# DEVELOPMENT OF THE DIAMOND LIGHT SOURCE PSS IN CONFORMANCE WITH EN 61508

M.C. Wilson, A.G. Price, Diamond Light Source, Oxfordshire, UK.

*Abstract*

Diamond Light Source is constructing a third phase (Phase III) of photon beamlines and experiment stations. Experience gained in the design, realization and operation of the Personnel Safety Systems (PSS) on the first two phases of beamlines is being used to improve the design process for this development. Information on the safety functionality of Phase I and Phase II photon beamlines is maintained in a hazard database. From this, reports are used to assist in the design, verification and validation of the new PSSs. The data is used to make comparisons between beamlines, to validate safety functions and to record documentation for each beamline. This forms part of a documentation process demonstrating conformance to EN 61508 [1].

## INTRODUCTION

The Diamond Light Source is a 3rd generation synchrotron, a particle accelerator that accelerates electrons close to the speed of light and uses insertion devices to cause the electron beam to produce intense beams of X-rays. It is used for research by the science community and industry. Inherent in the process is the risk of harm to personnel from ionising radiation, i.e. X-rays generated by design and neutrons and gamma radiation generated by collisions of high energy electrons with hard surfaces. As a result Diamond is subject to the UK's Ionising Radiation Regulations, IRR99 [2] and must provide an engineered safety system to manage the hazards. Diamond elected to adopt the safety system standard EN 61508 to guide the process. It is a generic international standard for the design of electrical / electronic and programmable electronic safety systems, which is applicable to environments without specific safety standards of their own, such as accelerators. Diamond has now been producing Personnel Safety Systems (PSS) to protect personnel from ionising radiation and other hazards since the project began in 2002. Protection against "Other hazards" may include crush hazards caused by robots, eye damage from lasers and any additional hazards which require a rigorous access control system.

The Diamond PSS includes:

- a Linac zone,
- 3 booster zones,
- 10 storage ring zones,
- 7 phase 1 beamlines
- 14 phase 2 beamlines

Phase 3 will consist of a further 10 beamlines.

Each system is an independent safety system which contributes to the overall safety system for the facility. This type of architecture allows for the addition of new systems and the removal of old without undue reconfiguration of the overall system. However, this amounts to a lot of safety systems to manage. As part of the safety management under EN 61508, a database of hazards was established. This has proven to be of little direct benefit, and so it was decided to extend its function to help manage the EN 61508 process. This paper describes the database and its role in the Diamond Personnel Safety System.

## EN 61508 IMPLEMENTATION

Diamond identified the desire to apply EN 61508 to the PSS early in the realisation of the project. An external contractor was employed to set up the process and, due to pressures of the programme, the first iterations of the design and conformance processes were established at the same time. Diamond safety management requires formal identification of hazards in a HAZard IDentification process (HAZID). The technique, in common with many others, identifies the hazards that fall within a specific area and for each hazard the initiating event that might lead to an incident, the consequences, the likelihood of the incident and the safeguards that will protect against it.

The information collected in the HAZID is used to generate a safety requirements specification and as a basis of a safety model.

The safety requirements specification lists and describes the safety measures required and allocates them to subsystems, where appropriate, using Safety Integrity Levels (SIL), derived from the safety model. SIL indicate the rigour required from the safety system with 1 the least and 4 the most rigorous requirement. The system is built and tested so that each safety requirement is tested against a functional performance test. The remaining EN 61508 implementation concerns the quality of the process, involving verification and validation and cross-checks to ensure what was built meets the SIL requirement and is as designed, that the design is as specified and that the specification mitigates the hazards.

## DATABASE OBJECTIVES

Diamond has an EN 61508 process which augments a traditional manufacturing process used to design, build and test the PSS. The EN 61508 process provides the means of managing the design and manufacture; however the manufacturing process is typical of manufacturing processes used elsewhere without the requirement for EN 61508. Hence, there was a possibility that the two processes could operate largely independently and on different timescales, undermining the safety design process. A means of consolidation was therefore sought, such that the manufacturing process should be able to

Copyright © 2011 by the respective authors — cc Creative Commons Attribution 3.0 (CC BY 3.0)

receive timely information from the EN 61508 process in a readily useable form. The EN 61508 should be able to accept data from the design process and provide cross checks to ensure that the design is complete. The EN 61508 process should be able to provide calculations which support the design prior to the detailed analysis being undertaken.

There are three main elements that make these requirements appropriate to a database:

- the large number of similar and comparable systems at Diamond,
- the quantisation of qualitative information,
- the ability to structure reports based on a common data set in many different arrangements for cross referencing and validation of the various stages of EN 61508

Having a large number of systems allows the comparison of data between systems. This is a valuable benefit, as the start point of the process requires human expertise and judgement, which is fallible. Cross referencing between systems helps to identify omissions and irregularities by requiring justification of the differences.

Entering information into a database provides the opportunity to put similar interpretations and numbers to qualitative assessments. This is the first stage of processing data to provide probabilistic assessment of risk.

Producing reports that contain the pertinent information in an appropriate order is a great help to verification and validation. Information from different points in the process can be brought together to generate new information and data, including calculations.

## DATABASE STRUCTURE

The database is built using Microsoft Access 2007 from the Microsoft Office suite. It consists of tables of hazards, safeguards, frequencies of opportunity and outcome severities. These are linked to interlocks and control measures by a logic table. Preliminary assessments can be undertaken and reports generated to support the EN 61508 process. Documentation is also included by linking the database into the SharePoint document repository. The following sections identify the processes and reports generated for the various stages.

## HAZARD IDENTIFICATION

The Diamond Safety Management plan requires hazard identification to be undertaken early in the project. As soon as the preliminary beamline layout has been established, it is reviewed for hazards, and the potential frequency and severity of incidents is assessed. Safeguards to prevent the incident are identified. The results are recorded in the "Preliminary Hazard Analysis" report. The records of the review are collated and recorded in the database. In entering the information, steps are taken to convert the qualitative results into quantitative values:

- Frequency of opportunity is commonly expressed as an interval during discussion and is converted into an explicit number of events per annum.
- Severity is allocated by table to provide a risk of fatality per event as a percentage. This provides common allocation of severity for similar hazards on different systems.
- The effectiveness of the safeguard is assessed and probability is assigned to the control measure.

The first output from the database is a report for checking the database records against the Preliminary Hazard Analysis report. The report is formatted to present the data in the same arrangement as the HAZID table for ease of comparison

### *"Sore Thumb" Checks*

The benefit derived from implementing a system to structure the design of a safety system can only be as good as the identification and analysis of the hazards presented. At Diamond we have the benefit of having built many safety systems and have records of the hazards identified on those systems. The database is used to generate two reports that compare hazards, frequency, severity and safeguards, in different formats, allowing the comparison and rationalisation of differences between hazards on different beamlines. The first format arranges the initiating event with consequence and frequency of opportunity grouped by beamline and beamline area. This allows comparison of hazards identified in similar areas on different beamlines. The second format arranges the data by cause, which generates a report that allows comparison of the treatment of a particular hazard on different beamlines.

### *Hazard and Safeguard Cross Reference*

Once the appropriate and correct data is in the database a cross-reference report is generated and appended to the Preliminary Hazard Analysis report.

## PRELIMINARY NUMERICAL ANALYSIS

Undertaking some preliminary analysis is a useful exercise, as iterations "around the EN 61508 loop" are quite time consuming.

### *Risk of Fatality Report*

Given that most safeguards contribute to additional safety, a very basic preliminary calculation can be undertaken that combines the safeguard contributions as a logical AND function of all the individual safeguards that contribute to the mitigation of the risk. It should be noted that accuracy of this calculation is limited by the simplicity of the model, which ignores the independence and common-mode failures of the safeguards, and does not replace the need for a more thorough analysis. However it does provide a useful early warning that more

Copyright © 2011 by the respective authors — cc Creative Commons Attribution 3.0 (CC BY 3.0)

safety measures may be required to provide adequate mitigation for a particular hazard.

### *SIL Rating Report*

Most of Diamond's safety systems have similar safety requirements and similar solutions; this allows the use of common analysis between safety systems. It is not unreasonable to assume that an equivalent system on similar safety systems will have the same SIL requirements and that the equivalent solution will achieve a similar SIL. The database also holds references to the evaluation of the solution.

The SIL report provides a list of SIL evaluations, SIL ratings and the Probability of Failure on Demand (PFD) for the function. This allows the development of safety models using consistent values.

## SAFETY REQUIREMENTS SPECIFICATION

The safety requirements specification contains definitions of the safety functions that the system will implement. It is derived from the safeguards and control measures defined in the database. The first report in this section lists the safety requirements for inclusion in the specification. It includes legal requirements and Diamond safety policy functional requirements, which may not be direct "safety" requirements placed upon the safety system. It should be noted that the report lists an occurrence of a particular safety function for each hazard that it mitigates. The safety function is incorporated only once in the design as it is effective for all of the hazards it mitigates, but the complete list of references is an important record in case of future changes of requirements.

The list of safety functions produced from the database is a significant element in the composition of the safety requirement specification, which is the document that specifies in detail the function of the personnel safety system and its components.

## SAFEGUARD COMPARISON REPORT

Again, as we have a history of safety systems design at Diamond, it is prudent to compare the current system with previous similar systems. A report listing the safeguards for particular hazards allows comparison and justification of differences between beamlines and assumptions made at the time of hazard identification.

## NON-PSS SAFETY REQUIREMENTS REPORT

Some of the safety functions required to achieve adequate safety fall outside the scope of Electrical / Electronic / Programmable Electronic (E/E/PE) systems and are managed by others. This report lists all Non-PSS safety requirements. Its use provides an effective mechanism for communicating and discharging responsibilities.

## LOGIC DESIGN

Safety functions translate into interlocks and control measures, or "permits". Often, the same control measures are required for several interlocks, and so logic functions are required to combine interlocks and provide permits to equipment. Generally the control measure is asserted only if the logical AND combination of the interlocks is present. By processing the beamline data in the database to produce a report of interlocks by control measure, a comprehensive design-checking tool becomes available. The database provides a method of recording the logic design so that each safety function is implemented and is recorded.

## VERIFICATION AND VALIDATION

The database allows the safety functions to be listed for the each system. A report can be generated which lists each safety function, its interlock and its permit. This is a valuable tool for checking that all safety functional requirements are tested in the functional test procedure. Further, the reference for the functional test for each safety function can be recorded to provide a cross-check that all safety functions have been included and are tested.

## DOCUMENTATION

The documents associated with a beamline are referenced from the database into the document repository. This allows generic documents and system-specific documents to be used for each safety system and the documents to be recalled simply and efficiently.

## CONCLUSIONS

The ability of the database to produce reports sorted and filtered on different criteria allows the production of reports tailored for specific stages of the EN 61508 process. Presenting similar data in different formats enhances the ability to check and compare data. Cross referencing and filtering on specific criteria provides valuable information for assisting audits. The database is a useful tool for checking validity, assisting design and verifying the safety system, but should not be employed blindly.

## FUTURE DEVELOPMENT

The database contributes to the processes involved with the development of safety systems, during which assumptions are made about the frequency of operation and reliability of components in the system. The database could be developed to accommodate data collected from operational experience allowing the assumptions to be validated. In practice, frequency-of-operation information is relatively simple to collect; however there are often other considerations to be taken into account and some sort of normalisation may be required before the number becomes useful. Reliability of components is a study that is likely to be too complex for a database of this type, and

Copyright © 2011 by the respective authors — cc Creative Commons Attribution 3.0 (CC BY 3.0)

is probably better studied elsewhere. Consolidation of failure data into subsystem failure and safety requirement failure would be of interest. Safety requirement failure rates could be added to the database for validation of SIL ratings. Subsystem failure data could be collected elsewhere for comparison with Failure Modes, Effects and Consequence Analysis (FMECA) and subsequent studies.

## REFERENCES

[1] EN 61508, "Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-related Systems"
[2] IRR99, "The Ionising Radiation Regulations, 1999"

Copyright © 2011 by the respective authors — cc Creative Commons Attribution 3.0 (CC BY 3.0)