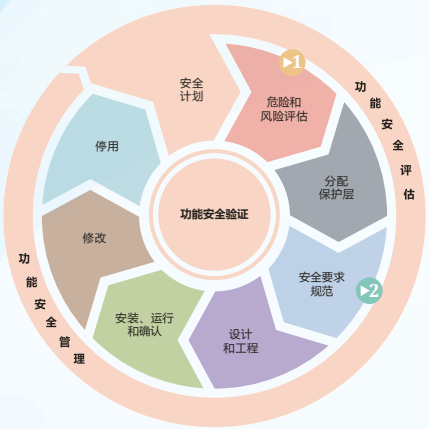
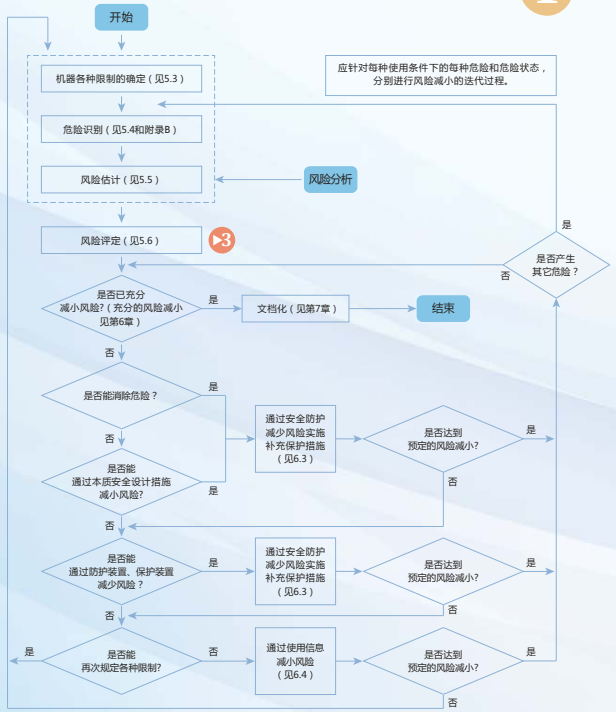
功能安全
Functional Safety

CHENZHU 辰竹

安全生命周期
Safety lifecycle



危险和风险评估
Hazard and risk assessment



来源：ISO 12100:2010

安全要求——过程工业 系统架构（SIL）
Safety requirements —— System architecture (SIL)

SFF		HFT		
Type A	Type B	0	1	2
-	＜60%	不允许	SIL1	SIL2
＜60%	60%~90%	SIL1	SIL2	SIL3
60%~90%	90%~99%	SIL2	SIL3	SIL4
≥90%	≥99%	SIL3	SIL4	SIL4

来源：IEC 61508-2:2010

SIL→ PFD（低要求操作模式） SIL→ PFH（高要求或连续操作模式）		
SIL	PFD_{avg}	PFH
SIL1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$
SIL2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
SIL3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
SIL4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$

来源：IEC 61508-1:2010

SIL	最低硬件故障裕度（HFT）
SIL1（任何模式）	0
SIL2（低要求模式）	0
SIL2（高要求/连续模式）	1
SIL3（任何模式）	1
SIL4（任何模式）	2

来源：IEC 61511-1:2016

安全要求——机械设备 估计由SRP/CS达到的PL
Safety requirements —— Evaluating PL achieved by SRP/CS

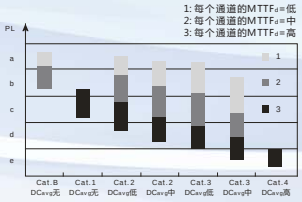
类别	Cat.B	Cat.1	Cat.2	Cat.2	Cat.3	Cat.3	Cat.4
DC_{avg}	无	无	低	中	低	中	高
每个通道的$MTTF_d$							
低	a	不包括	a	b	b	c	不包括
中	b	不包括	b	c	c	d	不包括
高	不包括	c	c	d	d	d	e

诊断覆盖率（DC）	
诊断指标	范围
无	DC ＜ 60%
低	60% ≤ DC ＜ 90%
中	90% ≤ DC ＜ 99%
高	99% ≤ DC

每个通道的平均危险失效时间（$MTTF_d$）	
每个通道的指标	每个通道的范围
低	3年 ≤ $MTTF_d$ < 10年
中	10年 ≤ $MTTF_d$ < 30年
高	30年 ≤ $MTTF_d$ ≤ 100年

PL 和 SIL 之间的关系

PL	SIL（参见IEC 61508-1）高要求或连续操作模式
a	无对应等级
b	SIL1
c	SIL1
d	SIL2
e	SIL3



来源：ISO 13849-1:2015

风险评定——过程工业 SIL风险图
Risk evaluation —— Risk graph of SIL

W3	W2	W1
a	-	-
SIL1	a	-
SIL2	SIL1	a
SIL3	SIL2	SIL1
SIL4	SIL3	SIL2
b	SIL4	SIL3

- = 无安全要求
a = 无特殊安全要求
b = 单独一个SIF是不够的

W = 不期望事件的发生概率
W1: 非常低
W2: 低
W3: 相对高

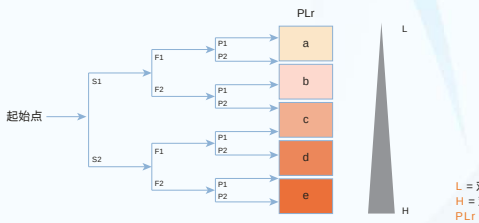
C = 后果参数
CA: 轻微人员伤害; 轻微有害环境影响
CB: 对一人或多人的严重永久伤害或一人死亡暂时的，重大的有害环境影响
CC: 几人死亡；持续的,重大的有害环境影响
CD: 灾难性后果；多人死亡

F = 暴露时间参数
FA: 很少到经常
FB: 经常到永久

P = 避开危险事件的概率
PA: 在一定条件下可能
PB: 几乎不可能

来源：IEC 61511-3:2016

风险评定——机械设备 PL风险图
Risk evaluation —— Risk graph of PL



L = 对风险减小的作用小
H = 对风险减小的作用大
PLr = 要求的性能等级

S = 伤害的严重度
S1: 轻微（通常是可恢复的伤害）
S2: 严重（通常是不可恢复的伤害或死亡）

F = 暴露于危险的频率和（或）持续时间
F1: 很少-不常和（或）暴露时间短
F2: 频繁-连续和（或）暴露时间长

P = 避开危险或限制伤害的可能性
P1: 在特定条件下可能
P2: 几乎不可能

来源：ISO 13849-1:2015

术语
Glossary

DC	诊断覆盖率	PL	性能等级
HFT	硬件故障裕度	SIL	安全完整性等级
PFD	要求时的平均失效概率	SIS	安全仪表系统
PFH	每小时危险失效概率	SFF	安全失效分数
$MTTF_d$	平均危险失效时间	SRP/CS	控制系统有关安全部件

上海辰竹仪表有限公司
SHANGHAI CHENZHU INSTRUMENT CO.,LTD.

地　　址：上海市民益路201号漕河泾开发区松江新兴产业园区6号楼　　邮　　编：201612
公司总机：021-64513350　销售服务：021-64360668
技术支持：400 881 0780　传　　真：021-64846984
邮　　箱：chenzhu@chenzhu-inst.com

【辰竹官方微信】　【辰竹官方网站】

SIL IEC61508 GB/T 20438　SIL IEC61511 GB/T 21109　SIL IEC62061 GB 28526　PL ISO13849 GB/T 16855