RISK SUMMING GUIDEBOOK

Understanding and Implementing Risk Summing as a Practical Element of Risk Management

Document No. CCT1-02000

June 21, 2011

Prepared for:
Concurrent Technologies Corporation (CTC)
101 CTC Drive
Johnstown, PA 15904

Prepared by:
APT Research, Inc.
4950 Research Drive
Huntsville, AL 35805
www.apt-research.com

A-P-T Research, Inc.

CONTENTS

1.0 INTRODUCTION 1
1.1 *Background* 1
1.2 *Rationale* 1
1.3 *Assumptions* 1

2.0 UNDERSTANDING THE ISORISK CONTOUR 2
3.0 IMPROVING CURRENT RISK MANAGEMENT PRACTICE 3
3.1 *Contemporary Practice — Opportunity for Improvement* 3
3.2 *Summing* 4
3.2.1 The Problem—A Statement of Need 7
3.2.2 Desired Characteristics in a Practical Summing Method 8

4.0 RISK SUMMING METHODOLOGY 9
4.1 *Analysis Path (Steps 1 through 6)* 10
4.1.1 Step 1: Define RAC Matrix 10
4.1.2 Step 2: Perform the Hazard Analysis 12
4.1.3 Step 3: Enter Hazards into Matrix 12
4.1.4 Step 4: Compute Partial Risks 13
4.1.5 Step 5: Sum Partial Risks to Compute Total Risk 13
4.1.6 Step 6: Compute Summed Risk Measures 14
4.2 *Management Path (Steps A through C)* 17
4.2.1 Step A: Define Total Risk Criterion 17
4.2.2 Step B: Compare Result to Criterion 19
4.2.3 Step C: Document the Risk Management Decision 19
4.3 *Interpreting Results* 20
4.4 *Potential pitfalls* 23

5.0 APPLYING RISK SUMMING METHODS TO A PRACTICAL EXAMPLE 23
5.1 *Step 1: Define the RAC* 27
5.2 *Step 2: Perform Hazard Analysis* 29
5.3 *Step 3: Enter Hazards in Spreadsheet* 30
5.4 *Step 4: Compute Partial Risks* 32
5.5 *Step 5: Compute Total Risk* 32
5.6 *Step 6: Compute Total Risk Measures* 32
5.6.1 Measure 1: Expected Loss Rate 33
5.6.2 Measure 2: Conditional Loss Rate 33
5.6.3 Measure 3: Risk Profile for Example Activity 34
5.6.4 Maximum Loss (Info Only) 34
5.6.5 Most Probable Loss (Info Only) 35
5.7 *Results Summary—Total Risk Assessment for Example Activity* 38
5.8 *Step A: Develop Total Risk Criteria* 39
5.9 *Step B: Compare Results to Criteria* 40
5.10 *Step C: Document Risk Management Decisions* 40

6.0 SUMMARY/CONCLUDING COMMENTS 40
7.0 REFERENCES 42

Appendix A : Background information
Appendix B : Defining RAC Axes/Scales
Appendix C : Assigning Severity to Human Harm
Appendix D : Hazard Sheets for Fast Asp Example
Appendix E : Chemical Processing Example (with Hazard Sheets)

FIGURES

Figure 1. Isorisk Contour Principle 2
Figure 2. System Safety I-A-R-A Process 3
Figure 3. Basic PHA Information Display 4
Figure 4. Bar Chart Paradigm 4
Figure 5. System Safety Process with Risk Summing 5
Figure 6. Summed Risk 7
Figure 7. Major Steps in Risk Summing Methodology 9
Figure 8. Example Risk Summing Spreadsheet 13
Figure 9. Example Risk Profile 16
Figure 10. Interpreting Risk Results 20
Figure 11. Tailored RAC with Qualitative Ratings, Isorisk Line, and Risk Measures 22
Figure 12. Simplified Fast Asp™ System 24
Figure 13. Fast Asp™ Missile Constraint-Deployment System 24
Figure 14. Selected RAC Axes 27
Figure 15. Probability and Severity Categories 28
Figure 16. Sample Hazard Sheet 30
Figure 17. Example Activity Risk Profile Plot – Initial, Pre-Mitigation 34
Figure 18. Example Matrix (Initial) with Data Selected 36
Figure 19. Computing Combined Probability for Severity Category I 37
Figure 20. Total Risk Results – Initial and Final 39

TABLES

Table 1. Example RAC Severity Definitions (Reference 3; MIL STD 882) 10
Table 2. Example RAC Probability Definitions (Reference 3; MIL STD 882) 10
Table 3. Risk Measures and Associated Questions 14
Table 4. Risk Summing Summary 21
Table 5. Initial Hazard Spreadsheet for Example Activity – partial 31
Table 6. Final (Post-Mitigation) Hazard Spreadsheet for Example Activity – partial 31
Table 7. Bottom Portion of Initial Example Spreadsheet with Total Risk and Risk Measures 32
Table 8. Mishap Probability Data (All Categories) 33
Table 9. Risk Profile Data – Initial, Pre-Mitigation 34
Table 10. Quantitative Results Summary – Total Risk 38

LIST OF ACRONYMS

AIS	Abbreviated Injury Scale
AISS	American Institute of Aeronautics and Astronautics
ATP	Acquisition and Technology Programs
CLR	Conditional Loss Rate
CTC	Concurrent Technologies Corporation
DoD	Department of Defense
DSOC	Defense Safety Oversight Council
ELR	Expected Loss Rate
FMEA	Failure Modes and Effects Analysis
FTCA	Federal Tort Claims Act
IARA	Identify, Assess, Reduce, Accept
MIL-STD	Military Standard
MLE	Maximum Loss Encountered
MPL	Most Probable Loss
PHA	Preliminary Hazard Analysis
RAC	Risk Assessment Code
RCC	Range Commanders Council
SESTC	System Effectiveness and Safety Technology Committee
STD	Standard
TF	Task Force
WOW	Weight on Wheels

GLOSSARY

Definitions are consistent with GEIA-STD-0010 (Ref 6) and MIL-STD-882D (Ref 1).

Π (Ip) – The co-function of pi (Π). It provides an exact solution for propagating probabilities through the OR gate.

Σ (Sigma) – Symbol indicating summation of the numbers or quantities indicated.

Acceptable Risk – That level or residual safety risk that the management authority is will to assume on behalf of the agency, users, and public.

Asset – Something of value. Assets include but are not limited to personnel, facilities, equipment, operations, data, the public, and the environment, as well as the system itself.

Frequency – Rate of mishap occurrence. Frequency is sometimes substituted for probability as a component of risk (example: loss events per 10^6 operating hours).

Hazard – (1) potential for harm; (2) a condition prerequisite to a mishap.

Hazardous – Containing some element of safety risk and capable of inflicting harm.

Life Cycle – All phases of the system's life including concept refinement, technical development, system development and demonstration, production and deployment, operations and support, and disposal.

Isorisk Contour – A tracing of all points having severity and probability coordinates yielding a fixed multiplication product, and displayed in the first quadrant of Cartesian coordinates against axes denoting the severity and probability components of risk. By convention, the Y-axis (vertical) coordinate conveys the severity component or risk and the X-axis (horizontal) coordinate conveys the probability component.

Likelihood – Expected mishap occurrence over a specified exposure interval.

Managing Authority – The entity that has management responsibility for the system.

Mechanism – The process or sequence of event that allows or enables the sources to cause the harm.

Mishap – An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Outcome – The harm that the source brings about through the mechanism to the asset.

Probability – Expressed as a value between zero and one. Probability is a component of risk and has no dimension but must be attached to an interval of exposure (example: one operating year, a mill vehicle miles).

Risk – A measure of the expected loss from a given hazard or group of hazards. Risk is a combined expression of loss severity and probability (or likelihood). When expressed quantitatively, risk is the simple numerical product of severity of loss and the probability that loss will occur at that severity level.

Risk Assessment – The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probability (or lielihooe0 of occurrence, and prioritizing them for risk mitigation actions.

Safety – Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Severity – An assessment of the potential degree of harm from a mishap. Severity is one component of risk.

Single hazard risk (r) – Risk associated with a single hazard of the system. A single hazard risk is typically y characterize by a severity-probability pair, assessed using a mishap risk assessment matrix.

Source – an activity, condition, or circumstance that has the potential to do harm to an asset.

System – An integrated composite of people, produces, and processes that provide a capability to satisfy a stated need or objective.

System safety – The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, with within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

System safety engineering – An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria and techniques to identify and eliminate hazards, in order or reduce the associated mishap risk.

Total Mishap risk (R) – An expression of overall system risk, comprising the combined separate properties of all partial risks.

PREFACE

Risk Summing ideas and techniques applied in routine system safety practice date back to 1972. This document incorporates some of the early concepts and strategies. Appendix A provides in-depth details of the early research and case studies used as a basis for this document. Specifically, Appendix A provides a summary of 1) comprehensive principles of System Safety (Lüsser's Law), 2) American Institute of Aeronautics and Astronautics/System Effectiveness and Safety Technical Committee (AISS/SESTC) Summary, and 3) a summary of the 2005 International Risk Summing Workshop.

1.0 INTRODUCTION

1.1 BACKGROUND

Department of Defense (DoD) readiness is enhanced significantly by sustainable practices in everyday military and civilian activities. Through its Task Forces and in response to the challenge from the Secretary of Defense's to reduce mishaps by 75%, the Defense Safety Oversight Council (DSOC) has identified a variety of initiatives to aid DoD commanders in their mishap prevention efforts. These initiatives constitute a broad base of approaches to reducing mishaps.

This document was generated in response to an Acquisition and Technology Programs (ATP) Task Force (TF)-sponsored initiative for Developing a Risk Summing Guidebook.

Summation of partial risks gives an engineering approach to supporting purposes of practical risk management. Risk summing is easily carried out for cases in which partial risks are quantitatively expressed. However, summing is frustrated by the non-numerical nature of risk assessments resulting from subjectively scaled matrices used in many assessments. Resolving this problem would enable risk acceptance authorities to judge the acceptability of system risk based on its true total value rather than on a view of the many individual partial risks embedded within the system. The focus of this initiative and Guidebook is to improve application of MIL-STD-882 (Reference 1) by providing guidance and techniques that lead to assessing the total risk of a system rather than evaluating only an inventory of partial risks.

1.2 RATIONALE

System safety, in majority practice, does not assess system risk. Instead, as most often applied, system safety subjectively assesses the separate partial risks of individual hazards identified as posing risk to valued assets. Risk acceptance authorities then judge the acceptability of whole system risk based exclusively on their consideration of these numerous partial risks. As a result, systems are committed to operation with acceptance of whole system risk but without knowledge of its overall value. This shortcoming has long been recognized, but has gone without remedial attention in the standards guiding practice of the discipline. In 2005, an international risk summing workshop arrived at consensus on criteria for a risk summing method (Reference 2). Such a method, now developed and described herein, satisfies requirements for simplicity, universal applicability, and interpretability of results. In addition to summing, it prescribes a family of aids for characterizing and interpreting total system risk. Opportunities for conservation of resources while lowering overall system risk are also made apparent. Application of the method is readily mastered. This Guidebook describes the method and guides users in applying it.

1.3 ASSUMPTIONS

This guidebook addresses a technique for summing total system risk. It is assumed that the guidebook user understands processes for identifying, mitigating, and tracking hazards. These topics are not covered in this document. It was decided however to provide a summary of the isorisk contour principle, found here in Section 2.0. Specific assumptions relating to methods, calculations, and equations are noted in the applicable Guidebook sections.

2.0 UNDERSTANDING THE ISORISK CONTOUR

The concept of the isorisk contour supports many risk management tools. An isorisk contour is a planar tracing of all points having severity and probability coordinates yielding a constant multiplication product and displayed in the first quadrant of Cartesian coordinates having axes denoting the severity and probability risk components. By convention, the Y-axis (vertical) coordinate conveys the severity component of risk and the X-axis (horizontal) coordinate conveys the probability component.

Thus, risk has a constant value at every point along an isorisk contour. Isorisk contours are:

a. Hyperbolas plotted in the first quadrant of classical Cartesian coordinates. (Most risk assessment matrices in current use appear in the second quadrant, defying a long-established engineering convention.)

b. In the mathematical form R = S × P, with R as risk, S as severity, and P as probability.

c. Useful aids in identifying risk allowances.

For many hazards, risk is greatest neither at the point of greatest severity nor of greatest probability. It is more rational to assess risk at its own *greatest* value i.e., a point at which the hazard risk characteristic is tangent to the isorisk contour for which hazard risk is greatest. Figure 1 illustrates the principle. Note that isorisk contours, which appear as hyperbolas when plotted against linearly scaled axes, become straight lines when displayed against log-log axes.

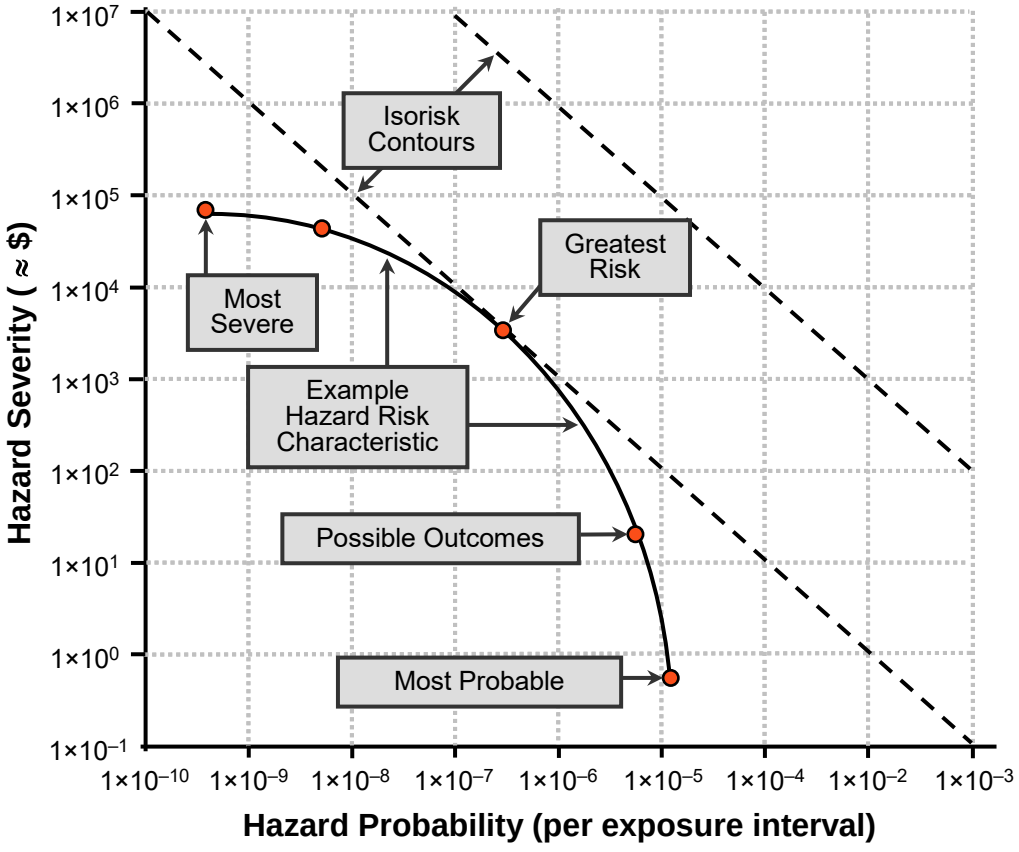


Figure 1. Isorisk Contour Principle

3.0 IMPROVING CURRENT RISK MANAGEMENT PRACTICE

The discipline of system safety is practiced throughout DoD and industry as an application of risk management. The Top Level Risk Management approach used has been characterized in numerous ways and in many standards covering many disciplines, e.g. explosives safety, range safety, occupational safety, insurance. Elements common to all of these applications are the minimal essential requirements of Risk Management: 1) Identify hazards and the assets they threaten; 2) Assess Risks, 3) Reduce Risks, and 4) Accept Risks. This is commonly referred to as the —I-A-R-A" approach as shown in Figure 2.

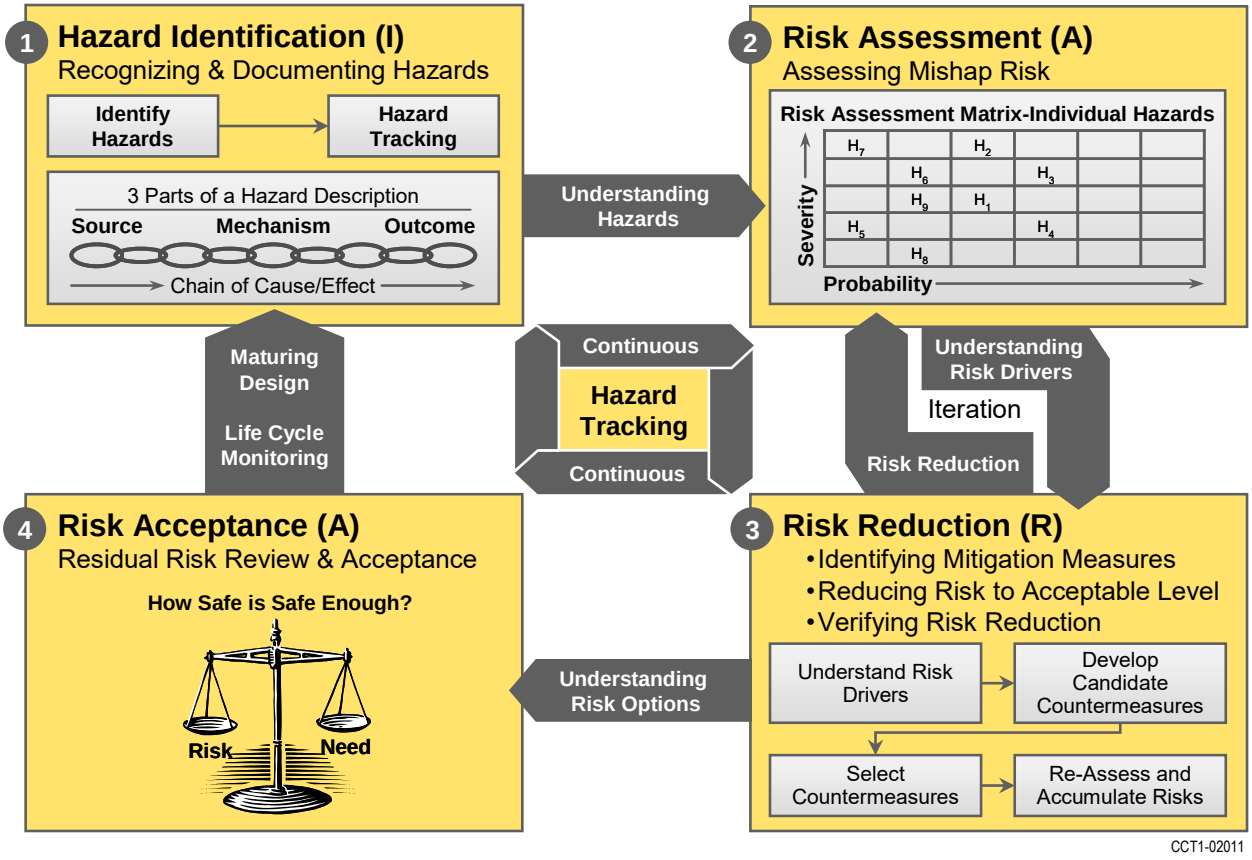


Figure 2. System Safety I-A-R-A Process

This document describes methods that can substantially improve this process in several ways. The basis of the improvement begins at Element 2 (Assess Risks) where methods are defined to calculate total system risk (characterized by R_T) by summing the risk from discrete partial hazards (characterized as r). The benefit of these calculations manifest itself at Element 3 (Reduce Risks) where an understanding of total system risk can lead to an optimum allocation of resources to reduce system risk and at Element 4 (Accept Risk) where decision makers have more complete information to form the basis of their risk acceptance decisions.

3.1 CONTEMPORARY PRACTICE — OPPORTUNITY FOR IMPROVEMENT

Basic system safety practice, viewed as a process and as customarily carried out, is performed as represented in Figure 2. Hazards are first identified using the myriad methods described in texts and standards. The risk posed to assets of concern by each of these hazards is then assessed, most

often using the analyst's judgment along with the subjective scales found together with risk assessment matrices. For those hazards posing risk that exceeds acceptance levels prescribed by the matrices, risk reduction measures are imposed. This assessment-reduction process is continued iteratively until a satisfactory resolution of excess risk is realized for each hazard.

The result of this process is a line-item inventory of identified system hazards together with their individual assessments of risk. Figure 3 provides a greatly simplified example; many other details may be included in such a display, but they do not influence the purposes here. The form of Figure 3 is that of a Preliminary Hazard Analysis (PHA). It differs only in its display format from the analytical result provided by a Failure Modes and Effects Analysis (FMEA). In FMEA parlance, the line item analyzed is analogous to the PHA *source*, the failure mode becomes the PHA *mechanism*, and the effect is the PHA *outcome*.

Hazard No.	Hazard Description	Severity s_i	Probability p_i	Risk r_i
1		IV	C	IV / C
2		III	C	III / C
3		IV	D	IV / D
4		I	B	I / B
5		II	E	II / E
n	?	?	?	?

CCT1-02012

Figure 3. Basic PHA Information Display

Results of the data display seen in Figure 3 may be represented as shown in Figure 4. Here, the risks of the individual hazards are plotted as a bar chart. Risk for Hazard 4 extends above the tolerance limit and would be scored as unacceptable by most risk assessment matrices. Further mitigation of Hazard 4 would be required. Final post-mitigation risk would be recommended in columns not shown in Figure 3.

It is important to recognize that throughout this process, contemporary standard practice has been represented. Hazards and their individual partial risks have been treated exclusively as stand-alone, line-item entities. It is upon this hazard-by-hazard risk assessment that the risk acceptance authority must make a decision as to the acceptability of total system risk.

3.2 SUMMING

The Approach

Summing partial system risks to produce a system total provides a remedy for the problem described above. Figure 5 differs from Figure 2 only by the addition of the step labeled "Risk Summing," seen in the Risk Assessment step. Inserted at this point, summing system risk provides the analyst and the risk manager an opportunity to appreciate both the complete inventory of partial risks and the effect of their individual contributions to the summed total.

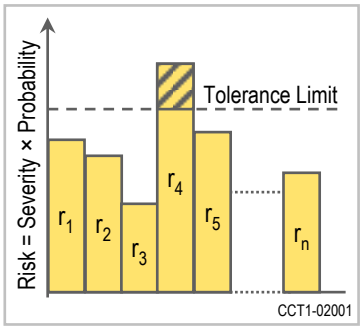


Figure 4. Bar Chart Paradigm

The result of summing of individual partial risks may be viewed as shown in Figure 6. Here, the partial risk bars from the display of Figure 4 have been arranged end-to-end to reveal their overall magnitude. Their sum is also described by the formula shown there.

Figure 6 provides a reminder that the unseen total risk posed by a system may be alarmingly large by comparison with the individual risks of the contributors to that total. Put realistically, the prevailing practice of viewing risk only on a partial-risk-by-partial-risk basis gives the analyst and decision maker an optimistically skewed view of system risk. The effect displayed in Figure 6 is never drawn to the attention of those who would benefit by realizing the sum of total system risk; they are constrained to view system risk only by incremental bites.

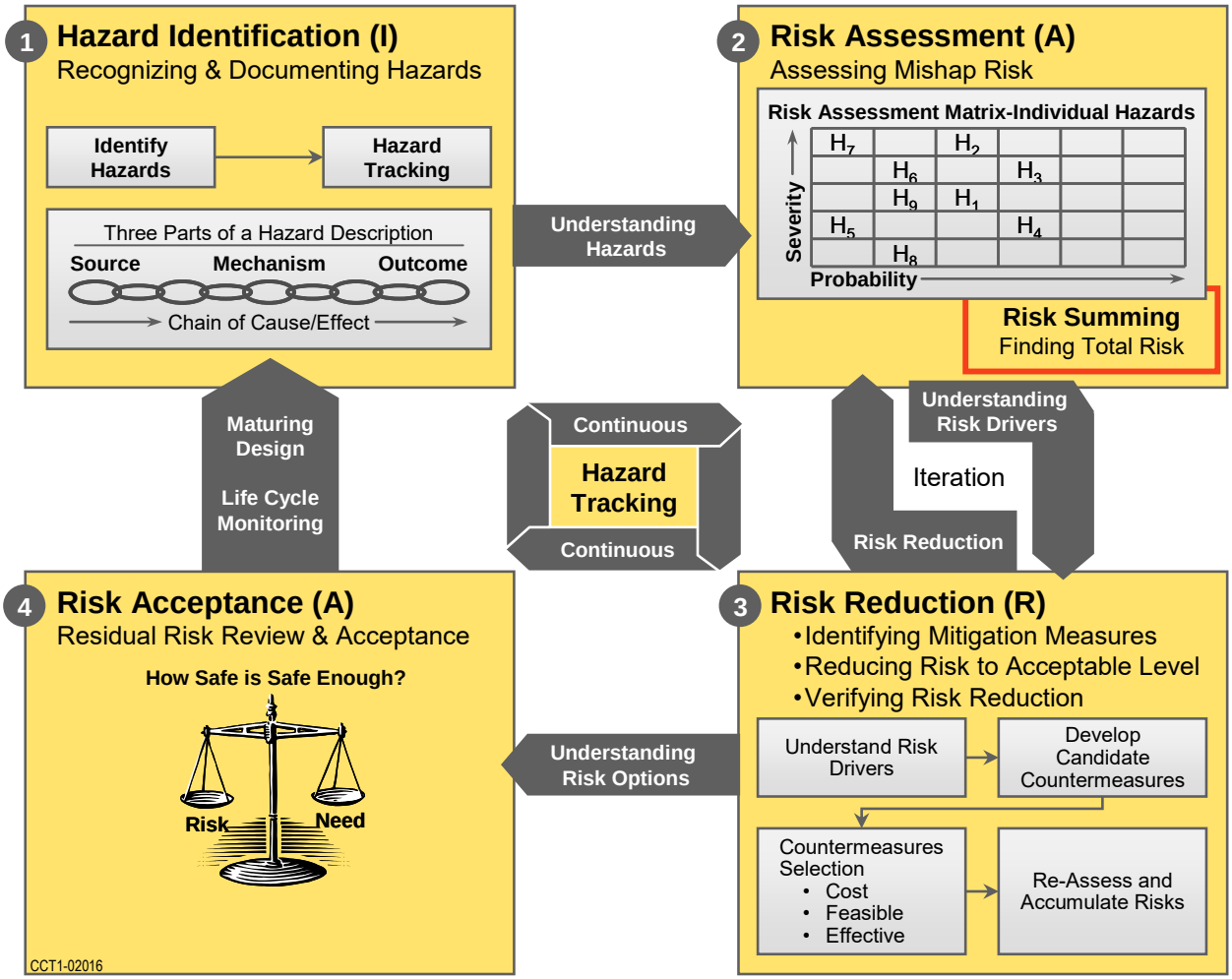


Figure 5. System Safety Process with Risk Summing

An Economic Advantage

The result modeled in Figure 6 makes apparent one of many advantages of risk summing apart from affording an opportunity to appreciate whole system risk. Notice that reducing the risk of Hazard 4 to a tolerable value would cost an estimated $437,000. Hazard 1, with risk that is now considered acceptable, can be eliminated altogether at less than one tenth of the cost of mitigating Hazard 4. The risk posed by Hazard 1 greatly exceeds the Hazard 4 overage. Eliminating Hazard 1 becomes the obvious preferred choice if concern for reducing overall system risk is paramount. The resources conserved, $414,000 in the case illustrated here, might also be applied to reducing risk among other hazards. If a total-risk viewpoint is made available

to the analyst and the risk acceptance authority, trade opportunities of this kind become dramatically evident. Reference 3 elaborates further on this phenomenon.

The Complete Mathematical Expression

Figure 6 includes an expression for the total of the partial risks shown there for this elementary example:

$$R_T \approx \sum_{i=1}^{i=n} r_i = r_1 + r_2 + r_3 + \ldots + r_n \quad [1] \qquad \text{(Eq 1)}$$

where:

R_T = Total Risk
r = Partial risk = Hazard Severity × Hazard Probability

This equation can be expanded to accommodate risk for numerous threatened assets exposed in varied operational or mission phases:

$$R_T \approx \sum_{i=1}^{i=n} M_i \sum_{i=1}^{i=n} A_i \sum_{i=1}^{i=n} (r_i = s_i \times p_i) \qquad \text{(Eq 2)}$$

where:

R_T = Total Risk
s_i = Hazard Severity for the i^{th} identified hazard
p_i = Hazard Probability for the i^{th} identified hazard
r_i = Risk posed by the i^{th} identified hazard
A_i = Identity of the i^{th} asset under threat
M_i = The i^{th} system Mission or Operational Phase under consideration

As can be seen, applying this equation to a family of identified system hazards results in assessing their summed total risk, taking into account both the threats they pose to multiple assets (A) and their appearance in multiple operational phases (M).

Assumptions Made

Three important assumptions are made in applying the approach implicit in Eq 2.

It is assumed that all identified hazards are statistically independent, meaning simply that no identified hazard can cause nor be caused by another. The manner in which hazards are conventionally expressed in hazard lists and hazard descriptions provides protection against this. Hazards that are not statistically independent are readily recognized and merged or dissociated.

Multiple hazards within a system sometimes share a common outcome. Because partial risks that form these Boolean unions are simply summed, an error arises in the final total probability for that shared outcome. This error, however can be assumed to be both quite small (i.e., much

[1] The approximate expression shown here is used throughout in the interest of simplicity. Its use produces a numerical result that is very slightly larger in value – i.e., pessimistic – when compared to an exact solution. Such substitutions, often used in system safety practice, are known as ―rare event approximations.”

smaller than errors introduced in making probability estimates) and pessimistic (i.e., producing larger rather than smaller values of total probability). The procedure is akin to the rare event approximations made in summing fault tree OR gated probabilities. This matter is discussed further in Reference 3, sheets 87-5 and 87-6. Moreover, studies have shown that first-pass analyses using such line-item methods as preliminary hazard analysis leave 20-40 percent of system hazards undiscovered (Reference 4). Pessimistic errors can partially offset this deficiency.

It is axiomatic that the sum of all system partial risks cannot be found unless all system hazards have first been identified. This logic would seem to be of trivial importance. However, recent work has shown than it is rare for more than 80% of the total of all significant system hazards to have been identified prior to committing a system to service. This matter is discussed at length in Reference 5, where recommended means to combat the problem also appear.

3.2.1 The Problem—A Statement of Need

Because each system hazard is dealt with singly in predominant current practice, the system designer, the system safety analyst, and later, the risk acceptance authority, all view system risk only on an item-by-item and asset-by-asset basis. This complete array of partial risks is then viewed as to its acceptability on the presumption that if risk is acceptable by parts, it is therefore acceptable in toto (Reference 5). While this approach is often mistaken for thoroughness, it is in fact quite misleading. It can end in adopting a viewpoint that a system's overall risk can be made to appear acceptable if its partial risks can be assessed at a systemic level sufficiently low that the combined severity and probability of each gives an acceptable result.[2] Figure 4 stands as a pictorial view of this paradigm. It is a view that true system nature does not see.

Figure 6 portrays a paradigm for the view of total system risk as seen by a viewer of true system nature. Here, the bars for item-by-item risk are stacked end-to-end to produce a representation of total system risk.

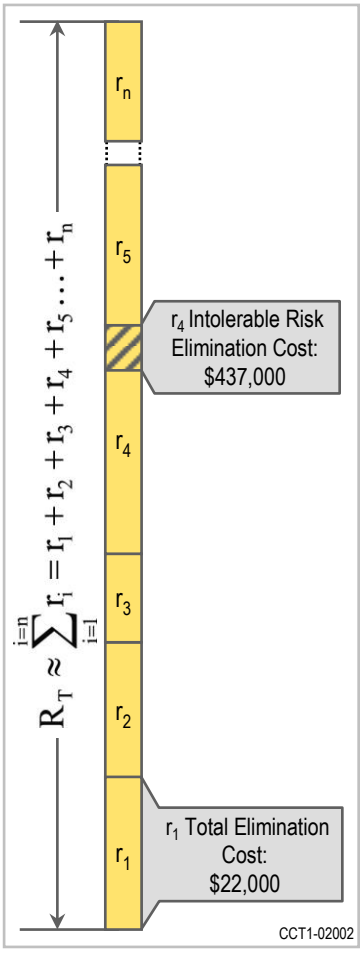


Figure 6. Summed Risk

[2] Also a threat to reason is the view that if risk is acceptable for one system of a particular kind, it is therefore equally acceptable for an entire inventory of many such systems. No insurer of taxicabs would accept the argument that the premium for a fleet of twenty cabs should be no greater than that for a single cab simply because they are all alike.

3.2.2 Desired Characteristics in a Practical Summing Method

Safety tools, methodologies, and approaches should satisfy numerous shared characteristics. Several are described below to encourage their use in both developing and applying the methodologies provided in Section 4.0.

3.2.2.1 Ease of Use

Safety practices can only gain widespread acceptance and application if the methodologies used are readily understood by new practitioners. The risk summing concept is no exception. This Guidebook's primary purpose is to enhance the reader's understanding of, and ability to apply, the techniques described here.

3.2.2.2 Defining Total Risk

The stated purpose for summing risk is to determine the combined effect of all identified hazards on the risks posed by a system or activity. To fulfill this purpose, the technique used to sum risk must aggregate estimates of potential losses for all identified system risks to produce a numerical result that represents the total risk due.

3.2.2.3 Directly Calculable, Producing Unique Result

The methodology used to sum partial risks should be structured to directly follow a hazard analysis as commonly practiced. The technique should be able to ingest both qualitative and quantitative risk results as inputs and should produce a single, numerical result in units that are commonly understood to represent the combined cost and probability of losses incurred.

3.2.2.4 Characterizing Total Risk in a Practical Way

The results obtained by applying risk summing techniques should provide the answers sought by those having the responsibility to make risk management decisions. In some instances, this requires that the results provide a valid estimate of one or more risk measures contained in established risk acceptability criteria. In other situations, the risk manager may request results that answer specific questions such as:

- *What is the total system risk (R_r) throughout the full life cycle (or within particular operational phases)?*
- *If a fleet of this system is operated, what will be the average loss per system operating life due to loss events?*
- *On average, how much will be lost if a mishap occurs?*
- *What is the probability that some loss event will occur as the result of this activity?*
- *What is the worst loss event that can occur if this system is operated or this activity is conducted?*
- *What is the most likely loss event if this system is operated or this activity is conducted?*

Several risk measures will be needed to communicate the total risk in ways that answer each of these questions. These measures are described in Section 4.1.1 and are illustrated by a worked example in Section 5.0.

3.2.2.5 Interpretability

Each method used to express total risk should clearly state that risk in units that communicate the potential impact that loss events might have on the hazardous activity. If key codes or interim translation is required for the result to have meaning, understanding is lost and with it a degree of usefulness.

3.2.2.6 Broad Applicability

The methodologies used for risk summing, like those used in hazard assessment, should be applicable across the widest possible range of systems and activities. Activities such as explosives handling, composite material manufacturing, flying experimental aircraft, and chemical processes vary immensely in many respects. The tools used to identify their hazards and assess their risks, however, should not. The practitioner who masters risk summing should have a skill that can be applied to any system or activity envisioned by an organization.

4.0 RISK SUMMING METHODOLOGY

The major steps in performing risk summing are presented in Figure 7. The figure separates the process into two complementary paths. The analysis path (labeled Steps 1 through 6) shows the effort required to complete the hazard identification and risk analysis. The management path (labeled Steps A through C) describes the top-level management actions required to incorporate summed risk into the risk management process. The steps are described individually in the sections that follow.

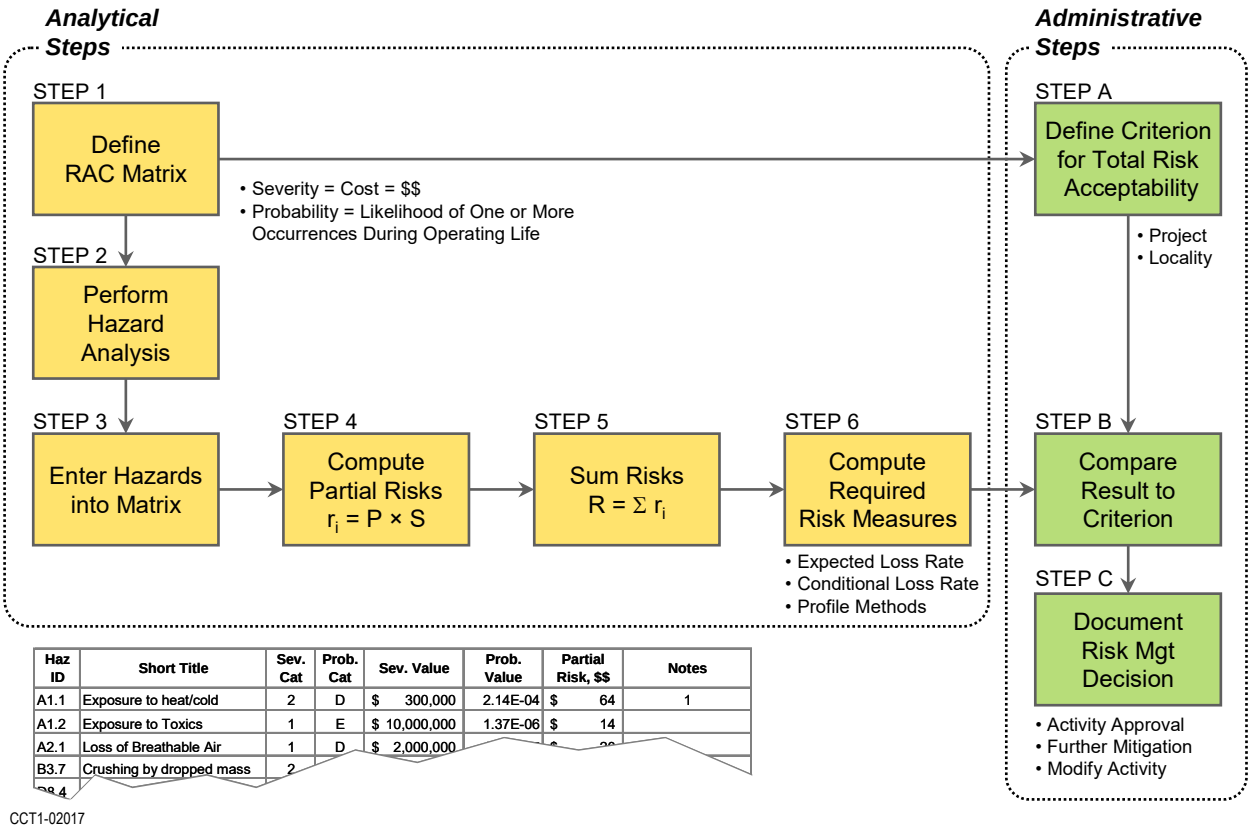


Figure 7. Major Steps in Risk Summing Methodology

4.1 ANALYSIS PATH (STEPS 1 THROUGH 6)

4.1.1 Step 1: Define RAC Matrix

Prior to performing the traditional hazard analysis element of the system safety program, the project manager should approve the Risk Assessment Code (RAC) matrix to be used. Examples are provided in MIL-STD-882D and that Standard explicitly approves project-specific tailoring. ANSI/GEIA STD-0010, Reference 6, provides a RAC matrix description and tailoring guidance if additional support is needed. RAC matrices define risk using two axes: probability and severity. Each axis is divided into categories that define differing levels of these two risk components. Table 1 and Table 2 provide typical category definitions taken from MIL-STD-882D examples. Matrix tailoring, then, is done by crafting the descriptions and numerical boundaries of the RAC probability and severity categories consistent with the unique aspects and needs of the project under evaluation.

Several characteristics are critical to successful risk summing. Other non-critical characteristics have been identified as desirable best practices. These are enumerated in the sections that follow.

Table 1. Example RAC Severity Definitions (Reference 1; MIL STD 882)

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 day(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.

Table 2. Example RAC Probability Definitions (Reference 1; MIL STD 882)

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 that 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
Improbably	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

To facilitate risk summing within the existing system safety management scheme, the Risk Assessment matrix must have quantitative scales for severity and probability. A detailed description of the method for developing a risk matrix of this type is found in Reference 6.

4.1.1.1 Critical RAC Qualitative Characteristics Supporting Risk Summing

The following guidelines assist in the definition of probability and severity categories in a manner that supports computing summed risk measures:

a. Probability categories must have numerically defined upper and lower boundaries, as well as a central value. The central value would typically be a proportional "middle" of the range—the same factor higher than the floor as it is lower than the ceiling. This value is commonly labeled the "geometric mean" or "logarithmic average" and is calculated as:

$$\sqrt{\text{Lower Boundary} \times \text{Upper Boundary}} \qquad \text{(Eq 3)}$$

b. Likewise, severity categories must have numerically defined upper and lower boundaries and a central value expressed in the same unit across all assets. Unless special care is taken in performing computations, the same severity categories and numerical values must be applied to all assets evaluated. Appendix C provides further discussion related to the units used for human harm.

c. Although one axis is traditionally labeled "probability," in practice it more closely resembles an "expected value" and is freely allowed to exceed a value of 1.0. This freedom is especially important when assessing systems expected to experience numerous loss events during an extended operating life. Aircraft systems, for example, anticipate multiple loss events during each exposure period (analyses typically use an exposure interval of 100,000 flight hours for the operating period of interest).

d. For a number of reasons, zero should not be used as the lower limit for either probability or severity. A zero boundary poorly supports common methods for determining the central value. In addition, zero values cannot be plotted on logarithmic scales that will be used to plot RAC categories, partial risk contributions, and summed risk results.

4.1.1.2 RAC "Best Practices"

Additional RAC characteristics that are desirable even though they are not strictly required to perform the remainder of the risk summing methodology described in Section 4.0. These include:

a. Proportionally equal category widths for both the probability and severity axes. This means that the upper bound divided by the lower bound is constant for each category used. Traditionally, most categories have spanned a factor of 10 from lower bound to upper bound. Polls have shown that most practitioners prefer this scaling (Reference 7).

b. Axes defined so that larger values of probability and severity are farther away from the origin (forming a Cartesian system). This approach pushes the highest risk hazards toward the upper right of the plot, making the plotting and comparison of hazard risks and summed risk measures more intuitive.

4.1.2 Step 2: Perform the Hazard Analysis

After the RAC matrix to be used is selected, a thorough hazard analysis is performed in accordance with applicable system safety program requirements such as MIL-STD-882D (Reference 1) or GEIA-STD 0010 (Reference 6). Though the hazard analysis is a prerequisite, this Guidebook will focus on the core tasks for summing risks rather than providing a detailed hazard analysis tutorial. Numerous resources, standards, and training classes are available to assist in understanding hazard analysis requirements and processes. Following a few guidelines associated with this step, however, may simplify the risk summing process, while making the results more useful:

a. Develop thorough understanding of the system, bearing in mind that it is never the system itself that is analyzed. Instead, it is an analytical model developed from a conceptual model (Reference 8).

b. Consideration should be given to performing a quantitative probability assessment for medium-to-high severity hazards for which credible analytical approaches are available and feasible. Using calculated probability values rather than the geometric mid-point of a probability category in risk summing is easily done by simply entering the assessed probability value in Column F of the matrix described in Section 4.1.3.

c. The risk summing techniques described in Steps 4 through 6 should be performed both prior to and following hazard mitigation. The change in summed risk due to mitigation actions provides a useful measure of their combined effectiveness in improving safety.

4.1.3 Step 3: Enter Hazards into Matrix

Steps 1 and 2 can be viewed as data gathering actions supporting total risk computation. In Step 1, developing the RAC matrix is akin to selecting the system of units in which measurements are taken. In identifying and assessing system hazards, Step 2 measured each of the system's individual risk components. Upon completion of the hazard analysis using a "risk summing friendly" RAC matrix, the data necessary to compute summed or total risk are ready.

This step can be considered the "data entry" step. Required information for each hazard is entered into a computational tool to facilitate computing the total risk and the associated summed risk measures. A Microsoft Excel® spreadsheet similar to the one shown in Figure 8 should be formatted to receive required data. As a minimum, the matrix should include an alphanumeric identifier that is unique to each hazard, a short title, the RAC severity and probability categories, numerical values for each severity and probability, and a column for the computed partial risk associated with each hazard.

A	B	C	D	E	F	G	H
Haz ID	**Short Title**	**Sev. Cat**	**Prob. Cat**	**Sev. Value**	**Prob. Value**	**Partial Risk, $$**	**Notes**
A1.1	Exposure to heat/cold	2	D	$ 300,000	2.14E-04	$ 64	1
A1.2	Exposure to Toxics	1	E	$ 10,000,000	1.37E-06	$ 14	
A2.1	Loss of Breathable Air	1	D	$ 2,000,000	1.00E-05	$ 20	
B3.7	Crushing by dropped mass	2	C	$ 300,000	5.16E-04	$ 155	1
D8.4	Laceration	4	B	$ 2,000	1.00E-03	$ 2	
			Expected Loss Rate	$ 255	1.00E+00	$ 255	**Total Risk**
			Conditional Loss Rate	$ 146,264	1.74E-03		
			Maximum Loss	$ 10,000,000	2.55E-05		
			Most Probable Loss	$ 254,700	1.00E-03		

Notes:

1	Probability value determined by Probabilistic Risk Analysis (Report # TR-09-01103)

Figure 8. Example Risk Summing Spreadsheet

In addition, it is recommended that an opportunity to enter notes or comments be provided. At the bottom of the matrix, a cell should be provided in which to sum the partial risks of the identified hazard producing the total risk, and cells for computing the components of each risk summing measure, as described in Section 4.1.6. The approach and equations used to compute these values are provided in Sections 4.1.4 through 4.1.5.

For the Guidebook user's benefit, the link below provides a spreadsheet configured to automatically calculate the four risk measures and the resulting risk profile based on data entered by the user. Calculating Spreadsheet.

4.1.4 Step 4: Compute Partial Risks

The partial risk posed by each identified hazard is the simple product of the expected loss incurred if the hazard produces a mishap and the assessed probability that a loss event will occur. In Figure 8, the partial risk is computed in Column G by multiplying the entries in Columns E and F for each hazard.

$$\text{Partial Risk} = \text{Severity} \times \text{Probability} \qquad \text{(Eq 4)}$$

4.1.5 Step 5: Sum Partial Risks to Compute Total Risk

The total risk posed by all applicable system hazards is the simple sum of all partial risks computed in Step 4. In Figure 8, the total risk is computed at the bottom of Column G by summing all values above the total risk cell.

$$\text{Total Risk} \approx \sum \text{Partial Risks} \qquad \text{(Eq 5)}^{3}$$

[3] The expression shown here is used throughout in the interest of simplicity. Its use produces a numerical result that is very slightly larger in value – i.e., pessimistic – when compared to an exact solution. Such substitutions, often used in system safety practice, are known as ―rare-event approximations."

4.1.6 Step 6: Compute Summed Risk Measures

While the Total Risk computed in Section 4.1.5 is the primary summed risk measure used to determine acceptance, the International Risk Summing Workshop identified five approaches for communicating and displaying total risk using a RAC matrix. These were subsequently described in a paper published in the Journal of System Safety, Reference 2. Of these five, three have been selected for inclusion in the Guidebook due to their direct applicability to risk management and are described in the sections below. The remaining two measures, Maximum Loss and Most Probable Loss, can easily be determined from the data used to compute Total Risk and provide useful information if needed. The example worked in section 5 calculates these measures for completeness.

Each of these three techniques develops probability-severity (P-S) pairs that represent the total risk from a unique perspective. The sections that follow describe the risk measures providing answers to the questions posed in Table 3.

Table 3. Risk Measures and Associated Questions

Section Measure	Answers the Question:
4.1.6.1 Expected Loss Rate	If a fleet of this system is operated, what will be the average loss per system operating life due to loss events?
4.1.6.2 Conditional Loss Rate	On the average, how much will be lost if a mishap occurs?
4.1.6.3 Risk Profile Methods	What is the probability that some loss event will occur as the result of this activity?

The sections below describe three total risk measures and provide the equations used to compute them. The total risk computed in Step 5, above, forms the basis for each risk measure described in the sections that follow. Section 5.0 uses a worked example to further illustrate the process for computing these measures.

4.1.6.1 Total Risk Measure 1: Expected Loss Rate

The Expected Loss Rate is the average loss per system life cycle that would be realized if numerous copies of the system were operated for one or more system life cycles. This measure answers the question, *"If a fleet of this system is operated, what will be the average loss per system operating life due to loss events?"*

To form the P-S pair associated with the Expected Loss Rate, the Probability (P) component is set to unity (1.0) since this measure represents the loss level expected every time the system is operated for the system life. The Severity (S) component is then the Total Risk divided by 1.0.

4.1.6.2 Total Risk Measure 2: Conditional Loss Rate

The Conditional Loss Rate measure is determined by assuming that some mishap results in a loss and then computing the conditional Expected Loss Rate based on that assumption. The result is mishap probability paired with the expected loss, given that a mishap has occurred. This measure answers the question, *"On average, how much will be lost if a mishap occurs?"*

The probability component of this measure is computed by determining the summed probability that a loss event occurs during the system lifetime. In academic terms, this is most rigorously computed as the probability of one or more loss events, which is equivalent to one minus the

probability that no loss event occurs. In equation form, the probability component is calculated as:

$$P_{CLR} = 1.0 - \Pi\left[1.0 - P_{hazard}\right] \quad \text{(Eq 6)}$$

where P_{hazard} denotes the probability that an individual hazard produces a mishap and the symbol Π denotes the product across all hazards. In many cases, the rare event approximation would reasonably permit computation of P_{CLR} by simply summing the individual hazard probabilities:

$$P_{CLR} \approx \sum P_{hazard} \quad \text{(Eq 7)}$$

This simplification always generates a higher probability value than the first equation. In many instances, a higher probability value would be viewed as desirably *pessimistic,* or *safe-sided*. The result here, however is that the elevated probability component of Conditional Loss Rate results in an underestimation of its severity component. For this reason, the second equation should only be used when the probability assigned to each hazard is low and the total number of hazards identified is not excessive. These conditions limit pessimism in the probability component and the degree to which severity is underestimated.

The severity component of this measure is computed as the effective severity required to produce the total risk when paired with P_{CLR}. It is computed using the equation:

$$S_{CLR} = \frac{\text{Total Risk}}{P_{CLR}} \quad \text{(Eq 8)}$$

4.1.6.3 Total Risk Measure 3: Risk Profile Methods

Risk profile methods provide a convenient way to display the combined probabilities of hazards within the same severity category. A hazard-based RAC plot may show multiple hazards plotted in the same probability-severity category grid. Risk profiles compute the mishap probabilities posed by all hazards within each severity category so that a single P-S point can be plotted. By plotting the points for each severity category, a —profile" is produced that envelopes the total probability for each severity level. This methodology answers the question, —*What is the probability that some loss event will occur as the result of this activity?"*

Two types of profiles are shown in Figure 9, a standard risk profile (blue) and a cumulative profile (fuchsia). The methods used to generate these are described in the subsections that follow. The figure also illustrates the total isorisk contour and the total risk measures previously described in Sections 4.1.6.1 through 4.1.6.2.

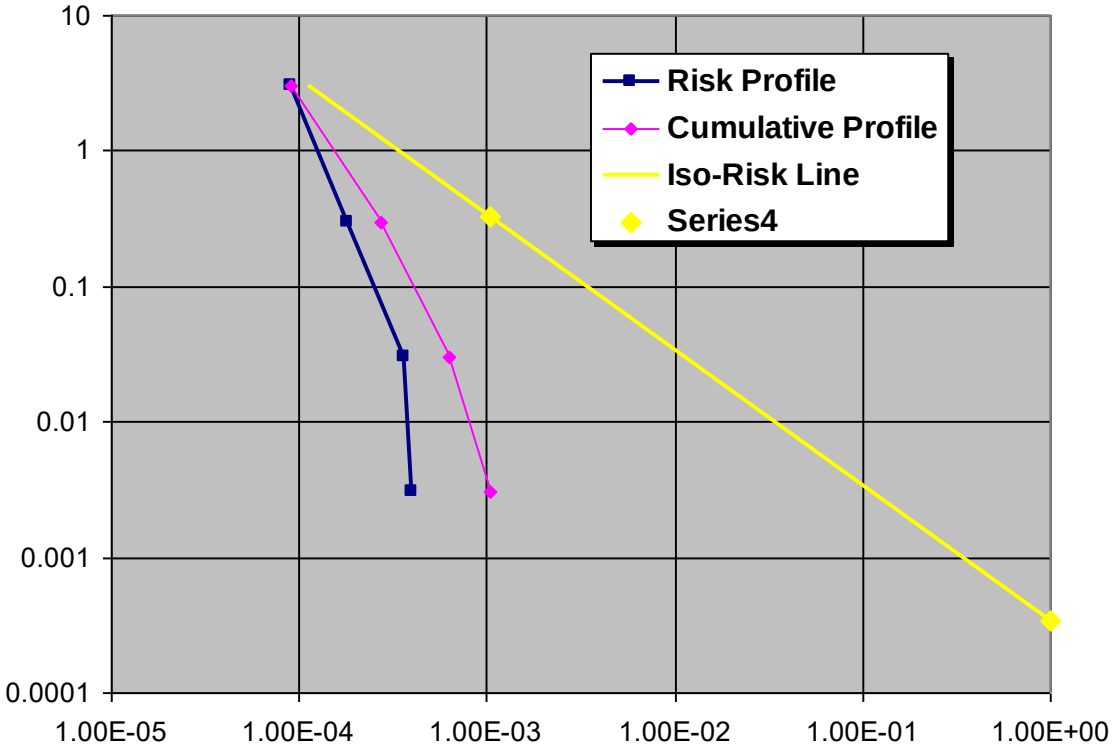


Figure 9. Example Risk Profile

4.1.6.3.1 Discrete Risk Profile

The steps performed to generate a risk profile are:

a. Complete Steps 1 through 3 as described in Sections 4.1.1 through 4.1.3.

b. Format a plot that encompasses the numerical values of the RAC matrix developed in Section 4.1.1, having probability as the *x*-axis and severity as the *y*-axis.

c. Aggregate the frequencies/probabilities of all hazards in the highest severity category using the approach shown in Section 4.1.6.2 (Conditional Loss Rate) and plot this point using the summed probability as the *x* coordinate and the center of the severity category as the *y* coordinate.

d. Repeat Step b for each severity category down to the most insignificant, plotting each point in turn.

e. Connect the points to produce the standard risk profile.

4.1.6.3.2 Cumulative Profile

To generate a cumulative profile:

a. Complete Steps 1 through 3 as described in Sections 4.1.1 through 4.1.3.

b. Format a plot that encompasses the numerical values of the RAC matrix developed in Section 4.1.1 having probability as the *x*-axis and severity as the *y*-axis.

c. Aggregate the frequencies/probabilities of all hazards in the highest severity category using the approach shown in Section 4.1.6.2 (Conditional Loss Rate) and plot this point using the

summed probability as the *x* coordinate and the center of the severity category as the *y* coordinate.

d. For each subsequent severity category down to the most insignificant, sum the frequencies of all hazards having that severity level OR GREATER. Plot each point using the newly summed frequency as the *x* coordinate and the center of the severity category for the *y* coordinate. Plot the point for each category in turn.

e. Connect the points to produce the cumulative profile.

4.2 MANAGEMENT PATH (STEPS A THROUGH C)

Sections 4.1.1 through 4.1.6 have described the analysis performed to evaluate total system risk and the computation of three measures used to convey these results. Sections 4.2.1 through 4.2.3 will describe three steps related to use of total risk in risk management and risk acceptance. See Figure 7.

Risk management processes give selected government decision-makers both the authority and the responsibility to make decisions accepting the risk posed by activities they direct. With that authority comes the potential for liability, in the legal sense, for mishaps resulting from those activities. The Federal Tort Claims Act (FTCA) provides protection from this liability under the Discretionary Function Exception (28 U.S.C. § 2680(a), Reference 9) if certain conditions are met:

- The decision was made by a duly authorized official of the federal government.
- The risk was assessed using the best available information computed using generally accepted methods and tools.
- The official fully understood the information used in forming the decision.
- The decision was formally documented including the basis for the decision.

The development of accepted analysis methodologies and standard criteria for use in risk acceptance decisions offers significant assistance to officials charged with such decisions.

4.2.1 Step A: Define Total Risk Criterion

Estimates of risk most effectively impact the risk management process when there is a standard for comparison that can be used to determine whether the risk, so measured, is acceptable or not. Program-specific RAC matrices typically have coded bands signifying acceptability levels for partial risks plotted on the matrix. These further specify the authority level at which each risk in each band may be accepted. These methods have served for many years as the —criteria” for accepting partial risks.

Activity risk standards have been developed independently by the National Ranges (Eastern Range, Western Range, Reagan Test Site, etc.) that specify standard criteria for launch risk acceptability. The Range Commanders Council has published a commonality standard (RCC321, Reference 10) that provides national risk guidance related to launch/flight operations. These standards provide multiple, clear criteria defining acceptable risk levels for individuals and groups, for single missions and annual risk accumulations, for the personnel performing the activities, as well as for the general public. Similar risk criteria have been adopted by the explosives safety community and are documented in DoD 6055.09 (Reference 11).

There currently exist no national standard criteria for accepting the total risk assessed by a system safety analysis for a developmental or operational system. For a time, no criteria may be required or used. Total risk could serve initially only as an additional data point given to decision-makers until a body of data is developed supporting the setting of standard safety criteria. In this environment, total risk could be used to judge the relative safety of programs or to assist in identifying the riskiest hazards when making mitigation decisions, and to support risk mitigation trade studies.

National standard risk criteria are customarily published as guidelines rather than as mandatory regulations. This is done to acknowledge that the decision-maker, having the legal liability for mishaps, should also have a measure of discretion in accepting or rejecting the risks posed by activities for which they are responsible. National standards give such decision-makers a measure of protection under the FTCA by establishing generally accepted criteria for risk acceptance (second condition in Section 4.2). Commanders and other responsible individuals have full freedom to establish requirements more stringent than those in national standards, but are generally very reluctant to relax such standards.

To expand this Guidebook's usefulness, the following paragraphs assist in understanding two key aspects necessary to criteria development: the *measure* and the *threshold*.

4.2.1.1 Risk Measure

A well-defined measure is critical to consistent and effective application of any criterion. It should not require that ―youmust be more than 3 feet" without specifying that the measure is height, rather than girth or width.

If the advice given in Section 4.1.6 is heeded, the basic unit of measure to use is straightforward: it should be the unit selected to measure the summed loss threat across all assets. If different loss units are used for different assets in the RAC matrix, then risk summing is limited to determining the total risk to each asset individually.

This basic measure should then be augmented with descriptive words stating the scope and exposure duration for the activity being regulated. The hazard analysis described in Step 2 cannot be adequately performed without first defining the system scope and the exposure interval, so these should be readily available to assist in setting the criterion. It should be noted that should formal, documented criteria regulating total risk become the norm, the reverse would be true—the project hazard analysis must then conform its scope and exposure duration to the measure specified in the criterion. This would be necessary to ensure that the analysis produces a valid estimate of the risk measure used to judge acceptability.

Examples: *Loss dollar value for a single system operated for five years*
Annual loss dollar value for the fleet
Expected annual fatalities experienced by the project (single asset)
Casualty[4] *probability for an individual exposed to a single activity*

[4] When *casualty* or another uncertain ambiguous term is used in the risk measure, a clear definition of the term must be provided. Reference 10 defines casualty as used by national ranges to be Abbreviated Injury Scale (AIS) level 3 or above.

4.2.1.2 Threshold

To provide a complete standard for total risk, the criterion must also specify a numerical value for the maximum quantity of the risk measure that is generally acceptable without waiver or other consideration. This value is considered the acceptability *threshold* and is required to completely specify any total risk criterion.

4.2.2 Step B: Compare Result to Criterion

The common adage demanding that apples be compared only with apples applies fully to the risk acceptance task. Valid comparison to a standard risk criterion can only be made if the hazard analysis has faithfully estimated using the same risk measure as that defined in the criterion. Verifying that equivalent measures are used requires examination of the following:

- The basic unit used ($$, fatality, casualty, etc.)
- The analysis scope (single system, fleet of systems of specified population, etc.)
- The activity duration or exposure interval (project lifetime, single operation, annual, etc.)

When these have been confirmed to be consistent, comparing the total risk estimate to the total risk criterion is no more difficult than comparing one apple to three apples. Since one apple is less than three apples, the criterion requiring that one eat no more than three apples is met.

A short note about the precision and uncertainty of risk analysis is necessary here. Protection under the FTCA (Reference 9) requires that the decision-maker fully understand the best available information when accepting risk. Those making acceptability judgments by applying risk criteria must then properly understand that there is art as well as science involved in risk analysis. A few points to consider are:

- Even when detailed analyses are performed to estimate mishap probability, the results are subject to significant uncertainty. When qualitative assignments to broad probability or severity categories are used, the uncertainty is even greater.
- The precision ascribed to such evaluations then should then be held to a reasonably low level. Computed risk estimates similar to 2.849573×10^{-4} should then be read as 3×10^{-4} when they are compared to risk criteria.
- Similarly, the decision-maker should qualitatively consider uncertainty in the analytical estimate when approving activities assessed by the hazard analysis to be slightly below the maximum acceptable risk.

4.2.3 Step C: Document the Risk Management Decision

Documenting risk decisions offers the opportunity to tie the decisions to input data, analytical approaches, and other information and rationale used to make them. The form used to document risk decisions is as varied as the projects whose risks they manage. The key requirements are that the decision document:

- be signed by the official duly authorized to make the decision,
- show evidence that the decision was based on the official's understanding of the best available information related to that decision, and
- indicate approval explicitly reporting any required conditions for approval.

4.3 INTERPRETING RESULTS

The risk summing methods described in this Guidebook provide several approaches to interpreting and using total risk results. Most important are approaches focused on using the results to manage the total risk of an activity. The paragraphs below describe several methods for applying total risk results to risk management, as illustrated in Figure 10.

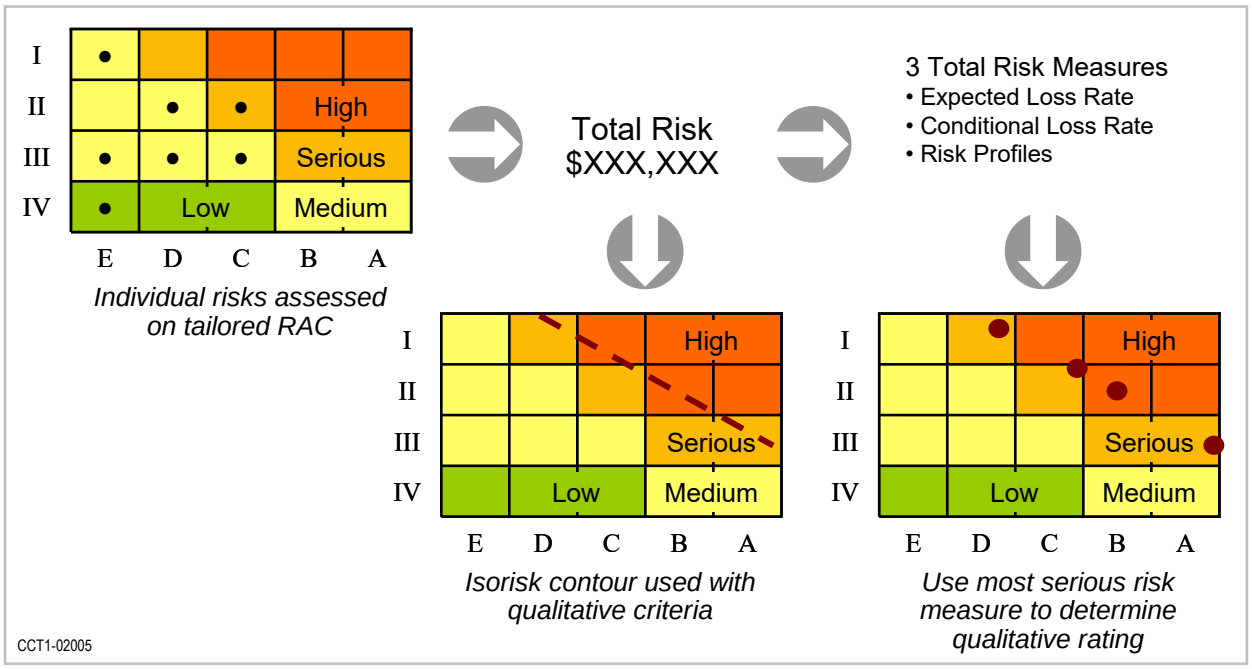


Figure 10. Interpreting Risk Results

Total Risk

As noted throughout this Guidebook, this result should be interpreted as a single, quantitative value for the total risk (losses due to mishaps) to be expected during the system's assessed operational life. This value can then be used for comparisons with expected benefits when making cost-benefit decisions and to select the most beneficial mitigating actions among identified alternatives.

Table 4. Risk Summing Summary

Question	Equation	Result
What is the total system risk (R_r) throughout the full life cycle (or within particular operational phases)?	$$R_T \approx \sum_{i=1}^{i=n} M_i \sum_{i=1}^{i=n} A_i \sum_{i=1}^{i=n} (r_i = s_i \times p_i)$$ (Risk Summing Guidebook Eq) where: R_T = Total Risk s_i = Hazard Severity for the i^{th} identified hazard p_i = Hazard Probability for the i^{th} identified hazard r_i = Risk posed by the i^{th} identified hazard A_i = Identity of the i^{th} asset under threat M_i = The i^{th} system Mission or Operational Phase under consideration	Total Summed Risk: for one full life cycle (or one particular operational phase): Sum of partial risks
If a fleet of this system is operated, what will be the average loss per system operating life due to loss events?	$$ELR = \frac{R_T}{1}$$	Expected Loss Rate: Anticipated loss in one average exposure interval.
On average, how much will be lost if a mishap occurs?	$$S_{CLR} = \frac{\text{Total Risk}}{P_{CLR}}$$ where: $$P_{CLR} \approx \sum P_{hazard}$$	Conditional Loss Rate: Expected loss amount in one average exposure interval.
What is the probability that some loss event will occur as the result of this activity?	Discrete: 1. Calculate R_T 2. Aggregate probabilities in the highest severity and plot 3. Repeat for remaining severities 4. Connect points to produce standard risk profiles Cumulative: 1. Calculate R_T 2. Aggregate probabilities in the highest severity and plot 3. For remaining severity categories sum the frequencies of hazards having that severity level or greater and plot 4. Connect points to produce cumulative profile	Risk Profile: Describes likelihood that loss occurs at each severity level occurs during system operating life. Risk Profile: Describes at each severity level, the likelihood that a consequence at that level or greater occurs during the operating life.
What is the worst loss event that can occur if this system is operated or this activity is conducted?	$$P = \frac{\text{Total Risk}}{\text{Maximum Loss}}$$	Expected Maximum Loss
What is the most likely loss event if this system is operated or this activity is conducted?	$$P_{MPL} = \frac{\text{Total Risk}}{S_{MPL}}$$ Where S_{MPL} = most probable severity category midpoint value	Expected Most Probable Loss

Isorisk Contour

This result provides a continuous representation of the total risk value that can be displayed on the project's tailored RAC along with assessments for each partial risk. One potential application of this result could be to determine the signature level at which the risk remaining after mitigations have been implemented must be accepted.

Risk Measures

The three risk measures provide single-point representations of the total risk that may be plotted individually on the tailored RAC. The qualitative rating associated with the highest risk level indicated by these three measures could be used when determining the approval level required for risk acceptance.

These approaches to interpreting total risk results are now illustrated using results from the risk summing example provided in Section 5.0. Figure 10 provides the tailored RAC matrix developed in Section 4.1.1 complete with high, serious, medium, and low qualitative ratings as well as black markers indicating the assessed partial risks for each hazard. Markers are shown at the center of the RAC category and may represent numerous individual hazards.

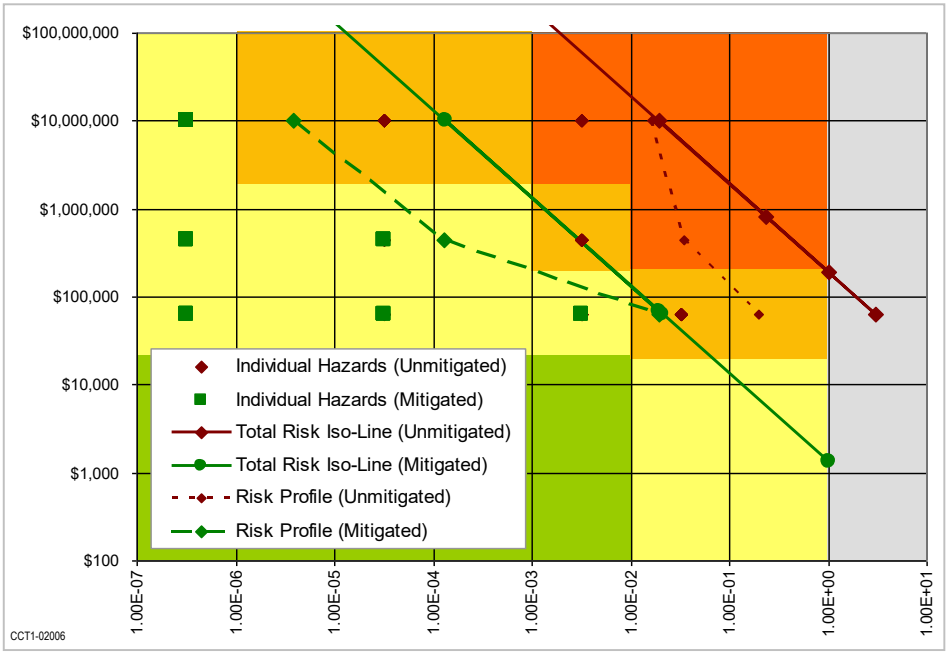


Figure 11. Tailored RAC with Qualitative Ratings, Isorisk Line, and Risk Measures

It is easily seen in Figure 11 that at least one individual hazard is assessed to have an unacceptably high partial risk prior to implementing mitigating actions (dark red). This high, unmitigated risk level is confirmed by both the unmitigated isorisk contour and the cumulative risk profile. Following risk mitigation (green), no single hazard is assessed to have a partial risk higher than Medium. The total risk represented by the isorisk line and the risk profile, however, is clearly rated as Serious.

If typical acceptance level criteria (per MIL-STD 882 Reference 1) were applied to this example:

- the unmitigated risk would require acceptance by the Component Acquisition Executive, and
- all mitigated partial risks could be accepted by the Program Manager, but
- the mitigated total risk would require Program Executive Officer approval.

4.4 POTENTIAL PITFALLS

Any technique used to aid in evaluating risk will present opportunities for introducing errors. The potential pitfalls listed below are to be avoided in applying the summing method set forth here:

Identifying All Hazards—The Total System Risk that results from applying the analytical method presented here, or from any other technique dedicated to that purpose, can only be expected to present the sum of risks of those hazards that have actually been identified. It has been shown incontrovertibly that the methods used for identifying hazards often leave twenty or more percent of all system hazards undiscovered. Reference 5 discusses this phenomenon and provides advice on minimizing its effect. This pitfall can only result in producing a lower-than-actual interpretation of total system risk.

Personnel Risk—Quantifying risk to personnel is fraught with both emotional and practical, actuarial problems. A discussion of matters leading to solutions of these problems can be found in Appendix C.

Cascading Outcomes—Some hazards have what might be considered as escalating outcomes. As an example, consider unprotected hand (asset) exposure to a sharp edged instrument (source) leading to laceration (mechanism). Various levels of severity (outcome) might be considered as outcomes. These might range from no concern or apparent need for care through application of an antiseptic and a band-aid, then use of one or more sutures, antibiotic treatment of infection, acquisition of methicillin-resistant staphylococcus aureus, and finally a fatal "adverse outcome." The analyst, seeking to be thorough, might include each outcome as representing a discrete hazard to be entered into the summing aggregate. Notice, however, that each of these hazards fails the test of being statistically independent. In such a case, the analyst should select the source-mechanism-outcome combination having the greatest individual risk for entry into the summed aggregate. Advice supporting this approach is found in Reference 6.

Risk Amplification—Combined exposure to certain hazards may result in risk exceeding the simple sum of the partial risks of the individual constituent hazards. As a well-known example, consider simultaneous exposure of personnel to hydrous ammonia and chlorine, as might occur through joint exposure to household ammonia and a chlorinated cleaning agent. The resulting chloramines may be disproportionately more lethal than either of the also-toxic constituents. In this example case, the analyst should recognize and separately assess risk for three separate potential personnel exposures, one each for exposure to each of the constituents, and another for exposure to the resulting chloramines.

5.0 APPLYING RISK SUMMING METHODS TO A PRACTICAL EXAMPLE

This section applies the methodology described in Section 4.0 to a practical example. The hypothetical system is first described and then each step is performed showing example products at each point in the process.

The example activity is a missile to be launched from the wing pylons of the Mk-2 Sea Chevre fighter aircraft. Certification requires system safety analyses for aircraft-missile interfaces. Figure 12 provides a simplified illustration of the example system.

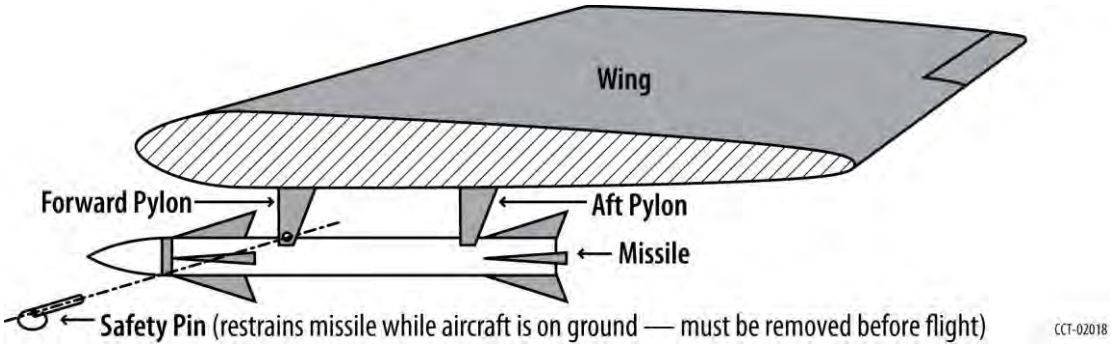


Figure 12. Simplified Fast Asp™ System

For this missile system example, the potential loss events of concern are:

1. Missile release on the ground is considered a "Catastrophic" outcome
2. Failure to arm the missile when fired is considered a mission failure
3. Other than a normal firing signal, Electromagnetic Environmental Effects (E^3) from external sources may initiate a missile "FIRE" command.

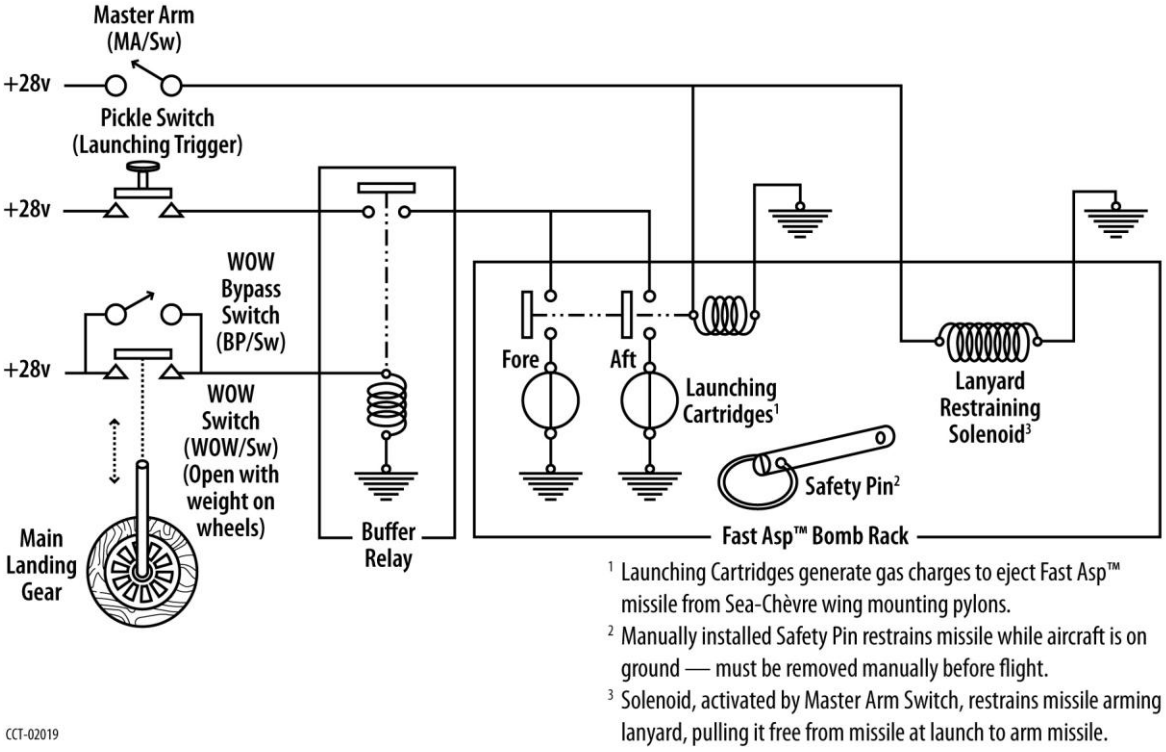


Figure 13. Fast Asp™ Missile Constraint-Deployment System

From an operations standpoint, for this missile example, to fire a missile the following must occur (Figure 13):

1. The Master Arm Switch must be selected "ON", this will do the following:
   a. Enables the pilot's Pickle Switch (i.e., "trigger").
   b. Enables missile-launching gas generator cartridges on fore and aft Missile Mounting Pylons.
   c. Energizes a missile-arming Lanyard Restraining Solenoid, increasing lanyard anchor tension.
2. The pilot must execute the "FIRE" command by actuating the Pickle Switch (i.e., "trigger").

The initial process/system design contains several controls to ensure that proper conditions are maintained. These include:

1. A Safety Pin at the pylon
   a. installation according to a written procedure by a trained mechanic
   b. supervisor monitoring and verification of the installation
2. Weight-on-Wheels (WOW) electrical interlock, which through a Buffer Relay disables the Pickle Switch
   a. A WOW Bypass Switch on the airframe temporarily restores the Pickle Switch function to enable system checkout on the ground
3. The missile is armed by a pull-away lanyard.
   a. Lanyard is restrained by a pincer-action solenoid inside the aft pylon
   b. The solenoid pincer lightly grips the arming lanyard during the aircraft flight but does not arm a jettisoned missile or one released unintentionally
   c. When the Master Arm Switch is selected "ON" the lanyard pincer retention force increases from 3 lbf to 65 lbf.
   d. As the missile separates from the aircraft, the lanyard is restrained by the solenoid pincer, extracting it from a missile onboard fuze to arm it.
4. A bomb rack with dual pyrotechnic launch cartridges is used to ensure clean separation and prevent the missile from striking the Sea Chevre when launched
   a. The cartridges are electrically actuated gas generators.
   b. The expanding gas is ported to pistons that eject the missile away from the aircraft.
   c. Differing gas orifices adjust missile separation characteristics (aft-last).
   d. The two cartridges are interconnected to enable a functioning cartridge to ignite an adjacent misfired cartridge.
   e. Either cartridge alone generates sufficient gas pressure to actuate both pistons.
5. To rid the aircraft of the munitions in an emergency, a "JETTISON" command enables the pilot to launch the Fast ASP™ without arming it.

Furthermore, for this example exercise the following assumptions should be noted to guide the hazard analysis and risk summing documentation:

1. Demonstrated reliabilities of the Master Arm Switch and Pickle Switch are extremely high. —FaultOpen" failure modes predominate. Discounting the —Fault Closed" mode is therefore justifiable for both.
2. Aircraft power is available full time.
3. Kinetic heating of the missile aboard the aircraft in flight has been verified as negligible. Thermal –eook-off" can be discounted.
4. Based on prior certifications/system history, failure of the separation control mechanism for the missile does not warrant consideration.
5. On-board electromagnetic radiation sources (e.g., Radar, ECM, IFF) function as intended and do not affect the Fast ASP™ interface.
6. Consider exposure intervals of 20 years for personnel and 120 mission/sorties for equipment.
7. Consider a single aircraft rather than a fleet.
8. Use the Risk Assessment Matrix (see Step 1) and Failure Probability Data provided (See Appendix D).
9. Fast ASP™ missile cost: $750K

The partial risk of individual hazards posed by this example activity must be assessed before risk summing can be implemented to compute the total risk and the total risk measures used to communicate the results.

5.1 STEP 1: DEFINE THE RAC

Those assessing the example activity desire to use a tailored RAC that is based on the guidance provided by MIL-STD-882D. Beginning with logarithmic, Cartesian axes have hazard probability as the X-axis and hazard severity for the Y-axis as shown in Figure 14.

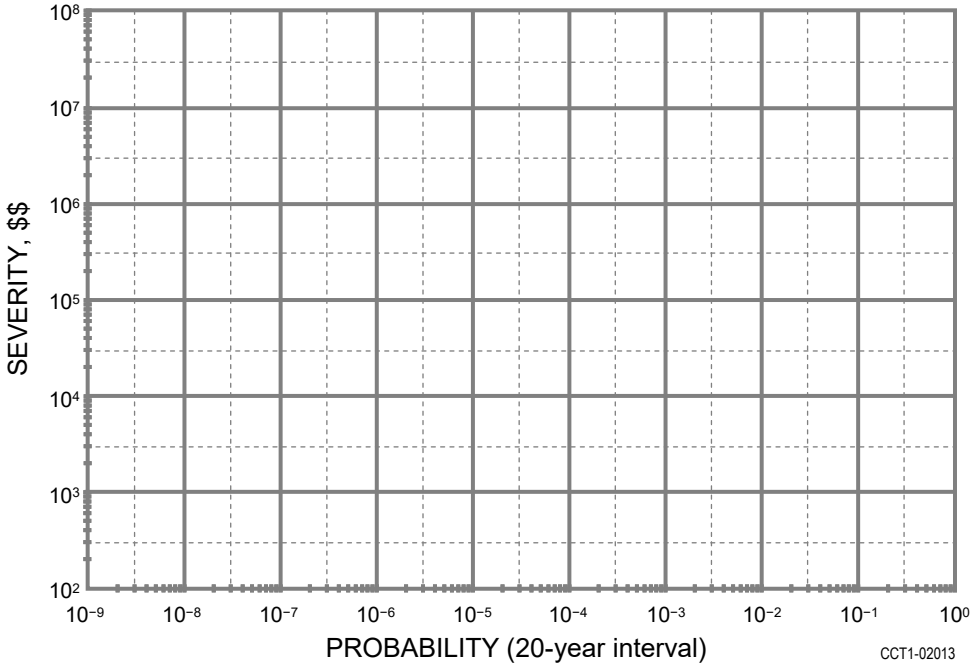


Figure 14. Selected RAC Axes

The figure depicts several decisions already made that will affect the manner in which risks of hazards in the example activity are assessed.

- The choice of Cartesian axes with values increasing further from the origin intentionally pushes the highest risk to the top right of the scale.
- The *X*-axis explicitly states the exposure interval. This is the activity duration over which risks for each hazard is to be analyzed.
- The *Y*-axis states the units used to express hazard severity. As the selected unit, dollars ($$) will be used to quantify the impact to all assets considered in the analysis.
- Though the X-axis shown in the figure ends at 1.0 (1×10^0), it is noted that this axis could be extended if likelihood were expressed as frequency rather than probability.

Next, categories are defined to be used for subjectively assessing hazard severity and the probability. As shown in Figure 15, numerical values assigned to define the severity categories are those identified in MIL-STD 882D with one exception: $20k is the value separating categories III and IV rather than $10k as shown in Table 1 in Section 4.1.1. Also note that dividing the probability axis into categories that span a decade each is desirable when subjectively assessing mishap likelihood. Category D is therefore broken into three sub-categories as shown in the figure.

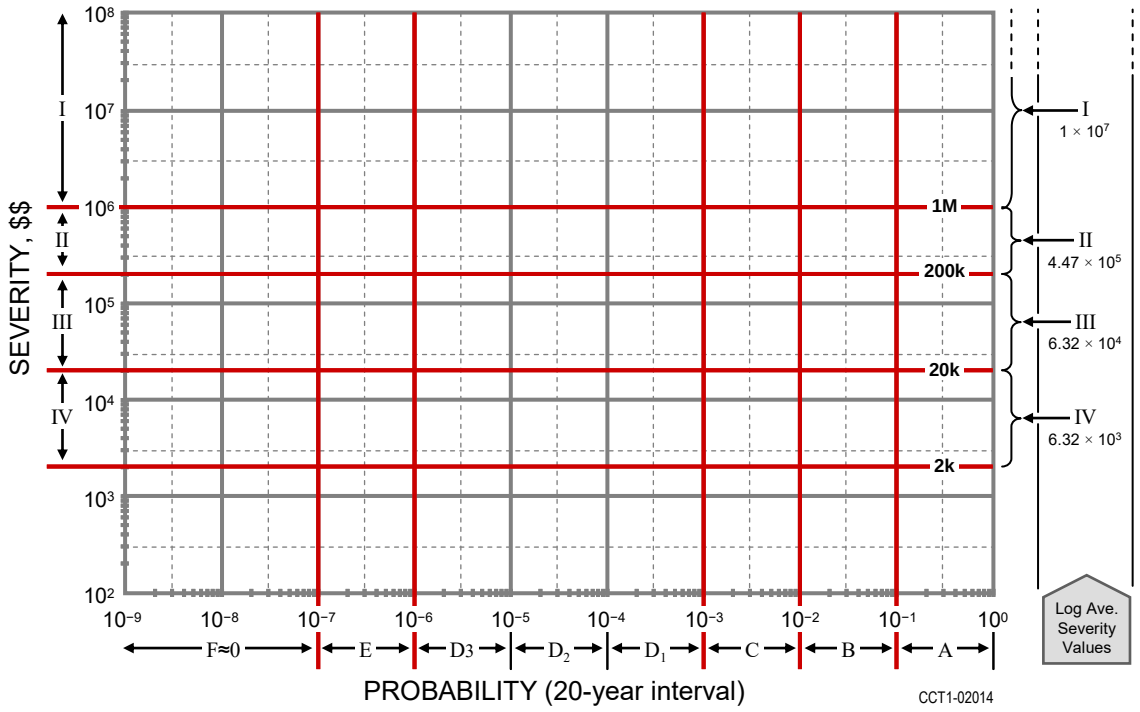


Figure 15. Probability and Severity Categories

Figure 15 also specifies mid-points to represent each severity category when performing risk summing calculations. These represent the geometric means or log averages of the categories. For example, the midpoint of category III is computed to be:

$$\sqrt{\$20\text{K} \times \$200\text{K}} = 6.32 \times 10^4 \qquad \text{(Eq 9)}$$

The midpoints of probability categories are each represented as 3.2×10^x, inasmuch as each category spans one decade.

Lastly, probability and severity category definitions must be finished by tailoring the text descriptions used when qualitatively assessing each hazard. The program is in accord with most definitions provided by Table 1 and Table 2 in 4.1.1. These definitions, however, do not completely satisfy the need since they only define harm to personnel, equipment, or the environment. Mishaps during the example activity can also produce quantifiable ($$) losses due to system down time. Since these are to be assessed in the hazard analysis, clear definitions for severity levels must be provided here. For this example activity, the severity definitions in Table 1 are augmented to include these; Program Management adjustment of equipment loss severities are also indicated for categories III and IV.

Category I:	Downtime exceeding 4 months. Greater than $1M in equipment loss.
Category II:	Downtime exceeding 4 weeks, but less than 4 months. Greater than $200K but not exceeding $1M in equipment loss.
Category III:	Downtime exceeding 1 day, but less than 4 weeks. Greater than $20K but not exceeding $200K in equipment loss.
Category IV:	Downtime exceeding one hour, but less than one day. Less than $20K in equipment damage.

5.2 STEP 2: PERFORM HAZARD ANALYSIS

A hazard analysis has been performed to:

- identify the hazards posed to the selected assets (personnel, equipment, and downtime),
- assess the cost of losses anticipated from mishaps resulting from identified hazards,
- assess the likelihood that these mishaps will occur during the 20-year life cycle, and
- identify mitigations available to reduce the cost impact or probability of a mishap.

The results of the first three actions have been documented in hazard sheets that will support summing the initial total risk prior to mitigations. Feasible changes (design, procedure, test, etc.) are documented in the hazard analysis as additional counter measures.

Additional countermeasures for hazard mitigation changes include:

1. Add level of formal, independent, sign-off, Safety Pin and WOW Bypass Switch inspections with –REMOVE BEFORE FLIGHT" banners.
2. Test/inspect launch system on ground w/dummy missile each 3 sorties.
3. Provide safe recovery area for hung-stores aircraft.
4. Verify valid Launching Cartridge dates.
5. Test/verify electrical ARM and FIRE functions with dummy electrical loads immediately prior to missile installation.
6. Add level of formal, independent, sign-off, Safety Pin inspections.
7. Train pilot in hi-G —pull-up" maneuver to jettison hung missile.
8. Test/verify Lanyard Restraining Solenoid tension during ARM and FIRE function test.
9. Redesign Master Arm circuit to –open" (disable) on jettison command.
10. Test/inspect WOW Switch each 3 sorties.
11. Replace WOW Switch after 60 sorties.
12. Test/inspect WOW Bypass each 3 sorties.
13. Replace WOW Bypass Switch after 60 sorties.
14. Test/inspect WOW Buffer Relay each 3 sorties.
15. Replace WOW Buffer Relay after 60 sorties.

The sample hazard sheet shown in Figure 16 describes hazards, assigns them unique identifiers, and assesses hazard risk before and after applying mitigations. The complete PHA and FMEA hazard worksheets used to assess the example activity are located in Appendix D. The analyses reflect both subjective and quantified hazards. Note that the analysis of the first hazard is scored as requiring a follow-on Fault Tree Analysis (see Appendix D) to reconcile confidence.

	HAZARD DESCRIPTION	TARGET	S	P*	RAC	ADDITIONAL COUNTERMEASURES	S	P*	RAC
1	Uncommanded release of missile from wing pylon on ground, resulting in mass fire/explosion.	Personnel Equipment Downtime	I I II	C D D	1 2 3	1. Add level of formal, independent, sign-off, Safety Pin and WOW Bypass Switch inspections with "REMOVE BEFORE FLIGHT" banners (P/W). NOTE: Verify adequacy of countermeasures by Fault Tree Analysis.	I I II	E E E	3 3 3
2	Hung missile in unknown state: mission aborted for that missile; uncommanded release now more probable; downloading now more hazardous.	Personnel Equipment Downtime	I I III	C D D	1 2 3	1. Test/inspect launch system on ground w/dummy missile each 3 sorties (P). 2. Provide safe recovery area for hung-stores aircraft (S/P). 3. Verify valid Launching Cartridge dates (P).	I I III	E E E	3 3 3
3	Failure to release missile on FIRE command; potential loss of missile and aircraft (Pilot may eject).	Personnel Equipment Downtime	I I II	C D D	1 2 3	1. Countermeasure 1 for Hazard 2 (P). 2. Test/verify electrical ARM and FIRE functions with dummy loads during missile installation (P). 3. Add level of formal, independent, sign-off, Safety Pin inspections (P). 4. Train pilot in hi-G "pull-up," maneuver (P).	I I II	E E E	3 3 3
4	Failure to release missile on JETTISON command; potential for recovery with damaged aircraft and ordnance on board.	Personnel Equipment Downtime	I I III	D E E	2 3 3	1. Countermeasure 1 for Hazard 1 to ensure Safety Pin withdrawn (P). 2. Countermeasure 1 for Hazard 2 (P).	I I III	E E E	3 3 3
5	Arming of jettisoned missile with potential for impact on inhabited area, causing collateral damage.	Personnel Equipment Downtime	I I III	E E E	3 3 3	1.Test/verify Lanyard Restraining Solenoid tension during ARM and FIRE function test (P)[1]. 2. Redesign Master Arm circuit to "open" (disable) on jettison command (E)[1]. [1]Optional; risk acceptable as-is.	I I III	E E E	3 3 3

*Life Cycle: Personnel: 20 yrs / Others: 120 missions/sorties

Figure 16. Sample Hazard Sheet

5.3 STEP 3: ENTER HAZARDS IN SPREADSHEET

When the RAC matrix has been fully defined and the hazard analysis completed, the individual hazards and their assessments must be entered into a software application to compute the quantitative results required by the next few steps. Microsoft Excel® provides a convenient and readily available tool for this purpose. In addition to performing straightforward partial risk computations and summing total risk, Excel® automates the more complicated calculations involved in computing the various risk measures.

A sample from the example matrix containing pre-mitigation data for the first four hazards is shown in Table 5. The complete matrix is provided in the Worked Example Spreadsheet.

Table 5. Initial Hazard Spreadsheet for Example Activity – partial

A	B	C	D	E	F	G	H
Haz ID	**Short Title**	**Sev. Cat**	**Prob. Cat**	**Sev. Value**	**Prob. Value**	**Partial Risk, $$**	**Notes**
PHA1-P	Uncommand Release - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
PHA1-E	Uncommand Release - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00	
PHA1-D	Uncommand Release - Down	II	D	$ 447,000	3.20E-05	$ 14.30	
PHA2-P	Hung Missile - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
PHA2-E	Hung Missile - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00	
PHA2-D	Hung Missile - Down	III	D	$ 63,200	3.20E-05	$ 2.02	
PHA3-P	Fail on FIRE - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
PHA3-E	Fail on FIRE - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00	
PHA3-D	Fail on FIRE - Down	II	D	$ 447,000	3.20E-05	$ 14.30	
PHA4-P	Fail on JETTISON - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
PHA4-E	Fail on JETTISON - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA4-D	Fail on JETTISON - Down	III	E	$ 63,200	3.20E-07	$ 0.02	

The same portion from the final (post-mitigation) matrix is shown in Table 6.

Table 6. Final (Post-Mitigation) Hazard Spreadsheet for Example Activity – partial

A	B	C	D	E	F	G	H
Haz ID	**Short Title**	**Sev. Cat**	**Prob. Cat**	**Sev. Value**	**Prob. Value**	**Partial Risk, $$**	**Notes**
PHA1-P	Uncommand Release - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA1-E	Uncommand Release - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA1-D	Uncommand Release - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
PHA2-P	Hung Missile - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA2-E	Hung Missile - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA2-D	Hung Missile - Down	III	E	$ 63,200	3.20E-07	$ 0.02	
PHA3-P	Fail on FIRE - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA3-E	Fail on FIRE - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA3-D	Fail on FIRE - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
PHA4-P	Fail on JETTISON - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA4-E	Fail on JETTISON - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
PHA4-D	Fail on JETTISON - Down	III	E	$ 63,200	3.20E-07	$ 0.02	

Numerous changes to the individual hazard-asset pairs assessments resulted from changes made to reduce activity risk. For example, the hazard PHA1-P (personnel) assessment changed from IC to IE reducing the assessed loss from $32,000.00 to $3.20. The partial risk posed by hazard PHA1-E to the environment was from ID to IE reducing the associated loss estimate from $320.00 to $3.20.

Table 7 shows the end of the initial matrix, including the total risk value and the values computed for each of the total risk measures.

Table 7. Bottom Portion of Initial Example Spreadsheet with Total Risk and Risk Measures

A	B	C	D	E	F	G	H
Haz ID	**Short Title**	**Sev. Cat**	**Prob. Cat**	**Sev. Value**	**Prob. Value**	**Partial Risk, $$**	**Notes**
FMEA6-E	WOW Buffer on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
FMEA6-D	WOW Buffer on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
FMEA7-P	WOW Buffer Coil OPEN with Volt - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00	
FMEA7-E	WOW Buffer Coil OPEN with Volt - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
FMEA7-D	WOW Buffer Coil OPEN with Volt - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
						$ 131,917.98	Total Risk
			Expected Loss Rate	$ 131,918	1.00E+00		
			Conditional Loss Rate	$ 9,956,038	1.33E-02		
			Maximum Loss	$ 10,000,000	1.32E-02		
			Most Probable Loss	$ 10,000,000	1.32E-02		

5.4 STEP 4: COMPUTE PARTIAL RISKS

As described in Section 4.1.4, the partial risk associated with each hazard-asset combination is computed as the simple product of the numerical severity value and the numerical probability value. In the example matrices (Table 5 and Table 6), the partial risk value is displayed in Column G; the partial risk value is the product of the values displayed in Columns E and F. For example, Table 5 shows a $10 million ($\$1.00 \times 10^7$) severity with a 3.20×10^{-3} occurrence probability for the hazard that PHA1-P poses to personnel. Multiplying these values produces a partial risk of $\$3.2 \times 10^4$, or $32,000.00, posed by hazard PHA1-P to personnel.

5.5 STEP 5: COMPUTE TOTAL RISK

Section 4.1.5 explains that the total risk parameter is obtained by simply summing the partial risk values for each hazard-asset combination. Table 7 shows the total risk value prior to applying mitigations for the example activity. Column G is summed to compute the $131,917.98 value shown in the figure. This value is then used as the basis for the risk measures computed in Step 6.

5.6 STEP 6: COMPUTE TOTAL RISK MEASURES

When potential for losses across multiple assets are assessed or the hazard population quantity is high, the matrix described in Section 5.3 and shown in Appendix B can become quite large. Manually computing risk measures for large matrices becomes cumbersome and presents many opportunities for human error in entering the data. Use of a spreadsheet tool is recommended even if the process used to calculate the risk measures has not been automated.

This section walks through a process that supports computing the risk measures when a fully automated spreadsheet tool is not available. For this exercise, it is assumed that the user has completed Step 3 by constructing a simple spreadsheet matrix similar to that shown in Table 5 and entering the data from the Hazard Sheets provided at Appendix D. It is further assumed that Steps 4 and 5 have been completed by entering the formulas needed to compute the partial risks

in Column G and to sum these partial risks to develop the total risk value displayed at the end of Column G, as shown in Table 7.

The following subsections walk through the steps required to calculate each risk measure using the initial, pre-mitigation data for the example activity. Repeating this process using the post-mitigation data provided in the Hazard Sheets at Appendix D is left as an exercise. Computed risk measure values for both pre- and post- mitigated activity risk are provided in Section 5.6.4 for use in verifying results.

5.6.1 Measure 1: Expected Loss Rate

The Expected Loss Rate uses the Total System Risk as its severity component and unity (1.0) for its probability component. For the example activity, then:

S = $131,917.98
P = 1.0

For similar systems operated for the planned 20-year duration used in the hazard analysis, one would expect that, on the average, systems would produce $131,917.98 in losses due to mishaps described in the analysis. This figure does not address losses due to unidentified hazards.

5.6.2 Measure 2: Conditional Loss Rate

The Conditional Loss Rate measure pairs the probability that a hazard in ANY severity category produces a mishap with the effective severity required to produce the total risk value. Good use is made of the values computed in Section 5.6.5 when computing Most Probable Loss. Table 8 provides convenient access to the data required to compute this measure.

Table 8. Mishap Probability Data (All Categories)

Severity Category	Mishap Probability	1 minus Probability
I	1.62×10^{-2}	0.9838
II	3.47×10^{-2}	0.9653
III	1.96×10^{-1}	0.804
IV	0.00×10^{0}	1.0000

Multiplying the values in the right-most column computes the probability that NO hazard in any category produces a mishap. Subtracting this value from 1.0 produces the probability that one or more mishap occur:

$$P_{CLR} = 1-(1-P_I)\times(1-P_{II})\times(1-P_{III})\times(1-P_{IV}) = 1-0.9838\times0.9653\times0.804 = 2.36\times10^{-1} \quad \text{(Eq 10)}$$

Using this value for *PCLR*, the severity component is computed by:

$$S_{CLR} = \frac{\text{Total Risk}}{P_{CLR}} = \frac{\$131{,}917.98}{2.36\times10^{-1}} = \$558{,}974.49 \quad \text{(Eq 11)}$$

5.6.3 Measure 3: Risk Profile for Example Activity

The risk profile described in Section 4.1.6.3 can be plotted by pairing the occurrence probability for each severity category (shown in Table 8) with that category's numerical ($$) loss value. Table 9 summarizes the previously computed data used to plot the pre-mitigation Risk Profile.

Table 9. Risk Profile Data – Initial, Pre-Mitigation

Severity Category	Probability (x-value)	Severity (midpoint)
I	1.62×10^{-2}	$10,000,000
II	3.47×10^{-2}	$447,000
III	1.96×10^{-1}	$63,200
IV	0.00×10^{0}	$6,320

Figure 17 plots this Pre-Mitigation Risk Profile along with the Individual Hazards, the total isorisk contour, and the four total risk measures computed in the preceding sections.

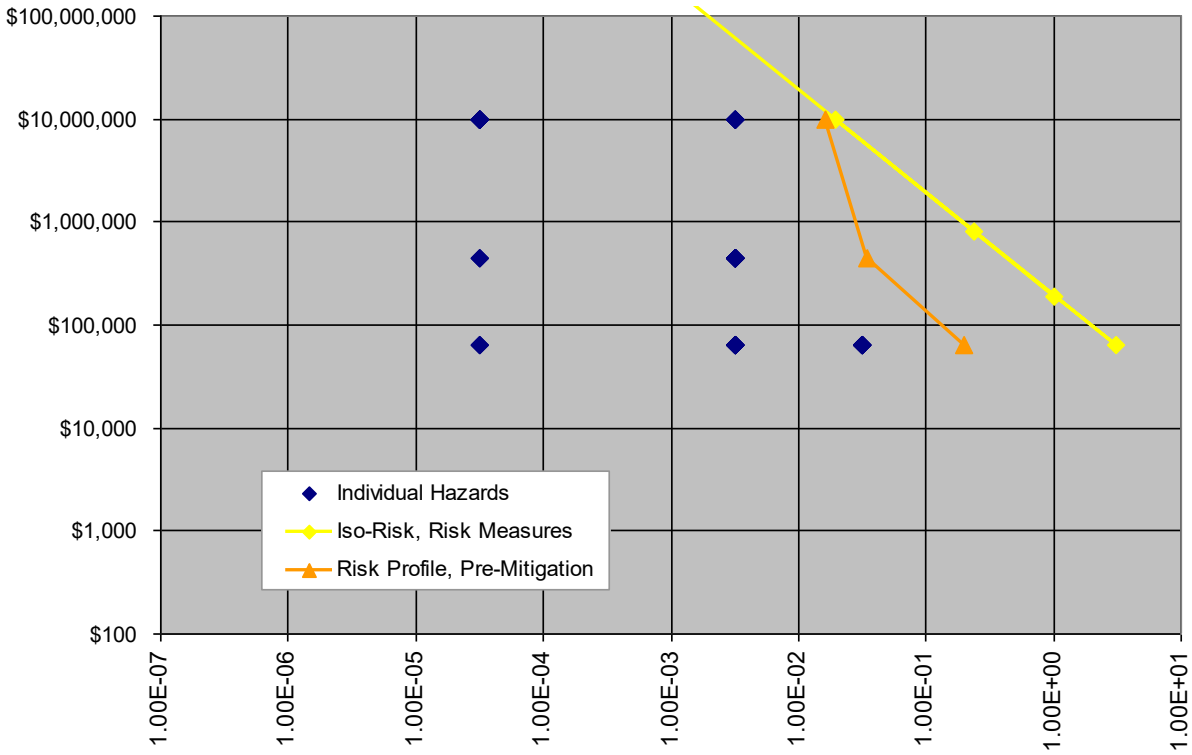


Figure 17. Example Activity Risk Profile Plot – Initial, Pre-Mitigation

5.6.4 Maximum Loss (Info Only)

To determine the probability and severity components for the Maximum Loss measure, one must first identify the highest assessed severity for any hazard-asset combination identified by the hazard analysis. If no studies have been done to quantify mishap severity, then one need only to

identify the highest severity category assessed in the matrix—its assigned midpoint value is then used as the Maximum Loss severity component. If ―non-standard" severities have been assigned, then these must be considered when determining the maximum severity. In either case, one can simply use the spreadsheet "MAX" function to determine the maximum severity value entered in Column E. For the example, the equation to enter into a spreadsheet cell would be =MAX(E3:E44). For the example activity, this process should yield a severity value equal to $10,000,000.00. The effective probability considering total risk for this example would be calculated by:

$$P = \frac{\text{Total Risk}}{\text{Maximum Loss}} = \frac{\$131,917.98}{\$10,000,000.00} = 1.31 \times 10^{-2} \qquad \text{(Eq 12)}$$

The maximum loss measure is then described by:

S = $10,000,000.00
P = 1.31×10^{-2}

5.6.5 Most Probable Loss (Info Only)

To determine the severity and total risk probability for the Most Probable Loss, first the severity level most likely to occur must be determined. Again, this can be done manually or by applying a computational tool. This is accomplished by determining, for each severity category, the combined probability that some hazard assessed to have that severity produces a mishap. All the hazard-asset pairs must first be sorted into the four severity categories. This can be done manually by selecting a severity category and recording probability values for each hazard-asset pair assessed to produce loss in that category. It may more easily be accomplished by using the Sort function in Microsoft Excel®. To sort, first highlight all columns for each hazard-asset pair as shown in Figure 18.

	A	B	C	D	E	F	G	H
1	A	B	C	D	E	F	G	H
2	Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$	Notes
3	PHA1-P	Uncommand Release - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
4	PHA1-E	Uncommand Release - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00	
5	PHA1-D	Uncommand Release - Down	II	D	$ 447,000	3.20E-05	$ 14.30	
6	PHA2-P	Hung Missile - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
7	PHA2-E	Hung Missile - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00	
8	PHA2-D	Hung Missile - Down	III	D	$ 63,200	3.20E-05	$ 2.02	
9	PHA3-P	Fail on FIRE - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
10	PHA3-E	Fail on FIRE - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00	
11	PHA3-D	Fail on FIRE - Down	II	D	$ 447,000	3.20E-05	$ 14.30	
12	PHA4-P	Fail on JETTISON - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
13	PHA4-E	Fail on JETTISON - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
14	PHA4-D	Fail on JETTISON - Down	III	E	$ 63,200	3.20E-07	$ 0.02	
15	PHA5-P	Arming Jettisoned - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.20	
16	PHA5-E	Arming Jettisoned - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
17	PHA5-D	Arming Jettisoned - Down	III	E	$ 63,200	3.20E-07	$ 0.02	
18	PHA6-P	Fail to ARM - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
19	PHA6-E	Fail to ARM - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00	
20	PHA6-D	Fail to ARM - Down	II	D	$ 447,000	3.20E-05	$ 14.30	
21	FMEA1-P	WOW Contact Open on CLOSE - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00	
22	FMEA1-E	WOW Contact Open on CLOSE - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
23	FMEA1-D	WOW Contact Open on CLOSE - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
24	FMEA2-P	WOW Close on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
25	FMEA2-E	WOW Close on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
26	FMEA2-D	WOW Close on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
27	FMEA3-P	WOW Bypass Open on CLOSE - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00	
28	FMEA3-E	WOW Bypass Open on CLOSE - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
29	FMEA3-D	WOW Bypass Open on CLOSE - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
30	FMEA4-P	WOW Bypass on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
31	FMEA42-E	WOW Bypass on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
32	FMEA4-D	WOW Bypass on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
33	FMEA5-P	WOW Buffer Open on CLOSE - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00	
34	FMEA5-E	WOW Buffer Open on CLOSE - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
35	FMEA5-D	WOW Buffer Open on CLOSE - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
36	FMEA6-P	WOW Buffer on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
37	FMEA6-E	WOW Buffer on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
38	FMEA6-D	WOW Buffer on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
39	FMEA7-P	WOW Buffer Coil OPEN with Volt - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00	
40	FMEA7-E	WOW Buffer Coil OPEN with Volt - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20	
41	FMEA7-D	WOW Buffer Coil OPEN with Volt - Down	II	E	$ 447,000	3.20E-07	$ 0.14	
42							$ -	
43							$ -	
44							$ -	
45							$ 131,917.98	Total Risk
46				Expected Loss Rate	$ 131,918	1.00E+00		
47				Maximum Loss	$ 10,000,000	1.32E-02		
48				Most Probable Loss	$ 10,000,000	1.32E-02		
49				Conditional Loss Rate	$ 9,956,038	1.33E-02		
50					1000000000	1.32E-04		

Figure 18. Example Matrix (Initial) with Data Selected

With all entered data selected, select the following menu options: [Data > Sort > Sort by: Column C, Ascending, No Header Row]. This operation should sort the hazard data so that all severity category I hazards appear at the top of the display, as shown in Figure 19, Columns A-H.

Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$	Notes			I	J
PHA1-P	Uncommand Release - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00		I	1.00E+07	0.996800	
PHA1-E	Uncommand Release - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00		II	4.47E+05	0.999968	
PHA2-P	Hung Missile - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00		III	6.32E+04	0.996800	
PHA2-E	Hung Missile - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00		IV	6.32E+03	0.999968	
PHA3-P	Fail on FIRE - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00		A	3.20E-01	0.996800	
PHA3-E	Fail on FIRE - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00		B	3.20E-02	0.999968	
PHA4-P	Fail on JETTISON - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00		C	3.20E-03	0.999968	
PHA4-E	Fail on JETTISON - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20		D	3.20E-05	1.000000	
PHA5-P	Arming Jettisoned - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.20		E	3.20E-07	1.000000	
PHA5-E	Arming Jettisoned - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20				1.000000	
PHA6-P	Fail to ARM - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00				0.996800	
PHA6-E	Fail to ARM - Equip	I	D	$ 10,000,000	3.20E-05	$ 320.00				0.999968	
FMEA1-P	WOW Contact Open on CLOSE - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00				0.999968	
FMEA1-E	WOW Contact Open on CLOSE - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20				1.000000	
FMEA2-P	WOW Close on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00				0.999968	
FMEA2-E	WOW Close on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20				1.000000	
FMEA3-P	WOW Bypass Open on CLOSE - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00				0.999968	
FMEA3-E	WOW Bypass Open on CLOSE - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20				1.000000	
FMEA4-P	WOW Bypass on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00				0.999968	
FMEA42-E	WOW Bypass on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20				1.000000	
FMEA5-P	WOW Buffer Open on CLOSE - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00				0.999968	
FMEA5-E	WOW Buffer Open on CLOSE - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20				1.000000	
FMEA6-P	WOW Buffer on OPEN - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00				0.999968	
FMEA6-E	WOW Buffer on OPEN - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20				1.000000	
FMEA7-P	WOW Buffer Coil OPEN with Volt - Pers	I	D	$ 10,000,000	3.20E-05	$ 320.00				0.999968	
FMEA7-E	WOW Buffer Coil OPEN with Volt - Equip	I	E	$ 10,000,000	3.20E-07	$ 3.20				1.000000	1.31E-02
PHA1-D	Uncommand Release - Down	II	D	$ 447,000	3.20E-05	$ 14.30				0.999968	
PHA3-D	Fail on FIRE - Down	II	D	$ 447,000	3.20E-05	$ 14.30				0.999968	
PHA6-D	Fail to ARM - Down	II	D	$ 447,000	3.20E-05	$ 14.30				0.999968	
FMEA1-D	WOW Contact Open on CLOSE - Down	II	E	$ 447,000	3.20E-07	$ 0.14				1.000000	
FMEA2-D	WOW Close on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14				1.000000	
FMEA3-D	WOW Bypass Open on CLOSE - Down	II	E	$ 447,000	3.20E-07	$ 0.14				1.000000	
FMEA4-D	WOW Bypass on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14				1.000000	
FMEA5-D	WOW Buffer Open on CLOSE - Down	II	E	$ 447,000	3.20E-07	$ 0.14				1.000000	
FMEA6-D	WOW Buffer on OPEN - Down	II	E	$ 447,000	3.20E-07	$ 0.14				1.000000	
FMEA7-D	WOW Buffer Coil OPEN with Volt - Down	II	E	$ 447,000	3.20E-07	$ 0.14				1.000000	0.000098
PHA2-D	Hung Missile - Down	III	D	$ 63,200	3.20E-05	$ 2.02				0.999968	
PHA4-D	Fail on JETTISON - Down	III	E	$ 63,200	3.20E-07	$ 0.02				1.000000	
PHA5-D	Arming Jettisoned - Down	III	E	$ 63,200	3.20E-07	$ 0.02				1.000000	0.000033
				$ -	0.00E+00	$ -				1.000000	
				$ -	0.00E+00	$ -				1.000000	
				$ -	0.00E+00	$ -				1.000000	
						$ 131,917.98	Total Risk				
	Expected Loss Rate			$ 131,918	1.00E+00						
	Maximum Loss			$ 10,000,000	1.32E-02					1.32500E-02	
	Most Probable Loss			$ 10,000,000	1.32E-02	10,000,000				1.32500E-02	
	Conditional Loss Rate			$ 9,956,038.41	1.33E-02						
				1000000000	1.32E-04						

Figure 19. Computing Combined Probability for Severity Category I

Next, when computed the probability that the hazard-asset pair did NOT produce a mishap. This is done by subtracting the probability that it *did* occur from unity (1.0) as shown in Figure 19, Column I. The equation used was:

$$\text{Column I Value} = 1.0 - \text{Column F Value} \qquad \text{(Eq 13)}$$

If this process is to be performed manually, care must be taken to retain enough significant figures.

Next, all the probabilities for severity category I in matrix Column I are multiplied together to determine the probability that NO hazard-asset pair in category I occurs. The probability that one or more category I mishaps occur is simply one minus the probability that none do. As Figure 19 illustrates, this can be accomplished by entering =1-PRODUCT(I3:I16) in the lone occupied cell in Column J. This cell's value [1.31×10^{-2}] is the probability that one or more category I hazards produce mishaps.

This is repeated for severity categories II, III, and IV, producing combined mishap probabilities of 9.82×10^{-5}, 3.26×10^{-5}, and 0.00×10^{0}, respectively.

In comparing the four probabilities, it is determined that category III is the severity in which a loss event is most probable. Category III is represented quantitatively by its midpoint value, $63,200.00, which is now assigned as the severity value (S_{MPL}) for this total risk measure.

Finally, the effective occurrence probability considering all hazards is determined by dividing the total risk by the category III severity value:

$$P_{MPL} = \frac{\text{Total Risk}}{S_{MPL}} = \frac{\$131,917.98}{\$63,200.00} = 2.09 \qquad \text{(Eq 14)}$$

Note that the 2.09 value does not properly represent a probability. Though labeled as probability, this risk measure component should be viewed as representing the expected number of mishaps occurring during the 20-year activity duration.

The total risk then, as represented by the Most Probable Loss Measure, is defined by P-S components:

S_{MPL} = \$63,200.00
P_{MPL} = 2.09

5.7 Results Summary—Total Risk Assessment for Example Activity

This section summarizes the results generated in Steps 1 through 6 (Sections 5.1 through 5.6) for the example activity risk prior to implementing hazard controls and provides corresponding results for post-mitigation risk. The information provided in Table 10 is used both for determining risk acceptability and for communicating activity risk to others (management, customer, public, etc.).

Table 10. Quantitative Results Summary – Total Risk

Activity X Total Risk Assessment	Initial Risk Estimate		Mitigated Risk Estimate	
	P	S	P	S
Total Risk		$ 131,918		$ 85
Risk Measures				
Expected Loss Rate	1.00E+00	$ 131,918	1.00E+00	$ 85
Maximum Loss	1.32E-02	$ 10,000,000	8.47E-06	$ 10,000,000
Most Probable Loss	1.32E-02	$ 10,000,000	8.47E-06	$ 10,000,000
Conditional Loss Rate	1.33E-02	$ 9,956,038	1.25E-05	$ 6,786,671
Risk Profile Data				
Severity Category I	1.31E-02	$ 10,000,000	8.32E-06	$ 10,000,000
Severity Category II	9.82E-05	$ 447,000	3.20E-06	$ 447,000
Severity Category III	3.26E-05	$ 63,200	9.60E-07	$ 63,200
Severity Category IV	0.00E+00	$ 6,320	9.60E-07	$ 6,320

Figure 20 provides the initial total risk results for the example activity. Each result is displayed both before and following mitigation actions. Results shown are probability-severity coordinates for each identified hazard and the isorisk contours with the risk measures. The total risk measures shown are Expected Loss Rate (ELR), Maximum Loss Encountered (MLE), Most Probable Loss (MPL), and the Conditional Loss Rate (CLR).

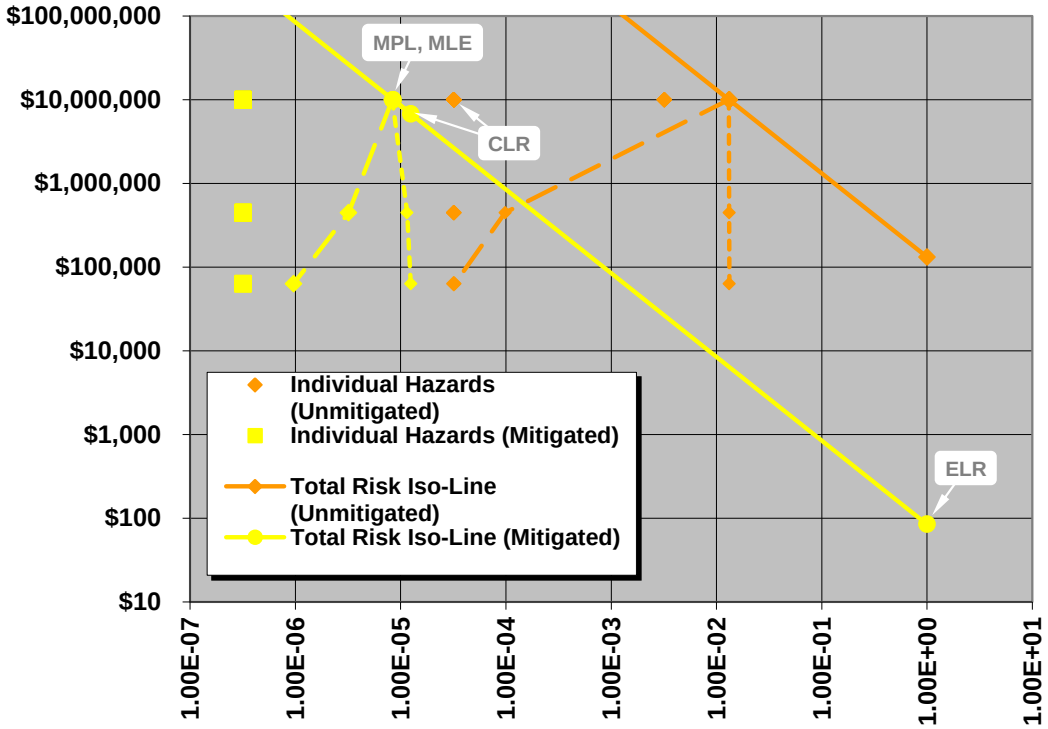


Figure 20. Total Risk Results – Initial and Final

This completes the total risk assessment process. In this process, a scale for assessing hazards has been developed, hazards have been identified/assessed/mitigated, and hazard data have been entered into a risk matrix to compute partial risks/total risks/total risk measures.

The next three sections discuss a hypothetical management approach describing activities that would occur in parallel with this analytical process as shown in Figure 7, Steps A through C.

5.8 Step A: Develop Total Risk Criteria

This section describes fictional deliberations used to set criteria for determining that risks posed by the example activity have been adequately mitigated prior to approving planned operations.

The Royal Frambesian Navy is updating the Mk-2 Sea Chevre aircraft weapons inventory to include the Fast Asp missile. Missile release on the ground is considered a catastrophic outcome and replacement of the missile is a critical hazard based on cost. Certification requires system safety analyses for aircraft-missile interfaces. The hazard analyses should consider personnel, downtime, and equipment as the system assets. The following Risk Action Codes have been set:

1. Imperative to suppress risk to lower levels: Catastrophic/Frequent (IA); Catastrophic/Probable (IB); Catastrophic Occasional (IC); Critical/Frequent (IIA); Critical/Probable (IIB).
2. Operation requires waiver: Catastrophic/Remote (ID); Critical/Occasional (IIC); Marginal/Frequent (IIIA); Marginal/Probable (IIIB).

The analysis should consider a single aircraft rather than the fleet. Failure probability data has been gathered and documented.

5.9 STEP B: COMPARE RESULTS TO CRITERIA

As shown in Table 10, the original engineering design was assessed to have a total loss risk exceeding $131,918.00. If this expected loss level were realized, the example activity would have met its goals.

Based on this result, an aggressive risk mitigation study was performed that identified numerous controls that were economically feasible. The value of each was considered based on the total risk reduction obtained and the cost to implement. The total risk post-mitigation was found to be $85.00, as shown in Table 10.

5.10 STEP C: DOCUMENT RISK MANAGEMENT DECISIONS

A joint meeting was held so that the cost analysts, the business strategists, and the system safety practitioners could present their collective findings to management. Upon clearly understanding the total risk results and the costs involved in mitigating hazards inherent in the original design, corporate management approved the engineering request to implement the added countermeasures.

The decision memorandum issued by headquarters provided clear guidance for proceeding with equipment purchases, testing changes, and manufacturing changes needed to implement the decision. It also included, as attachments, the presentations upon which the decision was based.

6.0 SUMMARY/CONCLUDING COMMENTS

To gain favor as a beneficial practice, risk summing must earn acceptance by senior analysts and seasoned risk acceptance authorities. Within the community of practitioners, there is a deep-felt concern for employing only well-established methods known to produce results that have been deemed acceptable in past practice. As a group, the practitioners and authorities are earnestly professional and steadfast in their approach to the practice of System Safety Engineering. As professionals, they are inclined to a healthy distrust of innovations in the absence of assurances that improved practice will result. This trait gives the profession a wholesome aspect of stability without which it might succumb to vagaries of practice leading to irresponsible wavering. Stability, however, if carried to an overdriven extreme, becomes indistinguishable from technological stagnation. Consequently, opportunities for advancing the practice may sometimes be dismissed with little consideration. Thus, although the principle underlying the summing of partial risks is unarguably sound, an initial reluctance to accept it is to be expected. Recognizing sound arguments and identifying useful means for overcoming this reluctance are therefore important to advancing the practice of the discipline.

Because they have strong backgrounds in technological pursuits, system safety practitioners and risk acceptance authorities are appealed to by sound engineering reasoning. Classroom training in the distinction between collective whole-system risk assessment, as contrasted with assessment by unsummed partial risks, will be readily understood and will impart appreciation for the need for summing. A training module has been prepared and tested in the classroom to support this approach. The point should be stressed in presenting the summing principle that it does not supplant any analytical method now in use. Instead, summing exploits the results of long-trusted methods. Those results are now given greater analytical value as a consequence of viewing total system risk in addition to the view of the many individual partial risks that is now seen.

Purists in the subject of probabilism will be quick to point out that the summing result produced by Eq. 1 is inexact. The simple summation that it produces assumes that the input partial risks are mutually exclusive. It therefore returns a rare event approximation rather than a true total risk value. (Line-item hazard inventories like those produced by Preliminary Hazard Analysis and Failure Modes and Events Analysis customarily comprise hazard probability entries that are statistically independent rather than mutually exclusive.) It can readily be shown that this rare event approximation will always convey a risk value slightly greater that the true result would be — that is, it returns a result that is slightly pessimistically biased.

Two conjoint arguments have led to a deliberate decision favoring use of this rare event approximation in evaluating total system risk:

1. The form of the Eq. 1 rare event approximation better conveys the purpose of summation and is more readily grasped by practitioners who may be newly introduced to summing than would be an exact solution.
2. Because not all hazards will have been discovered (Ref. 5), the expression of total system risk by the method described here is expected to be optimistically biased. As stated above, the error introduced by Eq. 1 is both small and pessimistic. Introducing this small pessimistic bias can only be expected to partially offset the optimistic bias introduced by failures at identifying hazards.

As application of total risk summing becomes commonplace, use of an exact summing solution and other refinements can be introduced. These would include various ways of displaying total risk results to support system design trade studies and allocations of resources among risk mitigation alternatives.

For questions or comments, contact Saralyn Dwyer, sdwyer@apt-research.com, or Melissa Emery, memery@apt-research.com.

7.0 REFERENCES

1. U.S. Department of Defense; *Military Standard — Department of Defense Standard Practice — System Safety;* MIL-STD-882D; February 2000.
2. Swallom, Donald W. and Clemens, P. L.; *Summing Risk — An International Workshop and Its Results;* Journal of System Safety, November-December, 2005, Vol. 41, No. 6.
3. Clemens, P. L.; *System Safety Scrapbook*; Tenth Edition; September 2004.
4. Cantrell, Susan and Clemens, P. L.; *Finding All the Hazards;* Professional Safety, November 2009.
5. Pfitzer, Tom and Clemens, P. L.; *Risk Assessment and Control — Is Your System Safety Program Wasting Resources?;* ASSE Professional Safety, January 2006.
6. TechAmerica; *Standard Best Practices for System Safety Program Development and Execution;* GEIA-STD-0010; February 2009
7. Clemens, P. L.; *Preferences in Interpreting the Risk Assessment Matrix*; Professional Safety, June 1995.
8. Clemens, P. L.; *Modeling in System Safety – A Significant Source of Error*; Journal of System Safety, February 2009, Vol.1, No.1
9. U.S. Code, Title 28, Part VI, Chapter 171, § 2680. Exceptions, http://www.law.cornell.edu/uscode/html/uscode28/usc_sec_28_00002680----000-.html
10. Range Commanders Council, Range Safety Group, *Common Risk Criteria for National Test Ranges*, Standard 321-07, June 2007.
11. U.S. Department of Defense, *DoD Ammunition and Explosives Safety Standards*, DoD 6055.9-STD, October 5, 2004.
12. Hammer, Willie; *Handbook of System and Product Safety;* Prentice-Hall, Inc.; ISBN 0-13-382226-5; 1972.
13. Clemens, P. L.; *Many Hazard Analyses Conceal Whole-System Risk;* Professional Safety, April 2000.
14. U.S. Department of Defense; *Military Standard — System Safety Program Requirements;* MIL-STD-882A; 28 June 1997.
15. Clemens, P. L.; *Hazards, Probabilism, Logic, and MIL-STD-882;* Hazard Prevention, 2nd Quarter, 1996, Vol. 32, No. 2, p9.
16. Swallom, Donald W.; *Source-Mechanism-Outcome: A Simple, Yet Effective Hazard Model;* Proceedings of the 24th International System Safety Conference, August 2006.
17. Clemens, P. L.; *A Method of Combinatorial Failure Probability Analysis Using MIL-STD-882A;* Hazard Prevention, July/August 1982, Vol. 18, No. 4, p 8.
18. American Society of Safety Engineers; *Prevention through Design: Guidelines for Addressing Occupational Risks in Design and Redesign Processes*; ASSE Technical Report; ASSE-TR-Z790-001-2009.

APPENDIX A: BACKGROUND INFORMATION

COMPREHENSIVE PRINCIPLES

The first truly comprehensive text describing the principles of system safety was published in 1972 (Reference 12). What has now come to be recognized as Lüsser's Law had its inception nearly three decades earlier (Reference 13). That law had led almost at once to the inception of the practice now known as Reliability Engineering, and with it, fully quantitative expression of the likelihood a system would function according to design intent on random command and for a prescribed period.

For the most part, and from the outset, system safety as a broadly viewed practice has avoided quantifying expressions of overall system risk. This persistent antipathy became particularly intense in the late 1970s and has continued in some circles through the first decade of the twenty-first century. This quotation from a leading standard, describing characteristics of its risk assessment matrix, illustrates the vigor with which antipathy toward quantitative methods of system safety practice has sometimes been expressed:

> *—This matrix design assigns a different index to each [severity-probability matrix cell] …avoiding the situation caused by creating indices as products of numbers …such as 2 × 6 = 3 × 4." (Reference 14).*

To further thwart quantification, the matrix axes were scaled using Roman numerals (severity scale) and Latin letters (probability axis) and the matrix was plotted in the second rather than the conventional first Cartesian quadrant.

Notable exceptions to this quantification aversion arose early in several fields where they have continued and are responsible for significant advances in method. Chemical processing, nuclear power, and medical devices are prominent among the industries that have adopted probabilistic risk assessment methods (Reference 15).

The use of subjective methods to assess risk on a hazard-by-hazard basis has been preferred even though quantifying would at once enable summation to produce expressions of total risk. This aversion has multiple origins. They can be identified only speculatively. These are a few:

- It can be argued that quantified data expressing the probability of failure among system elements at the lower levels of indenture are not available, and therefore whole system failure probability cannot be calculated. (This was far truer 30 years ago than today. Estimation methods now common in Reliability Engineering have largely removed this obstacle.)
- Widely accepted standards of practice, e.g., References 1 and 14 neither require nor mention needs for either quantification or summing. They rely almost exclusively on the use of subjective methods of assessing individual line items of risk and provide neither guidance in summing these partial risks nor acknowledgment of the need for recognizing overall total system risk. (The subject of quantifying and summing is, however, taken up in some depth in Reference 16.)
- There persists a misconception held largely by project managers that if Reliability Engineering is practiced rigorously, then applying system safety amounts to redundant

overkill. Moreover, reliability engineering does provide quantitative answers to such questions as, "What is the probability that this system will operate as intended during a period of h hours?" The numerically expressed complement of that probability is recognized as "unreliability," i.e., the overall probability of failure. This is taken as a substitute for a system safety finding. It is an obvious truth, however, that an extremely reliable system may be quite unsafe. Consider a system no more complicated than a hand grenade.

- Analysts having sufficient intellectual capacity to appreciate the need for risk summing are often the same ones who are repelled and driven into alternate pursuits by peculiarities found in purportedly prestigious documents governing the practice of system safety. Examples: The persistent use of a reversed coordinate scale in the Cartesian presentation of risk assessment matrices (References 1 and 14); formal adoption of absurd definitions, e.g.,

  > *"Mishap severity: An assessment of the consequences of the most reasonable credible mishap that could be caused by a specific hazard." (Reference 14)*

  If a mishap is "most reasonable," must it not also be "credible?" And why only one specific hazard? Might it not take several specific hazards beneath a logic tree AND gate to produce the mishap?

- Because each system hazard is dealt with singly in predominant current practice, the system designer, the system safety analyst, and later the risk acceptance authority all view system risk on an item-by-item and asset-by-asset, basis, perhaps further dissociated mission phase-by-mission phase. The complete array of risks is then viewed as to its acceptability on the presumption that if risk is acceptable by parts, it is therefore acceptable in toto (Reference 6). This approach is mistakenly assumed to impart thoroughness; in fact, it results in an analytical product that is quite misleading. It ends in adopting a mindset holding that a system's overall risk can be made acceptable if its individual partial risks can be assessed at a systemic level sufficiently low that the combined severity and probability of each gives an acceptable result.

To bring the practice of system safety abreast of that of other engineering disciplines, quantifying its chief findings is unarguably a necessity. Accomplishing that in one magnificent leap would be desirable but very unlikely to succeed. What is needed instead is a stepping stone plan — a way to take advantage of the subjective estimating skills of today's many trained and experienced system safety practitioners by providing them a disciplined means for moving their subjective estimates of partial risks through a regularized combinatorial arithmetic process and then back again into the world of subjectivity with a total risk result. That is one purpose of this Guidebook.

A brief discussion of the genesis of the summing methods that appears in Section 4.0 will provide insight into justification for their use and engender appreciation for the extraordinarily tedious pace at which progress is achieved in improving the practice of system safety. Although the discussion will begin in the early 1980s, some practitioners of system safety in the previous decade had begun to sense the distortion of true system risk that had become prevalent through the persistent practice of recognizing only a log of individually acceptable partial risks representing an accumulation of innumerable independent system hazards. Had true total system risk been known, it would now appear possible that many 1980-2000 era systems might never

have survived beyond the concept phase of their development. It is also possible that many of the loss events that were suffered might never have occurred.

SYSTEM EFFECTIVENESS AND SAFETY TECHNICAL COMMITTEE WITHIN THE AMERICAN INSTITUTE OF AERONAUTICS AND ASTRONAUTICS

In the early 1980s, members of the System Effectiveness and Safety Technical Committee within the American Institute of Aeronautics and Astronautics (AIAA/SESTC) had engaged in informal discussions of the partial risk aversion problem outlined above. Members of the Committee represented DoD, NASA, their contractors, the private sector, and academia. They partitioned their collective thoughts thusly:

Observations:

- Most system safety analyses log hazards in line-item inventories in which risk is assessed for individual hazard-asset pairs, using subjective assessment methods, and judging risk acceptability on the basis of prescribed tolerance limits customarily displayed in risk assessment matrices.
- Many practitioner-analysts have become proficient at applying these subjective analysis methods using the scales of severity and probability now found in MIL-STD-882A.
- Often it is discovered by an analyst that simultaneous outcomes of two or more line-item hazards at scattered points in a system can bring about a substantial loss event that is not accounted for in the hazard inventory. Individually those hazards pose readily assessed and acceptably low risk. However, the outcome of their coexistent play would induce a monstrous catastrophe. There is no mechanism for determining their conjoint probability using the subjective scalar system. Hence, the proficiency of analysts mentioned above goes untapped.
- For the reasons just given, whole system risk is never appreciated by analysts, program managers, or risk acceptance authorities. Instead, system risk is seen and judged as to its acceptability only on a misleading partial risk-by-partial risk basis.

The full Committee was in accord with these observations. To resolve them, it commissioned a working group in April 1982 to undertake a formal study and to develop suggested solutions.

The working group returned to their home locations and queried their senior system safety practitioners as to their views on combinatorial rules with which to manipulate Boolean unions and intersections of multiple disjoint hazards. Exchanges of viewpoints followed, as each member of the working group reported his findings to the group. The pooled results were then shared with the contributing practitioners. Following several iterations, a consensus emerged from which This protocol was developed:

The Method and Its Numerical Scale:

In Table A-1, an undimensioned numerical value is arbitrarily assigned to each probability level of a stepwise scale such as the one found in MIL-STD-882A. These —probability values" serve as the basis for straightforward combinatorial analyses using Boolean-based methods. The probability values that result can then be used to re-enter the stepwise scale. Threshold value levels are also allocated in Table A-1 to guide the re-

entry. The result is a determination of combined probabilities in the same judgment framework as had been used initially.

The probability values allocated in Table A-1 are without dimensions of frequency or period (e.g., failure per unit time). It is important that they remain dimensionless. The assignment of dimensions would endow the probability steps with an objective precision, which they cannot acquire through the exercise of subjective engineering judgment.

Table A-1. Probability Levels

See Text — From MIL-STD-882A

Threshold Level	Probability Value	Level	Descriptive Word	Specific Individual Item	Fleet or Inventory
8×10^{-2} →	3×10^{-1}	A	Frequent	Likely to occur frequently	Continually experienced
	3×10^{-2}	B	Reasonably probable	Will occur several times in the life of an item	Will occur frequently
8×10^{-3} →	3×10^{-3}	C	Occasional	Likely to occur sometime in the life of an item	Will occur several times
8×10^{-4} →	3×10^{-4}	D	Remote	So unlikely, it can be assumed that this hazard will not be experienced	Unlikely to occur but possible
8×10^{-5} →	3×10^{-5}	E	Extremely improbable	Probability of occurrence cannot be distinguished from zero	So unlikely it can be assumed that this hazard will not be experienced
	Indeterminate	F	Impossible	Physically impossible to occur	Physically impossible to occur

It is essential to recognize that the arbitrary values are allocated exclusively to enable combinatorial analyses by uncomplicated and widely practiced methods. Although the probability values shown in Table A-1 convey no true numerical failure rate significance, they satisfy several important criteria:

i. As a set, the values are internally consistent. There is general accord among the practitioners of system safety that decade steps characterize the MILSTD-882A probability scale. (Reference 17). Thus, the midpoint of each step in Table A-1 is separated by a factor of ten from the midpoints of its adjacent neighbors. This distribution also facilitates use of log-average estimation.

ii. The mid-step probability values and threshold levels satisfy a rationale for combinatorial scaling having these useful properties:

   1. The union combination of any two independent contributors having equal probabilities produces a probability within the same step of the scale. (This is the "OR" gate case, in fault-tree analysis.)

   2. The union of three equally probable contributors produces a one-step increase in probability. These properties hold whether exact methods or "rare-event" approximations are used in the combinatorial computations.

iii. At the highest probability level (i.e., A/"Frequent"), the intersection combination of any two independent contributors produces a probability within the same step of the scale. (This is the "AND" gate case, in fault-tree analysis.) At that same highest level, the intersection of three contributors produces a one-step decrease in probability. At the next lower level (i.e., B/"Reasonably Probable") the intersection of two contributors produces a one-step decrease in probability.

iv. Coefficients of the powers of ten making up midstep and threshold values over the entire scale are single-digit integers, simplifying mental arithmetic processes while satisfying the criteria above.

Omitting a probability value for step F of the scale ("Impossible") is intentional. It is arguable on philosophical grounds that an impossible event carries no risk and has no place in such a probability table. Nonetheless, its presence there serves as a convenient reference datum. Allocating a finite probability value, however small, would negate the definition "Impossible."

Members of the full AIAA Committee reviewed the method and tested it in instances of practical application. Figure A-1 provides a fault tree example of the method as used to evaluate the 10-year probability of loss of a very large machine bearing, one of six bearings on an 186KHP shaft.

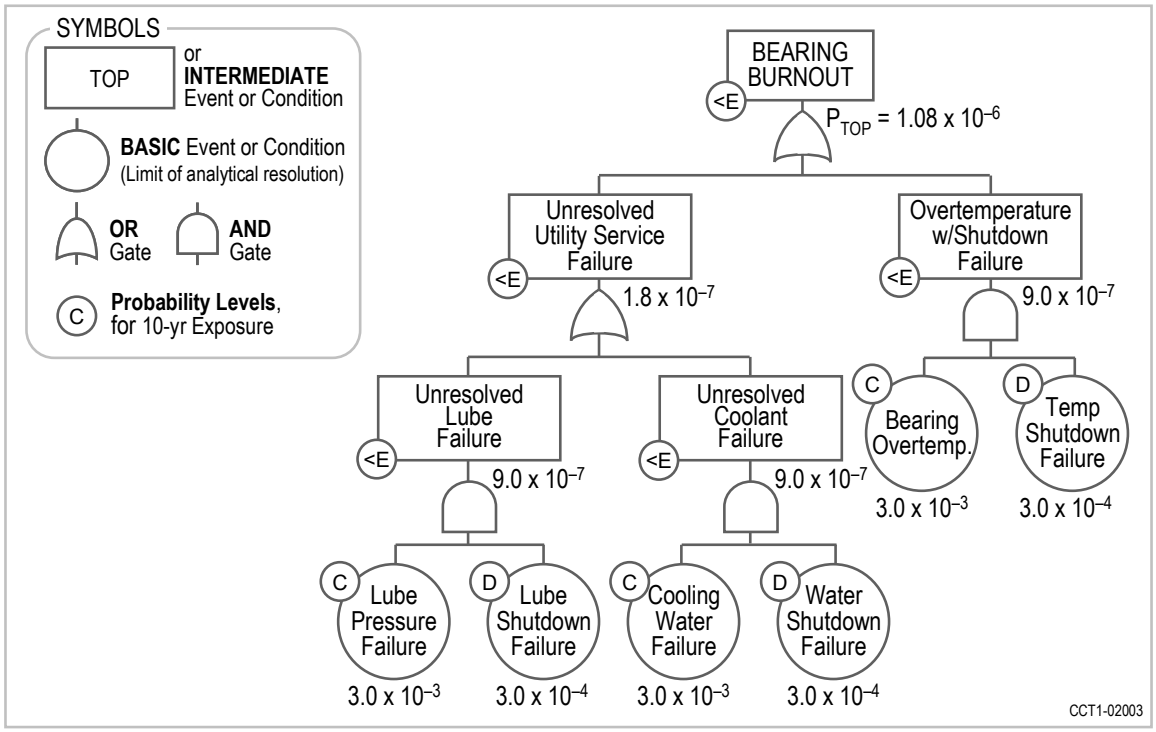


Figure A-1. Bearing Protection System Fault Tree (Adapted from Reference 18)

Quantitative data describing failure probabilities of individual system elements were not available, as is often the case. Plant engineers who were trained and experienced in the use of the subjective probability scale of Reference 5 provided judgments of the initiator probabilities. Both summation (i.e., OR gate) and multiplication (AND gate) logic appear in the fault tree and are

accommodated. Committee approval of the method followed. The method is described in complete detail in Reference 15, where additional examples of its use with test cases also appear.

The AIAA/SESTC combinatorial method has been introduced in classroom training sessions at many NASA and USAF locations, and on two university campuses. It has, however, seen very little application.

RISK SUMMING WORKSHOP

In February 2005, a two-day Risk Summing Workshop was conducted in Huntsville, AL under sponsorship of the U.S. Army Aviation and Missile Command. Nearly thirty attendees from two continents participated, and more than a dozen made formal presentations on the workshop topic. The purpose of the workshop was 1) to assess the need for summing risk of hazards at the system, level, 2) review current methods, and 3) provide recommendations for a path ahead.

The need for risk summation methods to augment or to replace partial risk assessments based on line-item inventory methods was recognized as having increasing importance. Summing techniques of 14 kinds were described. Many were adaptations of others that were described. At the conclusion, workshop participants reached consensus views on fundamental points related to risk summing. The following three stood out among the consensus points:

- Risk acceptance decision-makers should be provided information characterizing total system risk rather than, or in addition to, partial risks of line-items in a system risk inventory, as is customary today.
- Risks of individual hazards should be judged not based on ―worst consequence,” but based on ―worst risk.”
- The source-mechanism-outcome model (Reference 16) should be adopted universally in expressing hazard descriptions.

A complete report of the major methods presented in the workshop can be found in Reference 2. The methods showing the best promise appear in Section 4.0.

APPENDIX B: DEFINING RAC AXES/SCALES

The Non-Severity Scale

Probability vs. Frequency

The non-severity scale used in Risk Assessment Codes (RACs) for years has traditionally been labeled "probability." Probability, however, is limited by its very nature to the range from zero to one. The chance that a specified unwanted event occurs cannot exceed 100%. Assessment of hazards posed by a fleet of systems operated over a large number of years (or flight hours) requires the analyst to consider the possibility that multiple unwanted events could occur during the operating period under assessment. The mishap probability scale suggested in MIL-STD-882D (Reference 3) (see Table B-1) addresses the probability of occurrence in the life of a single item while concurrently allowing that mishaps within unquantified fleet or inventory might occur "several times," "frequently," or "continuously" during the operational lifetime.

Table B-1. MIL-STD 882D Suggested Mishap Probability Levels

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 that 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
Improbably	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

In some instances, the hazards assessed are related to extremely rare failures of highly reliable mechanical equipment (low probability). In others, the hazard is measured by the expected number of incidents per 100,000 flight hours (frequency).

When summing risk, then, what scale should be used for the axis representing likelihood of occurrence?

The needed scale would correctly address events having low probability of a single occurrence as well as those likely to occur multiple times during system operation.

In the rigorous sense, probability does not meet the need to address multiple events. Frequency appears equally ill-equipped to describe extremely rare events.

In statistics, the term "Expected Value" would aptly describe the average number of occurrences per system lifetime that would be observed if many systems were operated numerous lifetimes.

Using Expected Value as the likelihood measure supports risk summing across a continuous scale from rare events to those occurring multiple times during the average system lifetime.

The likelihood scale, then, could read ―ExpectedNumber of Occurrences During Operating Period.” The numerical scale would span as many decades as are needed to address the range of expected values (1.0×10^{-n} to 1.0×10^{n}).

APPENDIX C: ASSIGNING SEVERITY TO HUMAN HARM

Summing Risk to Human Assets

Vaulting a Primary Hurdle – A Common Measure of Harm

A prerequisite to aggregating the partial risks posed by individual system hazards is the ability to express the level of harm (severity) to the various assets using a common unit of measure. One can no sooner add the dollar value of facility damage to a schedule delay or the degradation of data collection than one can add feet to meters without first converting to a single measure of length.

It is widely agreed that the financial cost to a program provides a convenient basis for expressing the impact (harm) should a hazard become reality producing a loss event. Units of U.S. Dollars ($$) can be used to express the costs:

- to repair/rebuild a facility or to replace damaged equipment,
- to perform additional testing required to confirm or replace degraded or lost test data,
- to clean-up a contaminant restoring the environment,
- of schedule delays resulting in overtime payments or lost funding in future years, or
- of lost program reputation evidenced by mission changes or funding cuts.

For some losses, the conversion to dollars is straightforward since costs to perform recovery actions can be directly estimated. Other losses, such as schedule delays and damage to reputation are more difficult to estimate in dollar terms even though the financial impact to the program is easily recognized. Though the estimates may be less accurate, with proper urging, program managers should generally be able to assign a dollar value to such losses.

Human losses, however, are found to resist such quantification for a number of reasons:

- The belief that human life is simply beyond value (infinite).
- Wide variations in cultural beliefs throughout the world and locally.
- Differing approaches to valuation (value to society vs. intrinsic value).

Instinctive moral aversions aside, what basis should be used when assigning a severity value to such losses as fatality or life-changing injury? Can we indeed place a value on human life?

We cannot do so, nor should we, nor MUST we!

A common mis-perception is the view that correlating an accidental fatality with a dollar figure places a value on human life. This view presents a hurdle that must be overcome if risk management is to include total (summed) activity risk in decision-making processes.

On the contrary, risk analyses must establish the *cost* of a loss rather than its *value*. This distinction denotes a very significant difference. Typical dictionary definitions describe *value* as relative worth, merit, or importance – the worth of something in terms of the amount of other things for which it can be exchanged. Value is a voluntary process. Though there are things for which one might willingly offer one's life (to spare the life of another, in service to country, for sake of honor), the value ascribed is clearly extreme. *Cost*, however, is defined as a price paid, an outlay, or expenditure. In some exchanges, value exceeds cost. In others, it does not. Voluntary

transactions take place when both parties perceive that the value of what they receive exceeds the cost paid.

Loss of life due to a mishap is not a voluntary transaction. Something treasured has been taken from another, though unintentionally. A price must be paid. While this price represents a cost to the program, it in no manner represents the value of the life lost. The analyst, risk manager, decision-maker, etc. should not view cost quantification as ascribing value to human life. Instead, the risk assessment process should acknowledge that no payment adequately reimburses the *value* of such loss while providing the best estimate possible of its *cost*.

In the United States, the cost paid by an entity causing loss to another is typically determined by judicial action or by consensus agreement pre-emptive to judicial resolution. The results of past actions are closely watched by those paid to argue the cases of liable parties and victims alike (read as ~~l~~lawyers"). When the risk analysis job is viewed as requiring determination of cost rather than value, these records provide a rich resource for estimating the costs of fatality and serious injury.

A large number of RAC matrices have been devised for use in risk management. MIL-STD-882D offers the potential to tailor the risk matrix used by a program to suitable scales of severity and probability (or frequency). By examining the data presented above and the models developed from them, one can develop measures of severity (cost) across the range of potential outcomes. Assigning dollar values to severity descriptions enables one to aggregate the costs arising from human harm into summed risk measures supporting enhanced risk management.

Many interpretations can surely be drawn from the verdict data presented above producing a number of risk assessment matrices. Though certainly not the only scale that can be produced, the severity descriptions in Table C-1 illustrate a potential application of the data reviewed earlier. The left-most figures represent the upper and lower boundaries of each severity category. The figures shown in parentheses provide center values that could be used in quantitative assessment of summed risks that include the potential for human harm.

Table C-1. Example Severity Scale for Human Harm

$2B	
($630M)	100 or more fatalities, 1000s of serious injuries
$200M	
($63M)	10 or more fatalities likely, 100s of serious injuries
$20M	
($6.3M)	Single fatality likely, multiple fatalities possible, multiple serious injuries likely
$2M	
($630K)	Serious injury likely, fatality possible, multiple significant injuries
$200K	
($63K)	Significant injury, multiple minor injuries, serious injury possible, fatality unlikely
$20K	
($6.3K)	Minor injury, multiple lesser injuries
$2K	
($630)	Insignificant injury, perhaps multiple (figure is related to medical costs more than potential for lawsuits)
$200	

It should be noted that the severity Table C-1 includes hints of probability. This brings up several points worthy of mention:

- The probability scale on the RAC matrix is generally perceived to be the probability of a mishap occurring due to the hazard rather than the probability that a certain level of harm occurs.
- Many hazards having fatality as the worst outcome (severity 1) have a probability of fatality significantly less than 1 when it is GIVEN that the event occurs.
- Research of the literature surrounding settlements/jury awards related to wrongful death and serious injury reveals that the cost (not value) of human harm is very directly related to concepts such as intent and neglect.
- It might be expected that the cost (award/settlement) incurred for harm resulting from an event having a very low conditional probability of harm would be less than the payment exacted for the same level harm resulting from an event essentially guaranteed to cause harm if it occurred.
    - In other words, if you have reason to believe that an event is really likely to harm someone, you would be well advised to go to extremes to prevent its occurrence.
- While it is not recommended that the probability of harm/cost be explicitly included in the severity ($$) calculation, a qualitative assessment of harm likelihood given the hazard produces an accident could be used in selecting the severity ($$) to assign to a given level or injury/harm.

Summary

The discussion offered in this appendix is intended to encourage appropriate application of dollar cost assignment to human harm enabling the summing of risks across all assets exposed to system hazards. Accepting that payments represent program *costs* rather the *value* of human

assets is a critical first step. Published, *real world*, data have been reviewed and an example severity scale suggested. The example scale shown considers the impact of conditional probability of harm given the event on the resulting *cost*.

APPENDIX D: HAZARD SHEETS FOR FAST ASP EXAMPLE

Preliminary Hazard Analysis

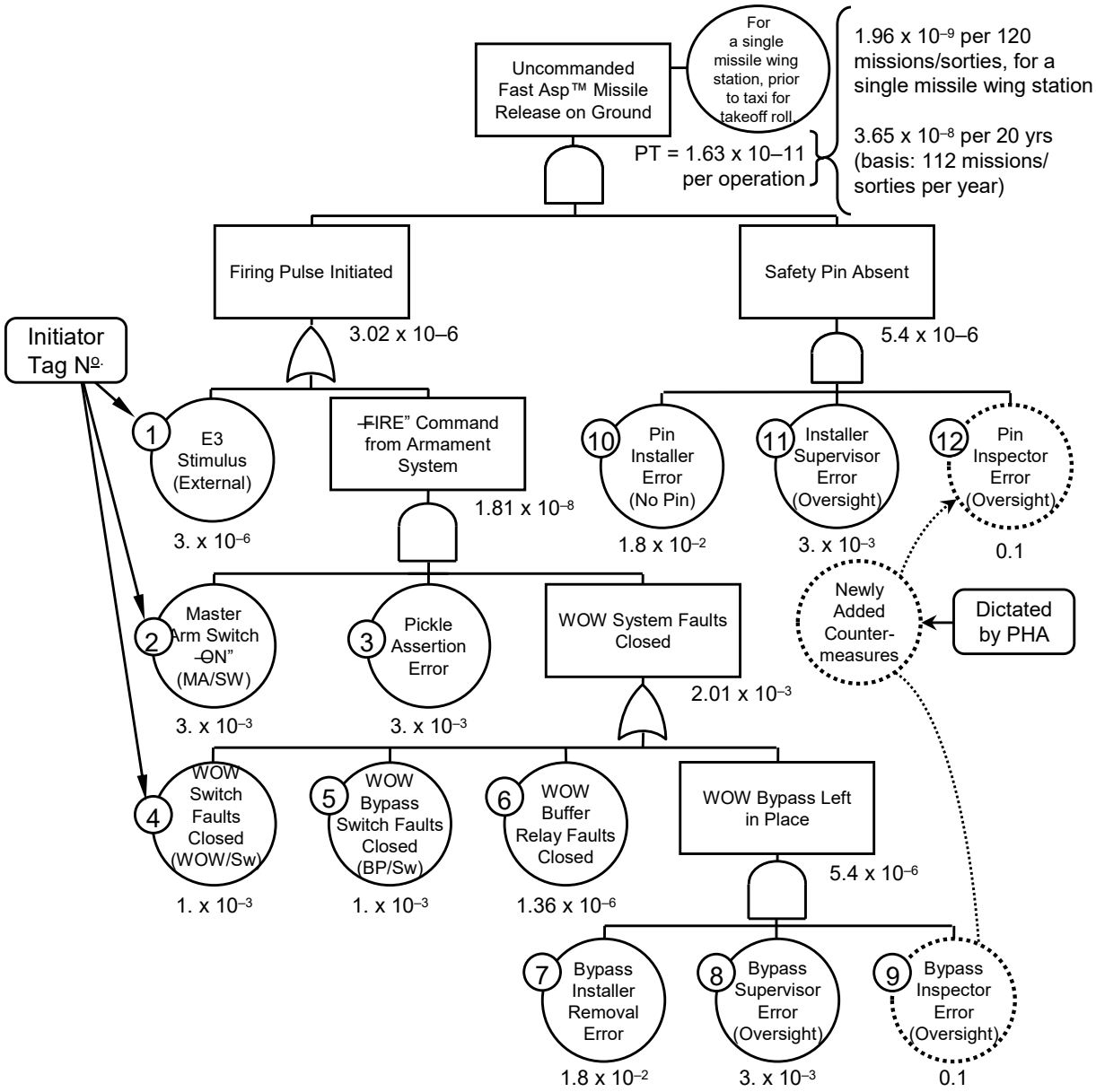
Hazard Description	Target	S	P*	RAC	Additional Countermeasures	S	P*	RAC
Uncommanded release of missile from wing pylon on ground, resulting in mass fire/explosion.	Personnel Equipment Downtime	I I II	C D D	1 2 3	1. Add level of formal, independent, sign-off, Safety Pin and WOW Bypass Switch inspections with —REMOVE BEFORE FLIGHT" banners (P/W). NOTE: Verify adequacy of countermeasures by Fault Tree Analysis.	I I II	E E E	3 3 3
Hung missile in unknown state: mission aborted for that missile; uncommanded release now more probable; downloading now more hazardous.	Personnel Equipment Downtime	I I III	C D D	1 2 3	1. Test/inspect launch system on ground w/dummy missile each 3 sorties (P). 2. Provide safe recovery area for hung-stores aircraft (S/P). 3. Verify valid Launching Cartridge dates (P).	I I III	E E E	3 3 3
Failure to release missile on FIRE command; potential loss of missile and aircraft (Pilot may eject).	Personnel Equipment Downtime	I I II	C D D	1 2 3	1. Countermeasure 1 for Hazard 2 (P). 2. Test/verify electrical ARM and FIRE functions with dummy loads during missile installation (P). 3. Add level of formal, independent, sign-off, Safety Pin inspections (P). 4. Train pilot in hi-G —pull-up," maneuver (P).	I I II	E E E	3 3 3
Failure to release missile on JETTISON command; potential for recovery with damaged aircraft and ordnance on board.	Personnel Equipment Downtime	I I III	D E E	2 3 3	1. Countermeasure 1 for Hazard 1 to ensure Safety Pin withdrawn (P). 2. Countermeasure 1 for Hazard 2 (P).	I I III	E E E	3 3 3
Arming of jettisoned missile with potential for impact on inhabited area, causing collateral damage.	Personnel Equipment Downtime	I I III	E E E	3 3 3	1. Test/verify Lanyard Restraining Solenoid tension during ARM and FIRE function test (P)1. 2. Redesign Master Arm circuit to —open" (disable) on jettison command (E)1. 1Optional; risk acceptable as-is.	I I III	E E E	3 3 3
Failure of live launch to arm, resulting in missile failure and loss of missile.	Personnel Equipment Downtime	I I II	C D D	1 2 3	1. Countermeasure 1 for Hazard 2 (P). 2. Countermeasure 1 for Hazard 5 (P).	I I II	E E E	3 3 3

Failure Modes and Effects Analysis

ITEM ID	FAILURE MODE	FAILURE CASE	FAILURE EFFECT	TARGET	S	P*	RAC	ACTION REQUIRED	S	P*	RAC
WOW Switch Contacts (WOW/Sw)	Open w/close command	1. Debris lodged in contacts 2. Arcing residue 3. Mechanical failure of contact spring	1. Lost launch-on-command capability 2. Potentially compromised jettison capability	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2. Replace switch after 60 sorties (P).	I I II	E E E	3 3 3
WOW Switch Contacts (WOW/Sw)	Closed w/open command	1. Overcurrent welding 2. Arcing (Over amps) 3. Mechanical failure of contact spring	1. Potential for inadvertent launch on ground (MA and Pickle protect)	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2. Replace switch after 60 sorties (P).	I I II	E E E	3 3 3
WOW Bypass Switch Contacts (BP/Sw) (Manual Toggle)	Open w/close command	1. Debris lodged in contacts 2. Arcing residue 3. Mechanical failure of contact spring	1. Ground tests of launch components compromised.	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2. Replace switch after 60 sorties (P).	I I II	E E E	3 3 3
WOW Bypass Switch Contacts (BP/Sw) (Manual Toggle)	Closed w/open command	1. Overcurrent welding 2. Arcing (Over amps) 3. Mechanical failure of contact spring	1. Potential for inadvertent launch on ground (MA and Pickle protect)	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2. Replace switch after 60 sorties (P).	I I II	E E E	3 3 3

Failure Modes and Effects Analysis

ITEM ID	FAILURE MODE	FAILURE CASE	FAILURE EFFECT	TARGET	S	P*	RAC	ACTION REQUIRED	S	P*	RAC
WOW Buffer Relay Contacts	Open w/close command	1. Debris lodged in contacts 2. Arcing residue 3. Mechanical failure of contact spring	1. Lost launch-on-command capability 2. Potentially compromised jettison capability	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2. Replace relay after 60 sorties (P).	I I II	E E E	3 3 3
WOW Buffer Relay Contacts	Closed w/open command	1. Overcurrent welding 2. Arcing (Over amps) 3. Mechanical failure of contact spring	1. Potential for inadvertent launch on ground (MA and Pickle protect)	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2. Replace relay after 60 sorties (P).	I I II	E E E	3 3 3
WOW Buffer Relay Coil	Open w/voltage applied	1. Burnout from prior use	1. Ground tests of launch components compromised.	Personnel Equipment Downtime	I I II	D E E	2 3 3	1. Test/inspect each 3 sorties (P). 2. Replace relay after 60 sorties (P).	I I II	E E E	3 3 3



Fault Tree Analysis

Failure Probability Data

Tag / Item	Probability*	Source	Comments
1 / E3 Stimulus (off-board sources)	3.0×10^{-6}	Engineering estimate, basis: compliance with MIL-STD-464 for pyrotechnic no-fire threshold protection of <16.5 dB	MIL-STD-464: Fast Asp™ complies
2 / Master Arm "ON" (MA/Sw)	3.0×10^{-3}	Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 / [Log 446]	General human error of commission
3 / Pickle Asserted	3.0×10^{-3}	Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 / [Log 446]	General human error of commission
4 / WOW Switch Faults Closed (WOW/Sw)	1.0×10^{-3}	WASH 1400 (NUREG-75/014), Appendix III; US Nuclear Regulatory Commission, October 1975 / [Log 1053]	"…high" probability rating from source is used here
5 / WOW Bypass Switch Faults Closed (BP/Sw)	1.0×10^{-3}	WASH 1400 (NUREG-75/014), Appendix III; US Nuclear Regulatory Commission, October 1975 / [Log 1053]	"…high" probability rating from source is used here
6 / WOW Buffer Relay Faults Closed	1.36×10^{-6}	IEEE Std 500 [Log 3.2.6.1]	Contacts fault closed in prior use
7 / Bypass Sw Installer Error	1.8×10^{-2}	Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 / [Log 442]	—Improper connection of mechanical linkage”
8 / Bypass Sw Installer Supervisor Error	3.0×10^{-3}	Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X / [Log 454]	—Failure of visual inspection for defined criterion”
9 / Independent Bypass Sw Inspector Error**	1.0×10^{-1}	Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X / [Log 460]	—Fail to recognize incorrect status on inspection”
10 / Pin Installer Error (Pin not fitted)	1.8×10^{-2}	Risk Analysis Report to the Rijnmond Public Authority, D.Reidel Publishing Co., 1981 ISBN 90-277-1393-6 / [Log 442]	Improper connection of mechanical linkage
11 / Pin Installer Supervisor Error	3.0×10^{-3}	Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X / [Log 454]	—Failure of visual inspection for defined criterion”
12 / Independent Pin Inspector Error**	1.0×10^{-1}	Reliability and Maintainability in Perspective, 3rd Edition, D.J. Smith, 1988 ISBN 0-333-46205-X / [Log 460]	—Fail to recognize incorrect status on inspection”

*Per operation
**If analysis indicates need for independent inspector (provisional)

APPENDIX E: CHEMICAL PROCESSING EXAMPLE (WITH HAZARD SHEETS)

- Chem/Int-001: Flange Seal A-29 Leakage
- Chem/Int-002: Backflow Preventer Failure
- Chem/Int-003: Cooler Leak
- Chem/Int-004: Catalyst Overcharge
- Chem/Int-005: Catalyst Agitation Failure
- Chem/Int-006: Macerator Failure
- Chem/Int-007: Float Switch Failure
- Reactor-001: Reactor Overpressure
- Reactor-002: Catalyst Under Feed
- Reactor-003: Incomplete Reaction
- Stack-001: Stack Fire/Explosion

APPLYING RISK SUMMING METHODS TO A PRACTICAL EXAMPLE—EXAMPLE 2

This section applies the methodology described in Section 4.0 to a practical example. The hypothetical system is first described and then each step is performed showing example products at each point in the process.

The example activity is a chemical process designed to cause a specific reaction generating the desired chemical product. In this system/process (Figure E-1), a day tank supplies a noxious catalyst to a reactor vessel at approximately constant pressure in order to sustain the reaction. The reaction is designed to produce a desired chemical product (i.e., propellant). The initial process/system design contains several controls to ensure that proper conditions are maintained. These include:

- a float switch/pump system that prevents the catalyst level from falling too low or rising too high by bringing additional catalyst from a reservoir when needed or interrupting flow,
- an overflow dump that captures overflow in the event of pump overrun,
- a cooling system ensuring the catalyst enters the reactor vessel at the proper temperature,
- a backflow prevention valve that prevents reacted catalyst from re-entering the day tank.

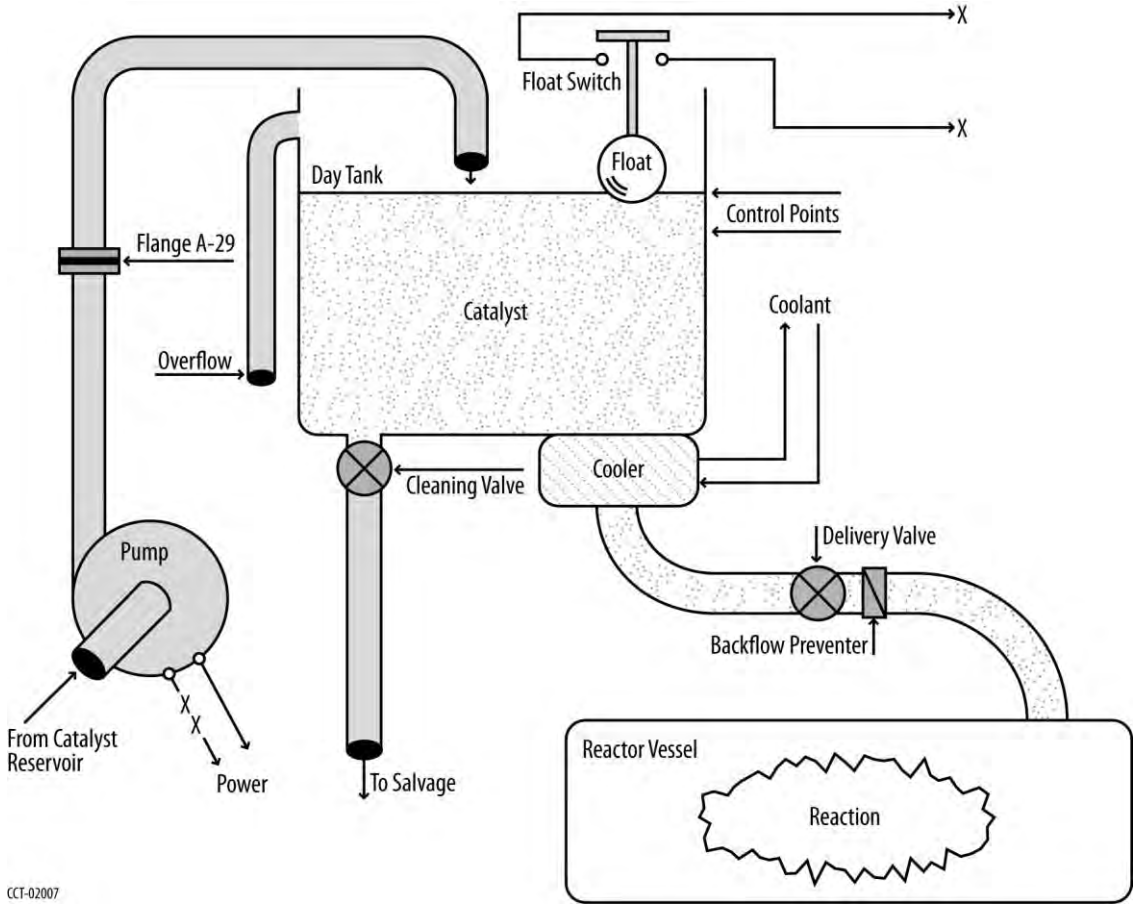


Figure E-1. System Assessed in Risk Summing Example

The hazards posed by this example activity must be assessed before risk summing can be implemented to compute the total risk and the total risk measures used to communicate the results.

STEP 1: DEFINE THE RAC

Those assessing the example activity desire to use a tailored RAC that is based on the guidance provided by MIL-STD-882D. Beginning with logarithmic, Cartesian axes have probability as the *x*-axis and severity for the *y*-axis as shown in Figure E-2.

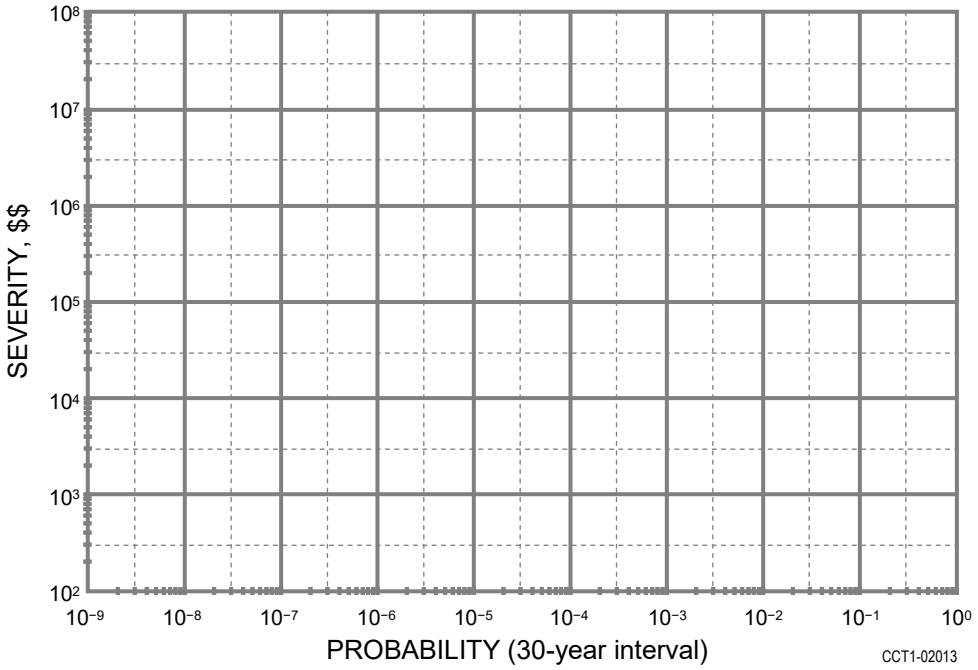


Figure E-2. Selected RAC Axes

The figure clearly depicts several decisions that have already been made that will affect the manner in which hazards of the example activity are assessed.

- The choice of Cartesian axes with increasing values further from the origin intentionally pushes the highest risk to the top right of the scale.
- The *x*-axis explicitly states the exposure interval. This is the time duration over which the example activity is to be analyzed.
- The *y*-axis states the units that will be used to express mishap severity. As the selected unit, dollars ($$) will be used to quantify the impact to all assets considered in the analysis.
- Though the *x*-axis shown in the figure ends at 1.0 (1×10^0), it is noted that this axis could be extended if likelihood were expressed as frequency rather than probability.

Next, categories will be defined that will be used for qualitatively assessing severity and the categories used to assess probability. As shown in Figure E-3, numerical values assigned to define the severity categories comply with those identified in MIL-STD 882D with one exception: $20k is the value separating categories III and IV rather than $10k as shown in Table 1 in Section 4.1.1. The reader should also note that dividing the probability axis into categories

that span a decade each might be desirable when qualitatively assessing mishap likelihood. In this case, category D would be broken into three sub-categories as shown in the figure.

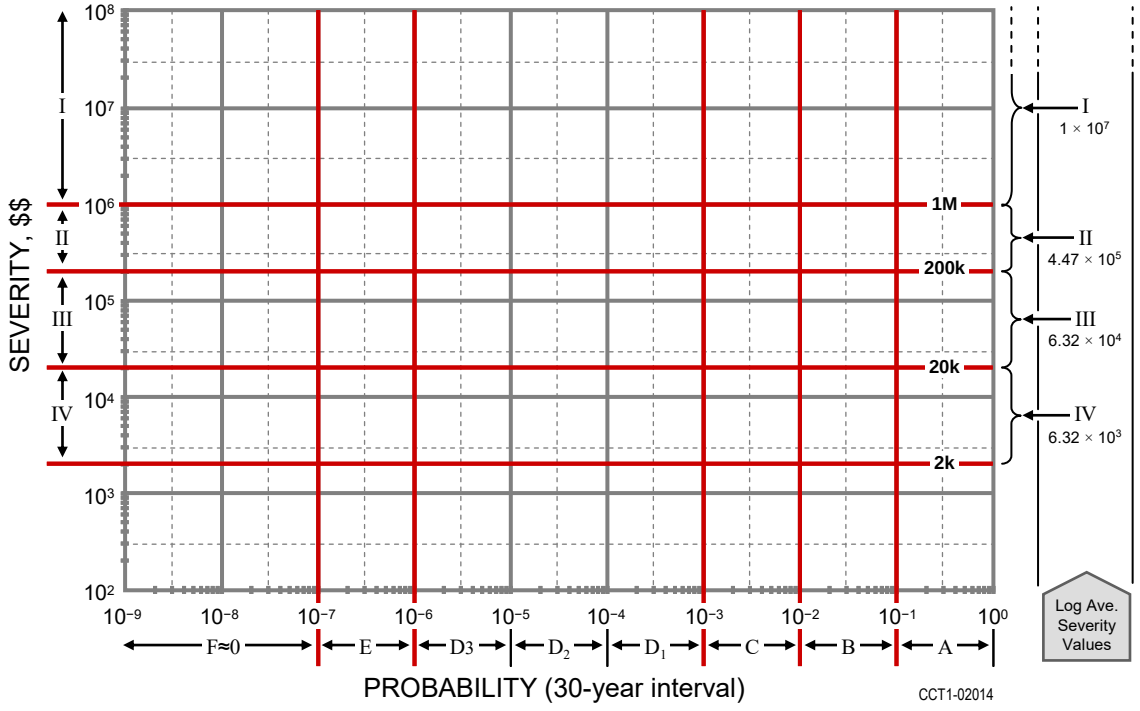


Figure E-3. Probability and Severity Categories

Note also that Figure E-3 specifies the mid-points used to represent each severity category when performing risk summing calculations. These represent the "geometric mean" or "log average" of each category. For example, the midpoint of category III is computed to be:

$$\sqrt{\$20K \times \$200K} = 6.32 \times 10^{4} \qquad \text{(Eq E-1)}$$

The midpoints of probability categories are each represented as 3.2×10^{x}, since each category spans a complete decade.

Lastly, probability and severity category definitions must be finished by tailoring the text descriptions used when qualitatively assessing each hazard. The program has no issues with the definitions provided by Table 1 and Table 2 in 4.1.1. These definitions, however, do not completely satisfy the need since they only define harm to personnel, equipment, or the environment.

Mishaps during the example activity can also produce quantifiable ($$) losses due to system down time and loss of product. Since these are to be assessed in the hazard analysis, clear definitions for severity levels must be provided here. For this example activity, the severity definitions in Table 1 are augmented to include:

Category I:	Downtime exceeding one month. Product spoilage exceeding one month's production.
Category II:	Downtime exceeding one week, but less than one month. Product spoilage exceeding one week's production, but less than one month's.
Category III:	Downtime exceeding one shift, but less than one week.

	Product spoilage exceeding one shift's production, but less than one week's.
Category IV:	Downtime exceeding one hour, but less than one shift. Product spoilage exceeding one hour's production, but less than one shift's.

These qualitative definitions are designed to correspond to the quantified cost of such losses based on profit generated by specific product quantities, and the value of raw materials, power, etc. involved in producing the spoiled product.

STEP 2: PERFORM HAZARD ANALYSIS

A thorough and complete hazard analysis has been performed to:

- identify the hazards posed to the five selected assets (personnel, equipment, downtime, environment, and product),
- assess the cost of losses anticipated from mishaps resulting from identified hazards,
- assess the likelihood that these mishaps will occur during the 30-year life cycle proposed for a single production line, and
- identify mitigations available to reduce the cost impact or probability of a mishap.

The results of the first three actions have been documented in hazard sheets that will support summing the initial total risk prior to mitigations. Feasible design changes that may be made to mitigate losses due to mishaps have also been selected as illustrated in Figure E-4 (in red).

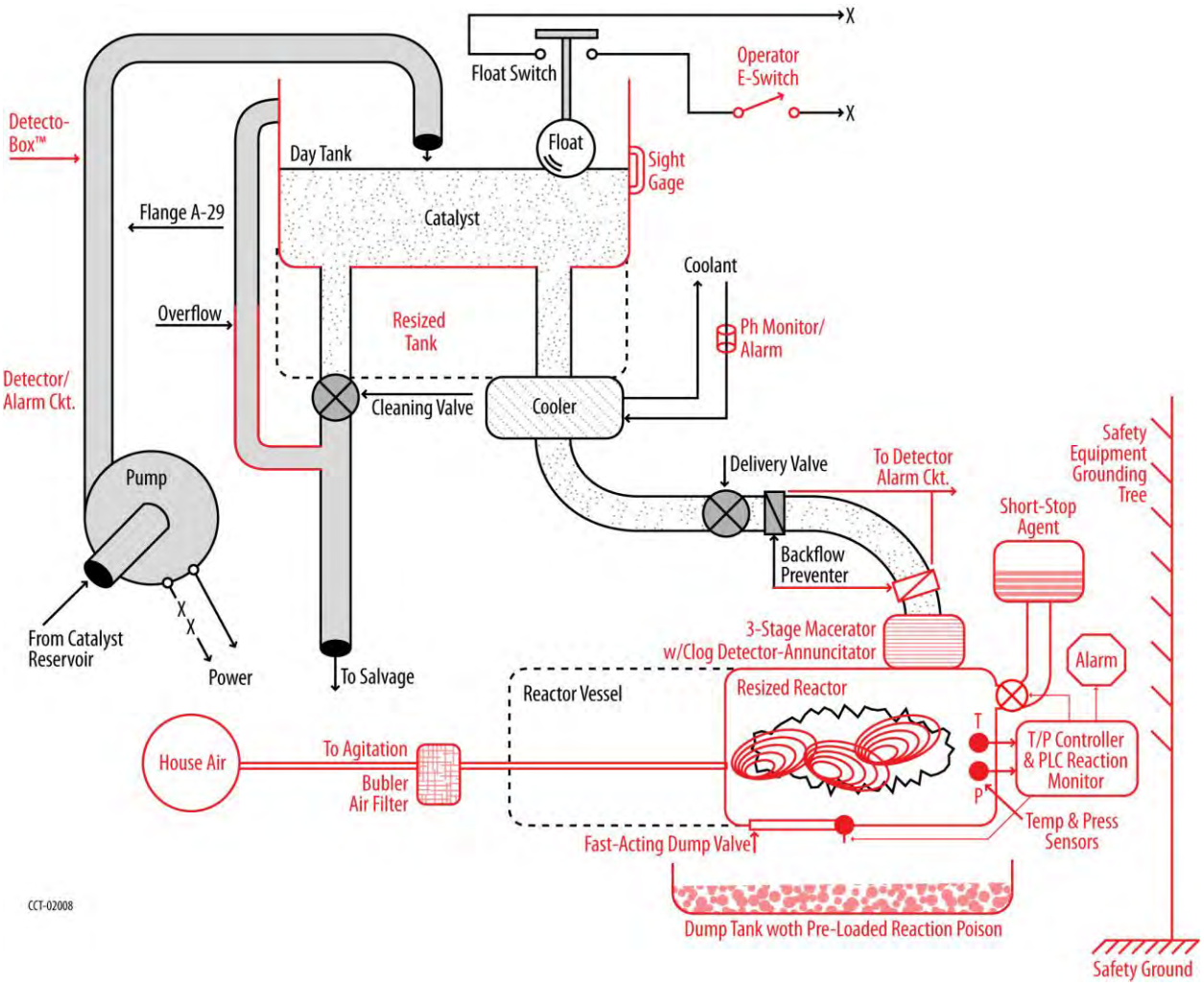


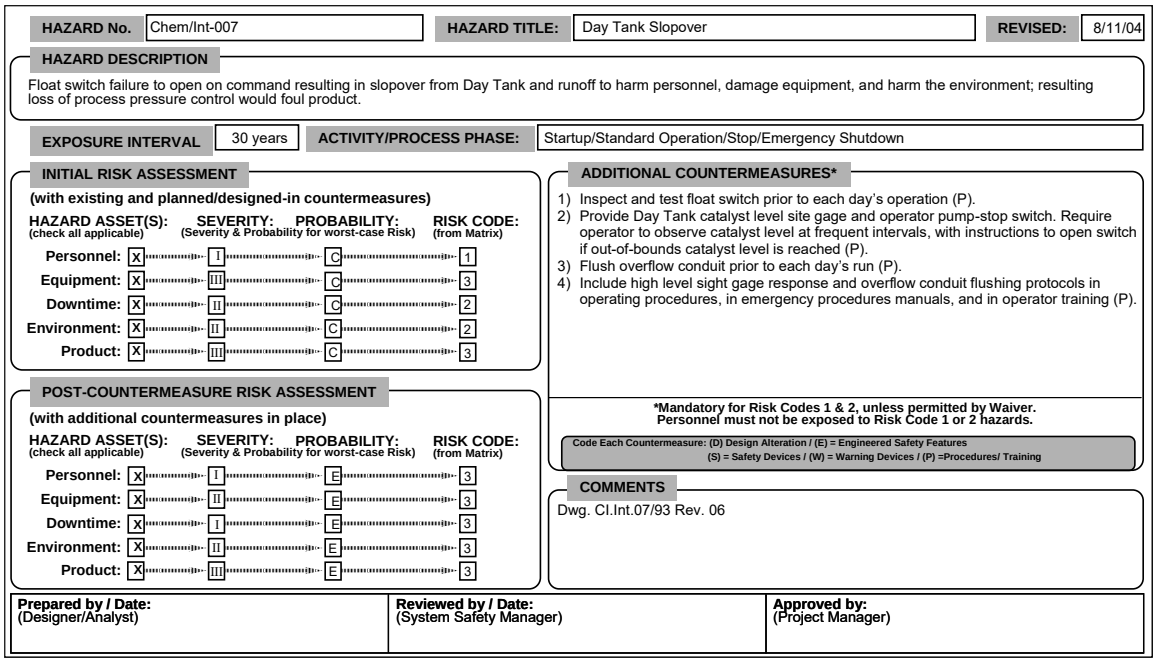
Figure E-4. Design Changes Supporting Mishap Mitigation

Hazard mitigation changes include:

- Elimination of unreliable components such as Flange A-29.
- Adding numerous alarms, sensors, operator monitors, gauges, and controls.
- Features to reduce loss of raw materials.
- Optimized tank sizing to better control the chemical reaction, reduce waste, and reduce quantity of catalyst available to contribute to a —caustic punch=thorough" spill.

The safety analysis proceeded to include re-assessment of each hazard's probability and severity component after these mitigations have been implemented.

The sample hazard sheet shown in Figure E-5 defines a hazard, assigns it a unique identifier, and assesses mishap probability and severity due to the hazard both before and after applying available mitigations. The complete hazard sheet set used to assess the example activity is provided at the end of this appendix.



HAZARD No. Chem/Int-007 **HAZARD TITLE:** Day Tank Slopover **REVISED:** 8/11/04

HAZARD DESCRIPTION

Float switch failure to open on command resulting in slopover from Day Tank and runoff to harm personnel, damage equipment, and harm the environment; resulting loss of process pressure control would foul product.

EXPOSURE INTERVAL 30 years **ACTIVITY/PROCESS PHASE:** Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY:	RISK CODE: (from Matrix)
Personnel:	X	I	C	1
Equipment:	X	III	C	3
Downtime:	X	II	C	2
Environment:	X	II	C	2
Product:	X	III	C	3

ADDITIONAL COUNTERMEASURES*

1) Inspect and test float switch prior to each day's operation (P).
2) Provide Day Tank catalyst level site gage and operator pump-stop switch. Require operator to observe catalyst level at frequent intervals, with instructions to open switch if out-of-bounds catalyst level is reached (P).
3) Flush overflow conduit prior to each day's run (P).
4) Include high level sight gage response and overflow conduit flushing protocols in operating procedures, in emergency procedures manuals, and in operator training (P).

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY:	RISK CODE: (from Matrix)
Personnel:	X	I	E	3
Equipment:	X	II	E	3
Downtime:	X	I	E	3
Environment:	X	II	E	3
Product:	X	III	E	3

*Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features (S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 06

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

Figure E-5. Sample Hazard Sheet

STEP 3: ENTER HAZARDS IN SPREADSHEET

When the RAC matrix has been fully defined and the hazard analysis completed, the individual hazards and their assessments must be entered into an application having the capability to compute the quantitative results required by the next few steps. Microsoft Excel® provides a convenient and readily available tool for this purpose. In addition to performing straightforward partial risk computations and summing the total risk, Excel® can automate the more complicated calculations involved in computing the various risk measures.

A sample from the example matrix containing pre-mitigation data for the first four hazards is shown in Figure E-6 and the complete matrix is provided at the end of this appendix.

A	B	C	D	E	F	G	H
Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$	Notes
CI-001	Flange Seal A-29 Leakage - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
CI-001	Flange Seal A-29 Leakage - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
CI-001	Flange Seal A-29 Leakage - Downtime	III	C	$ 63,200	3.20E-03	$ 202.24	
CI-001	Flange Seal A-29 Leakage - Environment	III	C	$ 63,200	3.20E-03	$ 202.24	
CI-002	Backflow Contamination - Equipment	III	B	$ 63,200	3.20E-02	$ 2,022.40	
CI-002	Backflow Contamination - Downtime	III	B	$ 63,200	3.20E-02	$ 2,022.40	
CI-002	Backflow Contamination - Product	III	B	$ 63,200	3.20E-02	$ 2,022.40	
CI-003	Cooler Leak - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
CI-003	Cooler Leak - Downtime	II	C	$ 447,000	3.20E-03	$ 1,430.40	
CI-003	Cooler Leak - Product	III	C	$ 63,200	3.20E-03	$ 202.24	
CI-004	Catalast Overcharge - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
CI-004	Catalast Overcharge - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
CI-004	Catalast Overcharge - Environment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
CI-004	Catalast Overcharge - Downtime	III	C	$ 63,200	3.20E-03	$ 202.24	

Figure E-6. Initial Hazard Spreadsheet for Example Activity – partial

The same portion from the final (post-mitigation) matrix is shown in Figure E-7.

A	B	C	D	E	F	G	H
Haz ID	**Short Title**	**Sev. Cat**	**Prob. Cat**	**Sev. Value**	**Prob. Value**	**Partial Risk, $$**	**Notes**
CI-001	Flange Seal A-29 Leakage - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.20	
CI-001	Flange Seal A-29 Leakage - Equipment	II	D	$ 447,000	3.20E-05	$ 14.30	
CI-001	Flange Seal A-29 Leakage - Downtime	III	D	$ 63,200	3.20E-05	$ 2.02	
CI-001	Flange Seal A-29 Leakage - Environment	III	D	$ 63,200	3.20E-05	$ 2.02	
CI-002	Backflow Contamination - Equipment	III	C	$ 63,200	3.20E-03	$ 202.24	
CI-002	Backflow Contamination - Downtime	III	C	$ 63,200	3.20E-03	$ 202.24	
CI-002	Backflow Contamination - Product	III	C	$ 63,200	3.20E-03	$ 202.24	
CI-003	Cooler Leak - Equipment	II	D	$ 447,000	3.20E-05	$ 14.30	
CI-003	Cooler Leak - Downtime	II	D	$ 447,000	3.20E-05	$ 14.30	
CI-003	Cooler Leak - Product	III	D	$ 63,200	3.20E-05	$ 2.02	
CI-004	Catalast Overcharge - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.20	
CI-004	Catalast Overcharge - Equipment	II	D	$ 447,000	3.20E-05	$ 14.30	
CI-004	Catalast Overcharge - Downtime	III	D	$ 63,200	3.20E-05	$ 2.02	
CI-004	Catalast Overcharge - Environment	III	D	$ 63,200	3.20E-05	$ 2.02	

Figure E-7. Final (Post-Mitigation) Hazard Spreadsheet for Example Activity – partial

Numerous changes to the individual hazard-asset pairs assessments resulted from changes made to reduce activity risk. For example, the hazard CI-001 (personnel) assessment changed from ID to IE reducing the assessed loss from $320.00 to $3.20. The partial risk posed by hazard CI-004 to the environment was reduced in both severity and probability (from IIC to IIID) reducing the associated loss estimate from $1,430.00 to $2.02.

Figure E-8 shows the end of the initial matrix, including the total risk value and the values computed for each of the total risk measures.

A	B	C	D	E	F	G	H
Haz ID	**Short Title**	**Sev. Cat**	**Prob. Cat**	**Sev. Value**	**Prob. Value**	**Partial Risk, $$**	**Notes**
S-001	Stack Fire/Explosion - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
S-001	Stack Fire/Explosion - Equipment	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
S-001	Stack Fire/Explosion - Downtime	II	C	$ 447,000	3.20E-03	$ 1,430.40	
S-001	Stack Fire/Explosion - Environment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
S-001	Stack Fire/Explosion - Product	III	C	$ 63,200	3.20E-03	$ 202.24	
						$ 192,197.13	**Total Risk**
	Expected Loss Rate			$ 192,197	1.00E+00		
	Maximum Loss			$ 10,000,000	1.92E-02		
	Most Probable Loss			$ 63,200	3.04E+00	10,000,000	
	Conditional Loss Rate			$ 814,168.82	2.36E-01		

Figure E-8. Bottom Portion of Initial Example Spreadsheet with Total Risk and Risk Measures

STEP 4: COMPUTE PARTIAL RISKS

As described in Section 4.1.4, the partial risk associated with each hazard-asset combination is computed as the simple product of the numerical severity value and the numerical probability value. In the example matrices (Figure E-6 and Figure E-7), the partial risk value is displayed in Column G; the partial risk value is the product of the values displayed in Columns E and F. For example, Figure E-6 shows a $10 million ($\$1.00 \times 10^7$) severity with a 3.20×10^{-5} occurrence probability for the hazard that CI-001 poses to personnel. Multiplying these values produces a partial risk of $\$3.2 \times 10^2$, or $320.00, posed by hazard CI-001 to personnel.

STEP 5: COMPUTE TOTAL RISK

Section 4.1.5 explains that the total risk parameter is obtained by simply summing the partial risk values for each hazard-asset combination. Figure E-8 shows the total risk value prior to applying mitigations for the example activity. Column G is summed to compute the $192,197.13 value

shown in the figure. This value is then used as the basis for the risk measures computed in Step 6.

STEP 6: COMPUTE TOTAL RISK MEASURES

When potential for losses across multiple assets are assessed or the hazard population quantity is high, the matrix described in Section 5.3 and shown at the end of this appendix can become quite large. Manually computing risk measures for large matrices becomes cumbersome and presents plentiful opportunities for human error to enter the calculations. Using a spreadsheet tool is recommended even if the process used to calculate the risk measures has not been automated.

This section walks through a process that supports computing the risk measures when a fully automated spreadsheet tool is not available. For this exercise, it is assumed that the user has completed Step 3 by constructing a simple spreadsheet matrix similar to that shown in Figure E-6 and entering the data from the Hazard Sheets provided. It is further assumed that Steps 4 and 5 have been completed by entering the formulas needed to compute the partial risks in Column G and to sum these partial risks to develop the total risk value displayed at the end of Column G, as shown in Figure E-8.

The following subsections walk through the steps required to calculate each risk measure using the initial, pre-mitigation data for the example activity. Repeating this process using the post-mitigation data provided in the Hazard Sheets is left as an exercise. Computed risk measure values for both pre- and post- mitigated activity risk are provided in Section 5.6.4 for use in verifying results.

Measure 1: Expected Loss Rate

The Expected Loss Rate uses the Total System Risk as its severity component and unity (1.0) for its probability component. For the example activity, then:

S = $192,197.13
P = 1.0

For similar systems operated for the planned 30-year duration used in the hazard analysis, one would expect that, on the average, systems would produce $192,197.13 in losses due to mishaps described in the analysis. This figure does not address losses due to unidentified hazards.

Measure 2: Conditional Loss Rate

The Conditional Loss Rate measure, pairs the probability that a hazard in ANY severity category produces a mishap with the effective severity required to produce the total risk value. Good use is made of the values computed in Section 5.6.5 when computing Most Probable Loss. Table E-1 provides convenient access to the data required to compute this measure.

Table E-1. Mishap Probability Data (All Categories)

Severity Category	Mishap Probability	1 minus Probability
I	1.62×10^{-2}	0.9838
II	3.47×10^{-2}	0.9653
III	1.96×10^{-1}	0.804
IV	0.00×10^{0}	1.0000

Multiplying the values in the right-most column computes the probability that NO hazard in any category produces a mishap. Subtracting this value from 1.0 produces the probability that SOME mishap occurs:

$$P_{CLR} = 1-(1-P_I)\times(1-P_{II})\times(1-P_{III})\times(1-P_{IV}) = 1-0.9838\times0.9653\times0.804 = 2.36\times10^{-1} \quad \text{(Eq E-2)}$$

Then using this value for *PCLR*, the severity component is computed by:

$$S_{CLR} = \frac{\text{Total Risk}}{P_{CLR}} = \frac{\$192{,}197.\text{B}}{2.36\text{x}10^{-1}} = \$817{,}168.\text{82} \quad \text{(Eq E-3)}$$

Measure 3: Risk Profile for Example Activity

The risk profile described in Section 4.1.6.3 can be plotted by pairing the occurrence probability for each severity category (shown in Table E-1) with that category's numerical ($$) loss value. Table E-2 summarizes the previously computed data used to plot the pre-mitigation Risk Profile.

Table E-2. Risk Profile Data – Initial, Pre-Mitigation

Severity Category	Probability (x-value)	Severity (midpoint)
I	1.62×10^{-2}	$10,000,000
II	3.47×10^{-2}	$447,000
III	1.96×10^{-1}	$63,200
IV	0.00×10^{0}	$6,320

Figure E-69 plots this Pre-Mitigation Risk Profile along with the Individual Hazards, the total risk isorisk contour, and the four total risk measures computed in the preceding sections.

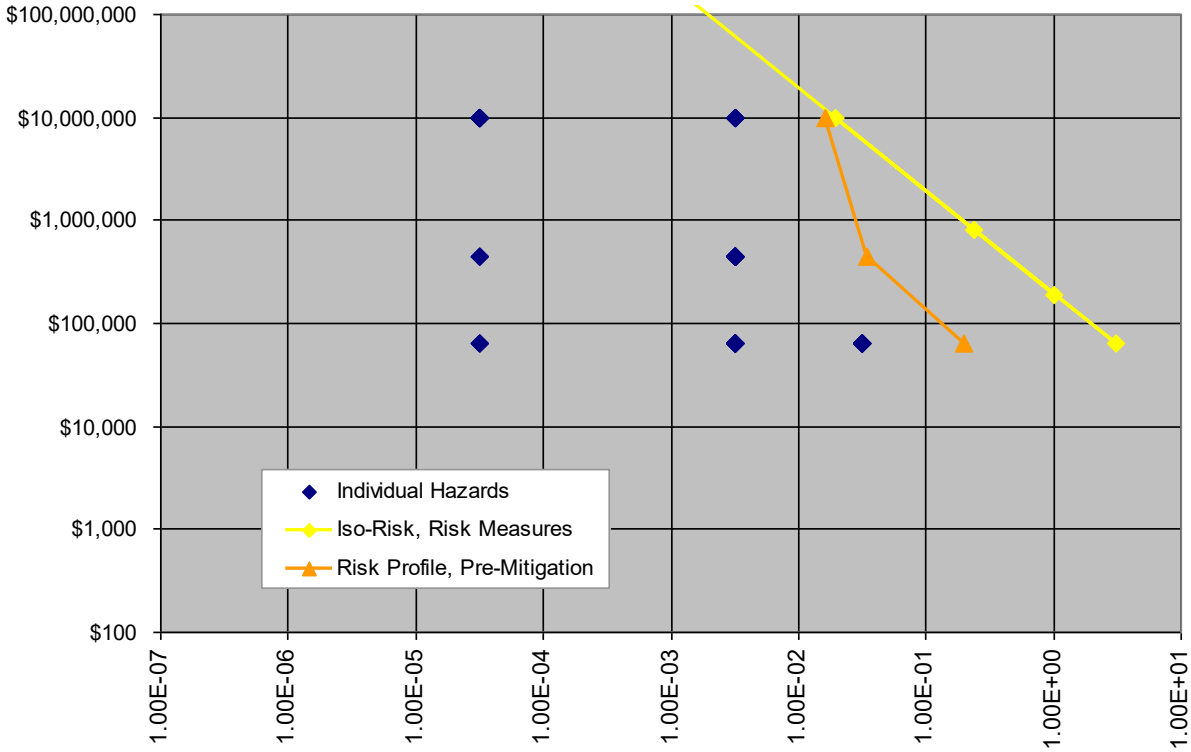


Figure E-9. Example Activity Risk Profile Plot – Initial, Pre-Mitigation

Maximum Loss (Info Only)

To determine the probability and severity components for the Maximum Loss measure, one must first identify the highest assessed severity for any hazard-asset combination identified by the hazard analysis. If no studies have been done to quantify mishap severity, then one need to only identify the highest severity category assessed in the matrix—its assigned midpoint value is then used as the Maximum Loss severity component. If "non-standard" severities have been assigned, then these must be considered when determining the maximum severity. In either case, one can simply use the spreadsheet "MAX" function to determine the maximum severity value entered in Column E. For the example, the equation to enter into a spreadsheet cell would be =MAX(E3:E44). For the example activity, this process should yield a severity value equal to $10,000,000.00. The effective probability considering total risk for this example would be calculated by:

$$P = \frac{\text{Total Risk}}{\text{Maximum Loss}} = \frac{\$192,197.13}{\$10,000,000.00} = 1.92 \times 10^{-2} \qquad \text{(Eq E-4)}$$

The maximum loss measure is then described by:

S = $10,000,000.00
P = 1.92×10^{-2}

Most Probable Loss (Info Only)

To determine the severity and total risk probability for the Most Probable Loss, first the severity level most likely to occur must be determined. Again, this can be done manually or by applying a computational tool.

This is accomplished by determining, for each severity category, the combined probability that some hazard assessed to have that severity produces a mishap. All the hazard-asset pairs must first be sorted into the four severity categories. This can be done manually by selecting a severity category and recording probability values for each hazard-asset pair assessed to produce loss in that category. It may more easily be accomplished by using the Sort function in Microsoft Excel®. To sort, first highlight all columns for each hazard-asset pair as shown in Figure E-7.

	A	B	C	D	E	F	G	H
1	A	B	C	D	E	F	G	H
2	Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$	Notes
3	CI-001	Flange Seal A-29 Leakage - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
4	CI-001	Flange Seal A-29 Leakage - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
5	CI-001	Flange Seal A-29 Leakage - Downtime	III	C	$ 63,200	3.20E-03	$ 202.24	
6	CI-001	Flange Seal A-29 Leakage - Environment	III	C	$ 63,200	3.20E-03	$ 202.24	
7	CI-002	Backflow Contamination - Equipment	III	B	$ 63,200	3.20E-02	$ 2,022.40	
8	CI-002	Backflow Contamination - Downtime	III	B	$ 63,200	3.20E-02	$ 2,022.40	
9	CI-002	Backflow Contamination - Product	III	B	$ 63,200	3.20E-02	$ 2,022.40	
10	CI-003	Cooler Leak - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
11	CI-003	Cooler Leak - Downtime	II	C	$ 447,000	3.20E-03	$ 1,430.40	
12	CI-003	Cooler Leak - Product	III	C	$ 63,200	3.20E-03	$ 202.24	
13	CI-004	Catalast Overcharge - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
14	CI-004	Catalast Overcharge - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
15	CI-004	Catalast Overcharge - Environment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
16	CI-004	Catalast Overcharge - Downtime	III	C	$ 63,200	3.20E-03	$ 202.24	
17	CI-005	Catalyst Agitation Failure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
18	CI-005	Catalyst Agitation Failure - Equipment	I	D	$ 10,000,000	3.20E-05	$ 320.00	
19	CI-005	Catalyst Agitation Failure - Downtime	I	D	$ 10,000,000	3.20E-05	$ 320.00	
20	CI-005	Catalyst Agitation Failure - Environment	II	D	$ 447,000	3.20E-05	$ 14.30	
21	CI-005	Catalyst Agitation Failure - Product	III	D	$ 63,200	3.20E-05	$ 2.02	
22	CI-006	Macerator Failure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
23	CI-006	Macerator Failure - Equipment	I	D	$ 10,000,000	3.20E-05	$ 320.00	
24	CI-006	Macerator Failure - Downtime	I	D	$ 10,000,000	3.20E-05	$ 320.00	
25	CI-006	Macerator Failure - Environment	II	D	$ 447,000	3.20E-05	$ 14.30	
26	CI-006	Macerator Failure - Product	III	D	$ 63,200	3.20E-05	$ 2.02	
27	CI-007	Day Tank Slopover - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
28	CI-007	Day Tank Slopover - Downtime	II	C	$ 447,000	3.20E-03	$ 1,430.40	
29	CI-007	Day Tank Slopover - Environment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
30	CI-007	Day Tank Slopover - Equipment	III	C	$ 63,200	3.20E-03	$ 202.24	
31	CI-007	Day Tank Slopover - Product	III	C	$ 63,200	3.20E-03	$ 202.24	
32	R-001	Reactor Overpressure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00	
33	R-001	Reactor Overpressure - Equipment	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
34	R-001	Reactor Overpressure - Downtime	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
35	R-001	Reactor Overpressure - Environment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
36	R-001	Reactor Overpressure - Product	II	C	$ 447,000	3.20E-03	$ 1,430.40	
37	R-002	Catalyst Underfeed - Downtime	III	B	$ 63,200	3.20E-02	$ 2,022.40	
38	R-002	Catalyst Underfeed - Product	III	B	$ 63,200	3.20E-02	$ 2,022.40	
39	R-003	Incomplete Reaction - Product	III	B	$ 63,200	3.20E-02	$ 2,022.40	
40	S-001	Stack Fire/Explosion - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
41	S-001	Stack Fire/Explosion - Equipment	I	C	$ 10,000,000	3.20E-03	$ 32,000.00	
42	S-001	Stack Fire/Explosion - Downtime	II	C	$ 447,000	3.20E-03	$ 1,430.40	
43	S-001	Stack Fire/Explosion - Environment	II	C	$ 447,000	3.20E-03	$ 1,430.40	
44	S-001	Stack Fire/Explosion - Product	III	C	$ 63,200	3.20E-03	$ 202.24	
45							$ 192,197.13	Total Risk
46		Expected Loss Rate			$ 192,197	1.00E+00		
47		Maximum Loss			$ 10,000,000	1.92E-02		
48		Most Probable Loss			$ 63,200	3.04E+00	10,000,000	
49		Conditional Loss Rate			$ 814,168.82	2.36E-01		
50	Notes:				1000000000	1.92E-04		

Figure E-10. Example Matrix (Initial) with Data Selected

With all entered data selected, select the following menu options: [Data > Sort > Sort by: Column C, Ascending, No Header Row]. This operation should sort the hazard data so that all severity category I hazards appear at the top of the matrix, as shown in Figure E-8, Columns A-H.

A	B	C	D	E	F	G	H	I	J
Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$	Notes		
CI-001	Flange Seal A-29 Leakage - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
CI-004	Catalast Overcharge - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
CI-005	Catalyst Agitation Failure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
CI-005	Catalyst Agitation Failure - Equipment	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
CI-005	Catalyst Agitation Failure - Downtime	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
CI-006	Macerator Failure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
CI-006	Macerator Failure - Equipment	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
CI-006	Macerator Failure - Downtime	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
CI-007	Day Tank Slopover - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00		0.996800	
R-001	Reactor Overpressure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320.00		0.999968	
R-001	Reactor Overpressure - Equipment	I	C	$ 10,000,000	3.20E-03	$ 32,000.00		0.996800	
R-001	Reactor Overpressure - Downtime	I	C	$ 10,000,000	3.20E-03	$ 32,000.00		0.996800	
S-001	Stack Fire/Explosion - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000.00		0.996800	
S-001	Stack Fire/Explosion - Equipment	I	C	$ 10,000,000	3.20E-03	$ 32,000.00		0.996800	1.62E-02
CI-001	Flange Seal A-29 Leakage - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430.40		0.996800	
CI-003	Cooler Leak - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430.40		0.996800	

Figure E-11. Computing Combined Probability for Severity Category I

Next, when computed the probability that the hazard-asset pair did NOT produce a mishap. This is done by subtracting the probability that it *did* occur from unity (1.0) as shown in Figure E-8, Column I. The equation used was:

$$\text{Column I Value} = 1.0 - \text{Column F Value} \qquad \text{(Eq E-5)}$$

If this process is to be performed manually, care must be taken to retain enough significant figures.

Next, all the probabilities for severity category I in matrix Column I are multiplied together to determine the probability that NO hazard-asset pair in category I occurs. The probability that SOME category I mishap occurs is simply one minus that probability that it does not. As Figure E-8 illustrates, this can be accomplished by entering =1-PRODUCT(I3:I16) in the lone occupied cell in Column J. This cell's value [1.62×10^{-2}] is the probability that some category I hazard produces a mishap.

This is repeated for severity categories II, III, and IV, producing combined mishap probabilities of 3.47×10^{-2}, 1.96×10^{-1}, and 0.00×10^{0}, respectively.

In comparing the four probabilities, it is determined that category III is the severity whose occurrence is most probable. Category III is represented quantitatively by its midpoint value, $63,200.00, which is now assigned as the severity value (SMPL) for this total risk measure.

Finally, the effective occurrence probability considering all hazards is determined by dividing the total risk by the category III severity value:

$$P_{MPL} = \frac{\text{Total Risk}}{S_{MPL}} = \frac{\$192,197.\text{B}}{\$63,200.00} = 3.04 \qquad \text{(Eq E-6)}$$

Note that the 3.04 value does not properly represent a probability. Though labeled as probability, this risk measure component should be viewed as representing the expected number of mishaps occurring during the 30-year activity duration.

The total risk then, as represented by the Most Probable Loss Measure, is defined by P-S components:

S_{MPL} = $63,200.00
P_{MPL} = 3.04

RESULTS SUMMARY—TOTAL RISK ASSESSMENT FOR EXAMPLE ACTIVITY

This section summarizes the results generated in Steps 1 through 6 (Sections 5.1 through 5.6) for the example activity risk prior to implementing hazard controls and provides corresponding results for post-mitigation risk. The information provided in Table E-3 is used both for determining risk acceptability and for communicating activity risk to others (management, customer, public, etc.).

Table E-3. Quantitative Results Summary – Total Risk

Example Activity Total Risk Assessment	Initial Risk Estimate		Mitigated Risk Estimate	
	P	S	P	S
Total Risk		$ 192,197		$ 1,320
Risk Measures				
Expected Loss Rate	1.00E+00	$ 192,197	1.00E+00	$ 1,320
Maximum Loss	1.92E-02	$ 10,000,000	1.32E-04	$ 10,000,000
Most Probable Loss	3.04E+00	$ 63,200	2.09E-02	$ 63,200
Conditional Loss Rate	2.36E-01	$ 814,169	1.93E-02	$ 68,276
Risk Profile Data				
Severity Category I	1.62E-02	$ 10,000,000	3.84E-06	$ 10,000,000
Severity Category II	3.47E-02	$ 447,000	1.30E-04	$ 447,000
Severity Category III	1.96E-01	$ 63,200	1.92E-02	$ 63,200
Severity Category IV	0.00E+00	$ 6,320	0.00E+00	$ 6,320

The plot in Figure E-9 provides the initial total risk results for the example activity. Each result is displayed both before and following mitigation actions. Results shown are probability-severity coordinates for each identified hazard and the isorisk lines with the risk measures. The total risk measures shown are Expected Loss Rate (ELR), Maximum Loss Encountered (MLE), Most Probable Loss (MPL), and the Conditional Loss Rate (CLR).

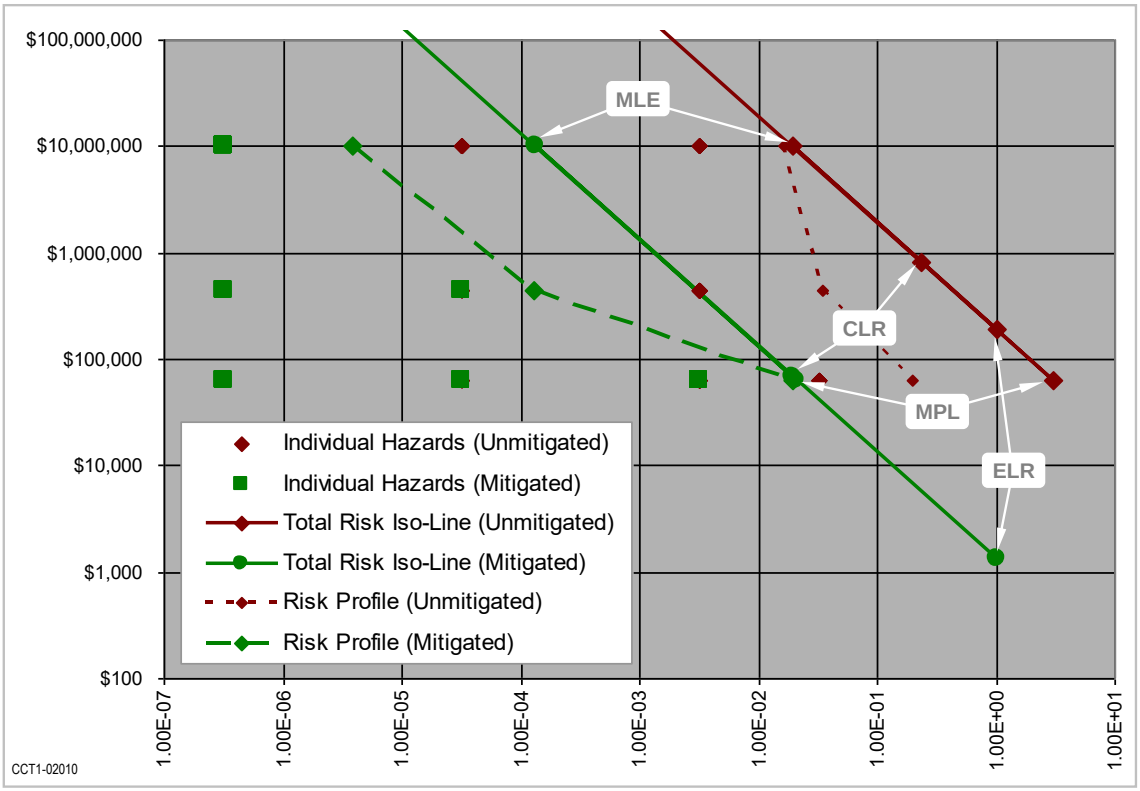


Figure E-12. Total Risk Results – Initial and Final

This completes the total risk assessment process. In this process, a scale for assessing hazards has been developed, hazards have been identified/assessed/mitigated, and hazard data have been entered into a risk matrix to compute partial risks/total risk measures.

The next three sections discuss a hypothetical management approach describing activities that would occur in parallel to this analytical process as shown in Figure 7, Steps A through C.

STEP A: DEVELOP TOTAL RISK CRITERIA

This section describes fictional deliberations used to set criteria for determining that the risks posed by the commercial example activity have been adequately mitigated prior to approving planned operations.

Two primary objectives have led Acme Activity Company management to assess the upgraded processes and equipment planned: protect workers and increase profits by limiting losses due to mishaps.

Quarterly profits obtained using the existing reaction system have not met expectations. Management is also sensitive to the damage that any mishap might cause to the company's reputation and acceptance by a nearby community.

The new system's initial design objective was product throughput. Corporate cost analysts have estimated equipment and retooling costs. Business strategists have set product price points for the planned activity duration. Profit estimates based on these analyses provide confidence that business goals will be met if losses held in check. Management has determined that profit goals will be met if losses due to mishaps remain below $150,000 during the 30-year operating life. To

provide additional confidence, management has stipulated that a 2.0 uncertainty factor be applied to estimated losses, requiring that the total loss risk be less than $75,000. Management also requires that any costs associated with design changes needed to mitigate loss be included in the financial decision.

STEP B: COMPARE RESULTS TO CRITERIA

As shown in Table E-3, the original engineering design was assessed to have a total loss risk exceeding $192,000. If this expected loss level were realized, the example activity would fail to meet its goals.

Based on this result, an aggressive risk mitigation study was performed that identified numerous controls that were economically feasible. The value of each was considered based on the total risk reduction obtained and the cost to implement. The design changes illustrated Figure E-4 were selected and implemented at a total cost of approximately $25,000. System hazards were then reassessed with these controls present.

The total risk post-mitigation was found to be $1,320 as shown in Table E-3. Per management requirements, this figure is doubled and then added to the design changes for a $27,640 total cost impact due to design changes and estimated lifetime losses.

STEP C: DOCUMENT RISK MANAGEMENT DECISIONS

A joint meeting was held so that the cost analysts, the business strategists, and the system safety practitioners could present their collective findings to management. Upon clearly understanding the total risk results and the costs involved in mitigating hazards inherent in the original design, corporate management approved the engineering request to implement the new process.

The decision memorandum issued by headquarters provided clear guidance for proceeding with equipment purchases and manufacturing changes needed to implement the decision. It also included, as attachments, the presentations upon which the decision was based.

HAZARD No.	Chem/Int-001	HAZARD TITLE:	Flange Seal A-29 Leakage	REVISED:	8/11/04

HAZARD DESCRIPTION

Flange Seal A-29 leakage, releasing pressurized catalyst from containment system, producing toxic vapors on contact with air and attacking nearby equipment.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	D	2
Equipment:	X	II	C	2
Downtime:	X	III	C	3
Environment:	X	III	C	3
Product:	O			0

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	E	3
Equipment:	X	II	D	3
Downtime:	X	III	D	3
Environment:	X	III	D	3
Product:	O			0

ADDITIONAL COUNTERMEASURES*

1) Surround flange with sealed annular stainless steel catchment housing, with gravity runoff conduit led to Detecto-Box™ containing detector/alarm feature and chemical neutralizer (S/W).
2) Inspect flange at two-month intervals and re-gasket during annual plant maintenance shut-down (P).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 06

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No.	Chem/Int-002	HAZARD TITLE:	Backflow Contamination	REVISED:	8/11/04

HAZARD DESCRIPTION

Internal failure of Backflow Preventer BFP.043, resulting in contamination of catalyst, sacrifice of product (one to three batches) and production interruption.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	O		0
Equipment:	X	III B	2
Downtime:	X	III B	2
Environment:	O		0
Product:	X	III B	2

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	O		0
Equipment:	X	III C	3
Downtime:	X	III C	3
Environment:	O		0
Product:	X	III C	3

ADDITIONAL COUNTERMEASURES*

1) Provide redundant backflow preventer having differing operating principle than prime unit (E).
2) Equip backflow preventers with detectors/annunciator-alarms to warn of failure of either unit -- situate alarms at both local and control room locations (W).
3) Include alarm response protocol in operating procedures, in emergency procedures manuals, and in operator training (P).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 06

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No.	Chem/Int-003	HAZARD TITLE:	Cooler Leak	REVISED:	8/11/04

HAZARD DESCRIPTION

Corrosion-induced leakage of catalyst into reaction-pacing cooler (C.009), contaminating coolant and damaging equipment in coolant circuit.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel: O			0
Equipment: X	II	C	2
Downtime: X	II	C	2
Environment: O			0
Product: X	III	C	3

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel: O			0
Equipment: X	II	D	3
Downtime: X	II	D	3
Environment: O			0
Product: X	III	D	3

ADDITIONAL COUNTERMEASURES*

1) Provide continuous-reading ph monitor in coolant circuit, immediately upstream of cooler, and equip with alarm set for trigger at ph readings greater than 7.3 (W).
2) Include alarm response protocol in operating procedures, in emergency procedures manuals, and in operator training (P).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 06

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No.	Chem/Int-004	HAZARD TITLE:	Catalyst Overcharge	REVISED:	8/11/04

HAZARD DESCRIPTION

Overcharge of catalyst, resulting in runaway reaction and explosive loss of reactor vessel and surrounding equipment, and injury/death of operating personnel.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel: X	I	D	2
Equipment: X	II	C	2
Downtime: X	III	C	3
Environment: X	II	C	2
Product: O			0

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel: X	I	E	3
Equipment: X	II	D	3
Downtime: X	III	D	3
Environment: X	III	D	3
Product: O			0

ADDITIONAL COUNTERMEASURES*

1) Provide pressure and temperature sensors, actuating a fast-acting, bottom discharge valve to drop batch into a dump tank with diluent, poison, or short-stopping agent (E).
2) Coupled with (1), above, provide automatic addition of diluent, poison, or short-stopping agent directly to reactor (E).
3) Provide temperature sensors with overtemperature alarm and E-Stop feature to trigger batch dump with diluent addition (W/P).
4) Include alarm response protocol in operating procedures, in emergency procedures manuals, and in operator training (P).
5) Reduce volume of catalyst Day Tank (D).
6) Reduce volume of reactor vessel (and batch volume) to 14 liters (half volume) (D).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 06

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No.	Chem/Int-005	HAZARD TITLE:	Catalyst Agitation Failure	REVISED:	8/11/04

HAZARD DESCRIPTION

Inadequate catalyst agitation in reactor vessel, resulting in hot spots and runaway reaction, producing overpressure and potential for vessel burst, with resulting equipment damage and personnel injury/death. (Multiple potential causes, e.g.: slowed feed, power outage.)

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	D	2
Equipment:	X	I	D	2
Downtime:	X	I	D	2
Environment:	X	II	D	3
Product:	X	III	D	3

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	E	3
Equipment:	X	II	E	3
Downtime:	X	I	E	3
Environment:	X	II	E	3
Product:		III	E	3

ADDITIONAL COUNTERMEASURES*

1) Provide full-time positive agitation (e.g., inert gas bubbler with loss-of-function alarm) (E).
2) Reduce volume of reactor vessel (and batch volume) to 14 liters (half volume) (D).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 06

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No.	Chem/Int-006	HAZARD TITLE:	Macerator Failure	REVISED:	8/11/04

HAZARD DESCRIPTION

Macerator performance compromise, resulting in catalyst return to semi-gel state, inhibiting proper reactant blending and reactor vessel ~~-~~hot spots," yielding fouled product and potential ignition sources within vessel; explosion may follow.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	D	2
Equipment:	X	I	D	2
Downtime:	X	I	D	2
Environment:	X	II	D	3
Product:	X	III	D	3

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	E	3
Equipment:	X	II	E	3
Downtime:	X	I	E	3
Environment:	X	III	E	3
Product:	X	III	E	3

ADDITIONAL COUNTERMEASURES*

1) Provide three-stage macerator with interstage witness detector screens to annunciate inadequate fluidizing (S/W).
2) Include alarm response protocol in operating procedures, in emergency procedures manuals, and in operator training (P).
3) Reduce volume of reactor vessel (and batch volume) to 14 liters (half volume) (D).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 06

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No.	Chem/Int-007	HAZARD TITLE:	Day Tank Slopover	REVISED:	8/11/04

HAZARD DESCRIPTION

Float switch failure to open on command resulting in slopover from Day Tank and runoff to harm personnel, damage equipment, and harm the environment; resulting loss of process pressure control would foul product.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	C	1
Equipment:	X	III	C	3
Downtime:	X	II	C	2
Environment:	X	II	C	2
Product:	X	III	C	3

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	E	3
Equipment:	X	II	E	3
Downtime:	X	I	E	3
Environment:	X	II	E	3
Product:	X	III	E	3

ADDITIONAL COUNTERMEASURES*

1) Inspect and test float switch prior to each day's operation (P).
2) Provide Day Tank catalyst level site gage and operator pump-stop switch. Require operator to observe catalyst level at frequent intervals, with instructions to open switch if out-of-bounds catalyst level is reached (P).
3) Flush overflow conduit prior to each day's run (P).
4) Include high level sight gage response and overflow conduit flushing protocols in operating procedures, in emergency procedures manuals, and in operator training (P).

***NOTE*: Verify Post-Countermeasure Risk by Fault Tree Analysis.**

1) Risk is high; all countermeasures are (P).

2) Multiple, co-existing faults result in slopover.

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 06

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No.	Reactor-001	HAZARD TITLE:	Reactor Overpressure	REVISED:	8/14/04

HAZARD DESCRIPTION

Reactor vessel overpressure leading to possible explosion, as caused by loss of temperature control, excessive feed rate, agitation failure, other sources.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	D	2
Equipment:	X	I	C	1
Downtime:	X	I	C	1
Environment:	X	II	C	2
Product:	X	II	C	2

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	E	3
Equipment:	X	II	E	3
Downtime:	X	I	E	3
Environment:	X	III	E	3
Product:	X	III	E	3

ADDITIONAL COUNTERMEASURES*

1) Provide temperature and pressure sensors actuating pneumatically operated vessel dump valve for gravity drop of reaction batch into dump tank with pre-loaded diluent poison and short-stop agent in response to out-of-bounds reaction (E).
2) Coupled with (1), above, provide automatic addition of diluent, poison, or short-stopping agent directly to reactor (E).
3) Provide dedicate temperature sensors with overtemperature alarm and E-Stop feature to trigger batch dump with diluent addition (W/P).
4) Include alarm response protocol in operating procedures, in emergency procedures manuals, and in operator training (P).
5) Reduce volume of reactor vessel (and batch volume) to 14 liters (half volume) (D).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. Vat.07/93 Rev. 03

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No.	Reactor-002	HAZARD TITLE:	Catalyst Underfeed	REVISED:	8/11/04

HAZARD DESCRIPTION

Catalyst feed rate insufficient to sustain reaction, leading to compromise of reaction and incorrect species production/loss of product.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	O		0
Equipment:	O		0
Downtime:	X	III B	2
Environment:	O		0
Product:	X	III B	2

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	O		0
Equipment:	O		0
Downtime:	X	III C	3
Environment:	O		0
Product:	X	III C	3

ADDITIONAL COUNTERMEASURES*

1) Provide Programmable Logic Controller reaction monitor with out-of-bounds alert / alarm (W/P).
2) Include alarm response protocol in operating procedures, in emergency procedures manuals, and in operator training (P).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. Vat.07/93 Rev. 03

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

HAZARD No. Reactor-003 **HAZARD TITLE:** Incomplete Reaction **REVISED:** 9/04/04

HAZARD DESCRIPTION

Incomplete reaction owing to curtailed reaction dwell time, low temperature, low pressure (or other causes) producing fouled, off-species product.

EXPOSURE INTERVAL 30 years **ACTIVITY/PROCESS PHASE:** Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	O		0
Equipment:	O		0
Downtime:	O		0
Environment:	O		0
Product:	X	III B	2

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)	SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	O		0
Equipment:	O		0
Downtime:	O		0
Environment:	O		0
Product:	X	III C	3

ADDITIONAL COUNTERMEASURES*

1) Provide continuous, on-line, composition monitoring with out-of-bounds alarm feature (W).
OR
Provide continuous monitoring of reaction health by inferential PLC computation of predominate species from reactor batch pressure and temperature readouts with out-of bounds alarm feature (W), AND include alarm response protocol in operating procedures, in emergency procedures manuals, and in operator training (P).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. CI.Int.07/93 Rev. 02

Prepared by / Date: (Designer/Analyst)	**Reviewed by / Date:** (System Safety Manager)	**Approved by:** (Project Manager)

HAZARD No.	Stack-001	HAZARD TITLE:	Stack Fire/Explosion	REVISED:	9/04/04

HAZARD DESCRIPTION

Electrostatic ignition of condensation deposits on exhaust ductwork inner walls, resulting in fire/explosion.

EXPOSURE INTERVAL	30 years	ACTIVITY/PROCESS PHASE:	Startup/Standard Operation/Stop/Emergency Shutdown

INITIAL RISK ASSESSMENT

(with existing and planned/designed-in countermeasures)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	C	1
Equipment:	X	I	C	1
Downtime:	X	II	C	2
Environment:	X	II	C	2
Product:	X	III	C	3

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD ASSET(S): (check all applicable)		SEVERITY: (Severity & Probability for worst-case Risk)	PROBABILITY: (Severity & Probability for worst-case Risk)	RISK CODE: (from Matrix)
Personnel:	X	I	E	3
Equipment:	X	I	E	3
Downtime:	X	II	E	3
Environment:	X	III	E	3
Product:	X	III	E	3

ADDITIONAL COUNTERMEASURES*

1) Ground and bond exhaust stack and all electrically conducting exhaust gas contact surfaces to suppress electrostatic ignition sources (S).
2) Provide exhaust stack flood/sweep blower system with continuous monitoring of gas stream and automatic blower ~~-ON~~" at 20% LEL (E).
3) Provide misting spray at upstream duct location to maintain elevated humidity in complete exhaust circuit (S).
4) Reduce volume of reactor vessel (and batch volume) to 14 liters (half volume) (D).

***Mandatory for Risk Codes 1 & 2, unless permitted by Waiver.**
Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) =Procedures/ Training

COMMENTS

Dwg. Stack 07/93 Rev. 01

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by: (Project Manager)

A	B	C	D	E	F	G	H
Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$	Notes
CI-001	Flange Seal A-29 Leakage - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320	
CI-001	Flange Seal A-29 Leakage - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430	
CI-001	Flange Seal A-29 Leakage - Downtime	III	C	$ 63,200	3.20E-03	$ 202	
CI-001	Flange Seal A-29 Leakage - Environment	III	C	$ 63,200	3.20E-03	$ 202	
CI-002	Backflow Contamination - Equipment	III	B	$ 63,200	3.20E-02	$ 2,022	
CI-002	Backflow Contamination - Downtime	III	B	$ 63,200	3.20E-02	$ 2,022	
CI-002	Backflow Contamination - Product	III	B	$ 6,320	3.20E-02	$ 202	
CI-003	Cooler Leak - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430	
CI-003	Cooler Leak - Downtime	II	C	$ 447,000	3.20E-03	$ 1,430	
CI-003	Cooler Leak - Product	III	C	$ 6,320	3.20E-03	$ 20	
CI-004	Catalast Overcharge - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320	
CI-004	Catalast Overcharge - Equipment	II	C	$ 447,000	3.20E-03	$ 1,430	
CI-004	Catalast Overcharge - Downtime	III	C	$ 6,320	3.20E-03	$ 20	
CI-004	Catalast Overcharge - Environment	II	C	$ 447,000	3.20E-03	$ 1,430	
CI-005	Catalyst Agitation Failure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320	
CI-005	Catalyst Agitation Failure - Equipment	I	D	$ 10,000,000	3.20E-05	$ 320	
CI-005	Catalyst Agitation Failure - Downtime	I	D	$ 10,000,000	3.20E-05	$ 320	
CI-005	Catalyst Agitation Failure - Environment	II	D	$ 447,000	3.20E-05	$ 14	
CI-005	Catalyst Agitation Failure - Product	III	D	$ 6,320	3.20E-05	$ 0	
CI-006	Macerator Failure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320	
CI-006	Macerator Failure - Equipment	I	D	$ 10,000,000	3.20E-05	$ 320	
CI-006	Macerator Failure - Downtime	I	D	$ 10,000,000	3.20E-05	$ 320	
CI-006	Macerator Failure - Environment	II	D	$ 447,000	3.20E-05	$ 14	
CI-006	Macerator Failure - Product	III	D	$ 6,320	3.20E-05	$ 0	
CI-007	Day Tank Slopover - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000	
CI-007	Day Tank Slopover - Equipment	III	C	$ 6,320	3.20E-03	$ 20	
CI-007	Day Tank Slopover - Downtime	II	C	$ 447,000	3.20E-03	$ 1,430	
CI-007	Day Tank Slopover - Environment	II	C	$ 447,000	3.20E-03	$ 1,430	
CI-007	Day Tank Slopover - Product	III	C	$ 6,320	3.20E-03	$ 20	

A	B	C	D	E	F	G	H
Haz ID	**Short Title**	**Sev. Cat**	**Prob. Cat**	**Sev. Value**	**Prob. Value**	**Partial Risk, $$**	**Notes**
R-001	Reactor Overpressure - Personnel	I	D	$ 10,000,000	3.20E-05	$ 320	
R-001	Reactor Overpressure - Equipment	I	C	$ 10,000,000	3.20E-03	$ 32,000	
R-001	Reactor Overpressure - Downtime	I	C	$ 10,000,000	3.20E-03	$ 32,000	
R-001	Reactor Overpressure - Environment	II	C	$ 447,000	3.20E-03	$ 1,430	
R-001	Reactor Overpressure - Product	II	C	$ 447,000	3.20E-03	$ 1,430	
R-002	Catalyst Underfeed - Downtime	III	B	$ 63,200	3.20E-02	$ 2,022	
R-002	Catalyst Underfeed - Product	III	B	$ 63,200	3.20E-02	$ 2,022	
R-003	Incomplete Reaction - Product	III	B	$ 6,320	3.20E-02	$ 202	
S-001	Stack Fire/Explosion - Personnel	I	C	$ 10,000,000	3.20E-03	$ 32,000	
S-001	Stack Fire/Explosion - Equipment	I	C	$ 10,000,000	3.20E-03	$ 32,000	
S-001	Stack Fire/Explosion - Downtime	II	C	$ 447,000	3.20E-03	$ 1,430	
S-001	Stack Fire/Explosion - Environment	II	C	$ 447,000	3.20E-03	$ 1,430	
S-001	Stack Fire/Explosion - Product	III	C	$ 6,320	3.20E-03	$ 20	
			Expected Loss Rate	$ 187,643	1.00E+00	$ 187,643	**Total Risk**
			Maximum Loss	$ 10,000,000	1.88E-02		
			Most Probable Loss	$ 63,200	2.97E+00		
			Conditional Loss Rate	$ 794,877	2.36E-01		
				1000000000	1.88E-04		

Notes:

1	Probability value determined by Probabilistic Risk Analysis (Report # TR-09-01103)
2	
3	

A	B	C	D	E	F	G	H
Haz ID	Short Title	Sev. Cat	Prob. Cat	Sev. Value	Prob. Value	Partial Risk, $$	Notes
CI-001	Flange Seal A-29 Leakage - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.200	
CI-001	Flange Seal A-29 Leakage - Equipment	II	D	$ 447,000	3.20E-05	$ 14.304	
CI-001	Flange Seal A-29 Leakage - Downtime	III	D	$ 63,200	3.20E-05	$ 2.022	
CI-001	Flange Seal A-29 Leakage - Environment	III	D	$ 63,200	3.20E-05	$ 2.022	
CI-002	Backflow Contamination - Equipment	III	C	$ 63,200	3.20E-03	$ 202.240	
CI-002	Backflow Contamination - Downtime	III	C	$ 63,200	3.20E-03	$ 202.240	
CI-002	Backflow Contamination - Product	III	C	$ 63,200	3.20E-03	$ 202.240	
CI-003	Cooler Leak - Equipment	II	D	$ 447,000	3.20E-05	$ 14.304	
CI-003	Cooler Leak - Downtime	II	D	$ 447,000	3.20E-05	$ 14.304	
CI-003	Cooler Leak - Product	III	D	$ 63,200	3.20E-05	$ 2.022	
CI-004	Catalast Overcharge - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.200	
CI-004	Catalast Overcharge - Equipment	II	D	$ 447,000	3.20E-05	$ 14.304	
CI-004	Catalast Overcharge - Downtime	III	D	$ 63,200	3.20E-05	$ 2.022	
CI-004	Catalast Overcharge - Environment	III	D	$ 63,200	3.20E-05	$ 2.022	
CI-005	Catalyst Agitation Failure - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.200	
CI-005	Catalyst Agitation Failure - Equipment	II	E	$ 447,000	3.20E-07	$ 0.143	
CI-005	Catalyst Agitation Failure - Downtime	I	E	$ 10,000,000	3.20E-07	$ 3.200	
CI-005	Catalyst Agitation Failure - Environment	II	E	$ 447,000	3.20E-07	$ 0.143	
CI-005	Catalyst Agitation Failure - Product	III	E	$ 63,200	3.20E-07	$ 0.020	
CI-006	Macerator Failure - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.200	
CI-006	Macerator Failure - Equipment	II	E	$ 447,000	3.20E-07	$ 0.143	
CI-006	Macerator Failure - Downtime	I	E	$ 10,000,000	3.20E-07	$ 3.200	
CI-006	Macerator Failure - Environment	III	E	$ 63,200	3.20E-07	$ 0.020	
CI-006	Macerator Failure - Product	III	E	$ 63,200	3.20E-07	$ 0.020	
CI-007	Day Tank Slopover - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.200	
CI-007	Day Tank Slopover - Equipment	II	E	$ 447,000	3.20E-07	$ 0.143	
CI-007	Day Tank Slopover - Downtime	I	E	$ 10,000,000	3.20E-07	$ 3.200	
CI-007	Day Tank Slopover - Environment	II	E	$ 447,000	3.20E-07	$ 0.143	
CI-007	Day Tank Slopover - Product	III	E	$ 63,200	3.20E-07	$ 0.020	

A	B	C	D	E	F	G	H
Haz ID	**Short Title**	**Sev. Cat**	**Prob. Cat**	**Sev. Value**	**Prob. Value**	**Partial Risk, $$**	**Notes**
R-001	Reactor Overpressure - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.200	
R-001	Reactor Overpressure - Equipment	II	E	$ 447,000	3.20E-07	$ 0.143	
R-001	Reactor Overpressure - Downtime	I	E	$ 10,000,000	3.20E-07	$ 3.200	
R-001	Reactor Overpressure - Environment	III	E	$ 63,200	3.20E-07	$ 0.020	
R-001	Reactor Overpressure - Product	III	E	$ 63,200	3.20E-07	$ 0.020	
R-002	Catalyst Underfee - Downtime	III	C	$ 63,200	3.20E-03	$ 202.240	
R-002	Catalyst Underfee - Product	III	C	$ 63,200	3.20E-03	$ 202.240	
R-003	Incomplete Reaction - Product	III	C	$ 63,200	3.20E-03	$ 202.240	
S-001	Stack Fire/Explosion - Personnel	I	E	$ 10,000,000	3.20E-07	$ 3.200	
S-001	Stack Fire/Explosion - Equipment	I	E	$ 10,000,000	3.20E-07	$ 3.200	
S-001	Stack Fire/Explosion - Downtime	II	E	$ 447,000	3.20E-07	$ 0.143	
S-001	Stack Fire/Explosion - Environment	III	E	$ 63,200	3.20E-07	$ 0.020	
S-001	Stack Fire/Explosion - Product	III	E	$ 63,200	3.20E-07	$ 0.020	
			Expected Loss Rate	$ 1,320	1.00E+00	$ 1,320	**Total Risk**
			Maximum Loss	$ 10,000,000	1.32E-04		
			Most Probable Loss	$ 63,200	2.09E-02		
			Conditional Loss Rate	$ 68,276	1.93E-02		