THE SAFETY INTERLOCKING SYSTEM AT THE NAC

K. Visser and H. Mostert
National Accelerator Centre, CSIR, P O Box 72, FAURE, 7131 Republic of South Africa

Summary

The central safety interlocking system (CSIS) controls the higher level of interlocking between the various cyclotron subsystems. It ensures the safe operation of the entire cyclotron facility as regards personnel safety and proper instrument operation. The system consists of a micro-processor with a ROM-based safety interlocking program, relay output modules providing "safety OK" instructions to all interlocked apparatus, alarm input modules connected to transducers providing binary alarm status signals and an interface to the central control computer. All solid state electronic components of the system are situated in a low level radiation area and are interfaced to cyclotron equipment by means of 24 V relays.

System Hardware

Micro-processor

An Intel 8085 central processing unit is used in a stand-alone mode with 1K bytes of random access memory for variables and 16K bytes of erasable read-only-memory containing the assembled safety interlocking program.

The ROM-based system ensures the immediate availability of the program in memory, ready to run at power-on, compared to a floppy-disc based system. It is also less prone to program corruption by power failures and offers a more stable program preventing the overriding of a particular interlock requirement by an operator at the control console.

The appropriate way to modify and extend the safety interlock requirements is to modify the assembly language program in the development system, burn the machine code into EPROM and test its functioning on the simulation system, before transferring the new EPROMS to the actual CSIS.

At present this section of the hardware is being upgraded to consist of a microcomputer running under the CP/M operating system. Furthermore, the safety interlocking source program is now being written in the Pascal language rather than in Intel 8085 Assembler, and will be compiled by the Pascal MT/PLUS compiler to give ROM-able executable machine code.

Relay output modules

Binary status "safety OK" outputs are issued by the CSIS to individual cyclotron equipment. The CSIS grants permission for the particular apparatus to be set to a potentially dangerous state either by the control computer or manually from the front panel of the equipment.

The "OK" signals are provided by means of relay contacts which are actively closed by the CSIS when the "OK" commands are granted. Actively closed relays provide electrical isolation between subsystems as well as fail-safe characteristics in that loss of line continuity is interpreted in the same way as a cancellation of a granted "OK". Withdrawal of a granted "OK" forces the interlocked equipment to revert to its safe state.

Each relay output module handles 32 binary variables which are transferred via individual twisted line pairs to the interlocked equipment. The "OK" signals include permission for various power supplies to be switched on or off, diagnostic probes to be moved beyond specified limits, vacuum valves to open or close, access doors to radiation areas to open and the magnet lift mechanism to be operated. By integrating the access control to radiation areas, the radiation monitoring system and the supervisory control of interlocked cyclotron equipment, the CSIS provides the necessary safety interlocking.

Relay input modules

Transducers controlling binary input status variables are used to indicate various "alarm" or potentially unsafe states to the CSIS. The "safe" status of a variable is indicated by a relay contact being actively closed by the transducer. This gives fail-safe features, since the loss of electrical power on the appratus or a break in the continuity of the line to the input module will be registered by the CSIS as an "alarm" state.

To prevent accidental loss of electrical conductivity causing a number of variables to be received incorrectly, time multiplexing of the input signals takes place only inside the relay input modules close to the processor. A twisted line pair from each alarm transducer and contact is connected to a 24V supply and activates a relay coil inside of the input module.

The alarm variables consist of the ON or OFF status of power supplies, status signals indicating whether variable currents and voltages are within their specified limits, the open or closed status of vacuum valves, the spatial position of the ion source as well as beam diagnostic probes, slits, Faraday cups and beam stops, the setpoint status from vacuum gauges, radiation monitors and smoke detectors and the area clear and secure status from radiation areas.

The area clear and secure status monitors are used to prevent the production of beam in areas that can normally be accessed by personnel. For each radiation area it consists of a dual set of switches on each access door and a number of watchman stations inside of the radiation area. When an area needs to be cleared for beam-on conditions, an audible and visible clearance warning is given and all access doors except the main one must be closed. A radiation officer has to inspect the radiation area visually and must activate each of the watchman stations in the proper sequence and within a set time limit, if the immediate vicinity of the watchman station is cleared of other personnel. After his inspection he leaves via and closes the main access door and activates the final watchman station just outside of the main door. An area clear status is then provided to the CSIS after completion of a successful clearance procedure.

CH1996-3/84/0000-0345 $1.00 © 1984 IEEE

Before being able to open an access door to a cleared area, permission must be obtained from the operator at the control console. This will be granted via the CSIS. Should an access door be opened without prior consent, as might happen in an emergency, the dual set of switches on the door will indicate an alarm state which will be latched as an alarm condition, while the CSIS will prevent "Beam ON" conditions in the affected area. If the status from the two switches on each door do not agree for a period of time longer than 0,1 second, an alarm condition is also flagged, since it is interpreted as one of the redundant switches being faulty.

Radiation monitor checking of the level of gamma radiation and the neutron flux density is also being implemented. The variable setpoint levels for each transducer are set to indicate a safe upper limit for personnel in the vicinity of the monitor. The setpoint operates a relay, the contacts of which couple to the CSIS in a similar way as do all other alarm inputs. The modular radiation monitoring system has its own visual and alarm units, while an analogue output signal is used as input to a CAMAC input module for continuous monitoring of the actual radiation level of each detector.

CAMAC interface

For communication with the central control computers an interface is provided which couples to a 16 bit input-gate/output-register CAMAC module. Via this CAMAC communication link the central control computers instruct the CSIS to compare the status of the "alarm" variables to the appropriate set of safety interlocking equations and to grant the associated set of "safety OK" commands for the particular radiation area being selected for BEAM ON or STANDBY by the operator at the control console.

Should the CSIS detect that any input variable indicates an "alarm" status and thereby negates an interlock equation, it will cancel a previously granted "safety OK" to the affected cyclotron subsystem to effect a partial shutdown of the beam. It will also transfer an encoded label to the central control computer to identify the variable indicating the "alarm" state. The control computer displays the associated error message(s) and logs the "alarm" in an error file.

To prevent an incorrect transfer of data between the CSIS and the control computer causing potential disaster by selection of another area, the communications protocol was programmed in such a way that any transferred data word is first echoed back to its source for comparison with the original. In case of agreement a single command is sent to indicate its correct transfer and permission to be acted on by the receiving processor. If three successive transfer failures occur, the CSIS reverts to its initial startup condition and the loss of communication is reported by the central control computer to the operator.

If the micro-processor in the CSIS should hang itself and stops executing its monitor procedure, a watchdog timer in the system times out and causes a hard-wired interrupt and transfer of an error code to the control computer. It also cancels all "safety OK" commands by disabling their latches, if the central control computer cannot reset the CSIS processor within a 1 second time limit. The watchdog timer consists of a mono-stable that has to be retriggered regularly by a software routine forming part of the monitor loop. Under normal conditions the retrigger time is shorter than its time-out period of 1 second.

Software implementation

To keep the system as flexible as possible use is made of equate tables in the program to identify the address of each "alarm" and "safety OK" variable which depends upon the hardware connection to a particular port and bit position in that port. This provides freedom in the laying of cables and the connection of the CSIS to the interlocked apparatus.

To provide a reasonable response time from the moment an alarm condition occurs until intervening action is taken, the program is structured in such a way that the appropriate set of "safety OK" signals is granted according to the "alarm" inputs and the safety interlocking equations. The status values of the implemented input variables are then polled on a byte-wide basis to check for a change of state condition. As soon as the change of state flag is set by an "alarm" variable changing its binary status, the safety interlocking equations and "safety OK" commands are re-evaluated and issued to the interlocked apparatus. For 100 "alarm" variables the response time is less than 1 millisecond which is of the same order as the relay switching time.

Conclusion

The attractive feature of the system is its flexibility in that modifications to the interlocking requirements can be made relatively easily by changing the software. The defining addresses for accessing the binary variables are also programmable. Another advantage is that the whole system can be expanded and upgraded to cope with the growing needs as the cyclotron facility expands.