ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA101

# REVIEW OF PERSONNEL SAFETY SYSTEMS AT DLS

M. C. Wilson, Diamond Light Source Ltd, Oxfordshire, UK

*Abstract*

Diamond Light Source is celebrating 10 years of "users" at its facility in Oxfordshire, England. Its safety systems have been designed to the standard EN61508 [1], with the facility constructed in 3 phases, which are just concluding. The final "phase 3" beamline Personnel Safety System (PSS) has been signed-off; hence it is timely to review our experience of the journey with these systems.

## INTRODUCTION

The Diamond Light Source Ltd (DLS) is a scientific research facility providing intense beams of light to expose samples in order to discover detail of structure or surface. The "light" is a broad spectrum of electromagnetic radiation from visible through to X-ray but predominantly used in the X-ray band. The light is generated by bending a beam of 3GeV electrons in a synchrotron. There are significant hazards to personnel from the light itself and from the consequences of accelerating electrons to high energy. It is necessary to provide a robust protection system to ensure that the hazards are managed effectively.

## HISTORY

The Diamond accelerator was conceived by a team of engineers and scientists at Daresbury Laboratory. Many of the initial concepts were already established when DLS was set up in 2002, to build and operate the research facility in Oxfordshire, England.

As the accelerator is capable of generating ionising radiation, DLS must comply with IRR99 [2], the statutory instrument concerning the production of ionising radiation in the UK. Provision is made in the regulations for facilities to operate accelerators under the "Prior Authorisation for the use of Accelerators" providing that the facility follows the "The Approved Code of Practice" [3] (ACOP).

The original concepts for the PSS were that it should be designed to EN61508 and use the Daresbury logic solver.

Hence Diamond Personnel Safety System has been built with the following constraints:

- It conforms to IRR99.
- It conforms to the ACOP.
- It complies with EN61508.
- It uses the Daresbury Logic solver.

The Daresbury logic solver [4] is a dual guardline relay system that is configured using "wire-wrap" to produce AND and OR logic functions. The operation of the logic solver can be monitored on the control system via a VME interface and Ethernet connection.

The project was split into 3 phases:

1. 3 accelerators (14 zones) and 7 beamlines.
2. 14 beamlines.
3. 10 beamlines.

Each system has been designed, built, tested and become operational in turn, with the first beamlines now celebrating 10 years of users in 2017.

## LESSONS LEARNED

The DLS PSS [5] has benefitted from the experience and support of staff at Daresbury Laboratory and other accelerators. Visiting other facilities enabled us to develop an understanding of "best practice" and establish policies of our own. This has enabled DLS to develop with confidence and without major incident.

In retrospect, there are always choices made and things done that we may have done differently with the benefit of hindsight. There have also been ideas that work better than anticipated or had unexpected benefits.

The following sections contain some of our "lessons learned"

### *Proof Testing and Diagnostic Coverage*

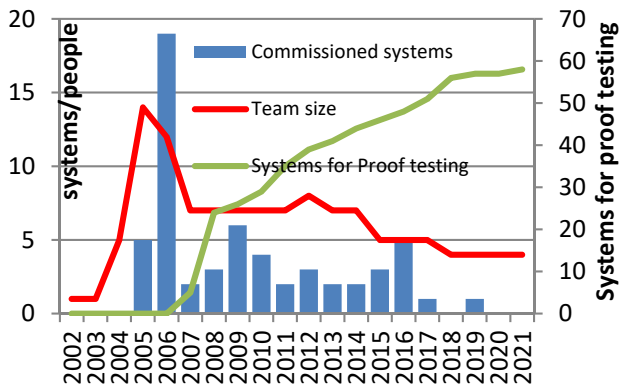


Figure 1: Development of DLS PSS.

Figure 1 above shows the development of DLS PSS over time. As new systems are built there follows a cumulative growth in proof testing requirements. We undertake proof tests on a 2 yearly programme which requires an average of 5 or 6 systems per shutdown. Even at this interval, this is a heavy burden and would require a larger team if the proof test period was any less. Consideration should be given to the level of diagnostic coverage in new systems to keep proof testing at a manageable level for a given team size and access periods for testing.

### *Architecture*

DLS PSS functions with a "2 out of 2" (2oo2) architecture, or dual guardline system. This offers complete redundancy from a safety point of view but a single failure may force the facility "off" until it can be resolved. This

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA101



places pressure on the safety system to be supported whenever the facility is operational. As a result the PSS team provides 24 hour, 7 day days a week repair cover during operational periods. It may have been prudent to adopt a more forgiving architecture, such as 2oo3, where the safety system is able to ignore a single fault.

### *Building a Big System*

DLS PSS is a big system which has been developed in stages. We have treated it as a lot of small, and mainly independent, systems which are combined to make a large system. This is achieved by dividing systems at "pinch points" where the fewest interlocks and permits between systems are required. This has allowed us to bring on systems independently, as required, when each system is ready. We have added the ability to "disconnect" a system (beamline) individually by a system of keys. This disables beamline operation but leaves the rest of the system safe and available for operation. This has proven to be a powerful feature which allows beamlines to be reconfigured without requiring extended facility downtime.

### *Setting Targets*

A probabilistic approach to safety management requires a target. DLS has set a general safety target for the facility of a probability of death of an individual of $1x10^{-5}$ per annum. This is a target which is agreed and understood by Directors and the Chief Executive Officer (CEO) at DLS.

The target probability is shared equally between 5 hazard groups, giving radiation related hazards a target of $2x10^{-6}$ per annum, shared between approximately 100 enclosures.

Taking the DLS facility risk target, with 500 employees and an expectation that the facility will be operational for 30 years, there is a 15% chance of a death at the facility at some time due to a work related hazard. This is an important process as it causes consideration of risk in human terms, which helps to establish a strong safety culture.

### *Documentation*

DLS has over 2000 Personnel Safety documents. Some of these are general project documentation such as minutes of meetings, design briefs and PSS policy but a large proportion relates to EN61508 implementation.

It had been determined that DLS would conform to EN61508 in the preliminary design study for the facility. Consultants were engaged to help set up a process and safety management plans were developed.

The safety management plan was split into 2 areas, one for the accelerators and the other for beamlines. In practice this was unnecessary and the 2 plans are nearly identical. It would have been better to have spent more time at this stage to have developed a common safety management plan and reduced the documentation.

Similarly the plan is followed for each of the beamlines, generating sets of documents which look very similar in which lots of EN61508 explanation is duplicated.

Many of the test procedures are common to all systems, as the systems are made up of common modules. The use of common test procedures saves a lot of duplication.

In many cases, the specific system detail is added to generic documents forming longer system specific documents. With a little more planning it would have been possible to use generic documents and add shorter system specific documents.

Change control is an important element of EN61508. DLS has a rigorous change control system which requires appropriate levels of authorisation for changes. Change request are assessed to 1 of 4 levels from trivial to a change to the functional safety, requiring engineer through to Directorial approval.

DLS has also developed a non-conformance system where a concession is allowed for a finite period before being amended. This often applies to systems under development where, for example, some equipment may not be available but operations can safely proceed meanwhile. Non-Conformance Reports are time-bound and are reviewed at monthly progress meetings.

### *Hazard Identification*

EN61508 is a quality standard relating to the design of safety related systems. It is concerned with the process of generating safety systems. However the safety system can only protect against hazards that have been identified. As a consequence hazard identification is potentially the most important and fundamental part of the process.

At DLS our initial hazard identification sessions were concerned with identifying PSS managed hazards. There were primarily radiation hazards but also included hazards that required "access control" as a primary defence, such as machines and robots. Our initial concept was that we could treat all beamlines under a generic model. It soon became apparent that:

- Each system was sufficiently different that a generic model wasn't adequate.
- We should include all hazards.

Having identified "all hazards" they can be subsequently allocated to be managed by the PSS or by other means.

DLS uses a Hazard Identification (HazID) process with a panel of "experts" with a broad range of skills and experience. It is the job of the chairman to promote discussion and encourage "stupid" questions. Most new members of the panel are reluctant at first but typically by the end of the session they can see benefit and recognise the process has generated additional thought.

There is a danger that, when evaluating similar systems, the analysis overlooks subtle difference between systems. This may allow an assumption to be made that the risks are the same. However it is important to explore the consequences of the differences, as this may give rise to the requirement for additional safety functions.

### *Frequency of Opportunity and Consequence*

A common outcome from assessment of the risks on systems is that the worst case frequency is combined with

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA101

the worst case consequence. This is seldom realistic and this is corrected in modelling the system, using more sophisticated models and frequency modifiers. In less formal modelling it may be necessary to consider the cases separately with analysis for each consequence and the appropriate frequency of opportunity.

### *Searching*

Searching enclosures is an integral part of the DLS PSS. Areas that are to be subjected to radiation must be searched by trained personnel prior to enabling beam. This ensures that no-one is left in the enclosure however analysis shows this to be the "weak link" in the PSS. DLS uses a card reader as a recognition tool for the searcher. Only trained searchers have their identity card enabled and therefore we are able to restrict searching to trained personnel. The card reader is a "stand alone" system with each card reader accepting new cards when preceded by a "trainer card" authorisation. Cards automatically expire after a predefined period of inactivity. The system has been effective and requires little management however in retrospect networking the readers from the outset would have provided easier management and the ability to record and preserve card numbers enabled on each card reader.

To ensure that searching can be undertaken efficiently, recognising the reduction of abilities of tired operatives, the following policies are followed:

- Search paths are designed to cause the searcher to walk through all areas that personnel can access.
- The search route is enforced by the sequential operation of search buttons.
- Inaccessible areas are viewed, with the searcher encouraged to view the area by the placement of the search confirmation button.
- "Chase arounds" are avoided by the use of fences and gates
- The final search button is external to the area and must be operated after the area is secured.
- Good housekeeping is encouraged, to avoid clutter and preserve access and visibility.

### *Key Exchange Systems*

DLS PSS must comply with IRR99 and its ACOP. The ACOP encourages the use of key exchange systems so DLS uses them widely. The keys are primarily used to disable systems and are routinely used in conjunction with a Permit-To-Work (PTW) process, often raised when other systems need to prevent operation for safety reasons. DLS also uses them to provide access to "user labyrinths", removable shielding and some areas of fencing. This gives the operator the ability to undertake tasks which would otherwise need to be controlled under an administrative process. This is particularly beneficial where access may be required frequently or out-of-hours. The keys are large and heavy and often operate in mechanical mechanisms which have a reassuring robust feel. Due to their size it is unlikely that anyone will walk away with the keys. The keys are often used in exchange applications where the key is removed from one barrel to be operated in a different location.

### *Failsafe Indicators*

To comply with the ACOP, visual displays should be "fail-safe". At DLS we have interpreted this as meaning that if a sign is not showing its warning message properly then the associated hazardous operation is inhibited. To prevent this from becoming restrictive, all DLS active indicators operate using Light Emitting Diode (LED) systems with redundant circuits. A warning is provided if one of the redundant circuits fails. If both circuits fail the permit to operate the equipment is removed. The LED function is checked by measuring the current that flows through the LED. The current must fall between the minimum and maximum required for normal operation, to detect open or short circuit failures.

Each indicator has redundant power supplies, capable of operating the complete indicator. Similarly each power supply is monitored.

The design has proven to be successful however there are some shortcomings:
The control should be "active OFF" in that if there is no signal from the PSS the light should come ON. Indicators in radiation environment have suffered radiation damage in some locations. The radiation damage to power supplies has reduced the current capacity of the power supplies with time. In some cases the power supplies have become unable to supply sufficient current to operate the indicators in the event of a failure of its partner. The serial operation of the indicators means that a single "A" channel failure with a single "B" channel failure on a different indicator appear as if a single indicator has completely failed. The LED indicator modules consist of many LED in series. An open circuit causes all LED on that module to go off which is interpreted as multiple failures.
LED now show signs of aging – after 10 years there is evidence of heat damage close to the semiconductor junctions, which now appear golden.

We have undertaken a programme of replacing all power supplies in the indicator units and are considering if a routine replacement of LED modules is due.

### *Shutters and Press Safety Valves*

DLS PSS implements redundant and diverse systems where possible. We have implemented a system which exhibits these qualities but in an unconventional way with our shutter system. Shutters can be large and expensive devices so duplicating their function is not an attractive option. Where exposure is controlled by shutters, we have 2 shutters between the source of radiation and personnel however only one shutter is required to be closed. We operate a "cascade" system. If a shutter fails to operate then an upstream shutter will be forced to close. If a shutter is not closed when it is required to be closed, e.g. when a door is opened, then the beam in the accelerator is dropped. This is the quickest way to prevent exposure, as shutters take about 2 s in transit. Shutters are design and operated with additional safety considerations:

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA101



- Shutters use positive pneumatic pressure to close, as well as open.
- Shutters will close under gravity in the absence of pneumatic pressure.
- Shutter closure is assisted by vacuum.
- Beamline and Accelerator-side shutters are operated from separate pneumatic air supplies.
- Each shutter has its own isolated air reservoir.

Each shutter has a pneumatic circuit that has a robust operating scheme. Actuation is controlled via a Press Safety Valve (PSV). This is a safety rated 5 port valve, operated by 2 separate coils and incorporating cross coupling pilots. Both pneumatic circuits must operate together or the PSV with close the shutter. Each pneumatic circuit has a pressure switch so that if the pressure is falling then the shutter will be closed before the air is depleted. The pneumatic circuit also featured a pneumatic low pressure change over so that the shutter would be closed without any external intervention. This circuit has since proven to be problematic with some components suffering radiation damage and has been removed.

### *Door Pulling*

Beamlines with shielded enclosures have heavy lead lined doors. The doors are fitted with 2 electric locks via independent mounting brackets. Each lock provides status signals of the door being closed and locked. There is also a coded magnetic switch mounted on the inside of the door which provides an indication of the door being closed. This arrangement provides protection against the door being forced open and the lock arrangements breaking away from the door or the door frame. On early beamlines the magnetic switch was set to be sensitive to force being applied to the door. When force is applied the locks will tension and the door will flex, providing some movement at the magnetic switch. However because the doors are heavy, personnel become used to having to pull the door quite hard to open it. This lead to a spate of beam trips caused by personnel pulling on a locked door. It became necessary to tighten the magnetic switches so that "obvious" force is required to cause the beam to be dumped.

### *Logic Tests*

The DLS PSS uses relay logic in a hardware logic solver. The logic is defined by wire wrap connections made on the backplane of the logic solver. The logic is defined by a circuit diagram, produced on a proprietary Computer Aided Design (CAD) package which is then used to produce a "net list" of connections. A post-processor produces a test pattern by which the logic solver is tested on an automatic test rig. Whilst connected to the test rig it is possible to verify the control system screens, providing confirmation of the operation of the system with the minimum of risk of human error. This has proven to be most effective.

### *Portable Radiation Monitors*

During the initial risk assessments of beamlines it was identified that ionising radiation posed a significant risk to personnel, caused by exposure to an invisible hazard. Personnel are dependent the PSS to protect them. The reliance on shutters to provide absolute protection when appearing to be closed has been identified as a concern. "Burning through a shutter" could cause the PSS to appear safe when it was not. Whilst the probability of burning through a shutter is small and there may be warning signs available to the control system, it was thought prudent to offer an additional independent protection. DLS requires all beamline operators to carry a hand held radiation monitor with them when they first enter a hutch. Carrying a radiation meter is an independent safety measure and allows the operator to be confident that they are not being exposed to radiation at their specific location. Unfortunately this is a safety measure that is dependent of the actions of the operator. The operator is unlikely to ever measure anything above background and there is a temptation for them to conclude that it is pointless exercise. Some meters are difficult to switch on and off or become discharged, contributing to a reluctance to bother with carrying a hand held meter. A resent meeting of the Technical Design Review committee concluded that this was a necessary function and its use is required. Consideration should be given to measures to encourage adherence to "best practice" and methods of reinforcing the use of radiation monitors should be investigated.

## SUMMARY

DLS has built a successful PSS based on "best practice" established at other facilities.

Some lessons that can be learned from DLS PSS are:

1. Identify safety targets early, get sign-up from the organisation's senior management and nurture a safety culture.
2. Visit other facilities and learn from their experience. Follow examples of "best practice".
3. Spend good time optimising your safety management in order to optimise the level of documentation you will need to produce.
4. Identify an architecture that supports the operational requirements of the facility, not just the safety requirements.
5. Keep systems independent so that they can be added and removed with the minimum of interference between systems.
6. Concentrate on thorough hazard identification at the onset.
7. Implement good diagnostics coverage to minimise the risk of unidentified faults and the requirement to proof test.
8. Use supporting risk reduction techniques to reduce the reliance on safety systems and help minimise Safety Integrity Level (SIL) requirements.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THPHA101

9. Recognise the importance of and vulnerability to "searching".
10. Beware of the operational consequences of introducing failsafe elements.
11. Analyse designs for adequate safety margins and avoid adding unnecessary safety measures that impact on uptime.
12. Invent automatic processes to avoid human error.
13. Use keys as physical permits to avoid reliance on administrative controls.

## REFERENCES

[1] *EN61508 Functional Safety of electrical/electron/programmable electron safety related systems*, BSI Standards, 389 Chiswick High Road, London, UK. ISBN 978 0 580 56233 4.

[2] *The Ionising Radiations Regulations 1999*, The Stationary Office Ltd. ISBN 0 11 085614 7.

[3] *IRR99 - Approved Code of Practice and Guidance*, HSE Books. ISBN 0 7176 1746 7.

[4] J. R.Alexander, *et al.,* "Upgrading the Daresbury Personnel Safety Interlock System"*, in Proc. ICALEPCS2005*, Geneva, Switzerland, October 2005.

[5] M. C. Wilson, *et al.*, "Diamond Personnel Safety System", in *Proc. ICALEPCS2003*, Gyeongju, Korea, October 2003.