MAJOR HAZARDS ANALYSIS
- AN IMPROVED PROCESS HAZARD ANALYSIS METHOD

by Paul Baybutt
Primatech Inc., 50 Northwoods Blvd., Columbus, OH 43235
paulb@primatech.com

A version of this paper appeared in Process Safety Progress, Vol. 22, No. 1, pps. 21 - 26, March, 2003.

Abstract

Process hazard analysis (PHA) often focuses on the major hazards of fires, explosions and toxic releases. Traditional PHA methods such as the Hazard and Operability (HAZOP) study and What-If analysis often necessarily include scenarios for other hazard types such as operability problems. This may be desired but sometimes is not. There is a need for a PHA technique that directly and exclusively addresses major process hazards. Such hazards are realized when process containment is lost so the method proposed here uses a categorization scheme to guide brainstorming of initiating events that will result in fires, explosions or toxic releases. It provides a more efficient and likely more complete identification of major hazard scenarios than current PHA methods.

Introduction

Process hazard analysis (PHA) is a key requirement of OSHA's Process Safety Management (PSM) standard, 29 CFR 1910.119 and EPA's Risk Management Program (RMP) rule, 40 CFR Part 68. These regulations require that PHA address toxic, fire and explosion hazards resulting from specific chemicals (called *major hazards* herein) and their possible impacts on employees, the public and the environment. The specific chemicals are defined in the regulations and are called Highly Hazardous Chemicals by OSHA and Regulated Substances by EPA.

The regulations specify six acceptable PHA methods and allow the use of "an appropriate equivalent methodology". The most commonly used PHA methods are the Hazard and Operability (HAZOP) Study and the What-If or What-if/Checklist approaches(1). Since OSHA's PSM standard became effective in 1992, many thousands of PHA studies have been performed using these methods. However, users of these techniques often find the studies tedious and time consuming and for these reasons it is not uncommon to find that potential team members do not want to participate in the studies. One reason for the tedious nature of these commonly used methods is that they do not identify major hazard scenarios in the most direct way. Furthermore, it has become apparent that they may not provide as complete an identification of major hazards in a process as possible. This paper proposes an improved approach, called Major Hazards Analysis (MHA).

Of the six PHA techniques listed in the PSM and RMP regulations, only HAZOP was developed specifically for use in the chemical process industries and it was developed many years before the regulations were enacted. Consequently, it is perhaps understandable that there may be a better way of addressing the PHA requirements of the regulations.

Hazards and Hazard Scenarios

Generally, a *hazard* is considered to be a situation or intrinsic property with the potential to create harm. In process safety, it means the potential for an accident with undesirable consequences. Processes can contain many different types of hazards, for example, chemical, e.g. toxic materials; physical, e.g. high pressure; mechanical, e.g. rotating equipment; electrical, e.g. high voltage power supply, etc. While PHA can be used to address any type of hazard, typically, in process safety, it is used to address the major hazards of fires, explosions and toxic releases. These occur when process containment is lost, directly or indirectly.

The principal objective of PHA is to identify *hazard scenarios*. These are specific, unplanned events or sequences of events that have an undesirable consequence resulting from the realization of a hazard. They are also called accident scenarios. Sometimes the word sequence is used in place of scenario.

The first event of a hazard scenario is called the *initiating event* or *cause* of the scenario (Figure 1). They may be failures of equipment or people, or external events (occurrences external to the process that have an adverse impact on it, e.g. lightning strike). *Intermediate events* follow. They are responses of the process and personnel to the initiating event. *Enabling events/conditions* may also be involved. They do not directly cause the scenario but make possible another event and they must be present or active for the scenario to proceed. The combination of these events results in a *consequence* which is the impact of the scenario in terms of its effects on people, the environment, property/equipment, the process, adjacent installations, etc. Consequences are characterized by *type* and *severity*. Type identifies what is impacted, i.e. people, the environment, property, etc. Severity is the degree of impact, e.g. single fatality vs multiple fatalities. *Measures* are the units used for severity, e.g. injuries, financial loss.

In PHA it is usual to identify *safeguards* that are in place. These are devices, systems or actions intended to interrupt or modify the chain of events following an initiating event to avoid or mitigate an adverse consequence. They prevent, detect or mitigate events in the hazard scenario. The PSM and RMP regulations require that PHA address "engineering and administrative controls applicable to the hazards" and "consequences of failure of engineering and administrative controls". The identification of existing safeguards not only indicates the risk control measures that have already been taken but also facilitates the identification of additional measures that may be required, i.e. *recommendations* for corrective action.

Hazard scenarios can be represented by the combinations of their starting and ending points, i.e. cause-consequence pairs and its is these combinations that are identified in PHA. When major hazards are of concern, the initiating events, or causes of interest, involve containment failure. Of course, PHA addresses only credible causes and realistic consequences that could reasonably be expected to occur under the circumstances of the hazard scenario. It is the identification of causes that is at the heart of PHA. If this is not done completely, hazard scenarios will be omitted. Once causes have been identified the determination of consequences is usually straightforward.

Causes may be expressed at different levels. For example, a PHA team may identify a credible cause as “pump fails off”. However, there is usually a need to identify why the pump failed, e.g. loss of power, switched off by operator, mechanical failure, etc. These *basic causes* help in identifying recommendations needed to reduce risk. There may be even more fundamental reasons for these basic causes. For example, operator error could be caused by inadequate procedures, inadequate training, stress, etc. These are called *root causes* and they are the underlying reasons why an event occurred. Various root causes may contribute to one basic cause. Usually, in PHA it is basic causes that are recorded in the worksheet.

Current PHA Methods

All PHA methods have in common that they identify initiating events (causes), consequences, safeguards, and recommendations (corrective actions). PHA methods are distinguished mostly by the way in which they approach the identification of causes.

In the case of HAZOP, deviations from design intent such as *no flow*, *high pressure*, *low level*, etc. are considered. The PHA team identifies credible causes of these deviations and then proceeds to identify their consequences, etc. The approach provides a thorough analysis, but, unfortunately, at the cost of considering many deviations that do not result in adverse consequences of concern. Many deviations result only in operability problems. However, users often want to focus only on identifying ways in which major hazards can be realized. In defense of HAZOP, as its name implies, it was developed to address both issues. Unfortunately, it is not easy to address only major hazards using the technique. Consequently, the effort involved in conducting such studies can be substantial.

Early practitioners of the HAZOP method realized this disadvantage and advocated a variant in which causes of deviations were identified only if an adverse consequence were apparent. This is the “consequence before cause approach”. Unfortunately, the approach can result in scenarios being missed because the possibility of adverse consequences is not always apparent from the deviation. Some adverse consequences can only be recognized after causes have been identified.

In the case of What-If approaches, the method considers questions that express causes of possible problems. The method can be used to focus more clearly on major hazards than HAZOP, although other undesired scenarios typically still arise. However, the method is less structured than HAZOP and generally does not provide the team with the same comfort level that they have identified hazard scenarios as thoroughly as with HAZOP.

Consequently, there is a need for a PHA method that directly addresses the identification of scenarios resulting from major hazards without including extraneous scenarios that wastes resources, distracts from identifying the important scenarios, adds to the time required to complete the study, and frustrates team members.

Major Hazard Analysis

Scenarios of interest that result from major hazards originate with loss of process containment. Causes of loss of containment can be direct, for example, valves left open or ruptures in lines or vessels. They may also be indirect, for example, runaway reactions resulting in releases through pressure relief devices or vessel and piping rupture. Therefore, MHA constrains brainstorming to such scenarios. It does so, by using a structured framework to guide the identification of initiating events.

All PHA methods subdivide the process so that individual parts can be analyzed. MHA can use the systems and subsystems typical of What-If studies or it can employ nodes (process lines and major vessels) as used by HAZOP. This allows MHA to be conducted at various levels of detail according to the user's needs.

MHA begins by considering the first node or system as do other PHA techniques. It then moves directly to the identification of causes of scenarios that originate in the node and result in loss of containment. In order to provide guidance to the PHA team and help assure completeness, it focuses brainstorming on specific categories of initiating events (causes) that can result in loss of containment. This focuses the team's brainstorming without narrowing their vision. A typical list of initiating event categories is shown in Table 1. Such lists can be customized for specific facilities or types of processes.

This categorization includes equipment and human failures as well as external events. The logic of the approach is that there is a limited number of categories of initiating events that result in loss of containment and within each category there is a limited number of ways this may happen. This enables the PHA team to use the scheme without being overburdened, while preserving their energy to consider items not in the scheme. The scheme prompts consideration of items not included in the lists.

The result of applying this categorization scheme using the MHA method is shown in Figure 2. The other columns of the worksheet are completed as for current PHA methods (Figure 3).

Two other enhancements are proposed for MHA. These are the addition of two columns to the MHA worksheet, "Enabling Event/Condition" and "Scenario" (Figure 4). These additions clarify the scenario and also provide valuable information for use in further analyses such as Layers of Protection Analysis (LOPA) or Quantitative Risk Analysis (QRA). Current PHA methods either do not include enabling events/conditions or combine them with other worksheet entries. Similarly, details of the scenario are sometimes not provided at all, or included, perhaps awkwardly, in other worksheet columns, e.g. the Consequence column of a HAZOP worksheet. It is possible to add these extra columns to the worksheets of current PHA methods but this has not often been done. The use of these columns encourages a fuller description of the hazard scenario.

It is also a good idea to add risk ranking columns to the worksheet so that qualitative risk estimates can be made for the hazard scenarios (Figure 4). They can be used to:

- help prioritize the recommendations
- determine if a recommendation needs to be made
- determine how quickly recommendations should be implemented
- distinguish between hazard scenarios
- screen scenarios for more detailed analysis, e.g. by LOPA

By constraining team deliberations only to those scenarios of interest, the MHA method helps preserve the most precious resource available to the team, namely their intellectual energy. This is vital when conducting studies on anything other than a small process since conventional PHA studies can become mind-numbingly tedious. Moreover, the MHA method offers structure comparable to HAZOP, while providing more specific guidance, without restricting brainstorming of major hazard scenarios.

Global nodes or systems in which issues that affect more than one node or system can also be addressed with MHA in a similar manner to existing PHA methods. This is also true for the consideration of facility siting and human factors which are regulatory requirements for PHAs performed to meet OSHA and EPA requirements.

Changing to MHA

One further advantage offered by MHA is the ease with which current PHA studies can be converted into MHA format. The format of MHA worksheets is very similar to those of other PHA techniques and information can be copied easily into the MHA format. This can be done when PHAs are revalidated. The revalidation can then address the analysis of process changes as well as the enhancement of the original PHA results by the use of MHA.

Tools to Apply MHA

Since MHA is a spreadsheet technique like other PHA methods, existing PHA recording tools can be used to perform MHA studies. The figures used to illustrate the method in this paper are screen captures from PHAWorks®, Primatech's PHA software package. PHAWorks® was modified to perform MHA studies using its existing capabilities without the need for any software coding changes.

Conclusions

MHA focuses the PHA team's attention on causes of loss of containment. In contrast, HAZOP focuses the team on process deviations that may or may not result in loss of containment. What-If analysis focuses the team on all types of accident causes but does not constrain brainstorming to loss of containment scenarios. Consequently, MHA is a more efficient way of addressing major hazards. Furthermore, the structured approach to identifying loss of containment scenarios provides confidence in the relative completeness of the method compared to What-If and HAZOP.

References

1. "Guidelines for Hazard Evaluation Procedures", Center for Chemical Process Safety, AIChE, 1985 and 1992.

Table 1. Initiating Event Categories For Major Hazard Analysis.

Leaks/ruptures
- Fracture: breaking open of a containment system by the propagation of a crack
- Puncture: a perforation or hole in a containment system as a result of impact
- Relief device stuck open
- Seal/gasket/flange failure
- Corrosion/erosion
- Flow surge or hydraulic hammer
- Other?

Incorrect actions or inactions by people
- Operator opens a valve, etc.
- Other?

Exceeding process limits
- Over/under pressuring
- Overheating
- Overcooling
- Overfilling
- Other?

Control systems failure
- Sensors
- Logic solver
- Final elements
- Communications interface
- Field wiring
- Power source
- Other?

Reactivity
- Runaway reactions
- Air ingress
- Inadvertent mixing of chemicals
- Other?

Structural failure
- Equipment supports
- Foundations/floors
- Cyclic loading
- Pressure fluctuations
- Other?

Utility failure
- Electricity
- Instrument air
- Plant nitrogen
- Cooling water
- Steam
- Other?

Natural external events
- Flooding
- Lightning
- High winds
- Earth movements
- Other?

Human external events
- Vehicle impacts
- Dropped objects from lifting devices
- Other?

Knock-on effects
- Incidents in adjacent processes
- Incidents within the process

Multiple failures
- Combinations of equipment failures
- Combinations of human failures
- Combinations of external events
- Combinations of any of these

Other
- Anything else?
- Anything unusual?

Figure 1. Elements of a Hazard Scenario.

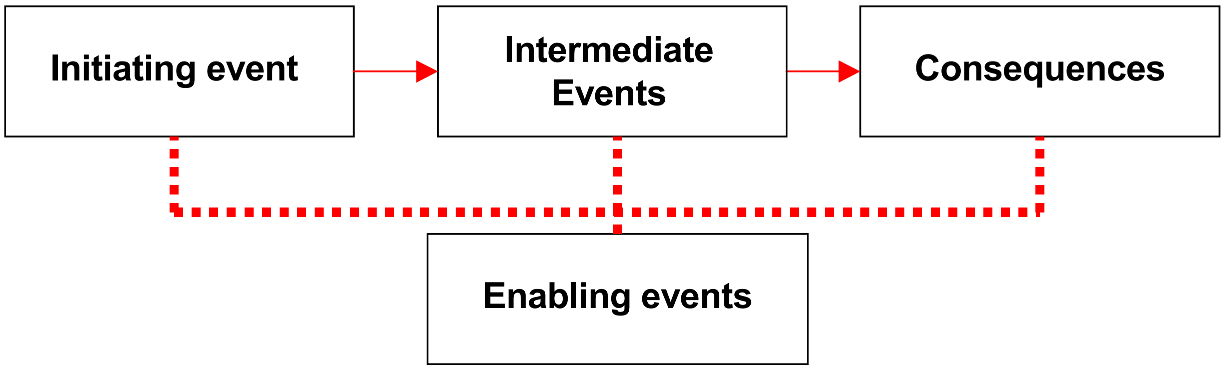


Figure 2. MHA Worksheet With Completed Initiating Event Column.

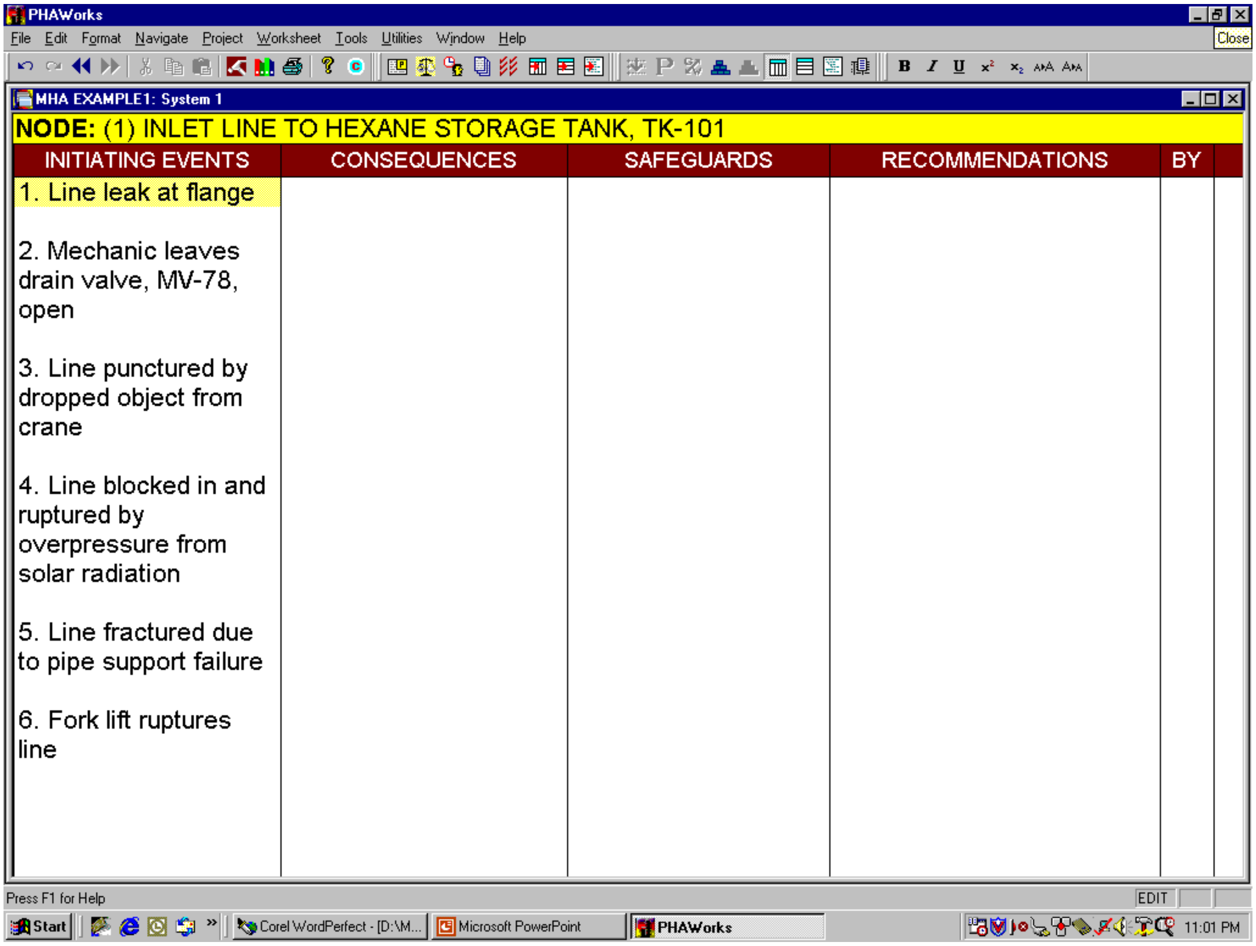
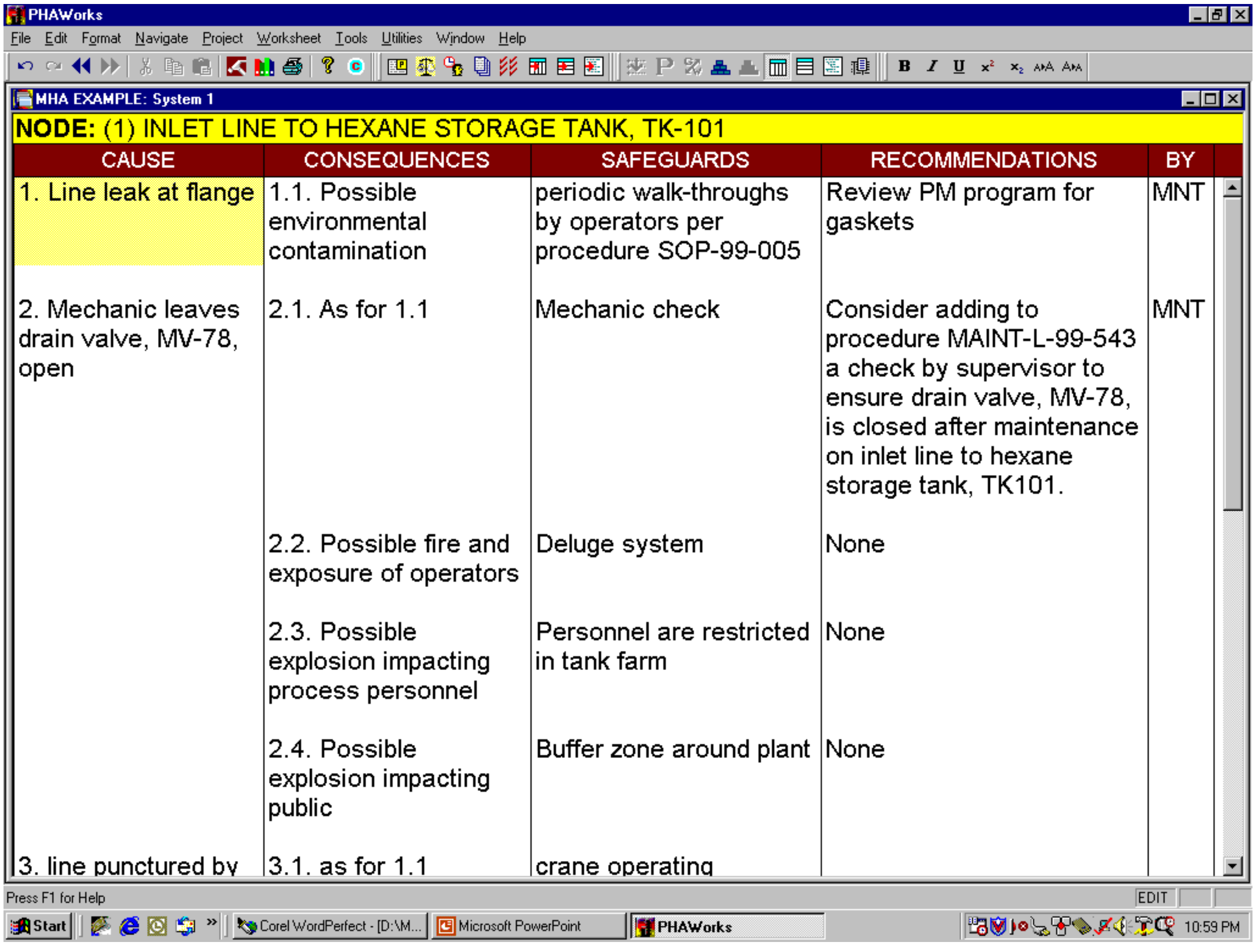


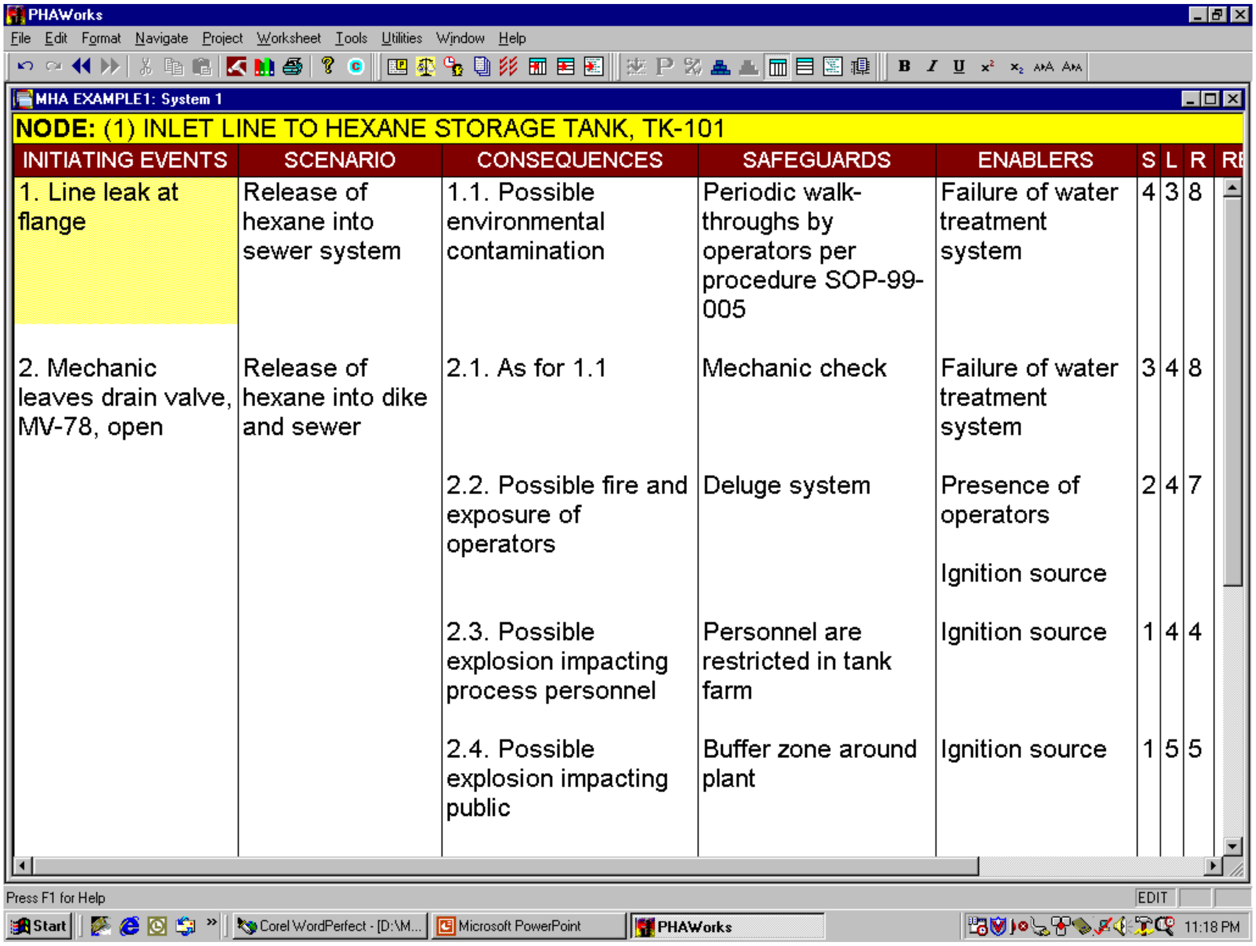
Figure 3. MHA Worksheet With Columns Completed.



NODE: (1) INLET LINE TO HEXANE STORAGE TANK, TK-101

CAUSE	CONSEQUENCES	SAFEGUARDS	RECOMMENDATIONS	BY
1. Line leak at flange	1.1. Possible environmental contamination	periodic walk-throughs by operators per procedure SOP-99-005	Review PM program for gaskets	MNT
2. Mechanic leaves drain valve, MV-78, open	2.1. As for 1.1	Mechanic check	Consider adding to procedure MAINT-L-99-543 a check by supervisor to ensure drain valve, MV-78, is closed after maintenance on inlet line to hexane storage tank, TK101.	MNT
	2.2. Possible fire and exposure of operators	Deluge system	None	
	2.3. Possible explosion impacting process personnel	Personnel are restricted in tank farm	None	
	2.4. Possible explosion impacting public	Buffer zone around plant	None	
3. line punctured by	3.1. as for 1.1	crane operating		

Figure 4. MHA Worksheet With Additional Columns.



PHAWorks

MHA EXAMPLE1: System 1

NODE: (1) INLET LINE TO HEXANE STORAGE TANK, TK-101

INITIATING EVENTS	SCENARIO	CONSEQUENCES	SAFEGUARDS	ENABLERS	S	L	R	RE
1. Line leak at flange	Release of hexane into sewer system	1.1. Possible environmental contamination	Periodic walk-throughs by operators per procedure SOP-99-005	Failure of water treatment system	4	3	8	
2. Mechanic leaves drain valve, MV-78, open	Release of hexane into dike and sewer	2.1. As for 1.1	Mechanic check	Failure of water treatment system	3	4	8	
		2.2. Possible fire and exposure of operators	Deluge system	Presence of operators Ignition source	2	4	7	
		2.3. Possible explosion impacting process personnel	Personnel are restricted in tank farm	Ignition source	1	4	4	
		2.4. Possible explosion impacting public	Buffer zone around plant	Ignition source	1	5	5	