CONF-970134--9

LA-UR- 96-3568

Title: LANSCE Radiation Security System (RSS)

Author(s): Floyd R. Gallegos

Submitted to: Health Physics Society 1997 Midyear Topical Meeting
San Jose, CA

Los Alamos
NATIONAL LABORATORY

LANSCE Radiation Security System (RSS) *

Floyd R. Gallegos
Los Alamos Neutron Science Center,
Los Alamos National Laboratory,
Los Alamos, NM 87545 USA

Abstract

The Radiation Security System (RSS) is an engineered safety system which automatically terminates transmission of accelerated ion beams in response to pre-defined abnormal conditions. It is one of the four major mechanisms used to protect people from radiation hazards induced by accelerated pulsed ion beams at the Los Alamos Neutron Science Center (LANSCE). The others are shielding, administrative policies and procedures, and qualified, trained personnel.

Prompt radiation hazards at the half-mile long LANSCE accelerator exist due to average beam intensities ranging from 1 milli-amp for H^+ beam to 100 micro-amps for the high intensity H^- beam. Experimental programs are supplied with variable energy (maximum 800 MeV), pulse-width (maximum 1 msec), and pulse frequency (maximum 120 Hz) ion beams.

The RSS includes personnel access control systems, beam spill monitoring systems, and beam current level limiting systems. It is a stand-alone system with redundant logic chains. A fault of the RSS will cause the insertion of fusible beam plugs in the accelerator low energy beam transport.

The design philosophy, description, and operation of the RSS are described in this paper.

Introduction

There are three major beam interlock systems at LANSCE, the Radiation Security System (RSS), the Run Permit System (RP), and the Fast Protect System (FP). See Fig. 1. When faulted these systems prevent particle beam creation or transmission. The RSS is a personnel protection safety system. As such, the operation and maintenance of this safety system are strictly controlled. The RP and FP provide equipment protection and serve to limit beam conditions to levels below the threshold of RSS faults. Since these systems are not involved in personnel safety a graded approach is applied to operation and maintenance requirements.

Beam Interlock Systems at LANSCE provide the following functions:

- provide protection for personnel
- provide equipment protection from beam induced damage
- provide a means to prevent exceeding general area radiation level thresholds
- minimize component activation due to primary beam spill (maintenance and ALARA concern)
- provide verification of proper equipment line-up and status for various modes of operation
- provide warning indication of possible reduction of protection in other beam interlock systems
- limit beam conditions below fault thresholds of the personnel protection system (challenges)

The RSS includes personnel access control systems, beam spill monitoring systems, and beam current level limiting systems. It is a stand-alone system which has redundant RSS-only inputs. The system may provide inputs to the other interlock systems. However, this interaction is diode-

* Work supported by the U.S. Department of Energy

like since it is permitted in only one direction, e.g., from the RSS to the Run Permit (RP) and Fast Protect (FP). A fault of the RSS will cause the insertion of fusible RSS-rated beam plugs in the accelerator low energy beam transport.

The RSS incorporates the following functions and subsystems:

- Shielding, Shielding Integrity
- Logic and Wiring
- RSS Backbones, relay logic, area 'safe' circuitry
- RSS Fusible Beam Plugs
- Dual-use Beam Plugs - Run Permit mode beam plugs with RSS rated in-limit switches
- Personnel Safety Systems (PSS) and Personnel Access Control Systems (PACS) - access control systems
- Beam Current Limiters (XL)
- Gamma Detectors (GD)
- Administrative Policies and Procedures

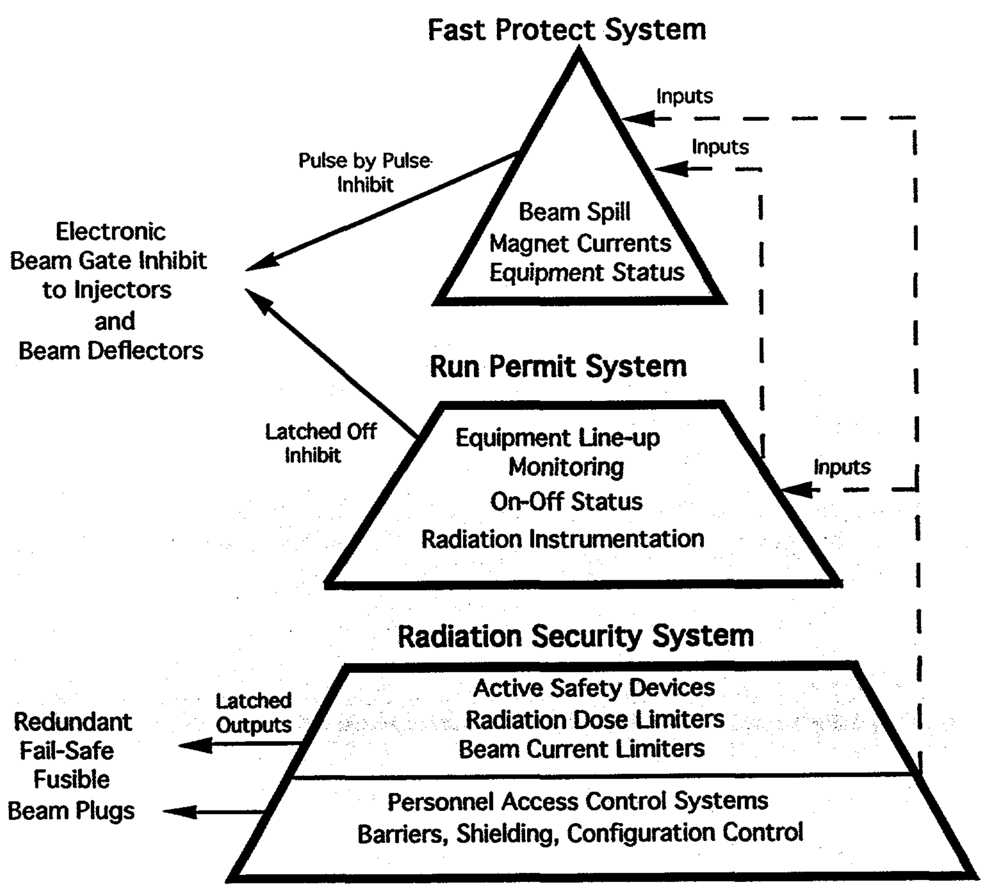

FIGURE 1. LANSCE Beam Interlock Systems.

Definitions

To improve understanding of the following report, it is necessary to define commonly used terms.

Challenge -- A challenge is the act of allowing conditions to exceed the RSS trip threshold. This results in activation of the safety system. Layered beam interlock systems are used to minimize the possibility of a safety system fault. For example this can be accomplished using other beam interlock systems to limit beam conditions below the fault threshold of the safety system. The Ion Chamber System (IR) and Activation Protection System (AP) respond to radiation levels produced by errant beam. These systems provide input to the Fast Protect System. They are set to trip at lower levels than the Gamma Detectors (GD) which input to the Radiation Security System, a personnel protection system.

Fail-safe -- System works as designed, or with any single failure works properly, works with more sensitive threshold, or shuts off beam. In the design of fail-safe devices, the device should be self-checking and where it is not feasible to accomplish this the circuitry must be redundant.

RSS-rated -- Subject to the requirements of the LANSCE Radiation Security System Quality Assurance Plan for design, procurement, inspection and acceptance testing, operation, maintenance, and calibration. (See Critical RSS Circuitry.)

RSS Beam Plugs -- Beam plugs (BL) or beam stoppers which provide the primary protection for the Radiation Security System. These plugs are RSS-rated.

Dual-use Beam Plugs -- Beam plugs (BL) or beam stoppers which provide RP and RSS functions. These devices are inserted or withdrawn to make up modes of accelerator operation. They also have RSS-rated in-limit switches which provide information to the RSS on their status. This information is used to determine "safe" status for downstream areas. For example, when an area's redundant beam plugs are inserted and their RSS in-limit switches are closed the RSS does not monitor downstream RSS components.

Safe Circuitry -- Circuitry and components which determine the conditions necessary to make an RSS controlled area "safe" for entry (bypasses the "secure" personnel access control system requirement). They shall be treated as RSS circuitry for the purposes of interlock control. Examples of circuitry and components used to establish "safe" conditions are experimental cave entry allowed or cave safe wiring, contacts, and relays, and beam plug in-limit switches and magnet status monitoring devices when incorporated as part of the experimental cave entry or cave safe circuitry.

Critical RSS Circuitry and Components -- Circuitry and components whose common characteristic is that if they fail or are bypassed, the ability of the RSS to provide the required protective beam shutdown functions is compromised, diminished, or defeated. (See RSS-rated.)

Supervisory RSS Circuitry and Components -- This circuitry may control the status and warning indications. It is also circuitry that prevents challenges to the critical safety functions of the RSS. Examples of this type of circuitry are key release circuitry, beam plug ready circuitry for dual-use beam plugs, and circuitry and components that enforce administrative sweep requirements (sequenced resets, time delays on horns, flashing lights, de-energizing lights, etc.). Supervisory functions are also hardware functions which backup administrative procedures for required personnel actions.

Status and Warning Circuitry and Components -- Status and warning circuitry and components give operators and other users information about the state of the RSS. Failure of a status or warning signal may cause confusion and misunderstanding, however it does not result in a loss of protection.

Fixed Barriers and Shielding -- Barriers and shielding which are part of the accelerator structure and not easily modified. Examples are beam tunnel walls, building walls, buried shielding, and natural barriers.

Movable Barriers and Shielding -- Barriers and shielding which can easily be removed or modified. Examples are shield blocks, fences, gates, and doors.

RSS Design Requirements

As an engineered safety system the overriding concerns in the design of the RSS are as follows:

- Fail-safe implementation or redundancy where fail-safe implementation is not practical. As an engineered safety system it is important that hardware failures do not compromise safety. Although failures are unavoidable, we try to design components such that they fail in a safe condition or utilize redundancy to ensure the full system is not compromised.
- Simplicity of design. Reducing the complexity will improve system understanding and ease of maintainability and testing.
- Reliability of design. Reliability develops operational trust in the system by minimizing the number of false alarms. Operators should feel that a trip of the system is a true fault and not a failure of the hardware.
- Integrity of critical elements of the system (configuration control). The system should be isolated to provide well-defined boundaries which lend themselves to configuration control.
- Quality of materials and workmanship. Improving the reliability and reducing the number of hardware failures are directly correlated with high quality, conservatively rated, materials and workmanship.
- Ease and completeness of testing. Since a complete fail-safe system is cost prohibitive and may be impossible to achieve, we must rely on frequent and complete testing to establish confidence that the system will respond as desired. The design of the system should accommodate testing from the sensors to the final trip actuation.
- Ease of maintenance and fault diagnosis.
- Use of the graded approach to system management.
- Designed to incorporate lessons learned from operational experience in order to mitigate injury to personnel. An important aspect is obtaining system requirements from personnel experienced in the operation.
- Compliance with DoE Accelerator Safety Order and Laboratory Standard LS107-01.

RSS Circuitry and Component Graduations

A philosophy of grading circuitry and components in the RSS has been developed. Differentiation in failure of status and warning, supervisory function, and critical circuitry and components is clarified in the following discussion. Using a graded approach, actions taken for failure of the three types of circuitry differ due to a difference in the consequences of failure. As such, corrective actions depend on the placement of components and circuitry in one of these categories.

Status and warning circuitry and components give operators and other users information about the state of the RSS. Failure of a status or warning signal may cause confusion and misunderstanding, however it does not result in a loss of protection. Some of these non-interlocked administrative warning signals are more important than others. For example, the failure of the audio or visual warnings used after a sweep of the personnel access control area is considered to be more important than a burned out lamp on a remote indicating panel or a computer indication.

Supervisory functions like status and warning indications are not directly coupled to the protective functions of the system. This circuitry may control the status and warning indications. It is also circuitry that prevents challenges to the critical safety functions of the RSS. Examples of this type of circuitry are key release circuitry, beam plug ready circuitry for dual-use beam plugs (see definitions), and circuitry and components that enforce administrative sweep requirements (sequenced resets, time delays on horns, flashing lights, de-energizing lights, etc.). Supervisory functions are also hardware functions which backup administrative procedures for required personnel actions. For example, personnel sweeping an area are required by procedure to ensure that the area is clear by a complete visual examination. Sweep reset buttons are a hardware means to ensure the sweeper visits all areas of concern. However, final responsibility for the performance of the sweep is dependent on the trained individual and hardware cannot enforce this. The goal of supervisory hardware is to reduce the probability of the failure of a personnel sweep due to area complexity, inadvertent failures to follow procedures, and/or procedural errors.

Critical circuitry and components have a common characteristic, that being if they fail or are bypassed, the ability of the RSS to provide the required protective beam shutdown functions is compromised, diminished, or defeated. Therefore they are directly coupled to the performance of the safety function. For example, access control gate switches and circuitry are critical components, since failure of the personnel access control system to detect the opening of a perimeter gate would be a loss of a safety function.

RSS Description and Operation

Backbone, Logic and Wiring

The basic RSS logic is simple. At the critical circuitry and components level it is fully redundant hardware (relay ladder logic and wiring). The newly designed Personnel Access Control System uses programmable logic controllers (PLC) at the supervisory, warning, and status level of circuitry. Software implementation is also required for computer indication and the various RSS status screens. All protective functions are implemented in hardware only. The logic is primarily located in LANSCE Standard indicator relay modules installed in NIM chassis in locked instrumentation racks. Cabling is installed in trays, armored cable, or conduit. All junction boxes where terminations are accessible are locked.

The RSS consists of redundant logic strings called "RSS Backbones". The Linac Backbone runs the length of the accelerator from the beam switchyard to low energy beam transport. At the switchyard, three redundant logic strings branch out to the experimental areas (Line A Backbone, Line D Backbone, and Line X Backbone). These backbones provide inputs to the Linac Backbone which then interfaces the RSS control of the RSS-rated beam plugs (01BL02 and 01BL03) at the low energy entrance to the first Linac accelerating cavity. Test circuitry is provided to test the operation of the Linac, Line A, Line D, and Line X Backbones. Frequent testing is performed according to the administrative requirements of the Operations Manual. Visual verification of beam plug operation at the beam line is also required prior to each operating period. See Figures 2 and 3.

Each RSS subsystem device (PSS, PACS, XL, GD) supplies a normally open contact (redundant fault channels) to each of the redundant backbone strings. If all systems are ready, relays are energized at the low energy transport allowing the automatic withdrawal of the RSS beam plugs (air-driven). Each plug is controlled by one leg of the Linac Backbone. If an RSS subsystem faults the corresponding relay de-energizes causing the insertion of the RSS beam plug.

The RSS logic also provides for operating the accelerator in various line-up modes while maintaining safety requirements. The insertion of beam plugs defines the modes of operation. Insertion of RSS-rated beam plugs (14BL02 and 14BL03) in the Linac allows operation at 211 MeV with access to downstream areas of the Linac and Experimental Areas. The in-limit switch contact of each plug shorts across its respective backbone, thus bypassing all RSS downstream requirements. Similar actions take place by insertion of Line A, Line D, and Line X dual-use beam plugs for other modes of operation. The RSS logic also provides an isolated contact in the "beam plug ready" circuitry of dual-use plugs. For example, a fault of the Line D Backbone will cause a loss of the beam plug ready for LDBL01 and LDBL02 and they will automatically be inserted.

An RSS Inhibit Switch provides means to lockout RSS so that the system will not be made up regardless of the state of the downstream logic. For example, if the RSS has not been operationally verified downstream of the 211 MeV beam plugs, one needs a way to prevent operation to downstream areas if these plugs are withdrawn. The Inhibit switch provides this capability. Inhibit switches are located in the Sector C and Switchyard equipment aisles.

Inputs to the RSS backbone from designated personnel access systems may be bypassed by logic. This logic is called "safe" circuitry. This logic determines the conditions necessary to make an RSS controlled area "safe" for entry. It is treated as RSS circuitry for the purposes of interlock control. See Definitions.

Access to all RSS hardware is controlled by lock and key. Authorization by the RSS Engineer or designate is required to release the key. A database for RSS configuration control locks locations has been established.

RSS Beam Plugs and Dual-Use Beam Plugs

RSS-rated beam plugs (also called fusible beam plugs) are designed to be fail-safe. These plugs may either be automatically controlled by the RSS, as in the case of redundant plugs in the LANSCE low energy beam transport (01BL02 and 01BL03), or they may be manually controlled, as with the beam plugs at 211 MeV (14BL02 and 03). If downstream protection is compromised, the plugs in the LANSCE low energy transport are automatically inserted. See Figure 3.

The personnel protection feature of RSS plugs is implemented by using a 'fuse' concept. The beam plug upstream face has a thin plate of stainless steel which will melt through if impinged by beam. The steel plate forms one wall of a cavity with the other walls being formed by a copper beam stop. Two pipes extend from the cavity to the atmosphere. If beam hits the plug, the plate will burn through allowing atmospheric pressure into the evacuated beam line. Beam will not transport at atmospheric pressure due to collisions with gas atoms. The RF cavities will also not accelerate beam since loss of vacuum will also trip the RF amplifiers. Thus beam will not be transmitted or accelerated removing the source of the prompt radiation hazard. On loss of air or electrical power the plugs will insert due to gravity. These plugs also have specially designed position limit switches to reliably indicate their state. See Figure 4. (See paper on fusible plugs presented at this Conference.)

The RSS beam plugs provide personnel protection and are part of the engineered safety system. To provide this protection it is necessary that they insert when the RSS is compromised. Non-safety equipment protection interlock systems are used to prevent damage to the inserted RSS plugs. Since damage to these plugs would require their replacement and loss of vacuum would also require considerable downtime for recovery, the Run Permit and Fast Protect Systems, "vacuum valve ready" circuits, and the "beam plug ready" circuits for 01BL01 and 14BL01 provide protection for RSS beam Plugs on a trip of the RSS. Recovery time from a trip is primarily due to the time required to investigate the cause and ensure conditions are safe to continue operation.

Dual-use beam plugs, as the name states, serve dual functions. They provide Run Permissive operating modes and physically isolate downstream beam transport areas for entry and maintenance (personnel safety function). As such, they provide inputs to the RSS when inserted to certify safe conditions. These are standard plugs without burn-through protection. Each area has a set of redundant plugs. Specially designed (high reliability) RSS-rated in-limit switches provide information to the respective RSS backbone on the status of the plugs. In this case only the in-limit switches, actuating hardware, and wiring are considered part of the RSS. Other components of the beam plug are treated as run permit or as only serving an indication function. Redundant plugs or a beam plug and an alternate equivalent means to prevent beam transmission are required to establish "safe conditions."

In cases where plugs are used to satisfy dual functions, run permit and RSS, they exist in pairs to adequately stop the beam and meet redundancy requirements of the RSS. Individually these plugs may not be designed to continuously stop the beam. These plugs are protected from inadvertent impingement of the beam by other systems designed to protect equipment, such as run permit and/or fast protect. Present plans are to provide backup RSS-rated protection for beam plugs with RSS in-limit switches which do not have burn-through protection. This will be accomplished by installing RSS-rated plug watcher radiation detection (GD) which will trip the upstream RSS if beam impingement is detected.

Since pairs of plugs actuate, the position states of the pairs of beam plugs should agree. Differences could indicate a failure of an RSS in-limit switch. To warn the operator of such a condition the states of the in-limit switches are monitored by the Fast Protect System. While the implementation of this status check is not in the RSS, such a check is a clear enhancement as a supplement to the periodic operational checks.

Personnel Safety Systems (PSS) and Personnel Access Control Systems (PACS)

The PSS and PACS are used to control access to areas of prompt radiation hazards due to accelerated beam and in some cases access to areas where high voltage hazards exist. The PSS is the original accelerator access control system which has had numerous modifications over the past twenty years. As a result of lessons learned and the necessity to upgrade the access control system to meet requirements of the DoE Accelerator Safety Order and the Laboratory Standard for Accelerator Access Control Systems an upgraded system (PACS) was designed.

The PSS and PACS provide redundant isolated fault contacts to the RSS backbones for each area being controlled. The PSS is not a fully redundant system and in many cases relies on single strings to provide protection. The Kirk key and key release system provide the redundant barrier to access. The PACS is a fully redundant system. Therefore, in the case of the PACS, the Kirk key and key release system prevent challenges to the access control system. (See paper on PACS presented at this Conference.)

LANSCE Current Limiter (XL)

The Current Limiter (XL) is designed to limit beam current to a specific level at a designated location in the beam line. The device is basically a current transformer with associated electro-magnetic (EM) shielding and electronic circuitry.

The function of the current limiter is to ensure that average current in a beam line is maintained below a desired level. This will effectively limit the magnitude of a spill problem due to mis-steered beam or, if the beam is well-tuned, limit the radiation levels at the beam dumps. The present minimum trip level was determined by hardware noise considerations. The current limiter incorporates various design schemes to provide the assurance of a "fail safe" protection instrument.

The XL is a self-contained unit which continuously (non-gated) monitors beam current. Redundant isolated contacts provide fault information to the Radiation Security System (RSS). Presently there are six units in service. (See paper on XL presented at this Conference.)

Fail-Safe Ion Chamber Errant Beam Detector (GD)

The GD is an ionization chamber based radiation detection device. The ion chamber is a closed, pressurized vessel that detects ionizing radiation by collecting the ions formed by the radiation. The output current is proportional to the incident radiation dose rate. The detector is a cylindrical ion chamber rigidly fixed to the walls of the experimental areas to provide overlapping coverage with other units in the system.

The GD system consists of the ion chambers, their power supply, and the ion chamber current monitor modules. The ion chamber current monitor consists of the current monitoring, the testing-trip-levels, and the fault trip circuitry. These modules are installed in an electronics instrumentation rack.

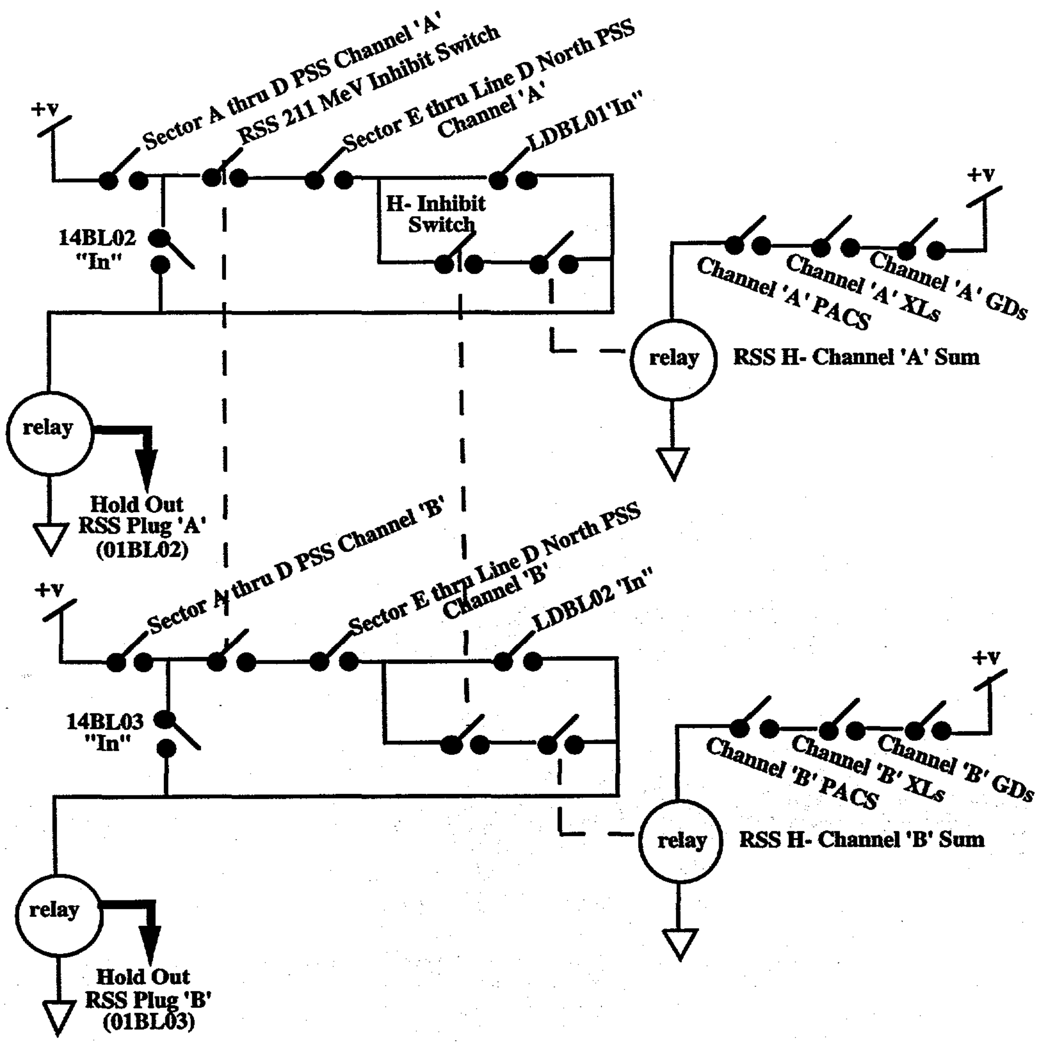

FIGURE 2. Schematic representation of Linac and Line D RSS Backbones.

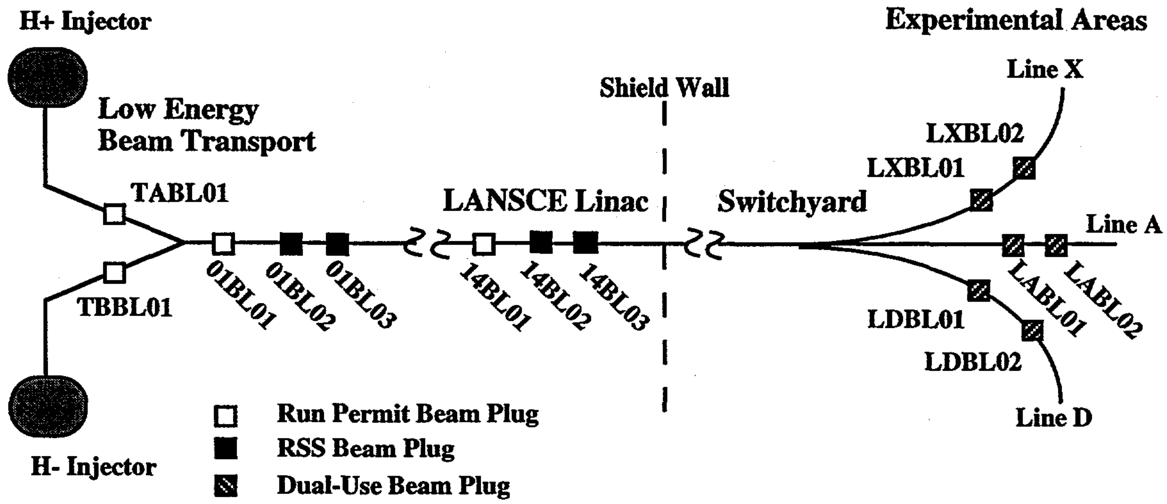

FIGURE 3. LANSCE Accelerator Beam Plugs.

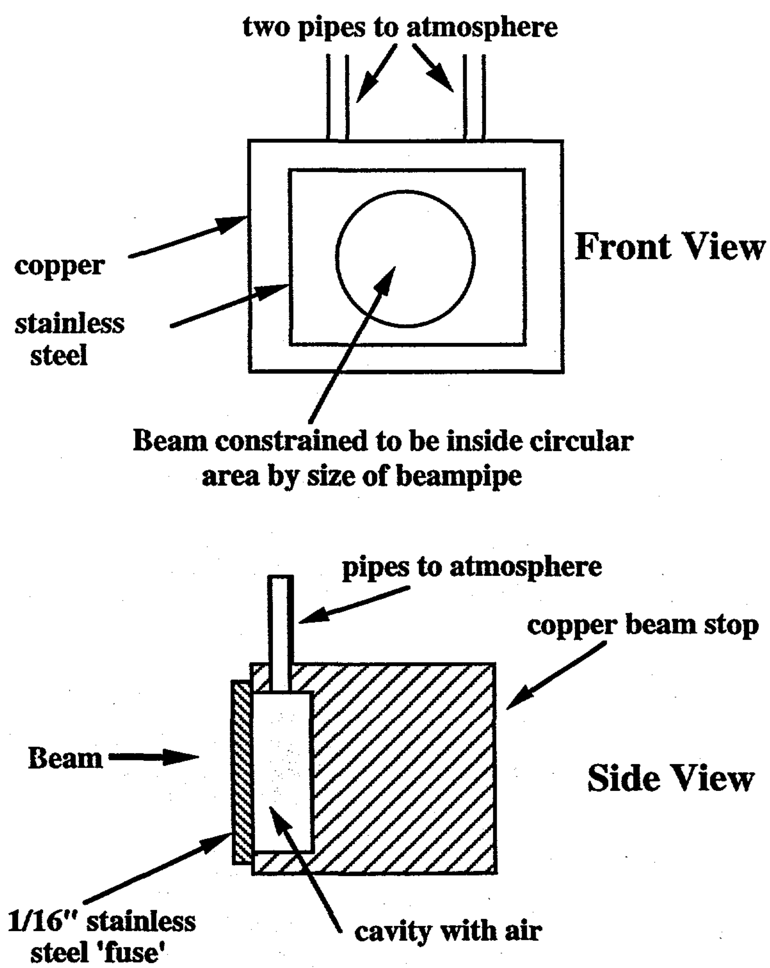

FIGURE 4. Schematic representation of RSS Fusible Beam Plug.

Shielding

Shielding is the primary passive component used to minimize prompt radiation levels. Evaluation of installations and modifications of the shielding barriers is a critical part of radiation security. In many cases shield blocks form the perimeter of the RSS and act as barriers to areas under RSS access control.

When operating, movable RSS shielding barriers are either posted as personnel access control perimeters or an alternate means of preventing a change in configuration is used; for example, the use of lock and tag or the integration of the shielding perimeter into the personnel access control system by using attached redundant barrier wires. If posting is used, then provision for verifying the labeling of these barriers is accounted for prior to beam operation in the area coming on-line. Configuration of this shielding must be controlled. Authorization for removal or modification of fixed or movable shielding must be designated and provision for differences of authority during facility operating or maintenance periods must be accounted for. During operation, modifications to the shielding configuration require a documented review of the possible impact to radiation safety. This is normally handled through the LANSCE Operations Safety Committee (LOSC), an arm of the Radiation Safety Committee (RSC).

Where bulk shielding is not adequate to reduce radiation levels to acceptable levels during accident conditions, other RSS devices as determined by the LOSC are required to provide sufficient safety margin to mitigate the hazards.

Administrative Policies and Procedures

Administrative policies and procedures are an important part of the operation and configuration control of the RSS. Reviewed testing procedures ensure a process is followed to verify proper operation of the safety system. Procedures establish consistent methods for entering and sweeping personnel access control areas and for addressing RSS hardware failures. Responsibilities and authorization paths are established by RSS policies. These procedures and policies are maintained in the Operations Manual. Training requirements, maintenance procedures, quality assurance plans, modification control requirements are being established and will reside in the RSS Systems Manual.

Summary

The Radiation Security System and its components have proven to be reliable. The safe operation of the facility depends on the proper response of the RSS. The system has evolved and standards have been developed. A recent external review of the RSS and PACS systems looked at compliance with the DoE Accelerator Safety Order. The reviewers agreed that requirements have been met. Suggestions for improvement were provided and are being implemented. The bottom-line is that the system has performed its job well and is undergoing a continual process of internal review.

Acknowledgments

The author would like to acknowledge the efforts of the RSS Team, the Beam Delivery Team, the Operations Physics Team, and the LANSCE Operations Safety Committee in the design, implementation, and maintenance of the present LANSCE Radiation Security System.