CONF-960409--2

LA-UR- 96-443

Title: BEAM-LIMITING AND RADIATION-LIMITING INTERLOCKS

RECEIVED
APR 01 1996
OSTI

Author(s): R. J. Macek

Submitted to: Radiation Protection, Vienna, Austria, April 1996

Los Alamos
NATIONAL LABORATORY

Beam-Limiting and Radiation-Limiting Interlocks

Robert J. Macek
AOT-DO
Los Alamos National Laboratory (LANL)
Los Alamos, NM 87545, USA

ABSTRACT

This paper reviews several aspects of beam-limiting and radiation-limiting interlocks used for personnel protection at high-intensity accelerators. It is based heavily on the experience at the Los Alamos Neutron Science Center (LANSCE) where instrumentation-based protection is used extensively. Topics include the need for "active" protection systems, system requirements, design criteria, and means of achieving and assessing acceptable reliability. The experience with several specific devices (ion chamber-based beam loss interlock, beam current limiter interlock, and neutron radiation interlock) designed and/or deployed to these requirements and criteria is evaluated.

INTRODUCTION

The title of this paper refers to active, engineered radiation-safety systems consisting of electronic devices which sense errant beam conditions or excessive prompt radiation and then command other devices to automatically limit or shut off the beam current. Such systems are increasingly used at a number of US accelerator Laboratories to mitigate potential prompt radiation accident scenarios. A number of factors motivate this practice including, most importantly, the cost of additional shielding but also the need to protect accelerator components from beam-induced damage and even to prevent potential failure modes of the fixed shielding. This paper will only be concerned with systems intended for personnel protection.

Common situations where instrumentation-based radiation-safety systems become an important option include: 1) changes in radiation safety standards, 2) upgrades that significantly increase beam power to an area, and 3) configurations where certain equipment or procedural failures can send high intensity beam to an area that normally receives low intensity beam.

At one time, it was considered adequate to design shielding to meet regulatory dose management limits for source terms corresponding to the highest beam losses expected to be encountered during normal operating conditions. There was less concern with what could happen under abnormal or accident conditions. Indeed, when the assumed source term was a local loss of the order 0.1 - 1% of the maximum normal operating beam power, then the worst case accident, a full-power spill, would not be life threatening even if the accident lasted as long as hour or so. In this case, the shielding would still limit the radiation fields on the outside of the shielding to less than 10 mSv/h (1 rem/h) for a full power spill (assuming that the shielding was designed to give 10 μSv/h for a 0.1% local spill). While radiation fields at this level are a serious matter, they will not lead to a life-threatening dose if the exposure time is an hour or so.

Modern high-powered accelerators and beam lines, such as those that serve the meson factories or spallation neutron sources, are designed and operated with maximum allowable losses of 10^{-6}/m or less over much of their extent. If shielded only for normal or expected losses, the accelerator has an accident potential that is now a much greater since a full power local spill could produce radiation fields of 10Sv/h (1000 rem/h) or greater outside the shielding. Life-threatening doses could be incurred if the spill lasts an hour or so. In these circumstances, instrumentation-based protection systems offer the promise of accident mitigation.

Even if the shielding for the initial accelerator capability was adequate for full-power spills, improvements and upgrades of accelerator beam power are the norm and create the potential for higher radiation fields under abnormal conditions. Shielding retrofits are frequently much more difficult and costly than the same shielding augmentation at the time of initial construction at a "green field" site. Here as well, active systems offer a possible solution.

From the beginning, LAMPF (now LANSCE) used automatic beam-loss limiting instrumentation to protect the accelerator from damage and keep activation low enough for hands-on-maintenance. The construction of the proton storage ring (PSR) required a high-intensity H^- ion source which was also used to provide highly chopped beam for a fast-neutron facility, WNR. With these new facilities came the capability for new errant beam situations where high intensity beams could appear in beam lines which normally saw much lower beam intensity. The same instrumentation used at LAMPF to limit activation was also used in these new facilities and was thought to be adequate for limiting loss in accident situations as well. Critical examination of these issues lead to the development of a more reliable system of beam limiting devices suitable for personnel protection. Retrofits to the shielding were still implemented where possible in the areas of greatest concern (1).

Each of the situations enumerated earlier have been encountered at LANSCE. Extensive use has been made of improved beam-limiting and radiation-limiting interlocks to reduce the probability of large doses in severe accident scenarios. The first preference was for shielding or physical barriers rather than instrumentation. However, in some situations we found that shielding retrofits sufficient to deal with the accident potential by shielding alone were very expensive or practically impossible to implement without a major rebuild of the facility. For these situations, there was no acceptable alternative other than greater use of active protection systems.

SYSTEM REQUIREMENTS AND DESIGN CRITERIA

Acceptance of beam-limiting and radiation-limiting interlocks for personnel protection, especially as a substitute for additional shielding, depends upon making the case that the interlocks will reliably prevent **any** unacceptably large beam spills. The system requirements and design criteria that further this goal are discussed below.

A. Ultra-High Reliability

A key issue in the acceptance of active safety systems is the achievement and demonstration of ultra-high reliability or equivalently, ultra-low failure rates for these systems to perform their safety function. Consensus on a single, suitable criterion for the reliability required of "active" protection systems has not been achieved. A frequently sought goal is that failure of the overall protection system leading to death or serious injury should be "incredible", which is often taken to be a failure rate of less than once in a million years. Demonstration of such low failure rates by direct observation is obviously out of the question. Rigorous proof through analysis and computation is also elusive. However, probabilistic analysis and assessment does have value as will be discussed later.

In a graded approach, reliability requirements and potential consequences of a system's failure to mitigate worst-case accident scenarios would be correlated such that higher reliability is required for the more serious consequences. Quantification of the relationship is another elusive goal because it is fundamentally a judgment of acceptable risk. In practice, one is driven to provide the most reliable system possible within a budget.

In lieu of numerical reliability specifications which can not be demonstrated by direct measurement, deterministic features or processes can be specified which are known to make positive contributions to reliability and which can be evaluated without much ambiguity. Included would be such features as redundancy, testability, fail-safe characteristics, and rigorous quality standards.

B. Criterion for "Fail-Safe" Operation

Fail-safe operation of the protection systems is a feature often required or sought after for engineered safety systems. In practice, no system can be shown to be truly fail-safe with respect to all possible failure modes. A definition or criterion that appears feasible in practice is to use the term "fail-safe" for systems which fail safe with respect to any single-point failure. At Los Alamos, this concept was pioneered by Andrew Browman and employed in the design of the both the beam loss interlock and beam current limiter interlock which are now part of the radiation security system (RSS). To be more specific, the criterion used was that any single point hardware failure will have one of three outcomes: the device continues to perform its protection function, or the device shuts off the beam and holds it off until the fault/failure is corrected, or the gain changes by less than some specified tolerance (20% was chosen the beam loss interlock) and the device continues to perform its protection function at the changed sensitivity. This definition of the term fail-safe will be used through out the rest of this paper.

Some techniques used to achieve fail-safe design include:

- Use of redundancy within a module,
- Continuous self-checking,
- Continuous monitoring of power supply voltages or other critical parameters.

To follow the fail-safe concept to its logical conclusion, one should also consider single-point human failures in design, construction, testing, operation and maintenance. However, this is rather difficult to do with completeness. Redundancy in the form of independent verification of construction, modifications, maintenance and testing is often used to minimize "single-point" human/administrative failures.

C. Redundancy

Redundancy is used extensively to improve reliability and avoid single-point failures. It primarily improves reliability and availability with respect to uncorrelated failure modes or events. The main weakness is common cause failures which reduce simultaneous multiple failures to an equivalent single point failure mode or event. Some examples of correlated or common cause failures are aging and wear-out phenomena, common environmental changes (such as temperature, humidity, dust, vibration, radiation damage, etc.), lightening induced failures, mechanical crushing from a single event, and design flaws in redundant systems employing identical units. The use of different physical principles or different technologies in the redundant devices is helpful in reducing common cause failure modes.

D. Complete Coverage by Radiation Detector Interlocks

To be most effective, the interlock system should be capable of detecting any unacceptable beam losses no matter where it occurs. In this context, unacceptable beam losses are those that can lead to unacceptable radiation exposure in areas where occupancy is not prevented by physical barriers. Therefore, sufficient devices are deployed in such a way that unacceptable beam loss at any point in the beam acceleration, transport or beam handling systems is detected at the required or specified minimum sensitivity (or at greater sensitivity). Mere sampling is not sufficient.

E. Required Dynamic Range

To provide protection against the full range of possible accident scenarios it is necessary that the overall system have a dynamic range that covers all possibilities from the minimum required sensitivity in normal operations to the maximum possible dose/dose rate that can be delivered under full- power beam spill accident scenarios.

F. Testability/Verifiability

Frequent testing is a well-known technique for improving device availability and one that the system design should facilitate. It should be possible to easily verify or test for proper functioning all essential safety features of the device while it is in place. Where redundancy is used to achieve fail-safe operation with respect to single-point failure modes, it is crucial to find and correct any single-point failures in redundant components shortly after they occur since such units or sub-systems no longer satisfy the fail-safe criteria (at least in the case of two-fold redundancy).

G. Acceptable False-Alarm Rate

Frequent false alarms discredit a device with operators. At some frequency of false alarms the device will be ignored or taken out of service even if the false alarms are fail-safe. In my experience, false alarms at the rate of one/month of operation are tolerable; once per week is not.

H. Isolation and Tamper Resistance

Safety-critical systems should be made resistant to inadvertent or willful tampering with components that are essential to the safety function. One reason for isolation of safety systems from other interlock or instrumentation systems is to avoid inadvertent compromise of the safety features; another is that isolation makes it easier to lock off the safety system components, and junction boxes and wiring plant.

I. Beam Plugs and Reliable Beam Shut Off

The active protection system is only as reliable as its weakest link. Care must be taken to ensure that the detection of an errant beam or excessive radiation condition results in a command that is reliably transmitted to a sound and reliable beam shut off system. Electronic beam deflectors will quickly shut off the beam, but, they should be backed up by fail-safe beam plugs. These would be beam stoppers that can take the full power of the beam indefinitely or else create a passive shutdown of the accelerator before the beam burns through the plug. The later feature is implemented for the fusible beam plugs used at LANSCE. The fusible beam plug is an idea picked up from SLAC. The face of the beam plug is a fairly thin metal window (the fuse) covering a cavity filled with air and connected by tubes to the atmosphere. If high power beam strikes the window it causes the window to melt and let air into the accelerator before the body of the plug can melt. The air is sufficient to ruin the vacuum and stop acceleration without destroying the accelerator.

J. Quality Control

Rigorous quality assurance and quality control standards for critical safety systems components, wiring plant, design, construction, installation, testing, maintenance, training, certification and documentation are needed to ensure that the design policies, principles and criteria are properly implemented. Quality standards approaching those used for critical safety systems in the nuclear industry are recommended.

SOME EXAMPLES

The concepts and principles discussed above have been applied to the very challenging situation at LANSCE. The aim was to have a redundant, three-layered, “defense in depth” where each layer employed a different technology so as to minimize common mode failures. The first layer was a system of fail-safe beam loss interlocks based on ion chamber detectors placed in the beam tunnels. The second layer employed fail-safe beam current limiters to prevent excess beam currents in critical areas. The third layer consisted of neutron radiation detector interlocks outside the shielding deployed to enforce limits on the maximum neutron radiation levels in occupied areas. The fail-safe ion chambers and the current limiter were developed specifically to meet these criteria for the Line D facilities at LANSCE and have since been used at other LANSCE facilities. The well known “Albatross” was used as the detector for the third layer. While it was modified to satisfy some of the criteria listed earlier, it proved to be not as robust and reliable as the other two.

A. Beam-Loss Interlocks

Ion-chamber based interlocks are used at several leading US accelerator laboratories. At LANSCE, the ion-chamber based, beam-loss interlock is referred to as the errant beam detector. Errant beams are detected by the radiation generated from beam losses somewhere in the vicinity of the detector. The unique features introduced to make it fail-safe and suitable as a safety interlock are discussed here. For details and other features refer to reference (2).

The ion chamber is filled with nitrogen gas at 1 std. atmosphere, so that if it leaks, the pressure will drop to about 0.75 std. atmosphere. (local atmospheric pressure), and remain mostly nitrogen. After a leak it will still function as a satisfactory ion chamber, albeit with a somewhat lower gain but still within the 20% tolerance.

The signal from the ion chamber is converted to a voltage and presented to two redundant processing channels. Fail-safe operation is achieved by self-checking the common portion and by redundancy in the rest of the unit. Continuous self-testing is implemented using a background current generated by a resistor assembly between the HV and signal electrodes. A fault signal is generated if the ion chamber current is not greater than 80% of the design value for the background current. This checks that the chamber HV has not dropped by more than 20% and checks continuity of the signal cable and HV cable. A fault signal due to excessive beam spill is generated when the ion chamber current (background + signal) is greater than the trip set point (background + threshold).

For those components that are not checked by the self-testing feature, redundancy is used to ensure that no single point failure is unsafe. The device has dual-redundant current sensing circuitry except for the analog input from the chamber (which is checked by the self-testing feature). Redundant fault outputs are supplied to the dual-line interlock system backbone to transmit the shut-off command to accelerator shut-off system. The design has been checked carefully to see that the following types of "single point" failures will be fail-safe: an open, short or significant change in value for resistors and capacitors; an open at any junction between two components; a short between any two junction points; a short between any junction point and ground; a short between any junction point and the power supply rails; and shorts between any number of pins on a single IC. Additional circuitry monitors power supply voltages and generates a fault signal if these are out of tolerance. On a complete loss of power the system will fault both channels.

A full suite of test functions are available via front panel switches. These are designed to test the full functionality of each leg of the redundant processing circuitry and are performed periodically. An overall test with a source placed on the detector is also perform periodically. Construction, bench testing, installation, repair, maintenance, operation and field testing are covered by documented and approved procedures (3-4).

The final level of redundancy within this layer is achieved by the deployment of extra detectors in the beam tunnel. A spill at any point in the tunnel is viewed by at least two detectors at a specified minimum sensitivity.

The response of this detector has been tested with beam over the full range of dose rates and spill conditions that could be encountered in service at LANSCE (5-6). At the very highest levels (~ 3 rads/pulse) with the short PSR pulse (200 nanosecond width), the response is non-linear but still monotonic. These tests did show the need to keep the threshold setting below the maximum available from the front panel adjustment (administrative control) in order to ensure that the device will always trip for any large spill regardless of pulse width and repetition rate. Administrative control of the threshold settings is also needed because the trip levels required for personnel protection vary with location depending on the configuration of the shielding and distance of the detector from the beam line.

We are convinced that this system now meets the criteria for being fail-safe in the limited sense defined in this paper. It was not easy, as is evidenced by that fact that the present version is Model III. Previous versions were found to have subtle flaws; some found by actual failures in the field, others by additional analysis of the design. Some forty units of Model III have been in service since 1992 with no "unsafe" failures i.e. no failures that were not fail-safe.

B. Beam Current Limiter Interlocks

Some beam facilities are designed or operated to take only a small fraction of the beam current that is possible from the accelerator. For these beam areas, errant beam conditions can include an unintended increase in the beam current directed to the facility. Here, a single device that detects excessive current can protect a large area.

A fail-safe beam current limiter based on a beam current transformer has been developed and implemented at LANSCE. The fail-safe feature is achieved by a combination of self-checking and redundancy. Self-checking is implemented using a test winding on the beam transformer toroid. The signal from the toroid is split and the signals sent to dual-redundant processing channels which present the fault status to the corresponding channels of the dual-redundant RSS "backbone". Faults are generated by failure of the self-checking circuitry or by excess beam current. Loss of power will fault both channels of the unit. The power supply voltages are also checked by the self-check circuitry. A calibrate winding is also installed though the toroid. It permits test signals to be injected to verify proper functioning of all critical features including the proper value of the trip point.

A reliability analysis of this device was performed by an experienced team of safety analysts from LANL in collaboration with the designers of the beam current limiter. It was part of a limited-scope, probabilistic safety analysis of selected safety systems at LAMPF (8).. An analysis of the beam current limiter was performed initially using failure modes and effects analysis and criticality tools to examine the system components and potential failure modes. This was followed by a fault tree analysis. The analysis provide estimates of system unavailability (ratio of average downtime to uptime in the time interval between testing) of 3.7×10^{-3} with an estimated error factor of 2.2. Annual testing and operation for half a year per year were assumed. These imply an estimated failure rate of 1.5×10^{-2}/y for unsafe failures.

Experience with the current limiters has been good. Several units have been in service since 1989 and there have been no unsafe failures. Experience has demonstrated its vulnerability to radiation damage. The electronics are placed near the toroid to minimize electrical noise. In one case a unit failed that was placed close to a beam stop, however, it failed safe and faulted until replaced. In another case, a unit faulted when exposed to a large radiation pulse produced by beam spill from an occasionally misfiring of the PSR extraction kickers. It always failed safe, but the rate of these false alarms was too high and the unit was withdrawn from service at this location.

There is set of circumstances or accident scenarios where the current limiter interlock will not provide the level of protection usually sought. The limiter operates by sensing the algebraic sum of currents passing through the toroid and does not sense neutral beams or equal mixtures of positive and negatively charged beam. This means it will not function as needed in situations where the beam is partially or totally neutralized. At LANSCE, where H^- beam is used, protection can be lost in accident scenarios where the beam is partially stripped either to H^0 or a neutralized mixture of H^-, H^0 and H^+ before passing through the toroid. Such stripping might be the result of poor vacuum or material that partially covers the beam.

C. Area Radiation Interlocks

An interlocked detector suitable for use outside of the shielding is also a challenging problem, particularly if it is to do double duty i.e. monitor routine levels and serve as an interlock to mitigate any and all prompt radiation accident scenarios. The albatross IV neutron detector was chosen at LANSCE for two reasons; it was designed for use at pulsed accelerators and it was already in routine use at this laboratory (8). It was modified to fail safely on power failures and a self-checking feature was added which required that the detector produce a minimum count rate from an internal gamma-ray source.

For a number of reasons, primarily limited resources and the over confidence that was a result of successful experience with it as a survey instrument, the design of this complex unit was not subjected to the same level of scrutiny as the two other instruments described above. In doing so an important limitation to the dynamic range was overlooked, but one that was pointed out in a subsequent safety review. The Geiger tubes in the unit were used in a counting mode and could "lock up" i.e. cease to count at all at high event rates just when the protection is needed most. The cure was to add current mode detection that is activated at high count rates so that the combination of detection modes covers the required dynamic range.

A radiation detector more suited to safety-interlock requirements is still needed. The Albatross was designed as a survey instrument not as an interlock. It is more complicated than desirable for the interlock function. Reliability has not been as high as with the other instruments. Failure rates in the LANSCE environment have been on the high side and there have been four failures that were not fail-safe. The unsafe failures were investigated and modifications made to prevent future occurrences. Reliability has improved since the last modifications. In the past two years, 40 units were in service and there have been no unsafe failures.

It should be noted that complete coverage outside the shielding is more difficult than in the beam tunnel primarily because the radiation distribution (from a local spill) coming through the shielding is more narrowly concentrated around the direction of the ray with the least number of attenuation lengths. Thus, the spacing of detectors needed for full coverage is reduced and the number required increases.

ASSESSMENT OF RELIABILITY

Demonstration of ultra-low failure rates is difficult. Direct measurement of such rates for a complete system is not practical. One has little choice but to rely on some type of analysis. The techniques of probabilistic risk assessment (PRA) used, for example, in the nuclear reactor industry constitute a well-developed methodology appropriate to this problem. The main thrust of this methodology has been applied to parts of the LANSCE radiation security interlock system (7,9). The reliability analysis of the beam current limiter discussed earlier is a good example. The analysis provides more than just an absolute estimate of failures rates. Once the model has been developed, it can be used to isolate the factors that make the greatest contribution to unreliability. One can also study the effect of changes to the design or to specific input parameters. Relative probabilities are often more accurate than absolute probabilities since common factors drop out of the ratio. Such analyses help to identify the most cost-effective measures for improving reliability, assuming that the costs of various changes can be estimated readily.

The complexity of probabilistic methods used in PRA is another barrier to acceptance of the conclusions. Those who must act on the results or conclusions often do not have the expertise to adequately judge the results. Peer-review of the study by PRA experts who do not have a vested interest in the outcome can help decision makers.

The operating experience with the 3 specific devices discussed above is reaching the stage where it provides useful data for assessment, perhaps even quantitative estimates, of device reliability. For example, over 100 device-years of service have been logged for the loss monitor device with no failures implying an upper bound on the failure rate in the neighborhood of 10^{-2}/y. Combining the device reliability estimates to produce a reliability estimate for the entire protection system is possible if one assumes statistical independence. The present data is inadequate to test that assumption in a straightforward way.

CONCLUSIONS

The use of instrumentation-driven, beam-limiting and radiation-limiting interlocks for radiation protection is on the increase at US accelerator laboratories. Most would agree that well-conceived and well engineered active protection systems can reduce the risks from prompt radiation accidents. The main debate centers over the extent to which these systems can be used to define the safety envelope for accelerator operations or, expressed in trade jargon, the amount of credit to give to these systems towards meeting safety goals. Acceptance of instrumentation-based radiation safety systems ultimately depends on the confidence that is developed in both the systems' reliability and the systems' "completeness". The latter term refers to the system's ability to deal effectively with all possible prompt radiation accident scenarios.

The set of system requirements and design criteria discussed in this paper are aimed at producing a personnel protection system that is both highly reliable and highly complete in its coverage of accident scenarios. In addition, the requirements and design criteria were formulated to make it possible to objectively determine compliance. The experience, to date, with systems designed to these requirements is encouraging. The problem is challenging but solvable.

ACKNOWLEDGEMENTS

Many people have contributed to the development of the concepts and systems discussed here. I want to acknowledge my many colleagues at LANSCE who made important contributions to development of the concepts and did all of the implementation. They include the LANSCE Radiation Safety Committee, now chaired by Olin van Dyck; Andrew Browman, Floyd Gallegos, Rich Ryder, Mike Plum, David Brown, Martha Zumbro. Mohsen Sharirli played a leading role in our effort to apply the methods of PRA to accelerator safety systems.

An important function was served by a workshop on the subject at Los Alamos chaired by Ralph Thomas. Many of the fundamental concepts discussed here were aired at this workshop and were peer-reviewed by a panel of experts from the field who were in attendance. Proceedings are available as an Los Alamos report (10).

REFERENCES

1. R. J. Macek, Proceedings of the Specialists' Meeting on Shielding of Accelerators, Targets and Irradiation Facilities, April 28, 1994, Arlington, TX, 163-177 (1994).
2. M. Plum et al., Proceedings of the 1989 IEEE Particle Accelerator Conference, 1556-8 (1989).
3. M. Plum, Verified Procedures for the Bench Check of the Model III Fail-Safe Ion Chamber Loss Monitor, LANL (1992).
4. K. Jones, AOT-6 Operations Manual, Chapter 6, updated annually, LANSCE Operations, (1995).
5. M. Plum and D. Brown, Proceedings of the 1993 Particle Accelerator Conference, 2181-3 (1993).
6. D. Brown et al., PSR Tech Note Series LANL, PSR-92-005 (1992).
7. M. Sharirli et al., Proceedings of the Probabilistic Safety Assessment International Topical Meeting, January 26-29, 1993, 554-558, (1993). Also LANL Report, LA-UR-92-3478.
8. D. Brown et al., *Health Physics*, **Vol. 38**, 507-521 (1980).
9. M. Sharirli et al., Proceedings of the Probabilistic Safety Assessment Internal topical Meeting, Jan 26-29, 1993, 559-564, (1993). Also LANL Report, LA-UR-92-3519.
10. R. J. Macek, G. B. Stapleton and R. H. Thomas, Proceedings of the Workshop on the Use of Instrumentation and Probabilistic Safety Criteria for Prompt Radiation Protection at LAMPF, December 9-11, 1991. Also LANL Report, LA-UR-92-0300, (1992).