ICALEPCS 2017 THPHA101

THPHA101 - Review of Personnel Safety Systems at Diamond.

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, with the facility constructed in 3 phases, which are just concluding. The final "phase 3" beamline Personnel Safety System has been signed-off; hence it is timely to review our experience of the journey with these systems.

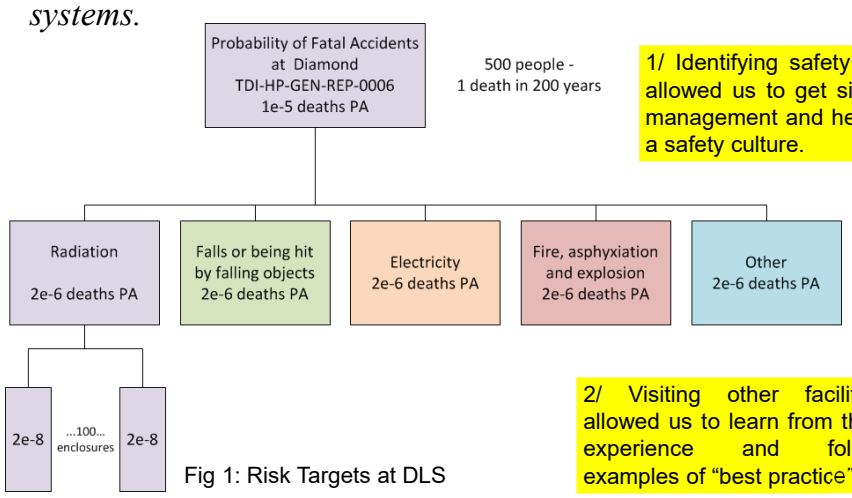


Fig 1: Risk Targets at DLS

1/ Identifying safety targets early has allowed us to get sign-up from senior management and helped us to nurture a safety culture.

2/ Visiting other facilities allowed us to learn from their experience and follow examples of "best practice"

Fig 2 Best Practice

3/ DLS is a large facility with many safety systems – This has lead to a lot of similar documentation. We could have identified a better documentation structure to minimise duplication

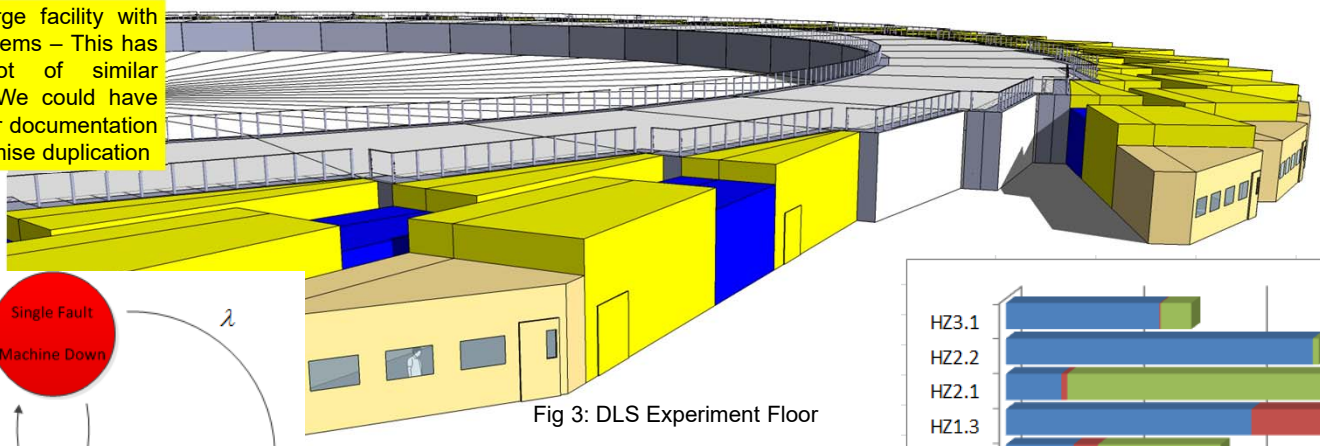
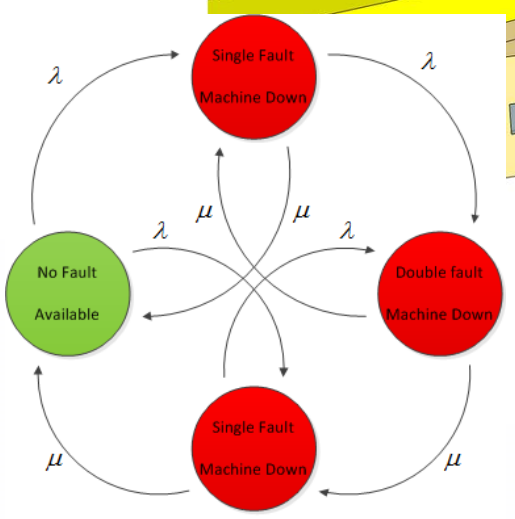


Fig 3: DLS Experiment Floor

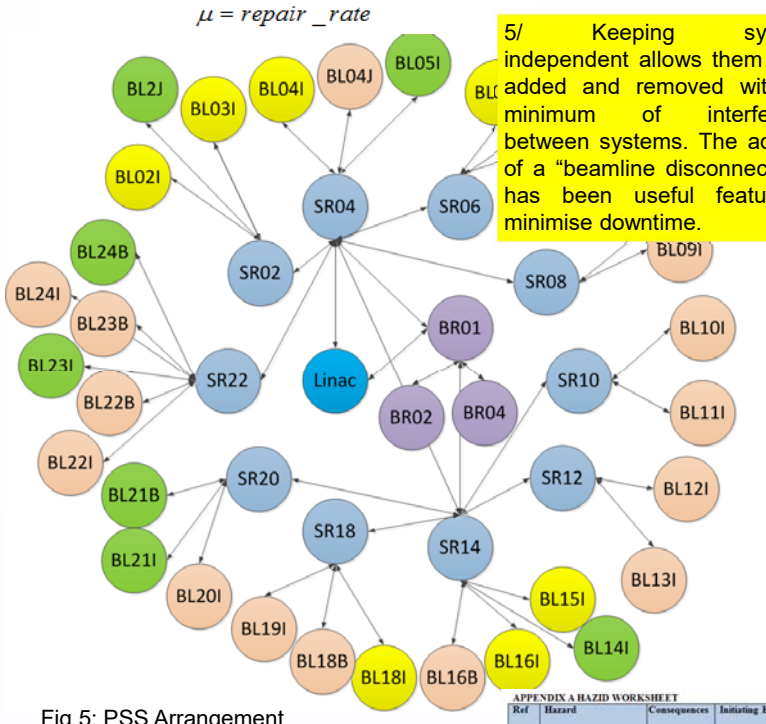


4/ A "2oo2" architecture improves safety but decreases availability. We could have identified an architecture that better supports the operational requirements, as well as the safety requirements, of the facility.

Fig 4: Markov model of a 2oo2 System

$\lambda = failure\_probability$

$\mu = repair\_rate$



5/ Keeping systems independent allows them to be added and removed with the minimum of interference between systems. The addition of a "beamline disconnect key" has been useful feature to minimise downtime.

Fig 5: PSS Arrangement

APPENDIX A HAZID WORKSHEET

Ref	Hazard	Consequences	Initiating Event	Frequency of Opportunity	Non-PSS Safeguards	PSS Safety Functions
Hazards from OH1						
1.1	Exposure to synchrotron radiation in the White Beam hutch OH1	Probable fatality	Trained person enters White Beam Hutch while beam on	1 per week	(i) Use of portable monitor when entering hutch (ii) Training (iii) Card access (iv) Safety operating procedures	(i) Annunciator outside door (ii) Safety shutter closed if door unlocked (iii) Door switches prevent beam entry (iv) Door locked if unsafe to enter (v) Shutter cascade
1.2	Exposure to synchrotron radiation in the White Beam hutch OH1	Probable fatality	Untrained person enters White Beam Hutch while beam on	1 per week	(i) Supervision (ii) Card Access	(i) Safety Shutter closed if door unlocked. (ii) Door switches prevent beam entry. (iii) Doors locked by PSS. (iv) Shutter cascade
1.3	Exposure to synchrotron radiation in the White Beam hutch OH1	Probable fatality	Beam initiated while trained person in White Beam Hutch	1 per week	(i) Safety operating procedures (ii) (iv) (v) MPS Vacuum Interlock prevents beam	(i) Door locked by PSS (ii) Open door inhibits start-up (iii) Unlocked door inhibits start up. (iv) Coloured light system inside (iv) Warning tones (vi) Beam Off buttons (vii) Annunciator inside
1.4	Exposure to synchrotron radiation in the White Beam hutch OH1	Probable fatality	Beam initiated while untrained person in White Beam Hutch	1 per week	(i) Supervision (ii) (iii) (iv) (v) MPS Vacuum Interlock prevents beam	(i) Door locked by PSS (ii) Open door inhibits start-up (iii) Unlocked door inhibits start up

Fig 6: HazID Table

6/ Concentrate on thorough hazard identification at the outset. When considering similar hazards focus on the differences.

7/ Good diagnostic coverage minimises the risk of unidentified faults and the requirement to proof test. We have a 2 year proof test cycle

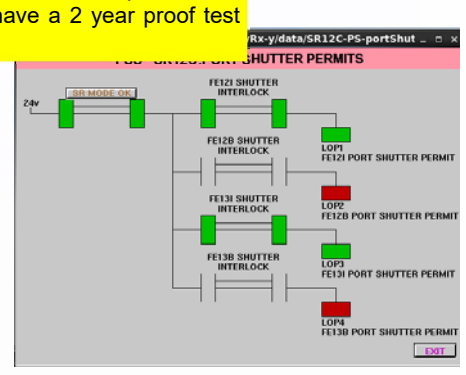


Fig 7: Diagnostic screen

8/ We have used supporting risk reduction techniques to reduce the reliance on safety systems and help minimise Safety Integrity Level (SIL) requirements

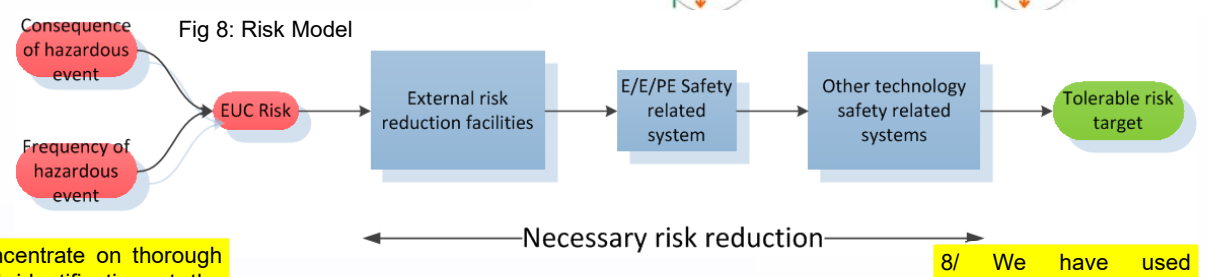
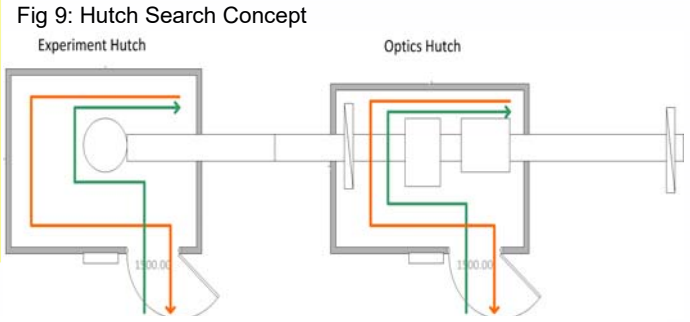


Fig 8: Risk Model

9/ We have recognised the importance of and vulnerability to "searching"

- *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.*
- *Storage in search areas is discouraged*

Fig 9: Hutch Search Concept



10/ Failsafe elements require careful design to avoid a negative impact on operations

Fig 10: Failsafe Indicator

11/ Analyse designs for adequate safety margins and avoid adding unnecessary safety measures that impact on uptime.

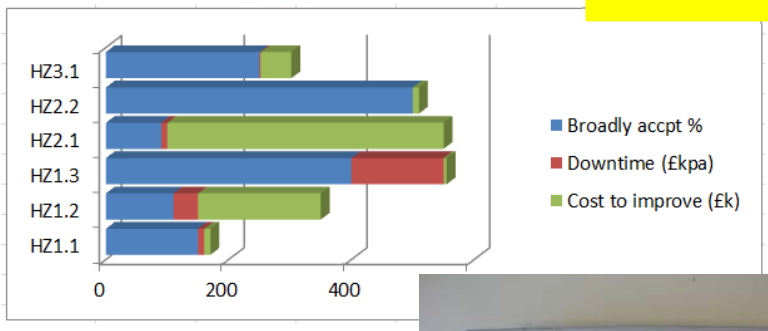


Fig 11: Analysis of adequacy of Risk reduction

Fig 12 Automation

12/ Invent automatic processes to avoid human error

Fig 13: Typical Key for a Captive Key system

13/ We have found that the use of keys as physical permits helps to avoid reliance on administrative controls in "frequent use" applications

For more information please visit www.diamond.ac.uk or contact Martin Wilson at martin.wilson@diamond.ac.uk

Martin Wilson, Diamond Light Source, Harwell Science and Innovation Campus, Didcot, Oxon OX11 0DE

ICALEPCS 2017 THPHA101