中国化学品安全协会

“化危为安”线上讲堂

HAZOP、LOPA、SIL 应用分析

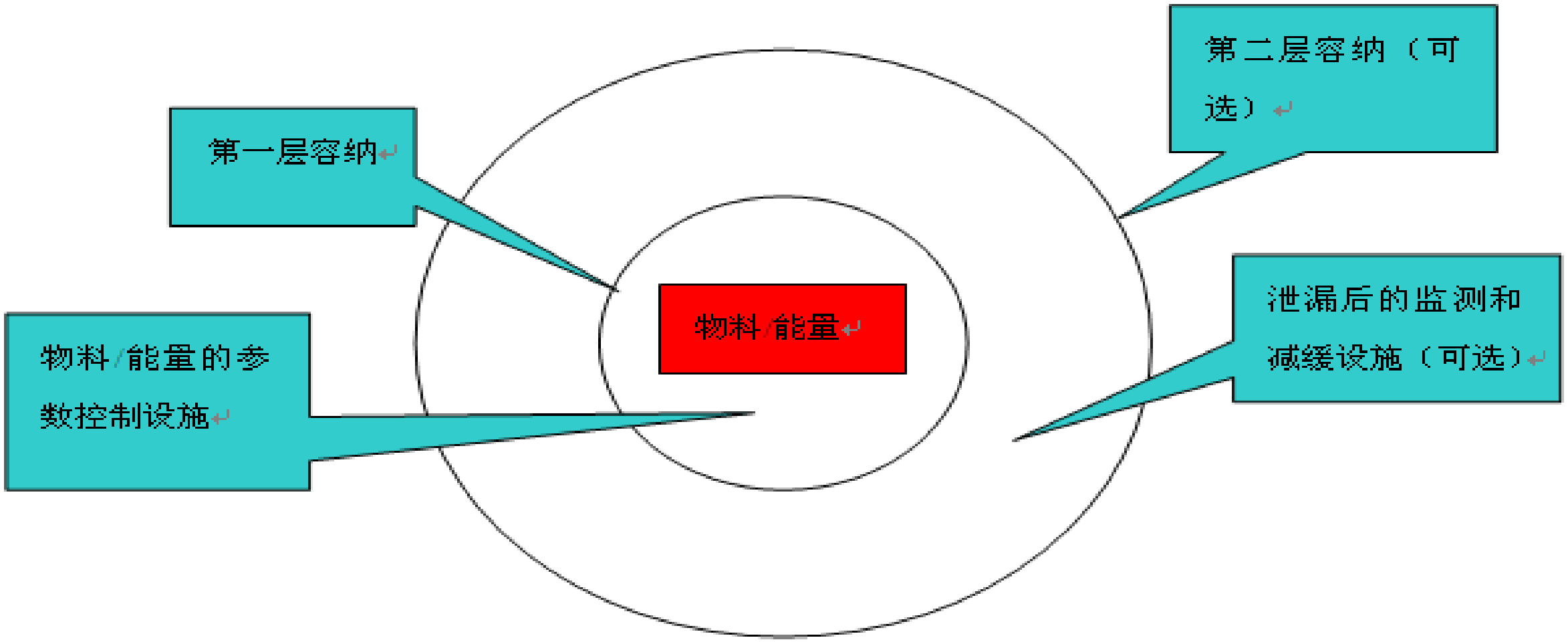
唐彬
北京安必达科技有限公司
13802084672
Beijing anbida technology co.LTD

专业/卓越/高效

目录
Content

01 HAZOP分析

物料/能量的控制模型



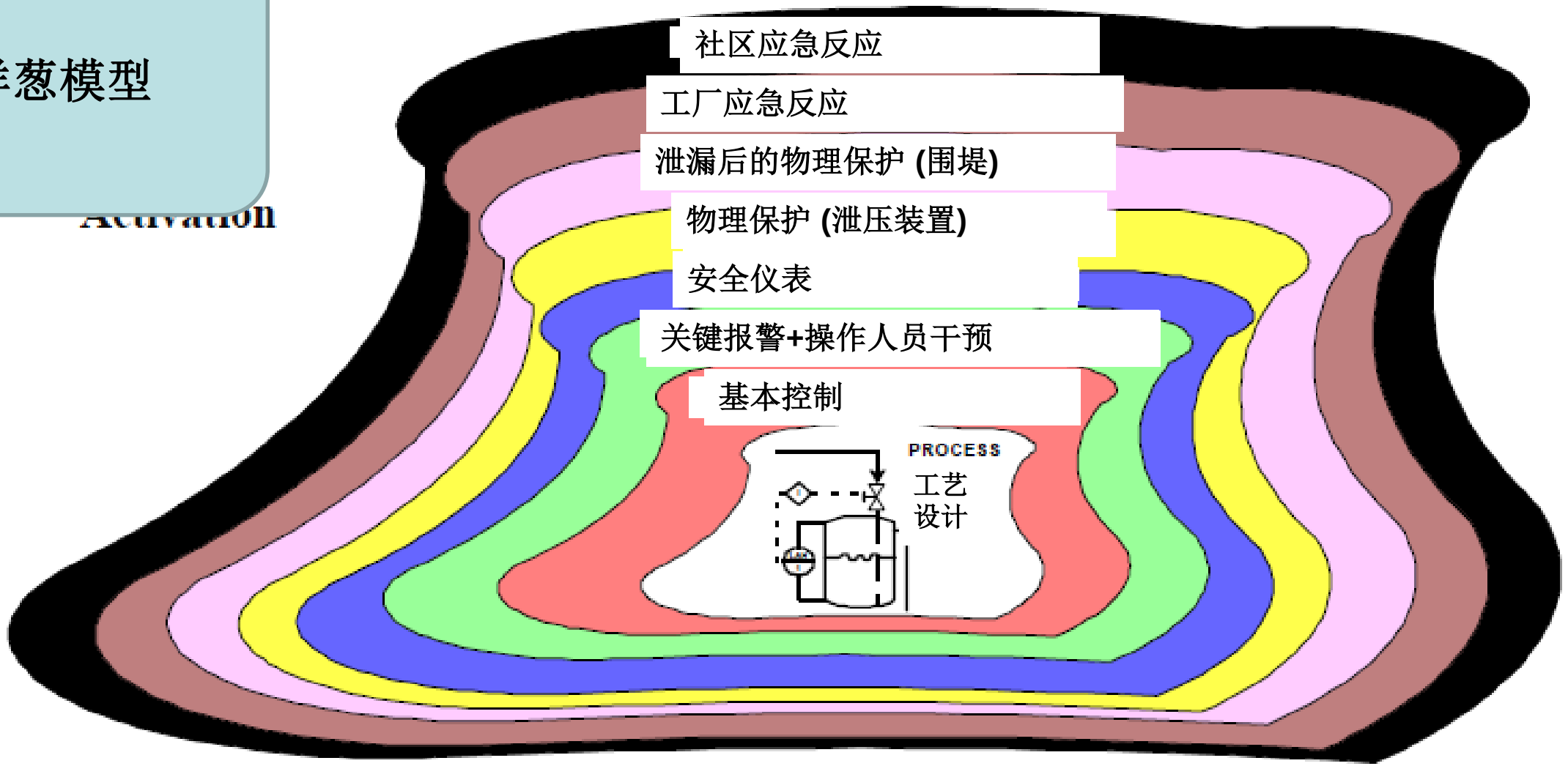
保证物料在正常生产时不意外泄漏的2个条件：

1. 物料参数在设计范围内，即没有偏离。

偏离：偏离设计意图，通常用参数和引导词组合来表达，例如：压力高，液位高，流量无，物料中含水量大等。

2. 第一层容纳完好性（MI）

洋葱模型

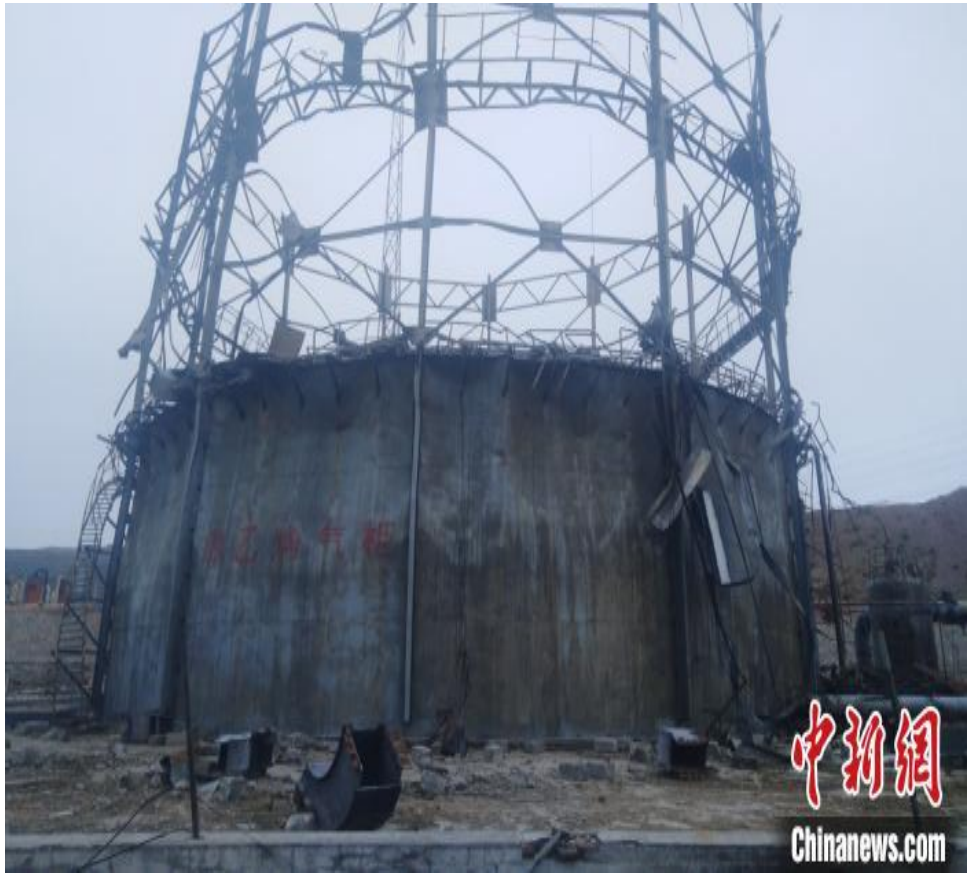

社区应急反应
工厂应急反应
泄漏后的物理保护 (围堤)
物理保护 (泄压装置)
安全仪表
关键报警+操作人员干预
基本控制
PROCESS
工艺
设计

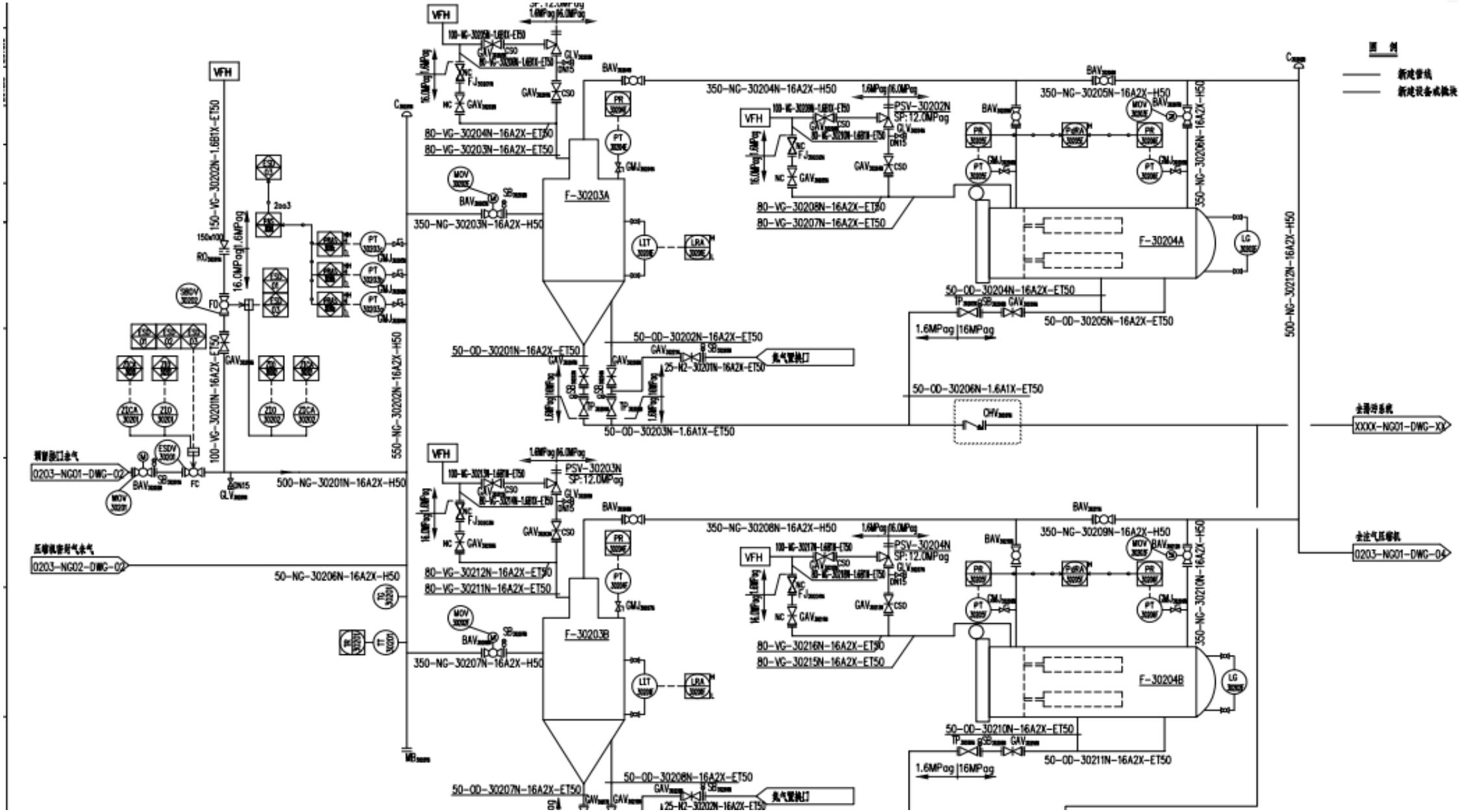
什么是HAZOP

- HAZOP - Hazard and Operability Study (Analysis)
- Hazard - 危险
- Operability - 可操作性
- Study - 分析、研究
- HAZOP - 危险与可操作性分析/研究

河北盛华-2018.11.28

内蒙古东兴化工-2019.4.24




F-30203A
F-30203B
F-30204A
F-30204B
350-NG-30204N-16A2X-H50
350-NG-30205N-16A2X-H50
350-NG-30206N-16A2X-H50
350-NG-30209N-16A2X-H50
350-NG-30203N-16A2X-H50
350-NG-30207N-16A2X-H50
80-VG-30204N-16A2X-ET50
80-VG-30203N-16A2X-ET50
80-VG-30208N-16A2X-ET50
80-VG-30207N-16A2X-ET50
80-VG-30212N-16A2X-ET50
80-VG-30211N-16A2X-ET50
80-VG-30216N-16A2X-ET50
80-VG-30215N-16A2X-ET50
50-OD-30204N-16A2X-ET50
50-OD-30205N-16A2X-ET50
50-OD-30210N-16A2X-ET50
50-OD-30211N-16A2X-ET50
50-OD-30201N-16A2X-ET50
50-OD-30202N-16A2X-ET50
50-OD-30203N-1.6A1X-ET50
50-OD-30206N-1.6A1X-ET50
50-OD-30207N-16A2X-ET50
50-OD-30208N-16A2X-ET50
500-NG-30212N-16A2X-H50
500-NG-30201N-16A2X-H50
550-NG-30202N-16A2X-H50
50-NG-30206N-16A2X-H50
150-VG-30202N-1.6B1X-ET50
100-VG-30201N-16A2X-ET50
PSV-30202N SP:12.0MPag
PSV-30203N SP:12.0MPag
PSV-30204N SP:12.0MPag
1.6MPag|16MPag
0203-NG01-DWG-02
0203-NG02-DWG-02
XXXX-NG01-DWG-XX
0203-NG01-DWG-04
新建管线
新建设备或撬块

HAZOP的原理（1）

HAZOP 原理总结-六步法（4+2）

- 看中间找偏离
- 看左面找原因

中间开始，双向推导

- 看右面找后果
- 看全局找保护
- 评估风险
- 接受现有风险或增加保护（强化保护）

HAZOP的目的

HAZ（危险）：分析隐藏在流程中， 由于工艺参数偏离，没有得到有效纠正的剧情事故场景，评估事故风险是否可以接受。接受剧情事故风险或降低剧情事故风险。兼顾部分非剧情事故。

OP（可操作性）：兼顾生产，包括质量、产量、稳定性、开车、停车、临时停车、取样、维修、排料、置换、吹扫等。

- 非过程安全事故分析：高空坠落、触电、机械伤害等。
- 非剧情事故：工艺参数没有偏离，但由于设计、 安装、制造、维护错误造成物料外漏，但兼顾重大非剧情事故发生后的切断隔离。

详细偏离	原因	后果	保护措施	建议措施
湿气储气柜TXXX高压	湿气储气柜TXXX浮盘上升过程中卡住	压力高导致水封破坏，含硫化氢沼气会从水封溢出，有人员中毒和火灾爆炸危险		#15.10 沼气进湿气储气柜TXXX前增加水封，水封排气管接至安全处

详细偏差	原因	后果	保护措施	建议措施
湿气储气柜低压	湿气储气柜TXXX浮盘下降过程中卡住	造成气柜内负压，气柜水封破坏，空气会进入气柜，空气和沼气混合物会送入RTO和发电厂作为燃料气，造成RTO和发电厂炉膛爆炸		#15.3 在增压风机CXXX入口增加氧分析仪，并设置氧含量高报
				#15.4 在增压风机CXXX入口增加压力变送器，低低压力时，停风机，且关闭增压风机入口阀

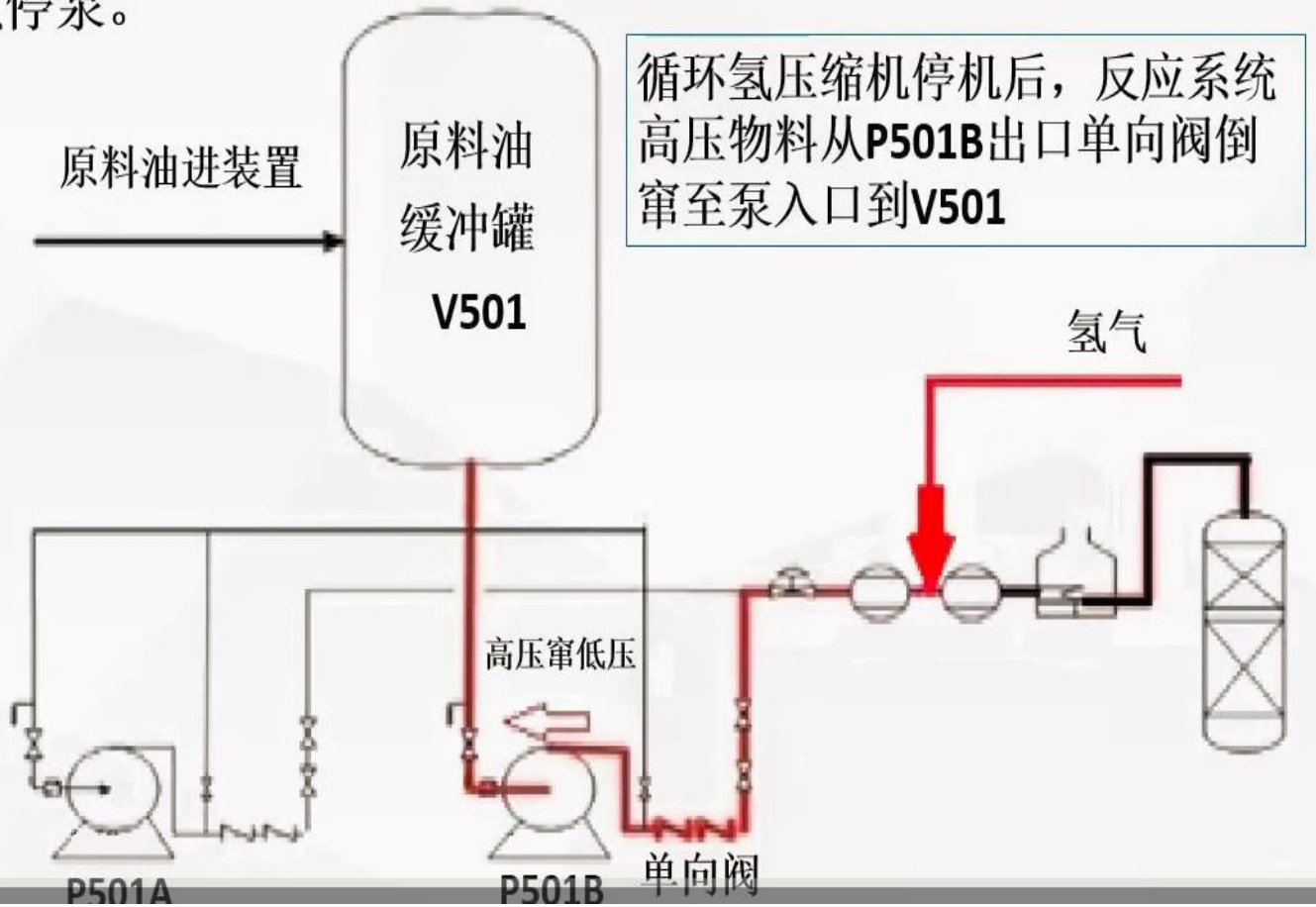
02 LOPA分析

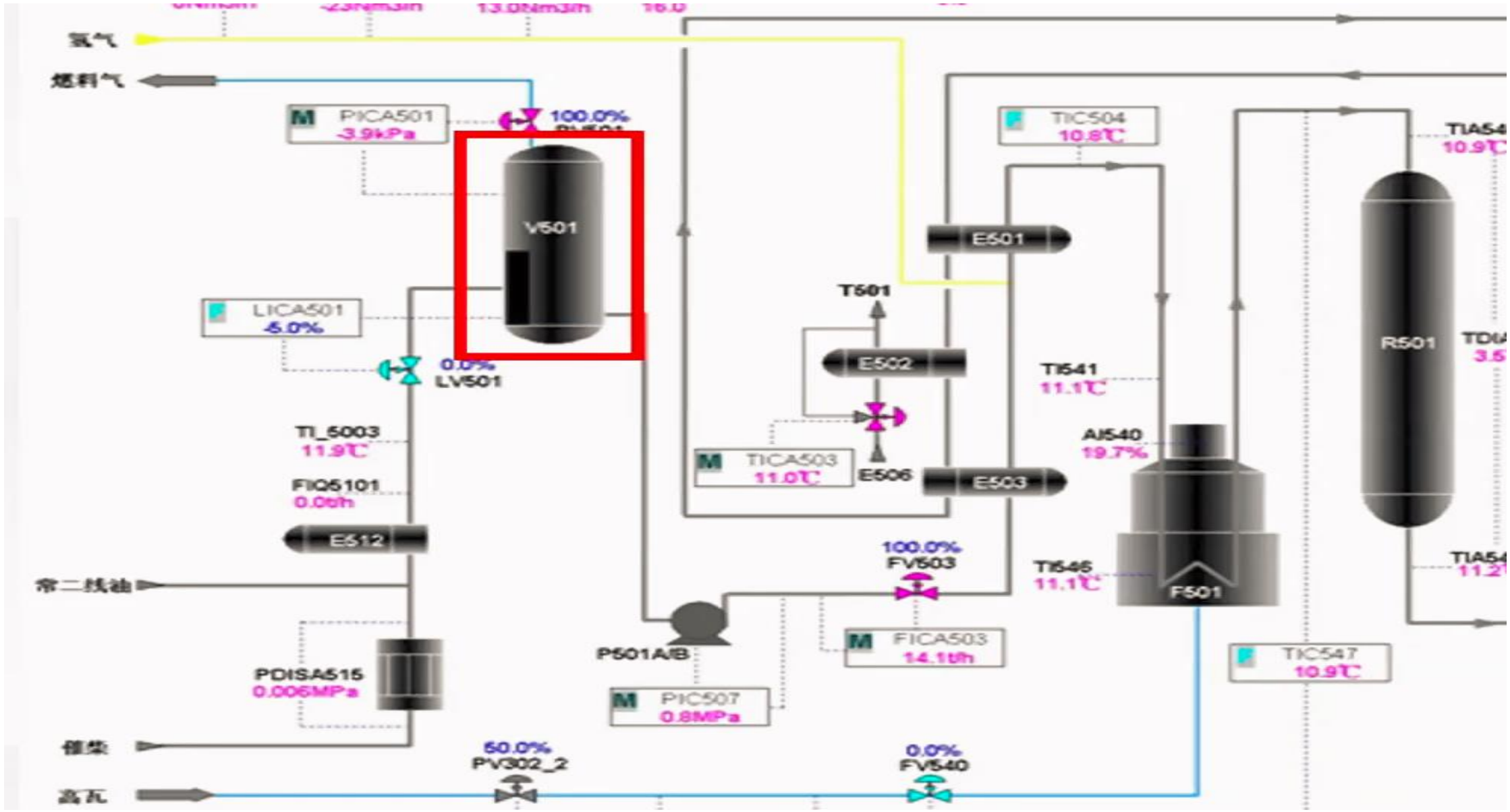
- HAZOP分析是定性分析，无法确定保护层的有效性
- 无法确定现有保护是否把风险降低到可以接受的程度
- 无法确定增加的建议，能否把当前风险降低到可接受程度

事故直接原因

循环氢压缩机C502B润滑油系统压力波动过程中，操作人员处置不当，导致循环氢压缩机C502B异常停机，加氢进料泵P501B联锁停泵。

P501B联锁停泵后的处置过程中，因出口阀门未及时关闭，且与P501B关联的两台单向阀失效，系统内的高压氢气通过停止运行的P501B反窜入V501，导致V501发生超压撕裂，并引发爆炸和火灾。



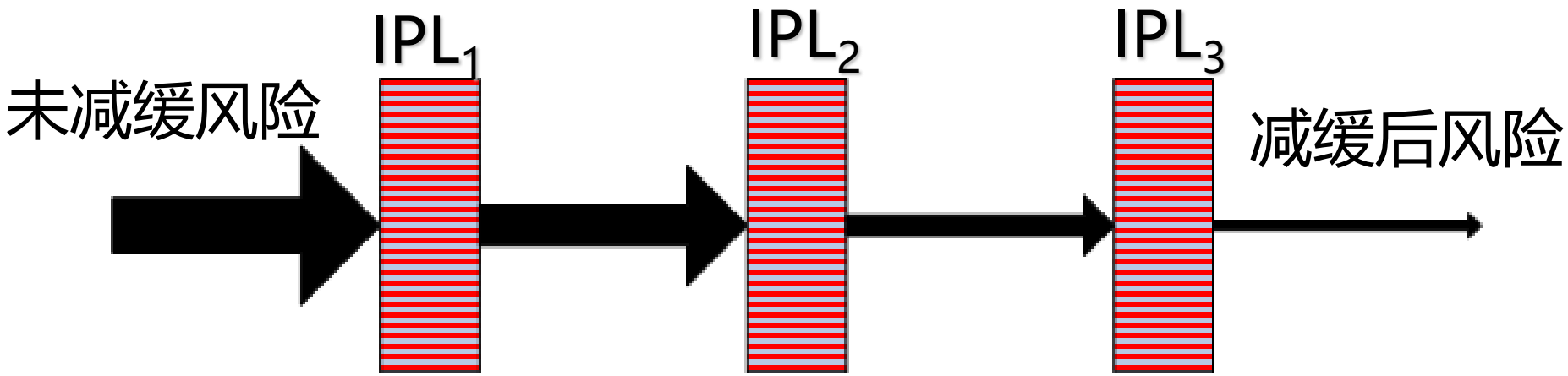

氢气
燃料气
PICA501
-3.9kPa
100.0%
V501
LICA501
6.0%
0.0%
LV501
TI_5003
11.9℃
FIQ5101
0.0t/h
E512
常二线油
PDISA515
0.006MPa
催柴
50.0%
PV302_2
高瓦
P501A/B
PIC507
0.8MPa
TIC504
10.8℃
E501
T501
E502
TICA503
11.0℃
E506
E503
100.0%
FV503
FICA503
14.1t/h
TI541
11.1℃
AI540
19.7%
TI546
11.1℃
F501
R501
TIC547
10.9℃
0.0%
FV540

假如本身无故障时，能够百分之百阻止特定的事故场景向后发展的一种设备、系统或行动， 独立于初始事件和其他独立防护层，且本身具有特定的失效概率（通常小于0.1）。

IPL 主要特性：有效性、独立性、可核查

表 E.3　化工行业典型 IPL 的 PFD

IPL		说明 （假设具有完善的设计基础、充足的检测和维护程序、良好的培训）	PFD
本质安全设计		如果正确执行，将大大地降低相关场景后果的频率	$1\times10^{-1}\sim1\times10^{-6}$
BPCS		如果与 IE 无关，BPCS 可作为一种 IPL	$1\times10^{-1}\sim1\times10^{-2}$
关键报警和人员响应	人员行动，有 10 min 的响应时间	行动应具有单一性和可操作性	$1.0\sim1\times10^{-1}$
	人员对 BPCS 指示或报警的响应，有 40 min 的响应时间		1×10^{-1}
	人员行动，有 40 min 的响应时间		$1\times10^{-1}\sim1\times10^{-2}$
安全仪表功能	安全仪表功能 SIL 1	见 GB/T 21109	$\geqslant1\times10^{-2}\sim<1\times10^{-1}$
	安全仪表功能 SIL 2		$\geqslant1\times10^{-3}\sim<1\times10^{-2}$
	安全仪表功能 SIL 3		$\geqslant1\times10^{-4}\sim<1\times10^{-3}$
物理保护	安全阀	此类系统有效性对服役的条件比较敏感	$1\times10^{-1}\sim1\times10^{-5}$
	爆破片		$1\times10^{-1}\sim1\times10^{-5}$
	防火堤	降低由于储罐溢流、断裂、泄漏等造成严重后果的频率	$1\times10^{-2}\sim1\times10^{-3}$

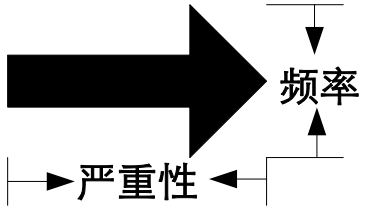


注：

箭头宽度代表后果频率大小，

长度代表后果严重性

IPL—独立保护层



$$f_i^C = f_i^I \times \prod_{j=1}^{J} PFD_{ij} = f_i^I \times PFD_{i1} \times PFD_{i2} \times \cdots \times PFD_{ij}$$

式中：

f_i^C——初始事件i的后果C的发生频率，单位为 /a；

f_i^I——初始事件i的发生频率，单位为 /a；

PFD_{ij}——初始事件i中第j个阻止后果C发生的IPL的PFD。

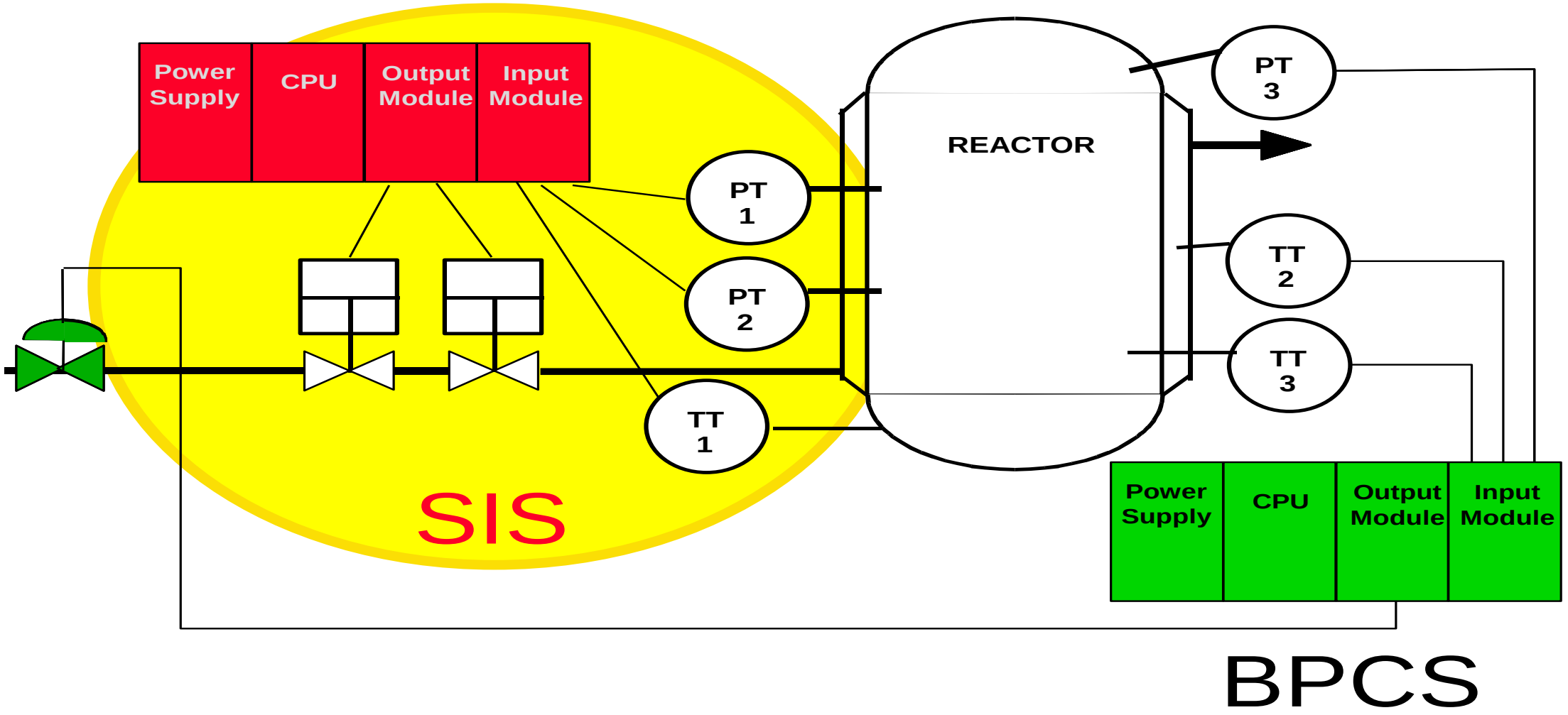
1.区别非独立保护层和独立保护层，防止以保护的数量来判断风险是否降低。

2.计算单一事故场景发生频率， 减少人为的判断。

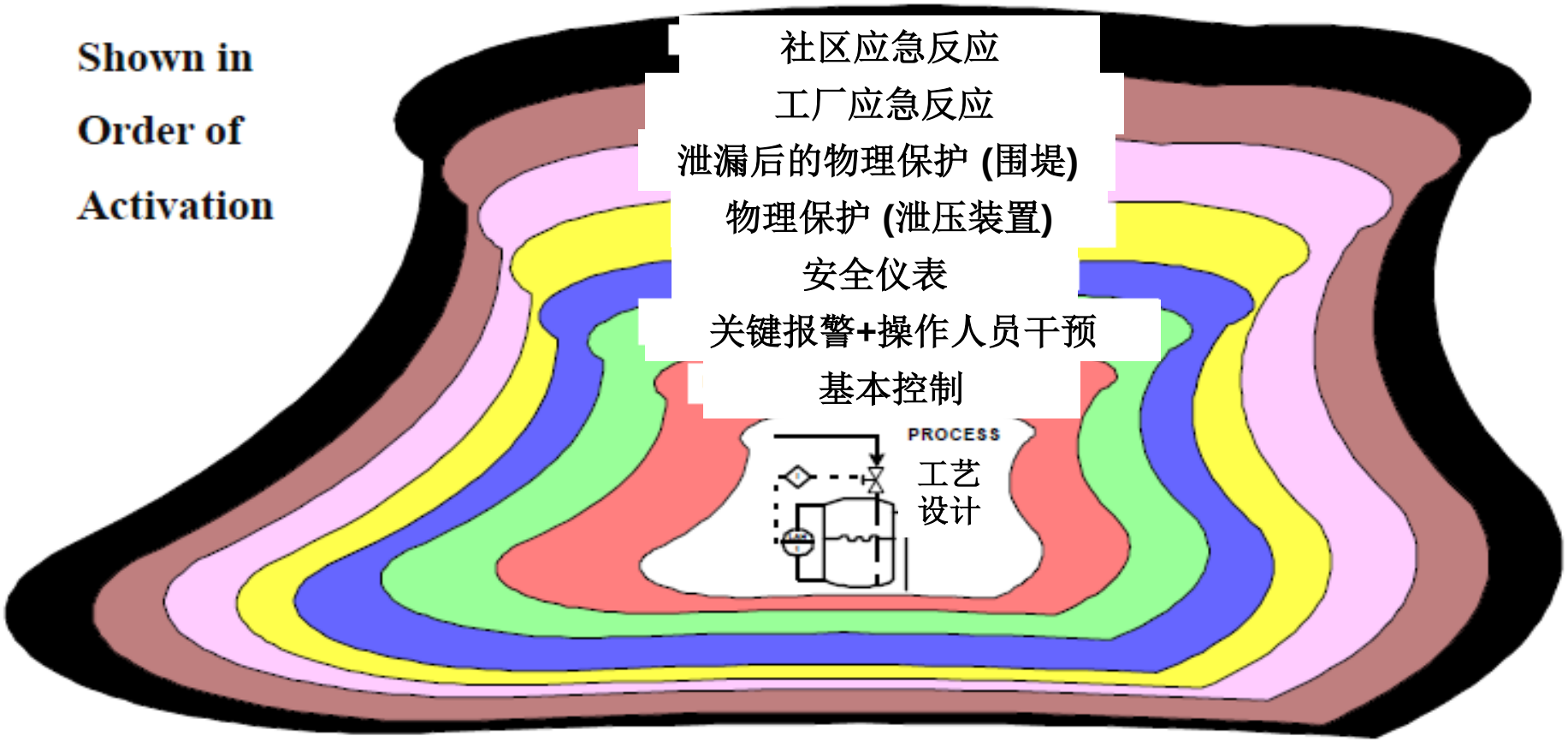
后果	初始事件描述	初始事件发生频率（次/年）	IPL1 描述	PFD1	IPL2描述	PFD2	IPL3描述	PFD3	条件修正描述	条件修正概率	事故发生频率(次/年)
5.7MPa氢气倒窜回0.35MPa低压柴油罐,导致低压柴油罐超压爆炸，造成2人死亡，1人受伤	循环氢压缩机停机	0.1	NA (虽然有两个止回阀，但15年没有检测，止回阀不算IPL)	1	NA	1	NA	1	在爆炸时,人员出现在爆区	1	E-01

03 SIL评估

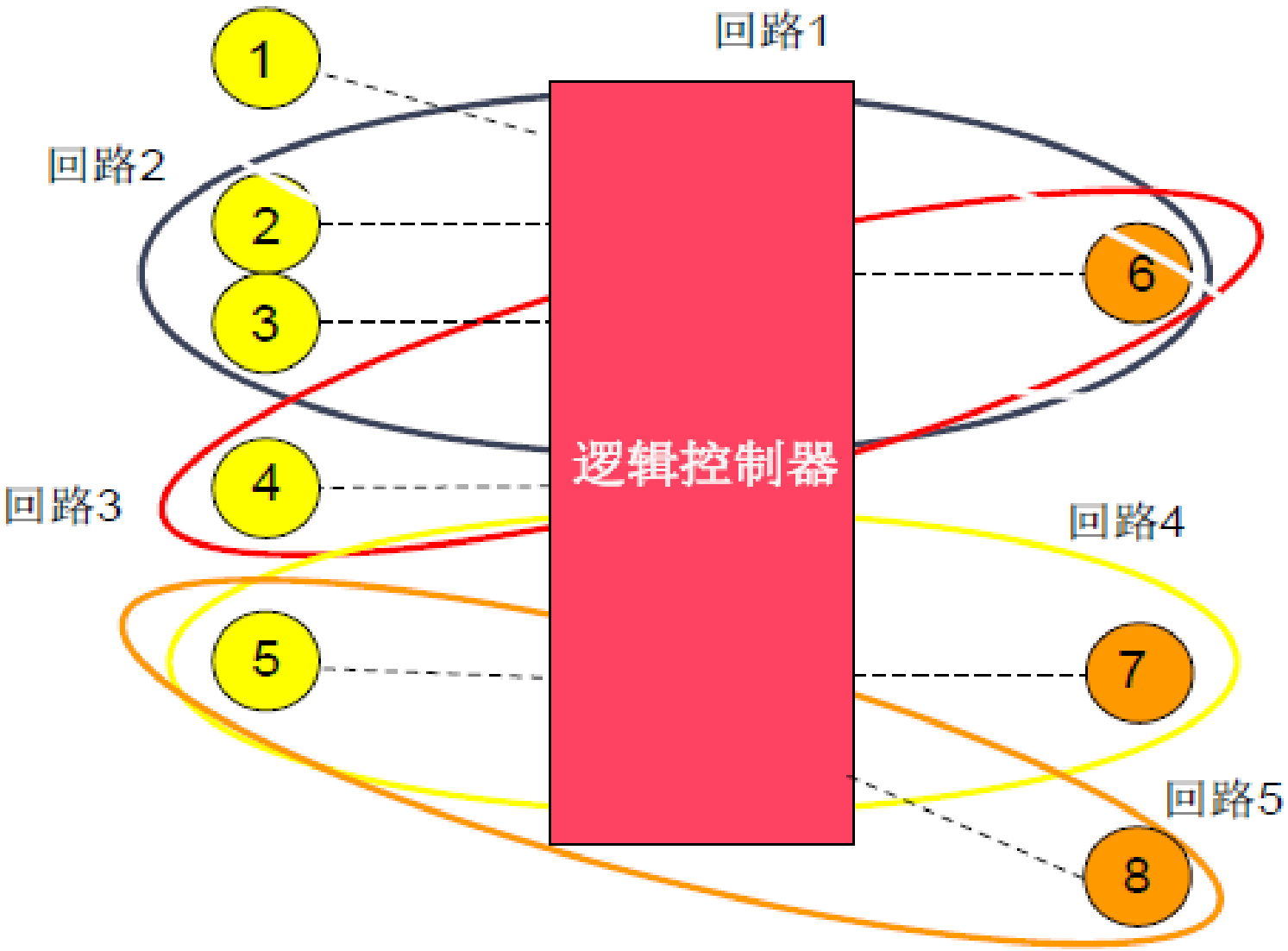
SIS与BPCS的区别



SIS与其他保护的区别



SIF-安全仪表功能



- 多个联锁回路构成SIS;
- 一个联锁回路中， 执行安全功能的回路为SIF, 且具有一定安全完整性等级(SIL)

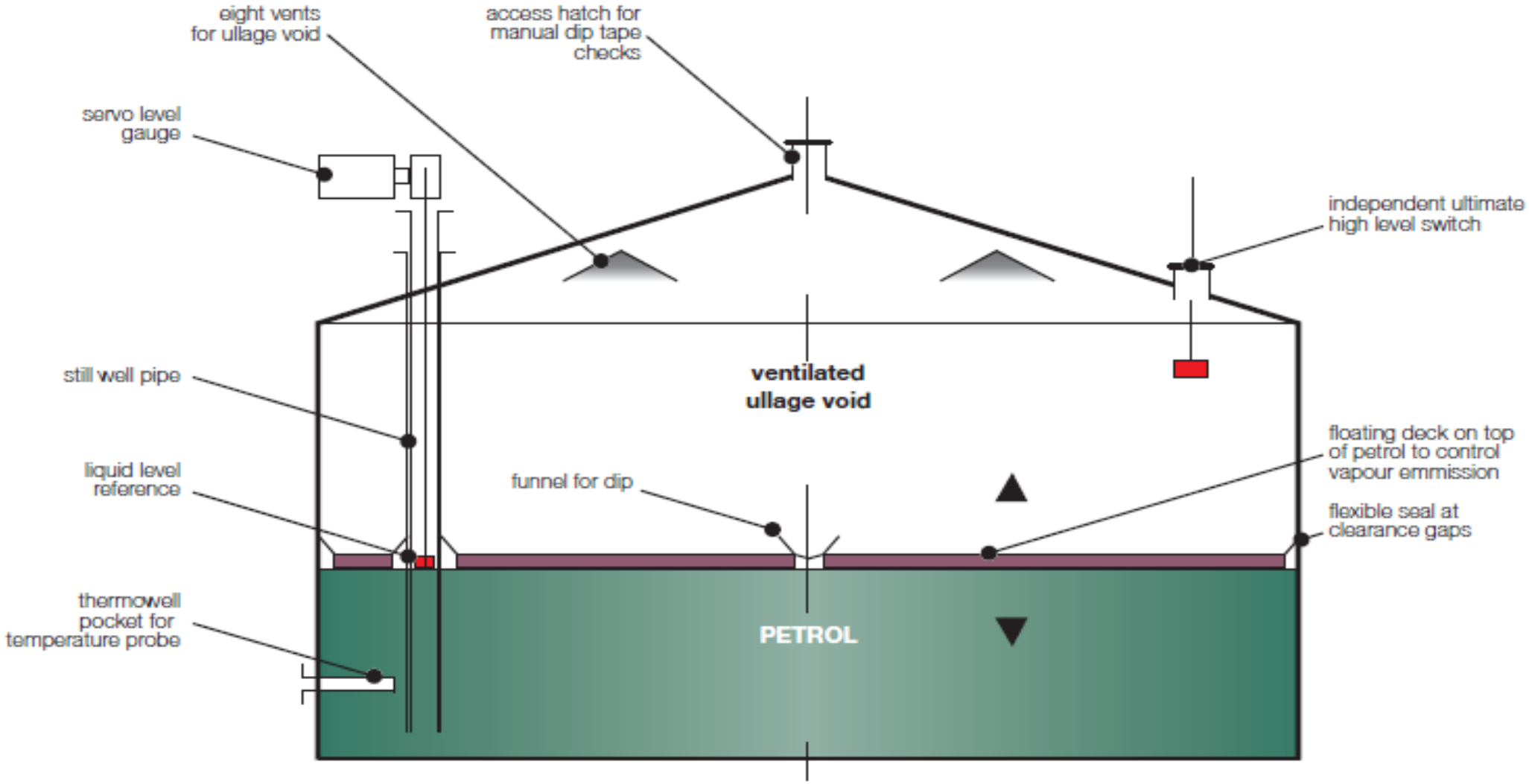
- 低要求要求操作模式

安全完整性等级 SIL	平均要求时失效概率 PFDavg	风险降低因子 RRF
4	≥ 10^{-5} to < 10^{-4}	> 10000 to ≤ 100000
3	≥ 10^{-4} to < 10^{-3}	> 1000 to ≤ 10000
2	≥ 10^{-3} to < 10^{-2}	> 100 to ≤ 1000
1	≥ 10^{-2} to < 10^{-1}	>10 to ≤ 100

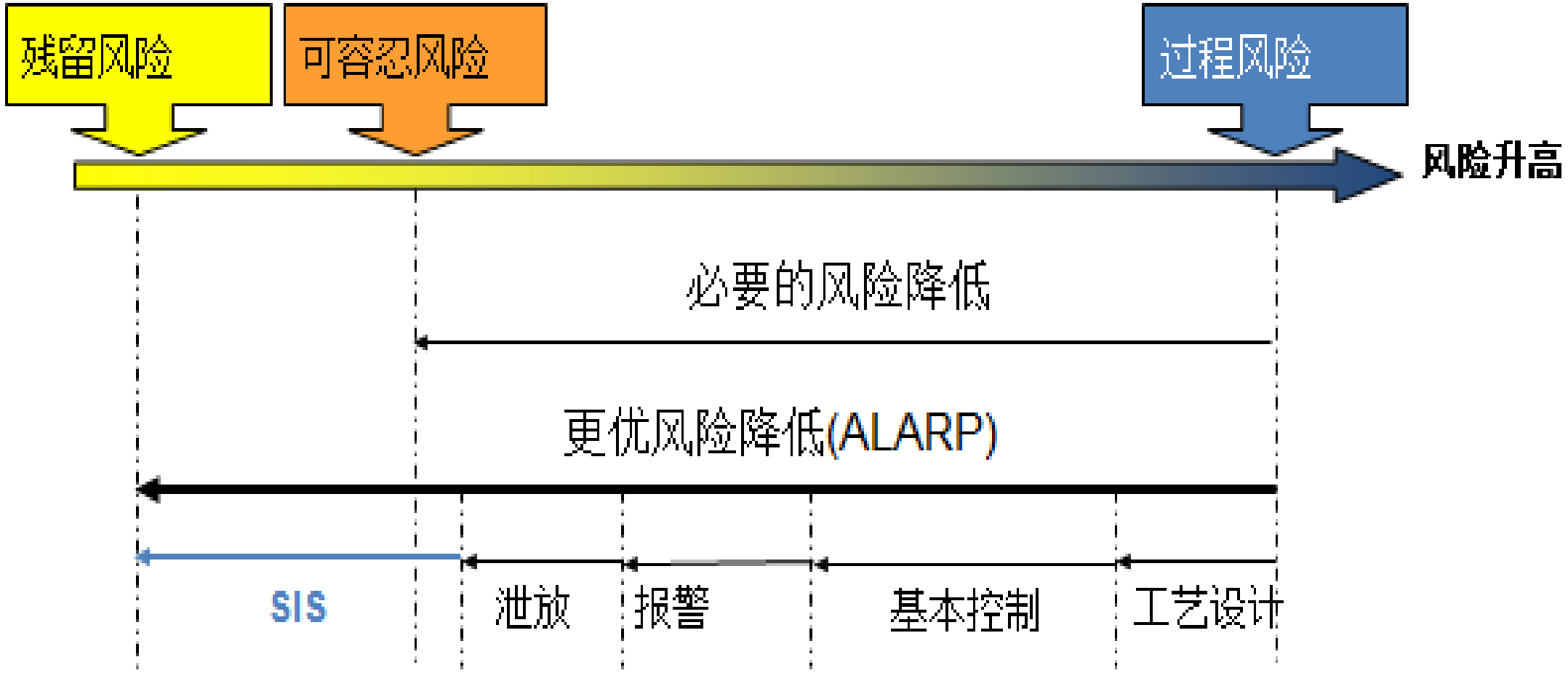
技术要求：

1.DCS/PLC 不能实现SIL1等级以上的联锁。

2. DCS 不能对同一场景提供超过2个独立保护层的保护。


eight vents
for ullage void
access hatch for
manual dip tape
checks
servo level
gauge
independent ultimate
high level switch
still well pipe
ventilated
ullage void
floating deck on top
of petrol to control
vapour emmission
liquid level
reference
funnel for dip
flexible seal at
clearance gaps
thermowell
pocket for
temperature probe
PETROL

如何降低风险

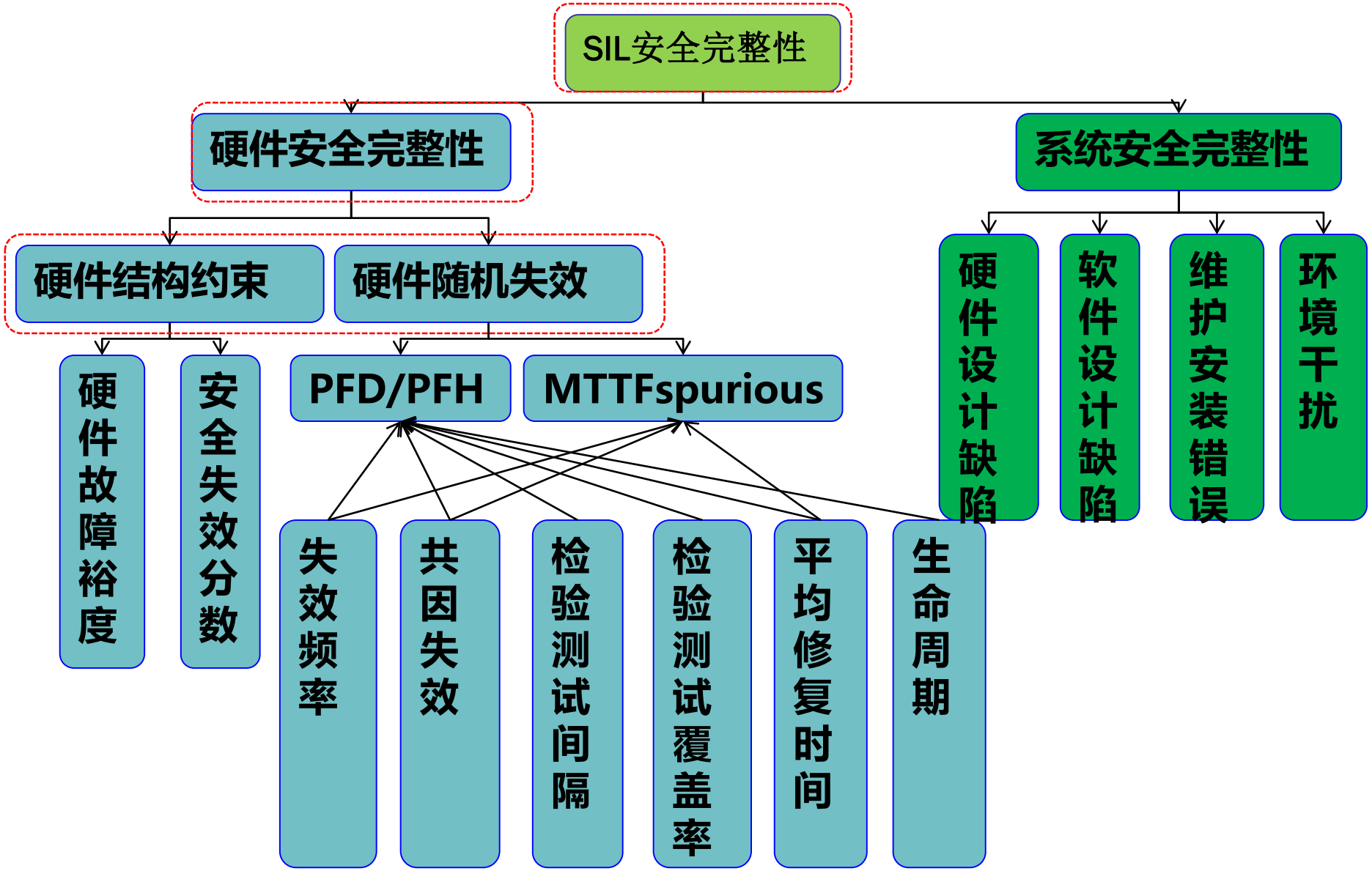

残留风险
可容忍风险
过程风险
风险升高
必要的风险降低
更优风险降低(ALARP)
SIS
泄放
报警
基本控制
工艺设计

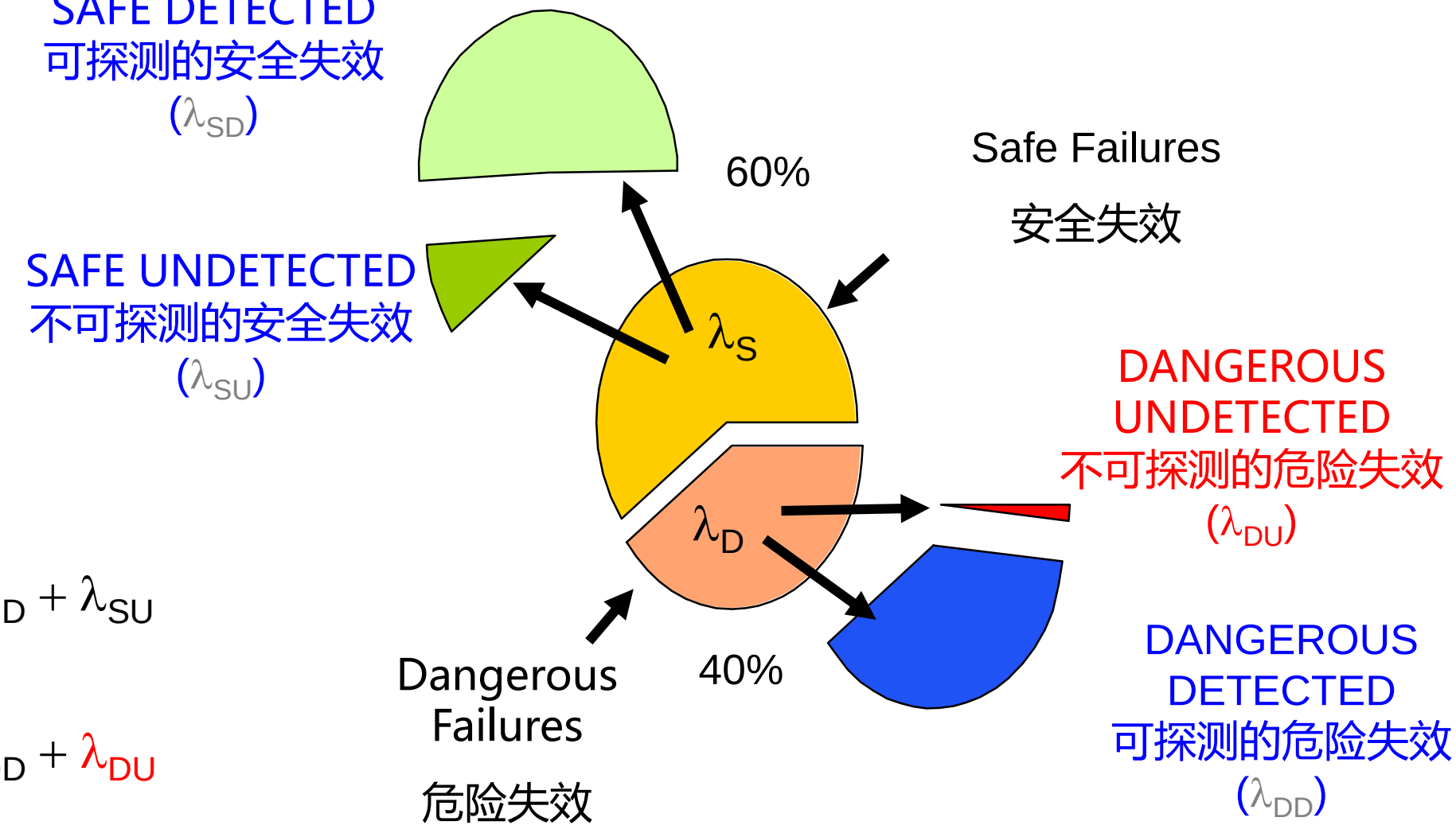
后果	初始事件描述	初始事件发生频率（次/年）	IPL1 描述	PFD1	IPL2描述	PFD2	IPL3描述	PFD3	条件修正描述	条件修正概率	事故发生频率(次/年
5.7MPA氢气倒窜回0.35MPA 低压柴油罐,导致低压柴油罐超压爆炸，导致2人死完，一人受伤	循环氢压缩机停机	0.1	差压信号通过SIS 关闭出口紧急切断和流量控制阀和流量控制阀, 选SIL3 回路	E-03	两个不同形式的止回阀,定期检测	0.1	NA	1	在爆炸时,人员出现在爆区	1	E-05

SIL 定级作用

- 确定现有的安全联锁回路是否进入SIS 系统
- 对于进入SIS 的联锁回路， 根据SIL等级以及对应的PFD，设计院进行仪表选型

- SIL验算时间：在设计院完成SIF设计后，仪表采购前，进行SIL等级验算，验算结束后，才能进行采购
- SIL验算：确定一个SIF回路是否达到SIL定级时的SIL级别
- SIL验算人员：由专业的安全仪表功能工程师负责


SIL安全完整性
硬件安全完整性
系统安全完整性
硬件结构约束
硬件随机失效
硬件故障裕度
安全失效分数
PFD/PFH
MTTFspurious
硬件设计缺陷
软件设计缺陷
维护安装错误
环境干扰
失效频率
共因失效
检验测试间隔
检验测试覆盖率
平均修复时间
生命周期



$$\lambda_S = \lambda_{SD} + \lambda_{SU}$$

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

Certificate / Certificat
Zertifikat / 合格証

ABB 1704100 C001

exida hereby confirms that the:

Symphony+ SPC700 System

ABB Inc.
Wickliffe, Ohio - USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 1 (SIL 1 Capable)

Random Capability: Type B Element

PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:
The Symphony+ SPC700 system will perform the configured safety logic and execute the automatic diagnostics in the specified time period.

IEC 61508 Failure Rates in FIT*

Application/Device/Configuration	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	#	SFF
644 Single T/C mode	0	0	362	39	136	90.3%
644 Dual T/C mode	0	0	371	39	140	90.5%
644 Single RTD mode	0	0	317	30	133	91.4%
644 Dual RTD mode (3-wire RTD)	0	0	330	31	135	91.4%

* FIT = 1 failure / 10^9 hours

查找SIF回路中包含的传感器（包括引压和变送）、安全栅、浪涌保护器、逻辑控制器、执行部分及执行继电器等器件相关的型号、规格，根据国际上可信的数据库确定各器件检测到的危险失效率（λDD）、未检测到的危险失效率（λDU）、检测到的安全失效率（λSD）以及未检测到的安全失效率（λSU）。

1OO1：$PFD_G = (\lambda_{DU} + \lambda_{DD})t_{CE}$ ……其中：$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}(\frac{T_1}{2} + \mathrm{MRT}) + \frac{\lambda_{DD}}{\lambda_D}\mathrm{MTTR}$

1OO2：$PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE}\, t_{GE} + \beta_D\lambda_{DD}\mathrm{MTTR} + \beta\lambda_{DU}(\frac{T_1}{2} + \mathrm{MRT})$

……其中：$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}(\frac{T_1}{3} + \mathrm{MRT}) + \frac{\lambda_{DD}}{\lambda_D}\mathrm{MTTR}$

2OO2：$PFD_G = 2\lambda_D t_{CE}$

1OO3：$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE}\, t_{GE}\, t_{G2E} + \beta_D\lambda_{DD}\mathrm{MTTR} + \beta\lambda_{DU}(\frac{T_1}{2} + \mathrm{MRT})$

……其中：$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}(\frac{T_1}{4} + \mathrm{MRT}) + \frac{\lambda_{DD}}{\lambda_D}\mathrm{MTTR}$

2OO3：$PFD_G = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE}\, t_{GE} + \beta_D\lambda_{DD}\mathrm{MTTR} + \beta\lambda_{DU}(\frac{T_1}{2} + \mathrm{MRT})$

2OO4：$PFD_G = 24((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE}\, t_{GE}\, t_{G2E} + \beta_D\lambda_{DD}\mathrm{MTTR} + \beta\lambda_{DU}(\frac{T_1}{2} + \mathrm{MRT})$

根据IEC 61508，IEC 61511（功能安全标准），为了弥补系统失效，以及随机失效率数据的准确性，应对不同SIL等级的SIF回路在结构上进行约束。约束分为逻辑计算部分的约束和非逻辑计算部分的约束。

- A型和B型相关子系统的结构约束将会依照如下所示的 IEC61508-2 中的表2和表3，并且SIL验证将会受限于安全失效分数（SFF）和硬件故障裕度（HFT）。
- 事实上对于逻辑处理器，硬件故障裕度的要求在 IEC61511 中有规定，这与 IEC61508 是一致的。IEC61511 通常在SIL验证中被采用，除非在IEC61508中， 通过传感器外部比较或阀的部分行程测试（Partial Valve Stroke Testing ）来获得一个高的SFF（Safety Failure fraction），以得到一个低的HFT (Hardware Fault Tolerance)。

Type A：”非复杂”元件			
SFF	依据IEC61508的HFT值		
	0	1	2
<60%	SIL1	SIL2	SIL3
60% to 90%	SIL2	SIL3	SIL4
90% to 99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4

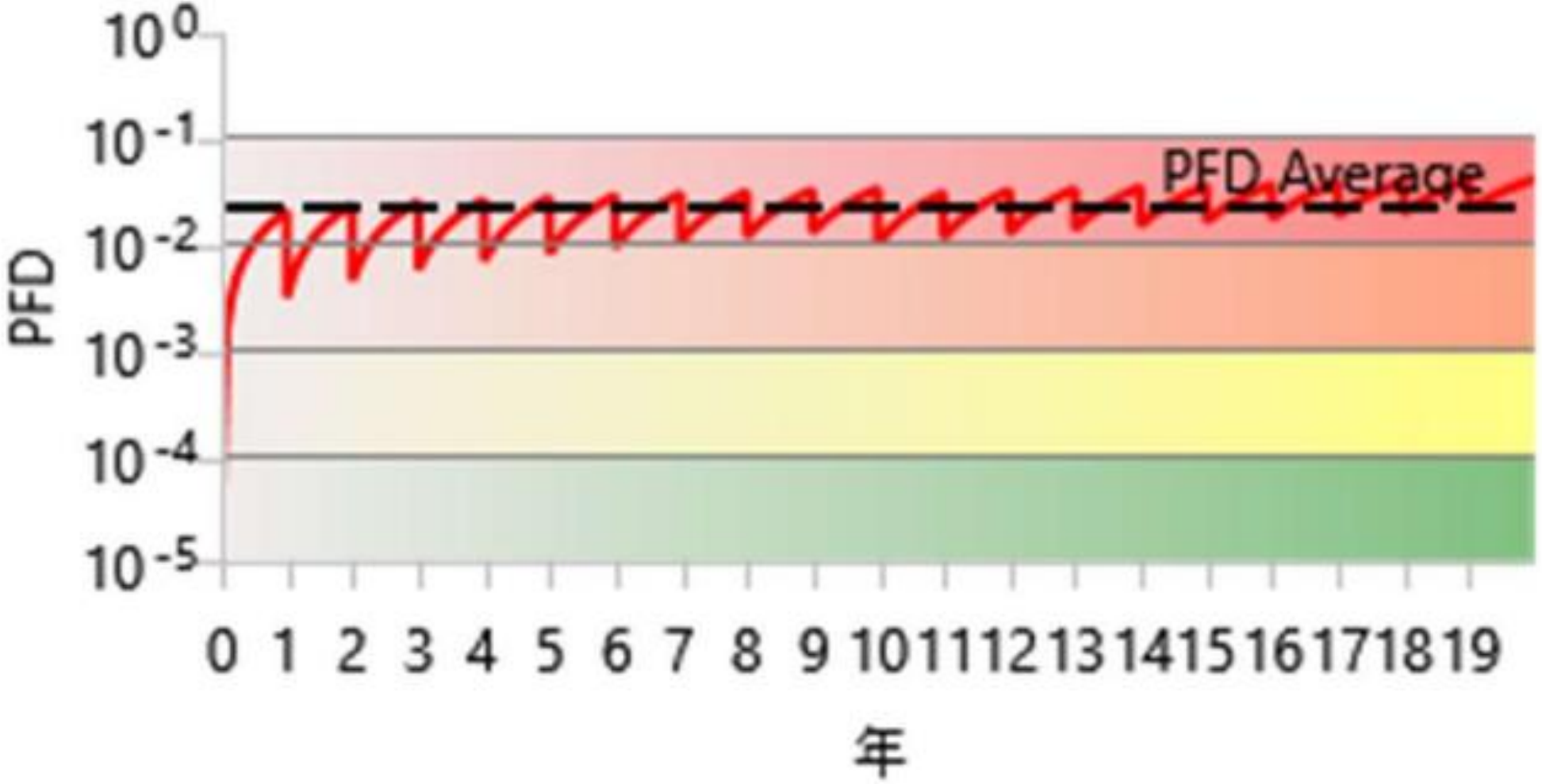
Type B：”复杂”元件			
SFF	依据IEC61508的HFT值		
	0	1	2
<60%	Not allowed	SIL1	SIL2
60% to 90%	SIL1	SIL2	SIL3
90% to 99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

SIL验算样例（结果）

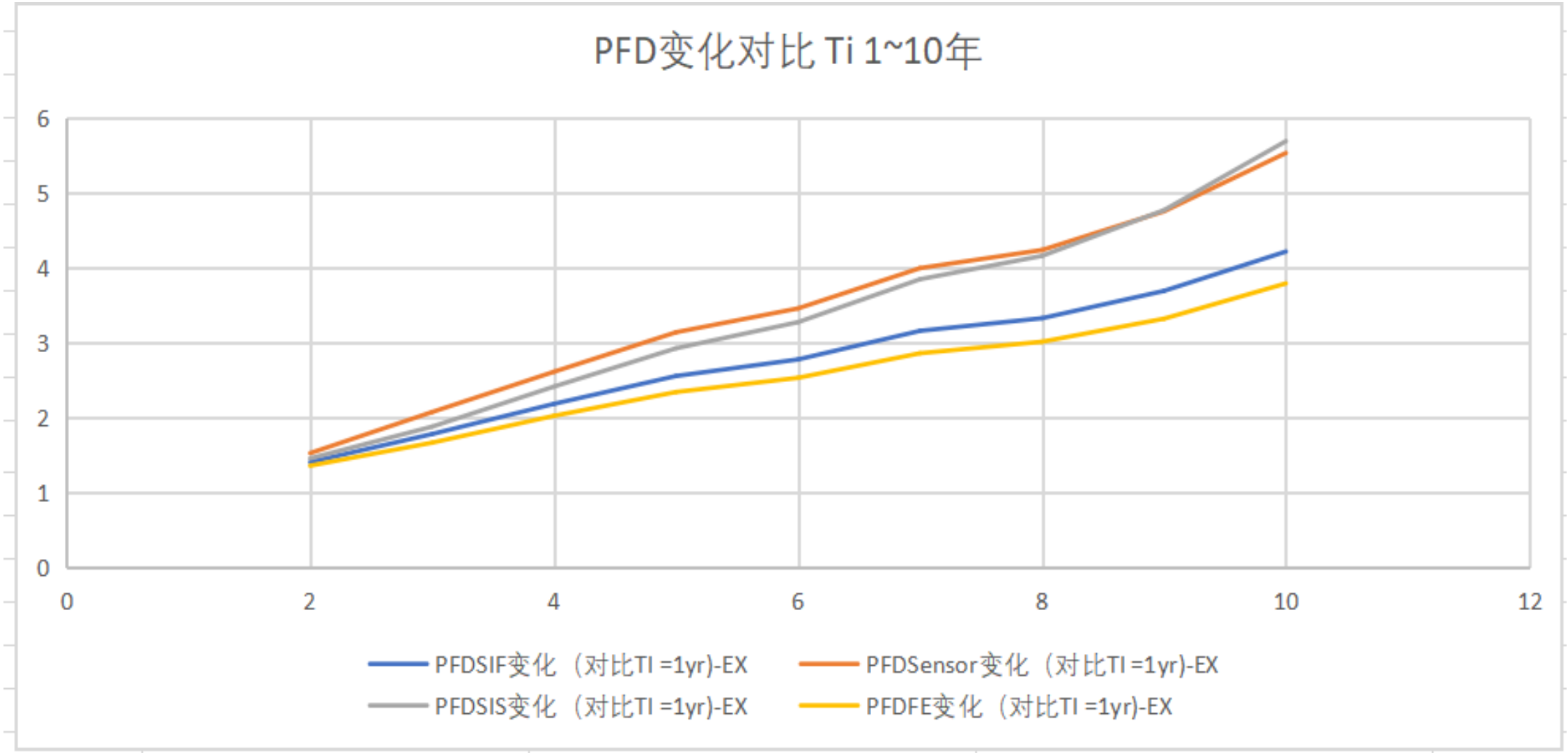
SIF验算结果汇总					
Target SIL		SILA	Achieved SIL		1
PFDavg	7.08E-3	RRF	141.53	MTTFS (years)	22.41
SIL(PFDavg)	2	SIL(AC)	1	SIL(SC)	2

	PFDavg	MTTFS	SIL		
			PFDAvg	AC	SC
Sensor	4.39E-4	520.99	3	3	3
Logic Solver	1.77E-3	24.66	2	2	2
Final Element	4.86E-3	462.56	2	1	3

回路测试周期对PFD的影响（定性）



回路测试周期对PFD的影响（软件模拟）



1. HAZOP 作用：识别异常工况下，是否有足够的保护措施。

2. LOPA: 计算单一事故场景发生的可能性，判断是否有足够的保护层。

3. SIL 定级：计算SIF 回路要求时的失效概率，以及SIL 等级。

4. SIL 验算：计算实际SIF回路是否达到要求的SIL 级别。

谢 谢！

直播回看、课件下载请上“中化协安全技能培训平台”
网址：https://ccsa.yunkeonline.cn/course/explore/5