THE PERSONNEL SAFETY SYSTEM AT IASA

M.P. Tzamtzi, D. Economou, P. Phinou, E. Stiliaris
IASA, Athens, P.O. Box 17214, 10024, GREECE

Abstract

This paper describes the design philosophy, the logic and the implementation of the Personnel Safety System (PSS) at the Institute of Accelerating Systems and Applications (IASA). The PSS aims to protect personnel from potential hazards coming from the operation of the Race Track Microtron electron accelerator (240MeV), which is under construction [1]. The implementation of the IASA's PSS is based on the Series One Programmable Controller of General Electric. The PSS's reliability is guaranteed by redundancy, multiplicity and diversity.

1 LOGIC STRUCTURE OF PSS

The PSS is functioning in three different modes of access (**Full Access Mode, No Access Mode** and **Controlled Access Mode**) (Fig. 1), which represent the level of access in the interlocked areas determined by the following two operational conditions of the accelerator:

- **Power Permit**, during which the operation of High Voltage and RF Power are enabled and
- **Beam Permit**, during which beam production is enabled.

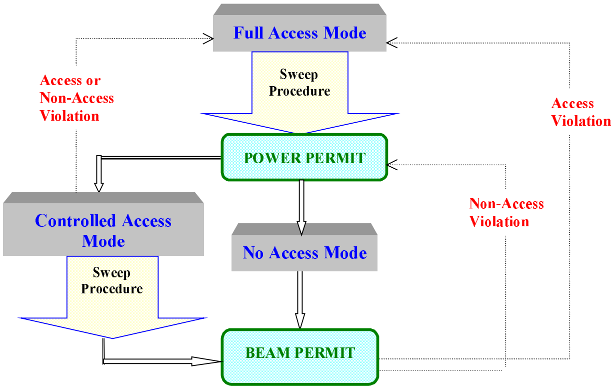

Figure1: Access Level Structure of the PSS

The **Full Access Mode** corresponds to the level of access before the establishment of Power Permit. In this mode the PSS permits free access to the interlocked areas.

The **No Access Mode** is the normal level of access during the Power Permit and Beam Permit operational conditions. In this mode, no person is permitted to access the interlocked areas.

The **Controlled Access Mode** can be established during Power Permit, in order to make possible the presence of technical personnel inside the interlocked areas while high power is present. In order to maintain personnel safety standards as high as possible, strict rules are followed during the whole procedure. The Radiation Safety Officer is informed of the identity and number of persons, hands out personal radiation dosimeters and logs down the procedure. Using a special Control Access key, he/she enables the use of Interlock Bypass keys, which are handed out to the personnel entering the interlocked areas and are returned after the end of the procedure. Each Interlock Bypass key can bypass the door interlock for 15 seconds and is used to get into the interlocked areas. It is important to mention that during Beam Permit, access is not allowed to the interlocked areas for any reason.

The **Sweep Procedure** is needed to certify that no person has remained in the interlocked areas before entering to the No Access Mode from the Full Access Mode or the Controlled Access Mode. It is controlled by a Master Search Station installed at the accelerator tunnel entrance. The Sweep Procedure is successfully completed after a series of switches in the form of push-buttons are energized in a specific sequence. If the right sequence is not satisfied, the sweep procedure is cancelled and must be repeated. The sweep procedure must be completed in a pre-specified period of time (e.g. 5 min).

As it follows from Fig. 1, the PSS returns to a safe operational condition, whenever an interlock violation occurs. The Non-Access violation refers to the case when excessive radiation is measured in occupied areas. When Non-Access violation occurs while the PSS is in No Access Mode, the power permission remains. In all other cases, violation causes power shut-down.

1.1 PSS Subsystems

<u>The Radiation Monitoring Subsystem</u> The Radiation Monitoring Subsystem provides alarm signals for excessive radiation, as well as analog control signals for continuous monitoring of the radiation levels. It consists of several area radiation monitors situated in two types of area: a) the No Access areas (accelerator tunnel and other interlocked areas) (Fig. 2) and b) adjacent areas open to the general public. The radiation alarm levels are set near background level and are connected to the PSS, causing a beam shut-off in case of excessive radiation. During the operation of the accelerator, only the alarm signals by the radiation monitors in the open to public areas are enabled. However, during the Controlled Access Mode, when people are present in the interlocked areas, the PSS enables all the hardware alarm signals.

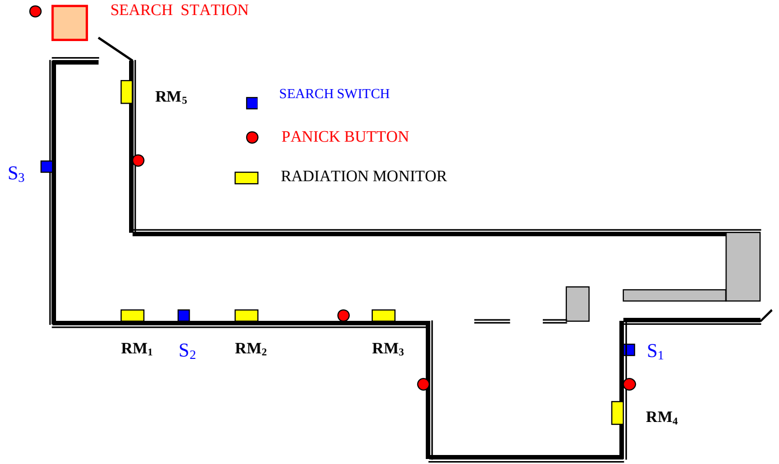

Figure 2: Location of Various PSS Components in the Accelerator Area

PSS Notification Subsystem This subsystem comprise of indicative signs and labels, verbal announcements and warning sounds which inform the personnel on the accelerator operating status, or alert for potential dangers.

Emergency Shutdown Subsystem This subsystem consists of a number of manually operated emergency shutdown switches (panic buttons), which immediately shut off the electrical power supply to the accelerator and the RF system, thus terminating also the possible production of radiation, and protect from other hazards that may occur. These switches are placed along the accelerator tunnel as well as in each area which contains high-to-extreme potential hazard and they are readily accessible to be used in an emergency (Fig. 2).

The Sweep Procedure Subsystem This subsystem consists of a Master Search Station located at the entrance of the accelerator vault and a series of search switches located along the accelerator vault and experimental area and in any other area which is kept interlocked (Fig. 2).

The Access Control Interlock Subsystem This subsystem will guarantee that no one enters the accelerator vault or any other interlocked area, when No Access Mode is established. It consists of a series of position sensors at the doors informing whether each door is open or closed. There are double switches on each door (redundancy) and of different technology (magnetic and mechanical switches). When the interlock logic for a given area is overridden, this subsystem provides a fast turnoff of the beam and high power.

The PSS Status Monitoring Subsystem This subsystem produces digital signals that report the status of the PSS system. These signals will be available to the system operator through special screens of the accelerator monitoring and control system, implemented with EPICS.

2 PSS RELIABILITY

The basic principles followed for the design and the implementation of IASA's PSS are based on the experience gained from large accelerator facilities and all aim in the system's operability and non-failure [2], [3]. The PSS is characterized by *Redundancy*, *Multiplicity* and *Diversity* [3]. **Redundancy** is achieved by the replication of interlock chains (Fig. 3), from the sensors (e.g. door switches) through to the devices that shut off the beam. The beam can be shut off by either one of these chains. Thus, the PSS would fail only if both chains would fail simultaneously. **Multiplicity** is the use of two or more methods to control the hazard, e.g. two shut off methods for the electron beam and high power. Both methods can be activated by either one of the two chains. Finally, **diversity** is the use of different technologies for the multiple shut off methods. For example, to stop the electron beam the bias voltage in the electron gun which suppresses the extraction of electrons is increased negatively and, simultaneously, a beam stopper is inserted at the output of the electron gun. If the stopper insertion is not confirmed properly, the PLCs proceed in the high voltage and RF shutdown.

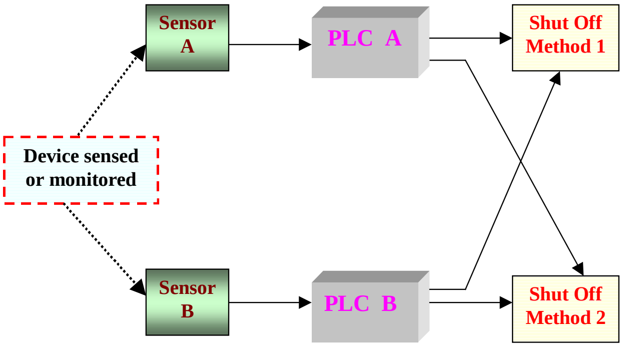

Figure 3: Redundancy and Multiplicity of PSS ([3])

3 IMPLEMENTATION

3.1 Programmable Logic Controllers

The PSS is implemented using Programmable Logic Controllers (PLCs). PLCs have important advantages in comparison with relays, since they provide flexibility and they can be easily reprogrammed if the requirements change. Thus, their use is perfectly suitable for facilities like the one of IASA, where a staged commissioning and operation of the accelerator is taking place. The PSS tailored to the needs of the present status of the facility, will be very easily expanded for future IASA development. In addition, the PLCs provide the possibility to use timers, they easily support complex logic, and moreover, they possess internal diagnostics, performing self-tests and shutting down whenever a fault is detected.

The PSS of IASA is implemented using the Series One Programmable Controllers (PCs) of General Electric. The base unit of this PC comprises of one CPU, which can contain over 700 words of user logic (or over 1700 if memory expansion is used), and digital I/O units. When using only one base unit, 64 I/O points are available (with I/O units of 16 circuits each). By adding expansion base units, 112 I/O points become available. Either the I/O units or the CPU can be easily replaced in case of damage. The program stored in the CPU is retained in case of power failure, since the memory is supplied with power from a battery. Moreover the Series One Programmable Controller continuously performs self-tests, and shuts itself off whenever an internal failure is detected. The maximum time that can pass between a change of the inputs of PC and the response at its outputs is less than 360msec. This is considered to be perfectly acceptable and adequate for the PSS functions. The PCs support programs written as ladder logic diagrams.

3.2 Monitoring of PSS Status

The PSS will allow each chain of PLCs to report a variety of information (including status of I/O points, faults, etc.) to various EPICS database records. Once it is available as a collection of EPICS database records, any authorized workstation has the ability to display the status of PSS. This information could be used for validation, fault tracing, alarming or user training and debugging.

Each individual PLC chain is responsible for sending the appropriate data to the EPICS database. It is also a requirement that the EPICS interface is not an integral function of the PSS operation (i.e. if the IOC goes down, the PSS must still function). Finally, it is also necessary that the communication is a read-only operation (the database must not have the ability to write into the PLC data space). A schematic diagram of this architecture is shown in Fig. 4. Status signals are interfaced to the VME bus and thereafter analyzed with the VMIVME-2534 module. Analog readout values from the radiation monitors are passed to the XVME-566 ADC module.

The EPICS tool MEDM (Motif based Editor and Display Manager) can be used to build a variety of screens indicating the status of PLCs and faults caused by abnormal conditions. The Alarm Handler can also be activated to generate software alarm or pre-alarm signals based on the analog information from the Radiation Monitoring System. Alarm signals will be also activated if differences between the corresponding I/O of the two PSS chains are detected, since this would indicate a malfunction of one of the chains (malfunctioning sensor, CPU or I/O unit).

REFERENCES

[1] E. Stiliaris et al, “The IASA 10MeV CW-Linac”, EPAC 2000, THP4A15.

[2] “Radiation Alarms and Access Control Systems”', NCRP Report No.88, National Council on Radiation Protection and Measurements, Washington, 1986.

[3] “Workshop on Personnel Safety Interlocks”, CEBAF TN-90-233, 1990.

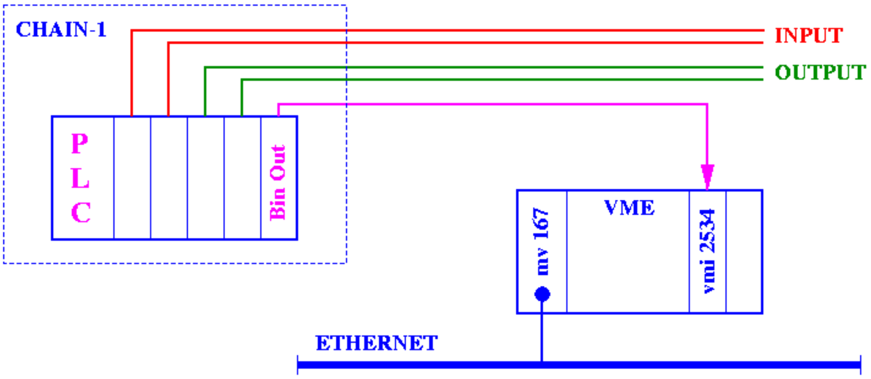

Figure 4: Schematic Layout of the Personal Safety System Architecture