Upgrading the Daresbury Personnel Safety Interlock System.

J. R. Alexander[1], M. T. Heron[2]

[1]CCLRC Daresbury Laboratory, Warrington, UK

[2]Diamond Light Source Ltd, Chilton, Didcot, UK

ABSTRACT

The Daresbury Personnel Safety Interlock System was designed in the late 1970s for use on the Daresbury Synchrotron Radiation Source (SRS), which started operation in 1980. It is a modular, relay-based, dual guardline logic system which uses wire-wrap backplanes to define the logic to be implemented. It has subsequently been used on the Daresbury Nuclear Structure Facility, and the European Synchrotron Radiation Facility at Grenoble; it will shortly be in use at the UK's new synchrotron light source, Diamond, and the Daresbury Energy Recovery Linac Prototype; and it will be used to replace the obsolete Personnel Protection System at ISIS (the UK's spallation neutron source) when a second spallation target is added in 2007.

The system incorporates a microprocessor bus to provide for remote monitoring of all interlock inputs and outputs. In the original design this bus was a modified CAMAC bus. A Mk II design of the late 1980's uses identical relay interlock circuitry, implemented on a 6U Eurocard format with readout via the G64 bus. The upgrade described in this paper retains the Eurocard format and the G64 bus, for backwards compatibility, but introduces a VME-to-G64 interface to allow the use of a commercial VME processor card in the logic crate. Processor cards with Ethernet connectivity have been used to implement stand-alone servers compatible with the SRS Control System, and with the EPICS control system to be used on Diamond. At the same time, improved test and diagnostics facilities have been incorporated into the PS system hardware.

INTRODUCTION

In 1999 an assessment was made of the options for implementing a Personnel Safety (PS) interlock system for Diamond, the proposed new synchrotron light source for the UK. The following basic options were identified:

- to adopt the relay-based Daresbury PS Interlock System, which was designed at Daresbury Laboratory for (and is still in use on) the existing Synchrotron Radiation Source (SRS) sited there;
- to design an entirely new system in house;
- to adopt a commercial solution.

The first of these options was eventually adopted, with the system modifications which are the main subject of this paper. However, it is worth reviewing the decision process which resulted in this outcome.

Firstly, a brief review of safety interlock systems used at other accelerator laboratories was undertaken. This indicated that there is no emerging 'standard' interlock system which could be adopted, and that most systems were designed in-house rather than being bought-in (proprietary) solutions. This is not surprising, since accelerator laboratories (and nuclear installations) generally required high integrity interlock systems before these became a general requirement in other industries. However this is no longer the case, as is evident from the publication of standards such as EN 954-1:1997 "Safety of Machinery – Safety related parts of control systems" and IEC 61508:1998 "Functional safety of electrical/electronic/programmable electronic related systems". Such specifications have led to the availability of high integrity safety interlock systems from industry. However, the adoption of one of these for the Diamond project was rejected because of the proprietary nature of the hardware which led to concerns about continued product availability, support and future adaptability, when measured against the typical 20-year timescale of an accelerator system.

The review of safety interlock systems indicated that those designed within accelerator laboratories mostly use redundancy (parallel chains of interlock logic, all of which must be satisfied before a safety-critical system can be operated) in order to achieve the desired levels of safety. These systems fell into two basic categories: those which are hardware based, often using relays (as does the SRS design); and those based on two or more parallel chains of PLCs (commercial Programmable Logic Controllers), which were generally programmed in-house. The PLC solution is attractive in using relatively cheap, commercially available hardware with a good track record of support from the manufacturers, but was rejected for the Diamond project due to a lack of in-house experience in programming and maintaining safety-critical software, together with project constraints on timescale and manpower which prevented such experience being acquired or developed.

The existing Daresbury PS Interlock System had the following advantages:

- It had proved extremely reliable over the (then) 20 years operation of the SRS.
- A recent formal review of the design's reliability had shown it to be more than adequate for the task [1].
- Staff with extensive experience in the application and use of the system on the SRS were available to work on the Diamond design.
- Spares and test hardware could be shared between the projects.

Similar considerations have led to the recent decision to use the Daresbury PS Interlock System to upgrade and extend the 'Personnel Protection' system on the ISIS spallation neutron source sited at the CCLRC's Rutherford Appleton Laboratory, as part of the project to install a second spallation target on this machine.

P.S. SYSTEM UPGRADE

As reported in reference [2], the Daresbury PS Interlock System is a modular, configurable, dual guard-line (i.e. having a redundancy of two) logic system which uses relays as the logic elements. The basic unit is the PS Module: a printed circuit board carrying the relays required to service four dual-guardline interlock inputs. Up to 22 modules are housed in a crate (or 'sub-rack'), where the required interlock logic is defined by wire-wrap connections on a backplane. A second backplane provides for remote monitoring of the system by allowing a microprocessor to read the status of the modules' relays, via auxiliary relay contacts, and the status of signals at the final output of each module onto the wire-wrap backplane, via opto-isolators within the modules. System monitoring is optional however, and the microprocessor bus may be omitted, or powered off, without affecting the operation of the interlock logic.

Two physical versions of the Daresbury PS Interlock system have been produced, using identical relay interlock circuitry but different relay types. The earlier Mk I system uses CAMAC mechanics, and the CAMAC backplane to read out the modules' status. The later Mk II system uses Eurocrate dual-height (6U) mechanics, the modules having two backplane connectors: one for the wire-wrap backplane and one for readout via the G64 bus.

By the time that Diamond was being considered, the commercial design and production of G64 modules had ceased, and thus the microprocessor modules used to monitor the PS system were no longer available. The design of a Mk III PS system, using the VME bus in place of the G64 bus, was considered; but this has the disadvantage of only accommodating 20 PS modules plus a processor module in a crate, since the width of VME modules is 4 HP whereas that of CAMAC and G64 modules is 3 HP. A further consideration was the need to support the large number of Mk II systems in use on the SRS. Therefore, it was decided that a VME-to-G64 Interface module would be designed, to be used together with a commercial VME processor in a modified Mk II Personnel Safety crate, – this would still leave space for 22 PS modules in the crate.

The one remaining problem was that Mk II PS modules are 200mm deep (front panel to backplanes), whereas standard VME modules are 160mm deep. The solution to this was to re-design

the layout of the Mk II PS module on a 160mm deep board, without altering the circuit design. At the same time a single 6U-high printed circuit backplane board was designed. This integrates the wire-wrap and G64 backplanes, a 2-slot single-height VME J1 backplane to connect the VME processor to the VME-to-G64 Interface module, and a connector for the triple-output power supply used to power the VME and G64 busses. At the VME processor position it also provides a J2 plug on the rear, to accommodate connection of any processor I/O routed via the 'user-I/O' pins on this connector.

Although this solution lacks full 'backwards compatibility' with the existing Mk II systems, it is possible to use the new backplane in a crate accommodating 200mm modules and to use a simple 40mm extender board for the VME processor module. A similar extender could be provided for the Interface module, but as this has no connectors on its front-panel the panel can simply be removed to allow the Interface to be recessed into the crate.

VME-TO-G64 INTERFACE

The VME-to-G64 Interface module is the size of a standard 6U VME module. It has a VME J1 connector at the standard (i.e. upper) position, and a G64 connector below this. It is fortunate that the PS modules already had their G64 connectors in the lower position, – allowing the G64 bus to directly span these and the Interface module. The modules' wire-wrap connectors are in the upper position; pins on these are tracked on the backplane PCB to provide a unique 'geographical address' for each PS module.

The Interface module maps a number of VME Short-I/O addresses to the G64 bus. It generates a synchronous G64 bus cycle when the VME processor accesses one of these, and synchronises the two bus cycles. As the PS modules only use the lower eight bits of the G64 data bus, the VME processor uses single byte transfers via VME byte1 (bits D07-D00) – which the Interface maps directly to the G64 bits D07-D00.

INCREASED TEST COVERAGE

A redundant safety system must be periodically tested to ensure that each parallel channel (two, in the case of a dual guardline system) is fully functional, since a failure to danger[1] of a single element (input device, logic element, or output device) renders its associated channel ineffective – so that the overall system effectively becomes 'single guardline'. The Daresbury PS Interlock System provided full test coverage of the logic elements within the modules, via the microprocessor readout system, but poor coverage of the crate output elements: the LOP, or Logic Output, relays. Three test relays have therefore been added to the new backplane PCB to overcome this deficiency.

The operation of these test relays can be explained by reference to Fig 1, which is a diagram of an interlock system consisting of a single PS module connected so as to generate a system output only when all four of its input channels are made. Prior to inclusion of the Test Relays A, B and C (on the left of the diagram) it was not possible to individually test the three LOP relays (on the right of the diagram), and thus a fail to danger of any one of these could not be detected.

The test relays can be energised in any combination to remove power from the associated backplane supply lines, – which should then de-energise the associated LOP relays of all LOPs within the crate. The test relays are controlled via a 3-bit register, implemented in the VME-to-G64 Interface module, which is addressed as though it were PS module 0 (the actual modules having addresses 1 to 22).

---

[1] A 'failure to danger' is when an element fails in such a way that it continually indicates a safe condition, whatever the true condition. In the Daresbury PS Interlock System the safe condition is indicated by the existence of a current path – e.g. a closed contact on a door switch or a relay – thus a failure to danger occurs when a contact fails to open. (This mode of operation is sometimes referred to as 'failsafe', because the dominant failure modes are failure to make contact, or a broken wire, which result in an 'unsafe' indication and therefore needlessly stop the equipment under control.)

Drive signals for the relay coils are routed via the Interface module's VME connector pins B5, B7 and B9. (In a normal VME system, these pins are used for three of the 'Bus Grant Out' signals, which are not used in the PS Interlock system.) In order to ensure that erroneous operation of the test relays cannot effect normal system operation, jumper links have been provided in parallel with the test relays' contacts; the jumpers of course have to be removed when testing the LOP relays.

SYSTEM SOFTWARE

The advantage of having a processor module in each crate of the PS system is that processors with in-built communications interfaces (usually Ethernet) can be used to allow the crates to be located close to the sources of interlock signals while providing readout to any other location(s); and the protocol by which this data is distributed can be tailored to match that of the accelerator's control system. Processor software has been written, and is in use, for the SRS Control System [3], the EPICS-based Diamond control system [4], and the EPICS-based ERLP control system [5]. The ISIS control system is based on a proprietary system [6], and for this a proxy server has been developed to communicate with the PS crates using the SRS Control System protocol, and the ISIS control system using a protocol based on HTML.

CONCLUSIONS

The developments described in this paper have enabled the tried and tested Daresbury PS Interlock system to be applied to two new accelerators in the UK, and also one which is soon to be upgraded, while maintaining a level of hardware compatibility with the existing SRS system, – for which it was originally designed. This has enabled the sharing of experience and expertise between the designers of these interlock systems, resulting in designs being implemented on shorter timescales than might otherwise have been the case, and enabling cross-laboratory support in the future.

REFERENCES

[1] JR Alexander, MT Heron, PD Quinn, "A Report on the Review and Formal Analysis of the SRS Personnel Safety System" PAC 2001, Chicago

[2] DE Poole, T Ring, "The Daresbury Personnel Safety System" PAC 1989, Chicago

[3] BG Martlew, "The SRS Control System: 25 Years of Operation and Development" ICALEPCS 2005, Geneva

[4] MT Heron et al, "Progress on the Diamond Control System" ICALEPCS 2003, Gyeongju

[5] A Oates et al, "Development of the Control System for ERLP" ICALEPCS 2005, Geneva

[6] http://www.vista-control.com/vsystem.htm

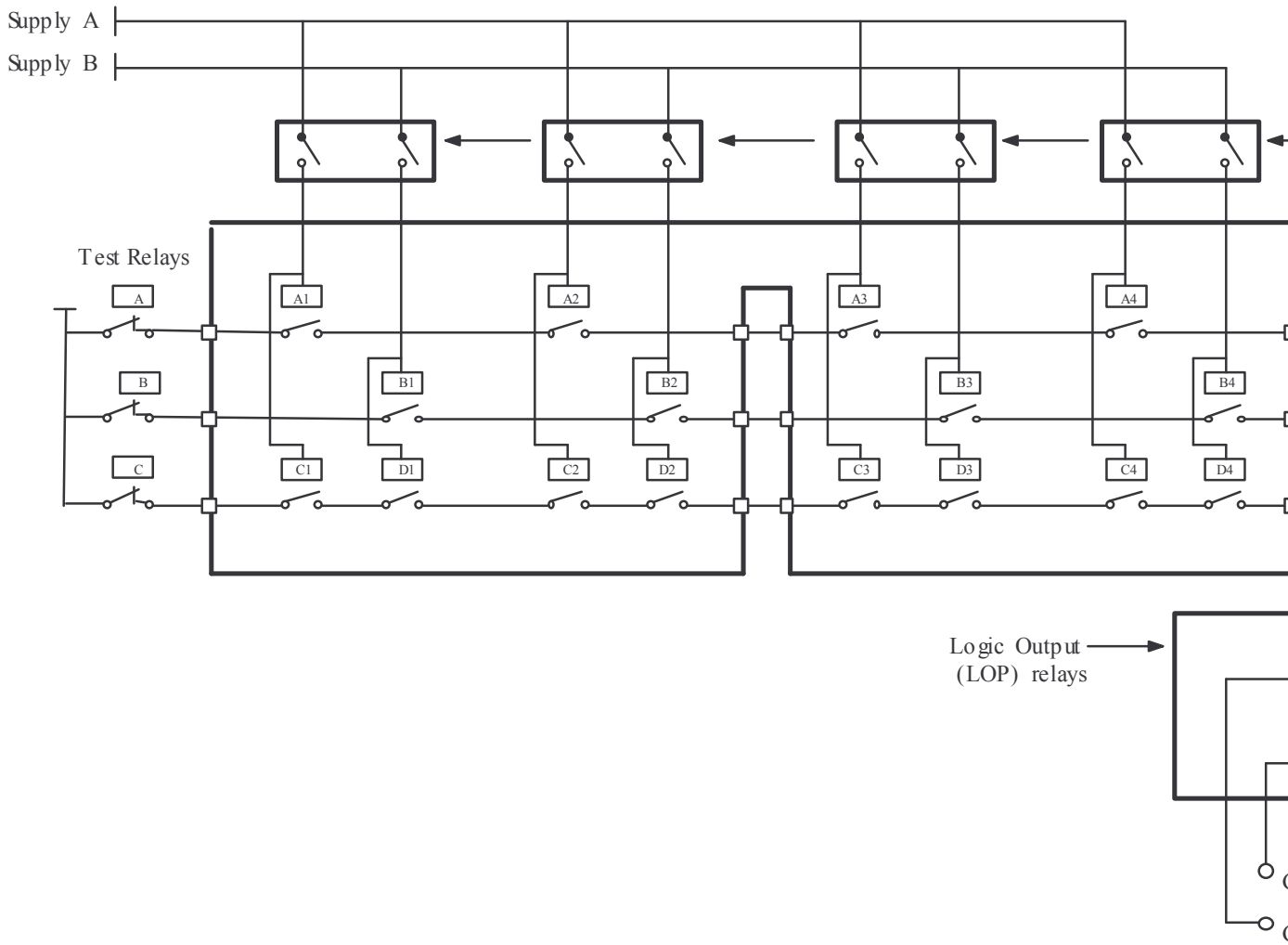

Figure 1: Basic Arrangement of the Interlock Module, Guardlines, and Logic Out