The Control of Prompt Radiation Hazards at Accelerator Facilities

Committee on the Accelerator Safety Order and Guidance

S. Musolino (BNL)
S. Rokni (SLAC)
G. Stapleton (TJNAF) chairman
M. Torres (ANL)
O. van Dyck (LANL)
K. Vaziri (FERMILAB)

Foreword

Recently some interest has been aroused over the early draft of a document written by a sub-committee from the Accelerator Section of the Health Physics Society entitled: The Control of Prompt Radiation Hazards at Accelerator Facilities. This article picks out some of the salient pieces of that draft to show the thinking of the authors and the possible shape of the revised document.

1.0 Introduction

The early draft was a written response to a hazard classification scheme set out in the guidance notes to the US Department of Energy Orders for the safety of accelerators (USDOE 1993). The concern of the accelerator community was that the DOE scheme discounted the use of integrated safety systems including those that would rapidly terminate the beam in the event of unplanned beam loss. The early draft document was produced by a working group commissioned by the Committee on the Accelerator Safety Order and Guidance (CASOG), an ad hoc committee of the Accelerator Section of the Health Physics Society which was set up in 1994 by the Section's President, N. Ipe. The draft report was presented to the Accelerator Section at the HPS Annual Meeting in 1995.

Subsequently, the DOE Accelerator Safety Order requirement for hazard classification was removed and, changes were begun in the manner some accelerator laboratories would be regulated, namely, the Necessary and Sufficient process (USDOE 1994a) was initiated. These developments to some extent overtook the need for the revised hazard classification scheme which was originally set out in the CASOG draft document so that work on producing a final report lapsed. However, many members of the Accelerator Section thought that the report contained useful information and would be of general value in stating the philosophy that already exists in the accelerator community with respect to the control of prompt radiation. Thus, at a meeting of the Accelerator Section in San Jose CA, January 1997, it was agreed that the draft CASOG paper on the control of prompt radiation hazards at accelerator facilities should be revised for publication.

Interest in the topic was also sustained by continued contact within CASOG on changes in the regulatory system and by two papers published by a group member evolving from the draft report. The papers (van Dyck 1996, 1997) explored the conceptual difficulty with applying a "hazard-based" safety oversight system to accelerators and argued for "risk-based" oversight. These papers contributed greatly to sustaining interest and convincing the accelerator community that the preparation of this particular document would be a worthwhile objective.

The first of the two papers mentioned above explored the conceptual difficulties that the current DOE's hazard-based regulatory framework and safety oversight system places on accelerators. Specifically, for large and complex accelerator facilities, determining the worst-case accident scenarios can be an endless exercise with little payoff seen in real safety. Probably everyone would be satisfied with risk-based management, if rational evaluation of risk were feasible. Without such an evaluation, facilities appear to be driven by DOE requirements and guidance to investment in a total shielding encasement at huge expense and little benefit. These discussions often end with the questions: how much risk is acceptable, and how can risk be quantified? Seeking possible answers to these questions is the goal of the final report. Although the work was initiated within the perspective of DOE funded facilities, it is hoped that the content will be of value to all accelerator facilities both national and international

An early approach to the management of risk is exemplified in the now withdrawn USDOE Orders on Safety Analysis and Review System (USDOE 1981 & 1986) where a risk matrix was adopted. This scheme used a combination of consequence and probability to characterize the risk of a hazard in the matrix format of Table 1. The system is of course applicable to any kind of accident and not specifically related to any radiological "event", although the hazard considered in the DOE Order was directed towards inventories of nuclear materials.

Table 1. Risk Matrix (Adapted from DOE-AL-5481.1b 1988)

	Probability Per Year			
CONSEQUENCE May Cause. . .	A-Likely > 1E-2	B-Unlikely < 1E-2	C-Extremely Unlikely < 1E-4	D-Incredible < 1E-6
I-Catastrophic Deaths, or loss of the facility/operation, or severe impact on the environment.	Unacceptable	Unacceptable	Marginally Acceptable	Acceptable
II-Critical Severe injury or death to a worker, or severe occupational illness, or major damage to a facility/operation, or major impact on the environment.	Unacceptable	Marginally Acceptable	Acceptable	Acceptable
III-Marginal Minor injury, or minor occupational illness, or minor impact on the environment, or moderate damage/impact to a facility/operation.	Marginally Acceptable	Acceptable	Acceptable	Acceptable
IV-Negligible No significant injury, occupational illness, or significant impact on the environment.	Acceptable	Acceptable	Acceptable	Acceptable

Perhaps the final difficulty CASOG saw was the notion that a rational regulatory system could be built on well-defined boundaries in consequence and probability, as in Table 1, based on subjective criteria, particularly non-fatal consequences which are much less frequent in irradiation incidents.

1.1 Radiation Protection Practices

In addition to specifying adequate shielding, it is a common practice at accelerator laboratories to implement other systems of radiation safety. Examples are: administrative systems such as search and secure procedures in conjunction with key-tree type access control, the use of electrical or other types of contacts on entry doors and beam line stoppers connected to the safety interlock chain in addition to the normal engineered beam-safety devices. All these systems together provide adequate safety to personnel by preventing occupancy or access during beam-on conditions and likewise preventing errant beams from entering occupied areas.

To safeguard them from costly damage, accelerators require a system of machine protection devices that are generally not included in any scheme of personnel safety. The reason for this is not that such systems are inherently less well engineered than those on personnel safety systems it is because such systems are essentially "open" to the accelerator operations crew to adjust or use in the most efficient way, nevertheless in the context of an overall integrated approach such machine protection devices have an important role in reducing the number of challenges to the personnel safety system and hence, enhancing the overall reliability of the personnel devices.

Traditionally, the systematic approach to safety at research accelerators has not relied on any single element for the safety of personnel or protection of the machine. A high level of protection has been achieved through integration of systems including shielding, automatically-responding systems, and human response. These various elements provide the "defense-in-depth" approach that has been successful in accelerator, nuclear power and other industrial safety systems. Failure of one barrier or element will not result in complete loss of protection. The combined system, through redundancy and technical diversity, minimizes the risk due to total failure.

2.0 Risk-based Standards

It is important to state that the safety systems we are concerned with in this note are primarily used for the protection of people against prompt radiation. Thus any failure of such a safety system could potentially result in some radiation exposure. However, not every safety system failure would result in an exposure. The failure might not occur during a challenge to the safety system, i.e., the fault might occur when the accelerator is running safely or the safety system could fail when challenged but no-one might be present in any exposed location. Thus there are many variables to take into account when assigning an appropriate level of reliability required.

In addition it is important to understand the level of radiation insult that might occur on any system failure. Potential maximum exposures of a few rem should not require the elaborate and expensive systems that would be appropriate where the insult could be radiation exposure at the hundreds of rem level. This assessment of the consequences of system failure requires considerable understanding of the accelerator operational parameters, because estimates must be made of the instantaneous dose rate that might occur under given beam loss condition, and how long the fault condition could be expected to be sustained.

Because of the extensive role of judgment by the accelerator designers, operators and radiation safety specialists, we believe that it is inappropriate to attempt to impose any arbitrary regulatory limits for any of these accelerator performance variables, whether dose rate or integrated time of exposure or even the probability of failure of any safety system. It is, however, important to provide a method that can assign a level of reliability to the various safety systems so that credit can be taken for each contribution to the overall combination.

2.1 Comparability with "Safe" Industries

A rational basis for evaluation and regulation of risk from prompt radiation accidents is by comparison to mortality rates in safe industry. It is highly appropriate, because we are considering radiation insult, to consider the opinion of the International Commission on Radiological Protection, which "...believes that for the foreseeable future a valid method of judging the acceptability of the level of risk in radiation work is by comparing this risk with that for other occupations recognized as having high standards of safety, which are generally considered to be those in which the average annual mortality due to occupational hazards does not exceed 1E-4", (ICRP 1977a).

Using this premise the Commission set a stochastic whole body limit for occupational practices at 5 rem per year. The Commission used the argument that the distribution of annual dose equivalents among a large group of workers had been shown to commonly fit a log normal distribution having an arithmetic mean of a tenth the limit with very few values approaching the limit. Thus, the Commission argued that the average risk in radiation occupations is comparable with the average risk in other safe industries (ICRP 1977b). The numerical value of a dose limit and the assumptions that go into deriving it are not critical here; the point is that the development of the limit starts from acceptance of a "safe industry standard" of a small but finite annual occupational mortality expectation.

Twenty years after the value was put forth by the ICRP in 1977, a suitable goal for USDOE occupational fatalities, exclusive of transportation and construction activities, might be fewer than one per 100,000 worker-years. It is of interest that non-fatal effects (injury) represent a large fraction of the cost of accidents. However, ICRP indicated that non-fatal effects from radiation are much less frequent than non-fatal effects encountered in other safe occupations, and hence the inclusion of non-fatal effects would result in less restrictive dose limits. Therefore, as a first approximation, an assessment based on mortality can be considered conservative.

The estimates of average annual beam loss and the assumptions for temporally and spatially averaging source terms are statistical; the notion that certain regions close to shield walls may or may not be occupied during the period when the machine is operational is clearly understood to result in average doses less than the design goal in a way somewhat analogous to the idea of setting a 5 rem annual whole body limit on exposure on the basis that average exposure results in one tenth this value. Finally the ultimate result of radiation exposure is assumed to be stochastic.

Thus we conclude that the use of all radiation protection systems for accelerators is based on probability and that even the notion that shielding can be inadequate or that shielding calculations are inaccurate, is implicitly included in the common practice of adding factors of safety by, for example, adding an extra foot or so of concrete. However, it is acknowledged that because the function of structural protection systems such as shielding or distance is very simple to grasp, they are often erroneously regarded in a different light from electrically or mechanically engineered systems that usually depend on a response to some "event" such as a misdirected beam or a gate opening. Because of their apparent complexity it is necessary for engineers who design them to have a clear understanding of the reliability standards to which they should design. Hence we have to make suppositions about what could happen should such "response" type devices fail to function as designed, although similar suppositions could be made with equal validity about failure of structural systems should we desire to do so.

2.2 Accidents Resulting in Mortality from Acute Effects

At most large accelerators, workers routinely occupy beam areas while beam is on in nearby beamlines. Interlocked systems are used to prevent beam delivery to the occupied area. However, it must be acknowledged that there is a finite probability of hardware failure, or failure to evacuate the area prior to starting beam delivery, in either case exposing personnel in the area. The consequence of such an accident could result in death from acute radiation syndrome. In this extreme case no credit can be taken for the stochastic nature of low level radiation exposure.

Five DOE accelerators have been operating for more than two decades with ~100 radiation workers per site routinely exposed to the radiation hazards of beam tunnel entries, with no fatalities (or to our knowledge even severe overexposures), thus indicating on the order of < one fatality per 10,000 worker-years. These facilities generally have similar procedures and safety systems, including redundant interlock chains, as reflected in (SLAC 1988). Redundant safety systems are also common for critical applications in industrial, commercial, and consumer safety, such as with motor vehicle brakes, helping to keep equipment-caused accidental deaths a very small fraction of the risks of ordinary life. Thus reliability of interlocks used to prevent direct beam exposure sets the standard for reliability of systems used to prevent exposure to less-than-lethal doses of radiation.

2.3 Accidents Resulting in Stochastic Effects

As we discussed above, a suitable standard for accelerator safety systems should be based on an overall fatality rate of 1E-5 per worker-year. Furthermore, assuming that the average radiation worker is exposed less than 10% of the time on-site, this will then imply a negligible individual risk of 1E-6 per year. Non-radiation workers at the accelerator facility might be expected to be exposed at the 1% level with a consequential mortality risk at even lower levels.

Although very high doses can result in death, one would expect that most radiation accidents - at least those outside beam tunnels - would result in less-than-lethal doses for which the long-term health effect is stochastic with risk of mortality 1E-4 per rem (ICRP 1977c; linear model). Therefore, for an accidental exposure, under fault conditions of a few 10's of rem the system failure rate need only be ~1E-3 per year to achieve comparability with overall mortality rates in safe industries. It is interesting that a much higher occupational risk at the level of one fatality per century (~1E-2) from stochastic effects is already implicitly accepted by allowing the DOE accelerator complex to accumulate ~100 man-rem collective dose each year - again using the linear model. For members of the public, who can be assumed exposed 100% of the time, mortality risk would be acceptable at the 1E-6 per year level. Because the estimated annual mortality is predicated on both the reliability of the safety system and the level of radiation exposure, and on the assumption that the amount of radiation exposure to the off-site general public from accelerators is not likely to be greater than a few 10's of millirem, the 1E-6 per year level can still be sustained at the 1E-3 failure probability.

2.4 General Approach to Determine the Required Reliability of Safety Systems

Accepting the premise that radiation exposure results in a risk of mortality and that failure of a protection system is also stochastic, we can equate the probability of mortality with the product of the reliability of the system and the level of radiation insult, should the safety system fail. This is a very simple concept but adequate for our purpose of screening the levels of reliability we must expect from our equipment:

annual probability of mortality (R) =
reliability of system (P) x radiation dose (H) x risk coeff (F)

In this equation, P is the probability of failure of the safety system and the product H x F is an estimate of the potential radiation insult.

It can be seen that for a large potential radiation dose we require higher reliability devices justifying the higher cost of development and verification. In the derivation of the reliability of the devices we need to include estimates of the likelihood of the system of devices being challenged by an errant beam, and an estimate of the probability of a failure of the system of devices resulting in personnel exposure. It should be emphasized that the probability P results from the combination of many system conditions such as the duplication or multiplicity of interlock chains and devices, the length of time during which the system is required to function properly, etc.

The highest level of protection needed at most facilities is for beam area occupancy, and Section 2.1 presented a mean time between failure (MTF) of 1E-5 worker-years as the standard. Depending upon the dose level anticipated in the exclusion areas (outside the shielding and/or barriers), a shorter MTF, lower by one or more orders of magnitude, can be accepted.

3.0 Assessing Reliability of Safety Systems

Given enough information about the reliability of its elements, the reliability of a system can be predicted. The mathematical foundation is well-established (Martz 1991) and there are established processes to use, including tables and computer programs. The approach becomes difficult and perhaps not very meaningful to apply starting from the circuit-level of detail with systems as complex and unique as the interlocks at a large accelerator. However, these concepts can be useful in comparing or optimizing simple combinations of system building blocks.

Testing and documentation can establish an upper limit on the length of time a subsystem in service was unavailable to respond safely, or the number of times a subsystem failed to respond safely. This can provide an empirical basis for estimating the unavailability of combinations of systems. It could be practical to accumulate data in a few years which might help support a claim of unavailability (fractional time out of service) at the 1E-3 to 1E-4 level for redundant systems, but the analysis is highly dependent upon knowledge of common-cause or correlated failure modes.

Two DOE-sponsored reports (Mahn 1995, Neogy 1996) gave reliability ranges for safety systems classified by level of redundancy and technological diversity. For example, a dual nondiverse interlock chain (two identical strings) is shown in Mahn's Table 7 with a demand/failure ratio of 200 to 20,000. In other words, at the low end, it is expected to fail once per 200 demands. A dual fully diverse system is shown as fifty times more reliable. Again, based on these criteria, it is not difficult to reach the reliability required to protect personnel outside exclusion areas. If the dual-diverse system meets whatever quality requirement necessary to achieve the high end of the scale, it is adequate for personnel safety inside beam delivery areas even with very high hazards. Accelerator experience may indicate that these numbers are reasonably conservative.

The reports gave many qualifications on the context for the estimates and references to the quality standards that provide the claimed reliability levels.

3.1 Standards

The preceding discussion in Section 3.0 has shown that solid and quantitative predictive evaluation of safety is very difficult. However, DOE accelerators have accumulated thousands of man-years of relatively safe operation using a somewhat standardized approach (SLAC 1988). Within this envelope of recognized community standards, the facilities continue inventive development of instruments and systems suited to their requirements.

In Section 2.1 we introduced the notion of comparability with "safe" industry as providing an underlying basis for determining the required levels of reliability of safety systems. This notion can also be sustained at the more practical level by comparing the standards and systems used in such everyday hazards of living such as elevators, railway trains, electrical appliances, electrical enclosures, power lines, security vaults, fire alarms and sprinkler systems, etc.

We believe that adequate safety for prompt radiation is best found by staying within the envelope of good practices developed over the last half-century in the accelerator community. These practices are similar to the measures used to manage risk in other areas of life.

We encourage further development of standards embodying these good practices, so that continual revisiting of the issue of quantification of risk can be avoided.

4.0 Conclusions

We argue that no safety system is totally free from risk. We show that, by utilizing a simple concept, the level of reliability needed for safety systems used to control exposures of differing severity can be estimated. The simple concept used is based on the mortality rates in safe industries and the stochastic risk factors for radiation exposure. It is stressed that while the methods proposed result in numerical estimates, these numbers must not be regarded as prescriptive in any way. They cannot replace the judgment and knowledge of an experienced accelerator radiation safety expert. We hope to achieve a means of demonstrating that regulatory prescriptions of excessively small failure probabilities at the system or device level are not necessary or appropriate for accelerators in achieving the safety standards acceptable in safe industries.

Acknowledgments

Many people contributed to the discussions which helped to produce this report, in particular the CASOG sub-committee would like to acknowledge the advice and encouragement of Robert Youngblood, who very kindly read the earlier drafts and made many helpful suggestions.

References

ICRP 1977a; "Recommendations of the International Commission on Radiological Protection", Annals of the ICRP, ICRP Publication 26, Volume 1 No 3 page 19 sect 96 1977, Pergamon Press, New York (1977).

ICRP 1977b; "Recommendations of the International Commission on Radiological Protection", Annals of the ICRP, ICRP Publication 26, Volume 1 No 3 page 20 sect 99-100 1977, Pergamon Press, New York (1977).

ICRP 1977c; "Recommendations of the International Commission on Radiological Protection", Annals of the ICRP, ICRP Publication 26, Volume 1 No 3 page 12 sect 60 1977, Pergamon Press, New York (1977).

Mahn 1995: Mahn, J.A., Hannaman, G.W, and Kryska, P.M, "Qualitative Methods for Assessing Risk", Sandia Report SAND95-0320 (Sandia National Laboratories, Albuquerque, April 1995).
See http://infoserve.library.sandia.gov/sd950320.pdf.

Martz 1991; Martz, H.F. and Waller, R.A, "Bayesian Reliability Analysis", (Krieger, Malabar, FL 1991).

Neogy 1996: Neogy, Hanson, & Davis (BNL), Letter Report DOE-EH 33 8/30/96

NRC 1989; "Procedures for Treating Common Cause Failures in Safety and Reliability Studies - Analytical Background and Techniques", NUREG/CR-4780, EPRI NP-5613 Vol 2. US Department of Commerce National Technical Information Service (1989)

SLAC 1988, "Health Physics Manual of Good Practices for Accelerator Facilities", SLAC Report 327, Stanford Linear Accelerator Center, April (1988).

USDOE 1981 & 1986,* U.S. Department of Energy, Safety Analysis and Review System, 5481.1A, (1981) & updated 5481.1B (1986).

USDOE 1988*, U.S. Department of Energy, Safety Analysis and Review System, AL5481.1B, Albuquerque Operations Office, January 27 (1988).

USDOE 1993*, U.S. Department of Energy, Safety of Accelerator Facilities, 5480.25, (1993).

USDOE 1994a*, U.S. Department of Energy, Criteria for the Department's Standards Program, DOE/EH/-0416, Office of Environment Safety and Health, (August 1994).

van Dyck 1996; O. van Dyck; Trends in Prompt Radiation Risk Management at DOE Accelerator Facilities. Proceedings of the Fourteenth

International Conference on the Application of Accelerators in Research and Industry [CAARI 96], AIP Conference Proceedings (in press).

van Dyck 1997; O. van Dyck; Radiation Risk Management at DOE Accelerators, in Health Physics of Radiation-Generating Machines, p. 81 (Proceedings of the 30th Midyear Topical Meeting of the Health Physics Society, January, 1997).

*Available via http://www.explorer.doe.gov:1776/htmls/directives.html. The Guidance and Interpretations are available only via http://www.er.doe.gov/production/esh/accelr8r.html, which also provides link to the Orders.]