BNL-62612
CONF-960647--3

Risk-Based Approach to Analyzing Operating Events*

A. R. Marchese
U. S. Department of Energy
Washington, DC , U.S.A.
and
P. Neogy
Brookhaven National Laboratory
Upton, New York, U.S.A.

RECEIVED
FEB 12 1996
OSTI

Introduction

Existing programs for the analysis of operating events at the Department of Energy (DOE) facilities do not determine risk measures for the events. An approach for the risk based analysis of operating events has been developed, and applied to two events [1]. The approach utilizes the data now being collected in existing data programs and determines risk measures for the events which are not currently determined. Such risk measures allow risk appropriate responses to be made to events, and provide a means for comparing the safety significance of dissimilar events at different facilities.

Risk-Based Approach

An overview of the approach is presented in Figure 1. Given an operating event, potential undesirable consequences (such as injury or fatality to workers or members of the public, property damage, impact on the environment, etc.) are identified. Qualitative estimates are made of the conditional probability of occurrence of the undesirable consequence(s), and of the magnitude of the consequence itself. The conditional probability is estimated on the basis of the residual protection, or the number of remaining barriers that provide protection from the undesirable consequence. If one (or fewer) barrier remains, the conditional probability is assessed as "high". It is assessed as "medium" with two barriers remaining, and as "low" with three or more barriers. The consequence is assessed as "high" if the potential exists for fatality or property damage in excess of $1,000,000, "medium" if the potential for severe injury or property damage in excess of $100,000 exists as a result of the event, and as "low" otherwise. The qualitative assessment of the conditional probability and the consequence allows an assessment of the conditional risk from the event. If this risk is less than "medium-medium", no further analysis is necessary, and the results of the qualitative assessment are documented.

---

*This work was supported by the U.S. Department of Energy under Contract DE-AC02-76CH00016.

MASTER

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

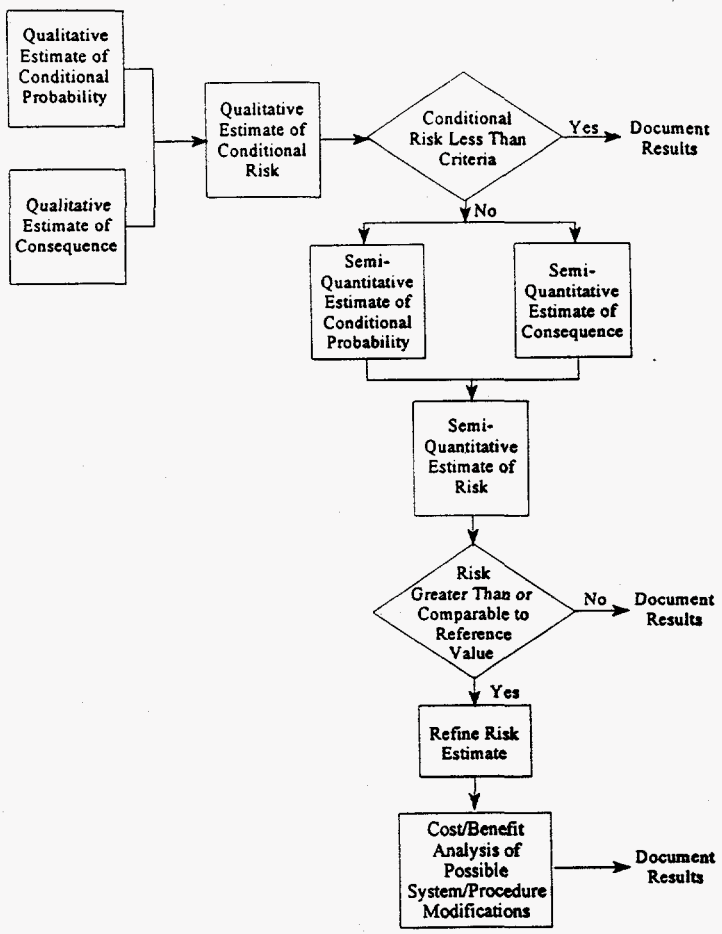

Figure 1 Overview of Risk Based Approach

A semi-quantitative estimate of the conditional probability is determined using a simplified event tree or a simplified fault tree that incorporates the barriers. The failure frequencies utilized are based on facility specific data if available, generic data or informed estimates. Similarly, a semi-quantitative estimate of the magnitude of the consequence is determined. For industrial hazards, the consequence is usually self-evident. For radiological and chemical hazards, an accident analysis approach similar to that developed within DOE's Defense Programs [2] is utilized to estimate the consequence. Since most events with a conditional risk of "medium-medium" or higher would have some likelihood of fatality to a worker, it is convenient to use the risk of fatality from the event as a risk measure to categorize the event. This risk measure gauges the safety significance of the event and helps in deciding what the appropriate level of response to the event should be. Before engaging in additional analyses, it is necessary to ensure that they are justified by the level of risk posed by the event. This is achieved by comparing a risk measure of the event, the fatality risk,

to some reference value. If the fatality risk is not greater than or comparable to this reference value, then a risk appropriate response to the event may not include any corrective actions. In this case, further analysis of the event is unnecessary, and the results of the analysis performed thus far are documented. If the fatality risk of the event exceeds the reference risk value or is comparable to it, then the risk estimates already obtained are refined. A more detailed consideration of the function and efficacy of the systems, components, structures and procedures that play a preventive or mitigative role during the event, particularly those that are likely candidates for upgrading as a corrective measure, is also undertaken at this time. Finally, a cost-benefit analysis of possible systems and procedure modifications is undertaken.

Applications

The analytical approach has been applied to (1) a glove box fire in a plutonium processing and fabrication facility, and (2) an electrical hazard event at a composite materials technology facility presently under construction. The results of the analysis are presented in the form of simplified event trees and fatality risks associated with the events. The choice of the events was made in part to demonstrate the applicability of the methodology to incidents involving radiological as well as non-radiological, industrial hazards.

Glove Box Fire

In November 1994, contaminated rags drying on the floor of a glove box in a plutonium processing and fabrication facility were found to be undergoing spontaneous combustion. The glove box was successfully isolated from any source of oxygen, and the smoldering rags were subsequently allowed to burn to completion by controlling the flow of oxygen to the glove box. The rags are believed to have self heated due to contamination with Pu^{238}. No radioactivity was released as a result of this event. Given the observed event, the spontaneous combustion of rags in the glove box, several barriers existed to prevent the release of radioactivity. These are: (1) detection of the fire and intervention to contain it, (2) maintenance of glove box contamination despite the fire, and (3) the ventilation system which maintains the glove box at a negative pressure with respect to its surroundings and minimizes a release when the glove box containment is lost. Based on the three barriers that remained, the conditional probability of release was characterized as "low". The consequence of the release was judged to be in the "medium" category based on the large specific activity and the large inhalation dose conversion factor of Pu^{238}, although the amount of Pu^{238} in the rags was presumed to be small. The conditional risk of the event is therefore "medium-low". At this point, the analyst may decide that no further analysis is necessary (in accordance with Figure 1). To illustrate the methodology, and determine that the conclusions based on qualitative analysis are valid, the remaining steps are described below.

Figure 2A presents a simplified event tree based on the barriers discussed above. The likelihood of a fire being detected depends on how frequently the room is checked by a worker during normal operational shifts or by a security personnel at other times. The

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.

likelihood of the fire being contained after detection will depend in part on the skill and training of the worker to perform this non-routine task. The fact that the fire was detected and contained in this instance indicates that the likelihood of detecting and successfully containing the fire is not considerably smaller than unity. In the absence of more detailed information or analysis, this likelihood was estimated to be about 0.5. If the fire escapes detection, there is still some likelihood that the fire would extinguish itself without breaching the glove box containment. This likelihood will depend on the size of the fire and its location (proximity to the flammable gloves). Since the amount of combustible material consisted of about a quarter pound of rags probably placed near the center of the glove box floor, the fire had the potential to be small and localized. The likelihood of the glove box containment to be maintained despite the fire burning undetected was again estimated to be about 0.5. At the facility in question, there have been incidents of release of radioactivity from a glove box after it is breached due to improper ventilation or improper worker response. The likelihood of the ventilation system to be defeated after a breach of glove box containment is estimated to be about 10^{-2}. The conditional probability of a significant release was, therefore, estimated at 2.5×10^{-3} ($0.5\times0.5\times.01$). Given a release, the maximum dose to a worker in the room was estimated at 19.2 rem (based on an estimated 18 g of Pu^{238} in the rags, and assuming instantaneous, uniform dispersal of airborne Pu^{238} particles within the room). The corresponding risk is presented in Figure 2B and compared to the threshold for significant risk adopted by the Occupational Safety and Health Agency (OSHA) in its final benzene rule (10^{-3} fatality) and the average lifetime accidental fatality risk in U.S. industries (4×10^{-4} fatality per work life of 40 years).

Electrical Hazard

In June 1994, an electrician working on a 480-volt main distribution panel in a composite materials technology facility received serious flash burns from an electrical fault and the subsequent electrical arc blast. The electrical fault occurred when a ground wire to be installed made contact with the exposed parts of energized incoming connections on the main breaker, which had been turned off. After an electrician removes the protective cabinet enclosure covering a distribution panel, several barriers exist in principle to protect him. The first of these is a work plan that acquaints him of the hazards involved and provides him with instructions to safely execute his task. A second barrier exists in the form of a procedure for electrical energy isolation and control (lockout/tagout). Lastly, protective equipment such as gloves, blanket and safety glasses provide a third barrier. For the event analyzed, as we shall see, the first barrier failed and, consequently, the second and third barrier failed as well. Because of the crucial role played by the failed first barrier, and the dependent nature of the subsequent barriers, the conditional probability of severe injury was judged to be "high". Since the potential for severe injury or fatality existed, the consequence was also judged as "high", leading to a "high-high" categorization of the conditional risk.

Figure 3A presents a simplified event tree for the electrical hazard incident. A work plan was generated for the activity but was deficient in several respects. The task was categorized as low risk based on considerations of public health and safety, not risk to the worker. The work plan was also deficient in that it did not require a high voltage lockout/tagout to completely de-energize the panel. The work plan also did not identify

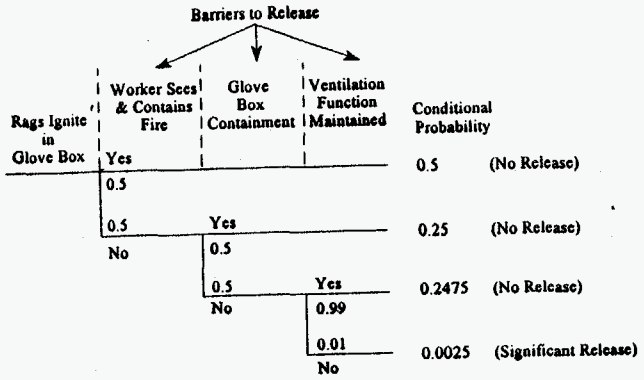

Figure 2A Simplified Event Tree for the Glove Box Fire

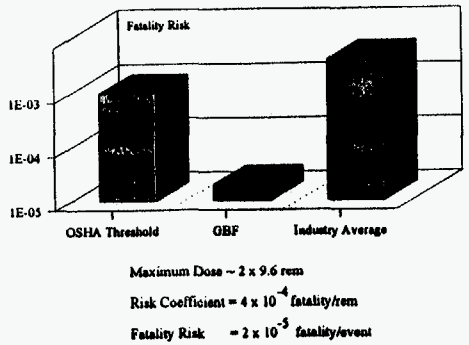

Figure 2B Comparison of Risk to Reference Risk for Glove Box Fire

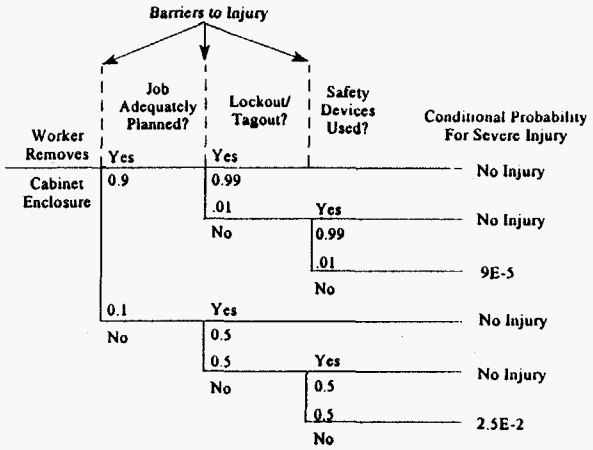

Figure 3A Simplified Event Tree for the Electrical Hazard Incident

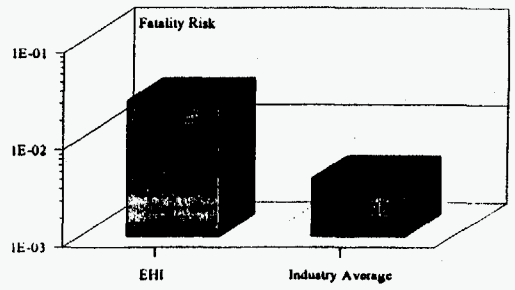

Figure 3B Fatality Risk from the Electrical Hazard Incident

which protective equipments, if any, were needed for the work, and did not make any provisions for making the equipment available to the worker. The deficiencies in the work plan were due to human errors. These human errors belong to the category of initiator actions, including slips and mistakes, that cause initiating events. This category of human error has nominal probabilities in the range of 10^{-2} to 10^{-4}. The probability may be an order of magnitude higher if a need exists for systems knowledge or for the interpretation of indirect information, as existed in this case. The probability of an inadequate work plan was, therefore, taken to be 10^{-1}. Because the work plan failed to specify lockout/tagout and protective equipment, these barriers were as likely not to be implemented as to be implemented. The conditional probability for a severe injury was, therefore, estimated at $0.1 \times 0.5 \times 0.5$ or 2.5×10^{-2}. Considering that fatal injuries are about an order of magnitude less likely than severe injuries, the conditional probability of fatality may be estimated at 2.5×10^{-3}, which is also the risk of fatality from this event. Figure 3B presents the fatality risk from the event and compares it to the average lifetime accidental fatality risk in U.S. industries. Clearly, the risk from the event is greater than the average accidental fatality risk, and further efforts are needed to reduce this risk. The following general observations are made here regarding the risks associated with this event and the benefits of reducing these risks. This event occurred due to human errors at two levels: (1) errors that led to an inadequate work plan, and (2) the failure on the part of the individual to take greater responsibility for his own safety and use appropriate safety equipment and safe work practices. Implementation of necessary actions to ensure that work plans are developed to take into account worker risks as well as public health and safety is a crucial step in reducing the frequency of similar incidents. Training the workers to take more responsibility for their own safety by using appropriate safety equipment and safe work practices will reduce both the frequency and consequences of such incidents.

Conclusions

In this paper we have presented a step-wise approach to reviewing operating events for their safety and risk significance. The risk-based approach allows a quick determination of the appropriate level of response to an event, and the cost-benefit aspects of any contemplated corrective action. Reference risk values have also been suggested for comparison to the risks from individual events. The calculation of a quantitative risk measure such as the fatality risk associated with events also allows a meaningful comparison to be made of the safety and risk significance of dissimilar events. Although we have restricted ourselves to individual events, the method could be extended to examine the risk significance of a class or family of events. By aggregating and analyzing operating events of a similar nature, it would be possible to examine the risk implications of the underlying safety issues.

References

1. Preliminary results of this analysis were presented at the 1995 Winter Meeting of the American Nuclear Society (P. Neogy and A.R. Marchese, Trans. Am. Nucl. Soc., 73, 280, 1995).

2. U.S. Department of Energy Defense Programs Safety Survey Report, D. Pinkston, editor, DOE/DP/70056-H1, November, 1993.