LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

UCRL-CONF-210895

Total Risk Approach in Applying PRA to Criticality Safety

S. T. Huang

March 29, 2005

American Nuclear Society Meeting
Knoxville, TN, United States
September 19, 2005 through September 22, 2005

TOTAL RISK APPROACH IN APPLYING PRA TO CRITICALITY SAFETY

Song T. Huang, Ph.D
Lawrence Livermore National Laboratory
P.O. Box 808, Livermore, CA 94550
Huang3@llnl.gov

ABSTRACT

As nuclear industry continues marching from an expert-base support to more procedure-base support, it is important to revisit the total risk concept to criticality safety. A key objective of criticality safety is to minimize total criticality accident risk. The purpose of this paper is to assess key constituents of total risk concept pertaining to criticality safety from an operations support perspective and to suggest a risk-informed means of utilizing criticality safety resources for minimizing total risk.

A PRA methodology was used to assist this assessment. The criticality accident history was assessed to provide a framework for our evaluation. In supporting operations, the work of criticality safety engineers ranges from knowing the scope and configurations of a proposed operation, performing criticality hazards assessment to derive effective controls, assisting in training operators, response to floor questions, surveillance to ensure implementation of criticality controls, and response to criticality mishaps. In a compliance environment, the resource of criticality safety engineers is increasingly being directed towards tedious documentation effort to meet some regulatory requirements to the effect of weakening the floor support for criticality safety.

By applying a fault tree model to identify the major contributors of criticality accidents, a total risk picture is obtained to address relative merits of various actions. Overall, human failure is the key culprit in causing criticality accidents. Factors such as failure to follow procedures, lacks of training, lack of expert support at the floor level etc. are main contributors. Other causes may include lack of effective criticality controls such as inadequate criticality safety evaluation. Not all of the causes are equally important in contributing to criticality mishaps. Applying the limited resources to strengthen the weak links would reduce risk more than continuing emphasis on the strong links of criticality safety support. For example, some compliance failures such as lack of detailed documentation may not be as relevant as the lack of floor support in answering operator's questions during operations. Misuse of resources in reducing lesser causes rather than on major causes of criticality accidents is not risk free without severe consequences.

A regulatory mandate without due consideration of total risk may have its opposite effect of increasing the total risk of an accident. A lesson is to be learned here. For regulatory standard/guide development, use of ANS/ANSI standard process, which provides the pedigree of consensus participation, is recommended.

Key Words: criticality, safety, PRA, accident, causes

1 INTRODUCTION

As the nuclear industry continues marching from an expert-base support system to a procedure-based compliant environment, it is important to revisit as applied to the total risk concept to nuclear criticality safety. The total risk concept is not new in criticality safety. A key objective of criticality safety is to minimize total criticality accident risk. There are several reasons for this. First, a criticality accident is just one of the hazards in nuclear facility operations. Other risks include fire, chemical hazards, high temperature / high-pressure excursion, and explosion, etc. For example, in the case of requiring a criticality alarm system, it is necessary to examine the impacts of a false alarm to plant/personnel safety to ensure that total risk is minimized.

Within the context of minimizing total risk, various compliant requirements to enhance criticality safety need to be assessed to ensure that they will not inadvertently introduce an overall adverse impact to criticality safety. The purpose of this paper is to assess key constituents of the total risk concept pertaining to criticality safety from an operational support perspective and to suggest a risk-informed means of utilizing criticality safety resources for minimizing total risk.

1.1 Historical Perspective on Nuclear Criticality Accidents

As we begin to examine total risk, it is important to bear in mind that the concept of risk involves both likelihood of occurrence and its consequence due to criticality accidents. For the purpose of this paper, we have limited the domain of criticality accidents to exclude nuclear power reactors. Given this definition, most of the consequence from a criticality accident would be limited to an area within a facility or on-site. However, impacts to operation personnel can be very severe including fatality due to excessive radiation exposure.

From the floor support perspective to minimize the risk of criticality accidents, the yield of a nuclear excursion depends more upon the types and the scope of nuclear operations and hence is less amenable to normal preventive measures once the criticality excursion occurs. To address reducing the risk from a criticality accident, we have taken the approach to focus more on the probability of a criticality rather than on its consequences.

Reference 1 provides an excellent review of criticality accidents which have occurred in the world. For the purpose of this paper, we choose the process criticality accidents for illustration. Of the twenty-two process accidents, twenty-one accidents occurred with the fissile material in solutions or slurries and one accident occurred with metal ingots. The contributing causes of the accidents are summarized in Table 1. For illustration, we have grouped the failures into human errors, hardware failures, and non-hardware support failures. The human errors are further categorized into individual operator errors and independent operational support failures. The individual operator errors include inadequate training, violation of procedures, and miscommunication. The category of hardware failures includes use of non-favorable geometry vessels, design error, and others. The categorization of main contributing causes is necessarily subjective in nature. Based upon the historical data as summarized in Table 1, it is quite clear,

however, that unfavorable geometry vessels used in the solution systems and human errors are the two pre-dominant contributing factors in those accidents.

Thus, we concur with the assessment in Reference 1 that the replacement with favorable geometry vessels in the processing facilities was one of the major reasons for reducing the criticality accident rate from once per year in the 1960's to about once per every ten years as seen in last few decades. However, improvement's in understanding and minimizing the human error causes appears to be very slow. Lack of research and development in this area also contributes to the apparent loss of focus on the total risk reduction from the operation floor support perspectives.

1.2 The Issues of Human Error in System Analysis

When assessing equipment failures, a tradition approach is to look at the various components and assess their failure mechanisms. This approach works reasonably well for hardware systems as the failures of component parts do relate to the failure of equipment in some identifiable ways in most cases. However, the same approach does not work well in assessing human failures. Thus, a mechanistic approach attempting to dissect the causes of the human errors, either errors of commission or omission, to the make-up of a person has not been fruitful up to this point. Instead, emphasis has been directed towards the assessment of a few selective human errors on a "performance base ". The terms such as failure to follow procedures, lack of training, miscommunication, stress, lack of safety culture etc., have been used in an effort to further refine the human error causes. The fundamental problem is that these terms are not well defined and they are not necessarily mutually exclusive nor do they lend themselves to linear relationships for objective formulation, let alone meaningful quantification.

This then presents a huge challenge to probabilistic risk assessment (PRA) approaches. Traditional PRA utilizes both event tree and fault tree formulations. The use of an event tree involves assignment of various "barriers" or "systems/functions " by which the propagation paths of an accident are defined through the success or failure of these "barriers". The fault tree is used to quantify the frequency of occurrence of the performance of each of the barrier branch in an event tree. These approaches generally work very well with hardware systems where the failure rates are available. However, the PRA approach would not be too productive for accidents where the main causes are due to human errors such as the case in criticality accidents as shown in Table 1.

The propagation of an accident sequence through various safety systems can be logically analyzed through PRA. The controls and/or system redundancy can be placed to enhance performance of a particular weak link in the accident path to minimize/mitigate that particular accident. However, when an accident sequence involves human failure as one of its main branches, such an assessment tends to be limited to a higher level unless further research is accomplished in human behavioral science to better define the various relationships among human failure mechanisms and thus enabling acquisition of their failure rate data bases.

Fortunately in the system analysis arena, there is another way of minimizing the total risk. Instead of trying to control the outcomes of an accident propagation path, effort can be spent to minimize the accident domain. For example, if a process system does not include a critical mass

inventory, it is criticality safe regardless of any process upset initiators and any failures of various safety system barriers, including human errors. In other words, mechanistic controls of any accident sequence are not relevant if the nature of process such as fissile mass, or neutron leakage limit the accident domain to be acceptably small. This may help to explain why the double contingency principle and the defense-in-depth approach, which are the corner stone of the national consensus standards for criticality safety, have proven to be very successful in last forty years.

2 Total Risk From the Operations Floor Support Perspectives

Although much more R&D is required to enable full quantification of the human behavior based failures, it is feasible to provide a relative qualitative assessment for various factors contributing to the total risk reduction in criticality accident from the operation floor support perspectives.

For the purpose of our discussion, the contributing factors may be portrayed conventionally as a fault tree in Figure 1. It is noted that other than the use of unfavorable geometry vessels in a process plant, human error is the main cause for criticality accidents. This observation on the human errors as one of the main causes for criticality safety concerns is supported also by several earlier studies of criticality safety violations (References 2 and 3). Thus, the discussion below is mainly limited to the human error branch in Figure 1 because it is the predominant contributing cause. The issue of reducing human errors may be conveniently divided into two main subcategories. The first one deals with issues associated with individual operators. This may include inadequate training, failure to follow procedures, and stress factors, etc. Failure to follow procedures could be due to lack of caring or other factors. Miscommunication could be due to stress factors. As mentioned before, there are other ways of presenting human errors. The second branch deals with lack of independent support to the operator. For example, an operation which utilizes a second independent verification of a proposed action, be it an independent computer checking system or a second person checking, is a very good way of enhancing operation safety. Similarly, floor support is a very important safety measure. This may include a second person knowing the process system operations and/or a criticality safety engineer ready to support an operator in resolving his/her questions on criticality controls, etc. The values of operation floor support cannot be over-emphasized as such support can directly be related to the mitigation of many potential error paths that an operator can commit without such a support.

Note that not all branches in Figure 1 are equally important in contributing to the total risk and that the human error branch has been identified as one of the main contributing causes throughout the actual history of criticality accidents. It is relatively clear that in addition to strengthening operator training to enhance individual operator's performance, a second independent verification means and an effective floor support to the operators by criticality safety professional are very important in criticality safety. Obviously, more research is required to provide a basis for quantification. However, it is quite easy to deduce that any actions which diminish the floor support would have a major negative impact on the total risk.

3 Other Major Stakeholders in the Total Risk Approach

Major stakeholders in criticality safety include more than just operators. Discussed below are some of requirements on these stakeholders from the total risk approach perspective.

3.1 Program/Facility

Program/Facility management is the line organization that is ultimately responsible for criticality safety in their operations. From Figure 1, it is clear that programmatic oversight should concentrate on providing the required support to minimize the high contributing factors. This would include providing geometry safe equipment, operator training, safety meetings, and second independent verification, as well as ensuring adequate floor support from criticality safety specialists.

3.2 Regulatory Oversight

In a compliance driven environment, regulators play an ever-increasingly important role in the total risk approach. The worst thing that can happen is to impose unfunded regulatory mandates. Given the fact that criticality safety engineer resources are limited at most facilities, it is important that regulatory actions should concentrate on enhancement of the factors that minimize operator errors. In this regard, any regulatory actions which take criticality safety engineers away from providing effective floor support, will have detrimental impacts to the total risk.

3.3 Criticality Safety Engineer

Assignment of criticality safety professionals to support nuclear facilities was credited as one of the measures which reduced the frequency of criticality accidents after the early 1960's (Reference 1). Historically, expert-based support has been used effectively to minimize the potential for criticality accidents. Floor support should provide available criticality safety specialists who perform regular walk-through inspections of work stations, answer operator questions, and serve as team members at the operations floor. Such floor support is a key element in an effective criticality safety program. Each criticality safety engineer should emphasize how to make criticality safety controls clear and user friendly to operations personnel.

Table 1. Survey of Major Contributing Causes for 22 Process Criticality Accidents

	Unfavorable Geometry Vessels	Human Failure	Design/Process Equipment Failure
Mayak (15-03-53)	X	X	
Mayak (21-04-57)	X	X	
Mayak (02-05-58)	X	X	
Y-12 (16-06-58)	X	X	X
LASL (30-12-58	X		X
ICPP (16-10-59)	X	X	
Mayak (05-12-60)	X	X	
ICPP (25-01-61)	X	X	
Tomsk (14-7-61)	X	X	
Hanford (07-04-62)	X	X	
Mayak (07-09-62)	X	X	
Tomsk (30-01-63	X	X	
Tomsk (02-12-63)	X		X
Wood River (24-07-64)	X	X	
Electrostal (03-11-65)	X	X	
Mayak (16-12-65)	X	X	
Mayk (10-12-68)	X	X	X
Windscale (24-08-70)	X		X
ICPP (17-10-78)	X	X	X
Tomsk (13-12-78)		X	
Novesibirsk (15-5-97)			X
Tokai-Mura (30-09-99)	X	X	

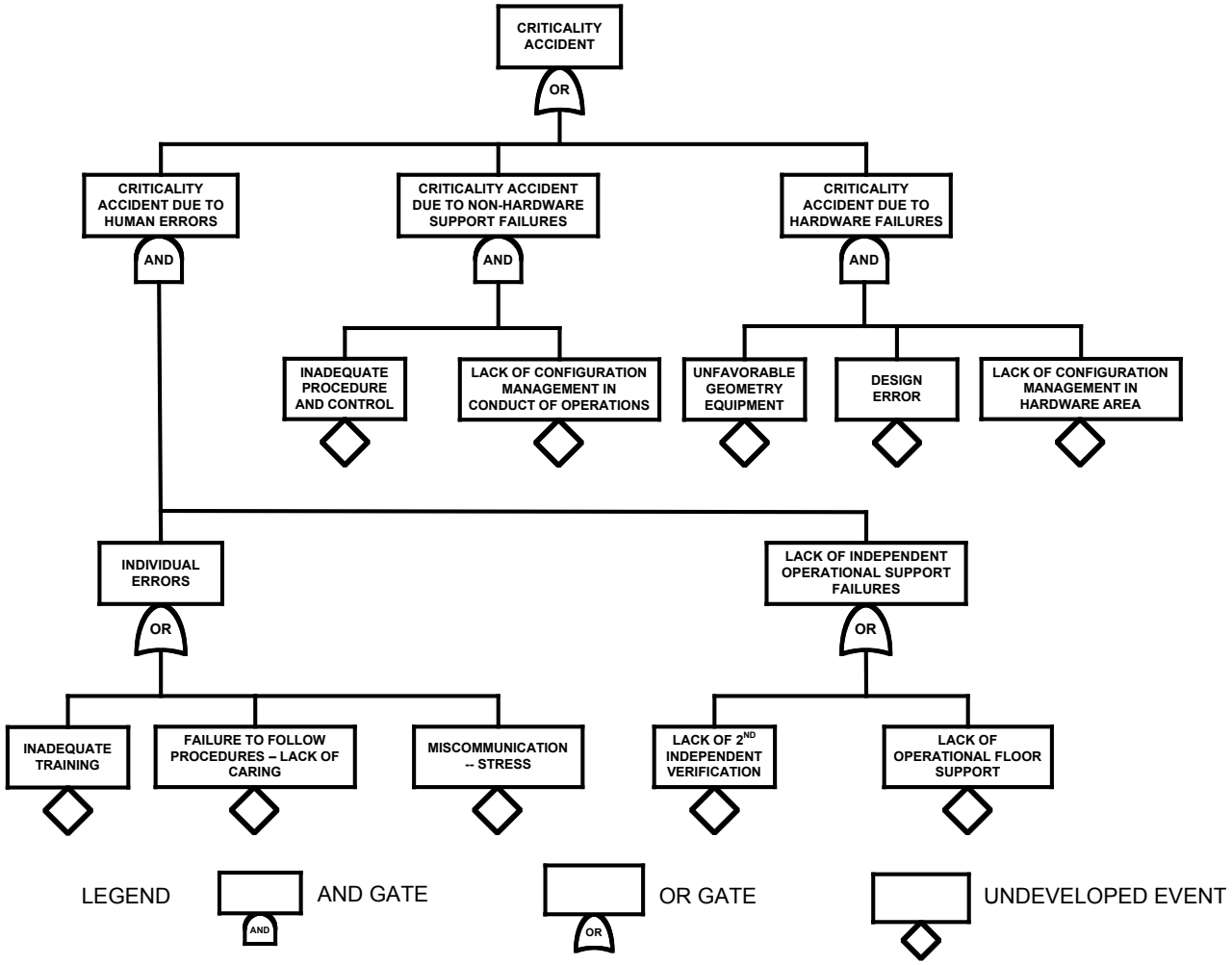

Figure 1 – A Fault Tree for Relative Assessment

4 CONCLUSIONS

By applying a fault tree model to identify the major contributors of criticality accidents, a total risk picture is obtained to address relative merits of various actions. Historically, human failure has been identified to be one of the key culprits in causing criticality accidents. Factors such as failure to follow procedure, lack of training, no independent verification means, and no expert support at the floor level are main contributors to human errors. Other causes may include inadequate procedures/controls, hardware failures, and others. However, not all of the causes are equally important in contributing to criticality mishaps. Applying the limited resources to address the major causes of criticality accidents, rather than applying those resources on the minor contributors, would be more significant in reducing the overall risk. For example, more emphasis should be placed on the enhancement of operation floor support to minimize the operator errors. All the major stakeholders should examine their actions from a total risk perspective. Misuse of resources by addressing lesser causes of criticality accidents rather than addressing major causes of criticality accidents is not risk free without severe consequences. Directing available limited criticality support resources according to the total risk concept should be a valuable guidance for all major stakeholders of criticality safety to enhance the safety of nuclear facilities. More research on the human error issues and more development and acquisition of the human error database for criticality operations are highly recommended.

5 ACKNOWLEDGMENTS

This work was performed under the auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.

6 REFERENCES

1. T.P. McLaughlin et al, “A Review of Criticality Accidents’, LA-13638, National Technical Information Service, Springfield, VA 22616, May, 2000.
2. R.C. Lloyd, E.D. Clayton, and R.D. Carter, “Criticality Safety Assessment, “ *Transaction American Nuclear Society*, **27,** pp.404 (1977).
3. R.C. Lloyd, SW. Heaberlin, E.D. Clayton and R.D. Carter, “Assessment of Criticality Safety”, *Nuclear Technology*, **42**, January 1979.