********* DRAFT *********

SNS EQUIPMENT PROTECTION STRATEGY

1. INTRODUCTION

1.1 Equipment Protection Systems

Operation of SNS beam while equipment is improperly configured or malfunctioning can cause a number of problems, including excess prompt radiation, equipment damage, and activation of components. Equipment protection systems will be provided to prevent or terminate-and-dump beam when conditions required for operation are not satisfied.

The systems described in this document are for the protection of equipment, and not personnel. Personnel protection is covered under a separate WBS, and is the responsibility of a different organization.

Equipment protection systems are neither "safety class," nor "safety significant;" however because they are responsible for protection of a significant investment, they must be built with as high a degree of reliability as allowed by budgetary constraints.

The equipment protection systems can be placed in five categories corresponding to distinct functionality:

- <u>Fast Protect System</u>. This system cuts off (interrupts) the beam at the source and "dumps" any stored beam within approximately 10μs of detection of an anomalous condition – typically high radiation. It is therefore active during each "minipulse." [Why not "macropulse"?] Some fast protect system trips are automatically reset so that the next pulse can proceed. [Require manual reset after a set number of aborts?] The fast protect function is carried out by a dedicated hardware system monitored and controlled by software.

- <u>Beam Pulse Enable System</u>. On detection of an anomalous condition, this system allows the current pulse to complete, but inhibits the start of the next "minipulse." ["macropulse?] Typical conditions would include vacuum excursions or a kicker magnet not charged and ready for the next cycle. [Some/all trips automatically reset? Require manual reset after a set number of aborts?] This function is carried out by a dedicated hardware system monitored and controlled by software.

- <u>Run Permit</u>. Unlike the previous two systems, this system does not interrupt the beam. Rather it is a high-level software-based *permit* system that confirms that the facility is configured appropriately for the operator-selected operational mode, and inhibits beam operation until it is. [What if configuration changes during operation? Granted this would be abnormal, e.g. operator screw-up or equipment failure.]

- <u>Inter-System Interlocks</u>. These refer to interlocks between systems and/or subsystems which do not turn off or inhibit beam, but rather other equipment. One example would be the need to turn off RF systems in the event of a vacuum excursion, whether or not beam is present. Another would be the need to prevent insertion of an intercepting diagnostic device when beam of too high power density is present or permitted. These interlocks may be effected either by software or hardware as appropriate. In some cases it may be possible to use the same hardware as for the fast protect and/or beam pulse enable systems.

- System Interlocks. These refer to interlocks that are contained within a single system, subsystem or device. It includes simple device interlocks (e.g. a power supply door interlock) and self-contained single-system interlocks (e.g. a Programmable Logic Controller (PLC) which protects a local vacuum system). These systems are *not* the responsibility of WBS 1.9, but of the provider of the device or subsystem.

1.2 Objectives of This Document

The objective of this document is to develop the conceptual design of SNS equipment protection systems in preparation for the start of preliminary system design. Specific objectives include:

- Develop adequate design requirements for the start of preliminary (Title I) design activities.

- Develop the conceptual design to the point that interfaces with other project WBSs can be clearly understood. (An Interface Definition Document for equipment protection systems will be developed after this report is issued).

- Obtain a better cost estimate.

- Formulate an implementation plan.

- Consolidate the above information into a single "consensus document" that can be signed off by the SNS collaboration.

The equipment protection needs of accelerator, target, and instruments will all be considered.

1.3 Document Organization

Chapter 2 describes the conceptual design for equipment protection systems.
Chapter 3 presents requirements imposed by the SNS technical systems.
Chapter 4 proposes a plan for design and fabrication of the equipment protection system.
Appendix A cites references, including papers describing how equipment protection systems are implemented at other comparable facilities.
Appendix B provides preliminary listings of input channels planned for the equipment protection systems.
Appendix C provides a draft "system requirements document" for the equipment protection systems.
Appendix D provides the basis for the cost estimate for the equipment protection systems.

2. CONCEPTUAL DESIGN DESCRIPTION

2.1 Fast Protection System

The fast protect system is described first since its conceptual design is the best developed.

The fast protect system cuts off production of beam and initiates dumping of beam stored in the ring when conditions occur that would otherwise damage or activate equipment. A prime example is that beam should be terminated when a beam loss is detected.

A time response on the order of 10μsec (from input to output) is expected. This corresponds to approximately 10 beam revolutions in the ring. (It is desirable that the fast protect system be as fast as possible in order to minimize activation, to accommodate changing requirements, etc. A response times of less than 10 μsec will be implemented if it does not require a major increase in effort).

While technically the system needs to be active only when beam is on (i.e. during the macropulse), the system will probably be left active between pulses as well. As long as there are no false alarms, then no harm is done by keeping the system continuously active. This eliminates the complication (and reduction in reliability) of having to interface with the timing system. It also prevents pulses from continuing to “trigger then abort” when critical equipment has failed.

Figure 2.1-1 shows a simplified physical block diagram of the fast protect system. The SNS system will be modeled after an equivalent system used at RHIC (unfortunately dubbed the “beam permit system”). It is hoped that significant design effort can be saved by using elements of this existing system. See references in appendix A for details on the RHIC system.

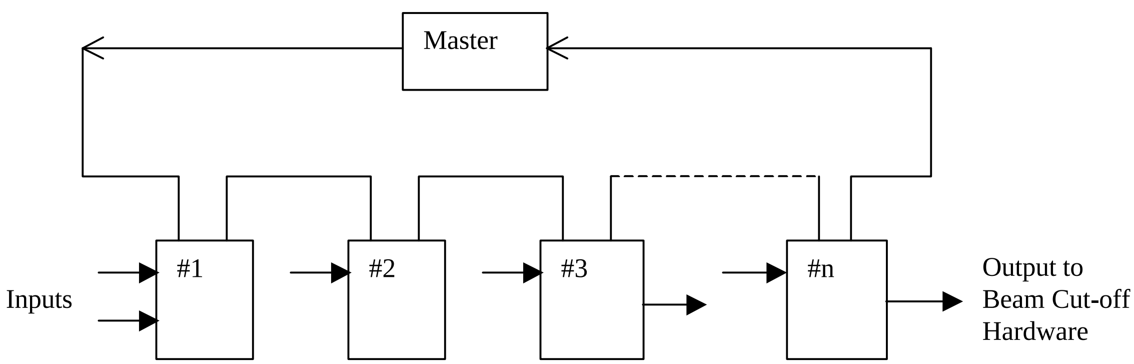

Fig. 2.1-1. Distributed Fast Protect Hardware

Inputs to the fast protect system are received via custom boards located in IOC VME crates. This approach simplifies the system design since packaging and power supplies are provided by the VME system. Boards are distributed throughout the facility near the sources of system inputs. The boards are interconnected by a fiber optic RF carrier signal loop. Each board receives several (perhaps 8) “enable” inputs and controls one or more interlock outputs. When all enable inputs on a given board are active then the input RF carrier signal is retransmitted to the next board in the loop. If the input carrier signal is lost or any of the input signals are disabled, then the board stops re-transmitting the carrier signal and disables its interlock outputs. The interlock output signals are used to enable/disable beam and to trigger other required actions (e.g dump beam stored in the ring; hold data needed to diagnose cause of trip; etc.).

Fast protect system components are designed so that component failures cause the system to revert to a safe state. The input signals are fail-safe in that a disconnected cable is detected as a “disable” input signal. Loss of the RF carrier signal is propagated around the loop until all boards are aware of the error condition. If the power is turned off to a module there can be no carrier and the system fails safe.

Any board can provide an output that can be used to disable beam. For reliability there will be at least two methods used to disable beam. Table 2.1-1 lists beam cut-off mechanisms currently planned for the fast protect system. These mechanisms were selected primarily due to their low impact on operations and their time response.

Table 2.1-1. Possible Set of Beam Cut-Off Mechanisms

Item	Abort Mechanism	Impact on Operations	Time Response	Fail Safe?	Other Comments
1	Kill RFQ r.f.	Low	~ 4 μsec	Yes	2 μsec to 85% gradient with Q = 5000. RF continues to transport partially accelerated beam down to 50% gradient. Some impact on operations, since RFQ tuning will change as RFQ cools. Time required to bring back on-line estimated at ~ 2 min. if RF power left off for relatively-long duration.
2	Stop ion source r.f. excitation temporarily	Low (if short duration)	μsecs	Yes	Good for fast equipment protection, but need to resume r.f. within 30 seconds or operations is impacted. There are additional problems if source uses cesium.
3	Kill source high voltage	Very low	seconds	Yes	Too slow for fast protection, but good for relatively-long duration shut-offs.
4	[Temporarily activate source chopper?]	None	μsecs	No	[Use of source chopper has problems: Difficult to design this chopper to sustain the high power level required for continuous beam cut-off service. Also, it is not fail-safe. Might be OK for short-duration cut-offs though.]

Two of the cut-off mechanisms listed in table 2.1-1 must be synchronized. Stopping ion source RF quickly stops beam, but will impact operations if left off for too long. Killing source high voltage effectively stops beam, but acts too slowly for fast protection. Thus, when beam cut-offs must be sustained for longer than a few seconds, the source high voltage will be tripped. Once source high voltage drops below the threshold required for beam cut-off, then the ion source RF can be restored. This switching function will be provided as part of the fast protect system.

An effort will be made to reduce the impact of spurious disable signals by allowing an automatic reset under certain circumstances. For example, a beam loss may be detected for just one pulse and then return to normal the next. Requiring a manual restart under this circumstance provides no benefit and hurts availability. One scenario is to require several disable inputs to occur in succession before forcing a manual reset. [Note that RHIC design has a long re-start delay. It takes 8 msec for each board to detect carrier and unblank. If you have 40 boards, then it takes 320 msec. to restore the beam enable. We only have ~16 msec between pulses. So every time we terminate beam, it will take on the order of ~320 msec. to recover. We will therefore lose ~20 macropulses. That seems OK to me as long as Beam Pulse Enable System knows it and doesn't try to trigger pulses during this time. Alternatively, we could try to modernize the design to speed it up, e.g. use 100Mbit ethernet front-end chip set instead of the 10 MHz RS-422]

[One way to implement automatic reset: Have IOC software automatically reset it after it has serviced the interrupt. Selection of auto or manual reset could be configured in software. Software could also force a manual reset if the number of trips exceeds an unacceptable rate.]

The use of VME boards that go in the IOC crates is important because software can be used to set up, test, and monitor the modules. For example, a "disable" input signal can generate an interrupt that causes the IOC to read out the reason for the disable. As each input or upstream RF carrier goes to the fault state, its time can be recorded. The software can then determine which input caused the failure by comparing timestamp information. Another software function is to mask inputs based on current operating mode. Inputs that are irrelevant to the current operating mode will be masked to prevent them from disabling beam. Software-initiated trips are yet another potential feature allowed by use of VME boards.

Transmission of the RF signal on the carrier loop is started by a master module. At RHIC, any fast protect input board can be configured to serve as the master board. A jumper on the board is used to enable this "master" functionality. The RHIC event timing system signals the master board to start up the fast protect system.

The response time for the fast protect system will be low, less than 10 microseconds. The RHIC protection system can provide a response time of about 40 microseconds. The actual hardware will respond in less than a microsecond. The time it takes to drop the output carrier signal after an error is detected is determined by chip gate times that are sub-microsecond. The response time of 40 microseconds is the result of signal propagation time over the long distances needed for RHIC. The SNS has shorter distances so it will be easier to meet the ten microsecond specification. The actual response time can be determined by measuring the distances involved. It should be pointed out that the maximum time is only for those modules that are a long distance from the hardware that actually does the beam dump or beam inhibiting. The response time for signals near the source are much lower.

In general, any necessary conditional logic to be applied to inputs must be implemented outside of the fast protect system. Examples follow:

- The radiation threshold signifying a beam loss in the ring will vary during each pulse. The threshold will increase as beam accumulates in the ring. The comparison of the beam loss monitor signal with the ramping alarm threshold will occur outside of the fast protect system. The resulting "OK / not OK" signal will then be provided to the fast protect system.
- Any others?

[Do we need to mask inputs for fractions of a pulse? Or can we assume masks only change between pulses (or only during changes in operating modes)?]

The interface between technical systems and the fast protect system is defined to be the terminal strips or connectors at the VME crates housing input signal boards. The instrumentation and cabling that provide the input signals are not considered to be part of the fast protect system. Similarly, the mechanisms that actually terminate and dump beam are not part of the fast protect system. The fast protect system simply provides an output signal to initiate the required action. For example, the hardware logic required to synchronize extraction of beam with the beam gap will be provided by BNL.

[Where is the "brain" that masks inputs according operating mode?

[Discuss what result of bad data and aborted pulses?]

2.2 Beam Pulse Enable System

The beam pulse enable system monitors conditions for which the next "macropulse" must be prevented and inhibits beam accordingly. If an anomalous condition is detected while a pulse is in progress, the current pulse is allowed to complete. Typical conditions include vacuum excursions or a kicker magnet not charged and ready for the next cycle.

While the response time of the beam pulse enable system is not as critical as that of the fast protect system, there is no reason why it should not be equally fast. If the response time is say x milliseconds, then there is a period x milliseconds before injection where the beam protect system will not protect the hardware. There will be many systems (e.g. vacuum, power supplies, magnets) that provide input signals to the beam pulse enable system. These systems are able to check the hardware some time before injection starts. Each system will have constraints on how far before injection it can check the data and yet still guarantee that the system is ready for injection. Some hardware has a response time that prevents very rapid changes in conditions. For example the vacuum can be checked a few milliseconds before injection with the assumption that even if a leak develops the vacuum cannot change sufficiently in a few milliseconds to cause a problem. The system response time of the beam pulse enable system has to be sufficiently low so that it can respond to all input signals before injection starts.

In many respects the beam pulse enable system is similar to that of the fast protect system. It must monitor geographically-distributed input signals. It must prevent operation of beam based on the status of these input signals. Its time response (at least for some inputs) should be approximately the same as that of the fast protect system. Given these similarities, it seems likely that much of the same hardware used for the fast protect system also be used for the beam pulse enable system.

At present there are two options being considered for implementation of the beam pulse enable system:

1. An independent system, with architecture very similar to fast protect system. It would inhibit the timing system instead of beam cut-off mechanisms.

2. Combine fast protect and beam pulse enable functions into one system.

The sections below describe these two scenarios.

2.2.1 Option #1: An Independent System

Figure 2.2-1 shows a block diagram of the beam pulse enable system implemented as an independent system. The same hardware used for the fast protect system would be used here as well. One major difference is that system outputs inhibit the timing system rather than actual beam cut-off mechanisms. The status of the fast protect system is input to the beam pulse enable system to prevent the timing system from futilely attempting to trigger pulses.

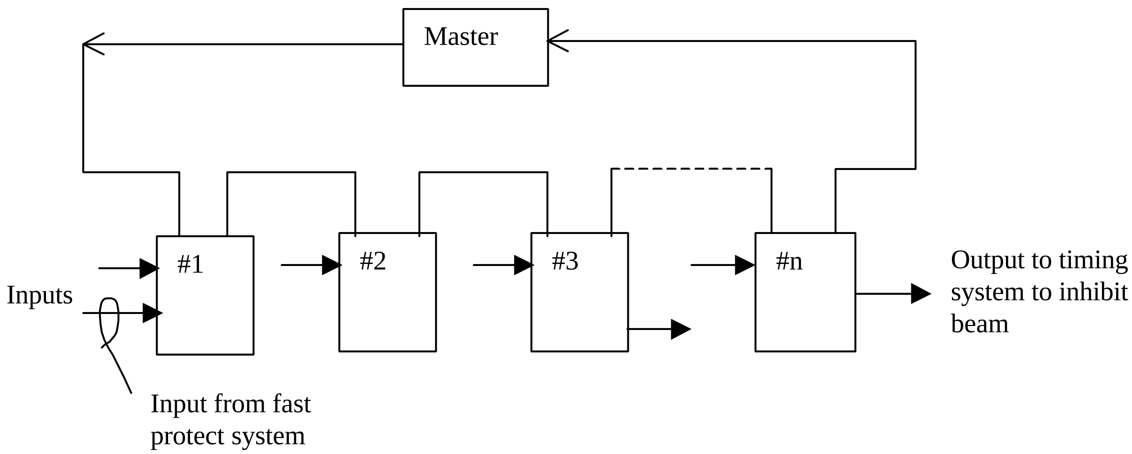

Fig. 2.2-1. Option #1 for Beam Pulse Enable System

As with the fast protect system, it may take several hundred milliseconds to reset after a system trip. This means that transient inputs may need to be masked for a portion of the pulse cycle in order to prevent false trips. This is illustrated in figure 2.2-2 for a fictional kicker magnet that must be charged and ready before the next pulse. In the first pulse cycle shown the magnet is ready in time for the next macropulse to take place. If the signal input to the beam pulse enable system were simply the "threshold detect" signal, then there would be a false trip (with resulting reset delay) between every pulse. The threshold detect signal needs to be "OR'ed" with a mask signal synched with the timing system in order to prevent the false trips. In the second pulse cycle shown, the magnet is not ready in time so the next pulse is aborted.

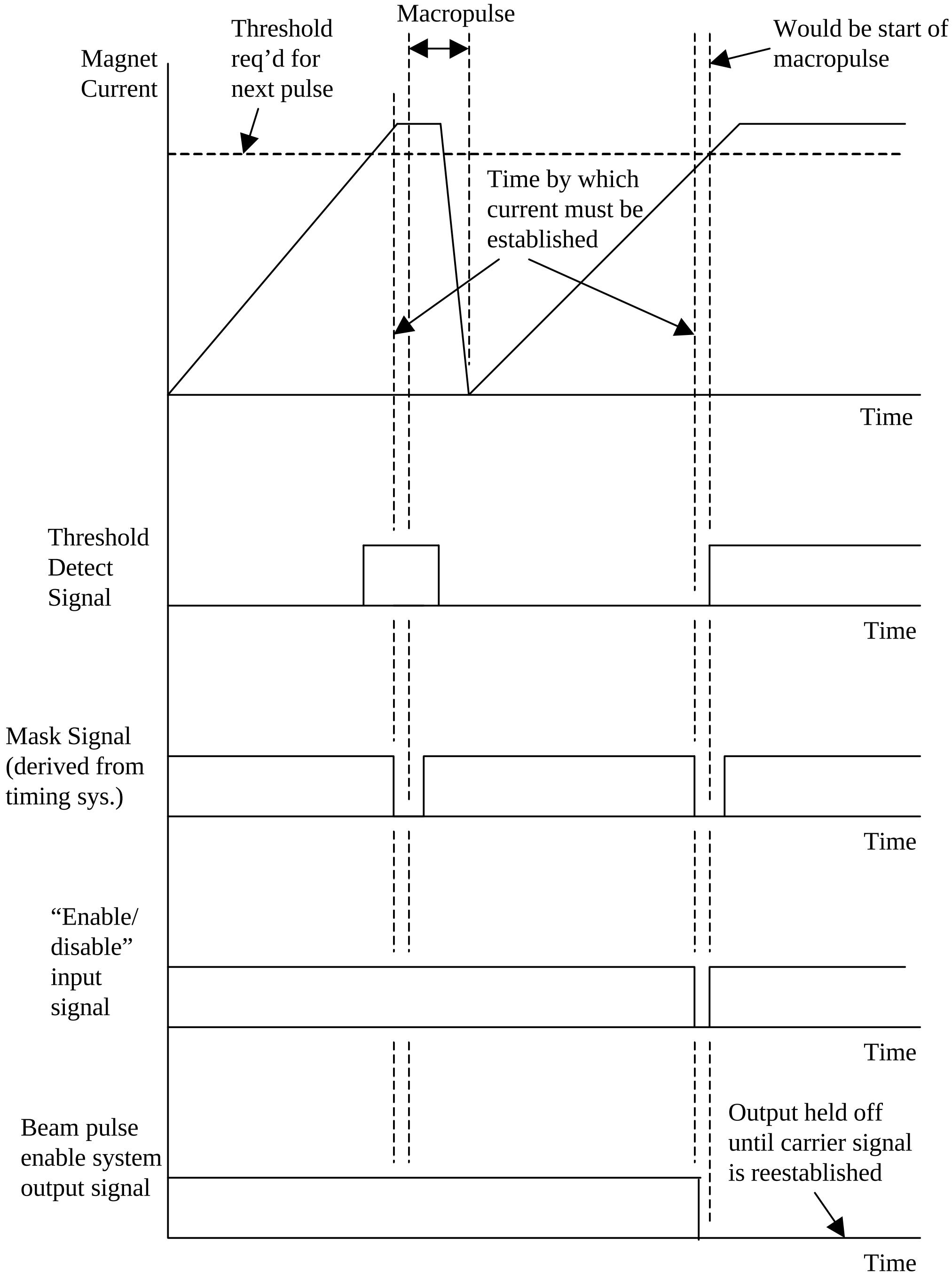

Fig. 2.2-2. Masking of Dynamic Inputs

2.2.2 Option #2: Combine with Fast Protect System

Given the similarity between the two functions, it seems plausible that the fast protect and beam pulse enable functions could be combined into one system. A block diagram of such a system is illustrated in fig. 2.2-3 below.

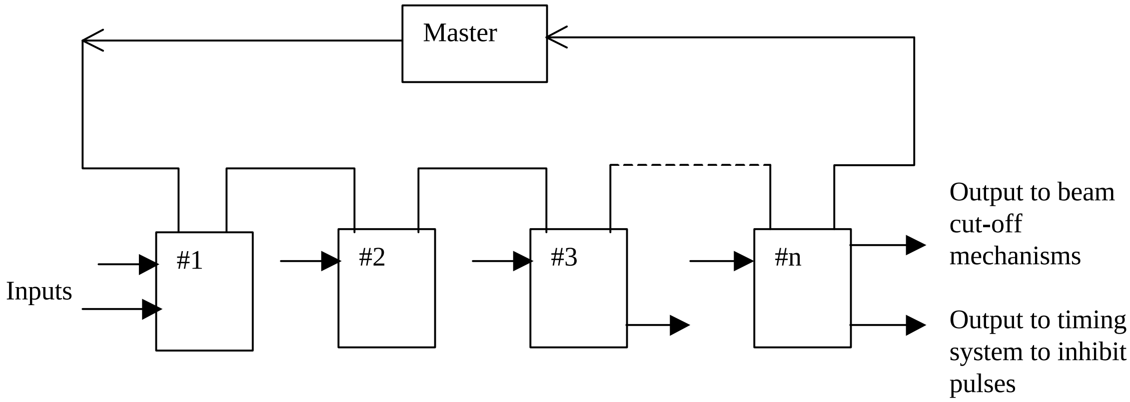

Fig. 2.2-3. Option #2: Combined System

One of the original reasons for considering an independent beam pulse enable system was to accommodate dynamic inputs such as the kicker magnet that must be charged before the next pulse can occur. In theory the system output could track the dynamic inputs so long as both signals were established soon enough before the next pulse. But as indicated in the previous section, the long reset time after a trip precludes this approach. Transient inputs must be masked anyway to prevent false alarms. This removes one incentive for an independent system.

Another incentive was that for some anomalous conditions a pulse in progress could be allowed to finish before an inhibit was required. [For these conditions, do we really care if beam is cut-off in the middle of the pulse? Even if we do care, is it worth the extra complication of an additional system?]

2.3 Run Permit System

[One scenario: Implemented via a central IOC. Make this IOC the “brain” that supervises changes in operating mode? Output to either FP or BPE system via software to prevent beam.]

[Philosophy: Operator selects mode. System says “OK / not OK”.]

2.4 Inter-System Interlocks

[One option: e.g. for linac: Implement a PLC with a field bus running the length of the linac. Interlock inputs and outputs could be hung off the field bus. The PLC could perform the inter-system interlock logic.]

[There has been some discussion providing an interlock for an intercepting diagnostic device when beam of too high power density is present or permitted. It is likely this would be based on operating mode, implying the system must somehow know the mode.]

3. EQUIPEMENT PROTECTION REQUIREMENTS BY SYSTEM

Specific requirements imposed by each technical systems are discussed in this section.

[NOTE: Many of the requirements listed in earlier versions of this document have been moved to Appendix C "Draft System Requirements Document" to put the detailed "boiler plate" stuff to the rear of the document.]

3.1 Front End Equipment Protection Requirements

[Steve Lewis: Please provide text for front end.]

A preliminary list of front-end-related inputs to the equipment protection systems is provided in Appendix B.1.

3.2 Linac Equipment Protection Requirements

[Dave Gurd: Please provide text for linac.]

A preliminary list of linac-related inputs to the equipment protection systems is provided in Appendix B.2.

3.3 Ring Equipment Protection Requirements

A preliminary list of ring-related inputs to the equipment protection systems is provided in Appendix B.3.

3.4 Target Equipment Protection Requirements

SNS targets include both the mercury target and the three beam dumps. All of these targets will have equipment protection system requirements.

Protection of the mercury target is of particular importance since there are a number of accident scenarios that could lead to the release of radioactive materials into the environment surrounding SNS. The equipment protection systems are part of "defense in depth" plans to prevent such accidents.

The draft <u>SNS Environmental Impact Statement</u> states that "The single most important parameter in any target facility accident sequence is timely cut off of the proton beam when unusual conditions occur". A breach in the primary containment boundary of the radioactive mercury can be fairly-easily handled. Continued operation of beam during such an event cannot easily be handled. Hence the reliability of beam cut-off systems becomes critical for target safety. Events for which beam must be cut off include:

- Loss of mercury cooling
- Too-high energy density of beam on target (e.g. too narrow focus)
- Loss of Hg vessel or pipe integrity

At this time, only the “loss of mercury cooling” event is considered to have the potential to release a significant amount of radioactive material outside the SNS facility.

A dedicated, safety-significant system dubbed the “Target Protection System” (TPS) will take primary responsibility for preventing a release. The equipment protection systems will provide a secondary layer of defense against accidents that could lead to a release. Equipment protection systems will provide the primary defense against all other target accident scenarios. Another layer of defense will be implemented via target EPICS and/or PLC controls. This third layer will likely interface with the equipment protection system to cut off beam.

Target equipment protection is limited to beam permit functionality only. For the identified accident scenarios the mercury target will be able to sustain a full-energy pulse before a beam inhibit is required. [May want to change this since fast protect system seems more reliable than beam pulse enable system.]

A preliminary list of target-related inputs to the equipment protection systems is provided in Appendix B.4.

[Include figure showing a beam dump? The target?]

3.5 Instrument Equipment Protection Requirements

[John Hammonds: please add text.]

3.6 Personnel Protection System Requirements

As indicated in Appendix B.6, the personnel protection system will provide an “OK/not OK” input to equipment protection systems.

4. IMPLEMENTATION PLAN

The following table reflects current plans for implementation of the fast protect and beam pulse enable systems.

Table 4-1. Implementation Plan		
Activity	**Responsible organization:**	**Oversight**
Interface & Project Mgmt.	SNS ICS	-
Preliminary Design	SNS ICS	-
Title I Design	BNL ___ group	SNS ICS
Title II Design	BNL ___ group	SNS ICS
Title II Design – Cable Plant	AE	SNS ICS
Title III Design	BNL ___ group, SNS ICS	SNS ICS
Procurement	BNL ___ group	SNS ICS
Construction Mgmt.	CM	SNS ICS
Start-up and checkout	BNL ___ group, SNS ICS	SNS ICS
Maintenance	SNS operations group	SNS ICS

AE = Architect/Engineer (Knight/Sverdrup)
CIND = Computing, Information, and Networking Division
CM = Construction Manager (Knight/Sverdrup)
SNS ICS = SNS Integrated Control System Group

Table 4-2 lists design documents that will be required to implement the control system network.

Table 4-2. Design Deliverables

Conceptual Design:
- WBS 1.9 Design Manual
- SNS ICS Equipment Protection System R&D Report (this document)
- QA Plan

Preliminary (title I) design:
- System Requirements Document
- Interface Definition Document (WBS 1.9.2.3&4 – WBS 1.9.x; WBS 1.9.2.1 – WBS 1.8)
- Block diagrams / schematic representations
- Preliminary location plan
- Equipment list/database
- Updated schedule and cost estimate

Detailed (title II) design:
- Fabrication drawings and specifications
- Detailed location plans
- Cable tables/database (for RF carrier loop)
- Cable installation documents (By AE)
- Test plans and "factory test" procedures
- Rack assembly details and bills of material for "master" equipment
- Updated schedule and cost estimate
- Working prototype system

Title III design deliverables:
"As-built" drawings
Post-construction, checkout, and start-up test procedures

APPENDIX A. REFERENCES

1. "RHIC Beam Permit and Quench Detection Communications System", Charles R. Conkling Jr., BNL, http://www.triumf.ca/pac97/papers/pdf/6P023.PDF

2. "V120 RHIC Beam Permit System Module", Charles R. Conkling Jr., BNL, http://www.rhichome.bnl.gov/Hardware/permit/permit.htm [See also for index of other BNL modules: http://www.rhichome.bnl.gov/Controls/IndexHardware.html]

3. "System Characteristics" (Slides from presentation on RHIC Beam Permit System), http://www.rhichome.bnl.gov/Hardware/permit/slidesho.htm

4. "Initial Strategy for SNS Beam Cut-off", [White paper; still in progress]

APPENDIX B. EQUIPMENT PROTECTION SYSTEM INPUTS

[On lists of points: It would be good to designate which signals are FP, which are BPP, and which are RP.]

B.1 FRONT END EQUIPMENT PROTECTION SYSTEM INPUTS

[Steve Lewis: Are there any? If so, please fix up this table of inputs.]
[Add diagnostic signals and protection of intercepting diagnostics.]

Table B.1-1. Front end equipment protection system inputs

System Monitored:	Time Before Extraction:	No. of Channels:
Beam loss monitors?		
Magnet power supplies?		
RF?		
Vacuum?		
LEBT vacuum valve?		
Cooling water?		
F.E. Personnel Protection System OK		
F.E. controls watchdog timer OK		

System Monitored:	Time Before Extraction:	No. of Channels:
No beam current entering linac [verifies beam containment]		

B.2 LINAC EQUIPMENT PROTECTION SYSTEM INPUTS

[Dave Gurd: Please fix up these tables of inputs. Inputs are grouped into DTL, CCDTL, and CCL to facilitate commissioning.]
[Add diagnostic signals and protection of intercepting diagnostics.]

Table B.2-1. DTL equipment protection system inputs

System Monitored:	Time Before Extraction:	No. of Channels:
Beam loss monitors?		
Magnet power supplies?		
RF?		
Vacuum?		
Vacuum valves?		
Cooling water?		
Linac personnel protection system OK		
Linac controls watchdog timer OK		

Table B.2-2. CCDTL equipment protection system inputs

System Monitored:	**Time Before Extraction:**	**No. of Channels:**
Beam loss monitors?		
Magnet power supplies?		
RF?		
Vacuum?		
Vacuum valves?		
Cooling water?		

Table B.2-3. CCL equipment protection system inputs

System Monitored:	**Time Before Extraction:**	**No. of Channels:**
Beam loss monitors?		
Magnet power supplies?		
RF?		
Vacuum?		
Vacuum valves?		
Cooling water?		

B.3 RING EQUIPMENT PROTECTION SYSTEM INPUTS

Following is a list of equipment protection inputs and timing requirements for SNS main ring. The timing parameter listed is the checking time just prior to the injection of the beam from the Source/Linac. The parameters were discussed amongst the various BNL Group Leaders and their input is reflected. The data was also brought up at the SNS Monthly Collaboration Meeting held in Washington, DC on 3/5-3/6/98.

Since some of the system monitoring needs such as the Beam Distribution on Target can only affect the next injected pulse, the information may have to be stored for approximately 16 milliseconds so that the next injected pulse is inhibited.

The list defines the deliverables for the main ring input to the equipment protection systems.

[Add vacuum valve open/close status to tables?]

Table B.3-1. Ring equipment protection system inputs

System Monitored:	**Time Before Extraction:**	**No. of Channels:**
LAMS Section:		
[Req’d?: LAMS magnets OK]		

System Monitored:	Time Before Extraction:	No. of Channels:
HEBT vacuum OK	1 millisec	
HEBT control system OK (e.g. watchdog timer for micros feeding equip. protect. sys.)	1 millisec ?	
HEBT beam loss monitor system - NG Signal - Detection of High Loss	 Next Pulse Inhibit mid pulse (fast protect)	
Achromat Section:		
[Req'd?: Acrhomat magnets OK]		
Achromat vacuum OK	1 millisec	
Main Ring:		
Main Ring Magnets: - Dipole current - Dipole field - Quad current	1 millisec.	
Injection: - DC Magnets - Current established in Kyn. KR magnets	 1 millisec. 5000 microsec.	
RF on	100 microsec	
Coupled Injection: - Beam Shape(quality) delivered OK	Next Pulse	
Ring vacuum OK	1 millisec	
Ring control system OK (e.g. watchdog timer for micros feeding equip. protect. sys.)	1 millisec ?	
Ring timing system OK	1 millisec?	
Damper	?	
Debuncher	?	
Ring beam loss monitor system - NG Signal - Detection of High Loss	 Next Pulse Inhibit mid pulse (fast protect)	
Extraction Ready - Fast KR PFN's Charged - Lambertson Sm current OK	 100 microsec. 1 millisec	
RTBT:		
RTBT PS's OK	1 millisec	
[Req'd?: RTBT magnets OK]		
RTBT vacuum OK	1 millisec	
RTBT control system OK (e.g. watchdog timer for micros feeding equip. protect. sys.)	1 millisec ?	

System Monitored:	Time Before Extraction:	No. of Channels:
RTBT beam loss monitor system - NG Signal - Detection of High Loss	 Next Pulse Inhibit mid pulse (fast protect)	
Beam shape(quality) delivered to target OK	Next Pulse	
Intensity variation, pulse-to-pulse at Hg target	Next Pulse	

B.4 TARGET EQUIPMENT PROTECTION SYSTEM INPUTS

NOTE: Time response required for all channels listed is “inhibit next pulse”.

Table B.4-1. Target equipment protection system inputs required for <u>linac tuning only</u>.

Signal Description:	No. of Channels:
Linac tune dump cooling water system OK	
Linac tune dump off-gas system OK	
[Others?]	

Table B.4-2. Additional target equipment protection system inputs required for <u>ring injection tuning.</u>

(This dump is used to catch the unusable H^- and H^0 particles emerging from the injection stripping foil, and so is used for more than just tuning. This dump is required for ring injection tuning, ring extraction tuning, and neutron production).

Signal Description:	No. of Channels:
Ring injection dump cooling water system OK	
Ring injection dump off-gas system OK	
[Others?]	

Table B.4-3. Target equipment protection system inputs required for <u>ring extraction tuning only</u>.

Signal Description:	No. of Channels:
Ring extraction tune dump cooling water system OK	
Ring extraction tune dump off-gas system OK	
[Others?]	

Table B.4-4. Target equipment protection system inputs required for <u>neutron production</u>.

(See *Design Manual* Section 6.8 for additional information on conditions these inputs protect against.)

Item #	Signal Description:	No. of Channels:
1	Beam energy density related:	
1.1	[Technically belongs under ring, but I've included it until I'm sure its covered.] Beam current density on Hg target OK	
1.2	[Technically belongs under ring, but I've included it until I'm sure its covered.] Beam-on-target focusing magnets OK	
2	Hg-Leak related:	
2.1	Leak detectors OK	
2.2	Hg sump tank level OK	
2.3	No voids detected in Hg in pipes	
2.4	Target annulus pressure OK	
2.5	Spill tank level OK	
3	Loss-of-Hg-cooling related:	
3.1	Target Hg return flow OK	
3.2	Target bulk inlet Hg flow OK	
3.3	Target window inlet Hg flow OK	
3.4	Hg pump discharge pressure OK	
3.5	Hg pump speed OK	
3.6	Hg pump power supply OK	
3.7	Hg temperature at target outlet OK	
3.8	Secondary cooling loop water flow OK	
4	Loss-of-H_20-flow-to-target-shroud related:	
4.1	Shroud outlet water temperature OK	
4.2	Target shroud H_2O flow OK	
5	Loss-of-H_20-flow-to-proton-beam-window related:	
5.1	Window outlet water temperature OK	
5.2	Proton beam window cooling water flow OK	

Item #	Signal Description:	No. of Channels:
6	Loss-of-water-flow-to-target-component-cooling-loops (H_2O moderator, reflectors, etc.) related:	
6.1	Target component outlet water flows OK	
6.2	Component outlet water temperatures OK	
7	Signals related to: Loss of H_20 or D_20 integrity in target component cooling loop; Loss of integrity of 2-m target vessel; Loss of He flow to 2-m target; Target cell ventilation system failure:	
7.1	Target 2m vessel pressure OK	
8	Loss-of-integrity-of-cryogenic-moderator related:	
8.1	“OK/not OK” signal from cryogenic mod. ctrl sys. (e.g. Hydrogen primary confinement breached, etc.)	
9	Misc.:	
9.1	Crash switch in target control room OK	
9.2	Equipment protection system watch-dog timers OK	
9.3	Shut-off signals from TPS OK	
9.4	Shut-off signals from EPICS and PLC systems OK	
9.5	Shut-off signals from PPS OK	

B.5 INSTRUMENTS EQUIPMENT PROTECTION SYSTEM INPUTS

[John Hammonds: Please provide table of inputs, if any.]

B.6 INPUTS FROM PERSONNEL PROTECTION SYSTEM

Table B.6-1. Equipment protection system inputs received from Personnel Protection System

Signal Description:	No. of Channels:
Personnel Protection System: OK for beam	
[Possibly area radiation monitors. Probably not.]	

APPENDIX C. DRAFT SYSTEM REQUIREMENTS DOCUMENT

C.1 SNS OPERATING MODES

SNS will have several distinct operating modes, ranging from front-end tuning to full-power neutron production. Some likely operating modes are listed in table 2.1.

Table 2.1 – Possible Operating Modes for SNS

Operating Mode:	
Beam Configured for:	**With Current Level:**
Front-end tuning	(N/A)
DTL tuning, (Commissioning only)	Low current
" " ,	High current
CCDTL tuning, (Commissioning only)	Low current
" " ,	High current
CCL tuning, (Commissioning only)	Low current
" " ,	High current
Linac tuning,	Low current
" " ,	High current
Ring injection tuning,	Low current
" " " ,	High current
Ring extraction tuning,	Low current
" " " ,	High current
Neutron production,	Low current
" " ,	High current

[Add different pulse rates to table somehow.]

To enhance SNS availability, equipment protection functions shall be limited to protect only equipment in use during the active operating mode. For example, faulty equipment in the ring shall not prevent linac tuning.

C.2 RELIABILITY, AVAILABILITY, AND MAINTAINABILITY REQUIREMENTS

The project will assign an availability budget to the ICS. The availability budget for the equipment protection systems will be derived from this number. The equipment protection systems shall be designed to meet the assigned availability numbers. [At the time of this report the availability budget was "to be determined". For now, it can be assumed that system architectures in place at other comparable facilities will be work for SNS as well.]

Steps taken to insure reliability should include:

- a hardware QA program (e.g. design reviews, test program, etc.),
- a software QA program (e.g. design and maintain input masking software to preclude erroneous masking)
- designing for reliability. (e.g. Design inputs and outputs to be fail-safe; design carrier loop to fail safe; use redundant internal logic; apply redundant inputs and outputs).

It should be noted that the reliability (and availability) of the equipment protection function will depend largely on the reliability of the instrumentation providing the input signals. Design reviews should be conducted for this instrumentation as well.

The equipment protection systems must be capable of reporting to operations personnel the cause of each system trip. “First-out” indication must be provided so that the actual cause of the trip can be determined when alarm conditions cascade. The primary operator interface should be via the ICS EPICS system.

Some technical systems are planning to provide data acquisition to support diagnosing the sequence of events leading to a trip. The equipment protection systems shall provide an output signal to initiate the holding of data when a trip occurs. [I think John Smith is planning data logging into cyclical buffers. Data logging stops when there is a beam trip. Operators can then look at the data to see conditions leading to the trip.]

The equipment protection systems must be designed and implemented to facilitate periodic testing. Automatic testing should be considered where feasible.

It should be easy to add new signals to the beam permit and fast protect systems at any time. It should also be easy to reconfigure existing functions to accommodate changes in operating strategy.

C.4 PREFERED DESIGN PARAMETERS

Form factor: VME board

Time response: [<10μ from input to output?]

Input channel requirements:

- Signal types and levels: [e.g. TTL? Include tolerance levels]
- Transient protection: [e.g. meet IEEE 472(?) for surge protection?]
- Isolation: Galvanic isolation required; isolated to [xxx] volts
- Fail-safe (i.e. disconnected cable should result in a “disable” input signal)
- Jumper-activated disable of software masking?
- Screw-terminal connections?
- [Provide on-board filtering options?]
- Max. allowable cable length from sensor to VME board: [?]
- Status indication via LED on module faceplate (LED on = “OK”)

Output channel requirements:

- Signal types and levels: [e.g. TTL? Include tolerance levels]
- Transient protection: [e.g. meet IEEE 472(?) for surge protection?]
- Isolation: Galvanic isolation required; isolated to [xxx] volts
- Fail-safe (i.e. disconnected cable should result in a “disable” output signal)
- Screw-terminal connections?

Electrical power: Supplied by VME backplane

Environmental requirements:

- Operating temperature range: [should match std. VME spec]
- Operating humidity range: [should match std. VME spec.]

Input card parameters:

- $\geq$ 8 inputs per card.

≥ 1 output per card

Carrier loop parameters:

Fail-safe

Transient protection: [e.g. meet IEEE ___ for surge protection?]

Isolation: Galvanic isolation required; isolated to [xxx] volts

Max. allowable cable length = [xxx].

Diagnostic indicators as required via LED on module faceplate (Carrier status, etc.)

[Some kind of "watchdog" electronics required?]

C.4 PREFERED OPERATING STRATEGY

[May be a bad title. This section ended up as a "catch-all" section. Needs work. But somewhere we need to pin down these issues/requirements.]

[Operator selects mode. Somehow input signals get masked accordingly.
How "disable" input signals get processed.
Etc.]

VME Bus interface for:

- Masking of input channels based on operating mode
- "First out" detection of parameter causing trip
- VME interrupt when trip occurs?

Event system interface needed?

Time stamp handled via software?

Master module:
- Same basic construction as other modules. Configured as master via jumper.

To accommodate cut-offs longer than a few seconds, output circuitry needs to be provided to:
(a) Turn off source high voltage if beam cut-off duration exceeds a few seconds, and
(b) Restore ion source RF once source high voltage falls below the threshold required for beam.
This could be done via a "black box" outside the standard VME boards.

C.5 INTERFACE REQUIREMENTS

[Elaborate on:

Interface with Timing System

Interface between sensors and equip protect sys

Interface with PPS

Cable plant

Beam cut-off mechanisms

Ring dump mechanisms]

C.6 ANY OTHER GENERAL STUFF?

Beam current accounting system?

C.7 COMMISSIONING REQUIREMENTS

Equipment protection functions shall be implemented in a manner that facilitates commissioning:

- It must be possible to incrementally expand the system for each commissioning phase. For example, it should be possible to implement equipment protection for the front-end and linac while ring construction is in progress.
- It must be possible to test downstream systems while upstream systems are being commissioned and/or operated. For example, it should be possible to test ring equipment protection functions while operation of the linac is taking place.
- Implementation of protection functions for the next commissioning phase should not disturb those portions of the system that have already been tested.

APPENDIX D. COST ESTIMATE

[To be done after conceptual design is fleshed out.]

Contributors:

John Smith, BNL
Bill DeVan, ORNL
Dave Gurd, LANL