RADIATION SAFETY SYSTEMS AT THE NSLS

T. Dickinson
National Synchrotron Light Source
Brookhaven National Laboratory
Upton, NY 11973 USA

Abstract

Design principles for radiation safety systems are presented. The safety systems at the NSLS are described and experience recounted.

Introduction

At the National Synchrotron Light Source in early 1987 there were 55 beam lines in operation, some with more than one experimental station. The majority of these beam lines have been designed, constructed, and managed by Participating Research Teams (PRT's) whose institutional affiliation and funding is from outside the NSLS. The PRT members are the principal users of their beam lines, but 25% of the research time is allocated to general users who apply to the NSLS for use of the facility. There are also a few lines which are operated by the NSLS and dedicated to general users. During fiscal 1986 there were over 800 registered users of the NSLS, and about 430 separate experiments were performed. The research carried out covers a wide range of disciplines, including atomic physics and biology, medicine and metallurgy, with scientific objectives ranging from pure research to proprietary industrial development. The users come from a wide variety of backgrounds, and some are not experienced at working at large facilities like the Light Source.

These factors have influenced the development of radiation safety systems at the NSLS. Careful integration of operations procedures and administrative controls with the personnel interlock systems has been needed to keep pace with increasing research activity.

Philosophy

Interlock Design Principles

The design principles discussed below have been developed during several years experience in the design, construction, and use of radiation safety systems at the NSLS and other facilities. No attempt has been made to list them in order of importance.

1. The system should be unrestrictive.
2. The system should be ergonomic.
3. The system should be redundant.
4. The redundant branches of a system should be different.
5. The system should be fail safe.
6. The system should be testable.
7. The system should be simple.

There are of course conflicts among these principles, and a final design must be a compromise.

The first rule is supported by the general idea that the need for a safety system comes up only because the research is worth doing in the first place. The system designer should not accept compromises to safe operation, but it is well to keep in mind the purpose of the institution. Apart from this, there are operational reasons for minimizing the restrictions of a safety system. Perhaps the most important is credibility. If a safety program has a reputation for being "no-nonsense", if convincing arguments can be made that each barrier protects against real danger, then users are likely to respect and accept the restrictions. Having said this, we arrive at compromise. Often restrictions are extended beyond what is needed in specific cases for reasons of simplicity, both in hardware and administration, and for standardization. These extensions should be recognized as compromises and justified as such.

Ergonomic design is a matter of enlightened self interest. The avoidance of missteps and blunders in the operation of a system is clearly an enhancement to safety. Also the safety of the experimental activities at a research facility depends largely on the cooperation of the users. An experimenter who has been wrestling with an awkward, balky, overly restrictive safety system is unlikely to be in a mood to cooperate.

The dictionary definition of redundant is "exceeding what is necessary or normal". With respect to interlock systems this is often taken to mean the duplication of active components. A better functional definition of a redundant system is one "where no single failure will render the system unsafe". To meet this definition, the redundant branches of an interlock circuit must have no common elements. The use of redundant systems can provide a large decrease in the incidence of unsafe failures in an interlock. If we estimate the frequency of single failures to be one per 20 years per system, and the interval between tests and hence the correction of a fault to be 6 months, then there would be a coincidence of two failures in a system every 800 years.

The calculations which show the advantages of redundant interlocks assume that failures will be random and unrelated. If the two branches of a redundant system are identical, there is a good chance that there will be related simultaneous failures, defeating the redundant protection. The qualities which can lead to related failures include the use of similar components, similar arrangements of logic, symmetrical location of terminal points on terminal strips, common power supplies or common reference points, and many other such features. The possibility of related failure brings a large reduction in system safety, and the avoidance of this deserves substantial design effort. Often this means that one of the alternate branches may not be optimum in terms of components or function. This is part of the overall compromise and must be evaluated as such.

A fail safe design is one in which the most likely failure modes leave the system in a safe condition. For example, loss of power, shorts to ground, and open circuits should all leave the system in a safe state. Determination of common failure modes comes from experience and engineering analysis. In most cases the objective is to reduce serious failures to a very low incidence, and it may be difficult to accumulate significant experience in a reasonable time. On the other hand, an analysis depends on knowledge of the details of the system and this may be difficult to obtain. For example, integrated circuit logic outputs may fail either open or shorted, depending on the nature of the stress and on manufacturing details which may not be part of the chip specification. Microprocessor systems are even less accessible to detailed failure analysis. Computer hardware bugs are seldom understood in detail. Sophisticated accelerated endurance tests can be devised, but there are lingering doubts about the final interconnected system in the operating environment. Since the issue of related failures can have a powerful effect on system reliability, such doubts weigh heavily. The aerospace industry has shown that such systems can be built, but at great expense. These considerations had a dominant influence in the choice of relay logic in

CH2387-9/87/0000-1605 $1.00 © IEEE
PAC 1987

the NSLS interlock systems, anacronistic as it may seem.

System testing is probably the single most important contribution to safe operation. The largest source of faults come from wiring errors which occur during construction and maintenance. Construction errors are expected, and are sorted out during the informal testing as a system is commissioned. Faults which arise during maintenance are more subtle, and experience has shown that the definition of maintenance must be broad. At the NSLS, a system must be tested whenever a circuit element inside the enclosure for the system logic has been touched. The history of selected failures at the end of this paper supports this policy. The encouragement of neatness and care is worthwhile for an efficient construction enterprise, but to expect perfection is hopeless. In any case, testing must be done for faulty components (and flawed design).

The test should include all of the protective elements of the system and verify their function. Each element of redundant features must be checked, and this capability must be part of the system design, since it is common for the action of one element to mask the effect of the other. The test should not only verify that the system works as expected, but also that improperly executed operations do not lead to unsafe conditions. In designing tests and interpreting the results, it is important not to rely too heavily on the system logic, since this is one of the things being tested.

Simplicity is a virtue which which appears in this discussion as part of the compromise that each actual system represents. When a choice must be made between covering all conceivable possibilities, and simplicity, the latter should prevail. Sometimes excessive extensions or layers of protection in a safety system represent uncertainty or lack of knowledge of the problem. The pronouncement "You can't be too safe..." often means that safety measures have been carried past the point of counter-productivity, that the hazard is not well understood, and that there is a lack of confidence in the basic safety system.

Administrative Controls

Hardware interlocks are appropriate for protection against hazards where the risk is high, or where mistakes are likely to occur as the user interacts with the system. In other cases safety can be maintained with administrative controls: procedures, rules, and sanctions. Most of the safety system design principles listed above apply as well to administrative controls, although in a less precise way. The avoidance of unnecessary restrictions, ergonomic design, and simplicity certainly apply. There needs to be backup supervision of performance, and an audit function, both periodic and after any breakdowns. The approach is clearly similar. Sanctions are necessary, but are difficult to apply. If they are too severe, violations are often overlooked, or let off with a warning, so less is better if this leads to consistent response to violations. In severe safety violations, the punishment must be appropriate, for example revocation of research privileges. A vital part of administrative control is the services of a skilled, disinterested operator (known at the NSLS as the Operations Coordinator). This person keeps track of experimental activities, monitors compliance with safety procedures, and serves as a resource in dealing with interlock, vacuum, and other user problems.

Description

Injector and Storage Ring Safety Systems

The interlock system logic is shown in Fig.1. Shutters serve to partition the four areas from each other. For example, if the injection shutters to the VUV ring and the x-ray ring are closed, then injector operation does not depend on the state of those systems. The interlocks for the injector and the x-ray ring are similar. One branch of the redundant system consists of door-closed switches, emergency stop buttons, and the search sequence. The other branch is a Kirk lock captive-key system which mechanically locks the doors and closes an electrical circuit when all keys are in place in the security system. The redundant branches are separate and act independently to shut down the radiation source if a system is breached. The VUV ring is not a high hazard radiation area, and the interlock for the center part of the ring serves only to control access to this area.

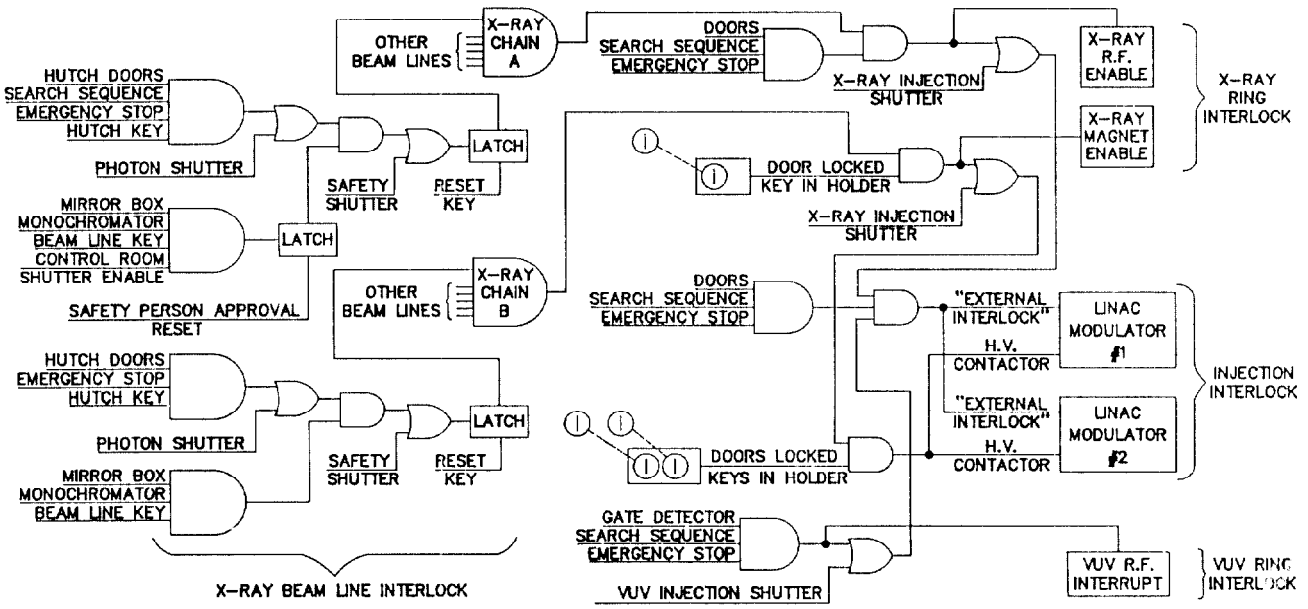

Figure 1. Interlock System Logic.

X-ray Beam Line Safety Systems

The energy spectrum of the synchrotron radiation in the x-ray beam lines extends to a few tens of kilovolts, and a millimeter of lead or a few milimeters of steel are usually an adequate shield. However, the radiation intensity in the beam is of order 10^{10} Rads/hour, and would cause instant serious injury, so the means of containment must be very secure. The beam lines also represent a hole in the storage ring shielding, so bremstrahlung shielding must be provided along the beam line.

Most x-ray beam lines end in a hutch which houses the experiments. This is a structure made of 1/8 inch steel, is typically two or three meters on a side, and is provided with overlapped seams, shielded view ports, and an interlock system. Some experiments require user access to the hutch 20 or more times an hour, so the interlock must be simple to operate, reliable, and fool proof. The user performs these accesses to the hutch, and also searches and returns to beam-on condition without intervention from the operations staff. Chain A of the beam line interlock is implemented with relays which provide sequencing and indicators as well as the interlock. Chain B uses only the various switches wired to provide the required logic, and thus is physically quite different from Chain A. Not shown on the logic diagram are the circuits which prevent opening a shutter when the hutch is open or opening a door when the shutter is open thus dumping the storage ring. These are considered convenience features and not fundamental parts of the protection system.

Because of the extremely high radiation levels inside the x-ray beam lines, access to these lines must be controlled as carefully as it is to the hutches.

Padlocks are used to lock the flanges on the lines so they are not opened in an uncontrolled way. This provides protection against the situation where a worker dismantles the wrong beam line due to confusion or misdirection. Obtaining the key to the padlocks has two results: it brings an Operations Coordinator to the scene who is familiar with the implications of opening a beam line, and the padlock key is attached to another key which disables the beam line interlock. The padlocks are provided in sets which are keyed the same, with a given set confined to a beam line.

Administrative Controls

Because of the large number of beam lines and the steady parade of new experiments and users, it has been necessary to formalize some of the administrative controls. Each beam line has a written description of the configuration of the line as it was approved in the formal safety review. This is in the form of a check list with each required item of shielding, exclusion zone, padlock, and the like. Photographs are often posted on location to aid in the description. This check list is executed before any new experiment is started, and before the line is reset after it has been locked out. An Experimental Safety Approval form is filled out by the user for each experiment and lists the nature of the experiment, the personnel, and the materials and equipment to be used. Most experiments are arranged directly with the Participating Research Teams at the beam lines, and the Safety Approval form is the only required notice to the Light Source. It is reviewed for hazards by the NSLS Safety Officer and the approved form must be posted at the beam line when the experiment is running. There it helps the Operations Coordinators to keep track of what is happening on the floor, who is there, and when the experiments change.

Experience

The radiation safety systems at the NSLS have operated for several years with no dangerous failures. However, much can be learned from the history of partial failures. The largest number of interlock faults and failures are found after construction or maintenance on a system, and serve as a constant reminder of the need for a rigorous testing program. Two such faults are particularly interesting. The first occurred after several new beam lines were added to the x-ray ring interlock. The test found that about half of the existing beam lines no longer affected the ring interlocks when they were tripped. The problem was that 24 volts was being fed into the circuits from a power supply at one of the new beam lines due to a wiring error. These supplies are supposed to float so they can't crosstalk, but the one at the beam line was grounded by another wiring error, and the ones in the ring circuit were grounded at faulty indicator light sockets. This failure is particularly hair-raising because an error at one beam line caused a failure at other beam lines, which might not have been tested. This situation has been corrected by more careful isolation of the power supplies, by periodic tests for ground faults, and by more vigilance for crosstalk possibilities.

The second failure was found in a test of the VUV interlock after a ring maintenance period. The assertion was that no work had been done on the system, but part of the interlock was found to be bypassed. It turned out that a technician had been assigned to attach numbers to some wires in the system, a few wires had to be pulled out to get the numbers on, and one was put back a quarter of an inch from where it came.

Recently it was discovered that the linac interlock could be left indefinitely in a partially searched state with the access door unguarded. This was due to a quirk in the circuit design and had been overlooked when the test was designed. It was found when an error was made in executing a test, and an attempt was made to reset the system by opening a door. The problem was easily corrected, and a much more careful analysis has been made of the circuit.

There have been two spontaneous, nonsafe faults in interlock systems during the last two years, when an average of 20 systems were in service. The estimate in the discussion on redundant circuits comes from this experience. One failure occurred after a jumper in an x-ray beam line interlock was removed to introduce a new interlock feature. The system passed the test at that time, but at the next periodic test it was found that the jumper, which had only been removed at one end, had moved back and was touching the terminal where it had been pulled. Jumpers are now removed at both ends. The second failure involved two faults: the power supply in a beam line interlock shorted its "high side" to ground, and a short to ground elsewhere in the system caused the shutter control circuits to be bypassed, allowing the shutter to be opened when the hutch was not secured. When this was done, both ring interlocks opened, and the storage ring dumped. The shutter control circuit is not part of the fundamental protection system, but this failure illustrates a significant failure mode.

Acknowledgements

The author wishes to thank George Schwender for the initial interlock design, Bob Best, John Gallagher and Steve Kemp for construction and installation, and Luis Aguilar, Steve Kemp, Len Pharr, Pete Ratzke, and Skip Thomas who as Operations Coordinators have kept the program running safely. Roger Klaffky, Norm Rohrig, and Bill Thomlinson contributed to many useful discussions.