A REPORT ON THE REVIEW AND FORMAL ANALYSIS OF THE SRS PERSONNEL SAFETY SYSTEM

J. R. Alexander, M. T. Heron, P. D. Quinn, CLRC Daresbury Laboratory, UK

Abstract

CLRC Daresbury Laboratory operates the SRS light source, which consists of a Linac, Booster Synchrotron, Storage Ring and 41 experimental stations. Protection of personnel from radiation and the hazards associated with the accelerators and photon beamlines is ensured through a dedicated Personnel Safety (PS) system. The design of the PS interlock hardware was produced over 20 years ago, and has been implemented using two generations of technology. The PS system has recently been reviewed due to changes in legislation and in preparation for future accelerator projects. This review included a formal analysis of part of the system using the technique of Fault Tree Analysis to examine likely failure modes and system integrity. The analysis takes into account both hardware and human factors. This paper briefly presents the SRS PS system and discusses the outcome of the recent review and analysis.

1 INTRODUCTION

The interlocks necessary to protect personnel from radiation hazards associated with the accelerators and photon beamlines of Daresbury Laboratory's Synchrotron Radiation Source (SRS) are implemented using the Daresbury-designed 'Personnel Safety (PS) system'[1]. This was developed in-house for the SRS some 20 years ago; and provides a modular, hardwired, dual guard-line, configurable logic safety system. Up to 22 hardware modules, each containing the relays to service four interlock inputs, plug into a crate where the required logic is defined by wire-wrap connections. Eight crates are used in the accelerator interlock systems, and 16 in those for the beamlines. Remote monitoring of the status of all system inputs and outputs is provided via a backplane bus in each crate (the CAMAC bus in the early version of the system, the G64 bus in the later). The dual guardline outputs from the system are used as 'permits to operate' those items of plant which control whether radiation can be generated in, or transported to, the various shielded enclosures of the SRS. It is usual to disable two independent items of plant to protect each enclosure.

The conditions which must be ensured before radiation can be allowed into an enclosure are generally that all personnel have been excluded, all entrances are closed, all shielding elements are in place, and the external radiation monitors indicate a safe level. Personnel are cleared from an enclosure by a search procedure, monitored by the PS system, which entails the pressing of search-point buttons in a pre-arranged sequence. During the search warnings are sounded, and on its completion warning signs are illuminated within the enclosure giving the instruction to press one of the Emergency Off buttons. A 'two-man' search is implemented in the accelerator enclosures, which requires that pairs of search-points, for example situated on opposite sides of the storage-ring tunnel, are pressed simultaneously; these searches may only be carried out by members of the SRS operations team. The experimental 'hutches' (steel or lead-lined rooms where the x-ray beams are brought into air to irradiate experimental samples) are smaller, and only require a one-man search; these are searched by users, who are often visiting scientists from universities or other research institutes.

A review of both the PS system hardware and the operating procedures, such as searches, has recently been undertaken. This was prompted by the introduction in the UK of revised statutory regulations for work with ionising radiation[2], and as a precursor to defining a system for use on the UK's proposed new synchrotron light source, DIAMOND. The review has involved internal studies; discussions with the UK's Health and Safety Executive; and the letting of a contract to study the reliability of x-ray hutch operations using the method of Fault Tree Analysis[3] to establish a quantitative failure rate, taking into account both hardware and human-behaviour failure mechanisms. The results of the review, the consequent changes being implemented, and the results of the Fault Tree Analysis are further discussed.

2 RESULTS OF THE REVIEW

All elements of the review, including quantitative data from the Fault Tree Analysis, have indicated that human factors dominate the probability of failing to an unsafe state. The hardware of the PS system has been shown to be highly dependable, – a conclusion which agrees with experience gained during the annual testing of the PS hardware which is necessary to re-establish the full integrity of a dual guard-line system. The review has mostly focussed on hutch operations, as these are searched and used by a large number of external users, some of whom may not be aware of the severity of the x-ray hazards. Changes to the PS system and operating procedures which have been, or are in the process of being, implemented are as follows:

2.1 Access Control

A proprietary access control system is being installed as a result of two conclusions of the PS review. The first is that the hutches must be designated as 'controlled' radiation areas due to the need "to follow special procedures designed to restrict significant exposure to ionising radiation in that area" (i.e. the search). A concomitant result of this designation is the requirement to measure, or estimate, the radiation doses of people

0-7803-7191-7/01/$10.00

working there. It was deemed impracticable to install individual access control on the 33 hutches, so the entire SRS complex will become a controlled area, with ingress and egress controlled and recorded by a 'badge reader' system. This will also satisfy a growing concern about the security of the experimental area, to which there is currently free access. The second conclusion is that the training of users to search hutches, and indeed to understand the danger posed by the x-ray beams, must be enforced and recorded. A part of the system to achieve this is the installation of a badge reader at each hutch to initiate the search, instead of a simple button. Each user's badge will be validated for a particular hutch, for the duration of his or her allocated beam-time, and only following appropriate training. All of this information will be recorded in a central database, allowing a user's badge to be re-enabled for a return visit if his or her training is up to date.

2.2 Review of hutch search-point positions

The positioning of the search-points in each hutch has been comprehensively reviewed, with a particular emphasis on ensuring that an unconscious person could not be missed by the searcher. Also considered was whether covers should be fitted on more of the search-points, or search-points re-orientated, to ensure that they cannot be operated remotely with a stick or other implement. Where covers are fitted, the PS system ensures that the search cannot be completed if the button is jammed down.

2.3 Hutch Radiation Monitors

Radiation monitors will be installed in each hutch. These will give a siren warning if the radiation signals are above a pre-set level and the hutch is open, or a background 'all clear' audible signal when levels are normal. When the hutch is searched and interlocked the siren will be disabled.

2.4 Personnel detectors

A re-evaluation was made of the use of detectors to indicate the presence of a person in a searched hutch. This is not an easy task, as it is necessary to detect an unconscious (and therefore immobile) person, or a person deliberately trying to defeat the interlock, – all in the presence of warm and moving detector equipment. In addition, one of the advantages of a hutch system is the ability to easily modify the type and position of equipment within, and this would be severely restricted by a system designed to detect a pre-defined floor occupancy. Instead, it was felt that the correct approach is to properly train users in the search procedure and the radiation danger in the hutch. Indeed, a searcher might be tempted to be less thorough if it was known that the presence of a person would be detected by other means.

2.5 Failsafe Warning signs

The warning signs within hutches and accelerator enclosures are being made failsafe, i.e. the signs must be illuminated to complete the PS interlocks for the enclosure. This is a specific requirement of the Approved Code of Practise[4] for the Ionising Radiation Regulations 1999. A light sensor in each hutch sign will provide an interlock into the PS system. As this is an electronic detector (and not a simple switch) the PS system will test the operation of the sensors at each search: unless all sensors show that the signs are off, a search cannot be initiated.

The accelerator enclosures are much larger and contain more signs, with more than one usually visible from any position, thus a simple current sensor will be used to ensure that at least 90% of the signs are illuminated. In addition, the currently unreliable filament bulbs in these signs are being replaced by panels of high intensity LEDs, to reduce the probability of the accelerator being stopped due to failed bulbs.

2.6 Backup for beamport shutters

A typical beamport on the SRS feeds light to several hutches or experimental stations. Each station has its own radiation shutter, and if this should ever be open without the associated PS interlocks being made, the beamport's shutter is closed by the PS system. A similar back-up to the beamport shutters is now being introduced, which will dump the electron beam in the storage ring upon failure of a port shutter. This is only likely to happen if both the port shutter and a station shutter fail, since injection into the storage ring is already conditional upon all beamport shutters being closed. The Fault Tree Analysis has shown this to be low on the list of probabilities; but a possible common failure mode for the two shutters has been identified: water in the compressed air supply to the shutter operating cylinders can cause them to jam.

3 FAULT TREE ANALYSIS

A contract was placed with a firm of safety consultants to quantify the level of safety provided by the hutch search and interlock procedure, using the technique of Fault Tree Analysis. The first step in this process is to agree a 'top event', i.e. the failure to be quantified, which for this review was defined as "Failure to ensure that no personnel are in hutch 9.4 when x-rays are present". (The hutch chosen is among the largest on site, and contains a substantial amount of experimental equipment.) The technique involves defining all the possible subevents which could independently cause the top event (in this case "Person present in hutch when x-ray beam is activated" and "Person enters hutch when x-ray beam is present"), then defining the subevents which could cause these, and so on. Eventually 'base events' are encountered which can be quantified without further sub-division; examples are 'bulb fails', 'relay contact fails closed' or 'person ignores warning sign'. Hardware failure rates can be derived from recorded failure data, or from libraries of data on similar devices. The derivation

of human failure rates is a specialisation which involves analysis of the tasks involved, and comparison of these to other tasks which have estimated or measured failure probabilities.

It is usual to draw the Event Tree using a proprietary software package, which then does Boolean reduction on the resultant event logic to derive 'minimal cut sets' (MCSs). A minimal cut set is a set of base events which together can cause the top event. The probability of each MCS is the product of the probabilities of the base events within it; while the probability of the top event is the sum of the MCS probabilities. In this case the probability of the top event was found to be $2{\cdot}6\text{x}10^{-8}$ per hutch search. Besides indicating a fairly good level of system safety, arguably the most useful finding is the relative contribution of the various MCSs to this figure. The complexity of the PS system (dual guardline, multiple shutters, etc) leads to a very large number of MCSs. The top 50 of these were analysed, and can be grouped into the following categories, for each of which the percentage contribution to the top event is given:

- The searcher presses the buttons in sequence but makes no attempt to search, AND someone was in the hutch, AND that person does not respond to either the audible search warning or the visual warnings following the search (– either deliberately, or due to being unconscious). 77%
- As above, but the person in the hutch does not respond because the warnings are not operational. 22.5%
- A person releases the hutch interlocks and enters, and both radiation shutters remain open. This also requires that the hutch door's electric lock fails to be engaged. 0.5%

These results clearly underline the need to ensure that users are properly trained in the hutch search procedure. They indicate the gain in safety which can be made by making the warnings failsafe, which should reduce the probability of the second category to the same order of magnitude as the third. They show that the next most likely cause of failure is the simultaneous failure of both shutters to close; this will be mitigated by the implementation of a beam dump on failure of the port shutter.

4 REFERENCES

[1] DE Poole, T Ring "The Daresbury Personnel Safety System" PAC '89

[2] "The [UK] Ionising Radiation Regulations 1999", Statutory Instrument 1999/3232

[3] "Reliability of systems, equipment and components. Part 7: guide to Fault Tree Analysis" British Standard BS 5760-7:1991, ≡ IEC 61025:1990

[4] "Work with ionising radiation, IRR 1999, Approved Code of Practise and Guidance" Health & Safety Executive. ISBN 0 7176 1746 7