SAFETY CRITICAL MONITORING FOR PROMPT RADIATION HAZARDS

L. Moritz, J. Drozdoff, G. Dutto, F. Mammarella, M. Mouat, R. Ruegg, TRIUMF, B.C., Canada

Abstract

At TRIUMF we have used both passive and active methods to protect against potential prompt radiation hazards produced by accidental beam losses in high-intensity proton beam lines. These methods consist of shielding, exclusion areas, and the use of fast acting radiation monitors. The latter are located within the shielded areas and are set to terminate beam production on the detection of abnormal beam loss. A recent risk analysis has suggested a need for higher reliability in the protection against potential prompt radiation hazards where the shielding is relatively thin. To address this requirement TRIUMF has developed a new approach using two systems of independent and redundant monitoring devices located outside the shielding to protect against safety critical events with the required level of reliability. Verification of the system reliability is achieved by weekly testing of the safety critical monitors as well as the trip devices. When used in conjunction with the traditional beam loss monitors we are able to distinguish between safety critical events and non-safety critical beam trips.

INTRODUCTION

One of the dilemmas of shielding high-intensity accelerators is whether to everywhere install shielding that is sufficient to reduce radiation fields to low levels under conditions of maximum possible beam loss or whether to shield low beam-loss areas only for expected operational losses and rely on active protection systems to terminate beam operation in case of total or high accidental beam losses. Generally the reliability or integrity of shielding is assumed to be very high (although this may not be justified in all cases), but the reliability of active protection systems needs to be demonstrated for each particular design. At TRIUMF we have used active protection systems for some time, but their reliability had not been formally demonstrated. At the request of the Canadian regulatory authority we re-examined this issue and found a solution for achieving the required level of reliability without performing a detailed fault tree analysis.

INITIAL SYSTEM

The radiation protection system that had been installed for many years at TRIUMF consisted of a series of detectors deployed *inside* the shielding. The detectors had no local electronics so that they were reasonably resistant to radiation damage. Analogue signals from these detectors were conditioned and then sent to a central processing unit where the signals were converted into digital values and read 10 times per second by a microprocessor. These values were compared to a set point and any reading above the set point generated a 'warn' signal to alert the operators to a beam loss. If a reading exceeded twice this 'warn' level, a 'trip' was generated that turned off the 500 MeV accelerator using several redundant and diverse devices. The system had a number of features built into it to enhance reliability, such as a watchdog timer, power monitoring, temperature monitoring, run time checksum check etc., and was powered by an uninterruptible power supply. The response time of this system to turn off the accelerator was measured to be between 150 to 200 ms, sufficient to prevent a significant radiation dose to anyone outside the shielding even under the highest expected dose rates.

ANALYSIS

System Configuration

The close examination of this system in response to the request to demonstrate its reliability concluded the following:

- The system had the dual purpose of personnel and machine protection. As a result the warn and trip levels were set very close to the operating beam loss levels and had no relation to the radiation fields outside the shielding.
- Many of the radiation detectors were located in high-radiation areas making them difficult to service and calibrate.
- The detectors were not fail-safe and subsets were powered by the same power supply.
- There was redundancy in the system only in that detectors were reasonably closely spaced and that several devices were used to trip the accelerator.

The conclusion was that it would be difficult to modify the system so that it would have the required demonstrable reliability.

Historical Data

An examination of the historical record showed that the number of failures of this system had however been very low. During a period of approximately 20 years there had been no instance where the system had failed to respond correctly to a beam loss that would have resulted in a high radiation field outside the shielding.

The system had in fact been exercised frequently (often several times per week) because of the machine protect function that resulted in accelerator trips whenever the beam loss anywhere exceeded four times the normal operational losses, even when these were very low. The

large number of accelerator trips made it difficult to separate out those beam loss events that might have led to very high, sustained radiation fields outside the shielding if the protection system had failed.

NEW APPROACH

In view of the above difficulties it was decided to use a new approach. This approach involved

- Creating a policy that defined the maximum tolerable radiation fields outside shielding under worst-case beam loss.
- Develop two completely independent systems for personnel protection with detectors located outside the shielding.
- Define a reliability goal for the remaining risk

Policy

A policy was defined that limits the maximum prompt radiation fields outside the accelerator and beam line shielding to 1 Sv h^{-1} for a point loss of the total beam intensity for which the accelerator or beam line is *licensed*. The rationale for this is that it is deemed not credible that a beam loss of this intensity could go undetected for more than 1 hour or could even persist without self-extinguishing itself via some catastrophic failure of the vacuum envelope. The maximum dose that could therefore be incurred would be 1 Sv, the threshold for immediate deterministic effects of a radiation exposure. This policy required that wherever a total beam loss could result in radiation fields greater than 1 Sv h^{-1}, the shielding would have to be upgraded or the area would have to be defined as an exclusion area that was interlocked so as to be inaccessible during operation.

New Protection Systems

Rather than attempting to improve the existing protection system it was decided that another system of similar design that was already used to measure neutron field levels outside the shielding and that used similar system architecture could be reconfigured to become a high-reliability system. This 'neutron monitoring system' had been used to generate alarms at relatively low ambient field levels, but had not been used to trip off the accelerator because of the slow response time of the neutron moderated BF_3 monitors. However, by incorporating a 'trip' function for these monitors at the relatively high level of 1 mSv h^{-1}, it was possible to have a response time as short as 200 ms.

To provide redundancy and therefore also to lower the reliability requirements for the neutron monitoring system, a second system with identical architecture but different detector technology was created. This second system uses plastic scintillators mounted on photomultiplier tubes and measures the current from these tubes as an analogue signal. These detectors are sensitive to both gamma and neutron fields and also differ in the way the signals are processed (analogue rather than pulse-counting for the neutron detectors).

Pairs of detectors, one from each system, were designated 'safety-critical' and were deployed outside the shielding in tamper-resistant metal locked cabinets with all wiring in accessible areas enclosed within metal conduit. The cabinets are provided with a port that allows insertion of an ^{241}Am-Be source for quick operational check.

Reliability Goal

As a goal for the level of reliability required, the value of 10^{-5} incidents per year was used, a figure that defines so-called 'safe' industries when applied to fatalities in the workplace [1].

An estimate of the number of events (such as magnets tripping off or vacuum valves being accidentally inserted into the beam path) that might initiate a total beam loss yielded a probability of approximately 10^{-1} per year. Therefore the requirement for the likelihood of occurrence of a failure of both systems to respond to such an event would be

$$10^{-1} \times 10^{-2} \times 10^{-2} = 10^{-5}, \qquad (1)$$

in other words each of the two independent systems must have a demonstrated failure rate of less than 10^{-2} per year.

In order to demonstrate that the systems in fact meet these levels of reliability, each of the detectors is tested on average once per week using the ^{241}Am-Be source and verifying that the correct level of signal is sent to the logic controller and then testing that the logic controller correctly trips the accelerator using all redundant devices. After two years of testing, the program will have established the required reliability of these systems.

In order to verify the estimate of the frequency of initiating events it is important to have a clear definition of what is meant by an 'initiating event'. The following definition was adopted: "a degradation or failure resulting in a sustained beam loss that, in the absence of the safety critical monitors, would lead to a dose rate outside the shielding greater than 50 mSvh^{-1}". Dose rates greater than 50 mSvh^{-1} if sustained for the postulated maximum credible duration of one hour would lead to doses in excess of the Canadian one-year regulatory limit on dose for Nuclear Energy Workers [2]. Although a dose in excess of 50 mSv may not necessarily have serious health consequences for the exposed individual such an exposure would have severe consequences for TRIUMF.

The definition then gives an operational way to decide whether a beam excursion that trips the protection systems should be classified as an 'initiating event': it must result in a trip of the 'safety-critical' monitors and be capable of generating a sustained radiation field outside the shielding greater than 50 mSv h^{-1}. Since the deployment of these monitors more than one year ago, only one trip has occurred. This was due to a dipole magnet located some considerable distance upstream of the thin shielding monitored by the 'safety-critical' monitors. A problem with the dipole magnet power

supply resulted in a 15% change in the magnetic filed that steered the high-power proton beam into the beam pipe. An investigation that involved intentionally steering a lower power beam through the full range of magnet settings demonstrated that although the radiation field during the incident exceeded the monitor trip level, it could not have exceeded 50 $mSvh^{-1}$ and therefore should not be counted as one of the initiating events. By keeping a record of all such events we hope to demonstrate the estimates of the frequency of such events.

CONCLUSION

TRIUMF has developed a new approach to demonstrate the required high reliability for active radiation protection systems by implementing two systems of independent and redundant monitoring devices located outside the shielding to protect against safety critical events. Verification of the system reliability is achieved by weekly testing of the safety critical monitors as well as the trip devices. When used in conjunction with the traditional beam loss monitors we are able to distinguish between safety critical events and non-safety critical beam trips.

REFERENCES

[1] U.S. Department of Labor Bureau of Labor Statistics, *Fatal Workplace Injuries in 1995: A Collection of Data and Analysis*, Report 913, April 1997.

[2] Canadian Nuclear Safety Commission, *Radiation Protection Regulations*, SOR/2000-203, May 2000.