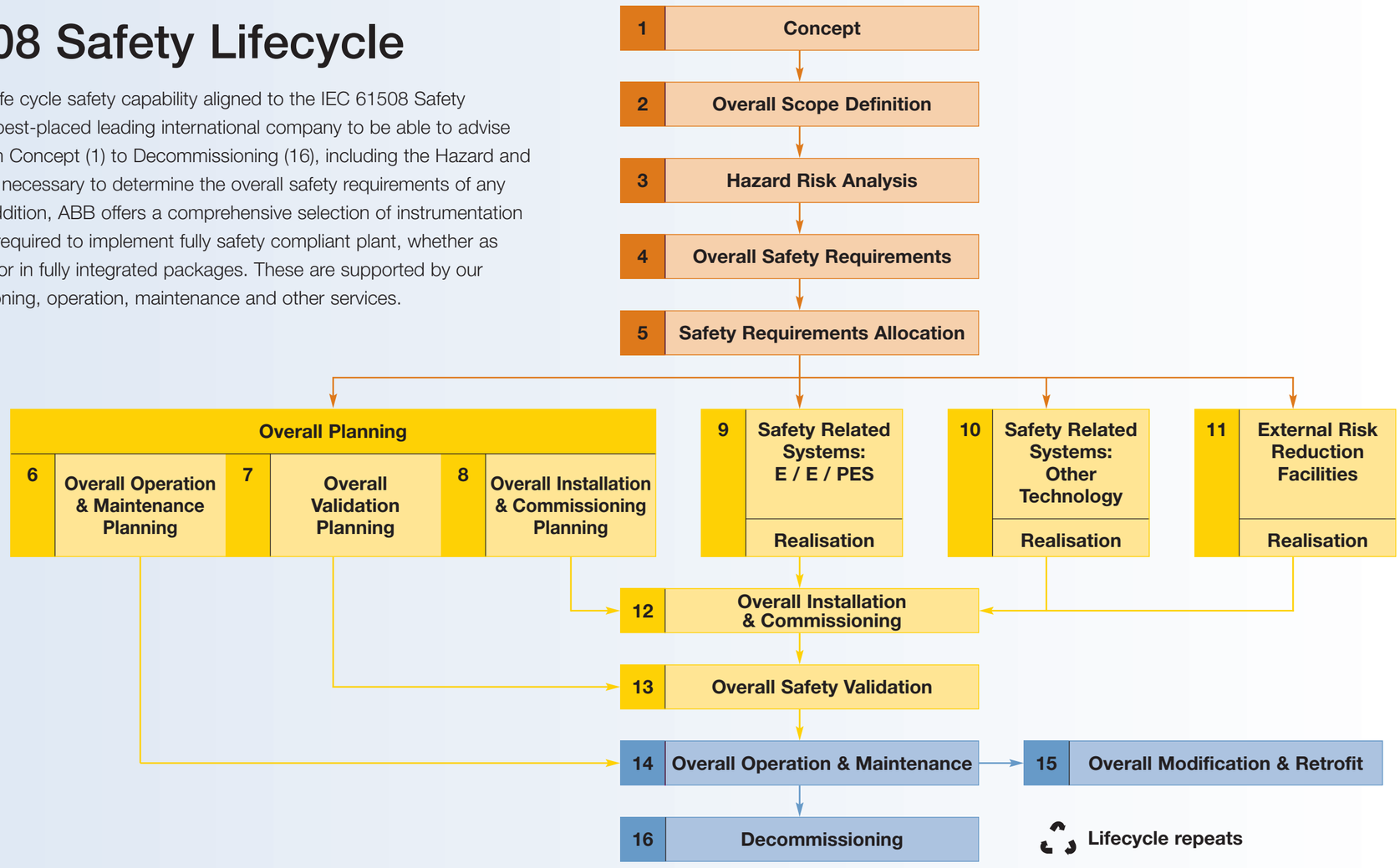
The ABB Guide to

Safety Critical Systems and International Standard IEC 61508

IEC 61508 Safety Lifecycle

ABB provides a total life cycle safety capability aligned to the IEC 61508 Safety Lifecycle. We are the best-placed leading international company to be able to advise you on all phases from Concept (1) to Decommissioning (16), including the Hazard and Risk Analysis which is necessary to determine the overall safety requirements of any plant or process. In addition, ABB offers a comprehensive selection of instrumentation and other equipment required to implement fully safety compliant plant, whether as stand alone products or in fully integrated packages. These are supported by our installation, commissioning, operation, maintenance and other services.



Overview of Lifecycle Phases

Pre-Design Phases 1-5
End User / Operator

Set the SIL target

Design and Installation Phases 6-13
(Engineering / Equipment Supplier)

Design the architecture / Provide the integrity information

Operation Phases 14-16
(End User / Operator)

Operate & Test to Verify Target SIL = Design SIL = Operation. Manage maintenance and modifications

Pre-Design Phases 1 – 5 (End User / Operator) Setting the SIL Target

Hazard & Risk Analysis

Safety Integrity Levels

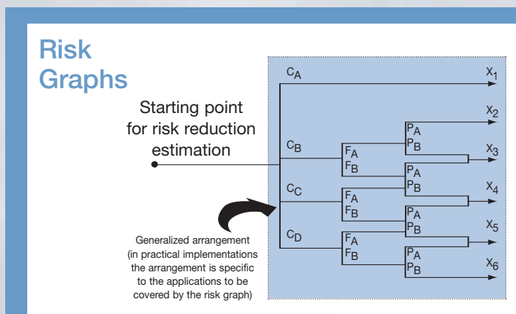
Safety Integrity Level	Average Probability of Failure on Demand (PFDavg)	% Reliability
1	0.1 to 0.01	90% to 99%
2	0.01 to 0.001	99% to 99.9%
3	0.001 to 0.0001	99.9% to 99.99%
4	0.0001 to 0.00001	99.99% to 99.999%

Typical Methodology

- Hazard studies and HAZOPs
- Evaluate possible consequences
- Establish tolerable frequencies vs ALARP
- Build event chain
- Estimate demand rates
- Define protection required
- Specify required Safety Integrity Level

SIL Determination Methodologies

Risk Graphs



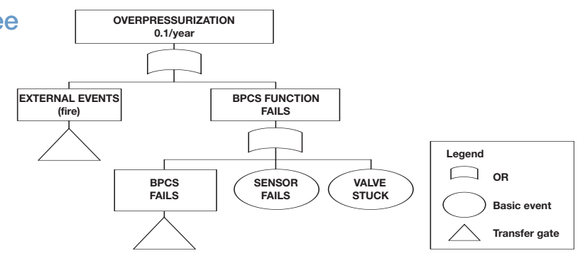
W_3	W_2	W_1
a	---	---
1	a	---
2	1	a
3	2	1
4	3	2
b	4	3

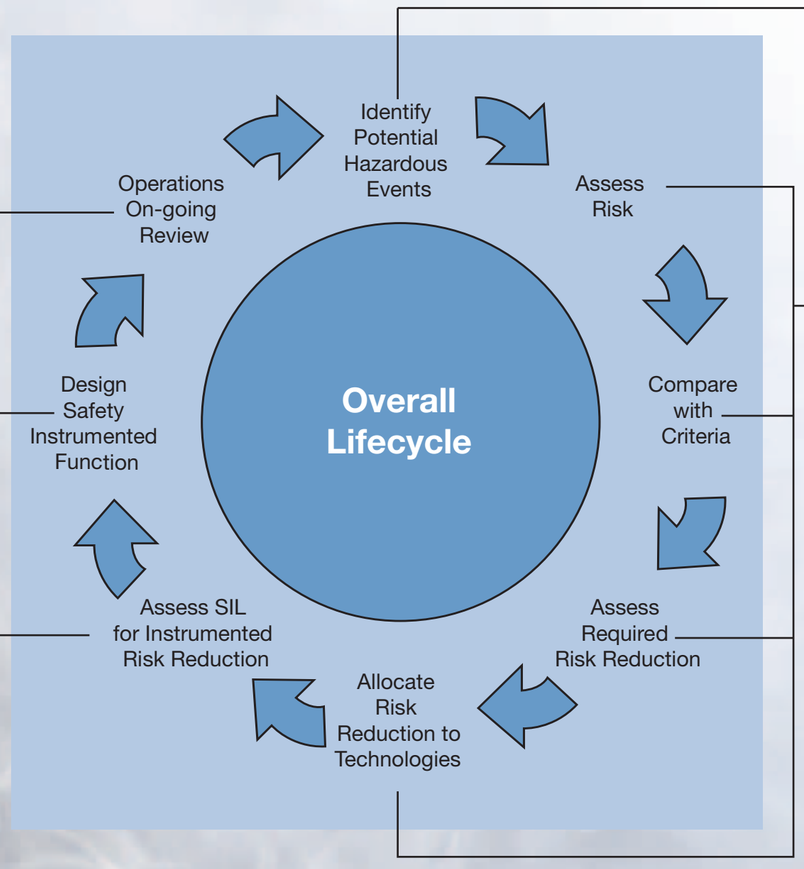
--- = No safety requirements
a = No special safety requirements
b = A single SIF is not sufficient
1, 2, 3, 4 = Safety integrity level

Layer of Protection Analysis

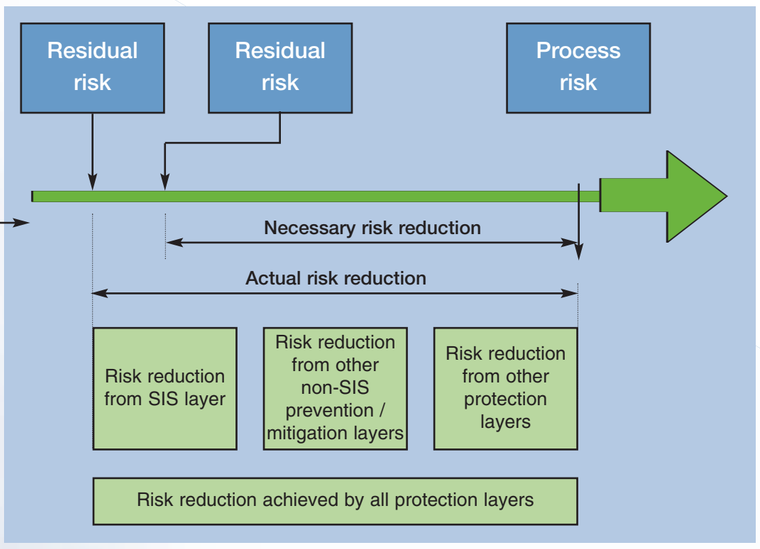
#	1	2	3	4		5		6	7	8	9	10	11
				PROTECTION LAYERS									
	Impact event description F.3 F.14.1	Severity level F.4 F.14.1	Initiating cause F.5 F.14.2	Initiation likelihood F.6 F.14.3	General process design F.14.4	BPCS F.14.5	Alarms, etc. F.14.6	Additional mitigation, restricted access F.8 F.14.7	IPL additional mitigation dikes, pressure relief F.9 F.14.8	Inter-mediate event likelihood F.10 F.14.9	SIF integrity level F.11 F.14.10	Mitigated event likelihood F.12 F.14.10	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0,1	0,1	0,1	0,1	0,1	PRV 01	10^{-7}	10^{-2}	10^{-9}	High pressure causes column rupture
2	Fire from distillation column rupture	S	Steam control loop failure	0,1	0,1		0,1	0,1	PRV 01	10^{-6}	10^{-2}	10^{-8}	Same as above
N													

Fault Tree Analysis





Introducing Risk Reduction and Risk Targets



Demand more from your instrumentation.
Demand more from your source.