10/12-21-89 JS①

SANDIA REPORT

SAND89—1982 • UC—607
Unlimited Release
Printed November 1989

Risk Assessment and Its Application to Flight Safety Analysis

David L. Keese, William R. Barton

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A02
Microfiche copy: A01

SAND--89-1982

DE90 004985

Distribution
Category UC-607

Risk Assessment and Its Application to Flight Safety Analysis

David L. Keese and William R. Barton
Aerospace Projects Division
Sandia National Laboratories
Albuquerque, New Mexico 87185

Abstract

The 1×10^{-6} figure has long been used as the maximum allowable non-participant casualty probability for hazardous test activities at Sandia National Laboratories. This level and those defined for participant casualty and property damage are supported by a wide variety of historical data, societal behavior, and risk assessment methodology. This report reviews these safety guidelines and provides insight into their origins and applications. These guidelines are also specifically discussed in relation to current rocket flight safety decisions at Sandia.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Contents

1 Introduction 5
2 Historical Background 6
3 Risk Assessment Methodologies 6
4 Ambient Risk Statistics 8
5 Unique vs Recurring Risk Exposure 9
6 Summary 10
7 References 12
8 Additional References 13
9 Appendix 14
10 Appendix References 16

1 Introduction

Potentially hazardous test activities have historically been a part of Sandia National Labs mission to design, develop, and test new weapons systems. These test activities include high speed air drops for parachute development, sled tests for component and system level studies, multiple stage rocket experiments, and artillery firings of various projectiles. Due to the nature of Sandia's test programs, the risk associated with these activities can never be totally eliminated. However, a consistent set of policies should be available to provide guidance into the level of risk that is acceptable in these areas.

This report presents a general set of guidelines for addressing safety issues related to rocket flight operations at Sandia National Laboratories. Even though the majority of this report deals primarily with rocket flight safety, these same principles could be applied to other hazardous test activities. The basic concepts of risk analysis have a wide range of applications into many of Sandia's current operations.

The expressed goal of all personnel involved in any type of hazardous test activity should be to prevent any situation that might endanger human life or cause unintentional property damage. In order to achieve this goal, it is proposed that the risks involved in any test should not exceed the following indicated levels.

10^{-6}	Non-participant fatality
10^{-5}	Participant fatality
10^{-3}	Probability of seriously damaging a government installation

These probability figures of acceptable risk levels are intended to be used only as guidelines. The determination of these guidelines, as well as the risk calculation for an individual test, includes some inaccuracies and can never be totally divorced from human judgement. If initial estimates of test risk exceed these guidelines, a more thorough study of the safety issues should be pursued including a detailed design review of the proposed test procedure and hardware. This additional analysis would be necessary since a high level authorization would be required to perform a test whose risks exceed these guidelines.

The following sections of this report present some historical background information related to these safety guidelines and statistical data that form the foundation of these principles. References are also made to the use of such guidelines at other DoD and DOE test ranges. A general discussion of risk assessment methodologies is also included along with a list of ambient risks faced by the general public. Finally, the report appendix includes a discussion of currently accepted methods for determining the casualty probability for several test environments.

2 Historical Background

The question "how safe is safe enough" has been widely debated for many years (Reference 1) and in recent years has been applied most strongly in connection with nuclear power plant construction (Reference 2). The very nature of this question implies that differences of opinion exist over the general issue of safety. For this reason, some consistent means for describing an acceptable level of risk introduced by some new activity is necessary.

The available literature indicates that the U.S. Air Force was one of the first organizations to utilize the common 10^{-6} criterion for accidents involving fatalities. However, the basis for the adoption of this particular level is uncertain and has been conjectured to simply be an emotional acceptance of a "one in a million" chance of a fatality (Reference 3). Regardless of its origin, this safety level (or one similar to it) was subsequently adopted by the Navy (Reference 4) and Army (Reference 5) for use in hazardous operations. This level of acceptable risk has also been adopted almost uniformly along with a 10^{-5} for test participants at NASA and most DoD and DOE test facilities. Test ranges currently using this standard include the Eastern Space and Missile Center, Atlantic Fleet Weapons Test Range, Pacific Missile Test Center, Kwajalein Missile Range, White Sands Missile Range, and the Tonopah Test Range (Reference 6). The following sections will discuss this accepted flight safety standard in relation with modern risk assessment methodologies.

3 Risk Assessment Methodologies

Most current risk assessment methodologies follow a similar pattern in safety analysis. This pattern is summarized below (Reference 7).

- Establish an acceptable risk reference level
- Determine the level of risk involved in the new proposed activity
- Compare the risk associated with the new activity with the reference level
- Proceed with the activity or modify the activity to adjust the risk as dictated by the previous comparison

This procedure provides a good stepwise approach to the decisions that must be made in any range safety process. The most difficult stage in this process, and the one in which most controversies arise, is the establishment of an acceptable risk reference level. Several methods that provide this initial risk reference level are listed below.

1. Cost-benefit comparisons: incremental costs to decrease risk compared with the increased safety benefit
2. Internally derived risk references: risk references derived from individual experience
3. Ambient risk level determinations: risk level associated with naturally occurring hazards
4. Society behavior principles: accepted risk level inferred from society's behavior patterns

Cost-benefit analysis is used primarily in industrial situations and is not entirely applicable to range safety operations. Internally derived risk references also suffer from a potential lack of objectivity and are not widely used. The approach which appears to have the most support in the current literature, and which applies most directly to flight safety operations, is a combination of methods 3 and 4. This approach, known as the "probability threshold" method, investigates the ambient level of natural or man-made risk that society will accept based on demonstrated behavior (Reference 8). This type of approach has been widely used and promoted by the Nuclear Regulatory Commision, the Environmental Protection Agency, the National Academy of Sciences, and other government and industrial groups.

The "probability threshold" method begins with the assumption that a small, finite amount of risk is acceptable. This initial premise is important because there are groups that advocate a "zero risk" level for any new man-made activities. This assertion is countered by the fact that nature itself does not provide a "zero risk" environment. Proponents of the "probability threshold" method contend that some threshold level of risk exists and that any risk below this level will produce only negligible effects on the ambient risk to society. This minimal threshold of risk is related to society's reaction to natural or ambient levels of risk prevalent in the environment. Based on this approach, the U.S. Nuclear Regulatory Commission announced in its January 1983 policy guidelines that "... an accident fatality risk to the public of 10^{-6} or lower is considered negligible" (Reference 9).

This level of an accidental public fatality demonstrates a strong industrial and governmental support base and should be considered a sound basis for risk levels incurred in hazardous test activities such as those performed at Sandia National Labs. Additional studies have also expanded the probability threshold position to account for benefits derived from these hazardous activities. These studies show that facilities or activities viewed by society as "essential," "beneficial," or "peripheral" warrant a decreasing level of risk-acceptance. These corresponding threshold levels were found to be 2×10^{-4}, 1×10^{-5}, 2×10^{-6} risk of death per year respectively (Reference 9) at a 90% confidence level. Non-participants in a test activity would most likely subscribe to the view that these tests would provide only "peripheral" benefits and thus accept the 2×10^{-6} risk threshold. This compares favorably (i.e., conservatively) with the 1×10^{-6} level mentioned as the currently accepted threshold. Additionally, participants in SNL tests would generally attribute "essential" or "beneficial" characteristics to these activities and would accept a risk threshold of 1×10^{-5} to 2×10^{-4} per year risk of death. This again compares well with the proposed guideline for participant fatalities of 1×10^{-5} .

As stated earlier in this section the "probability threshold" method is based upon the ambient level of risk that society regards as negligible. The following section provides a general data base from current accident statistics to serve as a foundation for this principle. A general review of society's reaction to various levels of risk is also included for reference.

4 Ambient Risk Statistics

Most statistical risk assessment analyses indicate that the lowest level for involuntary risks is set by the risk of death from natural events such as flood, lightning, earthquakes, poisonous bites, etc. (Reference 10). This has been traditionally accepted as about one death per million people per year. To improve the statistical significance of this number, the accident rates should be derived for the population actually exposed to the indicated risk. For this reason the most current available fatality rates are shown below for these types of hazards in the continental United States (Reference 11).

Table 1. Annual Probability of Death

Cause of Death	1981	1982	1983	1984	1985
Poisonous bites or reaction	2.35×10^{-7}	3.28×10^{-7}	2.73×10^{-7}	2.62×10^{-7}	2.30×10^{-7}
Lightning	3.79×10^{-7}	4.32×10^{-7}	3.97×10^{-7}	3.85×10^{-7}	3.56×10^{-7}
Tornados, floods, and earthquakes	4.71×10^{-7}	7.34×10^{-7}	5.21×10^{-7}	8.33×10^{-7}	9.25×10^{-7}
Total risk	1.09×10^{-6}	1.49×10^{-6}	1.19×10^{-6}	1.48×10^{-6}	1.51×10^{-6}

These statistics show that the average total probability of death from these ambient hazards is approximately 1.35×10^{-6} for the years 1981-1985. This is nearly identical to the accepted risk threshold of 1×10^{-6} used in flight safety analyses.

Society's general reaction to various perceived levels of risk is summarized in the following table from Reference 12.

Annual Fatality Risk Level	Society's Reaction
10^{-3}	This level is unacceptable to everyone. Accidents providing hazard at this level are hard to find. When risks approach this level, immediate action is taken to reduce the hazard.
10^{-4}	People are willing to spend public money to control a hazard (traffic sign, fire department). Safety slogans popularized for accidents in this category show an element of fear ("the life you save may be your own").
10^{-5}	People still recognize these hazards. People warn children about these hazards (drowning, firearms, poisonings). People accept inconvenience to avoid (air travel). Safety slogans have a precautionary ring ("never swim alone," "never point a gun," "never leave medicine within a child's reach").
10^{-6}	Not of great concern to the average person. People are aware of these accidents but feel it can never happen to me. Phrases associated with these accidents have an element of resignation ("lightning never strikes twice," "an act of God").

5 Unique vs Recurring Risk Exposure

Most of the literature references sited in this study (especially those dealing with nuclear power applications) and the national accident statistics are based on an annual risk exposure level. However, many hazardous test activities are more representative of single, independent risk exposures as opposed to risk generated by a recurring event. This section of the report addresses the differences between these types of risks, and how separate, independent hazardous operations can be viewed from an annual risk perspective.

Range safety analyses for sounding rocket applications assume that each of these tests represent single, independent events. Fatality and property damage probabilities are based on the unique mission and hardware characteristics for a "one-time" launch environment. Exposure to the calculated risk associated with this type of unique test event would have to be divided by 365 days/year to reflect the additional annual risk created by this test. Viewed another way, were this test to be conducted every day for one year, the annual risk would be identical to the calculated "one-time" risk level. The total annual risk produced by a large number of unique tests conducted throughout the year could be derived by the following expression.

$$\sum_{i=1}^{n} \frac{Test\ Risk_i}{365\ days/year} = Annual\ Risk\ Level$$

It should be apparent that the annual risk derived from this relationship will never exceed the maximum risk associated with any one single test event.

Continual hazardous operations that involve some recurring risk exposure due to a repetitive action or test activity should be approached in a fashion more similar to that used to analyze industrial safety issues (i.e., nuclear reactors). In this type of operation, the reliability of the entire system is estimated and used to predict failure probabilities that could lead to serious injury or death. These situations usually assign probabilities to certain key events over a given time period (i.e., one year) that might produce risk to operating personnel. A good flight system example of this type of risk would be the estimated reliability of the O-ring seals used in the Space Shuttle solid rocket boosters (SRBs). A 1983 Air Force risk assessment study indicated the probability of a shuttle failure due to booster rocket "burn-through" was approximately one in thirty-five missions (Reference 13). If the reliability of the SRBs is assumed to remain the same for each mission, and if their performance in each mission is independent of all other missions, the probability of a shuttle catastrophy due to the SRBs can be treated as a binomial random variable. Under these assumptions the probability of at least one catastrophic failure in twenty-five missions is 0.516 (or roughly 50-50). The Challenger shuttle flight was the twenty-fifth shuttle mission. This type of reliability approach could be applied to operations that include continual risk exposure due to repetitive events.

6 Summary

The proposed guidelines for participant and non-participant fatality probabilities governing tests at Sandia National Labs are shown to be consistent with similar factors used at the vast majority of other DoD and DOE test ranges. Use of these guidelines is also supported by current risk assessment methodologies and recent ambient risk statistics. As stated earlier, these probability figures should be used only as guidelines by the individual responsible for flight safety decisions.

The guideline specifically related to potential property damage has not been extensively addressed in this study for two reasons. First, the majority of information dealing with risk assessment and ambient risk was only directly related to human casualty, not property damage. Secondly, the type of facility (size, importance, cost, etc.) was thought to have a major effect on the acceptable risk level for the individual facility. This type of judgement would be made most intelligently by the specific range involved for each individual test. However, a single reference was found (Reference 14) specifying "...an impact probability causing property damage not to exceed 1×10^{-3} ..." for the NASA Wallops Flight Center. For these reasons the proposed guideline of 1×10^{-3} should serve as a reasonable level for this area of flight safety analysis.

The material presented in this report will hopefully clarify many of the issues surrounding flight safety requirements at SNL. Adherence to these principles in the past has produced a long and enviable record of safe operations at Sandia. Every effort should be made in the future to continue this safe testing environment.

7 References

1. Fischoff, B.; Slovic, P.; Lichtenstein, S.; Read, S.; Combs, B.; "How Safe is Safe Enough, A Psychometric Study of Attitudes Toward Risks and Benefits," Policy Science, 1978.

2. Nuclear Regulatory Commission, "Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG 75/014), October 1975.

3. Philipson, L., "Risk Assessment Methodologies and Their Uncertainties: A Review of Risk Evaluation Approaches," Volume 2, J.H. Wiggins Company, March 1982.

4. U.S. Navy, Ordnance Systems Command, "Weapons System Safety Guidelines Handbook," Part 1, NAVORD OD 44842, 1 May 1973.

5. U.S. Army, Office of the Project Manager for Munitions Production Base Modernization and Expansion, Dover, New Jersey, "PBM Operating System Manual No. 385-1, Change 1, System Safety Program for Modernization and Expansion Projects," 1 August 1979.

6. Barton, W.R, personal telecon with national ranges (White Sands Missile Range, Pacific Missile Test Center, NASA Wallops Island, NASA Washington: Shuttle Operations, Eglin Air Force Base), 1988.

7. Rowe, W.D., "An Anatomy of Risk," John Wiley and Sons, 1977.

8. Shrader-Frechette, K.S., "Risk Analysis and Scientific Method," D. Reidel Publishing Company, 1985.

9. Okrent, D., and Whipple, C. ,"An Approach to Societal Risk Acceptance Criteria and Risk Management," University of California at Los Angeles Report UCLA-ENG-7746, June 1977.

10. McCormick, N.J., "Reliability and Risk Analysis," Department of Nuclear Engr, University of Washington, Academic Press, 1981.

11. National Safety Council, "Accident Facts," 1988 Addition.

12. Otway, H.J. and Erdmann, R.C., "Reactor Safety and Design from a Risk Viewpoint," Nuclear Engineering Design, 1970.

13. McKean, Biddle, Robinson, Minneapolis Star and Tribune, February 11, 1986.

14. Range Safety Group, Range Commanders Council, "Unguided Rocket Safety: An Informal Compendium of Range Techniques for Assuring Safety in Rocket Testing," March 1982.

8 Additional References

1. Range Safety Group, Range Commanders Council, "Risk Analysis Techniques," March 1979.

9 Appendix

Several methods of calculating missile impact probabilities and casualty expectations are available. Acceptable methods currently in use at Tonopah Test Range are described in this appendix and in more detail in Appendix Reference 1. Other methods may be considered satisfactory if they can be shown to be more conservative or if data are available to support less conservative assumptions.

Random Impact Distribution

Distribution of impacts may be assumed random in the specified impact area. This method is often used for analysis of development systems where little is known about the true distribution because of limited experience or small sample size available.

"Normal" or Gaussian Impact Distribution

If data are available to substantiate the assumption of a "normal" or Gaussian distribution in two dimensions, the probability may be calculated in the following manner. This method assumes that the impacts may be considered to be normally distributed independently in each of the two coordinates (x and y). In the first special case the same standard deviation is applied to both dimensions. Impact probability for this type of circular distribution about a nominal impact point is shown below.

The probability ($P(dA)$) of striking a "small" area (dA) located at R is:

$$P(dA) = \frac{dA}{2\pi\sigma^2} e^{-R^2/2\sigma^2}$$

In this equation, σ is the standard deviation in both dimensions and R is the radius from the nominal impact point to the area dA. The criterion for "small" is that the value of $e^{-R^2/2\sigma^2}$ does not vary appreciably over the area dA.

When the "small" assumption is not valid, the probability of impacting within an area (A) is given by the following relationship.

$$P(A) = \frac{A}{\pi(b^2 - a^2)}(e^{-a^2/2\sigma^2} - e^{-b^2/2\sigma^2})$$

where...

P(A) = probability of hitting in area A
A = area in question
b = outer radius of boundary of A
a = inner radius of boundary of A
σ = standard deviation in both dimensions

The probability of impacting within a circle of radius R under these assumptions reduces to the following expression.

$$P(R) = 1 - e^{-r^2/2\sigma^2}$$

For a two-dimensional, "normal" distribution where the standard deviation is no longer equal in both directions, the probability of impacting within an area (A) is given by:

$$P(A) = \frac{1}{2\pi\sigma_x\sigma_y}\int\int e^{-0.5}\left(\frac{x^2}{\sigma_{x^2}} + \frac{y^2}{\sigma_{y^2}}\right) dxdy$$

where...

σ_x = standard deviation in x
σ_y = standard deviation in y
P(A) = probability of a hit in area A
x,y = coordinates with origin at nominal impact point

If multiple impact fragments are to be considered, the probability of one or more fragments impacting a site is given by the following relationship:

$$P(A)_N = (1 - P(A))^N$$

where...

N = number of fragments
P(A) = probability of impact in area A for one fragment

The casualty expectation for an area is a function of the casualty area for the impacting object, the population of the area, and the probability of the object impacting in the area. A casualty is assumed to be death or serious injury.

$$E_{c_i} = P(A_i)\frac{A_c N_i}{A_i}$$

where...

E_{c_i} = casualty expectation for A_i
$P(A_i)$ = probability of the object impacting in A_i
A_c = casualty area for object; the area around an impact which is ...... considered hazardous due to fragmentation or explosion at impact
A_i = area in question

N_i = population of area A_i

In the case where the casualty area for an impacting object is assumed to be the same as the area of the site in question, a hit within the area implies a casualty in the area. The following casualty expectation is determined if the population (N_i) is assumed to be uniformly distributed.

$$E_c = P(A_i)N_i$$

10 Appendix References

1. Ewing, R.I., "Normal Probability Applied to Missile Impact," SC-TM-68-864, December 1968.

External Distribution:

J. Charles Sawyer
NASA Headquarters - Code Q55
600 Independence Ave, SW
Washington, D.C. 20546

Ronald Sawyer
Head, Safety and Quality Assurance Branch
Goddard Space Flight Center
Wallops Flight Facility
Wallops Island, Virginia 23337

Weston C. Wolff
Range Commanders Council
STEWS-NR-CF
White Sands Missile Range
New Mexico 88002-5134

Commander, Pacific Missile Test Center
Point Mugu, California 93042 (M-1888)
Attn: Ms. Irene Hofer, Code 3032
Range Safety Office

Steve LaPoint - CSSD-KS
P.O. Box 26
APO San Francisco, California 96555

Internal Distribution:

C.W. Peterson, 1550
J.K. Cole, 1551
D.D. McBride, 1552
W.L. Hermina, 1553
D.P. Aeschliman, 1554
T.M. Jordan, 1555
W.A. Millard, 1555
D.E. Outka, 1555
L.R. Rollstin, 1555
W.L. Oberkampf, 1556
S.A. Landenberger, 3141 (5)
C.L. Ward, 3141-1 (8) for DOE/TIC
W.I. Klein, 3151 (3)
T.S. Church, 7290
C.M. Tapp, 7500
R.D. Bentley, 7510
L.W. Lathrop, 7511
G.L. West, 7513
T.J. Hoban, 7520
T.J. Hoban, acting 7523
R.L. Eno, 7525
P.L. Walter, 7526
T.L. Workman, 7530
F. H. Matthews, 7533
D.C. Bickel, 7535
J.A. Wackerly, 8524
R.G. Clem, 9100
D.J. Rigali, 9140
W.R. Barton, 1555
D.L. Keese, 1555 (10)