THE DARESBURY PERSONNEL SAFETY SYSTEM

D.E. Poole and T. Ring
SERC Daresbury Laboratory, Warrington WA4 4AD, U.K.

Abstract

The personnel safety system designed for the SRS at Daresbury is a unified system covering the three accelerators of the source itself, the beamlines and the experimental stations. The system has also been applied to the experimental areas of the Nuclear Structure Facility, and is therefore established as a site standard. A dual guardline interlock module forms a building block for a relay based interlock system completely independent of the machine control system, although comprehensive monitoring of the system status via the control system computer is a feature. An outline of the design criteria adopted for the system is presented together with a more detailed description of the philosophy of the guardline logic and the way this is implemented in a standard modular form. The emphasis is on the design features of a modern microprocessor based variant of the original SRS system. Experience with the original system during build-up and operation of the SRS facility is described.

1. Introduction

The SRS personnel safety system defines safe operating conditions and then authorises operation by presenting to the SRS machine and beamline control systems master 'permit to operate' interlocks. General categories of SRS operation supervised by the system are:

Injection

The primary concern during injection is to establish safe conditions for transferring beam from the linac, through to the booster synchrotron and then into the storage ring. Beam transfer is one of a number of alternative beam mode and test options provided by the system, figure 1.

Essential conditions required for transfer are that all interlocked machine areas are clear of personnel and secure, the main beam port shutter to each experimental line is closed and all interlocked beamline and area radiation monitors supervising levels during beam filling are below trip level.

Following the successful completion of the injection process and the ramping of stored beam to full energy, activity at the SRS facility proceeds in two main areas. Both involve the personnel safety system.

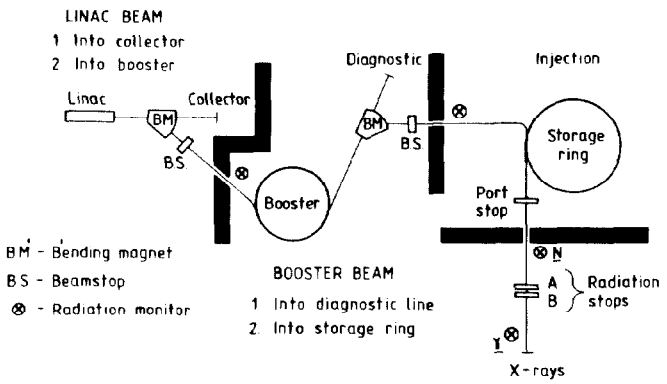

Fig. 1. SRS beam modes and main safety elements.

Exploitation

Beamlines and experimental stations are in operation with the line safety system protecting users against the hazards of exposure to the synchrotron radiation beam. Beamline radiation monitors interlocked to the beam port shutters protect against high energy gas bremsstrahlung.

Fully interlocked experimental hutches prevent exposure to the intense x-ray beam exiting into air at those stations exploiting the short wavelength end of the synchrotron radiation spectrum. Simple enclosure interlocks are adopted at the VUV stations where both the beam and the sample are contained within the beamline vacuum envelope. Each experimental station is interlocked to individual station shutters. Emergency off buttons at each station will trip both the station and the main beam port shutters.

Linac and Booster Development

During stable stored beam both the Linac and Booster machines can be operated as independent systems. Linac development can be carried out by switching the Linac beam into a local collector or the Booster can beam into a diagnostic line. Controlled access is available to both machines under no-beam conditions.

2. Philosophy

Very early in the SRS project a number of general guidelines were agreed. A common, or unified system covering all sections of the machine was to be adopted, later extended to cover the experimental beamlines and stations. The aim was to protect people and not items of plant so the system was to be fully independent and distinct from the machine control system. The system was to provide the operational flexibility required for the various modes of operation specified (injection and beam stacking, stable stored beam and a number of beam and test options) yet was to be sufficiently comprehensive and tightly defined so that reliance on administrative procedures was minimised. The system was to be simple to implement with progressive build-up during the construction phase of the SRS and easily adaptable during subsequent machine operation.

Stress was placed on simple, yet secure, operation of the experimental stations.

3. System Design

Three criteria were set in the initial phase of the SRS design study:

1. A system of hardwire interlocks would be adopted in which two independent interlock chains must give an agreed output to complete an interlock sequence. Such a system is unconditionally fail safe to any single logic element fault but there is then a comcomitant requirement that the system can detect any single fault condition.

2. Computer supervision down to the level of each interlock element was to be adopted. The SRS control

CH2669-0/89/0000-1931$01.00©1989 IEEE

computer would not exercise any authority over what is, or is not, a safe operating condition but would be used to generate colour display mimics and tabulated listings of system status as an aid to system operation, development and fault diagnostics.

3. A modular system was to be developed, applicable throughout the SRS facility.

The Personnel Safety Logic Module

Initial studies[1] determined the type of logic module required and the basic format of the guardline logic, figure 2.

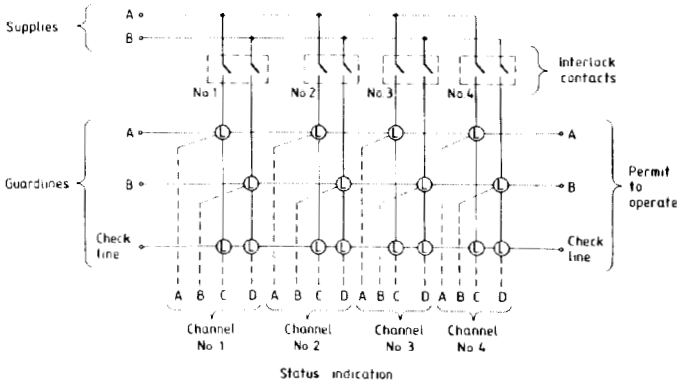

Fig. 2. Guardline logic network.

Essentially the adopted format is a dual guardline (A and B) system in which machine interlock contacts (door switches, key switches, etc.) are hardwire connected directly to logic elements forming a series logic sequence. However, a third guardline or checkline is added which appears to increase the complexity of the guardline logic, but a number of observations were made in the original design study:

1. The status of the four logic elements forming each interlock point (A, B, C and D) will be fed to the computer so that, when testing, the computer will be able to differentiate between single logic failures within a module and contact or wiring faults external to the module:

Logic Element Status:	A	B	C	D	
	0	0	0	0	Normal status OFF
	1	1	1	1	Normal status ON
	1	0	1	0	External fault
	0	1	0	1	
	0	1	1	1	
	1	0	1	1	Module fault
	1	1	0	1	(single bit error)
	1	1	1	0	

This ability to both identify and locate faults will greatly improve fault diagnostics and assist regular routine testing.

2. Simple logic elements designed to achieve maximum reliability can be adopted. This assumption is particularly valid if it is appreciated that overall system reliability is dominated by the reliability of installed switch mechanisms and contacts, and if regular testing of the network is possible.

3. If separate power supplies and reset facilities are provided the network will offer added security against common mode faults and a higher level of network security will be achieved.

Hardware

To test the guardline principles two modules were designed, one using simple relay latches for each logic element, the other solid state. An appraisal both in terms of cost and effectiveness in satisfying safety criteria established the relay system as the choice for the SRS system. Other sources gave some support to this decision.[2]

The modern variant of the original module design and the associated crate hardware is illustrated in figure 3. Each module contains the sixteen logic element relays servicing four separate interlock channels (doors, beamstops, etc.) and a latch reset relay. The standard module can perform a latching or non-latching function or can be set to perform a sequential latching function when a predetermined interlock sequence (area search) is required. The crate accommodates up to 22 interlock modules.

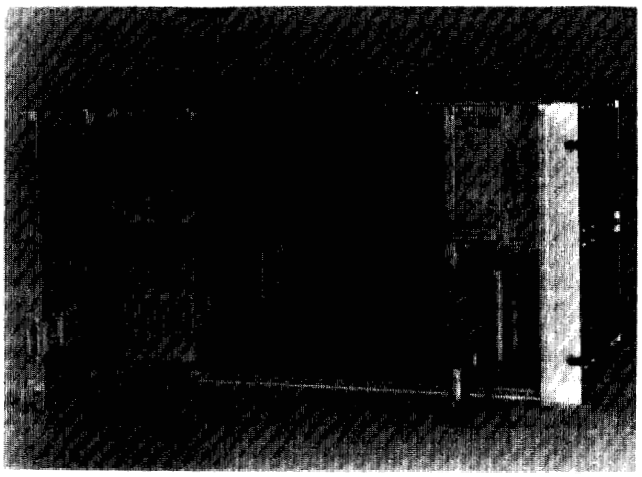

Fig. 3. The SRS personnel safety system logic crate.

Contacts from each logic element relay form the three independent guardlines (A B and checkline). These are linked out direct to a module wire wrap backplane where hardwire interconnections between modules are then used to complete the required interlock logical sequences.

The crate also incorporates a microprocessor backplane bus linking modules. This functions as a data highway and provides a channel for monitoring the status of each interlock relay, receiving interlock resets and monitoring the status of the three independent logic guardlines. A standard (G64) microprocessor with system I/O board serves as an intelligent crate controller. Up to sixteen distributed system crates can be linked direct through a parallel highway and CAMAC 24 bit I/O register to the SRS computer network. The monitoring and control electronics, crate power supply and earth system are completely isolated from the system interlock relays and hardwire guardlines. These are serviced by separate external power supplies.

4. Implementation

All systems logic functions are performed by standard interlock modules. In the SRS these are organised into three logic centres which are accessible at all times but located close to the areas served. A two crate system services the Linac and Booster machines, a six crate system provides all storage ring

system and area interlocks and a nine crate system provides centralised services for all installed beamlines and experimental stations.

Each logic centre is linked to the SRS control computer and each provides the master 'permit' interlocks to plant and also outputs to local area service boxes. These service boxes provide control of electrically operated door and keylock solenoids and supply services for all area warning and status signs.

Full supervision of all machine and beamline systems is available via computer generated mimic and status displays at a safety console located in the SRS control room. At this central point operations staff can monitor the operation of any beamline station or interlocked experimental hutch and can exercise more direct control and supervision over the machine personnel safety systems. Control features are:

a) Machine area search and lock-up with the computer supervising and timing correct search procedure.

b) Supervised access control to interlocked machine areas, the operator releasing the electrical door lock when it is confirmed that each individual entering the area has taken an access safety key.

c) General system control: beam mode and test option selection, beam port shutter control and set 'stable stored beam'.

In addition to the mimic and status displays automatically presented to the operator during area search and lock-up, the following status displays are available on demand:

a) Beamstat. This lists the operational status of all interlocks required to raise any one of three beam mode options, linac beam on test, booster beam on test and beam injection into the storage ring.

b) Radstat. This lists the operational status of all health physics monitor interlocks in the SRS. The analogue levels from each monitor are also linked via a central signal distribution amplifier system to the SRS computer for data logging and display.

c) Linestat. This displays the status of the safety interlocks at each beam port and provides access for displaying a constantly refreshed logic mimic of any beamline station and interlocked experimental hutch. Mimics are entered using an interactive graphics package and are immediately available on-line. A typical display mimic is shown in figure 4.

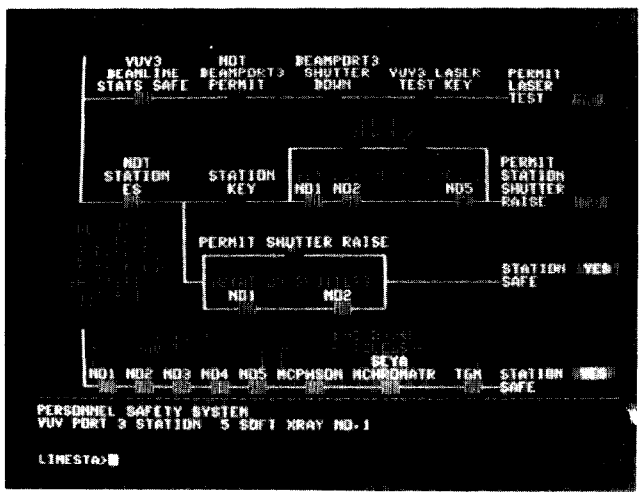

Fig. 4. A typical status display mimic.

d) PSDBUG. This is a tabulated presentation of the status of every logic element in the SRS personnel safety system and serves as the main diagnostic tool during system commissioning, fault finding and regular scheduled test.

The display is organised so that each crate of logic modules in the system can be displayed on demand, the operational status of all logic elements and guardlines in this crate being listed. The computer detects fault states and sets the appropriate flags to indicate either a fault within the interlock module or wiring or contact faults in the external machine area networks.

5. Operational Experience

The first sections of the SRS personnel safety system, those for the injection system, became operational in 1978. Since that time there has been a gradual and, because of the simple modular hardware, a graceful build-up to a full system installation involving in excess of three hundred interlock modules. Throughout this period, the build-up has been coordinated with the development of the SRS facility and the installation of new beamlines and stations.

Dominant features of the system are the flexibility of the modular construction and the ease with which new systems can be installed and commissioned. Use of the diagnostic PSDBUG has eliminated the need for extensive supervision and check-out during installation with system testing essentially limited to commissioning of a fully installed system. Modifications for operational reasons to the installed system can be very quickly introduced.

As expected, by far the majority of faults experienced during the period of operation have been associated with faulty switch mechanisms in the machine areas and the failure of mains driven systems, door and key lock solenoids and warning signs. The replacement and upgrade of switch mechanisms has gradually reduced the incidence of failure and simple procedures like better ventilation and planned maintenance have improved the reliability of mains driven solenoids and warning signs. Faults in the installed logic modules have been very much the exception. In the entire period of operation less than one dozen faults attributable to failure of the logic element relays have been detected (< 0.01% per 1000 hours) following an initial inspection, test and short infant mortality period. A potential fail danger (i.e. sticking contact) fault has never been detected.

Apart from regular, scheduled test exercises to confirm system integrity the system requires little operational support. During operation, any faults must be reported to the responsible section with the operations staff restricted to simple fault procedures such as the changing of logic modules. The frequency with which faults occur, however, is such that very few out of hours calls for assistance are required (recently less than two per year).

We take pleasure in acknowledging the contribution of E.V. Carter to developing and commissioning the installed system and M.J. Dufau, W.R. Rawlinson and K.S. Turner for software support.

6. References

1. T. Ring, 'SRS Personnel Safety: Sequential Guardline Logic', Daresbury Note SRS/NS/76/80 (1976).

2. N.G. Dennis, 'Insight into Standby Redundancy via Unreliability', IEEE Transactions on Reliability, Vol. R-23, No. 5, pp.305-313, December 1974.