# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD) SEVERITY, AND LEVEL OF CONTROL

**Clifford Watson, System Safety Engineer, CSP;**
***NASA; MSFC, AL USA 35812, Clifford.C.Watson@nasa.gov***

**KEYWORDS: Analysis, Probability, Severity, Likelihood**

## SYNOPSIS

Traditional hazard analysis techniques utilize a two-dimensional representation of the results determined by relative likelihood and severity of the residual risk. These matrices present a quick-look at the Likelihood (Y-axis) and Severity (X-axis) of the probable outcome of a hazardous event. A three-dimensional method, described herein, utilizes the traditional X and Y axes, while adding a new, third dimension, shown as the Z-axis, and referred to as the Level of Control. The elements of the Z-axis are modifications of the Hazard Elimination and Control steps (also known as the Hazard Reduction Precedence Sequence). These steps are: 1. Eliminate risk through design. 2. Substitute less risky materials for more hazardous materials. 3. Install safety devices. 4. Install caution and warning devices. 5. Develop administrative controls (to include special procedures and training.) 6. Provide protective clothing and equipment. When added to the two-dimensional models, the level of control adds a visual representation of the risk associated with the hazardous condition, creating a 'tall-pole' for the least-well-controlled failure while establishing the relative likelihood and severity of all causes and effects for an identified hazard. Computer modeling of the analytical results, using spreadsheets and three-dimensional charting gives a visual confirmation of the relationship between causes and their controls.

## INTRODUCTION

Practitioners of System Safety methodology are inventive by nature. In order to predict and control the risks of a new venture, the analyst must be able to identify the hazards that may be present, prescribe corrective actions, and provide some level of assurance that management has made the appropriate decision of safety versus acceptable risk.

Tools that may be used by System Safety analysts include the Preliminary Hazard Analysis (PHA), Fault Tree Analysis (FTA) or Logic Model (LM), and Failure Mode and Effects Analysis (FMEA). These methods are extremely detailed and, at times, very difficult for the uninitiated to understand. At the completion of each phase of the analysis, management is apprised of the residual risks that have been identified.

It is at this time that the Safety Professional must stand and explain, in detail, the status of the analysis. It is also at this time that Safety Professionals usually step out of their comfort zone. What is needed is a method, which utilizes the same 'dog-and-pony' techniques, which the managers are comfortable with…and familiar.

## BACKGROUND

As soon as a new project is identified, managers begin to theorize what gains are to be made from the venture, and what risks are involved. If a new, highly technical design is to be developed, such as a composite aircraft, a space shuttle, or robot, the call goes out for many varied and highly specialized technicians. These technicians include engineers, designers, accountants, and Safety Professionals.

When the new project is sufficiently detailed to identify what its purpose is to be, the professionals perform initial analyses. The engineers perform trade studies to identify the alternative methods or designs; the accountants perform risk assessments to determine what the marketability and return-on-investment is likely to be; and the

System Safety Professional performs a Preliminary Hazard Analysis (PHA). A checklist of Generic Hazards may be used to guide the creation of the PHA. A partial list is shown as Figure 1.

**LIST OF GENERIC HAZARDS**

(Page 1 of 2)

| GENERIC HAZARD | GENERIC HAZARD TYPE |
|---|---|
| I. CONTAMINATION/CORROSION | A. CHEMICAL DISASSOCIATION<br>B. CHEMICAL REPLACEMENT/COMBINATION<br>C. MOISTURE<br>D. OXIDATION<br>E. ORGANIC (FUNGUS/BACTERIAL, ETC.)<br>F. PARTICULATE |
| II. ELECTRICAL DISCHARGE/SHOCK | A. EXTERNAL SHOCK<br>B. INTERNAL SHOCK<br>C. STATIC DISCHARGE<br>D. CORONA<br>E. SHORT |
| III. ENVIRONMENTAL/WEATHER | A. FOG<br>B. FUNGUS/BACTERIAL<br>C. LIGHTNING<br>D. PRECIPITATION (RAIN/SNOW/SLEET/HAIL)<br>E. SOLAR/COSMIC RADIATION<br>F. SAND/DUST<br>G. VACUUM<br>H. WIND<br>I. TEMPERATURE EXTREMES |
| IV. FIRE/EXPLOSION | A. CHEMICAL CHANGE (EXOTHERMIC/ENDOTHERMIC)<br>B. FUEL AND OXIDIZER IN PRESENCE OF PRESSURE AND IGNITION SOURCE<br>C. PRESSURE RELEASE/IMPLOSION<br>D. HIGH HEAT SOURCE |
| V. IMPACT/COLLISION | A. ACCELERATION (INCLUDING GRAVITY)<br>B. DETACHED EQUIPMENT<br>C. MECHANICAL SHOCK/VIBRATION/ACOUSTICAL<br>D. METEOROIDS/METEORITES<br>E. MOVING/ROTATING EQUIPMENT |

**Figure 1 Partial List of Generic Hazards**

**THE ANALYSIS PROCESS**

The PHA, sometimes referred to as a Preliminary Hazard Screening, is the initial cut at identifying the hazards associated with a selected design or process. The PHA may be presented in a tabular format like that shown in Figure 2. As the analysis develops, Causes, Effects, Controls, and Verifications are added to the Hazardous Condition and Safety Requirements already identified in the earliest stages of analysis. The Severity and Likelihood are usually the last elements to be added, based on the perceived outcome of the hazardous condition following the application of controls the analysis may look like that in Figure 2.

PHA NO: _____

MISSION PHASE: Flight Operations, Mission Operations, Turnaround, Etc. ENGINEER: _____

SUBSYSTEM OR OPERATION: Identify EPS, ECLSS, GN&C, Etc. DATE: 06/30/86

EFFECTIVITY: Ascent, On-Orbit, Entry, Approach and Landing Turnaround SHEET 1 of 1

| HAZARDOUS CONDITION | HAZARD CAUSES | HAZARD EFFECT | SEVERITY LEVEL | SAFETY REQUIRE-MENTS | HAZARD ELIMINATION/ CONTROL PROVISIONS | VERIFICATIONS | LIKELIHOOD OF OCCURRENCE |
|---|---|---|---|---|---|---|---|
| Use the checklist below to identify potentially hazardous conditions.<br>1. Can the system/ subsystem fail to operate as intended?<br>2. Can the system/ sub-system operate inadvertently (untimely)?<br>3. Are there generic hazards? (See Figure 3-2)<br>Record the identified hazards. | Enter brief description of how each hazardous condition is created, i.e., rupture of the $O_2$ tank; wiring insulation overheating and igniting; etc. | Record the potential effect of each hazardous condition on critical equipment, personnel or the general public, i.e., loss of vehicle; emergency landing in inhabited area; etc. | Identify the severity level as one of the following for each hazardous condition:<br>CA – Catastrophic (see glossary)<br>CR – Critical (see glossary)<br>MR – Marginal (see glossary) | Identify the existing or proposed safety requirement that will eliminate or control the hazardous condition by document and paragraph number. | Identify proposed hazard reduction methods for open hazards and implemented reduction methods for controlled hazards. | Identify the methods used to verify the hazard controls. Include sufficient detail/explanation of testing, inspection, and analysis which mitigate the hazard and support hazard closure or risk rationale. Verification methods include analyses, tests, inspections, and operations and maintenance requirements. Identify the verification reference by document number and title. | Assess the controls that are in place and classify them as one of the following: Probable; Infrequent; Remote; or Improbable. |

**Figure 2 Preliminary Hazard Analysis**

Following the selection of the 'lowest-business-risk' model, additional designs or processes are refined. This design-analyze-redesign sequence is critical for the Safety Professional. It is at this point that the final controls are identified in order to reduce the risk to an acceptable level. The Safety Professional knows that by performing a high quality analysis, the product is more likely to be successful and profitable. The Safety Professional should 'lead the design' as much as possible. Identification of hazards late in the design phase is likely to result in costly redesign or cancellation of the venture if the perceived risk is too great. Either of these outcomes may be embarrassing for all parties.

However, it happens.

One of the causes of such an unfortunate outcome could be the lack of management understanding of the hazards involved. This could be as a result of "Safety people talking to Safety people because no one else will talk to them." It is an all-too-often occurrence that the message regarding the residual risks may have been undersold. A possible cause of this is the lack of management understanding of the risks due to an overwhelming amount of technical data thrown at a non-technical audience. One of the methods used by the Safety Professional to reduce this 'data overload' is the use of Severity-to-Likelihood matrices. Figures 3 and 4 are examples of risk matrices.

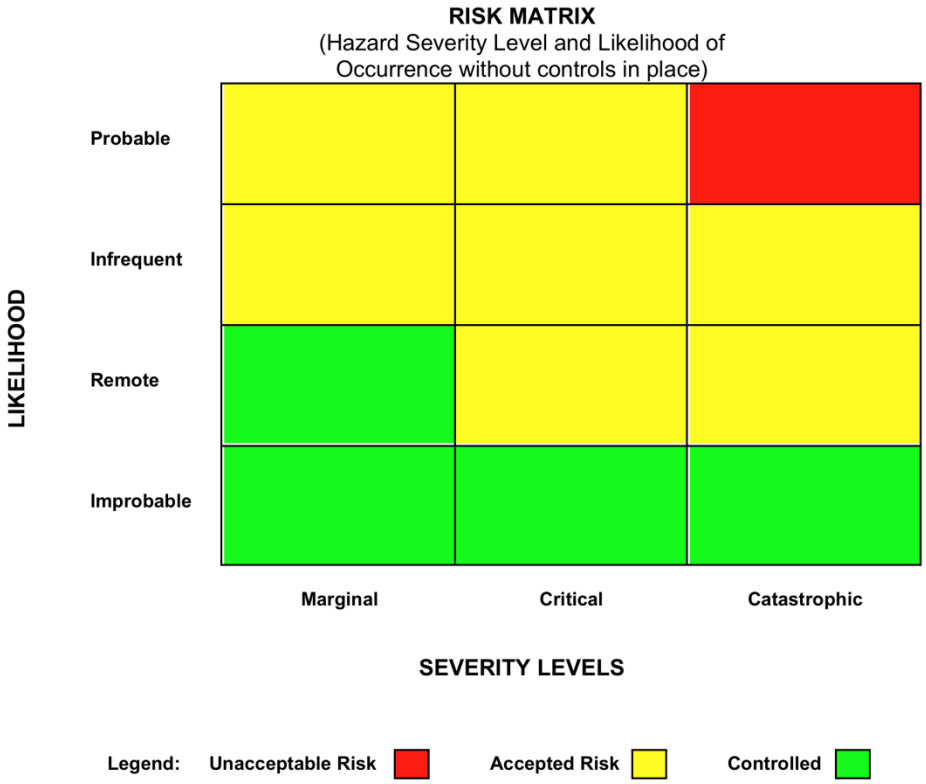



Figure 3 Risk Matrix (3 X 4)

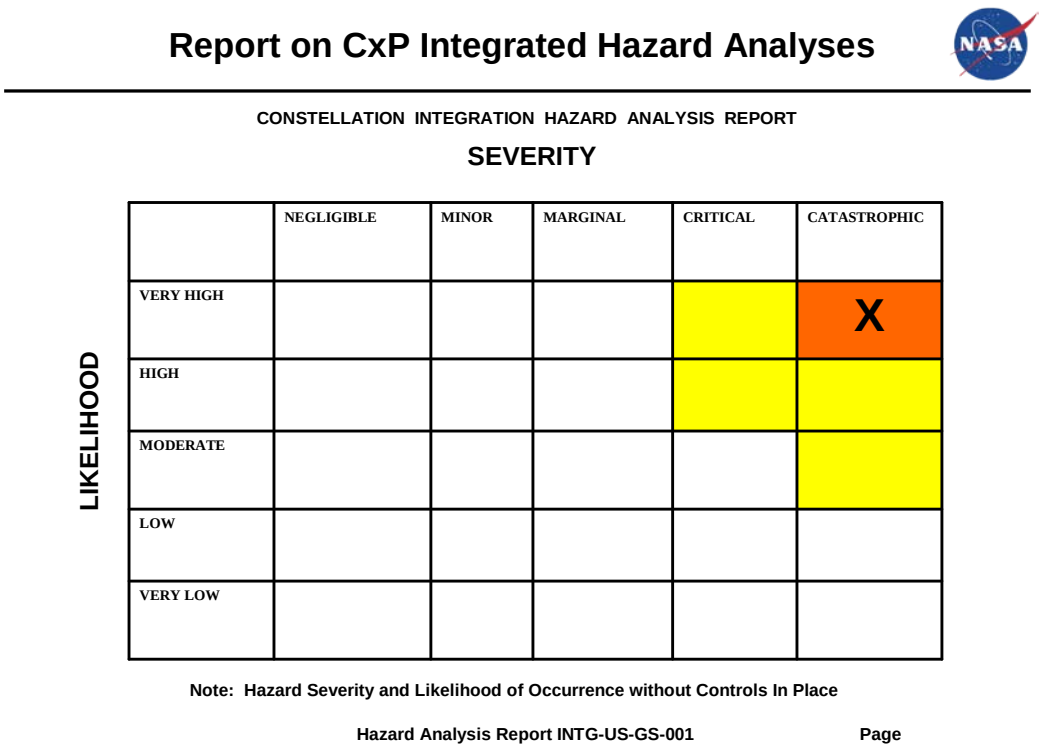



Figure 4 Constellation Program Risk Matrix (5 x 5)

**Hazard Categorization**

NASA's Methodology for Conduct of Space Shuttle Program Hazard Analyses (NSTS 22254) provides the following definition of Severity Levels.

The severity level is an assessment of the most severe effects of a hazard. Complete for each cause (with the exception of those causes which transfer to other Hazard Reports) for all controls and verifications by assessing the most severe effect and documenting it as catastrophic, critical, or marginal.

(a) Catastrophic: Hazard could result in a mishap causing fatal injury to personnel and/or loss of one or more major elements of the flight vehicle or ground facility.
(b) Critical: Hazard could result in serious injury to personnel and/or damage to flight or ground equipment which would cause mission abort or a significant program delay.
(c) Marginal: Hazard could result in a mishap of minor nature inflicting first−aid injury to personnel and/or damage to flight or ground equipment which can be tolerated without abort or repaired without significant program delay.

The severity is plotted on the X axis as seen in Figure 3. The severity increases from left to right.

The Likelihood of Occurrence is an assessment of the most severe effects of a hazard transpiring. Complete for each cause (with the exception of those causes which transfer to other HR[s] for all controls and verifications) by assessing the controls that are in place and documenting them as probable, infrequent, remote, or improbable.
Likelihood is assessed considering the effectiveness of the controls in place for the life of the program.

(a) Probable: Expected to happen in the life of the program. If quantitative risk analyses are used to assist in likelihood determination, then for a cause to be considered probable, the single mission risk should have a mean probability greater than 1 in 200.

NOTE: In cases where the mean probability is less than 1 in 200, a cause may still be classified as probable once other factors, such as the level of uncertainty associated with the controls, are taken into account. Conversely, a mean probability of greater than 1 in 200 in itself should not automatically result in a cause being classified as probable if certainty in the controls provides a basis for not doing so.

(b) Infrequent: Could happen in the life of the program. Controls have significant limitations or uncertainties.
(c) Remote: Could happen in the life of the program, but not expected. Controls have minor limitations or uncertainties.
(d) Improbable: Extremely remote possibility that it will happen in the life of the program. Strong controls in place.

The Likelihood is plotted as the Y axis, also shown in Figure 3 and increases from bottom to top.

Other reference documents utilize differing descriptions of the Severity and Likelihood; these are shown in Figures 5 and 6, representing the MIL-STD-882 definitions of severity and probability. For purposes of this paper, likelihood and probability are considered to be one and the same.
MIL-STD-882D has identified a set of mishap risk mitigation measures that identifies potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Mishap risk mitigation is an iterative process that culminates when the residual mishap risk has been reduced to a level acceptable to the appropriate authority. The system safety design order of precedence for mitigating identified hazards is:

a. Eliminate hazards through design selection. If unable to eliminate an identified hazard, reduce the associated mishap risk to an acceptable level through design selection.

b. Incorporate safety devices. If unable to eliminate the hazard through design selection, reduce the mishap risk to an acceptable level using protective safety features or devices.

c. Provide warning devices. If safety devices do not adequately lower the mishap risk of the hazard, include a detection and warning system to alert personnel to the particular hazard.

d. Develop procedures and training. Where it is impractical to eliminate hazards through design selection or to reduce the associated risk to an acceptable level with safety and warning devices, incorporate special procedures and training. Procedures may include the use of personal protective equipment. For hazards assigned Catastrophic or Critical mishap severity categories, avoid using warning, caution, or other written advisory as the only risk reduction method.

| Description | Category | Environmental, Safety, and Health Result Criteria |
|---|---|---|
| Catastrophic | I | Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation. |
| Critical | II | Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation. |
| Marginal | III | Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished. |
| Negligible | IV | Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation. |

**Figure 5 MIL-STD-882 Mishap Severity Definitions**

| Description* | Level | Specific Individual Item | Fleet or Inventory** |
|---|---|---|---|
| Frequent | A | Likely to occur often in the life of an item, with a probability of occurrence greater than $10^{-1}$ in that life. | Continuously experienced. |
| Probable | B | Will occur several times in the life of an item, with a probability of occurrence less than $10^{-1}$ but greater than $10^{-2}$ in that life. | Will occur frequently. |
| Occasional | C | Likely to occur some time in the life of an item, with a probability of occurrence less than $10^{-2}$ but greater than $10^{-3}$ in that life. | Will occur several times. |
| Remote | D | Unlikely but possible to occur in the life of an item, with a probability of occurrence less than $10^{-3}$ but greater than $10^{-6}$ in that life. | Unlikely, but can reasonably be expected to occur. |
| Improbable | E | So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than $10^{-6}$ in that life. | Unlikely to occur, but possible. |

**Figure 6 MIL-STD-882 Mishap Probability Definitions**

**THE THREE-DIMENSIONAL DISPLAY PROCESS**

Those same intuitive, inventive people who are called upon to perform hazard analyses are usually computer literate, either by desire or by requirements of the job. A plethora of software has been developed for the offices of worldwide businesses. Along with it came an infusion of new techniques that may be used to visualize data. It is not uncommon for the Safety Department to have high-performance computers available to the Safety Professional. In most cases, the computers have sophisticated software that aids in the analysis of hazards, generating charts, fault trees, tables, and other statistical reports. This enables the sharing of data and transfer of corporate intelligence to a wide and diversified audience who may incorporate this information into new reports.

One of the most useful of the personal computer software packages is the database/spreadsheet. It is through the use of spreadsheets, including Microsoft's Excel and Corel's Quattro Pro and their ability to produce three-dimensional charts that the generation of the Three Dimensional Risk Assessment is made possible.

| HAZARDOUS CONDITION | HAZARD CAUSE | HAZARD EFFECT | SEVERITY LEVEL | SAFETY REQUIREMENTS | HAZARD ELIMINATION /CONTROL PROVISIONS | VERIFICATION | LIKELIHOOD OF OCCURRENCE |
|---|---|---|---|---|---|---|---|
| Low pressure vessel ruptures | a) Inadequate design | Destruction of vessel | Marginal – hydro test will identify | Design to ASME Code | Qualified designer | Verified by independent engineer | Improbable |
| | b) Common connection between hi and lo pressure supply | Destruction of vessel | Critical | Systems shall not have interchangeable connections | Procedures require relief valve | Relief valve inspection program | Remote |
| | c) Inadequate Maintenance | Destruction of vessel; injury | Catastrophic | Periodic cleaning, painting | Scheduled proof test | On plant inspection schedule | Infrequent |
| | d) Vehicle collision | Destruction of vessel; injury | Catastrophic | Vessel must be protected from traffic | Signs limiting traffic in vicinity | Monthly Safety Dept. inspection | Probable |
| | e) Relief valve fails | Destruction of vessel; injury | Catastrophic | Install relief valve | Relief valve annual testing | Maintenance Dept. testing | Improbable |

**Figure 7 Preliminary Hazard Analysis for a Pressure Vessel**

In this example, the hazardous condition has been identified to have five potential causes. Each cause is lettered sequentially as a), b), c), d), or e). The Hazard Elimination/Control Provisions are developed based on the best-available information, including safety requirements that are anticipated, or in place prior to project initialization.

Figure 8, below, adds a note in the Hazard Elimination/Control Provisions column to indicate the perceived Level of Control represented by the controls.

| HAZARDOUS CONDITION | HAZARD CAUSE | HAZARD EFFECT | SEVERITY LEVEL | SAFETY REQUIREMENTS | HAZARD ELIMINATION /CONTROL PROVISIONS | VERIFICATION | LIKELIHOOD OF OCCURRENCE |
|---|---|---|---|---|---|---|---|
| Low pressure vessel ruptures | a. Inadequate design | Destruction of vessel | Marginal – hydro test will identify | Design to ASME Code | Qualified designer LOC= 0 | Verified by independent engineer | Improbable |
| | b. Common connection between hi and lo pressure supply | Destruction of vessel | Critical | Systems shall not have interchangeable connections | Procedures require relief valve LOC=2 | Relief valve inspection program | Remote |
| | c. Inadequate Maintenance | Destruction of vessel; injury | Catastrophic | Periodic cleaning, painting | Scheduled proof test LOC=4 | On plant inspection schedule | Infrequent |
| | d. Vehicle collision | Destruction of vessel; injury | Catastrophic | Vessel must be protected from traffic | Gates and lights limiting traffic in vicinity LOC=3 | Monthly Safety Dept. inspection | Probable |
| | e. Relief valve fails | Destruction of vessel; injury | Catastrophic | Install relief valve | Relief valve annual testing LOC=4 | Maintenance Dept. testing | Improbable |

## Figure 8 Preliminary Hazard Analysis for a Pressure Vessel with Level of Control added

The elements of the Z-axis contained in the Three Dimensional Risk Representation are modifications of the Hazard Elimination and Control steps (also known as the Hazard Reduction Precedence Sequence). These steps are:

0. Eliminate risk through design.
1. Substitute less risky materials for more hazardous materials.
2. Install safety devices.
3. Install caution and warning devices.
4. Develop administrative controls (to include special procedures and training.)
5. Provide protective clothing and equipment.

Figure 9 shows a typical screen from a Microsoft Excel spreadsheet that demonstrates the method of incorporating Severity, Likelihood, and Level of Control into a visual representation of the causes, the resultant risk, and the amount of control afforded to limiting the risk. In this table, the Level of Control is represented by the number, or level of control, of each cause.

| SEVERITY | MARGINAL | CRITICAL | CATASTROPHIC |
|---|---|---|---|
| LIKELIHOOD | | | |
| IMPROBABLE | 0a | | 4e |
| REMOTE | | 2b | |
| INFREQUENT | | | 4c |
| PROBABLE | | | 3d |

## Figure 9 Microsoft Excel Spreadsheet Screenshot

When converted to a three-dimensional view, the information contained in the spreadsheet generates the chart shown below.

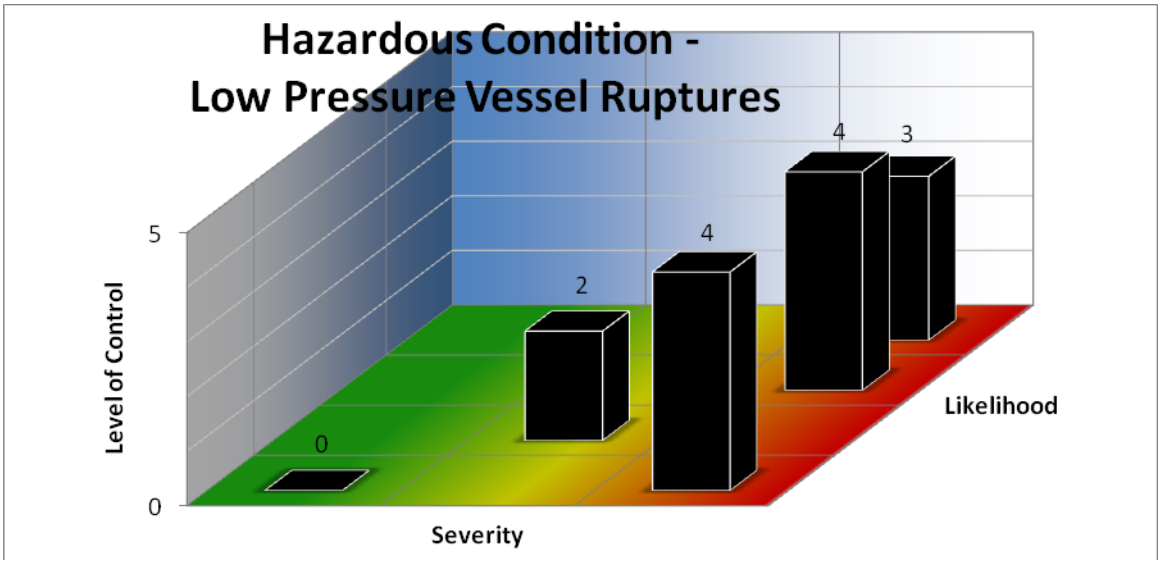



**Figure 10 Three-Dimensional View of Severity, Likelihood, and Level of Control**

**THE THREE-DIMENSIONAL REPRESENTATION**

It is true that during a hazard analysis or assessment, the analyst will determine what the likelihood of a hazard will be and the outcome if it is uncontrolled. This two-dimensional process is plotted on a matrix where it can be visualized. It is important that managers understand what they are viewing when a risk matrix is displayed. It is unfortunate that the controls identified during the analysis may be lost during the visual and oral presentations.

When automated, the spreadsheet prepares a standard presentation style chart such as that shown in Figure 10. As demonstrated by the chart, the level of Severity increases from left-to-right; the Likelihood of Occurrence increases from front to back; and the Level of Control is displayed in such a manner as to raise the lowest control measure to the highest point on the Z axis – thereby producing the 'tall-pole'.

A tall-pole in the left-front square may then be identified as a lower risk than a tall-pole in the right-back corner.

It is at this point in the analysis that the Safety Professional can demonstrate that reducing the risk through judicious use of the Hazard Reduction Precedence Sequence will result in a lower programmatic risk and a safer system. As controls are improved, the matrix can be modified to demonstrate a reduced level of exposure.

**CONCLUSION**

The Safety Professional has many tools available to assist in displaying the results of analyses. Traditional two-dimensional matrices have been used successfully for many years. Today's managers require easily understood presentations that demonstrate as much information as possible. Personal computers coupled with available software make this job easier.

With more information available at a glance, management has the opportunity to make business decisions that can improve the safety of the project under review, increase the profitability, and reduce costs of redesign at the earliest possible time.

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

PREPARED BY

CLIFFORD WATSON, CSP

NASA

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- INTRODUCTION

- Traditional hazard analysis techniques utilize a two-dimensional representation of the results determined by relative likelihood and severity of the residual risk.
- These matrices present a quick-look at the Likelihood (Y-axis) and Severity (X-axis) of the probable outcome of a hazardous event.
- A three-dimensional method, described herein, utilizes the traditional X and Y axes, while adding a new, third dimension, shown as the Z-axis, and referred to as the Level of Control.

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- Tools Used by the Safety Analyst
  - Preliminary Hazard Analysis (PHA)
  - Fault Tree Analysis (FTA) or Logic Model (LM)
  - Failure Mode and Effects Analysis (FMEA)

- These tools are detailed and may be difficult for uninitiated persons to understand

- System Safety analysts must be able to present the information developed by these tools to explain the results of these analyses

- Traditional tools are two-dimensional and present limited data from the analysis

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- New projects require early analysis by System Safety
- Early techniques may begin with the Preliminary Hazard Analysis
- As an aid to the analyst, Generic Hazard Lists may be used

**LIST OF GENERIC HAZARDS**

(Page 1 of 2)

| GENERIC HAZARD | GENERIC HAZARD TYPE |
|---|---|
| I. CONTAMINATION/CORROSION | A. CHEMICAL DISASSOCIATION<br>B. CHEMICAL REPLACEMENT/COMBINATION<br>C. MOISTURE<br>D. OXIDATION<br>E. ORGANIC (FUNGUS/BACTERIAL, ETC.)<br>F. PARTICULATE |
| II. ELECTRICAL DISCHARGE/SHOCK | A. EXTERNAL SHOCK<br>B. INTERNAL SHOCK<br>C. STATIC DISCHARGE<br>D. CORONA<br>E. SHORT |
| III. ENVIRONMENTAL/WEATHER | A. FOG<br>B. FUNGUS/BACTERIAL<br>C. LIGHTNING<br>D. PRECIPITATION (RAIN/SNOW/SLEET/HAIL)<br>E. SOLAR/COSMIC RADIATION<br>F. SAND/DUST<br>G. VACUUM<br>H. WIND<br>I. TEMPERATURE EXTREMES |
| IV. FIRE/EXPLOSION | A. CHEMICAL CHANGE (EXOTHERMIC/ENDOTHERMIC)<br>B. FUEL AND OXIDIZER IN PRESENCE OF PRESSURE AND IGNITION SOURCE<br>C. PRESSURE RELEASE/IMPLOSION<br>D. HIGH HEAT SOURCE |
| V. IMPACT/COLLISION | A. ACCELERATION (INCLUDING GRAVITY)<br>B. DETACHED EQUIPMENT<br>C. MECHANICAL SHOCK/VIBRATION/ACOUSTICAL<br>D. METEOROIDS/METEORITES<br>E. MOVING/ROTATING EQUIPMENT |

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- Using the Generic Hazard List, the Safety Analyst prepares a Preliminary Hazard Analysis (PHA)
- PHAs are developed as the design advances; Hazardous Conditions are identified first, with Safety Requirements identified as basic controls.

PHA NO: _____

MISSION PHASE: Flight Operations, Mission Operations, Turnaround, Etc. ENGINEER: _____

SUBSYSTEM OR OPERATION: Identify EPS, ECLSS, GN&C, Etc. DATE: 06/30/86

EFFECTIVITY: Ascent, On-Orbit, Entry, Approach and Landing Turnaround SHEET 1 of 1

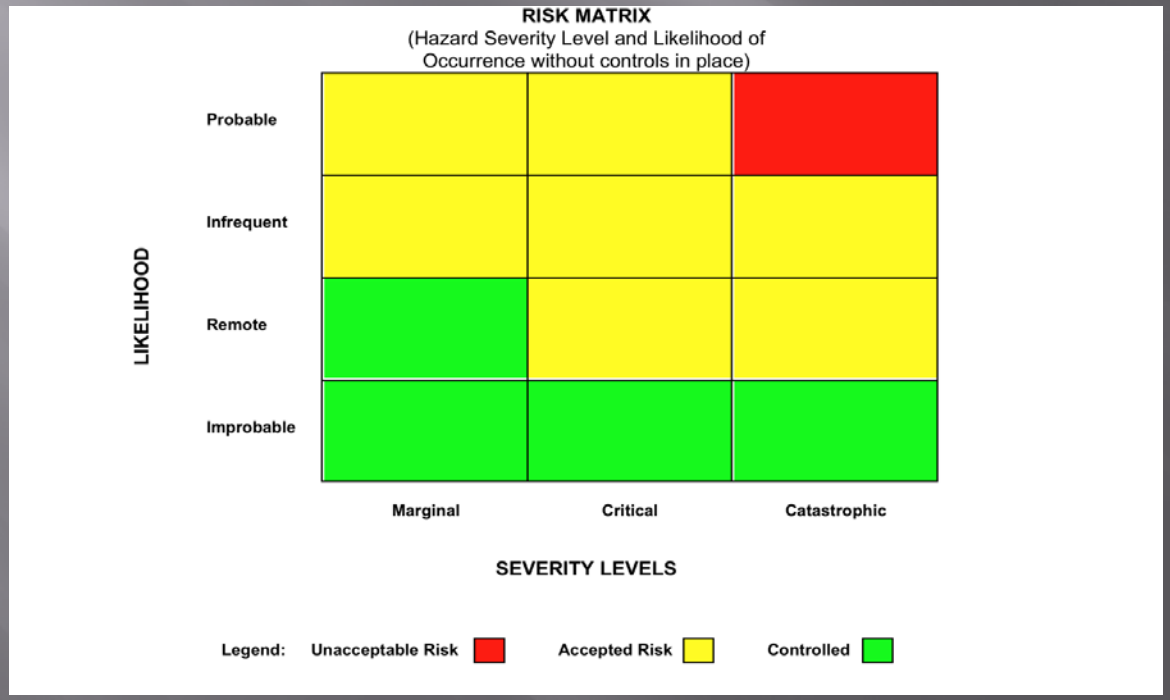
| HAZARDOUS CONDITION | HAZARD CAUSES | HAZARD EFFECT | SEVERITY LEVEL | SAFETY REQUIRE-MENTS | HAZARD ELIMINATION/ CONTROL PROVISIONS | VERIFICATIONS | LIKELIHOOD OF OCCURRENCE |
|---|---|---|---|---|---|---|---|
| Use the checklist below to identify potentially hazardous conditions.<br>1. Can the system/ subsystem fail to operate as intended?<br>2. Can the system/ sub-system operate inadvertently (untimely)?<br>3. Are there generic hazards? (See Figure 3-2)<br>Record the identified hazards. | Enter brief description of how each hazardous condition is created, i.e., rupture of the $O_2$ tank; wiring insulation overheating and igniting; etc. | Record the potential effect of each hazardous condition on critical equipment, personnel or the general public, i.e., loss of vehicle; emergency landing in inhabited area; etc. | Identify the severity level as one of the following for each hazardous condition:<br>CA – Catastrophic (see glossary)<br>CR – Critical (see glossary)<br>MR – Marginal (see glossary) | Identify the existing or proposed safety requirement that will eliminate or control the hazardous condition by document and paragraph number. | Identify proposed hazard reduction methods for open hazards and implemented reduction methods for controlled hazards. | Identify the methods used to verify the hazard controls. Include sufficient detail/explanation of testing, inspection, and analysis which mitigate the hazard and support hazard closure or risk rationale. Verification methods include analyses, tests, inspections, and operations and maintenance requirements. Identify the verification reference by document number and title. | Assess the controls that are in place and classify them as one of the following: Probable; Infrequent; Remote; or Improbable. |

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- An early use of the PHA may be the identification of the “lowest-business-risk” model
- Following this, redesign may be required
  - Early identification of hazardous conditions, and the resultant re-design can be a substantial cost savings, since hardware hasn’t been built, or the use of ‘boiler plate’ models is significantly less to manufacture
  - Thus, the System Safety Engineer becomes an integral participant in the design-analyze-redesign sequence.
- System Safety should be involved as early as possible in the analysis of new systems, and may, in some cases, ‘lead’ the design
- Identification of uncontrollable hazards late in design and lead to cancellation of the project if the perceived risk is too high

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- System Safety Engineers have the ability to address the hazards in a manner that is easy for Management to understand
- The selection of tools is important
- The most frequently used method of displaying relative risk is the Severity-Likelihood Matrix



# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- Matrices are frequently customized for the project

## Report on CxP Integrated Hazard Analyses

CONSTELLATION INTEGRATION HAZARD ANALYSIS REPORT

**SEVERITY**

**LIKELIHOOD**

| | NEGLIGIBLE | MINOR | MARGINAL | CRITICAL | CATASTROPHIC |
|---|---|---|---|---|---|
| VERY HIGH | | | | | X |
| HIGH | | | | | |
| MODERATE | | | | | |
| LOW | | | | | |
| VERY LOW | | | | | |

Note: Hazard Severity and Likelihood of Occurrence without Controls In Place

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- NASA's ***Methodology for Conduct of Space Shuttle Program Hazard Analysis*** (NSTS 22254) provides the following definition of Severity Levels

- Severity Levels
  - (a) Catastrophic: Hazard could result in a mishap causing fatal injury to personnel and/or loss of one or more major elements of the flight vehicle or ground facility
  - (b) Critical: Hazard could result in serious injury to personnel and/or damage to flight or ground equipment which would cause mission abort or a significant program delay.
  - (c) Marginal: Hazard could result in a mishap of minor nature inflicting first-aid injury to personnel and/or damage to flight or ground equipment which can be tolerated without abort or repaired without significant program delay.
- Severity is plotted on the "X" axis
- Severity increases from left to right

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- NASA's ***Methodology for Conduct of Space Shuttle Program Hazard Analysis*** (NSTS 22254) provides the following definition of Likelihood, or Probability of Occurrence

- Likelihood
  - (a) Probable: Expected to happen in the life of the program…a single mission risk should have a mean probability greater than 1 in 200
  - (b) Infrequent: Could happen in the life of the program. Controls have significant limitations or uncertainties
  - (c) Remote: Could happen in the life of the program, but not expected. Controls have minor limitations or uncertainties
  - (d) Improbable: Extremely remote possibility that it will happen in the life of the program. Strong controls in place.
- Likelihood is plotted on the "Y" axis
- Likelihood increases from bottom to top

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- LEVEL OF CONTROL

- MIL-STD-882D has identified a set of mishap risk mitigation measures that identifies potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method.
- a. Eliminate hazards through design selection.
- b. Incorporate safety devices.
- c. Provide warning devices.
- d. Develop procedures and training.

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- LEVEL OF CONTROL

- A Modified Hazard Reduction Precedence Sequence has been developed and adds two additional levels of control. They are:
- 0. Eliminate risk through design.
- 1. Substitute less risky materials for more hazardous materials.
- 2. Install safety devices.
- 3. Install caution and warning devices.
- 4. Develop administrative controls (to include special procedures and training.)
- 5. Provide protective clothing and equipment

As you see, this Sequence gives a weight to each level of control; the weighting is inverted to provide a ‘tall-pole’ in following charts to indicate low-level controls ‘poking up’

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

Now let us see how these elements come together in a traditional Risk Matrix

| HAZARDOUS CONDITION | HAZARD CAUSE | HAZARD EFFECT | SEVERITY LEVEL | SAFETY REQUIREMENTS | HAZARD ELIMINATION /CONTROL PROVISIONS | VERIFICATION | LIKELIHOOD OF OCCURRENCE |
|---|---|---|---|---|---|---|---|
| Low pressure vessel ruptures | a) Inadequate design | Destruction of vessel | Marginal – hydro test will identify | Design to ASME Code | Qualified designer | Verified by independent engineer | Improbable |
| | b) Common connection between hi and lo pressure supply | Destruction of vessel | Critical | Systems shall not have interchangeable connections | Procedures require relief valve | Relief valve inspection program | Remote |
| | c) Inadequate Maintenance | Destruction of vessel; injury | Catastrophic | Periodic cleaning, painting | Scheduled proof test | On plant inspection schedule | Infrequent |
| | d) Vehicle collision | Destruction of vessel; injury | Catastrophic | Vessel must be protected from traffic | Signs limiting traffic in vicinity | Monthly Safety Dept. inspection | Probable |
| | e) Relief valve fails | Destruction of vessel; injury | Catastrophic | Install relief valve | Relief valve annual testing | Maintenance Dept. testing | Improbable |

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

Now let us see how these elements come together in a revised Risk Matrix that adds Level of Control

| HAZARDOUS CONDITION | HAZARD CAUSE | HAZARD EFFECT | SEVERITY LEVEL | SAFETY REQUIREMENTS | HAZARD ELIMINATION /CONTROL PROVISIONS | VERIFICATION | LIKELIHOOD OF OCCURRENCE |
|---|---|---|---|---|---|---|---|
| Low pressure vessel ruptures | a. Inadequate design | Destruction of vessel | Marginal – hydro test will identify | Design to ASME Code | Qualified designer LOC= 0 | Verified by independent engineer | Improbable |
| | b. Common connection between hi and lo pressure supply | Destruction of vessel | Critical | Systems shall not have interchangeable connections | Procedures require relief valve LOC=2 | Relief valve inspection program | Remote |
| | c. Inadequate Maintenance | Destruction of vessel; injury | Catastrophic | Periodic cleaning, painting | Scheduled proof test LOC=4 | On plant inspection schedule | Infrequent |
| | d. Vehicle collision | Destruction of vessel; injury | Catastrophic | Vessel must be protected from traffic | Gates and lights limiting traffic in vicinity LOC=3 | Monthly Safety Dept. inspection | Probable |
| | e. Relief valve fails | Destruction of vessel; injury | Catastrophic | Install relief valve | Relief valve annual testing LOC=4 | Maintenance Dept. testing | Improbable |

# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

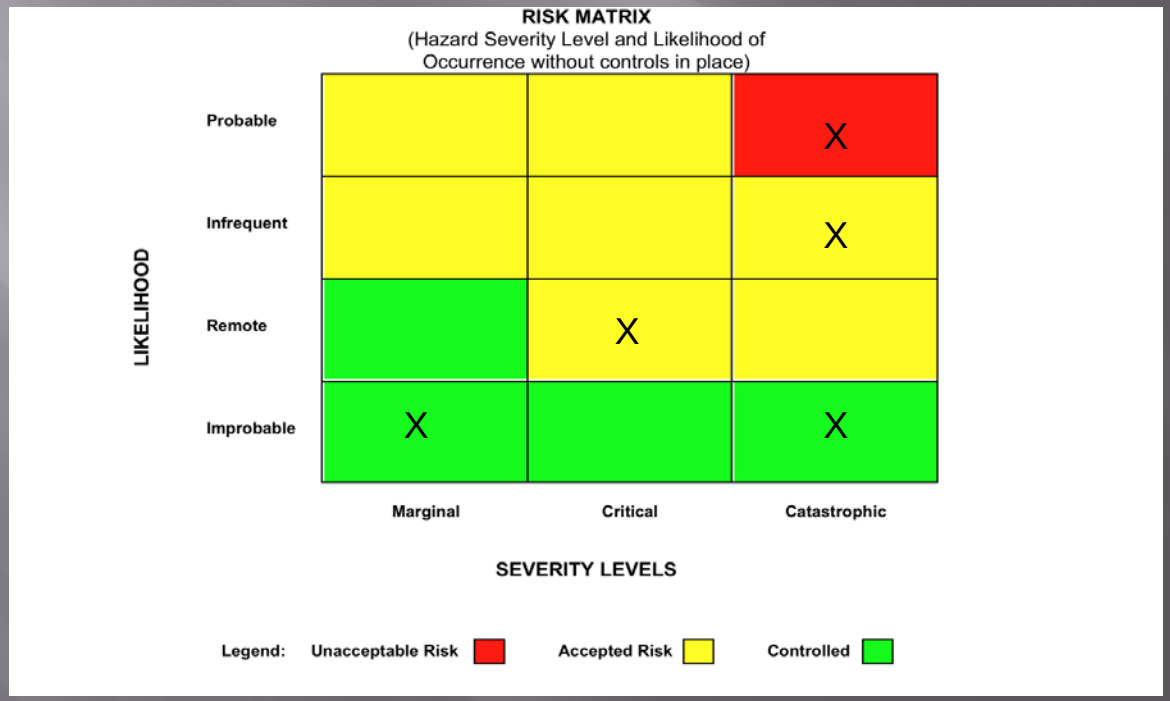
- Transfer the data from the table to a spreadsheet
  - Set up a Sheet that will create a 3-D chart from the information

| SEVERITY | MARGINAL | CRITICAL | CATASTROPHIC |
|---|---|---|---|
| LIKELIHOOD | | | |
| IMPROBABLE | 0a | | 4e |
| REMOTE | | 2b | |
| INFREQUENT | | | 4c |
| PROBABLE | | | 3d |

Figure 9 Microsoft Excel Spreadsheet Screenshot

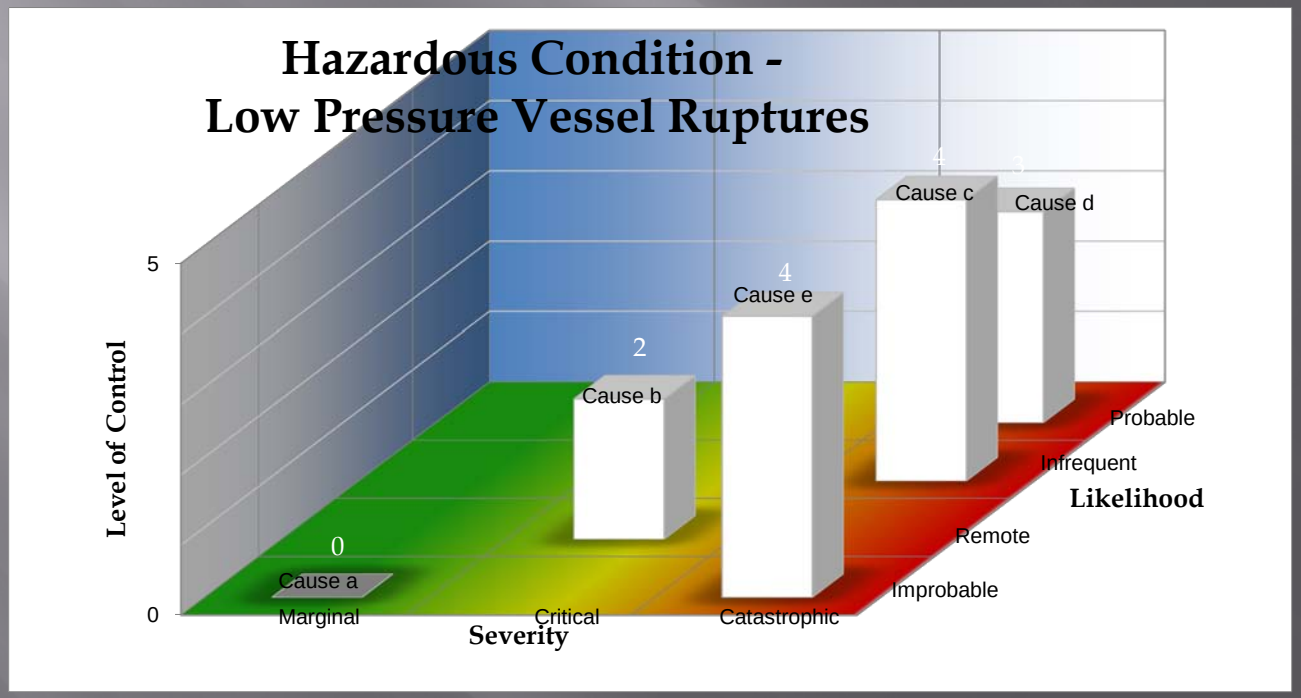
# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- Transfer the data from the table to a spreadsheet
  - This is a traditional two-dimensional matrix
  - Using the definitions for Likelihood, it is possible to identify the Level of Control, but it is not visible in this format



# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- Transfer the data from the table to a Three-Dimensional spreadsheet
  - The data quickly and visibly displays the three elements of Severity, Likelihood, and Level of Control
  - This format permits easy recognition of the ‘tall-poles’ that may be the most likely candidates for additional controls



# RISK ASSESSMENT USING THE THREE DIMENSIONS OF PROBABILITY (LIKELIHOOD), SEVERITY, AND LEVEL OF CONTROL

- Hazard Analyses are an important tool for Management
- Analyses should be able to answer these, and other, questions
  - Is the design adequate for the needs?
    - Is a redesign necessary, or prudent?
  - What are the issues that must be overcome?
  - What will it cost to fix the worst hazardous conditions?
  - How solid are the controls that prevent the hazardous conditions?
  - Is the project worthy of additional time, manpower, and expenditure?

- The Three-Dimensional Risk Matrix will provide visual answers to many of these questions.