

**This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-96SR18500 with the U. S. Department of Energy.**

**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, 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 any third party's use or the results of such use 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 or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.**

# **A Historical Perspective on Significance Relative to Safety Analysis and Actual Events**

**Edward J. Hallinan**

## **Abstract**

Since the early days of safety analysis there has been an overall goal to protect against accidents with significant risk. However, there has been considerable discussion and fluctuation in how to define "significant." This paper presents past and current attempts to define "significant." These include various siting evaluation guidelines, "small fraction" and "well within" for further division of the guidelines. These definitions were expanded to include identification of USQ, proper control functional classification and when a preliminary safety basis is required to authorize construction. Such schemes started with quantitative guidelines which have changed over time to today's climate of qualitative definitions. The differences, advantages and disadvantages are discussed and safety analysis expectations on what is significant are compared to a selection of actual events from the U.S. Department of Energy (DOE), the Nuclear Regulatory Commission (NRC) and the chemical industry. The paper concludes with an assessment of causal factors common to those actual events that are not generally considered in typical accident sequence identification and, thus, are not usually considered "significant" in the pre-event time frame. These common causal factors are still valid today and are important and recurring contributors to actual events.

## **Introduction**

Prevention of significant accidents has always been an important goal of DOE as well as other Government agencies and industry. However, the term "significant" is a judgment and everyone using it has their own opinion as to what events and consequences are significant. Webster defines "significant" as "important, momentous" and "significance" as "importance, consequence, moment." "Important" is defined as "having much significance, consequence or value." And "consequence" in this context is defined as "importance in rank." This circular logic provides much leeway in how the term can be interpreted. DOE and its contractors have struggled with various means to consistently apply the term using discrete numerical estimates, broad ranges of consequence and scenario frequency, and word definitions of injury or impact.

## Background

Two early attempts<sup>1,2</sup> to define "significant" resulted in slightly different sliding scales of event frequency (events per year) versus lifetime-accrued dose guideline in rem (offsite individual) as shown on Figure 1 and Table 1. The scales were slightly different, with the Brookhaven version exhibiting a slight anomaly (two dose numbers at one frequency). 25 rem offsite was the largest evaluation consequence guideline when considering rare, but credible, events. The lower values at higher frequencies corresponded to "well within" or "a small fraction," respectively.

Du Pont<sup>3</sup> also used numerical guidelines. It is worthwhile to note here that all of the numerical schemes were considered guidelines and not absolute indicators of acceptability. Called Farmer Plots, Du Pont plotted Design Basis Accidents from all their facilities onto one graph (Figure 2) to create a site risk envelope. The Brookhaven sliding scale was overlain onto the Farmer Plot and all but one point was "below the line." The NRC risk guidelines<sup>4</sup> of < 0.1% for prompt deaths and < 0.1% for latent cancer were also added and all points were "below the line."

In 1991, DOE adopted the NRC safety goals used in the Du Pont study. Called SEN 35-91, these goals were as follows:

"The risk to an average individual in the vicinity of a DOE facility for prompt fatalities that might result from accident should not exceed one-tenth of one percent of the sum of prompt fatalities resulting from other accidents to which members of the population are generally exposed. For evaluation purposes, individuals are assumed to be located within one mile of the site boundary"

"The risk to the population in the area of a DOE facility for cancer fatalities that might result from accident should not exceed one-tenth of one percent of the sum of cancer fatality risks resulting from all other causes. For evaluation purposes, individuals are assumed to be located within 10 miles of the site boundary"

From these goals a joint subcommittee of the Westinghouse M&O Nuclear Facility Safety Committee and the DOE Safety Envelope Working Group developed high-level waste tank guidelines<sup>5</sup> for both offsite and onsite radiological impacts, Figures 3 and 4, respectively.

1. W. J. Brynda, C. H. Scarlett, G. E. Tanguay and P. R. Lobner, "Nonreactor Nuclear Facilities: Standards and Criteria Guide," DOE/TIC-11603, Brookhaven National Laboratory, (1986)
2. J. C. Elder et. al., "A Guide to Radiological Accident Considerations for Siting and Design of DOE Nonreactor Nuclear Facilities," LA-10294-MS, Los Alamos National Laboratory, (1986)
3. R. F. Bradley, "Risk Acceptance Decisions," DP-1773, Savannah River Laboratory, (1988)
4. U.S. NRC, "Safety Goals for the Operations of Nuclear Power Plants, Policy Statement" 51, Federal Register 30028, (1986)
5. E. J. Hallinan, L. W. Muhlestein, L. F. Brown, R. E. Yoder, Radiological Risk Acceptance Guidelines for High-Level Waste Tanks, prepared for DOE ER and WM, (1992)

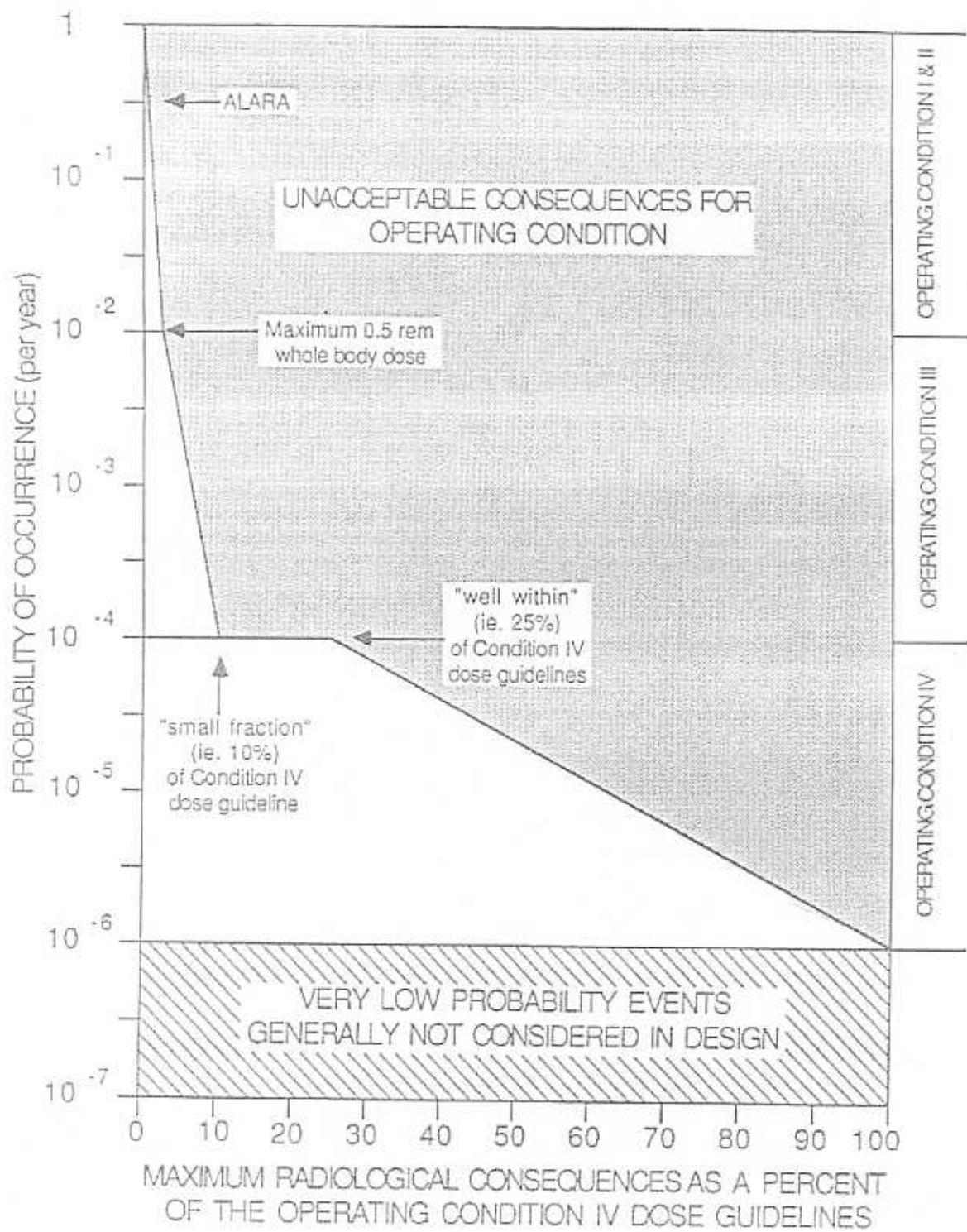


FIGURE 1.2-1. SIMPLIFIED ILLUSTRATION OF THE INTENT OF THE RADIOLOGICAL CONSEQUENCE GUIDELINES

TABLE VI. POTENTIAL RADIOLOGICAL DOSE GUIDELINES FOR ACCIDENT EVALUATION

Probability Category	Nominal Range of Probability ( $y^{-1}$ )	Dose Guideline (rem)				
		Whole Body	Lungs	Thyroid	Bone Surface	Other Organs <sup>a</sup>
Anticipated <sup>b</sup>	$>10^{-2}$	$<0.01$	$<0.03$	$<0.12$	$<0.12$	$<0.06$
Unlikely <sup>c</sup>	$10^{-4}$ - $10^{-2}$	0.01-0.50	0.03-1.5	0.12-6	0.12-6	0.06-3
Extremely unlikely <sup>d</sup>	$10^{-6}$ - $10^{-4}$	0.5-25	1.5-75	6-300	6-300	3-150
Incredible <sup>e</sup>	$<10^{-6}$	$>25$	$>75$	$>300$	$>300$	$>150$

<sup>a</sup>Based on ICRP recommendation of weighting factors assigned to each of organs receiving highest dose equivalent (ICRP 1977).

<sup>b</sup>Incidents that may be expected to occur once or more during the lifetime of the facility.

<sup>c</sup>Accidents that are not expected but may occur sometime during the life cycle of the facility.

<sup>d</sup>Accidents that will probably not occur during the life cycle of the facility. This category includes design basis accidents.

<sup>e</sup>Accidents for which a reasonable scenario is not conceivable.

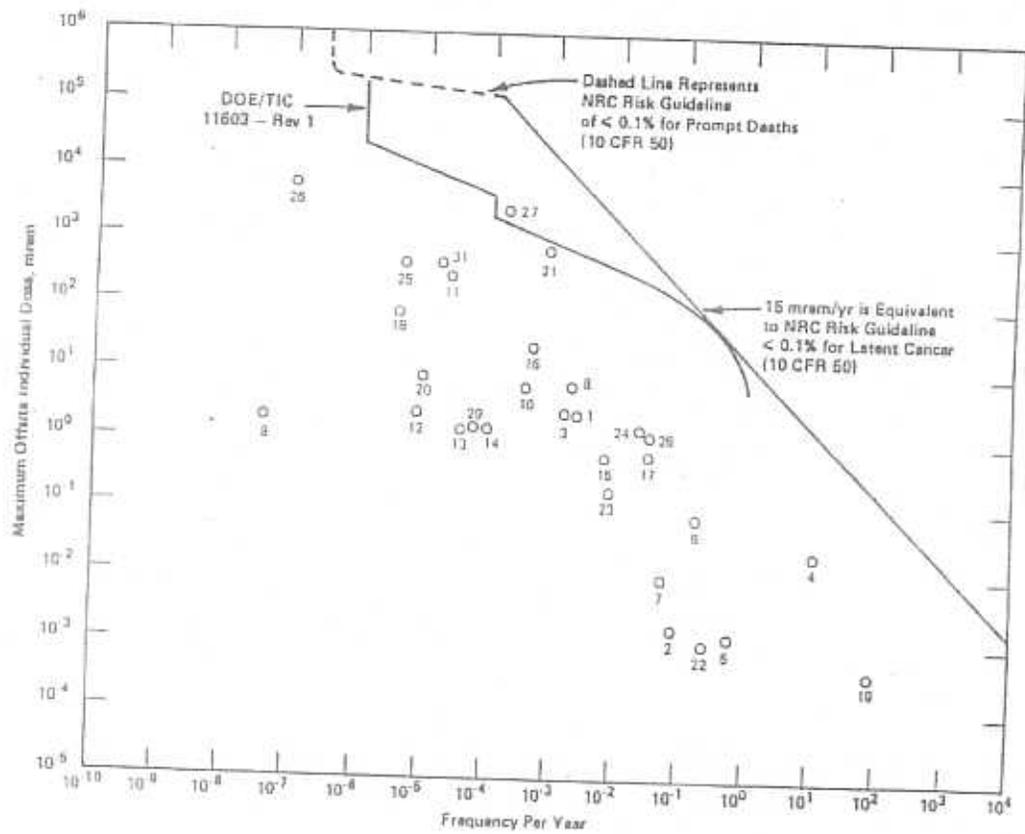
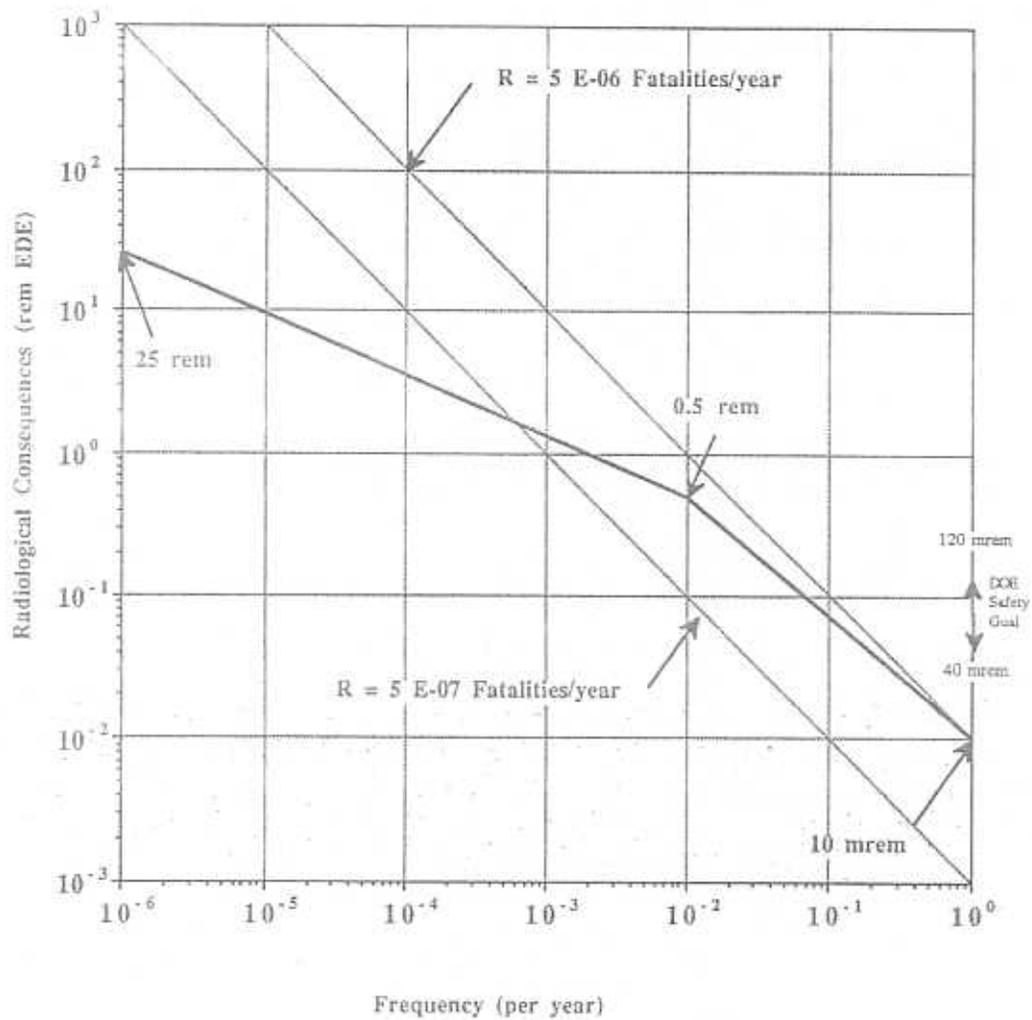
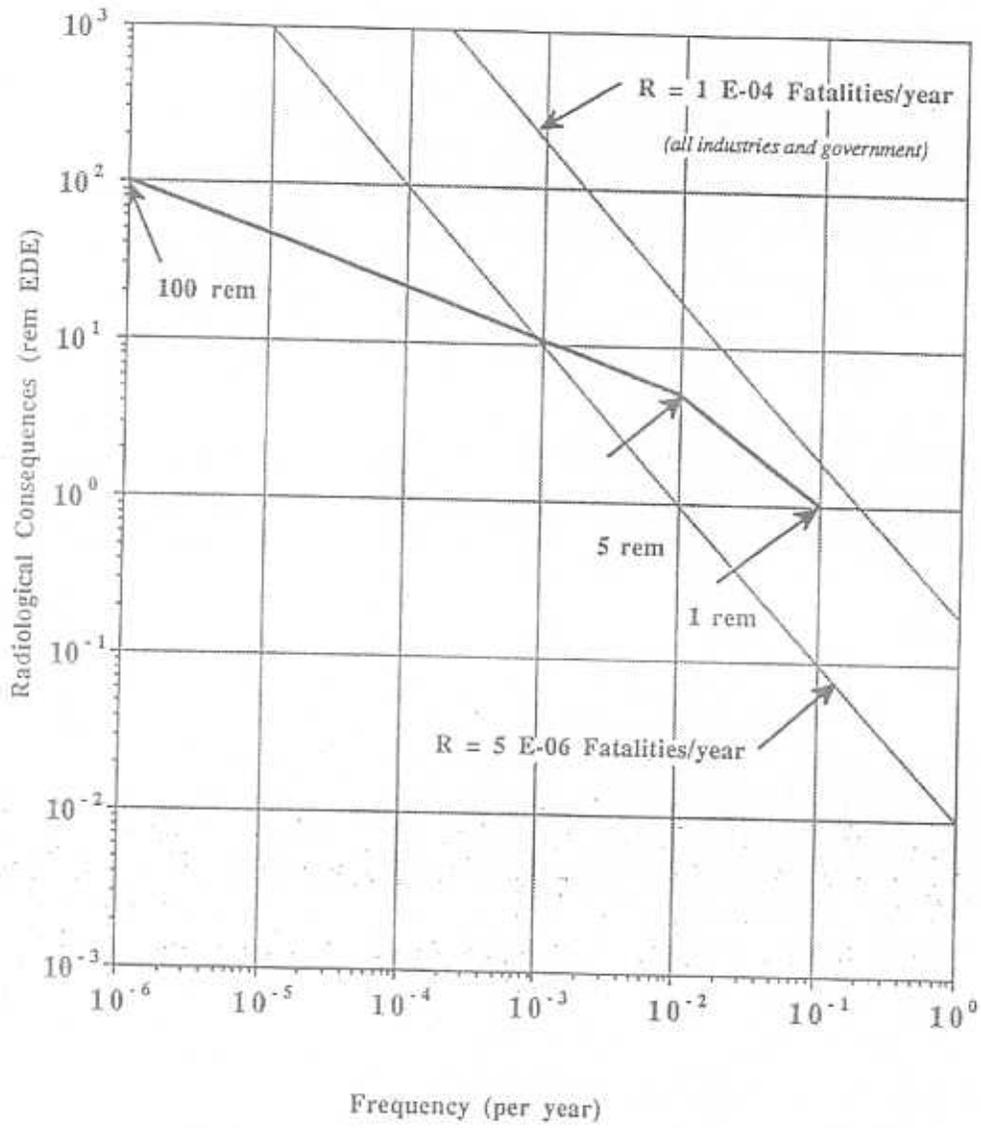


Figure 4. Comparison to NRC Guidelines

## Offsite Radiological Risk Comparison Guidelines



# Onsite Radiological Risk Comparison Guidelines



In 1994, DOE assembled a team to develop a new standard for preparing Safety Analysis Reports (SARs). This standard<sup>6</sup> established a risk rank matrix (Figure 5) to define risk goals. This is the typical three-by-three matrix that we are all used to. Word definitions were used to define bin consequences and three numeric ranges for frequency. The descriptions are presented on Tables 2 and 3, respectively. A consequence goal, originally intended for another standard that was never issued, was added into DOE-STD-3009 later as an appendix. This goal, called an evaluation guideline, is 25 rem independent of event frequency. The evaluation guideline is not supposed to be treated as a design acceptance criterion or an acceptable offsite exposure. It was, however, generally acceptable as indicative of no significant health effects. The standards went on to say that there was no predetermined frequency cutoff value, such as 1E-06 per year, and for operational accidents, no explicit need for a frequency.

Around the same time, DOE also issued a standard<sup>7</sup> containing guidance to address worker safety, mainly for the BIO as DOE-STD-3009 style Safety Analysis Reports (SARs) were being developed. An example was provided in DOE-STD-3011 that identified event frequency bin and consequence levels combinations called Scenario Classes (Figure 6):

Scenario Class IV	-	Negligible
Scenario Class III	-	Marginal
Scenario Class II	-	Serious
Scenario Class I	-	Major

The frequency bins were the same as for DOE-STD-3009. Consequence levels were defined as:

High	> 5.0 rem offsite or 25 rem at 600 m
Moderate	> 0.1 rem offsite or 0.5 rem at 600 m
Low	> Moderate

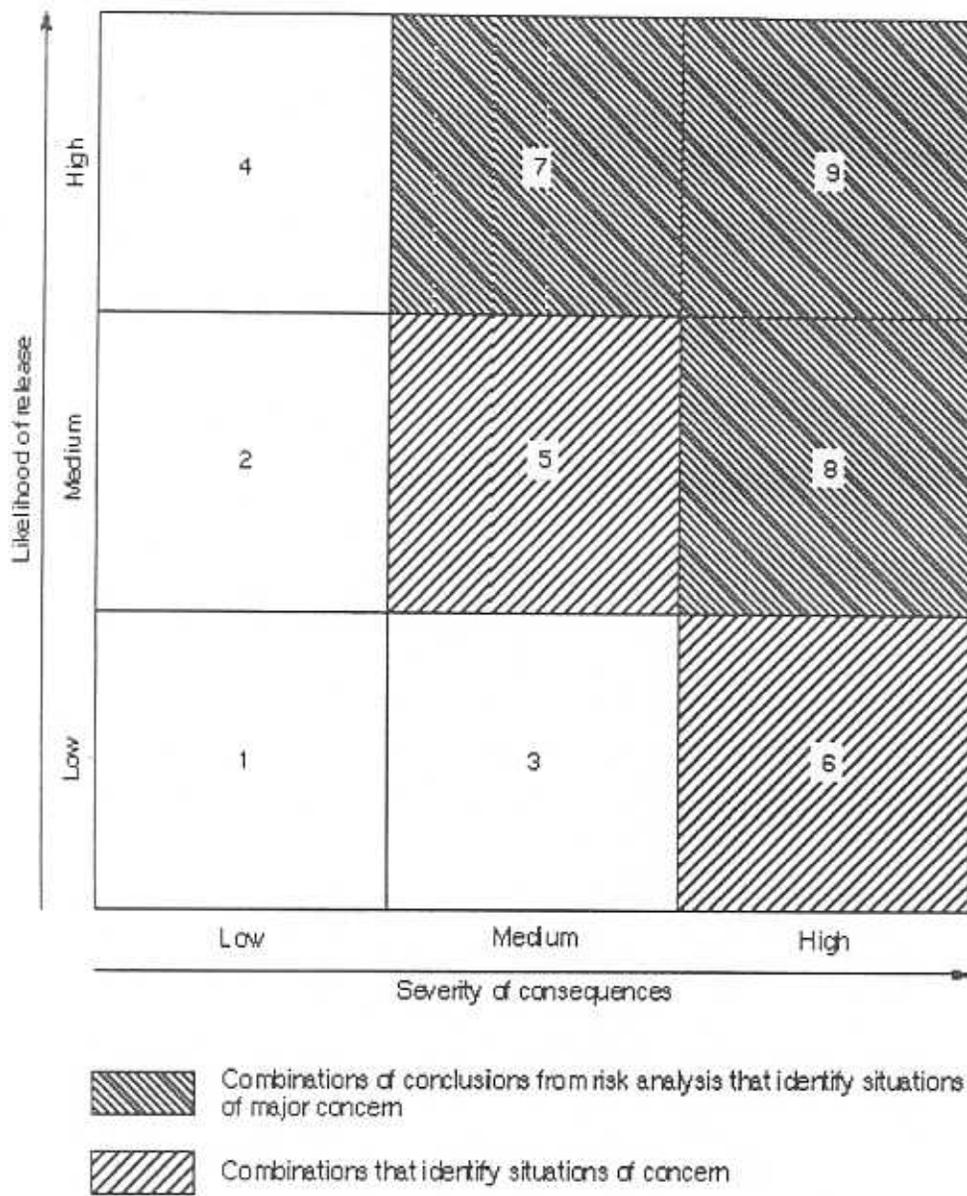
There were no lower or upper bounds. So any release was Low consequence and there was no suggestion that credible events should not exceed 25 rem offsite. And, from Figure 6, there were incongruities in the scenario classes definitions (e.g., High consequence events that are Anticipated have the same Scenario Class as High consequence events that are Unlikely). Plus DOE-STD-3011 introduced worker levels at 600 m where other standards did not specify a specific distance. Thus, this scheme was not very useful and could not easily be compared with any other scheme.

DOE-STD-3011 also introduced worker injury criteria (Prompt death, serious injury), and chemical exposure criteria offsite and onsite. Chemical exposure was based on Emergency Response Planning Guide (ERPG) levels. The standard was careful to say that values presented were intended for binning purposes and not to reflect acceptability of accident consequences. In 2002, the standard was extensively revised and the examples removed.

---

6. "Preparation Guide for U. S. DOE Nonreactor Nuclear Facility Safety Analysis Reports," DOE-STD-3009-94, (1994)

7. "Guidance for Preparation on DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans," DOE-STD-3011-94, (1994)



(Taken from EPA Technical Guidance for Hazards Analysis)

128/014-07 2001

Figure 3-3. A three-by-three likelihood and consequence ranking matrix for hazard evaluation.

Table 3-3. Qualitative severity classification table.

Descriptive word	Description
No	Negligible onsite and offsite impact on people or the environs.
Low	Minor onsite and negligible offsite impact on people or the environs.
Moderate	Considerable onsite impact on people or the environs; only minor offsite impact.
High	Considerable onsite and offsite impacts on people or the environs.

Table 3-4. Qualitative likelihood classification table.

Descriptive word	Estimated annual likelihood of occurrence	Description
Anticipated	$10^{-1} \geq p > 10^{-2}$	Incidents that may occur several times during the lifetime of the facility. (Incidents that commonly occur)
Unlikely	$10^{-2} \geq p > 10^{-4}$	Accidents that are not anticipated to occur during the lifetime of the facility. Natural phenomena of this probability class include: Uniform Building Code-level earthquake, 100-year flood, maximum wind gust, etc.
Extremely Unlikely	$10^{-4} \geq p > 10^{-6}$	Accidents that will probably not occur during the life cycle of the facility. This class includes the design basis accidents.
Beyond Extremely Unlikely	$10^{-6} \geq p$	All other accidents.

TABLE B.I. Example PHA Risk Matrix - Consequence Versus Frequency

High Cons.	II	I	I
Moderate Cons.	III	II	I
Low Cons.	IV	III	III
	below $10^{-4}$ /yr	$10^{-4}$ to $10^{-2}$ /yr	above $10^{-2}$ /yr
	Frequency		

TABLE B.II. Radiological Accident Consequence Levels\*

	Public	Workers
High Cons.	> 5 rem at site boundary	> 25 rem at 600 m or prompt death in facility
Moderate Cons.	> 0.1 rem at site boundary	> 0.5 rem at 600 m or serious injury in facility
Low Cons.	< Moderate	< Moderate

\*Values are intended for binning purposes only and do not reflect the acceptability of accident consequences.

TABLE B.III. Chemical Accident Consequence Levels\*

	Public	Workers
High Cons.	> ERPG-2 at site boundary	> ERPG-3 at 600 m or prompt death in facility
Moderate Cons.	Not applicable	Serious injury in facility
Low Cons.	< High	< Moderate

\*Values are intended for binning purposes only and do not reflect the acceptability of accident consequences.

## **Current Practices**

The DOE guidance remaining with respect to assessing risk is in DOE-STD-3009. As noted earlier, the standard contains mainly word definitions and only mentions the offsite evaluation criterion, 25 rem. With this and a prohibition against quantifying accident risk acceptability, contractors must use engineering judgment to make design and control decisions that are defensible and consistent. Many contractors still begin with some form of quantification, or risk binning matrices with numerical ranges, to guide their decisions while being careful not to treat numerical estimates as absolute limits in order to protect challenges as well as exceedances. "Challenge" is defined in Webster as "make demands on."

This qualitative philosophy has also been extended into determination of Unreviewed Safety Questions, the practice of assessing changes against approved risk. Since 10 CFR 830, Subpart B was promulgated, and guidance issued, contractors have been informed by DOE auditors that they cannot legally use numerical means to determine if a USQ exists. Instead, they must use informed engineering judgment to assess if the change in risk is "clearly discernible" and identify the direction of the risk change. "Discern" is defined in Webster as "to separate mentally" or "make out clearly."

Today, risk estimates in Documented Safety Analyses (DSAs) can consist of a word-defined frequency range (Anticipated, Unlikely, Extremely Unlikely) plus a numerical consequence estimate with associated error range or sensitivity. Usually consequence is calculated from the airborne source term via the "Five-Factor-Formula" using conservative material at risk, damage ratio, airborne release fraction, respirable fraction, and leakpath factor. The airborne source term is then transported to the receptor by standard meteorology equations and assumptions.

While accident frequency can be estimated quantitatively or by comparison with historical evidence, engineering judgment can also be used. Sometimes, events are simply declared to be Anticipated. This approach is more cost-effective than expensive quantitative analysis. If Safety Class or Safety Significant features are identified, they are assumed to work when challenged, because of stringent requirements for those functional classifications. For administrative controls, generic program functions are usually referenced (conducting bioassays) and compliance with requirements is assumed.

Finally, human factors credited in safety analyses typically use ballpark estimates such as failure of a single properly trained individual to perform a routine function at a certain rate (say once per hundred evolutions) depending on function. And workers are assumed to respond properly to accidents based on experience, training, and compliance with procedures.

## **Event Histories**

As important as predictions and assumptions are to the goal of preventing accidents, it is also important to verify that they accurately represent reality and identify actual precursors. This section will discuss a few past events selected from DOE as well as other sources. The events were selected to make a few points about precursor protection and the value of learning lessons.

The selection is not representative of the majority of past events and does not purport to address the most significant contributors to those events.

The events discussed below are covered roughly in chronological order starting with the earliest. Some of the material presented was extracted from the DOE Training Course on Prevention of Significant Events, taught in Idaho Falls June 3-6, 1985. Hopefully, the proposed DOE Safety Basis Academy curricula being developed by LANL will have modules on DOE adverse occurrences, including accident conditions, causes and lessons learned.

### **Savannah River Site Red Oil Explosions (circa 1954)<sup>8</sup>**

The 1953 explosion occurred while concentrating a uranyl nitrate – nitric acid solution destroying an evaporator and injuring two personnel. Tributylphosphate (TBP) was present in the solution. In 1975, a similar explosion occurred in A-Line, caused in part by TPB collecting at the bottom of the tanks. Again personnel injuries were minor due to quick actions. The building required six months to repair.

Even though it was known that organic layers could sink in a more dilute solution in the A-Line tanks, that fact was not mentioned in process documentation so operators were unaware of the unusual condition. Non-standard flush solutions were being processed. And personnel had become complacent because of favorable operating experience. A tank cleanout had been planned but was not made before this campaign.

### **Brown's Ferry Fire (1975)<sup>9</sup>**

The U.S. Nuclear Regulatory Commission, in its Notice of Violation, noted that there was no safety evaluation of operating the reactor while penetration checks were underway which was not covered in the SAR. As part of their response, TVA stated that unsealing and sealing penetrations were not considered a change to design (not needing safety evaluation) as long as limiting conditions from the Technical Specifications were maintained. Obviously the change contributed to the event, and was not adequately considered against SAR conclusions nor protected by the Technical Specifications.

Also detailed procedures had not been prepared for the work on the penetrations. [In today's language this might be called skill-of-the craft]. And conditions adverse to quality were not promptly identified and corrected, nor was required documentation supplied to management from two previous fires. Many electrical systems, considered independent, had failed from common-mode failures caused by feedback and close proximity.

---

8. W. S. Durant, "Red Oil Explosions at the Savannah River Plant," DP-MS-83-142, presented at the 1985 DOE Training Course on Prevention of Significant Events, Idaho Falls (1985)

## LLNL Plutonium Spills (1980)<sup>10</sup>

The first event resulted from glovebox over-pressurization from an Argon supply line that was a recent modification. An Argon pick was used as a trial to flush particles from threads in a reaction chamber flange. The lab was unoccupied at the time. A release occurred partially due to improper installation of both the modification and downstream HEPA filters.

The second spill resulted from a flash glovebox fire of ethanol vapor in air ignited by an ultrasonic cleaner inadvertently left on. Contributing factors included a lack of awareness of personnel to the flammable-mixture, and inadequate training and surveillance.

Some contributing factors were: absence of appropriate review of the modification, and inadequate QA, surveillance and training. In particular, the QA office was working with facility management to improve the building program, but progress was slow because of staffing problems and a heavy workload. There had been significant turnover of programmatic staff ranging from 50% to 70% in some organizations, leading to manning vital functions with inexperienced personnel. And facility operation had been interrupted by numerous tours.

## Space Shuttle (1986, 2003)<sup>11</sup>

The two Space Shuttle disasters are probably the best known and analyzed of all events, save TMI and Chernobyl. Everyone is familiar with the O-ring seal failure on the booster and foam strike impact on the wing direct causes of those accidents. And equipment failure is usually well considered in DOE safety analyses. But there are many other considerations that also may have relevance to DOE safety analyses and may not be adequately considered. The Accident Investigation Board pointed out several contributing factors including:

- Deferring aging infrastructure repairs
- Budget constraints impacting resources required for maintenance, upgrades and redundancy
- Workforce reduction and outsourcing culling layers of experience and hands-on knowledge
- No focus on past accidents to mentor new engineers or those destined for management
- No quantitative, program-wide risk and safety database to support risk assessments
- Lack of standardized structure in various safety program organizations
- Frequent reorganizations that reduce the budget for safety
- Decision-making process with little in the way of formal and consistent criteria
- Large number of hazards reports that contain subjective and qualitative judgment
- Hazards analysis processes that are applied inconsistently across systems and components
- Information systems that are extremely cumbersome and difficult to use

---

9. R. L. Scott, "Brown's Ferry Nuclear Power-Plant Fire," Nuclear Safety, 17, 5, (1976)

10. "Report of the Investigation of the Pu Bldg. Incidents at LLNL on April 8 and 16, 1980," presented at the 1985 DOE Training Course on Prevention of Significant Events, Idaho Falls (1985)

These are conditions that exist today within the DOE complex. While they may not directly lead to an accident, they do not help to anticipate or prevent accident conditions. And they are not usually considered in safety analysis as contributing events.

### **Texas City Refinery Explosion (2005)<sup>12</sup>**

The recent explosion at the BP refinery in Texas City killed eleven employees and spawned a number of bulletins and lessons learned within the DOE complex. The referenced Environment, Safety and Health Advisory notes that "the routine use of steadily decaying infrastructure poses an escalating probability of an event if managers and operators are unwilling to adopt an inquisitive safety posture and adjust their habits to reflect changing conditions." Also noted was a recommendation to "ensure that all personnel, including supervisors, have the required levels of expertise and that training or certifications are current." Again, aging infrastructure is usually not considered in safety analysis, nor protected by it. And most safety analyses assume that everyone has "adequate" training.

### **Conclusions**

This set of past events indicates that aging infrastructure, budget constraints, inadequate training, inadequate review, subjective judgment, loss of experience base, workforce restructuring, inconsistent or inadequate hazard analysis, non-standard operations and bad assumptions can contribute to real event occurrence.

Extensive numerical analysis has its drawbacks. If not careful, methodology can be overemphasized rather than focusing on the real impact to safety. Or, more effort can be expended on trying to defend unrealistic accuracies or mistaken assumptions in order to minimize cost impacts instead of making real safety improvements.

However, as can be seen from real events, relying on expert-based judgment with unclear goals is not without its drawbacks. Results of subjective analyses are notoriously inaccurate and hard to defend. They are also inconsistent both within a large site with multiple operations and field offices as well as across the DOE complex. And, as DOE and DOE contractors lose experienced personnel, adequate and consistent training is not available nor will help to make up the difference.

Finally, contributing conditions from past events such as those discussed above should be factored into hazards and safety analysis to ensure that all important assumptions are adequately protected, including adequacy of staff, training, review, and infrastructure. And increasing equipment failure for wear-out as well as failure estimates for Safety Class and Safety Significant functions should be incorporated to include their effects.