JLab VTA Personnel Safety Interlock Systems Requirements

Revision – 2.0

July 19, 2002

Prepared by the Jefferson Lab Safety Systems Group.

Table of contents

1 Introduction ____ *1*

2 Scope ____ *1*

3 Intention ____ *2*

4 Background ____ *2*

5 Responsibilities ____ *2*

6 References ____ *2*

7 Assumptions ____ *3*

7.1 No ODH system Required ____ **3**

7.2 Prompt Ionizing Radiation Sources ____ **3**

7.3 Prompt Ionizing Radiation RF Threshold ____ **3**

7.4 Non-Ionizing Radiation Hazards not Interlocked ____ **3**

7.5 No extra-VTA RF sources ____ **3**

7.6 Operational Assumptions ____ **4**

8 Functional Requirements ____ *4*

8.1 Operational Requirements ____ **4**

8.2 Area Radiation Monitoring ____ **5**

8.2.1 Alarm Function ____ 5

8.3 Dewar Radiation Monitoring ____ **5**

8.3.1 Alarm Function ____ 6

8.4 RF System Interface ____ **6**

9 Operator Interface ____ *7*

10 Configuration Control ____ *8*

11 Testing/Quality Assurance ____ *8*

12 Documentation ____ *8*

13 Non Safety System Functions ____ *9*

14 Hazard Analysis ____ *10*

15 Revision History ____ *11*

1 Introduction

The vertical test area (VTA) is used to test superconducting RF and other cryogenic components used in the production of accelerating structures. There are eight separate test units, designated "Dewars" 1-8. Dewars 1 and 2 are designed for low power testing of small components. Dewars 7 and 8 are designed for standard high power testing such as RF prototype and production tests. Dewars 4 through 6 are designed for reconfigurable high power RF tests required for research and development. Dewar 3 may be used with either the standard or reconfigurable RF systems, however it is not deep enough to accommodate the CEBAF production cavity pairs. Dewar 5 has a large cross sectional area thus requiring a significantly larger amount of helium to cool the device under test. Due to limitations on the cryogenic helium supply volume and lack of requirement for the larger volume for tests such as with lower frequency cavities, this dewar has not been used frequently.

RF testing of superconducting components can generate significant amounts of prompt ionizing radiation. Dewars 3 through 8 are equipped with movable radiation shielding. The shielding is interlocked such that operation at high power is not possible unless the shield is closed. Each dewar is also equipped with a radiation monitor as a back-up to the shield door interlocks. If the monitor measures a prompt radiation rate above a limit set by the radiation control group when the shielding is not in place, the monitor will alarm and shut off the RF source.

All dewars are occasionally operated at low power with the radiation shielding in the open position. At this time, dewars 1 and 2 operate at low power only and shall not be used for tests that are known to be potentially capable of generating ionizing radiation. An additional radiation monitor will be added to ensure that any unexpected radiation generated by these test stations does not exceed radiological control guidelines.

The RF power level for dewars 3 through 8 is switched between low power (<1W) and high power (1W < P < 500W) by two methods. The standard RF configuration of dewars 7 and 8 uses both a high power and a separate low power amplifier. The outputs are selected using a remotely controlled high power RF switch. The reconfigurable RF systems of dewars 3 through 6 use an attenuator at the input of a single high power amplifier. The attenuator is switched between high attenuation (low RF power) and low attenuation (high RF power).

2 Scope

This document covers the requirements for the personnel safety interlock systems for the vertical test area (VTA) of the Jefferson Lab Institute for SRF Science and Technology. The VTA consists of the dewar facility, the Production Control Room, and the R&D control room. During VTA rf operations these areas are posted as radiologically controlled areas.

Safety interlock systems include engineered systems designed to protect people from hazards that arise as a direct result of facility operation. They may include: radiation interlocks, RF interlocks, and other interlocks that may be needed in the operation of the VTA RF systems.

This document does not address hazards associated with cryo system operation, high voltage devices other than RF system components, and mechanical shielding operation. Nor does it cover RF or ionizing radiation from sources located outside the VTA area.

3 Intention

The VTA is a test facility for a variety of SRF related products. As such, the types of device under test (DUT) will likely change over the lifetime of the facility. Flexibility should be designed into the safety systems to the greatest extent practicable. However this should not result in overdesign of the systems involved. It is the intent that the safety system be both flexible and cost effective.

4 Background

The vertical test area has been in operation for over 10 years. During this time, the area has undergone several modifications to add functionality and capability. In August 2001, an incident occurred in which one of the test areas was operated while the shielding was not in place. This led to a reevaluation of the interlock systems in place and the requirement to bring the systems up to current JLab standards. The current standards stem from the JLab EH&S Manual chapter 6311.

5 Responsibilities

The JLab Associate Director, Accelerator Division is responsible for accepting the risk of VTA operations.

The VTA personnel safety interlock system shall be owned by the JLab Safety Systems Group.

The VTA RF systems shall be owned by the JLab Institute for SRF Science and Technology. If RF systems are integrated for temporary tests, the JLab SRF institute shall assume responsibility that the RF system meets all requirements of this document and other JLab EH&S Manual requirements.

6 References

1. Vertical Test Area User Requirements, draft 10/26/2001
2. Vertical Test Area Facility Safety Systems Reference and Operational Guidelines (no Date)
3. JLab PSS Configuration Control Policy
3. CEBAF Production Cavity Testing System – Mk I
4. JLab EH&S Manual Appendix 6310-T2 “Prompt Radiation Control Policy”
5. JLab EH&S Manual chapter 6311 “Prompt Radiation Control”
4. IEC d61511 Electrical/Electronic/Programmable Electronic Safety Systems for use in the Process Control Industries (Guidance only)

7 Assumptions

The following assumptions are an integral part of the VTA PSS design and form the basis for the design decisions.

7.1 No ODH system Required

The VTA uses only helium in large quantities. No large quantities of liquid nitrogen are used within the VTA that would require the use of an ODH monitoring system.
The VTA area is not enclosed on any side with the exception of the floor. Any helium release will not have enough capacity to cause an oxygen deficiency condition (<19.5% O2 partial pressure).

7.2 Prompt Ionizing Radiation Sources

The only potential source of prompt ionizing radiation in the VTA is from operation of the RF components within Dewars 1-8.

7.3 Prompt Ionizing Radiation RF Threshold

For dewars 3 through 8, it is assumed that operation with RF power levels below 1W peak power will not result in production of prompt ionizing radiation in excess of JLab limits.
Dewars 1 and 2 may have medium power RF, e.g. 10W peak power, but the devices under test are not expected produce significant amounts of prompt ionizing radiation. A local area radiation monitor will be added to dewars 1 and 2 to verify that this is correct.

7.4 Non-Ionizing Radiation Hazards not Interlocked

Hazards arising from non-ionizing radiation are not mitigated by the personnel safety system described in this document. See the JLab EH&S Manual chapter 6420 for a description of non-ionizing RF radiation hazards and mitigation methods.

7.5 No extra-VTA RF sources

Only approved RF sources[1] located within the VTA test area and control rooms shall be used. Use of RF sources from outside the VTA[2] for temporary tests shall require a separate hazard analysis to be prepared by the petitioner and approval of the Safety Systems Group Leader. Continued use of any medium to high power RF source from outside the VTA shall require a separate review and approval by the Safety Systems Group Leader and the Institute for SRF Science and Technology Facilities Manager.

[1] See section 8.4 "RF Interface".
[2] This must be carefully considered. Using energy sources form outside the VTA removes cognizance of hazardous equipment operation from the immediate area of the VTA. This can lead to elevated risk and a requisite elevation in risk reduction requirements put on the PSS.

7.6 Operational Assumptions

The PSS design shall assume that during operations the VTA is staffed in accordance with the Vertical Test Area Facility Safety Systems Reference and Operational Guidelines (ref.2) The VTA PSS shall not be left unattended while VTA RF systems are operating at high power.

8 Functional Requirements

The JLab Vertical Test Area personnel safety system shall be designed to meet the requirements of the JLab EH&S policy and guidance on prompt ionizing radiation as outlined in the JLab EH&S manual chapter 6311.
The VTA PSS shall be designed using accepted good practice for systems of similar risk mitigation and complexity.
The VTA PSS shall be designed to meet a calculated probability of failure on demand[3] of $2x10^{-2}$ per year, e.g. safety integrity level (SIL) 2.
The VTA PSS should be designed to have a false trip rate of less than one per year.
No single point failure shall result in the ability to generate prompt ionizing radiation in excess of the limits set forth in the JLab radiological control manual.
The VTA personnel safety systems shall be designed for operation by a minimally trained technical staff.
All PSS interlock faults shall be latched by the personnel safety system until reset by a VTA safety system operator. Reset of faults shall only be allowed after the faults are cleared.

8.1 Operational Requirements

The VTA personnel safety system shall inhibit introduction of RF power greater than 1W peak into dewars 3 through 8 unless the respective dewar shielding is confirmed as in place.
If the operational state of the RF, e.g. low power/high power is inconsistent with the status indicated by the dewar shielding or radiation monitors, the personnel safety system shall completely shut off ALL RF power to ALL dewars.
The VTA PSS shall shut down RF power to dewars 1 and 2 if the dewar 1 and 2 radiation monitor alarms.
Dewars 3 – 8 shall be configurable to be able to operate with either a local high power amplifier or a remote high power amplifier switched to the dewar from the RF multiplexer switching system, located in the VTA test area. In either case, the PSS shall be able to disable high power RF operation into any dewar.

[3] Probability of failure on demand (PFD) is the probability during time *t* that the system is unavailable to perform the safety function when required. The time *t* is normally taken to be the test (certification) interval.

8.2 Area Radiation Monitoring

Area radiation monitors shall be selected and installed by the JLab Radiation Control group.

As a minimum, the area radiation monitors shall provide protection against prompt ionizing radiation (PIR) in occupied areas of the VTA and surrounding areas.

Area monitors shall be located as prescribed by the Radiation Control Group leader or his designee.

Placement of area monitors shall be documented by and fall under configuration control of the JLab Radiation Control group.

The type, e.g. photon or neutron, and level of PIR that will initiate an alarm shall be determined and controlled by the Radiation Control Group leader or his designee.

The type and placement of PIR area monitors should be selected to minimize false alarms.

8.2.1 Alarm Function

Area monitors shall initiate audible and visual alarms in the VTA work area and control rooms if the detected prompt radiation level exceeds the setpoint determined by the radiation control group.

Area monitors shall include redundant fail-safe contacts that will open upon alarm. If an area radiation monitor alarms, the PSS shall immediately shut off all medium and high power RF sources in the VTA.

All area monitor alarms shall remain latched in the alarm state until reset by an individual authorized by the radiation control group leader.

The alarm contact ratings shall be consistent with the design requirements of the safety interlock system.

Fail-safe functions of the PIR area monitors should not initiate audible and visual area alarms. A remote status indicator may be incorporated in the control room. However, for a fail-safe condition, the contacts to the SIS shall remain faulted (open).

8.3 Dewar Radiation Monitoring

Concern: To be able to operate with a minimally trained staff, audible and visual alarms should only be activated when the prompt ionizing radiation rate exceeds a set level. False alarms should be kept to a minimum.

Intent: It is the intent of the PSS group to specify an alarm interface that has separate contacts for "Monitor OK" and "Alarm" functions. In the event of a monitor failure (loss of Monitor OK), the PSS will inhibit high power RF operation, however it will not set audible and visual alarms.

Dewar radiation monitors are designed as an assurance that the radiation level generated by an unshielded operating dewar does not exceed JLab radiation control requirements. When dewar shielding is closed, the radiation monitor is used as a diagnostic only.

Dewar radiation monitors shall be selected and installed in each dewar by the JLab Radiation Control group.
Placement of dewar monitors shall be documented by and fall under configuration control of the JLab Radiation Control group.
The type, e.g. photon or neutron, and level of PIR that will initiate an alarm shall be determined and controlled by the radiation control group leader or his designee.
The type and placement of dewar radiation monitors should be selected to minimize false alarms.

8.3.1 Alarm Function

Dewar radiation monitors shall initiate audible and visual alarms in the VTA work area and control rooms if the detected prompt radiation level exceeds the setpoint, as determined by the radiation control group, when the shield lid is not fully closed.
Dewar monitors shall include redundant fail-safe contacts that will open upon alarm.
All dewar radiation monitor alarms shall remain latched in the alarm state until reset by an authorized individual.
The alarm contact ratings shall be consistent with the design requirements of the safety interlock system.
Fail-safe functions of the dewar monitors should not initiate audible and visual area alarms. A remote status indicator may be incorporated in the control room. However, for a fail-safe condition, the contacts to the SIS shall remain faulted (open).

8.4 RF System Interface

Concern: The safety system is only as good as the device used to control the energy source, in this case RF. This section includes stipulations about the approval and configuration control of these devices.
Intent: It is the intent of the PSS group to design a modular RF amplifier interface such that a safety envelope is maintained but the specific amplifier used may be changed to support test operations as needed. This would eliminate the need to tightly couple the RF amplifier interlock design to the PSS system.
The “safe” state of any RF source interlocked by the PSS shall be “OFF”.
Allowable “ON” states may include both low power and high power modes.
The interface between the PSS and any RF system shall fail to “Safe”.
The PSS shall shut off any RF system that is unsafe or indeterminate.
The RF inhibit chain shall be under safety system group configuration control.
The shutdown method must be approved by the safety system group leader or his designee. The method shall be consistent with the required safety integrity level (SIL) of the overall safety system.
At least two methods shall be used to inhibit each RF system capable of generating prompt ionizing radiation. Each of the two systems shall receive a separate permit from the PSS system.
The PSS interface to any RF control function shall be the final control element in the RF interlock chain.

All PSS control devices shall be capable of lockout-tagout using standard commercially available LOTO devices[4].
Off/Safe: All RF systems shall include a redundant fail-safe indication of the ON/OFF status of the respective RF system. The safety system shall use this information as verification of the RF permit logic.
The PSS RF system interlocks for all dewars shall include a modular connection method to facilitate routine reconfiguration of amplifiers and dewars.
The requirements specification for the modular RF interface shall be a separate document.
The personal safety system may include RF power monitoring as part of the high/low power verification. If RF power monitoring is used to verify the RF power level, it shall be designed to be as fail safe as practicable.
The PSS shall receive fail-safe independent redundant status signals from the RF power switching devices.
All RF amplifiers used for high power tests shall be reviewed by the safety systems group for compatibility with the VTA safety system. A list of qualified amplifiers shall be maintained by the VTA facility manager.

9 Operator Interface

The operator interface for the VTA PSS shall be centrally located.
Operator interface shall consist of:

- Status indicators for dewar interlock systems
- Status indicators for RF PSS interlock systems
- Status indicators for radiation alarm systems
- Fault reset switch
- RF Emergency shutdown switch in each control room and in the central RF amplifier rack.
- Audible fault alarm.

The operator interface should include:

- PSS System enable switch
- RF routing information
- Latched first fault indicators
- Separate fault reset switches for the standard and each of the reconfigurable RF and dewar PSS interlock systems
- Computer display of PSS status
- Logging of PSS alarms and faults

The operator interface may include:

- Remote computer display of PSS status
- Paging of VTA staff for a class of faults

[4] The PSS design should include the ability to disable the PSS interface to a device and still be able to maintain "equivalent protection and configuration control." This situation normally comes up during certification and when jumpers are required to support a specific test, removal of equipment, or unusual PSS configuration. Administrative lock and tag is the preferred method for accomplishing this task.

The operator interface should be simple and intuitive to a minimally trained VTA operator.

10 Configuration Control

All VTA safety system components and wiring shall be labeled.
All devices interfaced to the VTA PSS shall have PSS configuration control labels.
All VTA PSS components shall fall under JLab safety system group configuration control policy.

11 Testing/Quality Assurance

The VTA PSS shall be certified within a time period consistent with reducing the probability of an undetected unsafe failure of the system to less than 2 $x10^{-2}$ per demand however, no more than one year shall pass between certifications.
Certification shall include both static and functional tests.

All certifications shall be documented in writing. Documentation shall be maintained by the JLab Safety Systems group.
The VTA facility manager or his designee shall serve as the test director.

The VTA PSS design shall undergo at least one design review before installation. The chair of the design review panel should not be associated with the JLab SRF institute. The composition of the design review panel should include VTA users as well as technical experts from outside the JLab SRF institute. Findings and recommendations of the design review panel shall be documented, as well as the safety system group response to these items.

All components used in the VTA PSS design shall be evaluated for compatibility with the intended application and should be derated in order to minimize the stress that could lead to failure.

12 Documentation

Documentation shall include:

- Requirements Document
- Design documentation
  - System wiring diagrams
  - Equipment location drawings
- Design review documentation and disposition of action items
- Safety System operator user training

13 Non Safety System Functions

Non safety system functions should not be incorporated in the safety system design. However, ALARA functions may be incorporated if shown to be beneficial.

The following administrative functions are required to successfully maintain the required safety integrity level in the VTA but are not specifically part of the safety interlock system:

> Prior to every RF test in an unshielded dewar, the Principal Investigator shall estimate and document the maximum energy level that the test can produce. The test may only proceed in the unshielded dewar if the estimated energy level is below the limit set by the JLab Radiological Control Group.

Any test capable of producing an effective vacuum gap voltage of > 10kV must be documented and reviewed, and approved by the Radiation Control Group and the SRF Institute Director prior to implementation in an unshielded dewar[5].

[5] This requirement stems directly from the JLab EH&S Manual chapter 6311 "Hazard Avoidance."

14 Hazard Analysis

See reference 2 – Hazard Analysis

15 Revision History

Revision 1.0 November 15, 2001 – Initial release

Revision 2.0 July 19, 2002

- Deleted Tables 1 and 2 in section 8.1. Replaced with paragraph requiring dewars 3-8 to all be capable of operating in either high or low power modes.
- Revised section 8.4 to require modular RF connection method for dewars 3-8