THE SAFETY INTERLOCK SYSTEM AT TRIUMF

J. Drozdoff, L. King, L. Moritz and G. Wait
TRIUMF, 4004 Wesbrook Mall, Vancouver, B.C., Canada V6T 2A3

ABSTRACT

The TRIUMF central safety system is a microprocessor-based interlock system that handles both the personnel access control functions as well as many machine protect functions. The latter have been included in the system because of its high reliability. There are twelve separate exclusion areas each with its own small local controller for monitoring area status and lock-up sequences. All inputs to the central system are in the form of isolated contact closures indicating the safe status. There are at present some 300 such inputs. The interlock conditions reside in erasable programmable read-only memory (EPROM) in the form of a sequence of logic equations in Boolean algebra. Whenever the system senses a change in state of any of the input parameters all the equations are scanned to evaluate the output parameters. Permissives are then generated as +24 volt D.C. levels in accordance with the logic equations. A large, page-selectable CRT monitor displays the status of all input devices as well as the state of the permissives. Operator input is provided via a CRT touchpanel. Changes to the logic equations are verified on an identical system used as a simulator before being burned into a new set of EPROMs. Making a change to the system thus requires only a few minutes of down-time. This system has been in operation for several years with a high degree of reliability.

INTRODUCTION

The central electronics for the TRIUMF safety system consists of two CAMAC crates and related interfacing equipment. Intelligence for both crates is provided by a single Kinetics 3880 microcomputer which reads 24 volt binary inputs, executes a series of logic equations, and generates both internally defined intermediate values and 24 volt outputs. The conditions that cause these outputs to be set essentially define the central safety system; the outputs enable access key release units, drive beamstops, annunciate alarms, and in general, ensure the cyclotron is operating safely. Although the crates operate as a stand-alone system, the use of a CAMAC dual port memory allows the transfer of data to and from the TRIUMF central control system. The status of all input, output, and intermediate value bits is available in this memory to the control system computers which perform the display tasks. Figure 1 shows an overall schematic of the system hardware.

1) Inputs

All inputs to the central safety system are in the form of 24 volt D.C. signals. The 24 volt level is provided by the safety system bus at a central break-out panel and is derived from an uninterruptable power supply. Device status is indicated by an isolated contact closure, the closed contact being interpreted as a logical '1' or safe condition. The system is thus 'fail safe' in the sense that a localized power failure or a cut or disconnected signal cable indicates a logical '0' or unsafe condition. Figure 2 illustrates how the status of two typical contacts reaches the microcomputer via the Kinetics 3471 input registers.

Routing all inputs through a central break-out panel (BOP) also provides the capability of simulating any input should contacts fail or require over-riding. Safe states are simulated by shorting the input with a jumper consisting of a

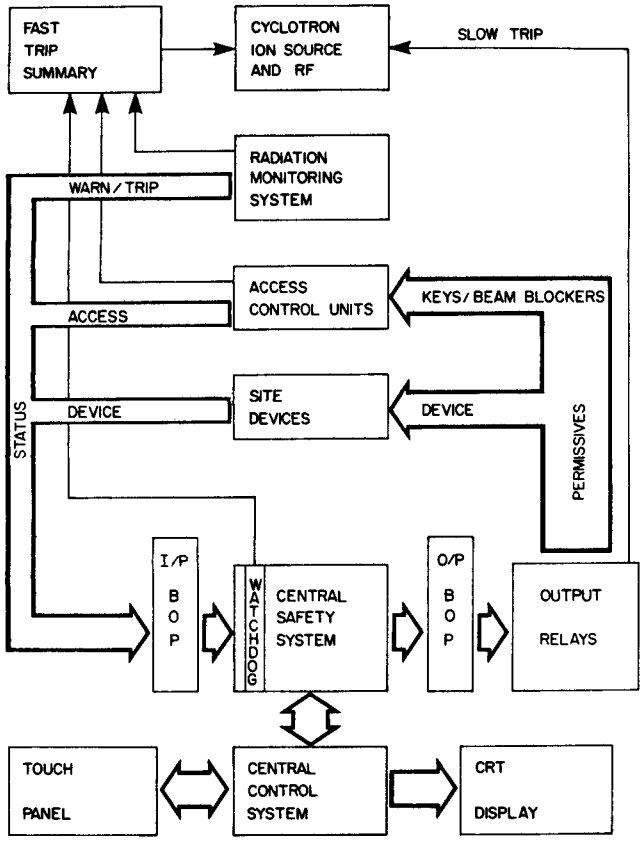

Fig. 1. Overview of the TRIUMF safety system.

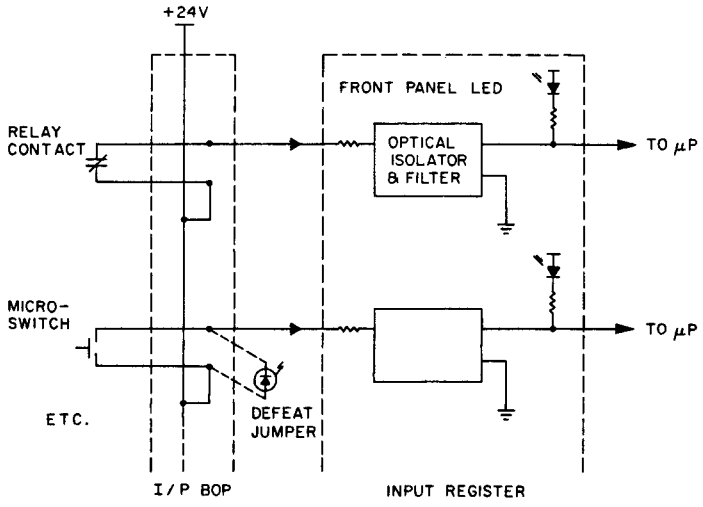

Fig. 2. Typical input configuration for the TRIUMF safety system.

bi-polar LED. In this way the real status of the input is immediately apparent, the LED being 'ON' only if the contact closure is open. A timer inside the locked input panel must be acknowledged once per shift by the operators to force a checking of defeats against a log. Defeating of input signals can only take place over the shift supervisor's signature.

2) Design of Firmware and Logic

The conditions for safe operation of the facility are currently defined by a set of 385 logic equations executed by a Kinetics 3880 microcomputer based on the 8 bit 8080A microprocessor, although each revision typically adds a few more statements. The program is written as a set of equations in Boolean algebra, using mnemonics to represent input and output variables, and the symbols *, + and / to represent the Boolean operators AND, OR, and NOT respectively.

The first section of logic generates a series of internally stored intermediate variables which evaluate expressions repeatedly used in other equations in order to shorten computing time. Much of this section of code is devoted to generating "truly in" (IN AND NOT OUT) and "truly out" (OUT AND NOT IN) values for every device that has two limits. A typical equation defining the cyclotron off condition is:

YCYCOF = YISOF * (MM + RF)

i.e. cyclotron off = ion source off AND either Main Magnet off OR RF system off.

The next section of code uses the intermediate variables and input states to generate hardwired 24 volt outputs. The remaining lines of logic coding create more intermediate values using the output states in the logical expressions. These are used exclusively for display purposes.

The equations are 'stored' in EPROMs located in a Kinetics 3816 memory expansion unit. One single 'base' EPROM resides in the 3880 and executes CAMAC cycles and controls two software timers used in the access key release function. The microcomputer continuously scans all inputs without actually executing the logic equations. When it detects a change of state of any input, however, it runs through all logic equations, executing each once. While a read cycle takes about 5 ms, the time required to execute the logic is 70 ms. On every read cycle the microcomputer strobes a Joerger Watch dog WT module. If the watch dog is not strobed within the specified time (100 ms), a relay contact in the module opens and trips the ion source via a fast direct line. Such direct lines paralleling the computer system are also provided for two other functions; the trips from the radiation monitoring system caused by excessive beamspill and the trips from the emergency push button summaries of the controlled access areas.

3) Outputs

Hardware outputs are generated in eight 32 channel GEC 1617 output registers. These sink current to ground energizing 24 volt relays (Fig. 3) and powering a green LED. 24 volts is sent to a normally open contact of each relay via a 24 volt bus and it is this voltage which is used to turn on status lights, sound alarms and enable site devices. Thus a power failure disables all devices.

4) Communications

The central safety system writes the current status of all inputs, intermediate values, and outputs to a bi-directional CAMAC memory in the central control

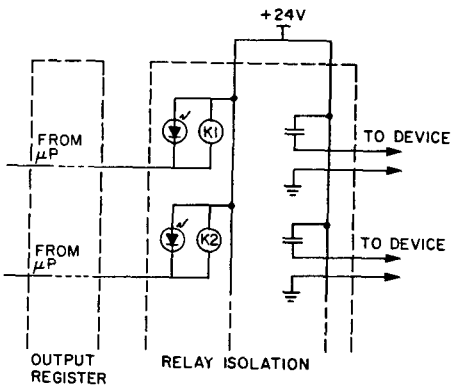

Fig. 3. Typical output configuration for the TRIUMF safety system.

system. The computers of the control system then generate the display on a dedicated CRT monitor. The display is page selectable and there is a general summary page as well as a page for every access control area and major system. Operator control is exercised through a Kinetics 5209 Touchpanel, a device consisting of a 22.5 cm CRT monitor with a touch-sensitive transparent screen. Imbedded in the screen is a 4 × 4 matrix of capacitance switches so that the legend and function of the 16 switches can be changed at will under computer control. Currently any one of 15 existing pages can be called up from an index page. A separate push button must first be pressed to activate any of the touchpanel switches in order to prevent accidental or inadvertent use of the panel. Touchpanel inputs are relayed to the safety system by the central control system but are treated like all other inputs in the logic equations.

5) Altering the Logic

The logic equations written in Boolean algebra are normally edited on the University of B.C. Amdahl V8 computer. We have written a compiler which generates a code composed of macro calls from the Boolean logic equations and replaces input mnemonics with 3880 address codes. The compiled logic is then transferred to a development system, linked with the required CAMAC and timer routines and tested on a simulator. The simulator is virtually identical to the central safety system except that inputs are simulated by a panel of shorting pins and outputs by a panel of LEDs.

Once the program has been debugged it is burned into a set of EPROMs and given a final check on the simulator.

6) Experience and Reliability

The central safety system as described has been operating without substantial interruption since December of 1978. The only regular 'down-times' are approximately 10 minute long periods occurring at intervals of one to two months in order to replace the set of logic equations to accommodate changes required by alterations and additions to the site.

There has been one failure of the central system since it was installed, the failure being in the uninterruptable power supply to the CAMAC crates. Due to the fail safe design no unsafe condition occurred during this failure.