Domino Effect Analysis and Assessment of Industrial Sites: A Review of Methodologies and Software Tools

2.1 "What-If" Analysis

INTRODUCTION

The "What-if" analysis is the simplest technique used to identify hazards.

It is based on the question

"What will happen if...",

an essential component of a process or plant does not operate according to its design.

This method may be applied to all components comprising a process or plant, even including the procedures governing its operation, depending on the analysis requirements.

Identifying Hazards
procedure
What-if Analysis
HAZOP Analysis
FMEA Analysis
Qualitative Evaluation Techniques

It is a brainstorming approach according to which a group of experienced people familiar with the subject ask questions or voice concerns about possible undesired events. Although it is not as inherently structured as HAZOP or FMEA analyses, it encourages the team to think of questions that begin with "What if...".

Assembling an experienced, knowledgeable team is probably the single most important element in conducting a successful "What-if" analysis. Individuals experienced in the design, operation, and servicing of similar equipment or facilities are essential. Their knowledge of design standards, regulatory codes, past and potential operational errors, as well as maintenance difficulties, brings a practical reality to the review. Team members may include Process or Laboratory Manager, and representatives with specific skills as needed (from maintenance, compressed gas, manufacturing, etc.).

The next most important step is gathering the needed information. The operation or process must be understood by the review team. One important way to gather information on an existing process or piece of equipment is for each team member to visit and walk through the operation site. Additionally, piping and instrument diagrams, design documents, operational procedures, and maintenance procedures are essential information for the review team.

If these documents are not available, the first recommendation for the review team becomes clear: *Develop the supporting documentation!* Effective reviews cannot be conducted without up-to-date and reliable documentation. An experienced team can provide an overview analysis, but the nuances of specific issues such as interlocks, pressure relief valves, or code requirements are not likely to be found without documentation.

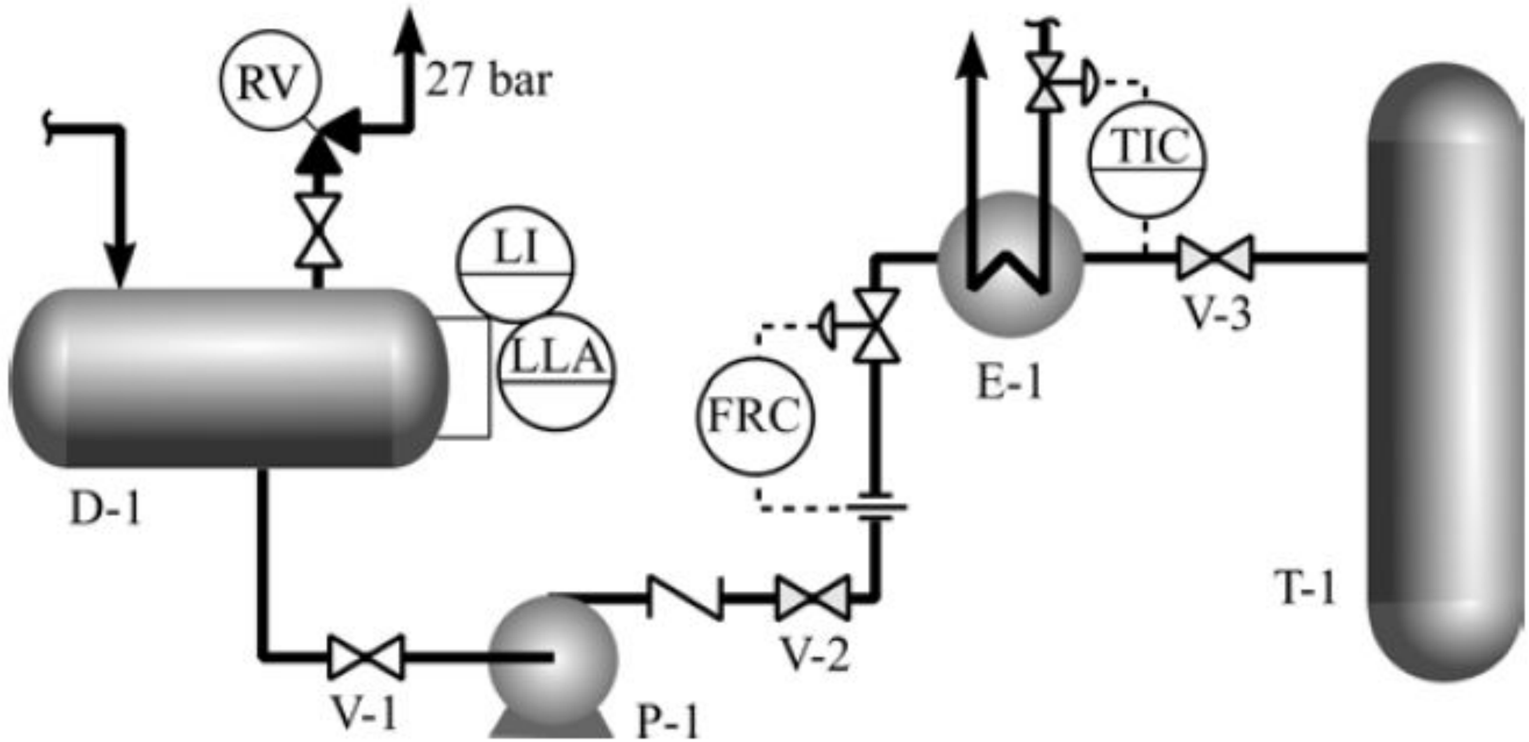
If these documents are not available, the first recommendation for the review team becomes clear: Develop the supporting documentation! Effective reviews cannot be conducted without up-to-date and reliable documentation. An experienced team can provide an overview analysis, but the nuances of specific issues such as interlocks, pressure relief valves, or code requirements are not likely to be found without documentation.

The great advantage of the "What-if" analysis is its flexibility. In essence it can be applied in any stage of a process or plant using any available information in connection with the available knowledge. The disadvantage of the technique is that it requires personnel with detailed knowledge of the process or plant, who will also be able to conceive and predict deviations from normal operation.

EXAMPLE A 2.1.

A simplified flow diagram for the feed line of a propane-butane separation column system is shown in Figure A2.1. The mixture enters the vessel D-1 at 75°C and 22 bar. The mixture is pumped from the bottom of the vessel to the separation column T-1, by the P-1 pump. An FRC valve controls the flow rate. The mixture is pre-heated to 85°C using steam at the heat exchanger E-1. Perform the What-if analysis (only for the flow parameter).

Figure A2.1. Feed line of a propane-butane separation column system.



Symbol Interpretation

RV : Relief Valve
LI : Level Indicator
LLA : Low Level Alarm
FRC : Flow Recorder Controller
TIC : Temperature Indicator Controller

According to the aforementioned discussion, the analysis, the consequences and the recommendations for this particular example are shown in Table A2.1.

In the following section, the same example will be examined with the HAZOP analysis, so that the advantages and disadvantages of each technique will become apparent.

Table A 2.1. "What-if" Analysis.

Question "What-if"	Consequences	Recommendations
… the operator accidentally closes the valve V-1?	• Liquid level rises in D-1 vessel. • Operational upset of the T-1 column due to feed interruption.	• There is a level indicator LI. In case LI fails, the relief valve RV will open.
… the pump P-1 shuts down?	As above	
… the flow control valve FRC is leaking?	• Risk of generating a flammable mixture, and potential fire.	• More frequent valve maintenance. • Consider installation of double-seal systems.
… there is a fire close to the vessel D-1?	• Temperature and pressure increase in the vessel. Possible boiling of the contents.	• Check the capacity of the relief valve to vent the generated vapors. • Install a pressure indicator, PI, on the vessel, along with a high-pressure alarm signal PHA in the control room.
… a crack appears on the tubes of E-1 due to corrosion?	• Hydrocarbon carry-over to the steam network - a hazardous source in other uses of the steam.	• Consider replacing the steam with another heating fluid.

2.2. Hazard and Operability Analysis (HAZOP)

The HAzard and OPerability study, HAZOP was originally developed by engineers in ICI Chemicals, UK, during the middle of 1970. It is one of the most structured techniques to identify hazards in a process plant, and aims to find all possible deviations from the normal function of process parameters. A list of "key- words," Table A2.2, is used to define the deviations.

The HAZOP analysis can be applied to all processes. It is based upon the assumption that any operating problem arising in equipment will be the cause of, or have as a consequence, the deviation from the normal operation of a parameter of one of the lines connected to the equipment concerned.

The primary purpose of the HAZOP analysis is the identification of possible hazard scenarios. The team must not waste time in finding solutions. If the solution is obvious, the team recommends it, otherwise it is referred to the corresponding engineering team. The HAZOP study should preferably be carried out as early in the design phase as possible in order to have influence on the design.

On the other hand, to carry out a HAZOP we need a rather complete design. As a compromise, it is usually carried out as a final check when the detailed design has been completed. A HAZOP study may also be conducted on an existing facility to identify modifications that should be implemented to reduce risk and operability problems.

HAZOP studies may also be used more extensively, including:

- ❖ At the initial concept stage when design drawings are available.
- ❖ When the final piping and instrumentation diagrams (P&ID) are available.
- ❖ During construction and installation to ensure that recommendations are implemented.
- ❖ During commissioning.
- ❖ During operation to ensure that plant emergency and operating procedures are regularly reviewed and updated as required.

In recent years HAZOP analysis has been widely accepted as the most preferred technique for hazard identification.

Table A 2.2. Keywords.

Keywords	Deviations from normal operation
NO	Complete negation
LESS	Quantitative decrease
MORE	Quantitative increase
PART OF	Qualitative decrease
AS WELL AS	Qualitative increase
REVERSE	Logical opposite
OTHER THAN	Complete substitution

EXAMPLE A 2.1.

This simplified flow diagram in Figure A2.2 shows the mixing of phosphoric acid and ammonia to produce diammonium phosphate, which is not toxic. Perform the HAZOP analysis in Table A2.3 (only for the flow parameter.)

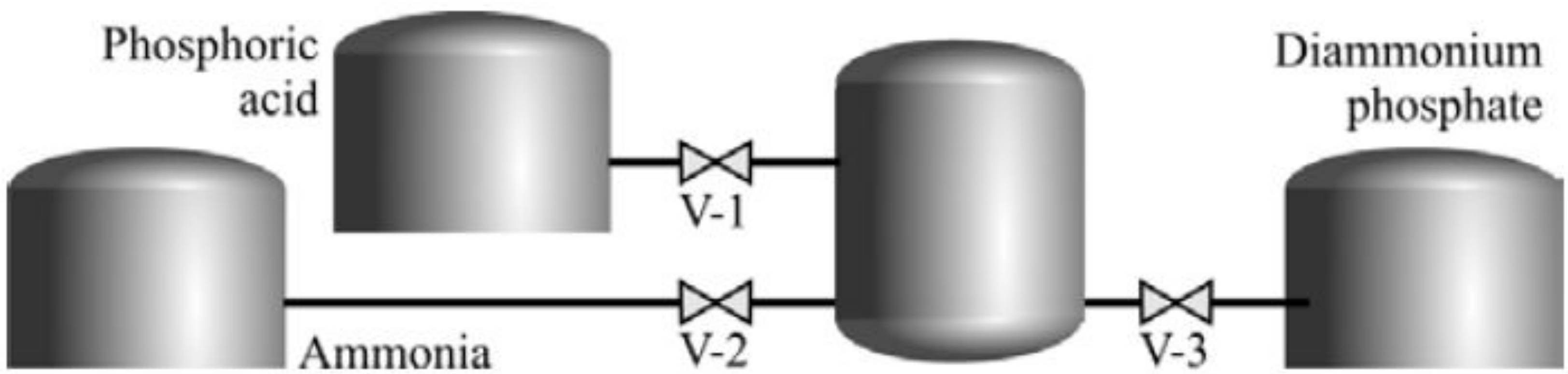


Figure A2.2. Mixing of phosphoric acid and ammonia.

Identifying Hazards procedure

What-if Analysis

HAZOP Analysis

FMEA Analysis

Qualitative Evaluation Techniques

Table A2.3. HAZOP Analysis.

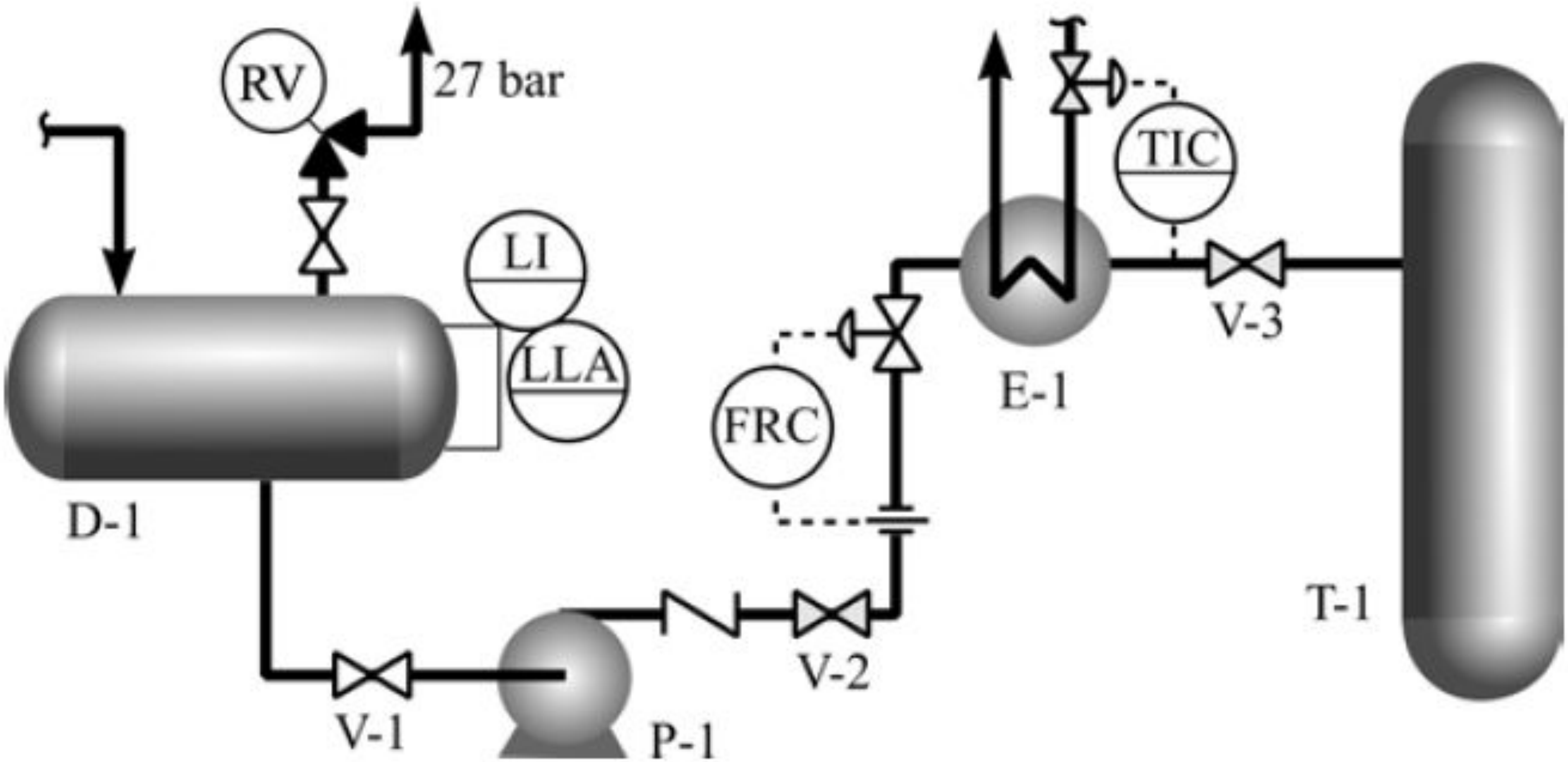
Key- word	Deviation	Possible cause	Consequence	Necessary corrective action
NO	No Flow	•Valve V-1 closes. •Phosphoric acid supply exhausted. •Plug in pipe or pipe rupture.	Excess ammonia in reactor. Release to work area.	Automatic closure of valve V-2 on loss of flow from phosphoric acid supply.
LESS	Less flow	Valve V-1 partially closed. Partial plug or leak in pipe.	Excess ammonia in reactor. Release to work area, with amount released related to quantitative reduction in supply.	Automatic closure of valve V-2 on reduced flow from phosphoric acid supply.
MORE	More flow		Excess phosphoric acid degrades product.	No hazard to work area.
PART OF	Partial flow	Delivery of wrong material or wrong concentration. Incorrect filling of vessel.	Excess ammonia in reactor. Release to work area with amount released related to supply reduction.	Check phosphoric acid supply tank concentration after charging.
AS WELL AS	Flow		*Not applicable*	
REVERSE	Flow		*Not applicable*	
OTHER THAN	Other flow	Delivery of wrong material.	Depends on flow.	Properly check material before filling.

EXAMPLE A 2.3.

A simplified flow diagram for the feed line of a propane-butane separation column system is shown in Figure A2.3. The mixture enters the vessel D-1 at 75°C and 22 bar. The mixture is pumped from the bottom of the vessel to the separation column T-1, by the P-1 pump. An FRC valve controls the flow rate. The mixture is pre-heated at 85°C using steam at the heat exchanger E-1. Perform the HAZOP analysis (only for the flow parameter).

EXAMPLE A 2.3.

Figure A 2.3. Feed line of a propane-butane separation column system.



Symbol Interpretation

RV : Relief Valve
LI : Level Indicator
LLA : Low Level Alarm
FRC : Flow Recorder Controller
TIC : Temperature Indicator Controller

The analysis, consequences and recommendations for this particular example are shown in Table A2.4. In the previous section, the same example was examined with the "What-if" analysis, so that the advantages and disadvantages of each technique become apparent.

Table A 2.4. HAZOP Analysis.

Guide Word	Deviation	Possible cause	Consequence	Necessary corrective action
NO	No Flow	Loss of suction of the P-1 pump, due to the low liquid level in the D-1 vessel.	a) Pump overheating that may result in leak from the mechanical seal, and possible fire. b) Operational upset in Operational upset in column T-1.	1) A low-level alarm, LLA already exists on the D-1 vessel. 2) Place a low flow alarm LFA on the recorder FRC.
		The P-1 pump stops (due to failure or power loss).	c) Liquid level rise in the D-1 vessel. d) As (b) above.	3) There is a safety valve, RV. It is recommended to place a high level alarm, HLA on D-1
		There is a major leak due to damages to the mechanical seal of the P-1 pump.	e) Increased likelihood of fire. f) As (b) above.	4) More frequent maintenance. 5) Investigate the cause of damage to the mechanical seal. 6) Install a double-seal system.
		The V-1 valve in the suction line is accidentally closed by an operator.	As (a) and (b) above.	7) Point out the error in the operating procedures.

Table A 2.4. (cont.) HAZOP Analysis.

Guide Word	Deviation	Possible cause	Consequence	Necessary corrective action
NO	No Flow	The FRC valve is closed due to failure (human error, power or instrument-air loss, etc.).	g) As (a) and (b). Furthermore, pressure is rising in the discharge line (until the valve) up to the shut- off pressure of P-1.	8) As (2) above. Furthermore, check if the shut-off pressure of P-1 exceeds the design pressure of the discharge line. 9) Consider modification of the FCV valve so as to remain open in case of power or instrument air losses.
		The V-2 valve, in the discharge line of P-1, is closed due to human error.	As (g) above.	10) As (2) above. Furthermore, consider installing a recirculation line from the discharge line of P-1 to the vessel D-1.

Table A 2.4. (cont.) HAZOP Analysis.

Guide Word	Deviation	Possible cause	Consequence	Necessary corrective action
NO	No Flow	V-3 valve is closed.	As (g) above.	11) As (2) above. Furthermore, check if a problem on the shell and tubes of E-1 is expected as the pressure rises up to the shut-off pressure of P-1.
		Mechanical pipe failure and cracking (due to external cause, corrosion, etc.).	h) Significant release of hydrocarbons to the air. Risk of fire or explosion.	
MORE	More flow	Malfunction of the FRC valve.	i) Operational upset in T-1. j) Level decrease in D-1.	12) Preventive actions (more frequent inspection - regulation). As (1) above.

Identifying Hazards
procedure
What-if Analysis
HAZOP Analysis
FMEA Analysis
Qualitative Evaluation Techniques

Table A 2.4. HAZOP Analysis.

Guide Word	Deviation	Possible cause	Consequence	Necessary corrective action
LESS	Less Flow	Malfunction of the FRC valve.	As (i) above. k) Level rise in D-1.	As (12) above. As (3) above.
		Minor leak (from the FRC valve, or the P-1, or flanges).	l) Hydrocarbon release in the air. Risk of fire.	13) More frequent preventive actions. 14) Investigate the causes of damage of the existing seal. 15) Consider installing double-seal systems on the valve and pump, or replacing them with up-to-date equipment. 16) Minimize the use of flanges where possible.
		Leaking tubes on the E-1 heat exchanger (from cracks due to corrosion).	m) Hydrocarbon carry-over to the steam network - a hazardous source in the other potential use of the steam.	17) Consider replacing the steam with other heating fluid.

2.3. Failure Modes and Effects Analysis (FMEA)

The Failure Modes and Effects Analysis, FMEA, evaluates the ways in which equipment can fail and the effect these failures can have on an installation. These failure descriptions provide analysts with a basis for determining where changes can be made to improve a system design. Single equipment failures are defined by the analysts and the effects of such failures, both locally and on the system as a whole, are investigated. Each individual failure is considered as an independent occurrence with no relation to other failures in the system, except for the subsequent effects which it might produce.

The FMEA analysis is usually applied to systems, subsystems, components, procedures, interfaces etc. The technique is most suited to installations where the danger comes from mechanical equipment and electrical failures, but not from the dynamics of the processes. This is in contrast to the HAZOP technique which is applied to whole processes, whereby the danger comes from hazardous materials in chemical process systems.

Identifying Hazards
procedure

What-if Analysis

HAZOP Analysis

FMEA Analysis

Qualitative Evaluation Techniques

In order to determine and define priorities, usually the following three criteria are employed:

- **S** — Severity of the consequences.
- **P** — Probability of occurrence of the event over a period of one year.
- **b** — Difficulty in identifying the particular event.

These three criteria define the Risk Priority Number, RPN, as

RSN = S x P x b

Teams determine the minimum RPN values, as a measure of comparison for further analysis and investigation.

The principles of an FMEA analysis are easy to understand and to learn. It is, however, more important that the analysts are familiar with the components of the system to be analyzed. They must know the failure modes of the components and the effects of those failure modes on the system as a whole. Thus, although the technique is not difficult to apply, it is enormously time-consuming. Although only failure modes (e.g., component faults) are explored, both types of failure modes (those which will, and those which will not result in great harm) must be investigated to fully develop the analysis.

2.4. Overview of Qualitative Evaluation Techniques

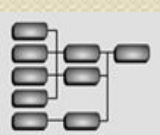
Qualitative evaluation techniques are normally applied to identify any potential hazard as a consequence of the operation of a facility. For the existing technology and an experienced evaluation team, a simple qualitative evaluation technique may be sufficient to identify any conceivable hazard. For new technology applications of limited past experience, the hazard evaluation team may brainstorm using techniques like "What-if" analysis. Once a design progresses into the pre- engineering phase, a more detailed technique like HAZOP or FMEA is certainly preferable for hazard identification and evaluation [TNO 2005, Clemens 1982].

2.4.1 Safety Review

The Safety Review, also known as Process Safety Review, or Design Safety Review, can be employed at any stage during the life cycle of the plant. It can typically comprise anything from a simple walk-through visual inspection (completed in a day or less) up to a formal examination by a specialized team that can take several weeks. In the case of plants still in the stage of design, the Safety Review can consist of an inspection of documents and drawings.

Safety Reviews intend to identify those operating procedures or plant conditions that could lead to injuries, significant property damage or environmental impacts. A typical Safety Review includes interviews with many people in the plant: operators, engineers, maintenance personnel and others. It should be regarded as a cooperative effort, aiming to improve the overall safety and performance of the plant.

The Safety Review Team must have a lot of experience in applying safety standards and procedures, but also expertise in the evaluation of facilities, electrical systems, pressure vessel inspections and materials characteristics. The plant personnel should be ready to fully cooperate with the team.



2.4.2 Checklist Analysis

Checklist Analysis uses a written list of objects or procedural steps that must be checked so that the status of a system/facility is verified. The written list includes possible failures and causes of hazardous events. It is based on the personnel experience and it is most useful to identify customarily recognized hazards.

As a minimum, a Checklist Analysis can be employed to ensure that the design is in accordance with standard practices. The Checklist Analysis depends directly upon the experience of those personnel involved in its composition, and it is very simple in its application.

2.4.3 Preliminary Hazard Analysis

Preliminary Hazard Analysis refers to the effort to identify possible hazards from a very initial stage, preferably at the design stage of the plant or the facility. The technique can be employed in all systems, subsystems, components, procedures, etc., and aims at the identification of possible hazards.

The Preliminary Hazard Analysis is not a discrete technique, but it depends on the expert team, who will apply it based upon its experience. It can incorporate any other technique of hazard identification, as long as it is applied at the design stage of the plant or facility.

2.4.4 Criticality Analysis

Criticality Analysis ranks the damage potential of system elements according to a scale which represents the harm each element might cause in case of failure. The purpose of the analysis is to rank the criticality of components through unconnected failures, according to

a) their effects (injury, damage, or system degradation, etc.).

b) the probability for this particular failure to occur.

Identifying Hazards
procedure
What-if Analysis
HAZOP Analysis
FMEA Analysis
Qualitative Evaluation Techniques

2.4.5 Change Analysis

Change Analysis is based upon the examination of possible changes of a system/plant/facility. The original system is taken as a base, and on this, possible changes, by themselves or in cooperation with others, are considered as well as the effects they could cause. Usually another hazard identification technique is considered as a base, and on it new possible changes and their effects are examined.

In this case, the full understanding of the physical principles governing the behavior of the system being changed is essential, so that the effects of the change can be determined with an adequate degree of confidence for the analysis.

2.4.6 Critical Incident Technique

The Critical Incident Technique is based upon the critical evaluation of previous mistakes, failures, hazards and near misses. It identifies dominant high-risk cases. The technique requires interviews and/or distribution of questionnaires to all personnel and uses the collective accumulated experiences. In recent years, there is a tendency to substitute the "What-if" analysis for this technique (Section A2.1).

2.4.7 Energy Analysis

Energy Analysis refers to the identification of all energy sources within a system, and the examination of the adequacy of barriers to the unwanted flow of that energy to "targets" which might suffer harm. The technique is usually applied to all systems that store, use or incorporate any form of energy.

2.4.8 Worst-Case Analysis

Worst-Case Analysis technique examines all possible failures that could occur and focus on the worst case of all of them. It subsequently investigates all possible causes that could lead to this worst case.

Identifying Hazards
procedure

What-if Analysis

HAZOP Analysis

FMEA Analysis

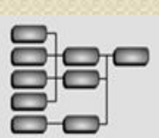
Qualitative Evaluation Techniques

2.4.9 Network Logic Analysis

Network Logic Analysis describes the system operation as a network of logic elements, and develops Boolean expressions for proper system functions. Following this, it analyses the network and/or expressions to identify elements of system vulnerability to mishap.

2.4.10 Scenario Analysis

Scenario Analysis is based upon the examination of possible scenarios proposed by personnel with a great deal of experience in the operation of the plant or facility.



2.4.10 Systematic Inspection

Systematic Inspection uses checklists, codes, regulations, industrial standards and guidelines, prior mishap experiences, and common sense to methodically examine a design/system/process and identify discrepancies representing hazards.

Thank you for your attention!