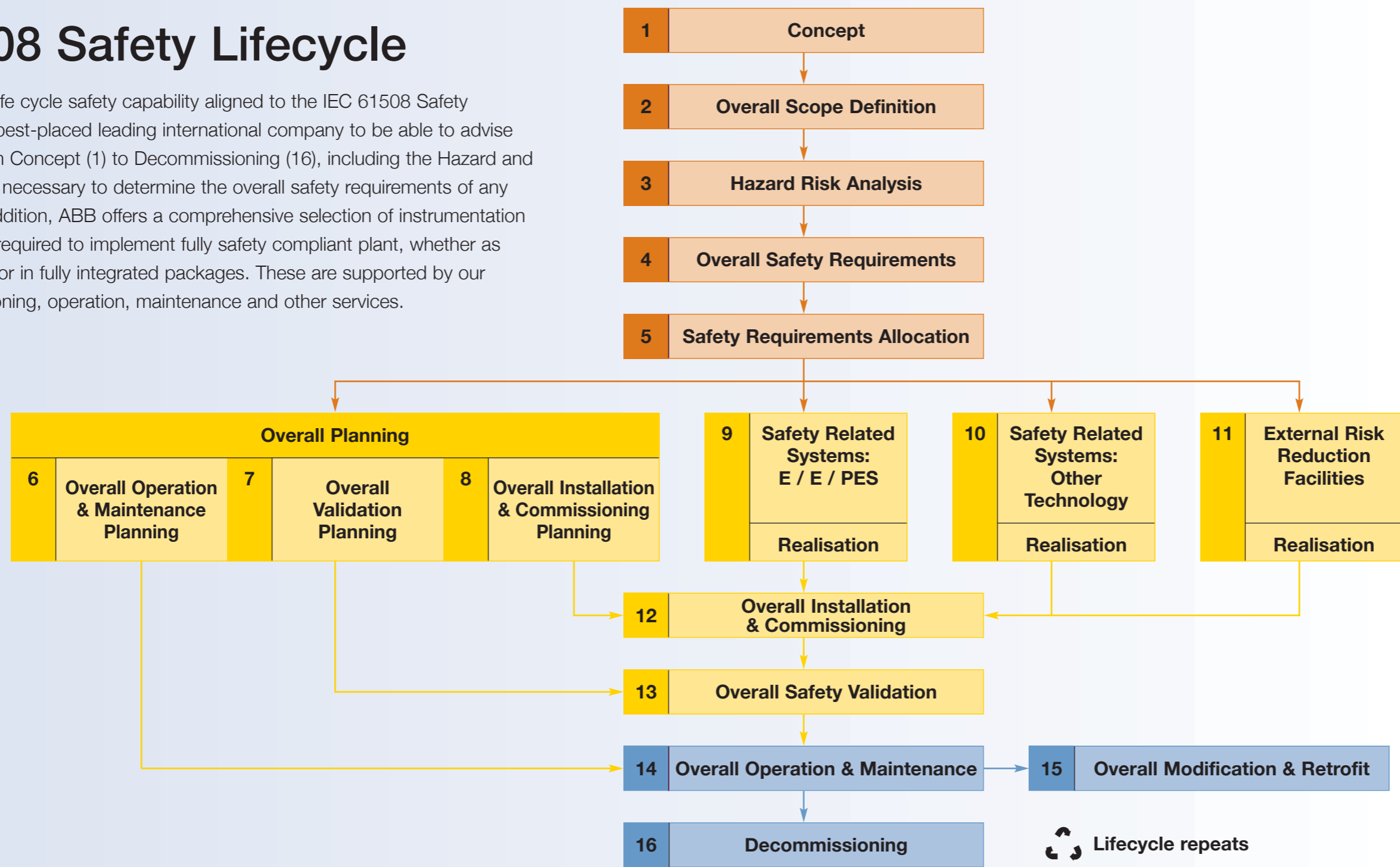


# The ABB Guide to Safety Critical Systems and International Standard IEC 61508

## 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

### Safety Integrity Levels

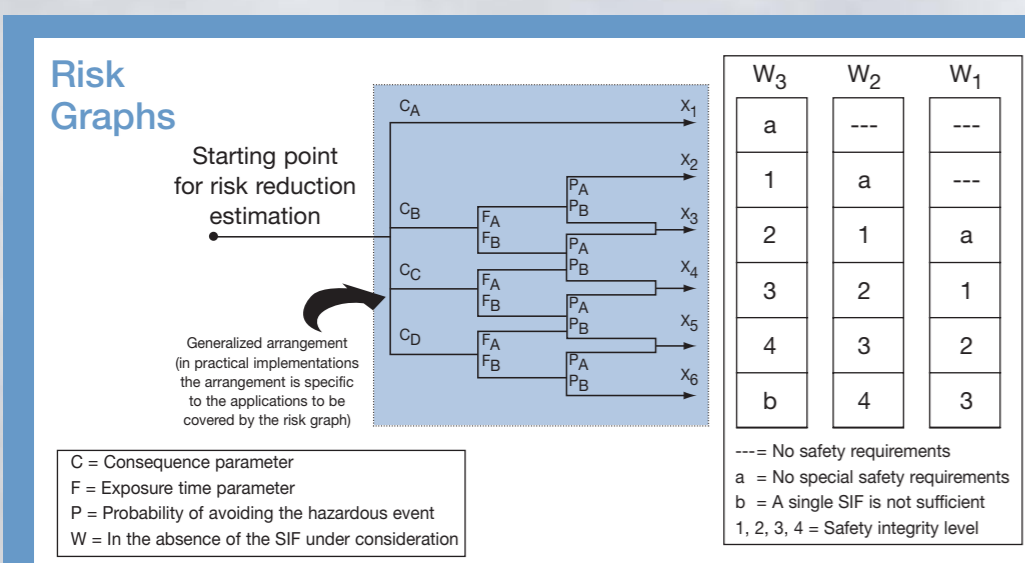
Safety Integrity Level	Average Probability of Failure on Demand (PFDavg)	% Reliability
1	0.1 to 0.01	90% to 99%
2	0.01 to 0.001	99% to 99.9%
3	0.001 to 0.0001	99.9% to 99.99%
4	0.0001 to 0.00001	99.99% to 99.999%

## Hazard & Risk Analysis

### 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

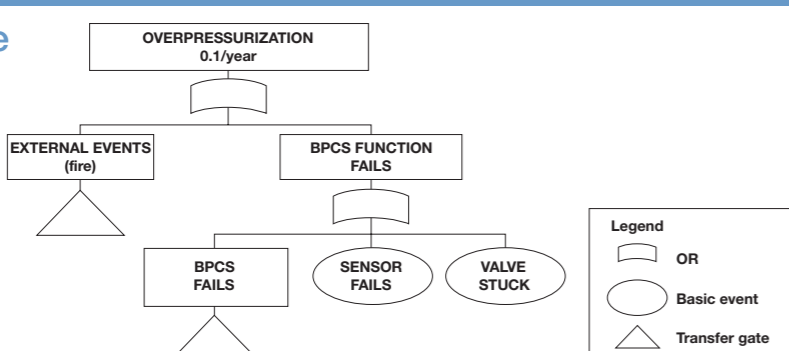
### SIL Determination Methodologies



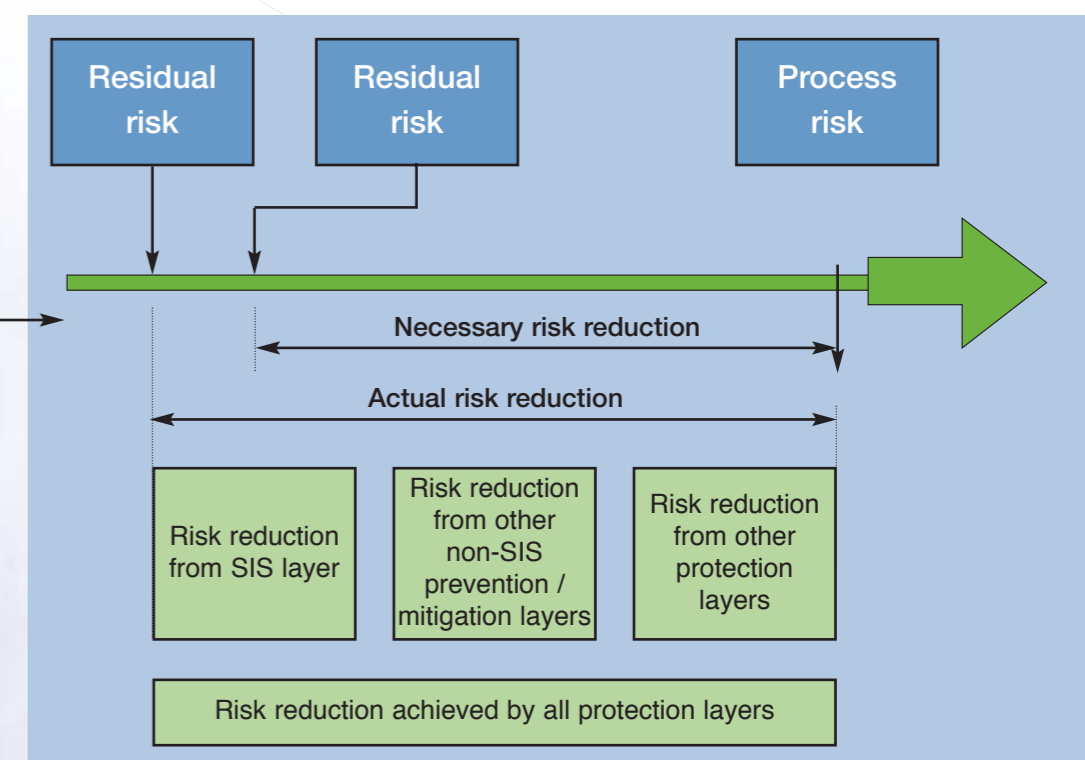
### Layer of Protection Analysis

#	1	2	3	4	5	6	7	8	9	10	11	
	Impact event descriptor F3 F14.1	Severity level F4 F14.1	Initiating cause F5 F14.2	Initiation likelihood F6 F14.3	General process design F7 F14.4	BPCS F8 F14.5	Alarms, etc. F9 F14.6	Additional restricted access F10 F14.7	IPL additional mitigation dikes, pressure relief F11 F14.8	Inter-mediate event likelihood F12 F14.9	SIF integrity level F13 F14.10	Mitigated event likelihood F14 F14.11
1	Fire from distillation column rupture	S	Loss of cooling water	0,1	0,1	0,1	0,1	0,1	PRV 01	10 <sup>-4</sup>	10 <sup>-4</sup>	10 <sup>-4</sup>
2	Fire from distillation column rupture	S	Steam control loop failure	0,1	0,1	0,1	0,1	0,1	PRV 01	10 <sup>-4</sup>	10 <sup>-4</sup>	10 <sup>-4</sup>

### Fault Tree Analysis



### Introducing Risk Reduction and Risk Targets



For Safety Lifecycle and Hazard Analysis advice, please call 01642 372000.  
For details of relevant ABB Instrumentation, Systems and Equipment, please call 0870 600 6122.

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

