklist analysis is that the effectiveness or safety benefit is limited by the experience of the analysts making the checklist. Analysts must be very familiar with all aspects of the project to complete a comprehensive checklist. Experience is the key to doing quality checklist analysis.

It is common for checklist analysis to consist of a list of codes, standards, regulations, or company safety practices. A complete checklist analysis helps to keep all organizations current with critical safety requirements. Checklist analyses are commonly combined with other types of hazards analyses to better meet the needs of the project.

Table 1 - Sample Checklist Analysis

Item To Check	Action Assigned to	Status (signature & date)
1. Weld Inspection for Tooling a. Certification of Welders b. Ground & polished ($\leq 180\mu$-inch) c. Dye penetrant indication free. d. Full penetration and continuous.	JLP	Closed, 2/12/96
2. Load Test Tooling a. Test at 150% load. b. Stencil w/ rated load (100%), and date.	JLP	Closed, 2/12/96
3. Complete Operating Procedure a. Verify compliance w/ APS 8. b. Circulate for Signatures.	JLP	Closed, 2/12/96
4. Complete Pre-Operational Safety Review	JLP	Closed, 2/14/96
5. Facility Startup	Scheduled for completion, 3/96	Open
6. Inspection & Load Test, Bldg.. Hoist	JLP	Closed, 2/09/96
7. Label Pipe Runs	JLP	Closed, 2/09/96
8. Pressure Vessel Hydrotest	JLP	Closed, 2/14/96
9. Relief Valves a. Verify set at 150 psig. b. Vents connected to condensate return	JLP	Closed, 2/13/96

What-if

The What-if methodology is a relatively unstructured approach that takes advantage of the team brainstorming technique. The team leader assembles information on the process and invites individuals with the appropriate backgrounds in safety, processing, engineering, maintenance etc. to be part of the What-if team. Someone is designated as the scribe to record the results of the session. The team steps through the process, and members are encouraged to verbalize their safety concerns by posing "what if " questions such as "What if the ingredient feed line develops a leak?" or "What if the reaction vessel becomes overheated?" Discussion resulting from each questions is pursued and the consequences/ hazards, safeguards/ design safety and recommendations or other comments recorded. Assignments may be made to follow up on questions that cannot be answered by the group. The team leader may prepare a list of questions beforehand to help continue discussion if the team runs out of questions to ask. The basic rules of brainstorming prevail, that is--no question is considered insignificant and criticism of ideas is not permitted. Someone's supposedly trivial comment may lead someone else to a very important concern. The sessions will have appropriate breaks and will

continue as long as necessary to cover the entire process.

The team leader arranges to transform the notes onto a table format or perhaps the team findings may be formulated in a narrative format. An example of part of a GES What-if table is shown as Table II. This table uses the column headings shown below. Some alternate column headings are shown in parentheses. Sometimes a Resolution column is added that records how issues were resolved or assigned. Software is available to help document the findings, but use of a standard word processing or spread sheet program is sufficient.

What-if table column headings and alternate headings:

- Item No.
- Consequence/ Hazard (Failure/ Hazard, Potential Hazard and Effects)
- Safeguards (Design Safety)
- Recommendation (Comments/ Recommendations)
- (Resolution)

There are a number of advantages of the What-if technique. It is easy to organize and conduct and is relatively unstructured compared to the other methods. Like all brainstorming sessions it promotes the interaction of people with different backgrounds and experiences and tends to bring out and develop ideas that one may not think of alone. Usually the what-if technique will be used with relatively simple processes and if the sessions are well disciplined and don't have too many people involved it is quite cost effective. It can be used during any phase of the process development.

Disadvantages of the what-if methodology are the flip side of its advantages. Since it is relatively unstructured, the PHA team may not have sufficient discipline to reveal some safety issues that may be caught by a more structurally systematic method. This is particularly so if the process is quite complex. Sometimes the brainstorming technique does not lend itself to the depth of thinking that comes from the more detailed or systems oriented methodologies. The depth and quality of the analysis is quite dependant on the people taking part. Good note taking is essential for adequate documentation and follow-up.

What-if/ Checklist

The What-if/ Checklist methodology combines both the What-if and Checklist techniques. Essentially a What-if brainstorming approach is conducted but a Checklist appropriate for the process to be analyzed is used to help generate the what-if questions. This will help to make the analysis more complete but the combination is still limited by being relatively unstructured and is not the systematic approach needed for the more complex processes.

Table II - What-If Summary Table

No	What-If	Consequence/ Hazard	Safeguards	Recommendation
8	Recovery Facility 1			
8-1	Interface failure	Carry-over of light organics	Pump the contents of V-2 back to V-1 using the organics unloading pump (P-4)	
8-2	Vacuum in V-2	Implosion of vessel	Pressure safety valve (PSV 1)	Confirm the existence of a conservation vent for V-2 and identify the set pressures
8-3	Vessel is overfilled with water during hydrostatic test (more water entering the vessel than can be relieved)	Vessel bows or is lifted off of its foundation	Pressure test with air to test for pipe leaks	
8-4	Failure of LI -2 results in a false low level indication in V-2	Both vessels are completely full of liquid and subject to the discharge pressure of the well pumps	Both V-1 and V-2 are equipped with level instrumentation and independent high level switches	
8-5	The contaminated water pump (P-2) fails and the increased level in V-2 goes unnoticed	High level in V-2	V-2 has a 20-minute surge capacity	
8-6	High pressure in the carbon adsorbers	Rupture	No identified safeguards	Calculate the relief scenarios and consider the addition of a pressure relief valve at the carbon adsorbers Consider CSO valves in the vent lines Consider painting CSO/CSC valves
8-7	Personnel exposure to nitrogen in the vapor space of V-1 and V-2	Nitrogen asphyxiation	No identified safeguards	Update P&ID to show nitrogen bubbler tube Place warning signs on V-1 and V-2 for confined space entry and nitrogen hazards
8-8	Pump fails	Unable to remove liquid from vessels	An extra connection is provided for an air-operated diaphragm pump The transfer of liquid is an attended batch operation	
8-9	High level on the water side of V-1	Water in the organics side and eventually (after 10 minutes) to the carbon adsorbers	Level switch (LS -1)	
8-10	Instrument leaks	Release of organic liquid and/or contaminated water	Sealed process-side instrument taps	
8-11	Cannibalization of system components	Removal of critical equipment components resulting in an incident	Magnets are the only cross-utilized component	
8-12	Samples are taken from different locations in the recovery facility	Lack of sample uniformity and consistency	No identified safeguards	Identify approved sample points on the P&ID Remove out-of-date notes on the P&ID
8-13	Thermal expansion of blocked in liquid	Rupture	No identified safeguards	Identify thermal expansion scenarios and address thermal expansion in the SOPs Generate a valve alignment diagram referenced in the SOPs and incorporate a daily morning valve alignment check
8-14	Oxygen enters the system due to vacuum in V-1 or from blowing out the production header with air	LEL	The production header is blown out with air twice per month	Evaluate the LEL of the vapor space in V-1 and V-2 and evaluate the need for a nitrogen blanket

Hazard and Operability Study (HAZOP)

The HAZOP is a structured technique in which a team with varied backgrounds performs a systematic study of a process using guide words to determine how deviations from the design intent can occur in equipment, actions, or materials, and to establish if the consequences of these deviations can result in a hazard. The team's findings include identification of potential hazards and the recommendations for changes in design, procedures, etc. to improve the safety of the system.

The following terms are used in the HAZOP process and in the table documenting the team's findings:

- **Design intent** - the way a process is intended to function
- **Deviation** - a departure from design intent discovered by systematically applying guide words to process parameters
- **Guide Word** - simple words such as "high pressure", "high temperature", "leak" etc. that are used to modify the design intent and to guide and stimulate the brainstorming process for identifying process hazards
- **Cause** - reason why a deviation might occur
- **Consequence** - results of a deviation
- **Safeguard** - engineered systems or administrative controls that prevent the causes or mitigate the consequences of deviations
- **Category** - an assessment of the hazard risk of the operation. GES uses the MIL-STD-882C technique which uses a two character term which expresses the seriousness and the frequency of the undesirable event.
- **Actions (Recommendations)** - recommendations for design changes, procedural changes, or for further study

The HAZOP process requires a well prepared and disciplined leader. He or she prepares the information, documents, and procedures for the team to review and prepares sheets with the process deviations to drive the brainstorming process and to document the findings. The steps taken by the team in the analysis are listed below. (An example of part of a HAZOP table is shown as Table III).

HAZOP Steps:

- Select the operating process section and operating step
- Explain the design purpose of the operating step
- Select a process variable or task (for example liquid flow)
- Apply a guide word to the process variable or task that develops a meaningful deviation (for example "high flow"). A typical list of guide words includes the following:

High flow	Low/no flow	Reverse/ misdirected flow
High level	Low level	
High interface	Low interface	
High pressure	Low pressure	
High temperature	Low temperature	
High concentration	Low concentration	
Tube leak	Tube rupture	
Leak	Rupture	

- List the possible causes of deviation
- Document the consequences associated with the deviation assuming all protection fails
- Identify existing safeguards to prevent deviation
- Assess acceptability of risk based on consequences, causes and protection. (GES uses a Category column and the MIL-STD 882C system to document the assessment of risk.)
- Develop recommendations (actions)
- Repeat the evaluation process for all guide words, process variables/ tasks, sections/ steps, and facility process

As you can imagine the HAZOP process can become quite time consuming if every guide word is applied to every part of the process. Various methods have been used to reduce the time and cost of a HAZOP by eliminating redundancy of guide words and otherwise streamlining the HAZOP procedure. One method, the library-based approach, uses a predetermined list of deviations that apply to various types of components. For example the guide word "high level" will apply to a vessel but not to a pipe line. Other predetermined rules to eliminate redundancy can also be applied.
Another way used in a well-established process is the knowledge-based approach. Knowledge of the process and checklists are used to replace part of the guide words and other questions will be raised to be considered. In other words, a more direct question may be asked based on experience with a component that gets the same result as prompted by use of a guide word. GES uses a form of the library-based approach because we look at different processes for different clients.

The HAZOP has many advantages that make it a very popular methodology. It is particularly useful for chemical or petroleum processes that have interconnected equipment. The list of guide words given above indicates the history with these industries. The evaluation process can occur very quickly if the team is well prepared and disciplined. It can apply to design level as well as existing processes. If done properly the analysis is comprehensive, with every component considered. Some items may be looked at from several approaches. The end products are a well documented table of issues considered, their consequences and defined recommendations. The advantages of a brainstorming approach results in most issues being considered.

There are some disadvantages to the HAZOP approach. If many people are involved it can become expensive if it is not properly disciplined and bounded. The proper mix of personnel on the team is important. Sometimes safety issues are given a backseat to issues related to proper operation if many of the team members are process oriented. Sometimes there is a tendency for team members to overlook some credible abnormal safety issues such as energy coming from sources outside the process. The nature of the team approach and the practice of moving along quickly may limit the time for reflective thinking that may uncover hidden hazards. The HAZOP technique is a single failure analysis and may not address well the situation of multiple component failures leading to an undesirable event.

Table III - HAZOP Summary Table

No.	Item	Deviation	Causes	Consequences	Safeguards	Haz Cat	Recommendations
1	**Organics Storage & Loading**						
1-01	**Organic Liquid Transfer Line from Module**						
1-01.1		High Flow		No significant consequence		NA	
1-01.2		Low/No Flow	Plugged line Closed valve (ball valve at V-1) Pump failure at module Rupture Low level at module	Delayed liquid transfer Increased pressure	Operating history The system is designed for the maximum discharge pressure of the module pump Auxiliary storage	3D	
1-01.3		Reverse Flow	V-1 is completely full Regulator failure (PCV 1)	Upset inventory (increased level at module due to reverse flow through pump)	Check valve at module pump Independent high level switch (LSHH -1) Level transmitter (LT -1) and alarm Pressure relief valve (PSV 2)	4D	
1-01.4		Misdirected Flow	Improper valve alignment (pump to the wrong tank)	Increased level (wrong tank) Contaminated storage (wrong tank)	Valves at the tank are locked out upon reaching the 85% level	4D	
1-01.5		High Pressure	Thermal expansion of blocked in liquid (between check valve at module pump and ball valve at V-1)	Rupture Release of organic liquid	Procedures	3C	Ensure procedures address the appropriate tagging of the ball valve at V-1
1-01.6		Low Pressure	Storage tank is pumped empty	Partial vacuum	Vacuum relief valve (PSV1) CSO valve beneath PSV 1 Nitrogen pad Pipe is rated for full vacuum	4D	
1-01.7		High Temperature	Radiant heat Fire Restricted pump discharge	Material failure	There are no other flammable materials stored in the area Fire monitor RTD shuts down the pump on high temperature (system is rated for RTD shutdown temperature)	4D	
1-01.8		Low Temperature		No significant consequences		NA	

Failure Modes and Effects Analysis (FMEA)

The FMEA identifies failure modes of equipment or operations in the process that could directly result in or significantly contribute to an accident. An FMEA uses *inductive* reasoning in which specific cases lead to a general conclusion. The failure modes and root causes may be identified by an analyst working alone or as the result of a team effort. In some cases failure modes may come from another methodology such as a fault tree or logic diagram. The FMEA can be used for a DHA as well as an OHA.

The FMEA example in Table IV illustrates how the FMEA is organized. Typically, the items addressed follow the process flow. Hazards identified with each major process equipment item or system are grouped together. One or more failure modes for each item are identified. The causes of each failure mode are developed; these causes can be either actual or potential, and can result from normal or abnormal operation, equipment failure, or human error. Next the analysis determines the potential effect of each failure cause if the hazard is not corrected; the effects may apply to the item being analyzed or to operations elsewhere in the process. Existing elements of design safety are listed that would either mitigate the proposed failure consequences or make it unlikely to occur. A qualitative risk assessment is usually made, GES uses the alpha-numeric method of MIL-STD 882C which indicates the level of severity of consequences and the level of frequency of the hazard. Finally, actions are recommended to lessen or mitigate the hazard. Recommendations may include equipment modifications, additional or modified procedures, process controls and interlocks, the use of protective equipment, or other methods of risk control.

Many of the advantages of the FMEA technique are a result of its detailed, system safety approach. It is well suited for many facility process uses. The FMEA worksheet is usually developed by one or two analysts with the other team members serving in a resource and review function. For this reason it does not tie up a lot of key people on the plant at one time and can be very cost effective. The analyst is forced to examine the process in a detailed manner and to understand it very well. This is done by studying the drawings and talking to the design engineers in the case of the DHA and by visiting the process, studying the procedures and talking to the operators in the case of an OHA. The analyst has the time to ponder the issues brought up in the analysis and is able to do more complete research than often done in a HAZOP or other brainstorming type approach. If desired, a more active team brainstorming approach can be used for part or all of the analysis. The FMEA table provides a detailed record of the analysis and sources of the recommendations that are developed from it.

The FMEA usually does not have the full advantages of the brainstorming interaction; however that aspect can be incorporated. The background and ability of the analyst is very important. If the analyst is not knowledgeable of the process or is not given the appropriate information the analysis may not be complete. On the other hand, if the potential problems in the process are of a special nature such as one would find in a highly hazardous or explosive process, outside help by specially trained analysts may be a very wise choice.

Table IV
Failure Modes and Effects Analysis for the GNU PROCESS

LINE NO.	ITEM	FAILURE MODE	FAILURE CAUSE	POTENTIAL EFFECTS	DESIGN SAFETY	HAZ CAT	RECOMMENDATIONS
1A	Lee Ball Valve	Friction initiation during valve operation.	Stainless steel/mica-filled Teflon friction between ball and intake or discharge seals.	Propagation of reaction to reactor or receiver vessels.	Friction pressure limited by the yield properties of the mica-filled Teflon seals; Initiation unlikely. Friction velocity low. Testing indicates that propagation unlikely.	2D	None.
1B			Stainless steel/mica-filled Teflon friction between stem and stem seals.	Propagation of reaction to process vessels.	Friction pressure limited by the yield properties of the mica-filled Teflon seals; Initiation unlikely. Friction velocity low. Testing indicates that propagation unlikely.	2D	None.
1C		Propellant solution out of place due to valve position.	Improper fail-safe conditions if air failure.	Increased risk to personnel and equipment. Increased cost for cleanup and safety management issues.	System will be designed to have valve fail safe in desirable position to maximize safety.	3D	Verify that the fail safe condition of the ball valve between the reactor and receiver functions as intended to avoid propellant solution out of place when air pressure is lost. SAR 28-001.
1D			Operator or control system failure.	Increased risk to personnel and equipment. Increased cost for cleanup and safety management issues.	Safeguards to be incorporated in system and procedure to avoid problem.	3D	Verify that interlocks and safeguards are present in control system and procedure to ensure that ball valve between the reactor and receiver cannot be inadvertently put in wrong position. SAR 28-002
1E		Leak at valve connection	Improper assembly/installation or component failure due to attack by chemical A or propellant ingredients.	Increased risk to personnel and equipment. Increased cost for cleanup and safety management issues.	Materials compatible with Chemical A and propellant ingredients specified and tested if in question. Pressure testing prior to process runs to check for leaks and other problems.	3C	None.
1F		Initiation of material trapped in ball valve cavity after valve closed.	Material trapped in valve becomes heated resulting in pressure buildup and reaction.	Damage to valve with possible propagation to system.	It is planned to drain liquid from cavity by means of a small hole drilled in the ball or by other valve design means.	3C	Verify that cavity draining of the ball valve is adequate to avoid trapping of material in ball cavity after ball valve is closed. SAR 28-003
			Friction initiation during disassembly.		Significant contamination unlikely. Personnel will be trained and procedures will indicate caution and techniques for disassembly of potentially contaminated equipment	3E	Ensure that appropriate disassembly techniques for potentially contaminated ball valve fittings and components are covered in training and procedures. SAR 28-004
1H			Friction in contaminated fittings during removal of valve from associated equipment.	Risk to person working on valve.	Significant contamination unlikely. Personnel will be trained and procedures will indicate caution and techniques for disassembly of potentially contaminated equipment.	3E	Ensure that appropriate disassembly techniques for potentially contaminated ball valve fittings and components are covered in training and procedures. SAR 28-004
1I		Initiation from water-hammer type shock in system from valve operation.	Shock transmitted through liquid in system to sensitive mixture at other location.	Equipment and facility damage.	Solutions in process expected to be dilute and insensitive enough to make initiation unlikely.	3E	Compare calculated water hammer type shock conditions in pilot plant process with solution/mixture sensitivity to shock. SAR 28-005
1J		ESD initiation during valve operation.	ESD initiation from flow through valve.	Equipment and facility damage.	charging is unlikely due to conductivity of solutions and grounding conditions. Conductivity of Chemical A is in range of 10^{-8} Ohm^{-1} cm^{-1} which is considered quite conductive. Ingredients such as AP, NG and BTTN should add to conductivity.	3E	None.
1K			ESD initiation from valve actuation.	Equipment and facility damage.	Charging unlikely due to presence of conductive solutions and limited movement and velocity of valve components.	3E	None.
1L		Incompatibility reaction in valve.	Incompatibility of Chemical A/propellant solution with valve seals, packing etc. causing reaction of the propellant ingredients.	Ignition of Chemical A/propellant mixture causing equipment and facility damage.	All materials tested or verified for compatibility with materials in process. Materials controlled to prevent inadvertent use of incompatible materials.	3C	None.
1M			Incompatibility of Chemical A/propellant solution with actuator lubricant causing reaction of the propellant ingredients.	Ignition of Chemical A/propellant mixture causing equipment and facility damage.	Where necessary, Specifications for equipment require use of lubricants and materials that are compatible with AP and propellant ingredients. Material testing conducted as needed. Lubricant in actuator unlikely to reach Chemical A/propellant solution because of valve design.	3C	Check likelihood of lubricant and Chemical A/propellant solution contact. If contact possible, specify compatible lubricant in actuator or verify compatibility of normal lubricant. SAR 28-006
1N			Incompatibility of the valve materials with Chemical A causing degradation of the valve components resulting in improper operation or leaking.	Operations affected and increased risk to personnel.	Materials selected to be compatible with Chemical A. Policy is that any problems resulting in safety concerns will be corrected.	3D	None.

Fault Tree Analysis

Fault tree analysis is an analytical process where a top undesirable event is specified and a formal logic process is used to find all the credible ways by which the undesirable event can occur. The fault tree is the graphical representation of the combination of faults such as component failures, human errors and other events that lead to the top event. The analysis is a *deductive* process in that a top event such as a fire, chemical release or leak, system malfunction or personnel injury is assumed and the minimum, immediate, necessary and sufficient causes for this event is determined. Then the causes for those events are determined and so on until the basic component faults or failures are found, further information is not available, or the decision is made to not proceed any further. Logic symbols such as "And" and "Or" gates are used to show relationship of parallel and sequential events. The symbols used in fault tree analysis are defined in Figure 5. Fault tree software is available to both draw the tree and to quantitatively assess it to determine "Cut Sets" or the fundamental paths leading to the top event or to also calculate the probability of events if sufficient input failure information is available.

Fault tree analysis is most useful for complicated, interactive systems where the top event can result from several paths. Specific training is necessary to perform the analysis correctly and the process can be quite time consuming and expensive if applied overall to a large process. Excessive time and expense can be avoided by only using the technique with critical sections and components of a process requiring that analysis level. It is best done with a team effort to make sure all events are considered. Sometimes it is best for the work to be contracted out if the need for a fault tree analysis is determined. For a very complicated mechanical and/or electrical system it is one of the best ways to ensure that most hazards and combination of events leading to hazards are addressed. The process will not be discussed in detail here, but a small section of a fault tree is shown in figure 6 to give a feel of how it may be used to assess part of a process that may be more complicated than the rest of the system.

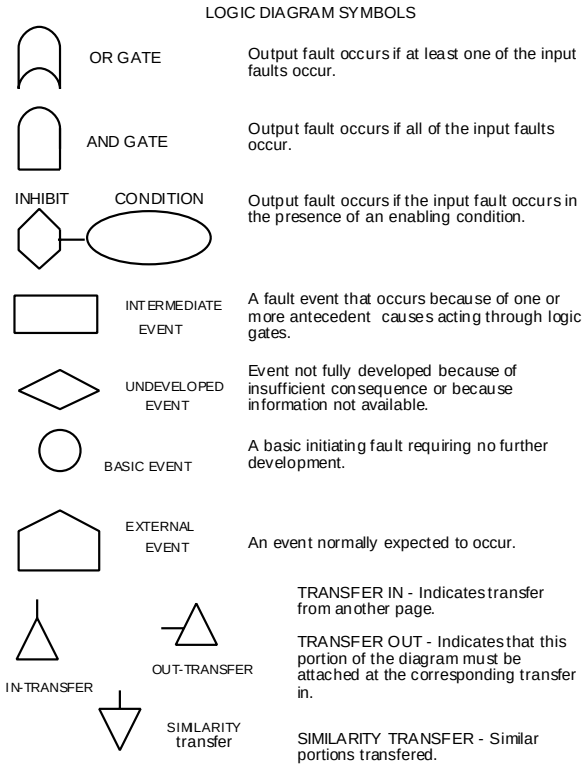


Figure 5. Fault Tree Symbols

Figure 6. Fault tree example showing documentation of the deductive thinking process

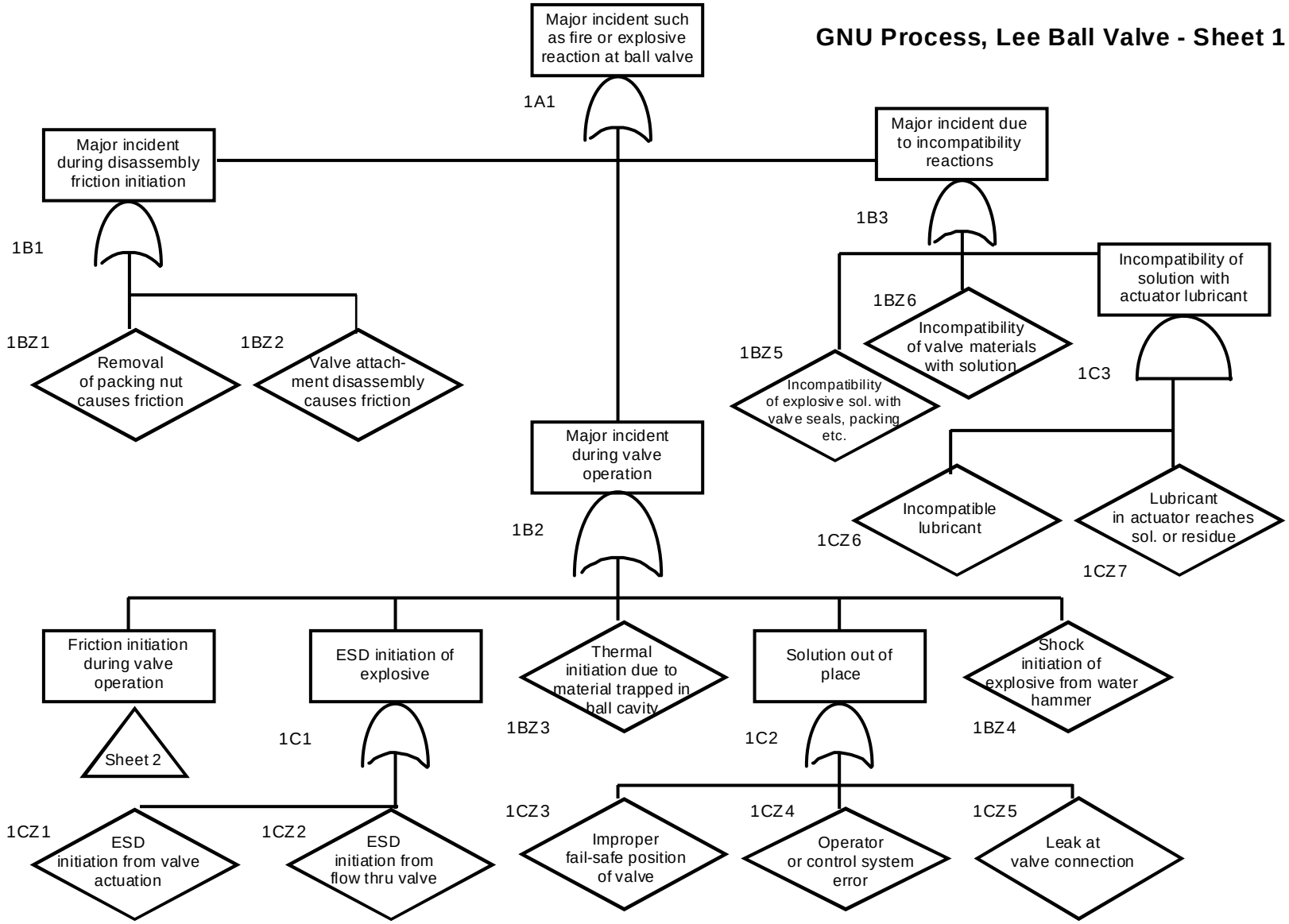
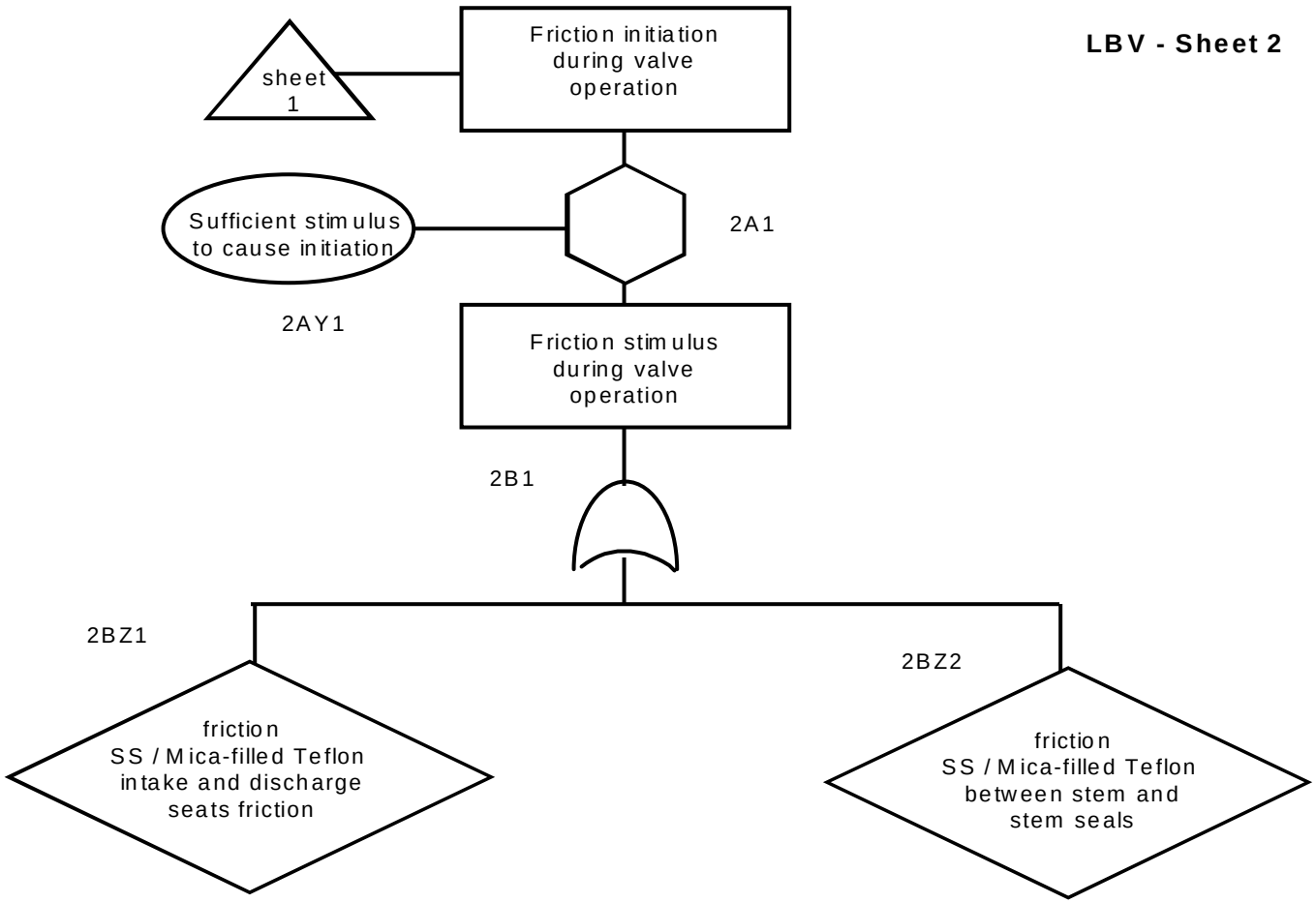


Figure 6. Fault tree example showing documentation of the deductive thinking process



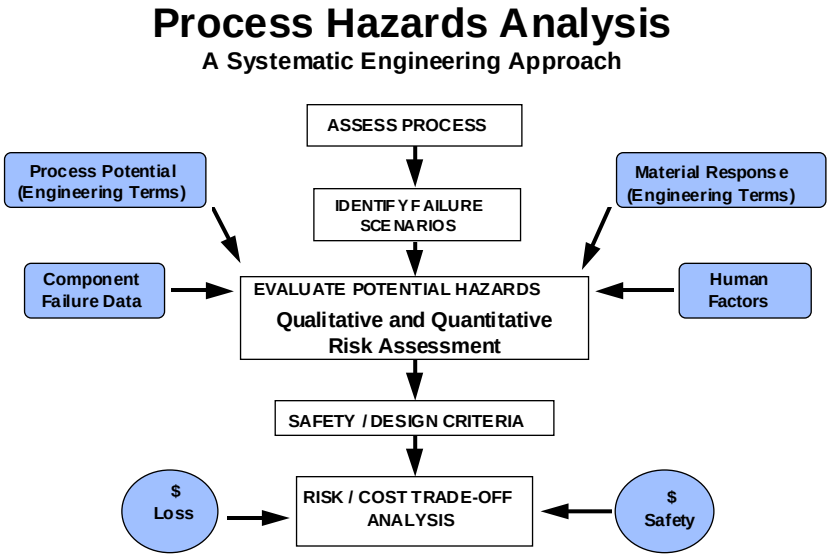
Using a Combination Logic Diagram and FMEA or HAZOP and a Systematic Engineering Approach

GES uses a combination of the fault tree and the FMEA or HAZOP methodologies along with selective quantitative engineering analysis for many of the PHAs we perform for our clients. This approach uses high-level fault trees or "logic diagrams" as a *deductive* approach to identify potential hazards in the process. These scenarios are then used as a starting point for the *inductive* FMEA or HAZOP analysis that is performed to develop failures, effects, design safety and recommendations in more detail. A team is established as mentioned above in the FMEA discussion with issuing of SARs to assign and track recommendations. A report is issued which includes the logic diagram and the FMEA or HAZOP table to provide the documentation of the thought process and analysis detail.

The GES Systematic Engineering Approach is outlined in Figure 7. This shows the sequence in an analysis where energy in a process and reactive process materials can be evaluated and compared using engineering testing and analysis techniques to help in making decisions about the process. For example, the data obtained from sensitivity testing such as impact, friction, electrostatic discharge, thermal property testing, etc. can be used for comparison against the calculated or measured energy, pressure, temperature etc. in the process. From this comparison, a safety factor or probability of initiation can be obtained. Combined with component failure rates, human error probabilities and other process event probabilities, a probability of a major event can be determined. Such data can be used to decide if the process meets the safety criteria of the facility. It can also be used in a risk/ cost trade-off analysis to compare the cost of safety with the potential cost of an accident to help management make decisions related to safety programs.

Excerpts from a GES PHA analysis using the logic diagram and FMEA approach were previously shown in Figure 6 and Table IV as fault tree and FMEA examples. It can be seen how the techniques we have discussed can be combined to tailor a PHA to best suit a given situation. There is no reason why the same methodology or the same depth of analysis needs to be continued throughout a whole facility or even within a single process. The method or methods best suited to the specific situation and the available resources of the company should be used.

Figure 7. The GES Systematic Engineering Approach for PHA



SELECTING THE RIGHT PHA METHOD

A successful hazards analysis must have the following elements:

- Management support
- Trained hazards analysts
- Quality information about the process
- The hazards analysis technique or combination of techniques that is appropriate for the complexity of the process.

Fortunately, safety professionals now have a wide variety of hazards analysis tools or techniques to choose from. Selecting the proper tool may require some thought, but is relatively straight forward. Don't let over-concern for cost, schedule and resources or lack of expertise mislead you to select the wrong technique. Let the complexity of the analysis reflect the complexity of the process.

The "best" hazards analysis may consist of a combination of individual techniques. A good example of this is completing a FMEA, sorting the resulting failure scenarios using hazard categories, then performing fault tree analysis on the worst scenarios.

The main objective of the hazards analysis report is to document the findings and to communicate the safety recommendations to the decision makers. Management must be able to read and understand the finished product. Then the best risk/ cost trade-off decisions can be made between the cost of safety and the potential costs due to accidents.

The size and complexity of the hazards analysis is not directly proportional to quality. Certainly, large chemical plants will need a large hazards analyses effort, but the size of each report should be as small as possible without sacrificing completeness. The key to doing hazards analysis for a large chemical plant is to divide the project into smaller manageable pieces. Care must be taken in doing this to ensure that process overlap and equipment interaction is handled properly so gaps do not occur in the analysis. Use of a Logic Diagram for the overall process in combination with the other methods used for the smaller analysis sections is one way to help maintain an overall perspective.

It is hoped that this brief summary of the elements of a good process hazards analysis program and review of the PHA method choices available will help you in your ongoing efforts to manage an appropriate, cost-effective safety program.

BIBLIOGRAPHY

1. Process Safety Management of Highly Hazardous Chemicals, 29 CFR 1910.119, U.S. Department of Labor, Occupational Safety and Health Administration.

2. Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples, Center for Chemical Process Safety of the American Institute of Chemical Engineers, 345 East 47th Street, New York, NY 10017.

3. Fault Tree Handbook, NUREG-0492, Systems and Reliability Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555.

4. Handbook of System and Product Safety, W. Hammer, 1972, Prentice Hall, Inc. Englewood Cliffs, N.J. 07632.

5. GES PSM Compliance Audit Guidelines, D. Hall, Global Environmental Solutions, Inc., 4100 South 8400 West, Annex 16, Magna, UT 84044.

6. Process Safety Management FMECA Training Course, L. Losee and K. Hendrickson, Global Environmental Solutions, Inc., 4100 South 8400 West, Annex 16, Magna, UT 84044.