

Subject Personnel Safety Interlock System (PSIS) Design Standard	Effective Date 8/22/94	Prepared  R. Mika/W. Rauch
	Supersedes New	Approved  Engineering Department Head

1.0 APPLICABILITY

This standard is applicable to all major modifications to existing projects and to all new installations of Personnel Safety Interlock Systems (PSIS) for systems over 600 V at PPPL. The schedule and decision for bringing existing installations into conformance will be determined by PPPL project management, with the appropriate ES&H approval, on a case-by-case basis.

2.0 INTRODUCTION

This standard describes engineering and design criteria including:

- 1) the PSIS transition states
- 2) interlock components
- 3) human factors for PSIS

The PSIS safety criteria are defined by ES&HD-5008, PPPL Safety Manual, Section 2.

3.0 REFERENCES

- | | |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ES&HD-5008 | PPPL Environmental Health and Safety Manual, Section 2 |
| ENG-011 | PPPL Interlock Key Control Procedure |
| ES-ELEC-004 | PPPL Electrical Construction for Installations Operated 600 Volts & Below |
| PPPL-STD-001 | Programmable Logic Controllers (PLC) Qualification/Application Standard |
| UCID-20560 | Lawrence Livermore National Laboratory Human Factors Engineering Guidelines |
| NUREG-0700 | U.S. Nuclear Regulatory Commission Guidelines for Control Rooms
PPPL Drafting Standards Manual
TFTR Final Safety Analysis Report, Section 9.3
PBXM Final Safety Analysis Report |
| DOE Order 5480.19 | Training Requirements for the applications of PSIS's and Procedures
Independent Verification of the PSIS's |

4.0 STANDARDS

The purpose of the Personnel Safety Interlock System is to limit the possibility of injury to personnel and damage to equipment resulting from **electrical hazards**.

Chapter 4, paragraph 4.1 of the ES&HD-5008 document specifies: "Energized parts of high-voltage (above 600 V ac or dc) equipment and circuits shall be isolated from surfaces exposed to personnel by **two acceptable, independent energy barriers**, both of which shall be

designed to survive any credible (i.e. having probability greater than 10^{-6} / year) failure mode". The PSIS shall be designed to assure this separation.

4.1 DEFINITIONS

DISABLED - This condition is obtained, if an "Enable" permissive from any subsystem or PSIS is "Not true".

DISARMED - This condition is obtained, if an "ARM" permissive from any subsystem becomes "Not true".

EQUIPMENT - The two major categories of experimental equipment, Type 1 and Type 2 are defined by the hazards associated with them.

Type 1: Equipment in this category can be operated without causing injury to personnel in the vicinity. Type 1 equipment is not interlocked with the PSIS.

Type 2: Equipment in this category, typically belongs to class C, D, or E as defined in Section 2 of ES&HD-5008, may present a personnel hazard when in operation. For example, the field coil power supplies can generate unsafe conditions for personnel in the vicinity of the field coil or other equipment electrically coupled. Type 2 equipment is interlocked with the PSIS.

EMERGENCY STOP (E-STOP) - A manual or automatic action via an emergency push-button or interlock which results in returning the PSIS to its "SHUTDOWN" state (see definitions 4.2.1). If an E-stop is activated all input power to Type 2 equipment is removed.

EXPERIMENTAL DEVICE - A device, generally classified as Type 2 equipment, designed to conduct physics experiments, e.g. Tokamak.

FAIL-SAFE - A system designed to assume a safe state upon experiencing a most probable failure. For instance, if the most common failure is loss of power, the PSIS should transfer to a lower and safer state. A fail-safe control system is also the one whose outputs are de-energized (safe state) when a component or circuit failure occurs in the control loops and interlocks associated with a particular output.

INTERLOCKED-ACCESS area - An area dedicated to Type 2 high voltage equipment. Personnel access is controlled by PSIS.

LOAD - A device or piece of equipment to which energy is delivered, for instance a solenoid or RF antenna.

PERMISSIVES - Conditions that allow transition to the higher state, e.g. "NO E-STOP". Removal of these conditions causes a transition from the higher state to a lower e.g. ARMED -> ENABLED

PSIS - Personnel Safety Interlock System.

SAFETY DISCONNECT SWITCH ensures that the coil circuit is electrically grounded and disconnected from its power system when the area is in FREE ACCESS or CONTROLLED ACCESS.

SAFETY LOCKOUT DEVICE, when placed in the **SAFE** position, provides a mechanical means of removing operational power (electrical, air pressure, or other) from **SAFETY DISCONNECT SWITCH** and **Grounding Switches** once they are all in the safe position. The operational power must be removed by the **SAFETY LOCKOUT DEVICE** and key lock-out before any access, other than **HOT ACCESS**, to the interlocked-access area is permitted.

STATES - Physical conditions of the **PSIS**, the experimental device, and associated area.

SUBSYSTEM - A group of devices or equipment which can deliver energy to the load.

4.2 TRANSITION STATE DESIGN CONSIDERATION

The transition states for machine equipment protection and personnel safety are defined in the following paragraphs and by the state diagram of figure 1. The transition to the higher state can only be allowed if all permissive requirements are met. For less complex systems there may be fewer states required. The examples of less complex systems states may be: **ON/OFF** or **START/STOP**.

4.2.1 EXPERIMENTAL DEVICE PROTECTION TRANSITION STATES

The definitions described below refer to the permissive conditions and transition states which generally apply to equipment which may present a personnel hazard when in operation (Type 2 equipment). For example, the Tokamak field coil power supplies can generate unsafe conditions for personnel in the vicinity of the field coils. Such equipment is interlocked with the **PSIS**.

STATES:

The relationship of the four transition states for a **PSIS** are shown in the state diagram of figure 1, and are defined below. The status of each state shall be monitored by the **PSIS**.

SHUTDOWN - This state is obtained when an E-stop has been activated by the **PSIS** or any other subsystems. All Type 2 equipment is positively de-energized (refer to the truth table of figure 1).

STARTUP - In this state, input power may be applied to the subsystem, but not to the experimental device (refer to the truth table of figure 1).

ENABLED - This state is obtained provided all "Startup and Enable" permissive conditions from the **PSIS** and selected subsystems are "true". In this state selected subsystem outputs may physically be connected to the experimental device (refer to the truth table of figure 1).

If an "ENABLE" permissive from any subsystem or **PSIS** is "Not true", the **PSIS** shall monitor the **DISABLED** condition, transition to the next lower state (**STARTUP**), thereby preventing operation of the experimental device.

ARMED - This state is obtained provided all "Startup, Enable, and ARM" permissive conditions from the **PSIS** and selected subsystems are "true". In this state selected subsystems are ready for operation to the experimental device (refer to the truth table of figure 1).

If an "ARM" permissive from any subsystem or **PSIS** is "Not true", the **PSIS** shall monitor the **DISARMED** condition, transition to the next lower state (**ENABLE**), thereby preventing operation of the experimental device.

4.2.2 ACCESS CONTROL TRANSITION STATES

Typically the experimental, interlocked-access areas have up to four levels of Access Control. The type of access control used in each area depends on the hazards existing within the area and on the type of experimentation planned.

A. Level 1. FREE ACCESS

This level provides free access in and out of the area to authorized personnel. All Type 2 equipment in this area is in the SHUTDOWN state (positively de-energized). PSIS interlocks prevent Type 2 equipment from leaving positively de-energized state. The satisfactory radiation survey, if required, has been performed. Type 1 equipment may be operational. This form of access is available only if the SLD is in the safe position.

B. Level 2. CONTROLLED ACCESS

This level, similar to FREE ACCESS, is achieved when an area has been searched and secured. In addition, the following actions may be taken to further assure safety: visual surveillance via TV, badge verification, logging for all personnel entering and leaving is performed. In compliance with the PPPL ES&HD Manual, chapter 10, radiation levels are always assessed prior to personnel entering CONTROLLED ACCESSED areas.

Type 2 equipment must be in the SHUTDOWN state. Type 1 equipment may be operational. If under these conditions, CONTROLLED ACCESS procedures are not being properly followed, the PSIS will detect an error and revert to Level 1, FREE ACCESS. Another search and secure process of the interlocked-access area will be required before returning to Level 2, CONTROLLED ACCESS.

C. Level 3. HOT ACCESS

This form of access allows personnel to be present in the interlocked-access while certain Type 2 equipment is operated. The formation of plasma and its resulting radiation are prevented administratively by inhibiting any combination of coil/power systems which could generate plasma.

D. Level 4. NO ACCESS

At this level no personnel are permitted to enter the interlocked-access because hazardous electrical, mechanical, or radiation conditions exist. If the integrity of the PSIS is violated during NO ACCESS mode, an alarm will sound and all equipment within the area reverts to the STARTUP state. Since radiation hazard can still exist inside the area, the cause of the problem is determined and the appropriate corrective action is taken by the operating personnel, prior to declaring area FREE ACCESS.

4.3 HARDWARE STANDARDS

These standards apply to the following functions:

- Personnel Safety Access Control
- Emergency Shutdown
- KIRK Key Interlock
- Programmable Logic Controller (PLC)
- Annunciators and Displays

The designer of interlock systems has a wide choice of hardware equipment from which to choose, ranging from the common electromechanical relay to PLC's. In addition to the following list of

associated equipment parameters, refer to PPPL Engineering Standard, ES-ELEC-004, for electrical construction specifications for installations operated at 600 volts and below.

- Relays:** Electromechanical Relays are recommended for use with PSIS.
- A. Contact blocks used with the hardwired PSIS shall be Form A, B, or C. Contact rating 10 amps at 120 volts, makes 30 amps for 30 ms, 100,000 operations. All equipment is required to be listed using UL Standard 508.
 - B. Contacts open on coil de-energization or power failure.
 - C. The relay has gravity dropout or springs.
 - D. Properly designed energy limiting devices will be used to reduce possibility of contacts being welded closed.
 - E. Proper arc suppression across the contacts for inductive loads shall be used.
- Wires:** Wire size of the hardwired Personnel Safety Systems shall be adequate to support the current rating of devices used. Refer to the Engineering Standard ES-ELEC-004 and National Electric Code.
- Raceways:** All PSIS wiring shall be installed in separate dedicated raceways. Refer to the Engineering Standard ES-ELEC-004 and National Electric Code for more details.
- E-Stop Stations:** According to ES&HD 5008, section 2.5.10.2 all Emergency Stop Stations (E-STOPS) shall be manually operated push-button stations with mechanical "RESET" function, and light. Stations shall be clearly visible and located at the entrance doors and at other strategic locations around the experimental device.
- A. Personnel within an interlocked-access area shall not have to travel more than 50 feet to reach an E-Stop.
 - B. The E-Stop shall automatically de-energize all Type 2 equipment within the interlocked area.
 - C. E-Stops shall be guarded against accidental operation and be clearly labeled indicating both "EMERGENCY SHUTDOWN" and the name(s) of the affected system(s).
 - D. There shall be at least one E-Stop operable from the outside of an interlocked-access area.
- Door Latches:** Electromechanical door latches shall require operational power to allow access to the area. The unsafe side of the door will be equipped with the crash bar to allow emergency egress at any time.

- Door Switches:** At least two independent Door Switches are required at each access door to the interlocked-access area. Positive action mechanical limit switches will de-energize (simulate E-Stop) all Type 2 equipment when integrity of the PSIS is violated.
- Emergency Access:** A key or a push-button for emergency access shall be installed in a locked box with a clear glass face. Breaking a glass and activating Emergency Access device shall cause an E-Stop. This action shall release an access key for the interlocked area.
- KIRK key devices:** KIRK key devices are used in no personnel traffic areas like capacitor enclosures, switch gear, high voltage power supplies etc. Access to normal traffic experimental areas, such as Test Cell, is controlled by Door Latches and doors equipped with crash bars for easy egress.
- Lamps:** Incandescent or neon lights are permitted for PSIS status display. Color codes are described in section 4.4. All lamps are to be equipped with lamp test function. Required rated life of operation is minimum 1000 hours.
- Displays:** Back lighted window unit or CRT displays are permitted for Personnel Safety Interlock Status Display. Refer to section 4.4 for Human Factors Standards and color codes.
- PLC:** Refer to PPPL-STD-001 (to be replaced by PPPL Engineering Standard No. ES-COMP-TBD)

4.4 HUMAN FACTORS STANDARDS

Several human factor standards are available which define guidelines that apply to PSIS, such as UCID-20560, Lawrence Livermore National Laboratory Human Factors Engineering Guidelines, and NUREG-0700 U.S. Nuclear Regulatory Commission Guidelines for Control Rooms. A summary of these standards as they apply to PSIS follows:

General Layout: The general layout should facilitate operator coverage of PSIS instrumentation and equipment. The arrangement should ensure complete and timely coverage of controls, displays, and other equipment during all modes of operation. The equipment should be suited to the ergonomic characteristics of the expected operator population.

The placement of PSIS equipment should:

- adhere to an acceptable anthropometric basis for equipment dimensions and human engineering guidelines
- permit operators to view all control and display panels (including annunciation panels) from the operators' area
- facilitate voice communication between operators
- provide unobstructed movement

Location of CRT Displays: To assure the readability of displays and annunciators, their height and orientation relative to the operator's position should be considered.

Labeling equipment: PSIS controls, displays, user interface equipment, and most other equipment manipulated should be appropriately and clearly labeled to permit rapid and accurate human performance.

Push-button functions: When several annunciators or lamp cabinets operate as a system, the push buttons should be arranged and connected to allow the following operation from appropriate locations:

- 1) Silence push buttons should be located on all supervision and control panels and connected to silence the alarm audible device for any alarm in the control room. This avoids continued noise while retaining the flashing visual displays.
- 2) Acknowledge push buttons should only be located on control panels where corrective control action can be taken to acknowledge new alarms related to the controls on that panel. This encourages observation of related indicators and controls.
- 3) Reset push buttons should be located on all supervision and control panels and connected to reset any latched type inputs. A return to normal, unlatched conditions usually do not require acknowledgment.
- 4) Test push buttons should be located only near annunciators or lamp cabinets and connected to test the related annunciator or lamp cabinet only. This avoids disrupting the entire annunciator system during test.

Annunciator Warning Systems

The PSIS should provide an annunciator warning system as the primary control interface that will immediately alert the operator to facility conditions. Auditory signals should provide clear, unambiguous, nonverbal signals that direct or cue operators. The annunciator warning system should include three elements:

- an auditory alert
- a visual alarm
- an operator response

System Status Display

The PSIS Status Display should mimic the status of all KIRK key stations, door interlocks, E-Stops and other personnel safety related equipment. According to the PPPL Drafting Manual, page S/278, the mimic boards and CRT pages will use the following color coding:

Color	Function
Red	Equipment Running, Load Condition, Valve Open, High Voltage Present, Laser Turned On, No Access, Emergency Condition, Danger, HI-HI Alarm, LO-LO Alarm
Green	Equipment Not Running, No-Load Condition, Interlocks in Permissive State, Ready to Operate, Valve Shut-off, High Voltage OFF, System Grounded, System OK, Free Access

Yellow	HI Alarm, LO Alarm, Fault Condition, Trouble
White	Failed, System Not Ready, Interlocks Tripped
Cyan	
Magenta	
Blue	System Status and Mode Indication (Positive/Negative Polarity, Pulse/Steady, Recycle/Single Cycle)

5.0 DOCUMENTATION

All documentation should be done in accordance with the PPPL Drafting Standards Manual. Some of the items a documentation package should include but are not limited to are:

- for KIRK Key interlock PSIS, a key interlock schematic diagram, example shown on figure 2
- for Hardwired PSIS, a control elementary schematic diagram, example shown on figure 3
- for PLCs a graphic printout of the program, usually in relay ladder form.

In addition, a documentation package should provide for assignment of labels to contacts, coils, and I/O points, cross reference between system components and associated systems. Additional documentation should include parts list, family tree, block diagram, etc. as required.

6.0 PROCEDURES

The requirements for the PSIS procedures are defined in paragraph 5.8 of chapter 5 in ES&HD-5000.

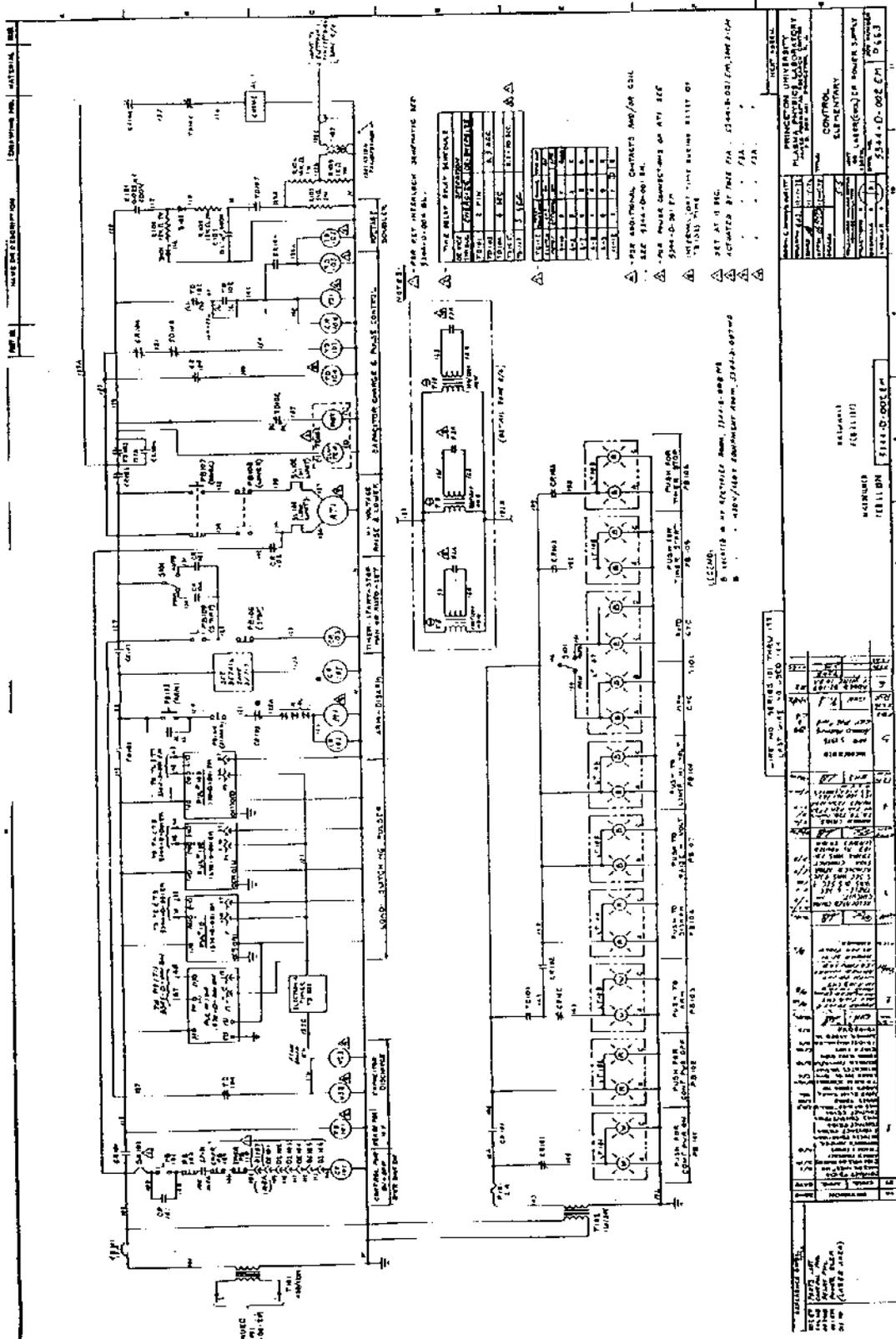


FIGURE 3
PSIS CONTROL ELEMENTARY DIAGRAM