Oxford Gray Institute linac personnel safety interlock system

1. Introduction

All ionising radiation producing sources must incorporate a personnel safety interlock system to restrict entry into potentially dangerous areas and to isolate/turn off the source at appropriate times; the arrangement used with the Oxford Linac is described here.

The linac is situated in a concrete vault in the basement of the Gray Institute Radiation Oncology and Biology Institute. Access to the radiation areas is controlled by two doors: a lead-shielded maze door 2 and maze door 1, which restrict access and must be closed before the accelerator modulator can be energised. There are two additional doors in the Faraday cage which restrict access to the accelerator itself and which must be closed before machine energisation. A cutaway view of the installation is shown in Figure 1.

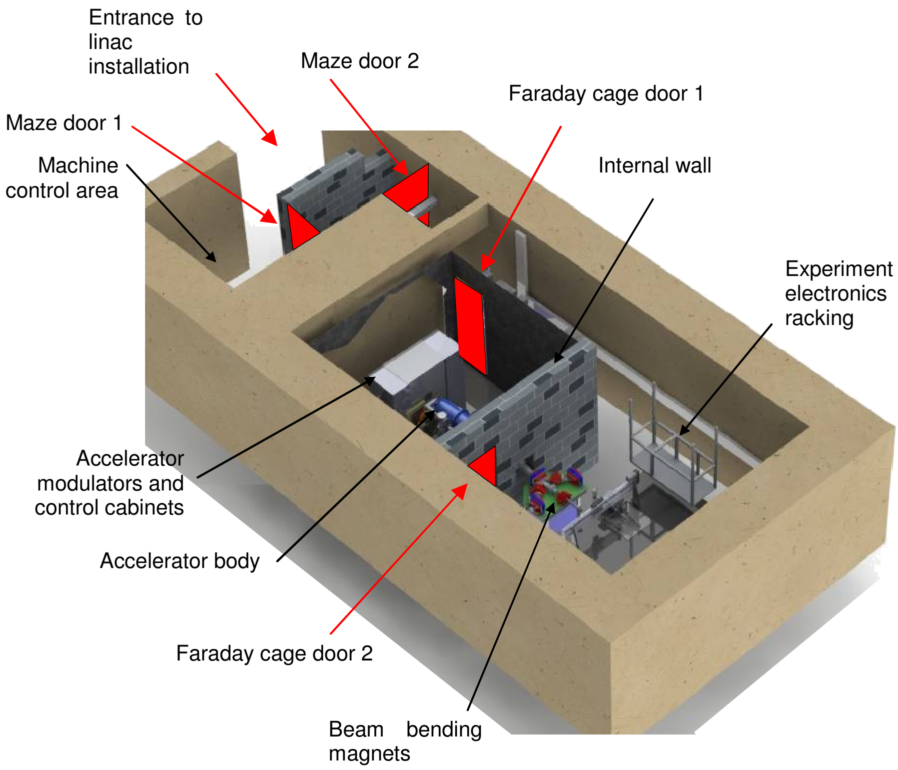

Figure 1: A 'bird's eye' view of the linear accelerator installation.

The reliability of the personnel safety interlock system must of course be near perfect; in the event of a fault, the system should behave in a fail-safe manner. In practice this means that any arrangements based on software or on complex electronics are best avoided and that reliable sensing of door status is essential. We opted for a system based on electromechanical relays arranged in such a way that any potentially 'stuck' contacts prevent operation of the accelerator, combined with a 'cross-linked' energisation system and a 'panic button' circuit which cannot be accidentally reset when activated. Since circuits based on cross-linked relays are not well known, we start the description of the interlock system with an explanation of this simple but reliable arrangement which only allows operation of the accelerator when *two* electromechanical relay contacts are in the same state.

2. Cross-linked relay circuits

Electromechanical relays are often employed in safety applications, as part of a safety interlock system to protect personnel or equipment from dangerous situations. Although relays are in most cases significantly more reliable than either electronic devices or software systems, particularly under transient overload conditions, there are instances when a relay failure cannot be tolerated. An obvious example is where a relay is the final output of some complex safety interlock: should that relay fail, one may as well not have any previous circuitry. A common way to overcome such issues is to duplicate all safety-critical components and use some form of 'AND' logic, e.g. in the final output, place relay contacts in series: both systems have to agree for the final output device to be energized. While this is at first a sensible solution, there is a problem: should one of the subsystems fail in e.g. an energized final output, the user would not be aware of the problem, as the system would still behave apparently properly until such time as the second subsystem fails. In this instance, there is again no protection. The same is true if one adds further subsystems.

A much more satisfactory approach is to use two subsystems which have to ‘agree’ in both energized and de-energised states. In practice this can never be achieved, since there will always be disagreement momentarily, during a change of state. However, this time can be made very short (of the order of several tens of milliseconds) so that in effect, the ‘on’ and the ‘off’ states are constantly monitored. This is achieved using a cross-coupled relay system, as shown in Figure 2. We start by examining what is the system state when both inputs are off (circuit A). In this case, both relays are de-energised and both of their series-connected ‘output’ contacts definitively provide an open circuit in the output. Now imagine that one of the inputs is present, e.g. on RLA energises through RLB/2, as shown on circuit B. From now on, even if the second input becomes active, RLB can never energise since RLA/2 and RLB/1 contacts are both open. This situation is shown in panel C. In contrast, circuit D shows the situation when both inputs were applied simultaneously: both RLA and RLB are now energized. Closer inspection shows that this can only happen if there is enough inertia in the relay mechanics. In addition, once the contacts start to move, they carry on doing so,

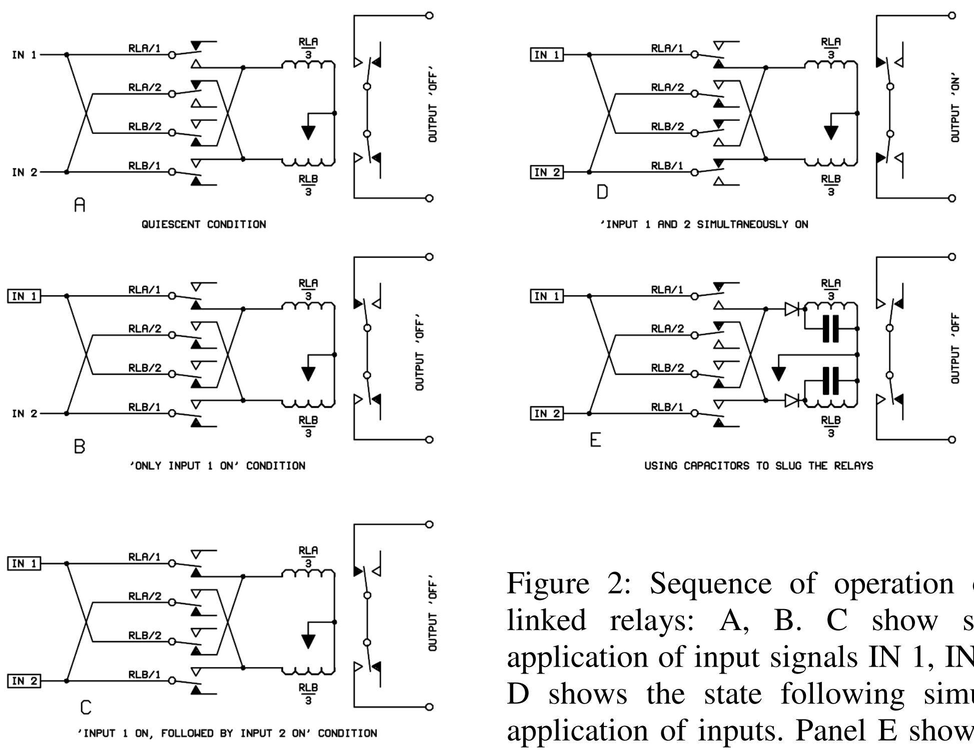

Figure 2: Sequence of operation of cross-linked relays: A, B. C show sequential application of input signals IN 1, IN 2, while D shows the state following simultaneous application of inputs. Panel E shows the use of capacitors to slow down, or ‘slug’, the relays. Delayed-off relays may also be used.

while coil power is momentarily removed before being restored through the ‘opposite’ relay contact. In practice, fast acting relays may not behave in this manner, and some form of delay circuit, such as that shown in circuit E, may be required. This is required because it is very unlikely that the operating times of both relays would be identical: one will always be faster than the other. The capacitors provide enough stored charge, during the momentary loss of coil power, to keep these energized. The diodes are only required if appropriate isolation form the drive circuits is deemed to be required. Reasonable values for the storage capacitors range from ~47 µF to ~220 µF, in a 24Vdc circuit typically used in such applications. This of course depends on coil resistance, i.e.

power, and just as importantly, on the release voltage of the relay coil. In general, lower voltage relays are to be avoided as the capacitor values tend to become impractically large.

3. Accelerator power supplies

The primary accelerator power is derived from the building’s 3-phase supply. This is routed to the Faraday cage, filtered with custom RFI filters. Since some of the subsystems require a permanent power supply (e.g. the accelerator vacuum system, cage lighting etc.) one of the phases is dedicated for this purpose. The other phases are switched by ‘system on’ contactor energised externally by a 24 V ac supply, described later. When this contactor is energised, various internal subsystems are energised but the accelerator is still inherently safe at this stage. The critical power feed is to the main modulator HT supply which is controlled by two independent 3-phase contactors, RLX and RLXX shown in Figure 3. Both these contactors must be energised for the installation to become potentially dangerous.

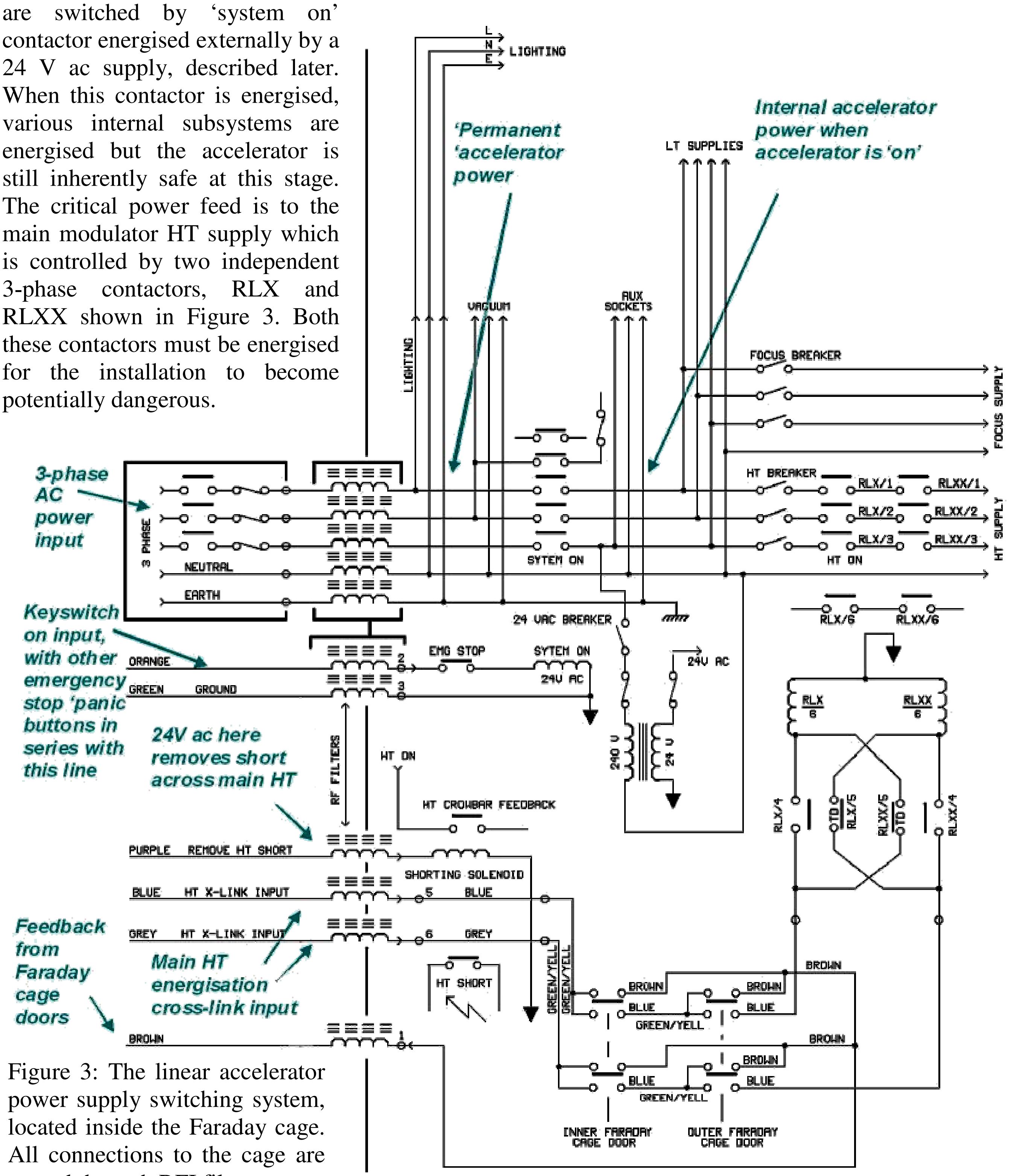

Figure 3: The linear accelerator power supply switching system, located inside the Faraday cage. All connections to the cage are passed through RFI filters.

The energising coils of these contactors are cross-coupled as previously described. The power to these coils is derived from the Faraday cage door switches. If either door is open, the survey of the area, described later, is inhibited. In addition, a high voltage solenoid is present, placed across the output of the modulator HT output. This solenoid removes the short across the HT supply when the maze doors are closed, enabling energising of the HT supply only after the doors are closed.

Should any of the 'panic' buttons be activated, 3-phase power is removed from the 'system on' contactor coil, ensuring that primary 3-phase power to modulator HT supply is removed. In addition the main 3-phase RFI filter, six additional lines are RFI filtered and these are the only hard-wired connections to the Faraday cage. All other connections are made with fibre-optic links. It was considered important to minimise copper connections to the cage to minimise the possibility of accelerator induced interference from being re-radiated outside the cage.

An electron linear accelerator operating at energies <15 MeV is essentially safe when AC power to it is switched off, i.e. there is no activation of materials used in its construction. However, it is noted that not *all* AC power is removed in a 'safe' condition, as it is essential that vacuum pumps, gauges and lighting circuits remain operational at all times.

4. Accelerator cooling

The accelerator is cooled with a pump-driven closed loop circuit. A single phase pump circulates water around the system and into the Faraday cage. Since water is of course electrically conducting, RFI shielded ports are used to prevent excessive RFI outside the cage. The water pump is energised with a contactor with a 24 V ac coil; this can be energised manually, turned off permanently or turned on automatically when the accelerator is energised. Of course when the pump is turned off, water-pressure-activated switches within the accelerator prevent energisation of critical subsystems. The pump control circuit is shown in Figure 5. The 24 Vac is derived from a transformer located in a unit which controls a range of Building Management System (BMS) processes. This 24 V ac supply is also used as the primary power to the safety interlock system, described next.

5. Safety interlock system

This system is constructed in a wall-mounted cabinet adjacent to the BMS unit. It is connected to several additional subsystems and the complete system consists of:

(1) A wall-mounted 'survey' unit within the radiation area housing a time-delayed survey push-button, a siren, an indicator of machine status, and a series of 'panic' buttons which allows complete turn-off of power in the event of an emergency, as described earlier. These panic buttons are fitted with a key release mechanism. The survey unit is placed at the far end of the radiation area in a position where visual inspection of this area is possible and where the buttons cannot be accidentally operated.

(2) Two pairs of switches operated by the entrance doors. A proven design is employed, whereby a door-coupled wedge operates simultaneously two independent changeover switches. These switches are arranged to drive relays in a cross-linked arrangement and will be described later.

(3) The wall-mounted cabinet housing all interlock power supplies, local indicators and relays, as well as a master, key-operated switch and 'standby' and 'energise' push buttons.

(5) The contactor relay sub-assembly within the accelerator Faraday cage, containing the main HT-supply contactors, arranged in a cross-linked fashion, as described earlier.

(6) Several wall-mounted indicator units (red/yellow/green) which indicate system status: one is near to the first entry door, a second one is placed at the far side of the radiation areas and one is placed in the Faraday cage. No provision for monitoring lamp failure in this is provided as the 'lamps' are in fact light emitting diodes which have an essentially infinite operational life. These

indicate to personnel the radiation readiness of the machine. The indicators inside the Faraday cage are driven directly from the accelerator system internal to the cage.

The outer an inner radiation area doors (maze door 1 and maze door 2 in Figure 1) form the primary barriers to the radiation area. Maze door 2 (the inner door) is particularly important as this is a lead-shielded door which must be closed for safe operation of the accelerator. The status of the doors is monitored by an elegant, fail-safe double-switch arrangement developed by Brian Hall at the 'old' Gray Laboratory in Mount Vernon Hospital, Northwood, Middlesex, as part of a personnel safety interlock system used with a Van de Graaff accelerator. Since this had proved to be reliable and operated for >25 years without problem, and since imitation is the sincerest for of flattery (!), we decided to use the same arrangement, shown in Figure 4. A pair of reliable switches is mounted on a plate on the wall adjacent to the door hinge; these switches are operated 'simultaneously' by a triangular plunger between the switches driven by sliding rod, itself attached to a hinged rod which is attached to the door through a second hinge. The position of the hinged rod is adjusted so that the switches energise only when the door is closed (or rather de-energise as soon as the door is opened). Because of the triangular block, it is not possible to easily 'fool' the system and moreover, should the mechanics fail, a 'door open' condition is reported.

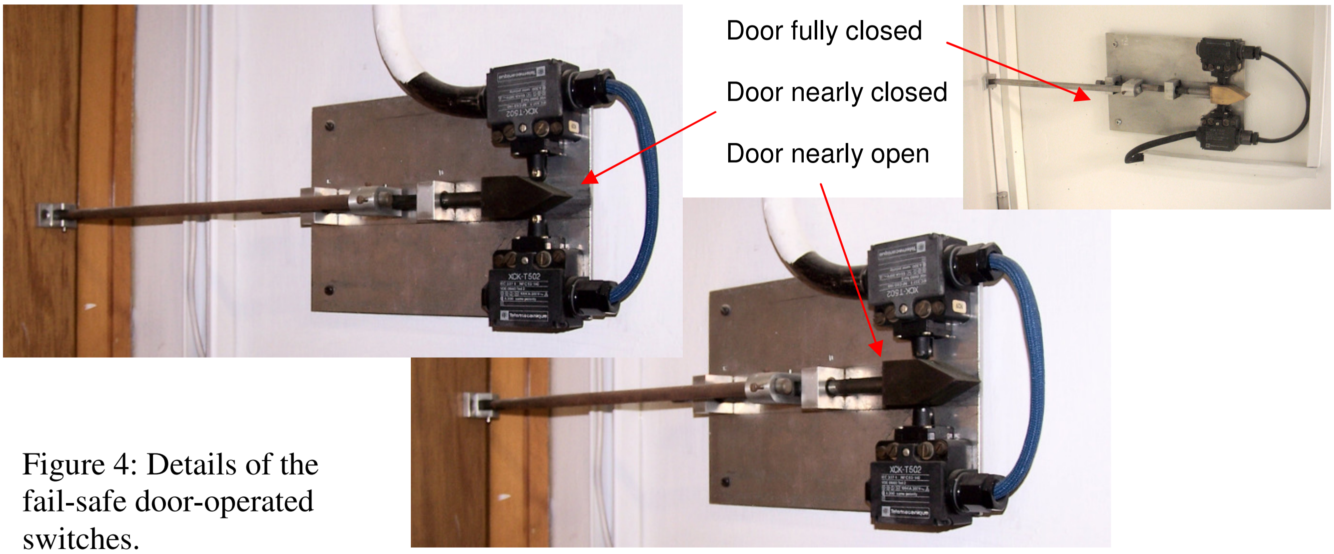

Figure 4: Details of the fail-safe door-operated switches.

The interlock circuit is shown in Figure 5. Its operation is best described by the normal sequence of events in the accelerator turn-on procedure. This consists of turning on the system with a keyswitch, performing a survey of the accelerator area, closing the inner door, closing the outer door and activating the accelerator 'enable' push-button.

(1) Assuming that 24 V ac is present (derived from the BMS system), operation of the keyswitch provides power to energise the 'system on' contactor shown in Figure 3. The key to operate this keyswitch is available only to trained personnel and local procedures ensure that this is so. The keyswitch also provides power to a 24 V ac internal line.

(2) This line provides power to the 'survey' sounder through normally-closed contacts of RLC.

(3) If the outer door is open, relays RLA and RLB are energised and their series-connected contacts provide a 'safe' indication.

(4) If the outer door is open, when the 'survey' button is pressed (a delayed-off action switch) the 'bottom end' of the inner door cross-linked arrangement (consisting of RLF, RLFD, RLG and RLDG) is grounded. RLFD and RLGD are delayed-off relays, while RLF, RLG are slave devices.

(5) This allows the inner door cross-link to energise when that door is closed; this action applies power to the coil of RLC (through contacts RLF/1 and RLF/2).

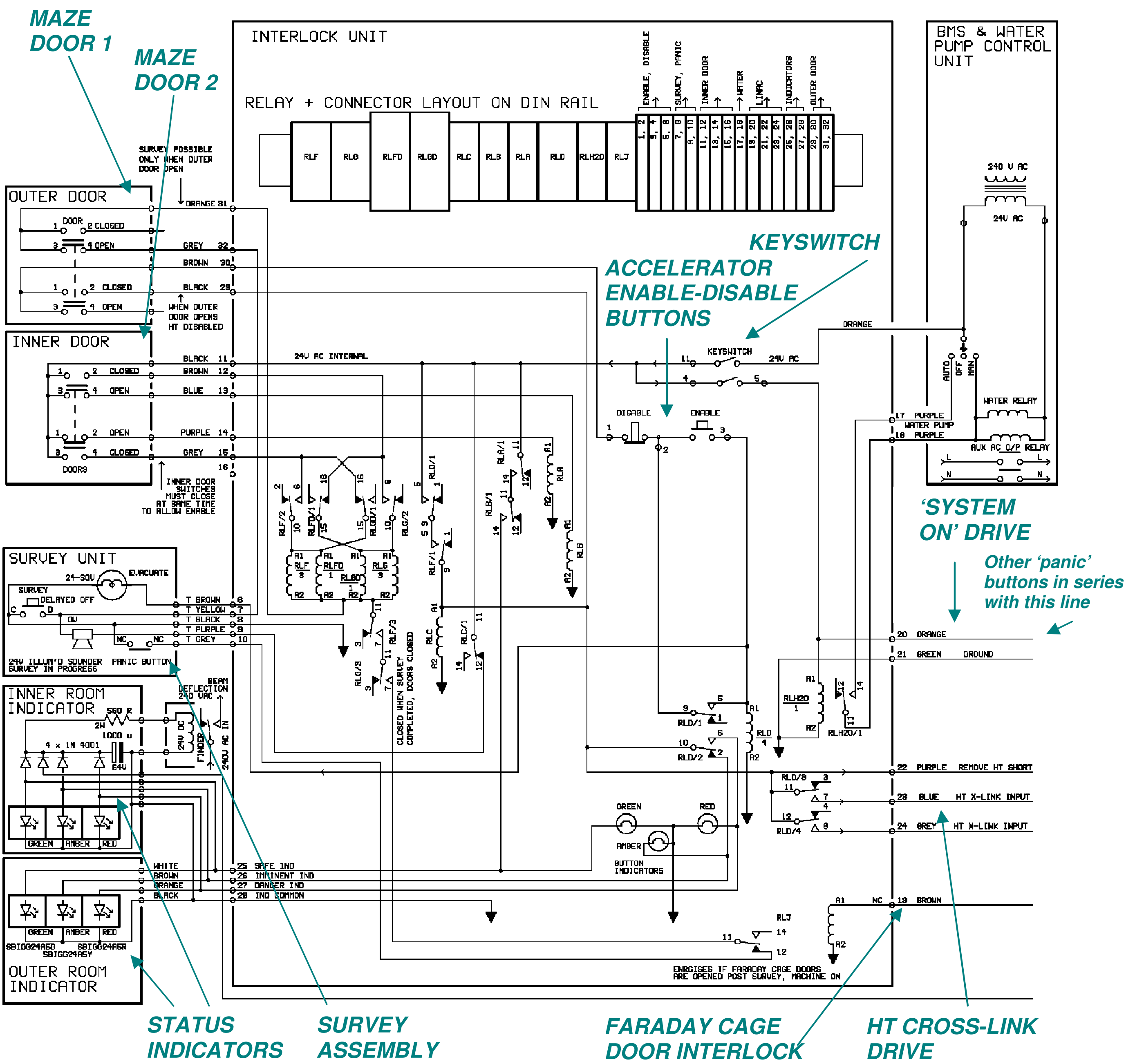

Figure 5: Circuit diagram of the personnel safety interlock system.

(6) As soon as the inner door is closed, relays RLA and RLB de-energise, removing the 'safe' system status indication.

(7) When the 'outer' door is closed, 24 V ac is made available to the junction of the 'enable' and 'disable' push-buttons, through the normally closed contacts of the 'disable' push-button.

(8) By pressing the 'enable' push-button, relay RLD energises and latches itself in the energised state, through contact RLD/1.

(9) Contact RLD/2 changes the status indication form 'amber' (= imminent) to 'red' (= beam on).

(10) Contacts RLD/3 and RLD/4 provide the drive to the HT cross-link circuit shown in Figure 3.

(11) The accelerator is now enabled and ready for pulsing.

Examination of the complete circuit, shown in Figure 6, should satisfy the reader that any stuck contact or switch will immediately result in the removal of power to the output cross-link. In several instances the wiring has been routed in such a way that tampering with the wiring will result in a non-operational system.

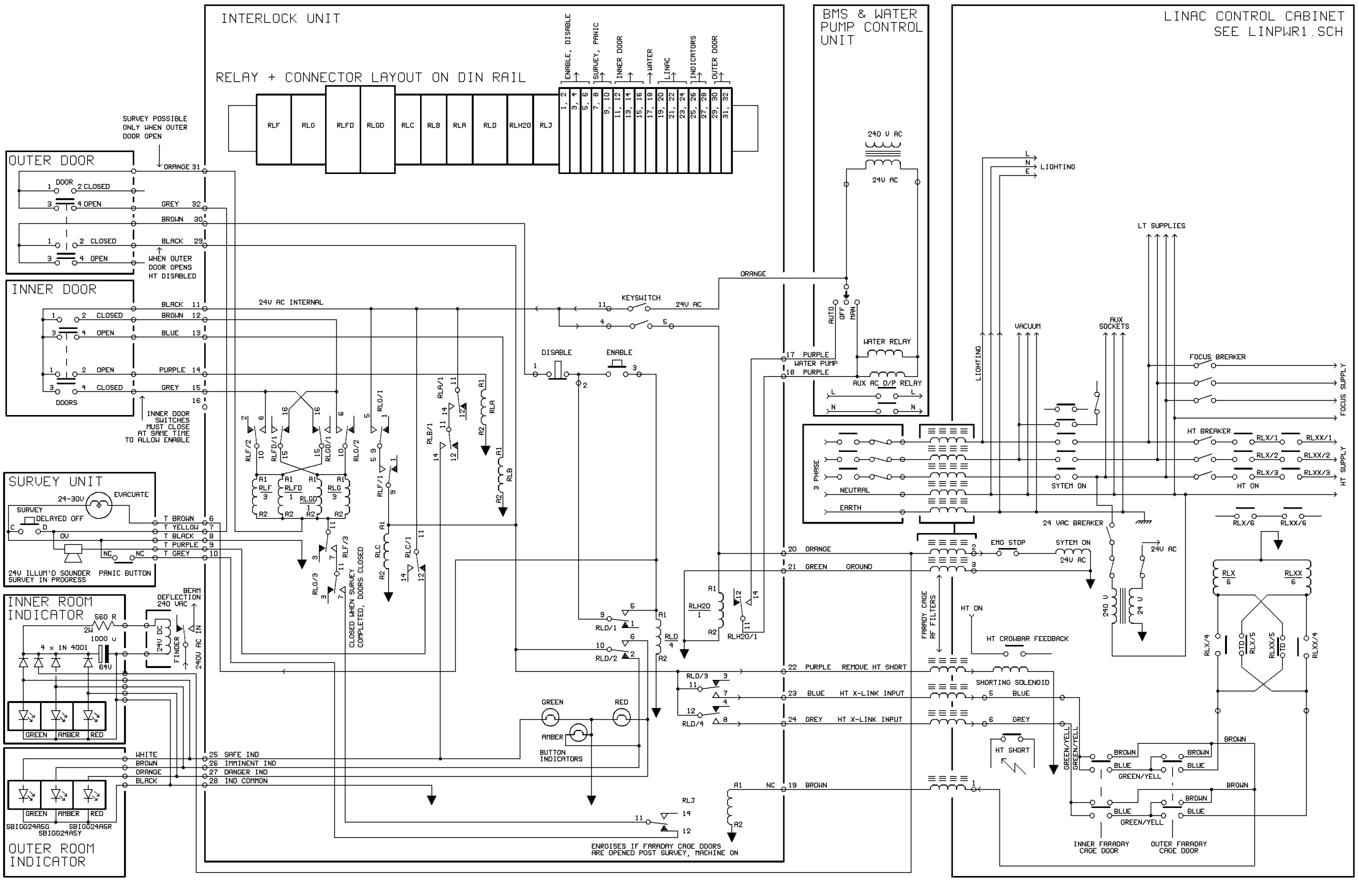

Figure 6: Complete circuit diagram of the interlock and power energisation arrangements.

The room status indicator at the far end of the radiation area (inner room indicator) also contains four rectifier diodes. These were fitted to detect the fact that the accelerator is turned on, since at any time at least one of the diodes is conducting. The resulting DC voltage provided by these diodes is used to drive a relay in the external beam deflection rack so as to 'save' mains AC power to the rack when the accelerator is turned off. This somewhat peculiar arrangement is used because of the routing of the various cable trunking systems in the radiation area.

Figure 7: The room survey unit (left), the inner (SAFE – IMMINENT - RADIATION) and outer (SAFE – IMMINENT – NO ENTRY) status indicators (middle), one of the status indicators used in the Faraday cage (middle right) and of the 'panic' buttons (right).

Figure 7 shows the various satellite components associated with the interlock system, while the wall-mounted unit external and internal views can be seen in Figure 8.

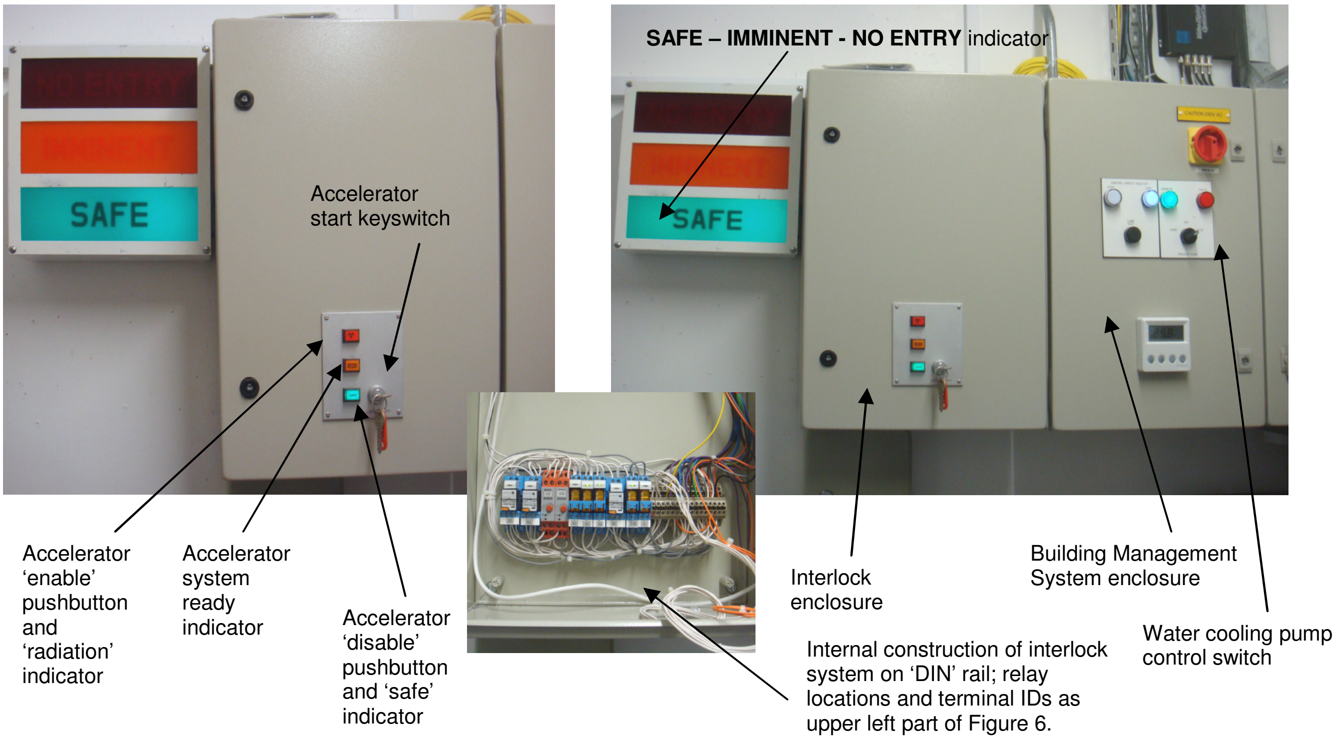

Figure 8: Practical implementation of the personnel safety interlock system.

6. Conclusion

We have implemented a simple and reliable fail-safe personnel safety interlock system. The use of simple electromechanical relays in combination with cross-linked relay systems is cost-effective and guaranteed not to give us sleepless nights! The system allows a straightforward procedure for energising the accelerator:

Turn on accelerator keyswitch (which is normally kept in a locked key cabinet)
Survey the room
Close all doors
Push the 'enable' push-button and start irradiations, as controlled by the accelerator software
When entry is required, push the 'disable' button and enter the radiation area. Of course any irradiation can also be terminated at any time by opening the outer door.

This document was prepared by S. Gilchrist and B. Vojnovic during January and February 2012. The system was designed by B. Vojnovic in collaboration with R.G. Newman, a system which so far has proved completely reliable, since we are able to write about it several years after it was installed! The assistance of R.G. Newman was of course invaluable since he 'pulled' most of the wires associated with this interlock system and performed almost all of its construction. We also acknowledge J. Prentice's extensive assistance with drilling walls (high density concrete can be pretty tough stuff!) and producing metalwork required by the system.

We acknowledge the financial support of Cancer Research UK and the Medical Research Council.