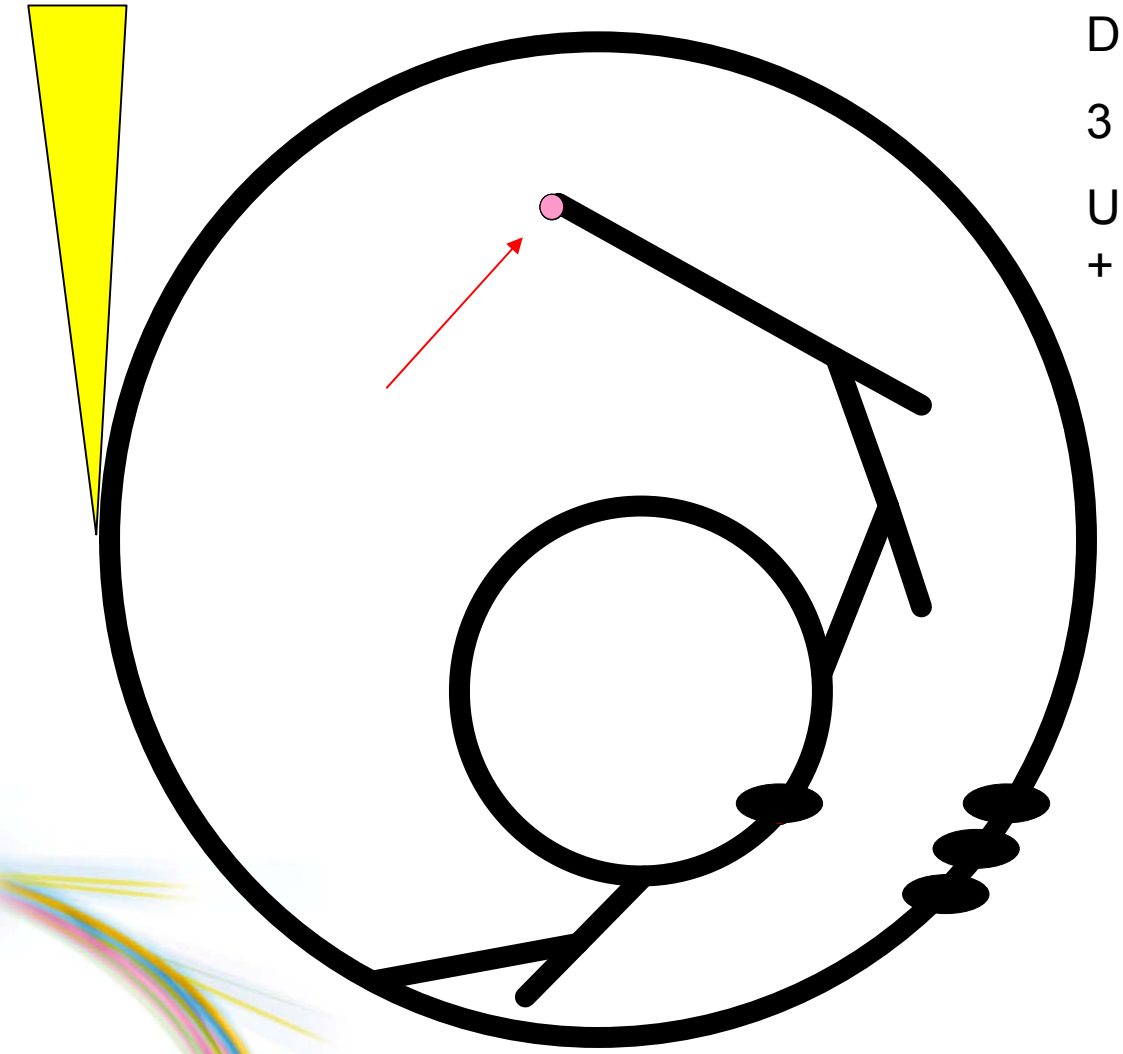
Development Of The Diamond Light Source PSS In Conformance With EN 61508

- Presented by Martin Wilson
- Principal Personnel Safety Engineer
- Diamond Light Source

What is this talk about?

- What is Diamond Light Source?
- Personnel Safety System organisation
- The need for a database
- Quantization
- Calculations
- Report generation

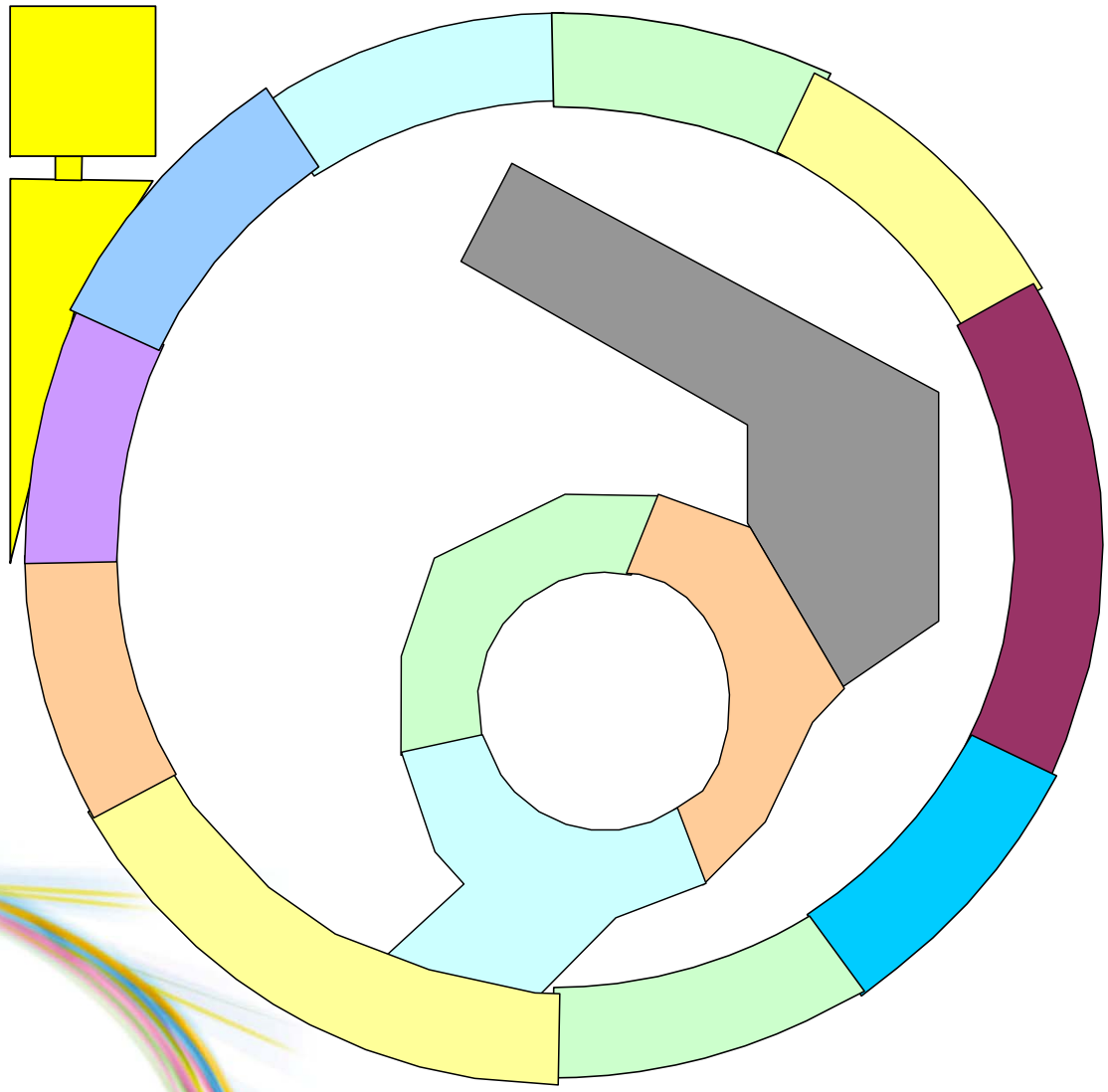


DLS

3 accelerators

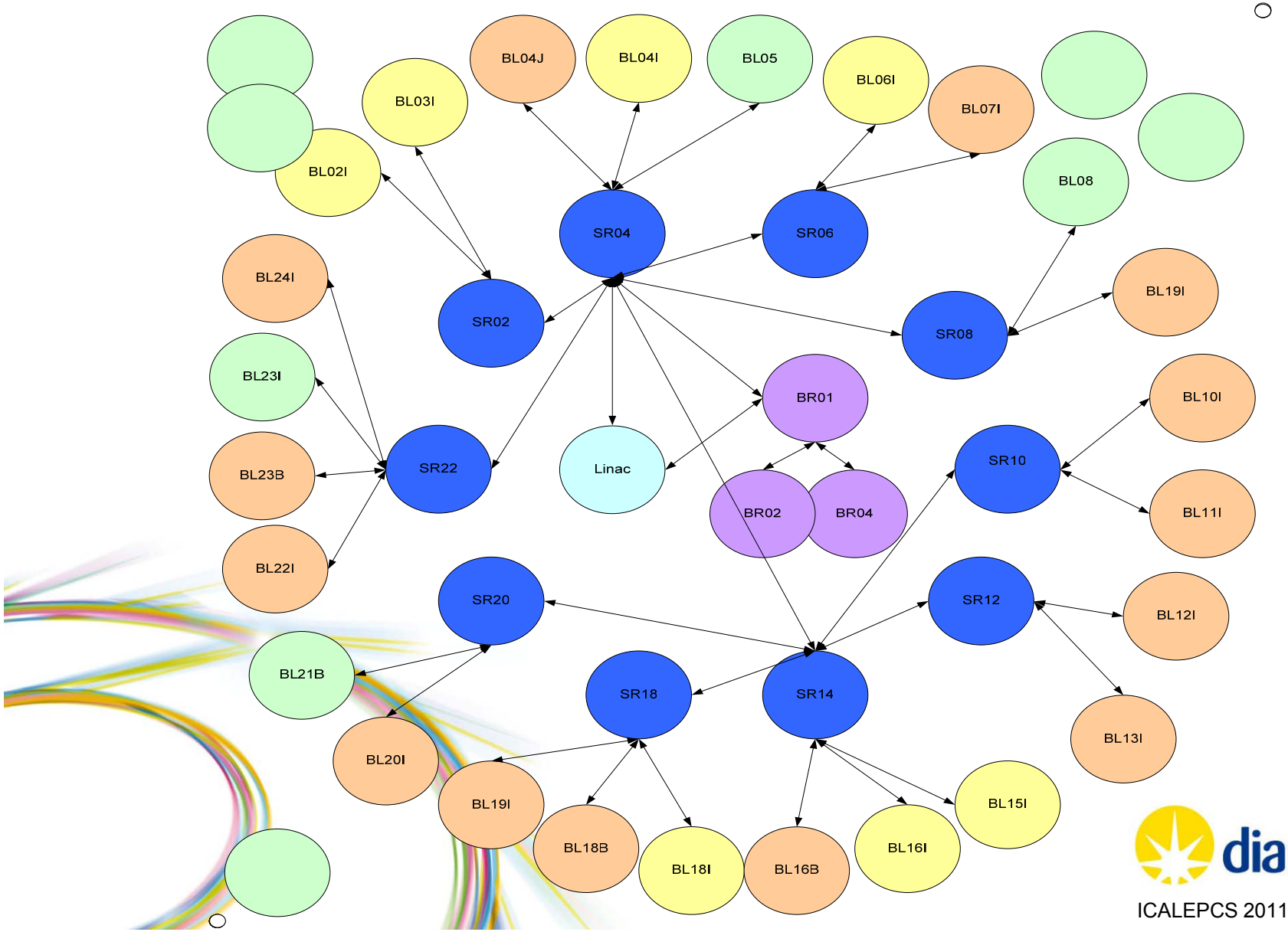
Up to 40 beamlines
+ branches

Machine operation

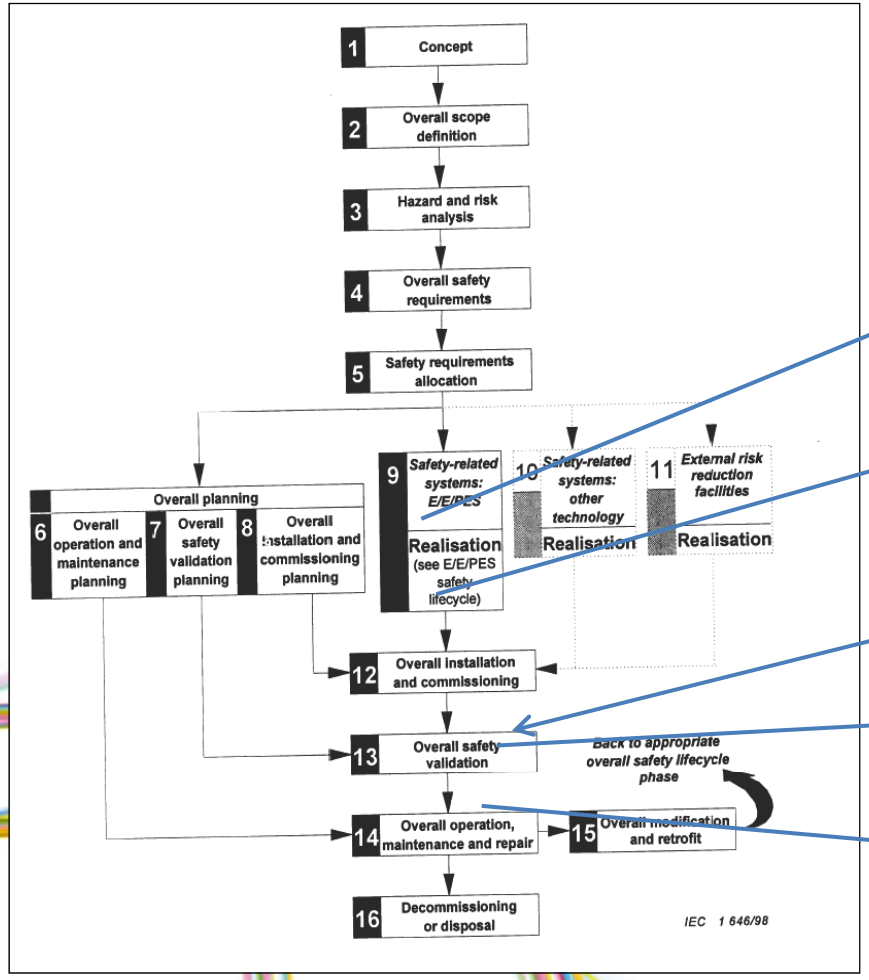


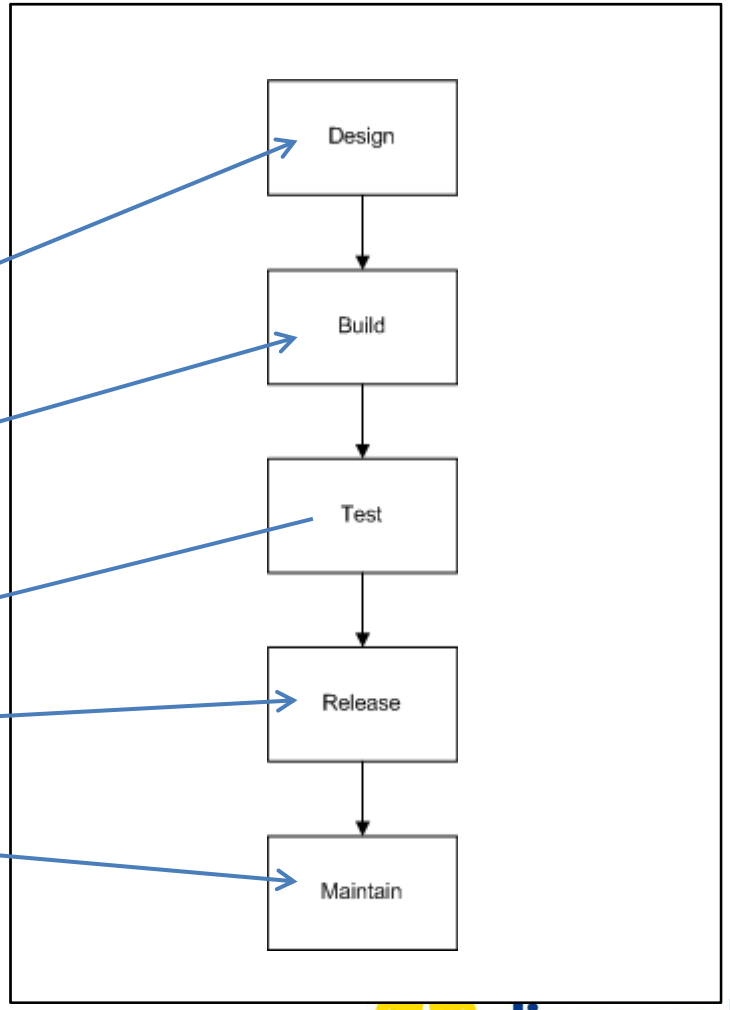
Protection - Shielding

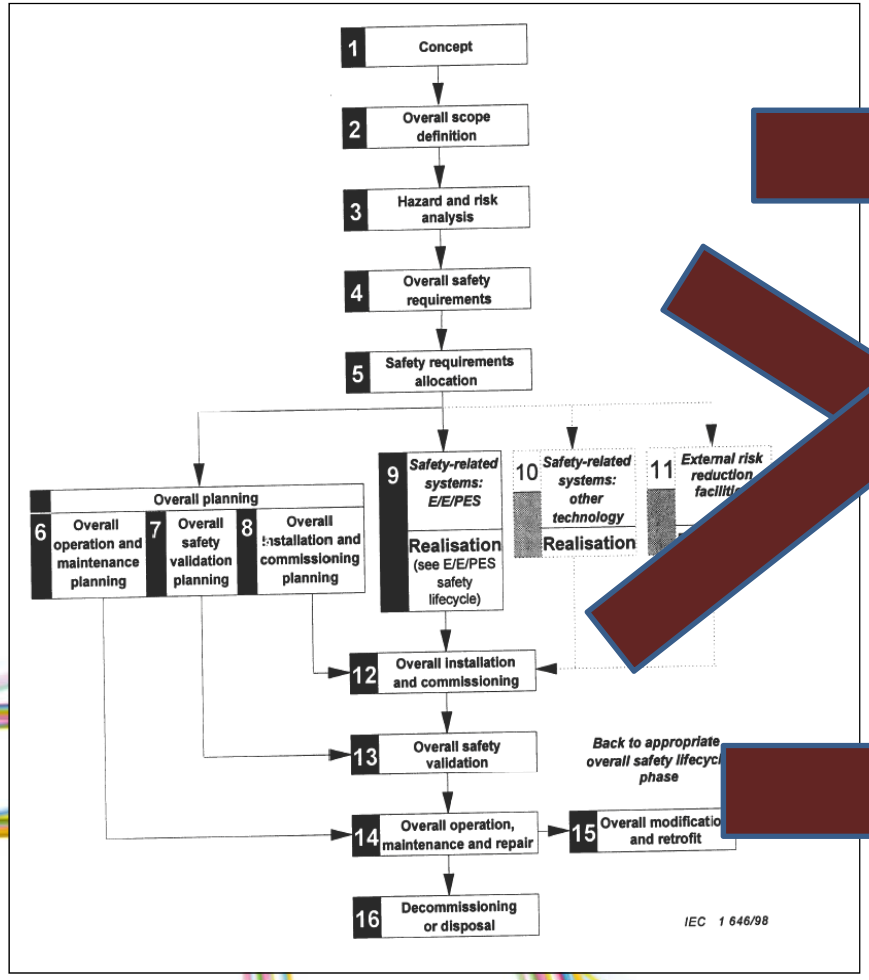
PSS Organisation

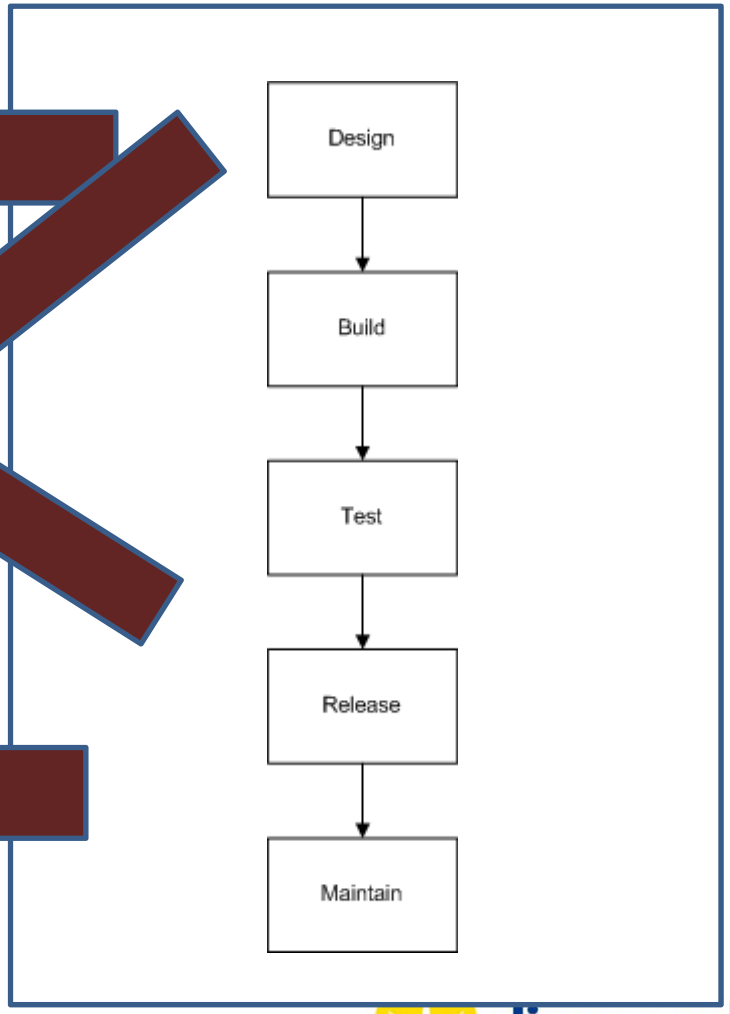


Design process






1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety-related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety-related systems: other technology
Realisation
11 External risk reduction
12 Overall installation and commissioning
13 Overall safety validation
Back to appropriate overall safety lifecycle phase
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal
IEC 1 646/98


Design
Build
Test
Release
Maintain

Database

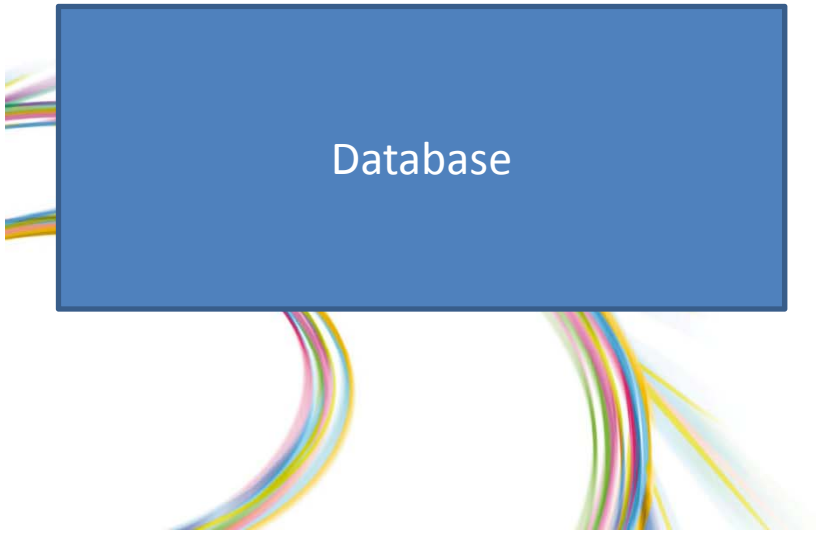
STUFF

Safety requirements

Safety model

Verification

Validation



Hazard Identification

- Identify hazards
- Estimate frequency
- Estimate consequence
- Identify safety measures
- Control measures

HAZID Form

Ref	Hazard	Consequences	Initiating Event	Frequency of Opportunity	Non-PSS Safeguards	PSS Safety Functions
1.1a	Exposure to radiation in Linac Vault	Possibility of fatality	Trained person attempts to enter vault with Linac operating	1 per day	(i) Trained personnel (ii) Card access (iii) Safety Operating Procedures prevent entry while Linac operating. (iv) Use of radiation monitors	(i) Annunciator outside door (ii) Key exchange interlock (iii) Door switches stop Linac (iv) Coloured light system inside
1.1b	Exposure to radiation in Linac Vault	Possibility of fatality	Visitor attempts to enter vault with Linac operating	1 per week	(i) Supervision by trained guide (ii) Limited group size	(i) Annunciator outside door (ii) Key exchange interlock (iii) Door switches stop Linac (iv) Coloured light system inside
1.2a	Exposure to radiation in Linac Vault	Possibility of fatality	Linac started with trained person in vault	1 per day	(i) Vault searched before start-up (two trained person search) (ii) Use of radiation monitors (mitigation)	(i) Key exchange interlock (ii) Open door inhibits start-up (iii) Search confirmation buttons (iv) Coloured light system inside (v) Warning announcements (vi) Beam Off buttons.

Database

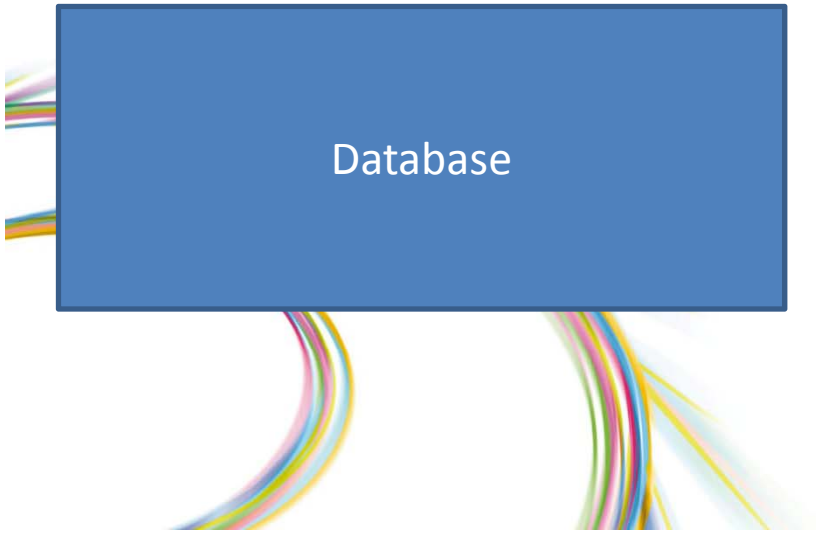
Hazards

Opportunity

Consequence

Safeguards

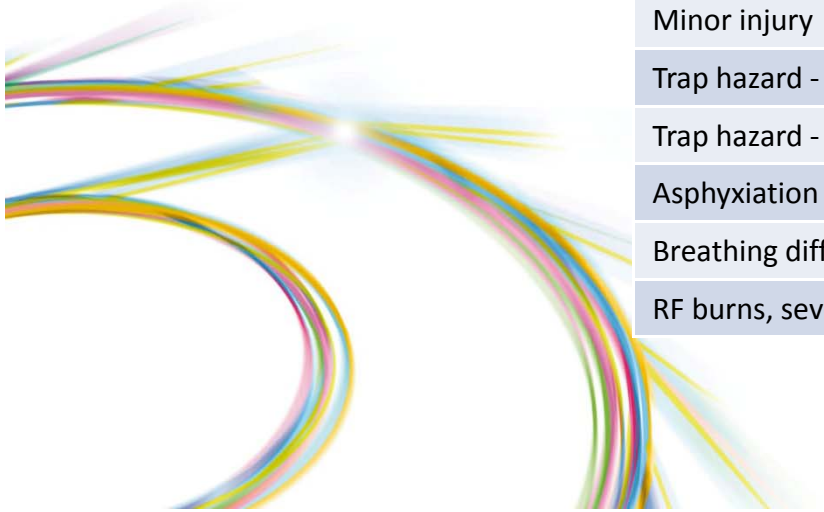
Control measures



Convert from Qualitative to Quantitative

Hazards

hazard_con	
Exposure to White Beam - Probable fatality (100%)	1
Exposure to Pink beam - Probable fatality	0.8
Exposure to Monochromatic beam - Possible fatality, serious injury	0.01
Exposure to soft beam - possible blindness, cataracts	0.01
Overexposure	0.001
Probable fatality (100%)	1
Possible fatality (50%)	0.5
Possible fatality (20%)	0.2
Serious injury	0.2
Minor injury	0.01
Trap hazard - Death or serious injury (minimise inertia by design)	0.8
Trap hazard - Serious injury	0.2
Asphyxiation	1
Breathing difficulties, irritation	0.001
RF burns, severe injury, cataracts	0.01



Convert from Qualitative to Quantitative

Opportunity

hazard_op	
once every 20mins	26280
25 per day	9125
once per day	365
once per week	52
once per month	12
once every 6 months	2
once per year	1
1 in 5 years	0.2
1 in 10 years	0.1
Not in the life of the machine	0.01

Convert from Qualitative to Quantitative

Safeguards

safeguard_ref	safeguard_function	Failure
BL_PSS_SR01	Handheld radiation monitors shall be used to detect radiation in the Beam Line Hutches.	0.1
BL_PSS_SR02	Personnel will be provided with adequate and suitable Beam Line training to enable them to work on the Beam Line unsupervised.	0.1
BL_PSS_SR03	Access to the facility will be restricted by means of a Card Access system.	0.1
BL_PSS_SR04	Operating procedures shall provide details of when it is unsafe to enter the Beam Line Hutches.	0.1
BL_PSS_SR05	The PSS shall provide an external visual indication that it is unsafe to enter the Beam Line Hutches.	0.1
BL_PSS_SR06	The PSS shall close the beam safety shutter if the door to the Beam Line Hutch is unlocked.	0.003
BL_PSS_SR07	The PSS shall dump the beam if the shutter is open and the door to the Beam Line Hutch is open.	0.003
BL_PSS_SR08	The PSS shall provide the Beam Line Hutch with an internal visual indication of danger.	0.1
BL_PSS_SR09	All untrained personnel shall be closely supervised to prevent unauthorised access to the Beam Line Hutches.	0.01
BL_PSS_SR10	The Beam Line Hutches shall be searched by a single trained person before operation of the beam.	0.1
BL_PSS_SR11	The PSS shall inhibit beam operation until search pattern has been confirmed by operation of search buttons.	0.003
BL_PSS_SR12	The PSS shall switch the Beam Line Hutch internal lighting to blue following the completion of the search until the system moves to standby.	0.1

HAZID validation

HAZID report

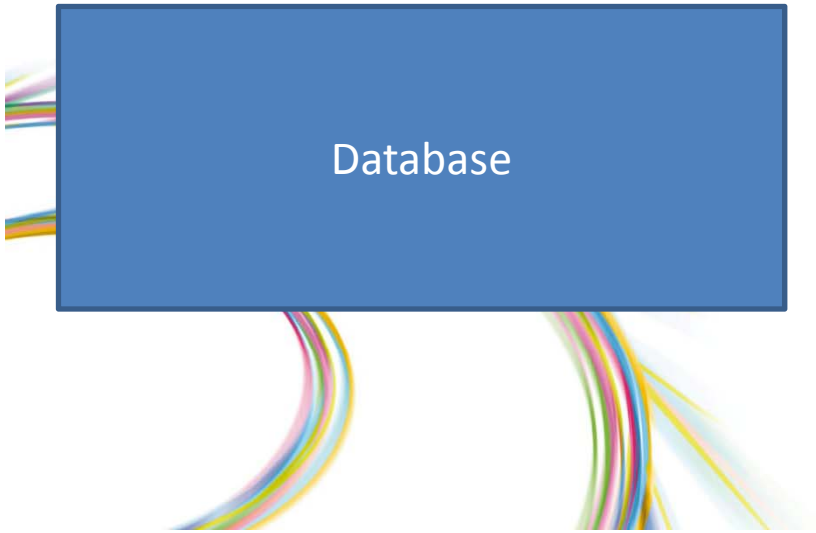
Hazards ← Hazards

Opportunity ← Opportunity

Consequence ← Consequence

Safeguards ← Safeguards

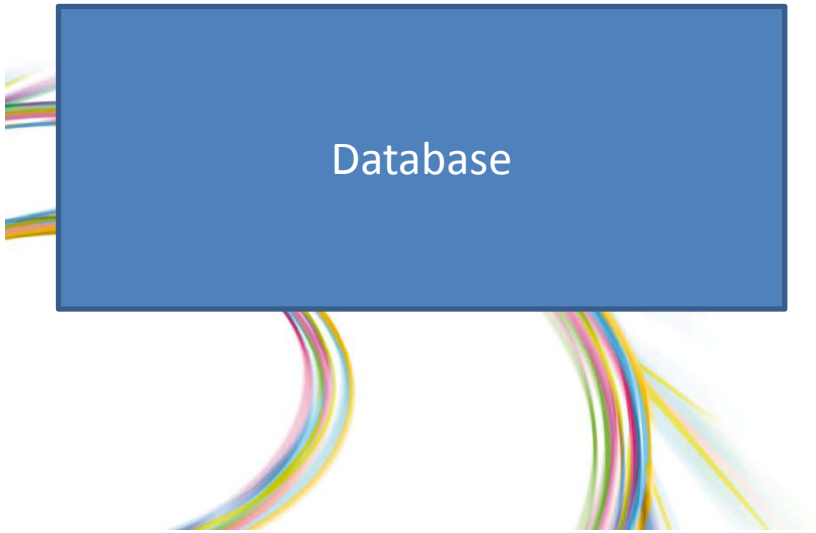
Control measures ← Control measures



HAZID validation

RUBBISH

- Hazards √
- Opportunity √
- Consequence √
- Safeguards √
- Control measures √



RUBBISH

Comparison report 1

Comparison report 2

Risk reduction

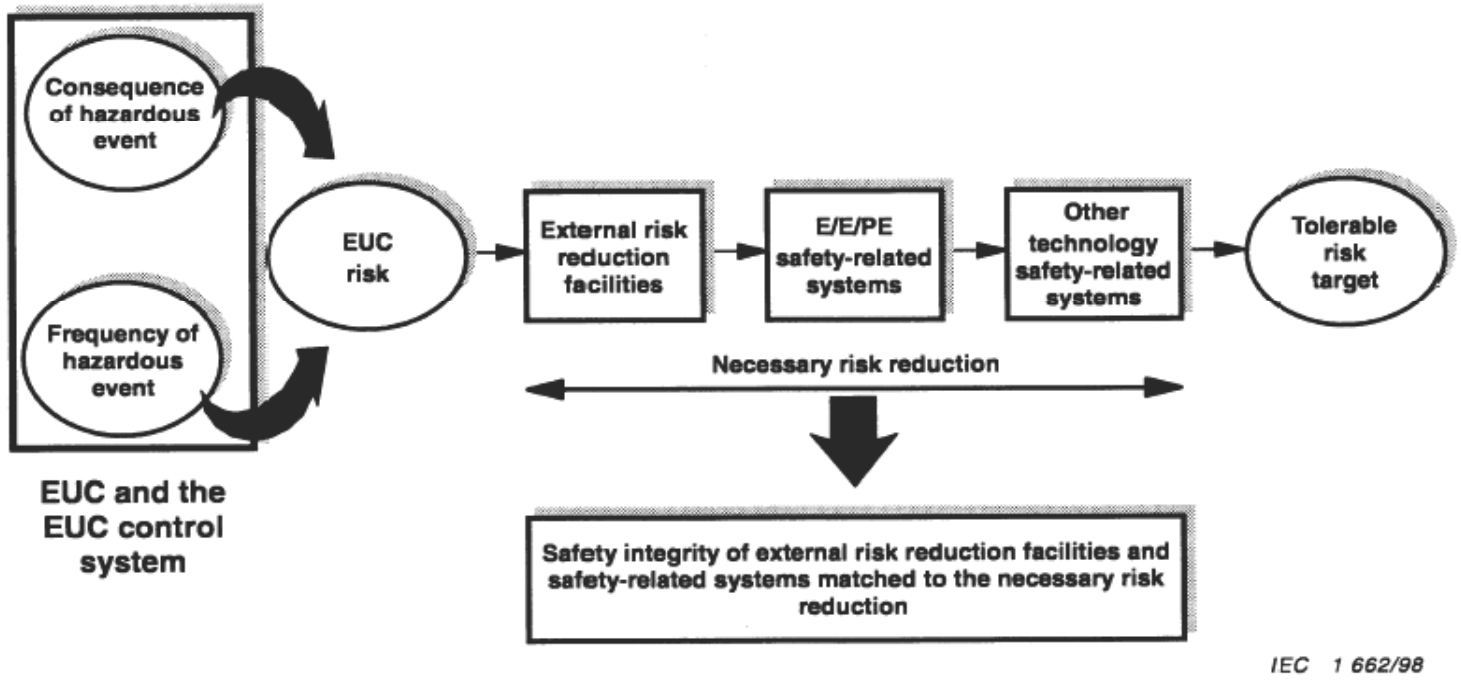
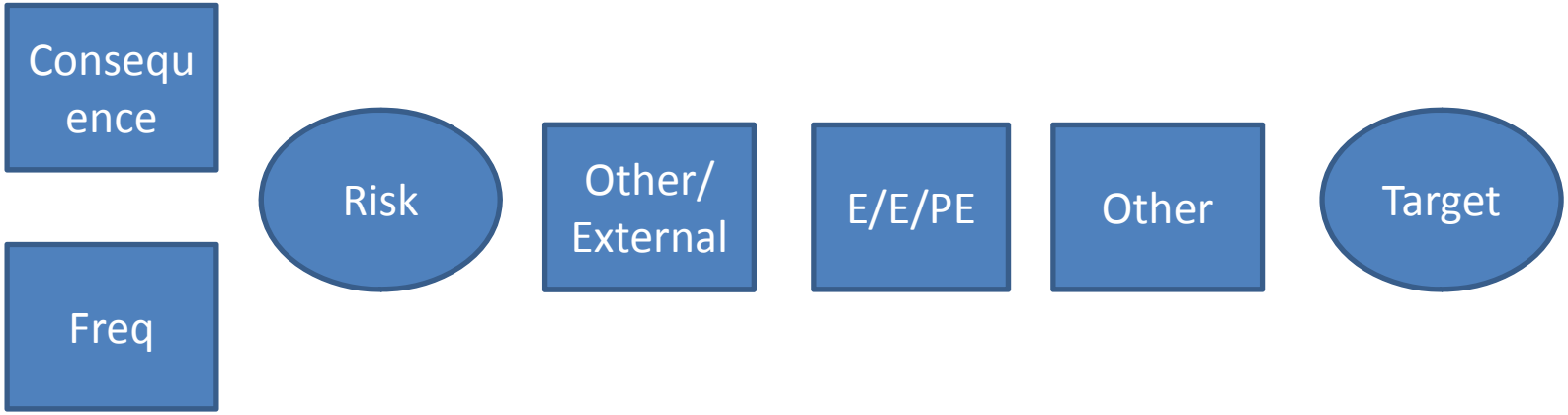


Figure A.2 – Risk and safety integrity concepts



- Local Rules
- Use of hand held rad mon
- Training
- Card Access

- Annunciator
- Door locked by PSS
- Door open interlock
- Door locked interlock
- Search confirmation
- Blue lights
- Warning tones
- BOB

Database reports – Safety margin and SIL

Hazards

Opportunity

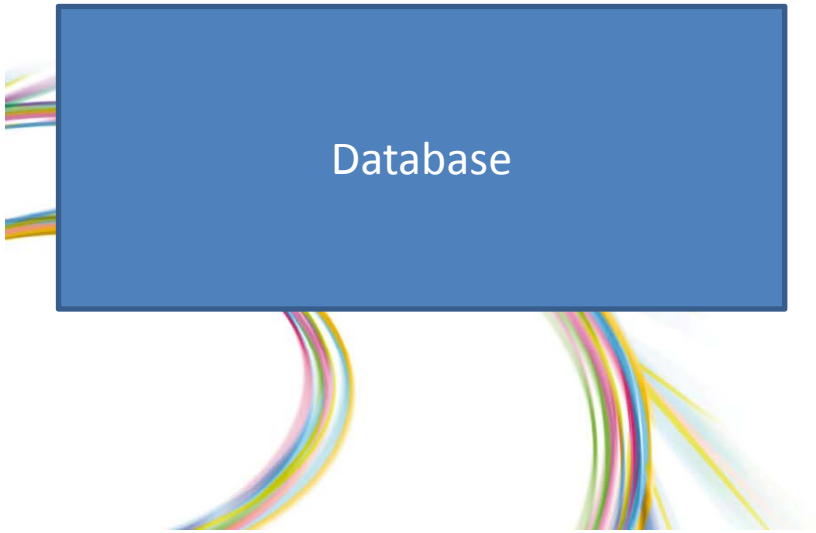
Consequence

Safeguards

Control measures

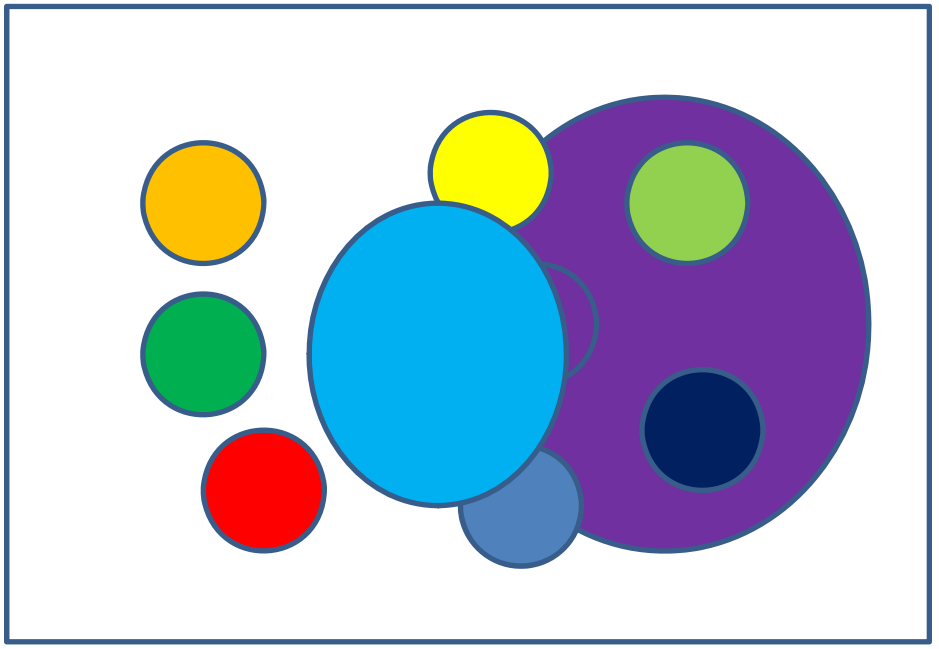
Safety Margin report

SIL Requirements report



Shortcomings and benefits of calculation

- Independence of safety measures



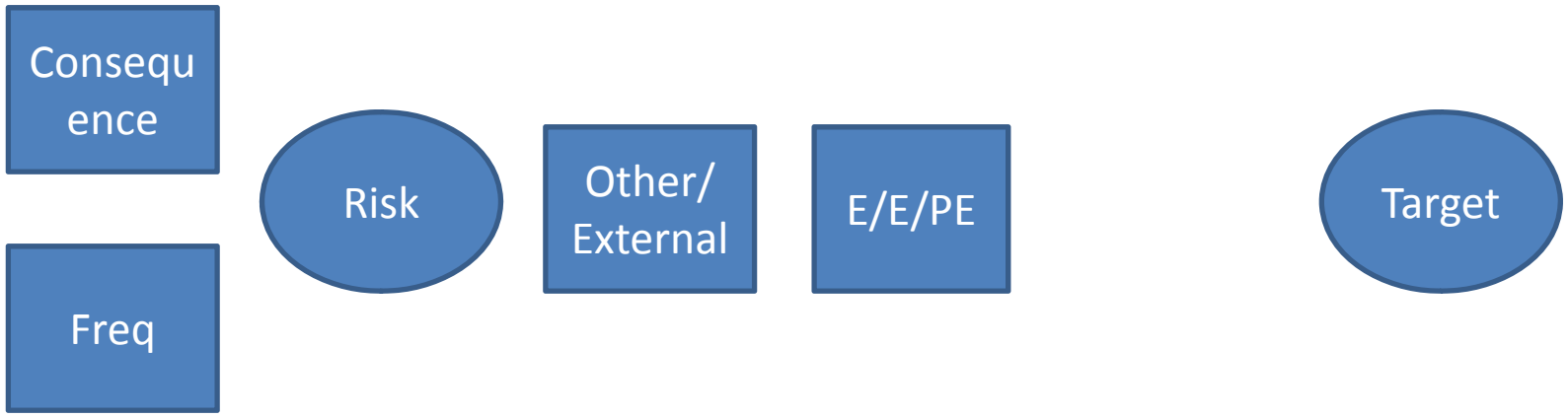
Shortcomings and benefits of calculation

- Independence of safety measures
- Common mode effects
- Human Factors

Benefits

- Quick
- Easy
- Good indication
- Reduced number of passes

Refining risk

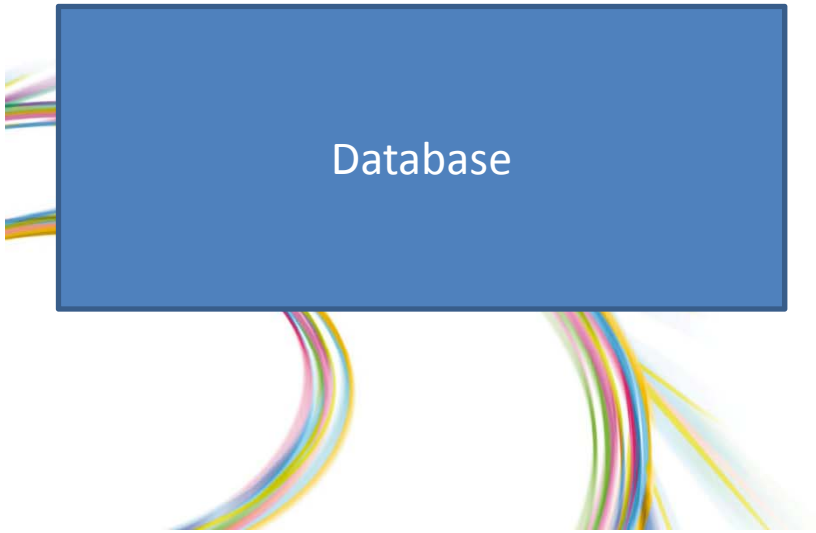


- Try to reduce the severity
- Try to reduce the frequency of opportunity
- Increase the non E/E/PE safety measures
- Increase the E/E/PE safety measures

Database reports- Safety requirements

Sort the hazard data by area to generate a safety requirements report with SIL ratings

Safety Requirements Report → Safety Requirements Specification

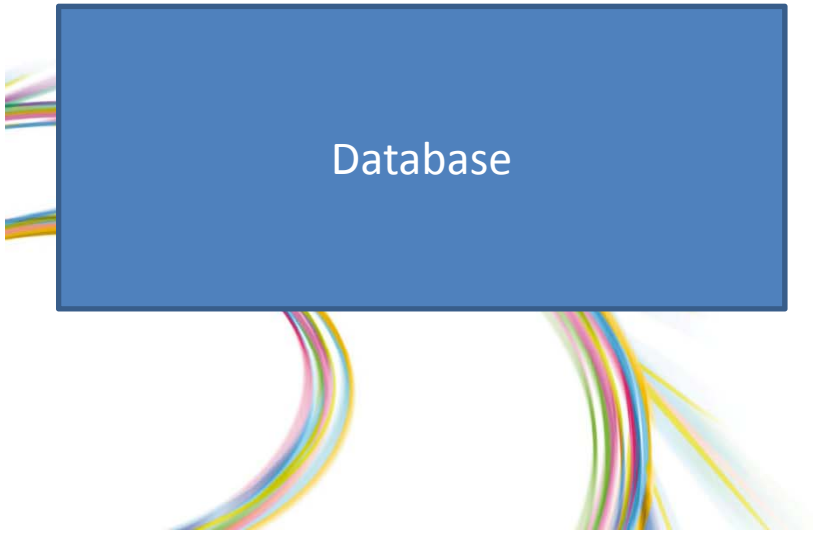


Functional performance test

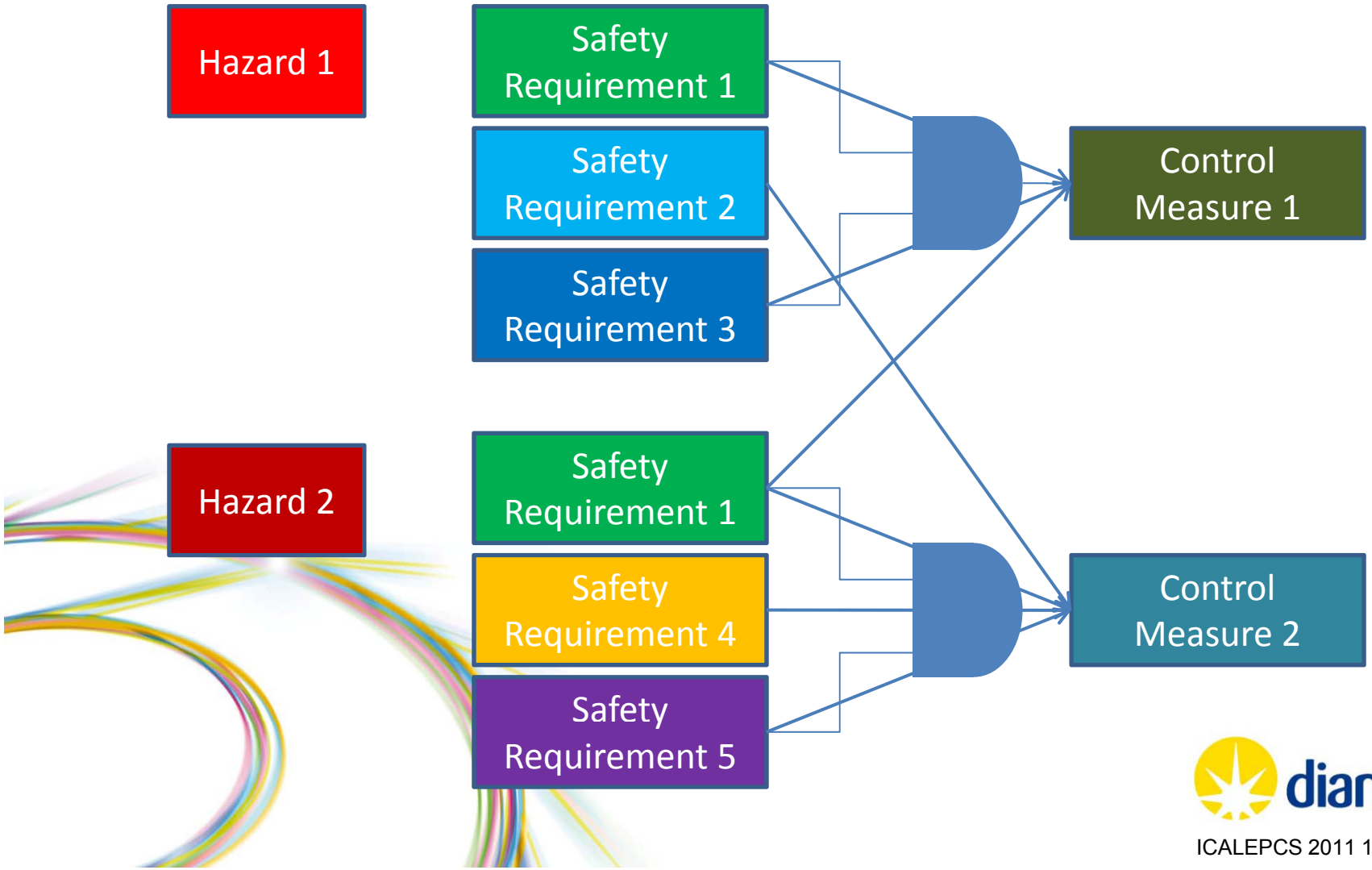
- For every Safety requirement there will be a functional performance test

Functional tests reference

Functional tests/Safety requirements cross reference Report



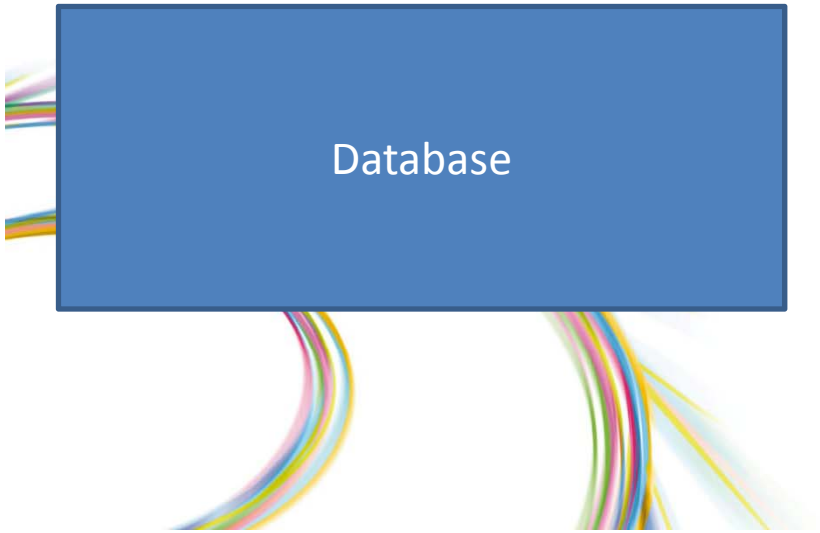
Control measures



Database Reports- Logic

Sort the hazard data by area and control measure to generate a logic report for cross checking design

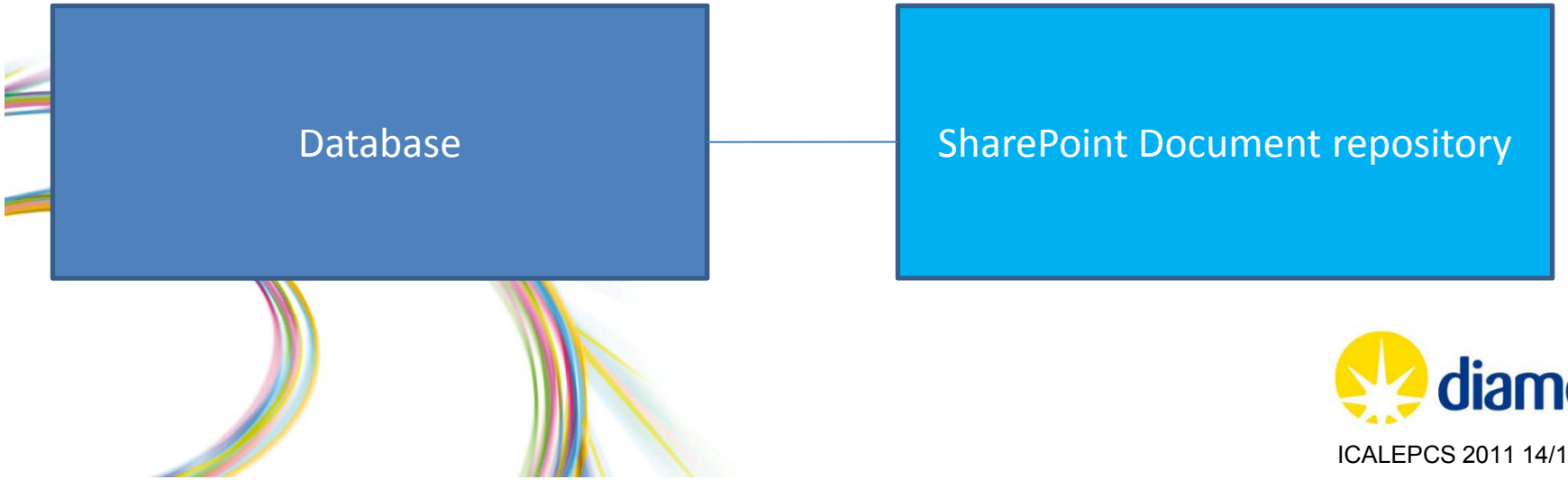
Logic design check ← Logic report



Documentation

- Each system has a suite of documents, some of which are common, recorded and linked in the database

Documentation Report



Conclusions

- The database strengthens the EN 61508 process in DLS
- It generates useful reports and cross references
- Calculations do not replace more formal assessments
- Shouldn’t be used blindly
- A useful accompaniment to normal process

Questions?

- Martin Wilson
- Principal Personnel Safety Engineer
- Diamond Light Source
- martin.wilson@diamond.ac.uk
- +44 (0)1235-778049