Documentation Related to Frequency of Testing Interlocks

Attached are the documents that describe the complexity and reliability of interlock systems found at the C-A Department at Brookhaven National Laboratory. As indicated in NCRP Report 88, Radiation Alarms and Access Control Systems, page 43, the frequency of testing should be related to the complexity and demonstrated reliability of the access control system. The specific wording regarding frequency of testing is found in the BNL RadCon Manual Appendix 3A, which is located at:

https://sbms.bnl.gov/program/pd01/pd01d231.htm

Building 701
P.O. Box 5000
Upton, NY 11973-5000
Phone 631 344-4211
Fax 631 344-7630
musolino@bnl.gov

managed by Brookhaven Science Associates
for the U.S. Department of Energy

Memo

date: *January 16, 2001*

to: *T. Sheridan*

from: *S. Musolino (signed original on file)*

subject: *RPWG Meeting 01-01, January 10, 2001*

In attendance: W. R. Casey, W. Gunther, P. Jones, H. Kahnhauser, S. Layendecker, E. Lessard, S. Musolino, P. Williams

The e-mail vote on the subcommittee proposal in Attachment 1 for the CAD exemption from six-month interlock testing was completed at the meeting to obtain a quorum. The proposal was passed. Therefore, the Working Group recommends approval of the proposed change to the BNL RadCon Manual.

Attachment 8.11 to the Radiation Work Permit procedure (shown in Attachment 2) to evaluate the use of respiratory protection to minimize total effective dose equivalent was reviewed. It was accepted with e-mailed comments 1 and 2 from Bob Miltenberger, Attachment 3. Comment 3 was deemed valid, but should be handled by the BNL respiratory protection program document and not the RWP procedure. The exemptions were left in but will require concurrence from RCD management on a case-by-case basis. Since allowance of a facial contamination to reduce TEDE would cause and ORPS to be issued, Steve Layendecker was asked to review the issue with DOE.

Attachments: 3
cc: RPWG
M. Bebon
T. Kirk
M. Lynch
R. Osgood
B. Sack
P. Paul
N. Volkow

Attachment 1

Current Wording in RadCon Manual CHAPTER 3

APPENDIX 3A Physical Access Controls for High and Very High Radiation Areas

1. Area Interlock Requirements for High Radiation Areas >5 rem/hr:

    a. …

    b. All security systems which are in use shall have the functioning of all components tested at least every six months. Devices which establish a threshold on a variable parameter signal (such as magnetic current interlocks, or beam or radiation intensity interlocks) shall be tested following as established procedure so that the threshold trip point is known. For independent and redundant systems, the tests shall examine proper functioning of each redundant subsystem.
    NOTE: For systems that have ongoing operations exceeding the six-month testing cycle exemptions from this testing requirement may be requested from the Manager, Radiological Control Division.

    c. …

Proposed Change:

1 Area Interlock Requirements for High Radiation Areas >5 rem/hr:

a) …
b) An interlock system shall not be used to provide protection unless it has been tested within the interval specified below. Such tests shall be done according to written procedures, and the results of the tests shall be recorded. Devices that establish a threshold on a variable parameter signal, such as magnetic current interlocks, or beam or radiation intensity interlocks shall be tested following an established procedure so that the threshold trip point is known. For redundant systems, the tests shall examine proper functioning and independence of the redundant subsystems.
    i) For the accelerators, accumulators and beamlines that have an annual running period and a shutdown period, a rigorous functional test of all components shall take place within an interval of 12 months. For all other accelerators, accumulators and beamlines, a rigorous functional test of all components shall take place within an interval of six months.

NOTE: Exemptions from these testing requirements may be requested from the Manager, Radiological Control Division.

Attachment 2

Attachment 8.11 Evaluating the Use of Respiratory Protection to Minimize Total Effective Dose Equivalent

Introduction

Respiratory protection is primarily used to minimize or prevent the intake of radioactive materials by workers. This usage is, therefore, an effective technique to minimize or prevent internal dose from internally deposited radioactive materials (uptake). Historically, radiological control personnel have assigned respiratory protection without significant regard to the drawbacks of its use. This was primarily due to the stigma associated with internal deposition of radioactive materials, and sometimes due to the mistaken belief that internal dose is more hazardous than external dose. Sound radiation protection principles and federal guidance/regulations recognize and require that radiological control programs evaluate the use of respiratory protection to ensure that the Total Effective Dose Equivalent (TEDE) is minimized.

Total Effective Dose Equivalent (TEDE) is a summation of internal (committed effective dose equivalent) and external (effective dose equivalent) radiation dose expressed in the units of rem. Obviously, the use of rem (or millirem) ensures that the total risk from internal and external dose is the same for the same unit measured, (i.e., 1 rem of internal dose has the same health effects as 1 rem of external dose).

<u>Policy</u>
It is a requirement of the BNL Radiological Control Program (Article 514.B.2 of the Radiological Control Manual) that the use of respirators will be avoided if its use increases the TEDE of the worker.

<u>Implementation Strategy</u>
BNL Radiological Control Division (RCD) will perform TEDE evaluations on all work activities where the estimated dose from external radiation exceeds 50 millirem to a worker per work evolution, and respiratory protection is being considered to minimize internal dose.

RCD will assume that the use of respiratory protection results in a decreased work efficiency of 15-25%, i.e., of increased exposure time to external radiation of 15-25%. For normal planning purposes a value of 20% will be used. The work planning group may approve values other than 20%, but within the range of 15-25% depending on the following factors:

- relative health and conditioning of the individual worker
- previous experience using respiratory protection by the worker
- necessity of verbal communication between workers to ensure successful completion of the activity
- expected length of the time spent in respiratory protection
- physical exertion needed for the activity
- any other pertinent factors

Values outside the range of 15-25% may only be used with the concurrence of the Facility Services (FS) Manager, or Health Physics Technical Services (HPTS) Manager, or RCD Manager.

RCD will calculate the TEDE with and without the use of respiratory protection assuming that one DAC-hour of airborne radioactivity is equal to 2.5 mrem TEDE.

3.1 If the TEDE using respiratory protection exceeds the TEDE without using respiratory protection by less than or equal to 10 mrem, respiratory protection may be used at the discretion of the FS Representative or designee.

3.2 If the TEDE using respiratory protection exceeds the TEDE without using respiratory protection by greater than 10 mrem but is less than or equal to 25 mrem, the use of respiratory protection should be avoided.

3.3 If the TEDE using respiratory protection exceeds the TEDE without using respiratory protection by greater than 25 mrem, respiratory protection shall not be used unless specifically authorized by the FS Manager or the HPTS Manager or the RCD Manager.

<u>Exception 1:</u>
RCD will normally assign respiratory protection to an individual regardless of TEDE evaluations if the surface or airborne contamination levels would likely result in a facial contamination without the protection provided by the respirator.

<u>Exception 2:</u>
RCD will normally assign respiratory protection to an individual regardless of TEDE evaluations if the individual is expected to exceed Special Bioassay Monitoring Requirements as described in FS-SOP-4025.

TEDE evaluations shall be formally documented by memorandum to the FS Manager for all evaluations where an individual is expected to enter an area where they will be exposed to greater than 1 DAC-hr/hr airborne concentrations without respiratory protection. The memorandum will include RWP number, individuals affected (names and identification numbers), and date of exposures. The HPTS Manager and PM Manager will be copied on said memorandum.

Attachment 3

From: Miltenberger, Robert P
Sent: Friday, January 05, 2001 6:21 AM
To: Musolino, Stephen; Layendecker, Steve; 'Kahnhauser@bnl.gov'
Cc: Miltenberger, Robert P
Subject: Proposed Modifications to Attachment 8.11

As I reviewed this document again, I noticed three things that I believe need to be fixed:

1. On page 2, line 2, the second use of TEDE on point 3 should be replaced by CEDE.

2. Point 4 on page 2 seems to be in conflict with the starting premise that you only do the documentation if the external dose will be > 50 mrem.

3. The attachment doesn’t address the issue of a person requesting a respirator even when one isn’t required. I believe that OSHA allows this freedom to a worker. In the first draft I recommended that we have an exception 3. I still think that we need this and suggest that the wording should be something like:

Exception 3:
If a worker requests a respirator when it is not required and not in their dosimetric interest, the respirator can be issued after counseling the worker that their decision will most likely increase their TEDE. When this occurs, the FS Representative shall document the action by memo to the FS, HPTS and PM Managers.

Interlock Testing Frequency
Presentation to Radiation Protection Working Group
November 21, 2000

Introductory slides are at:
http://www.rhichome.bnl.gov/AGS/Accel/SND/RSC/RPWG%20Interlock%20Talk_files/frame.htm

Notes on "Impact of Test Frequency on Reliability" by M. A. Azarm of the BNL Energy Sciences and Technology Department, and notes by D. Beavis of the BNL Physics Department on "Frequency of Interlock Testing, Failures in PLC Based Access Control System and Failures in Relay Based Access Control System" are attached here.

Primer on Impact of Test Frequency On PASS Reliability

Conceptual Discussion

1. The Concept of Stand By Equipment
2. The Impact of Human Errors (Maintenance, ...)
3. The Concept of Redundancy
4. The Impact of CCF
5. The Impact of Types of Tests: Functional, Sequential, and Staggered Testing
6. The Concept of Diversity

Examples:

Relay System with No Redundancy
Relay System with a Redundancy
Relay System with Diversity
Relay System with Compensatory Measure (Functional and administrative)

Conceptual Discussion

1. The role of fault tree analysis
2. The concept of minimal Cutsets
3. The role of detail quantification

Summary:

The Bounding Effect of Reducing the test frequency by factor of 2

The Bounding Effect of Reducing the test frequency by a factor of 2 but supplementing with functional testing

The Bounding Effect of Reducing the test frequency by a factor of 2 and supplementing it with both the functional testing and tightening the administrative control.

Building 911B
P.O. Box 5000
Upton, NY 11973-5000
Phone 516 344-2625
Fax 516 344-8178
lopresti@bnl.gov

BROOKHAVEN
NATIONAL LABORATORY

managed by Brookhaven Science Associates
for the U.S. Department of Energy

Collider-Accelerator Department
Radiation Safety Committee

Memo

date: November 13, 2000

to: S. Layendecker

from: D. Beavis

subject: **Estimation of time to Loss of Protection—The D downstream gate**

I have estimated the mean time to loss of protection for the D downstream gate for the D target cave at the AGS. It is hoped that this specific example will provide a more realistic estimate of the mean time to loss of protection due to component failure, then simple generalizations. The result of the analysis is that it takes approximately 1,000,000,000 years for a loss of protection to occur at this gated due to component failure.

I have assumed that all components have the same mean time to failure. I have previously estimated this to be between 1300-2000 years for the AGS relay system. Only the lowest order in component failure is important. I have assumed that there are no shorts, which can bypass multiple components at one time.

There are two ways component failure can lead to the potential for exposure of personnel at the D downstream gate. Either the person accesses the area while the beam is on or the operators turn the beam on after a person has entered the cave.

Three independent failures are required for a person to access the area with the beam on.

1) The relay for controlled access must fail and give a false indication that the area is on restricted access. This will then allow the 256 key to open the gate. A similar failure can occur for the operator key. The probability of this failure is 2R, where R is the probability for the relay to fail unsafe.

2) The redundant door reset must fail. This can happen if the microswitch or the associated relay fails to an unsafe state. The probability is 2R.

3) The door reset must fail. This can happen only if the reset relay fails unsafely, which has a probability R.

All three of these must occur for access and the beam not interlocked off. The probability to enter the gate with the beam on is $4R^3$. This gives a mean time to loss of protection of 500,000,000 to 2,000,000,000 years for this gate, with a one-year interval between testing.

The second method for loss of protection is for the beam to be turned on while a person has entered the cave through this gate. It is possible for the operators to reset the gates from the outside without sweeping the cave of personnel. I will ignore this possibility. To get the beam on then requires items 2 and 3 above to fail unsafely, thus a probability of $2R^2$. The area would have been on restricted access to enter. This means that the resets on all the gates are dropped for the area. The D cave has two gates. A relay for the controlled access at the D upstream gate would also be required to fail. This gives a combined probability of $2R^3$. Additionally, the operators would need to become confused and turn the beam on without sweeping. Thus this will happen about once every 250,000,000 to 1,000,000,000 years. For an area with only one gate the mean time to failure would be of the order 1,000,000 years.

A few remarks are in order.

The above ignores the training of personnel and operators. In the above example, the person would be working/entering a cave with the lights out (the indicator that beam is allowed on). It also ignores the procedures that operators follow to turn the beam on in a cave or allow a person into a cave.

The relay system has substantial redundancy. This causes many potential correlated pairs to be of lower order, i.e. additional powers of R. However, if one allows for wiring shorts at arbitrary locations then these can be reduced to the same order as above and could reduce the mean time to loss of protection.

A crude estimate for the time to loss of protection at the entire complex can be estimated by scaling by the number of gates. There are approximately 100 gates at the AGS. This would suggest that the time to loss of protection somewhere in the complex is of the order of 5,000,000 years. This is substantially longer than the 140-340 years I previously suggested (memo of Nov. 6, 2000). The two reasons for the substantial change are the requirement for a third component to fail and the number of failure pairs is very low.

It is my opinion that the most likely cause for failures, which could lead to a loss of protection are related to the human interaction with the system. This includes design flaws, implementation flaws, etc. In addition there may be common modes of failure, which simultaneously act on multiple components including components in independent systems. Periodic testing is not effective is removing human errors and common mode failures. It is therefore important that effort should go to reducing the human error and not testing for component failure.

I close with a few caveats. There may be failure times which are shorter than those used above. It is possible that I missed failure modes in the analysis. Finally, although I think the numbers above are accurate, I do not think they are relevant. It is the unknown rare modes of failure, the common modes of failure, and human error, which dominate the time to failure of the system.

CC:

RSC Info Dist.
T. Dickinson
RSC Chair File

Building 911B
P.O. Box 5000
Upton, NY 11973-5000
Phone 516 344-2625
Fax 516 344-8178
lopresti@bnl.gov

BROOKHAVEN
NATIONAL LABORATORY

managed by Brookhaven Science Associates
for the U.S. Department of Energy

Memo

Collider-Accelerator Department
Radiation Safety Committee

Date: Nov. 6, 2000
TO: S. Layendecker
From: D. Beavis DB
Subject: Frequency of Interlock Testing

I would like to provide you some information related to the issue of the frequency of interlock testing for C-A Dept. radiation safety interlocks systems. In addition, I have a few comments regarding the RPWG minutes of August 30,2000. Hopefully the information and remarks will provide you with increased confidence in granting extensions to the 6-month testing rule and in changing the time interval between testing to one year.

I have attached two memorandum related to component failure in the radiation protection systems used by the C-A Dept. The component failure numbers for the relay-based system suggest that the time to failure of a component to an unsafe state is 1300-2000 years. It is difficult to extract the equivalent number for the plc-based systems in the fastbeam and RHIC. I offer the opinion that it is probably comparable or somewhat better due to the average age of the components and newer infrastructure. It is my opinion that the C-A Radiation Safety Committee (RSC) has strong confidence in both these systems.

Estimating the number of years till a dual independent system losses protection due to component failures depends on several items. Firstly, it is proportional to the square of the ratio of the time interval between tests and the mean time to fail unsafe. For the discussion below I will use a testing interval of 1 year. A loss of protection in a dual system requires two failures for a specific system function, such as gate 1 closed. For the C-A relay system this is between 1.7 to 4 million years for a particular pair. Now, one needs to sum over the number of possible failure pairs in the system, which can lead to loss of protection. This is not a simple number to calculate. I will make a crude estimate of 12,000. This number is large because I have tried to take into account the issue that certain components sum the results of others and, therefore, their failure overrides the correction functioning of the components which they sum. Only a detailed and time-consuming review of the entire configuration can provide a correct number. It is estimated that once every 140 to 340 years protection may be lost in the relay-based system due to component failure in the dual portion of the interlocks.

I do not consider the 140-340 years to be indicative of the actual time for the interlocks to fail in a manner that protection is lost due to component failure. Several factors contribute to this remark. There are substantial differences in the size of the areas. I believe that the 12,000 pair combinations is an overestimate. There are additional features in the interlocks, which go beyond the simple dual interlock requirements and add additional protection. More indicative of the system protection would be to estimate the chance to obtain exposure in a specific area. I plan on providing such an estimate to you in the next few days for the D

target cave at the AGS. My guess is that the result will be many thousands of years for one year between tests.
Other items can contribute to interlock failures besides component failure. These can include such items as human error, design flaws, loss of configuration control, implementation error, and testing error. In addition, for dual systems it is open expected that there are unconsidered rare failures, which cause a correlated failure in the independent interlock chains. It is therefore believed that one never achieves the simple time to failure for dual interlocks that one calculates from squaring the singles failure rate. Regular periodic testing is not affective in finding most of the problems discussed above.

There are functions in the interlock system and areas that do not have dual system protection since the potential dose rate is 50 rem/hr. One of these sub-systems is the radiation monitoring system of chipmunks. These devices have local audio and visual means of warning local personnel of the dose rate even if the interlock fails. The chipmunk units are also monitored in MCR and an alarm would alert operators that there were high dose rates and the OPMs require that they respond to these alarms. Therefore, there is probably minimal risk of exposure to personnel due to component failure of this system. There may be 1 or 2 experimental areas that still have single interlock chains. These areas may deserve future consideration.

A few comment regarding the minutes of the RPWG Meeting of August 30,2000:

1) For dual systems the failure to an unsafe state where protection is lost is proportional to the square of the frequency of testing.
2) There is no evidence that the RHIC system is more reliable than the older AGS relay system.
3) From discussion with T. Dickinson (NSLS) there have been only two failures to an unsafe state due to component failure at NSLS. This gives a time to failure for a component of greater than 10,000 years (for the AGS this is 1300-2000 years). Whether this is due to a younger average age of the components, the working environment, or better components is not known to me. The time to loss of protection due to dual component failure is estimated (by me using the numbers in the minutes, 4900 failure pairs, and the above time to failure) to be greater than 80,000 years at the NSLS for 6 months between tests. Naturally, this number can be substantially different depending on the actual distribution of components in the system.

CC:

T. Dickinson
RSC Chair File
RSC Info. Dist.

Attachment: Memo dated October 30, 2000, Beavis to RSC *"Failures in the AGS Relay Based Access Control System"*.
Memo dated October 31, 2000, Beavis to RSC (info. dist) *"Failures in the PLC Based Radiation Safety Systems"*.

BROOKHAVEN
NATIONAL LABORATORY

Building 911B
P.O. Box 5000
Upton, NY 11973-5000
Phone 516 344-2625
Fax 516 344-8178
lopresti@bnl.gov

managed by Brookhaven Science Associates
for the U.S. Department of Energy

Memo

Collider-Accelerator Department
Radiation Safety Committee

Date: Oct. 31,2000
To: RSC (info dist.)
From: D. Beavis
Subject: Failures in the PLC Based Radiation Safety Systems

N. Williams has reviewed the failures that have occurred in the PLC based radiation safety systems. Attached are his summaries of the failures, which have been logged for the RHIC system and the fastbeam (g-2) system. The time intervals for these failures are 1.5 years for the g-2 system and 1.25 years for the RHIC system. I will make a few remarks regarding the failures.

There are a substantial number of failures to a safe state. Many of these failures can be attributed to implementing a new design with a PLC based system. In addition, the numerous wiring errors are probably an "infant mortality" issue with commissioning such a large system. It is expected that the number of wire failures will decrease substantially in the future. Some of the problems such as the latch switches for the gates are a result of poor component choice, which causes a failure to a safe state. These switches have been replaced with low current switches. It is anticipated that the number of failures to a safe state will decrease dramatically.

The only failure to an unsafe state was a token-key switch in a fastbeam key tree. This was an implementation error, which was not detected on initial installation/testing. It was detected later on a system check.

Comparison of the reliability and safety of the older AGS relay system to the new PLC based PASS systems is difficult at this time. The overall system logic for RHIC is substantially simpler that the AGS system. The total number of interlocked doors is similar between the combined PASS systems and the AGS. There are substantially more critical devices in the relay based system. Effectively, the combined plc-based systems are somewhat smaller than the relay-based system at this time. Any comparison of failures to an unsafe state is hampered by the low statistics and short time interval that the plc-based systems have been used. The failures to a safe state are hampered by the various system-commissioning issues in the plc-based systems discussed. Data collected over the next few years should provided useful in making a comparison between these two types of systems.

The plc-based systems have been less flexible than the relay based system. This is a result of the difficulty in verifying the software for the plc-based systems. Several times desired modifications for the plc-based systems have been incorporated by using relays to perform the necessary logic change and then the relay output feed into the PLC system in a manner, which does not require software, changes. This decision is based on the ease to verify the logic implementation with relays and not on whether one method is more reliable than the other. This is potentially an impediment for using plc-based systems where one expects changes such as in the AGS slow beam program. It might be possible that changes to the architecture for the software and hardware of the plc-based systems could remove this impediment.

RHIC PASS fault summary (FY00).

Sub-systems	*Failed safely*	*Failed-unsafe*	Comments
PLC Software	9	0	The majority of these faults were in the MCR Panelviewer software.
PLC Hardware	2	0	
Wiring (Gate, cabinets, etc)	8	0	Mostly due to an intermittent short at Phenix 8GE1 gate. The gate was rewired.
Loops (gate, sweeps, etc)	10	0	We had problem with the high current rated switches (10A) use in the electric strike. These were replaced with gold contact, low current switches (10mA). The rate of failure reduced significantly.
Remote I/O blocks	2	0	The critical device R I/O block lost power.
Switches (gates, crash, etc)	6	0	Loose wire at gates, PLC cabinets, etc.
UPS	6	0	Occurred during power dips. Will replace UPS with true on-line units.
ODH	4	0	Sensor drifted out of calibration during the summer months.
Chipmunks	6	0	
Other (design fault, etc)	4	0	

G-2 PASS fault summary.

Sub-systems	*Failed safely*	*Failed-unsafe*	Comments
PLC Software	6	0	The majority of these faults were in the MCR Panel viewer software.
PLC Hardware	25	0	Ninety percent of this failure was due to the processor software interrupts.
Wiring (Gate, cabinets, etc)	5	0	Mostly loose wiring.
Loops (gate, sweeps, etc)	12	0	We had problem with the high current rated switches (10A) use in the electric strike. These were replaced with gold contact, low current switches (10mA). The rate of failure reduced significantly.
Remote I/O blocks	1	0	The critical device R I/O block lost power.
Switches (gates, crash, etc)	6	0	Loose wire at gates, etc.
UPS	5	0	Occurred during power dips. Will replace UPS with true on-line units.
Chipmunks	6	0	
Power Supplies	0	0	
Other (design fault, etc)	4	1	The B-division was not responding to one of the Uup (P23) key tree key. This was resulted from a wiring error. The A-division responded correctly.

CC:

N. Williams
RSC chair file

Building 911B
P.O. Box 5000
Upton, NY 11973-5000
Phone 516 344-2625
Fax 516 344-8178
lopresti@bnl.gov

BROOKHAVEN
NATIONAL LABORATORY

managed by Brookhaven Science Associates
for the U.S. Department of Energy

Collider-Accelerator Department
Radiation Safety Committee

Memo

date: October 30, 2000

to: Radiation Safety Committee

from: D. Beavis

subject: ***Failures in the AGS Relay Based Access Control System***

I have reviewed the failures log for the AGS access control system. Below I will briefly summarize the findings of that review. It is hoped that this review will provide some results, which can aid in future design as well as address how frequent the system should be tested. Assumptions are required to extrapolate the results of this review to recommendations on system design and testing and therefore will not be presented in this memorandum.

The failures log has been kept since April 1991 to the present. The last entry for this review was Sept. 11, 2000. This review does not cover failures in the PASS system used at RHIC or the fastbeam. The time interval over which these failures occurred is 9.5 years. Most configuration changes to the system have occurred in the secondary beam areas. The total number of components has been reasonably constant during the 9.5 years, although several secondary beam areas have not been active the last few years.

Consultation was done with D. Meany and A. McGeary in understanding the entries of the log.

The totals number of failures during this period was 110. These failures have been classified as failed safe and failed unsafe. The classification of these failures has not been done by an independent person. **None of the failures to an unsafe state resulted in an unsafe condition for personnel**. 13 of the failures were classified as failed-unsafe. Table I presents a summary of the failures.

Table I

Component	Failed-safe	Failed-unsafe	Total
Relay	51	9	60
Micro-switch	4	2	6
Wiring	8	0	8
Other	34	2	36

Not included in these list is the failure of two water flow vanes which are interfaced into the ACS for equipment protection. They were detected failed in an unsafe-state during system checking.

There are approximately 250-300 micro-switches in the system. The two failures to an unsafe state were caused by water damage to the switch. The mechanical housings were installed in a manner that allowed water to enter the housing. The mounting orientation was changed on these micro-switches when they were replaced. In addition, the other existing micro-switches were inspected for proper mounting orientation. One failure was detected as part of the functional checks. The other was noticed during a summer shutdown.

There are approximately 1400-1500 relays in the access control system. The relays implement the logic of the system. Time delay heads caused nine of the failures to a safe state. The most common failure to a safe state for the relays was failure of the coil. There are approximately 140 relays in the Booster 24 volt system, which is the newest of the major sub-systems. The booster system had one relay fail to an unsafe state. The statistics are too low to compare failure results between the older relays and the newer Booster relays to see if aging causes greater failures to an unsafe state in the older relays. Four of the relay failures to an unsafe state were detected during the interlock functional testing and the other five were detected during operations. Three of the failures to an unsafe state were caused by water damage (these were detected during operations).

The components classified as other include various miscellaneous components of the access control system. The failures to an unsafe state were two sticking air solenoids on beam stops. These occurred during system testing.

A simple calculation would suggest that the components have a failure rate to an unsafe state of approximately 1300 years. If the five caused by water damage are removed form the statistics then the rate becomes 2000 years.

CC: D. Meany
N. Williams
From RSC Chair File

Building 701
P.O. Box 5000
Upton, NY 11973-5000
Phone 631 344-4211
Fax 631 344-7630
musolino@bnl.gov

BROOKHAVEN
NATIONAL LABORATORY

managed by Brookhaven Science Associates
for the U.S. Department of Energy

Memo

date: *September 14, 2000*

to: *K. Brog*

from: *S. Musolino*

subject: *RPWG Meeting 00-6, August 30, 2000*

In attendance 00-6: T. Dickinson, W. Gunther, P. Jones, H. Kahnhauser, R. Karol, S. Layendecker, R. Miltenberger, S. Musolino, A. Queirolo, D. Schlyer, P. Williams

Others present: K. Carney, R. Karol

1. ***Proposal by K. Carney to add waste management training to contamination control training.***

It was proposed that a few overheads be added to RWT-300 to address proper disposal of waste and prevention of adding mixed waste to radioactive waste. The training would be at the awareness level and not qualify personnel to categorize waste. It was noted that the challenge exams and other related documentation would also have to be revised.

The Working Group recommends approval of the proposal.

2. ***CAD Proposal on Interlock Testing***

In the attached memorandum, the Collider Accelerator Department requested a change in the BNL RadCon Manual on the frequency of interlock testing. It should be noted that such a change would require a revision to ES&H Standard 1.5.3 prior to a modification of the RadCon Manual, which is a Program Document. This is an administrative point that has no impact on the technical question.

All but one member the Working Group in attendance, A. Queirolo, voted against making a recommendation that the Assistant Laboratory Director approve the proposal in its current form. The Working Group requests the proposal be resubmitted after considering the following topics discussed at the meeting:

- In a redundant interlock system, the reliability of the system against failure of both chains of protection by faults, which can be detected by test, is proportional to the frequency of testing.

- Tom Dickenson noted that based on experience at the NSLS during the first 11 years of operation when about 50 independent access control systems were in operation (with a total of about 75 interlocked doors, 75 beam stops and other critical devices, and 2000 relays), there were 11 unsafe single failures detected during test. There were no redundant failures, and hence no personnel placed at risk. Using that failure rate, a six-month testing interval, and the current inventory of 65 access control systems, it was calculated that a double failure would occur on average once every 70 years at the NSLS. With operational experience and improved QA, the current estimate of the failure rate is about 3 times less. This rate is much greater than the life of the facility and thus achieves the level of risk expected by DOE.

- There was general agreement that the RHIC PASS should have a reliability as good or better than the NSLS access control systems, but based on observations and information on the older AGS interlock system from over the last 10 years ago, there was much less confidence in the relay-based system.

- Lessard cited seven failures that resulted in DOE Reportable Occurrences in 13 years with respect to the relay-based access control system at the AGS, and pointed out that few of these would have been prevented by testing. He argued that since testing is of limited importance, doubling the required interval is justified. The Working Group did not find that the DOE Occurrences alone support that conclusion. An additional set of data is also needed on failures of protective functions discovered during interlock tests and routine maintenance. The statistics on lower level failures are superior predictors catastrophic events in complex systems. Steve Musolino pointed out that these data are being collected by procedure in RHIC/AGS OPM 4.91. Ray Karol was requested to research that data on PASS, as well as any similar data on the AGS relay-based system.

- An alternative approach that CAD might consider is to develop a different strategy towards functional testing that makes the task less time consuming, and modular so as to cover only one segment or aspect of the accelerator complex at a time. This allows testing to be carried out during periodic maintenance periods instead of waiting until annual shutdowns.

Electronic attachment: Memo, E. T. Lessard to S. Layendecker, "Request for Rule Change on Six-Month Testing of Interlocks," April 20, 2000.

3

Acrobat Document

cc:	RPWG	R. Osgood	T. Fryberger
	M. Bebon	B. Sack	T. Sheridan
	T. Kirk	S. Ozaki	M. Schlender
	M. Lynch	P. Paul	N. Volkow

BROOKHAVEN
NATIONAL LABORATORY

Building 911
P.O. Box 5000
Upton, NY 11973-5000
Phone 631 344-4250
Fax 631 344-5954
Lessard@bnl.gov

managed by Brookhaven Science Associates
for the U.S. Department of Energy

Memo

date: *Thursday, April 20, 2000*

to: *S. Layendecker*

APR 2 0 2000

from: *E. T. Lessard* ETL

subject: *Request for Rule Change on Six-Month Testing of Interlocks*

With regard to extending the testing period at the end of a six-month interval, such as using an extension period similar to that in use at BNL, we feel the Laboratory should not establish any rule that unduly impedes the operation of a facility and then has to be amended in order to work. The National Commission on Radiological Protection (NCRP) weighs in directly on this issue and states that: "the system should be tested periodically; the frequency should be related to the complexity and demonstrated reliability of the access control system or alarm system, but it should be done no less frequently than once per year."[1]

NCRP indicates the weakest link in any system of personnel protection is not the hardware but the people themselves. The single leading cause of accidents according to NCRP 88 is the failure of personnel to follow established procedures. This is somewhat evinced by my experience at the AGS in which personnel were inside accelerators twice in the last 13 years when the accelerator's access control system was reset for operation. Fortunately, the accelerators were not operated at those times.

The Linac, AGS, Booster and TVDG access control systems consist of electro-mechanical relays interfaced with position sensors that detect open or closed gates, radiation sensors that detect abnormal levels of radiation and micro-switches that denote the position of beam stops. For Very High Radiation Areas where interlocks are required, any combination of two independent relays, two independent sensors or two independent micro-switches, which protect any single location, must fail unsafely in order to allow exposure to high levels of radiation. It is apparent from failure rates listed below equipment failures are not common. The risk of failure due to faulty equipment is not going to be significantly reduced with twice per year testing as opposed to annual testing.

IEEE Standard 500-1977

Reliability Data, Recommended Values for Failure Rates

Part	**Failure Rate, All Modes, y^{-1}**
Relays	8.7×10^{-8}
Low Power Control and Instrumentation Switches	1.7×10^{-7}
Displacement Sensors	2.8×10^{-6}

[1] NCRP 88, Radiation Alarms and Access Control Systems, 1986.

In the last 13 years, there were seven occurrences at AGS related to access control system (ACS) hardware:

1) an ACS interlock was improperly jumpered,
2) an intrusion alarm was improperly wired into the ACS,
3) a wire was improperly removed from an ACS relay,
4) an un-powered device connected to ACS was worked on while the ACS was energized,
5) a bypass was installed but ACS bypass paperwork was not properly completed,
6) an ACS lighting circuit was worked on by electricians without proper authorization, and
7) an ACS beam-plug drive-controller was improperly plugged into a power strip instead of an ACS relay chassis.

Of these, only two occurrences were detected during testing. They were number 3, improper removal of a wire from an ACS relay, and number 6, an ACS lighting circuit worked on by electricians without proper authorization. The ACS lighting-circuit occurrence happened following a beam-line modification. Following any beam-line modification, the ACS is always tested upon re-start. Thus, annual versus twice per year testing has no bearing on detection of an occurrence of this type. Regarding occurrence number 3, testing occurred following an accelerator shutdown. The removal of the wire had to occur during the shutdown period as the ACS will not allow reset for beam unless ACS circuits are energized. One may conclude annual versus twice per year testing would not be relevant in this case.

Of the remaining five occurrences, twice per year testing had no bearing since they happened after a test was passed, or they could not be detected by an interlock test.

The U-line, V-line, ATR line, g-2 ring and RHIC access controls are PLC-based systems that interface with position sensors that detect open or closed gates, radiation sensors that detect abnormal levels of radiation and micro-switches that denote the position of beam stops. In addition, the g-2 and RHIC rings have sensors that detect an oxygen deficiency hazard due to the presence of helium in these areas. The PLC-based systems are redundant and independent, and both must fail unsafely in order to allow exposure to high levels of radiation. The risk of failure due to faulty equipment in a PLC-based system is not significantly reduced with twice per year testing as opposed to annual testing.

For the past three years, there has not been an occurrence related to the unsafe failure of a PLC-based system. There have been instances where the program in the processors became corrupted, due to outside interferences. In each case the system shutdown into a safe state.

Finally, it is planned that the Collider operates 37 weeks per year. The draft Guidance to the Accelerator Safety Order, DOE 420.2, indicates:

5. Testing of Interlocks

a. Testing (i.e., validation that the system works as designed under conditions of use) should validate the interlock system at least annually. An interlock system should not be used to provide protection unless it has been validated within the specified testing period. A short grace period could be allowed if specified in the administrative procedures. A successful testing program will depend on a system design, which

accommodates testing and the commitment of machine time and resources to accomplish the tests. Testing intervals should also take into account the system reliability and the overall reliability design goal as specified by the probability of the protective electronic system to fail on demand of a safety challenge.

b. A functional test should also be completed after modification or maintenance work is done on an interlock system. Those maintenance and service actions, which are deemed to be trivial and which do not require functional testing, could be identified and justified generically or individually.

Based on the preceding rationale, the staff of the C-A Department feels the BNL RadCon Manual rule is best stated as follows:

"The test shall be performed every 12 months with a maximum extension of 3 months between any 2 consecutive tests. A functional test should also be completed after modification or maintenance work is done on an interlock system."

* * *

Copy to:

D. Beavis
A. Etkin
R. Karol
D. Lowenstein
S. Ozaki
C. Schaefer
N. Williams