

中国化学品安全协会

“化危为安”线上讲堂



化工企业报警和联锁管理

孙彦东 18826213299

珠海安彦企业管理咨询有限公司



前言

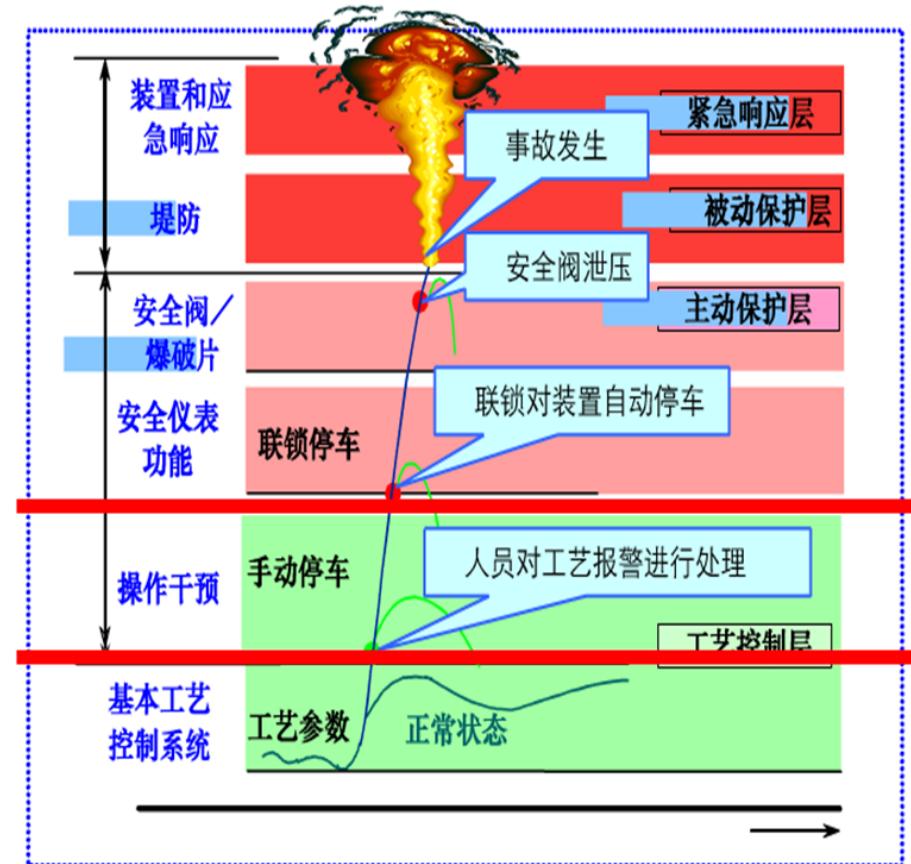
安彦咨询

随着化工等行业进入规模化生产，装置越来越连续化、大型化，工艺过程越来越复杂，具有高温、高压、易燃易爆、有毒等特点，造成重大工艺安全事故的可能性也随之增大。

如何及时发现工艺设备的**异常工况**，并进行有效的处置是预防重大工艺安全事故发生的前提，保护现场工作人员和环境安全，以及减少由于生产事故造成的经济损失越来越成为安全生产所关注的重点。

有效的**报警和联锁管理**作为落实工艺安全防线的重要措施，在提高企业应对工艺过程异常和紧急工况有效处置时起着越来越重要的作用。

“化危为安” 线上讲堂





课程目标

“化危为安” 线上讲堂

安彦咨询

1. 了解国内外报警和联锁管理规范、标准和最佳实践，规范企业报警和联锁系统全生命周期管理；
2. 指导企业人员系统科学地开展本企业报警和联锁系统管理改进和优化工作，包括建立完善本企业的报警/联锁管理规范，以及报警/联锁管理工作规划和有效实施改进；
3. 了解如何结合风险分析技术科学规划设计报警和联锁系统的管理要点，提高报警和联锁系统的本质安全和可靠性；
4. 改善在役装置报警和联锁系统管理绩效，提高对工艺和设备等异常工况情况的反应和处置能力，避免报警泛滥和联锁失效导致发生重大安全事故。



安彦咨询

“化危为安” 线上讲堂

目录

CONTENTS

- 01 报警和报警管理定义
- 02 报警管理标准和规范
- 03 报警全生命周期管理
- 04 联锁和联锁管理定义
- 05 联锁全生命周期管理
- 06 基于6西格玛的报警联锁管理改进



安彦咨询

“化危为安” 线上讲堂



报警和报警管理定义



北美大停电事故

安彦咨询

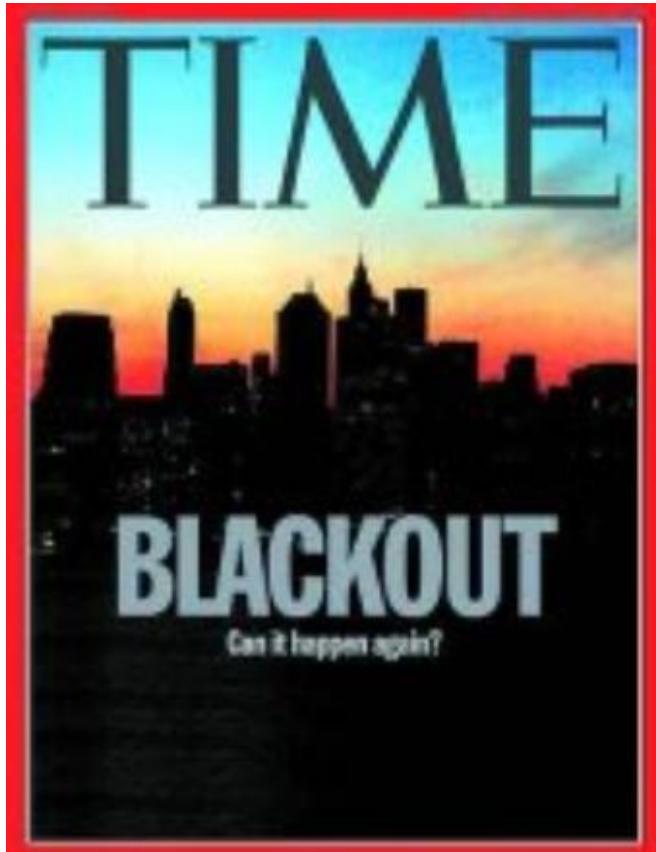
2003年8月14日下午4时10分到15日晚，美国发生了历史上最大规模的停电：从美国的纽约、克利夫兰、底特律，到加拿大的多伦多等各大城市瘫痪了近30个小时，影响到美国的纽约等7个州和加拿大安大略省。

世界上电气化程度最高地区的5000万人，过了30个小时没有电的生活，大停电给美国造成的经济损失高达300亿美元。

事故直接原因：

报警泛滥导致提醒工程技术人员电网故障的**报警系统失灵**。

“化危为安” 线上讲堂



事故教训：

报警系统可靠性不足，关键工艺设备故障异常报警未被工程技术人员准确识别和响应。



报警管理的意义

“化危为安” 线上讲堂

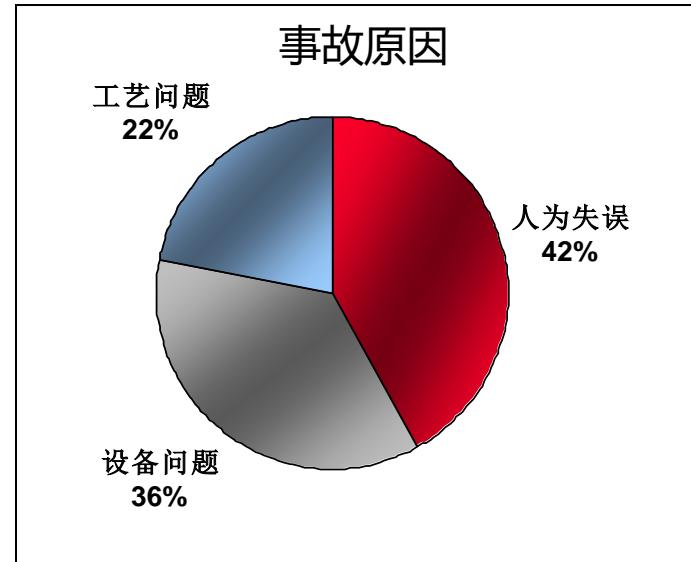
安彦咨询

提高企业对异常工况的发现和处置能力，避免重大和灾难事故发生

不正常状态（工艺过程紊乱）造成的损失

根据异常工况管理协会ASM统计

1. 每年造成约200亿美元损失 *
2. 生产损失，如产品不合格、产量损失、设备损坏造成工厂产值损失 3 - 8 %
3. 造成损害人身健康和人身安全的严重后果
4. 环境污染



* 异常工况管理协会Abnormal Situation Management Consortium



《国家安全监管总局关于加强化工安全仪表系统管理的指导意见》安监总管三[2014]116号

9、加强过程**报警管理**，制定企业报警管理制度并严格执行。与安全仪表功能安全完整性要求相关的报警可以参照安全仪表功能进行管理和检验测试。

《国家安全监管总局关于加强化工过程安全管理的指导意见》安监总管三（2013）88号

六、试生产安全管理

联动试车安全管理。联动试车应具备下列条件：所有操作人员考核合格并已取得上岗资格；公用工程系统已稳定运行；试车方案和相关操作规程、经审查批准的仪表**报警**和**联锁值**已整定完毕。

二十三、严格变更管理

工艺技术变更。主要包括生产能力，原辅材料(包括助剂、添加剂、催化剂等)和介质（包括成分比例的变化），工艺路线、流程及操作条件，工艺操作规程或操作方法，工艺控制参数，仪表控制系统(包括安全**报警**和**联锁**整定值的改变)，水、电、汽、风等公用工程方面的改变等。



报警和报警管理的定义

“化危为安”线上讲堂

安彦咨询 报警

是一条诊断的、预测的或知道的声光信息，用来提醒操作人员设备故障、过程偏离、或者需要进行特定响应的异常状态，操作人员需要响应以保证系统正确运行，报警可用于提醒控制室操作人员需立即采取对应行动。

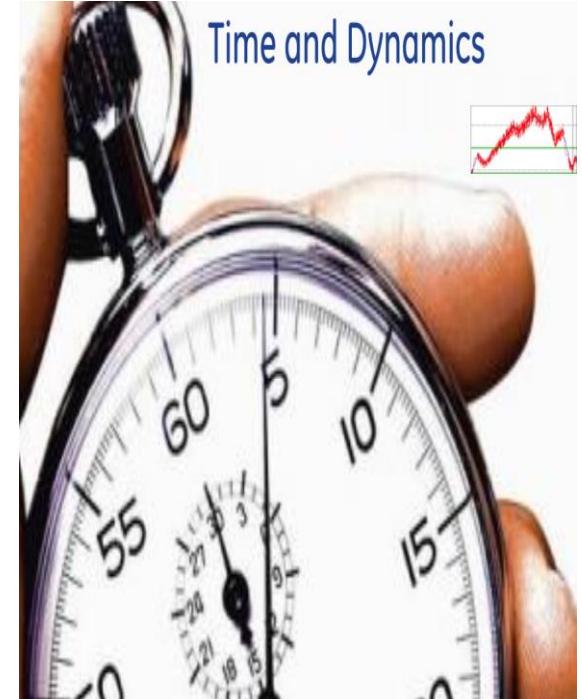
报警管理

确定、设计、运行、监控、记录及维护报警系统的过程和实践。
报警管理必须持续进行以保证报警系统的有效性并进行周期性的实施审核来指出持续改进的机会。

报警类型

工艺报警、安全报警、维护报警、系统报警、提示性报警

报警=行动



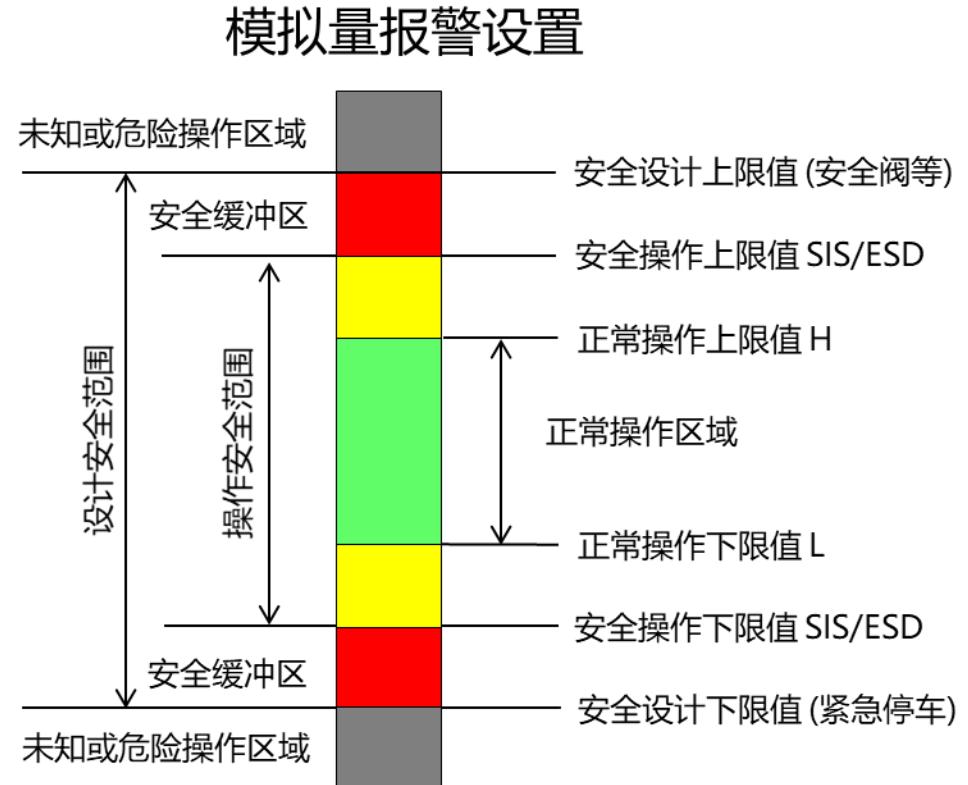


报警的设置

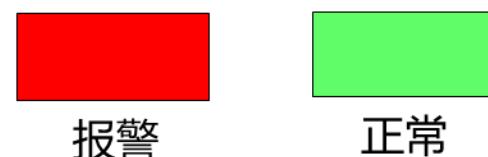
“化危为安” 线上讲堂

安彦咨询 工艺报警设置范例

模式	含义
Normal 正常	过程参数的值在正常的工作范围内。（介于高和低限值之间），参数运行在安全和稳定的操作范围内，不会给操作者发送警告消息。
Abnormal 异常	过程参数的值已经超过了一个需要注意的限值。非正常的低限（TAL）或高限值（TAH）。 表示参数已经和正常运行值有了较小的偏差，因此要求操作员注意一些设备相关的操作参数
Critical 紧急	过程参数已经超过了危险的极限值。高限值（TCH）或低限值(TCL)。 表示参数已经和正常运行值有了较大的偏差，强烈要求操作员对相关的设备执行正确的操作，以消除危险的警报。
Shut-down 停车	过程参数值已经超出了停车限值，TSL或TSH极限值。 参数值已经严重偏离了正常运行范围而，就要接近停车的条件了。操作者被强烈要求根据设备指定的操作参数采取一系列的正确操作



开关量报警设置





企业报警系统面临的问题

“化危为安” 线上讲堂

安彦咨询

1. 过多的报警
2. 无效报警
3. 报警阈值设置不当
4. 滋扰报警 (Nuisance Alarms)
5. 驻留报警 (Standing Alarms)
6. 陈旧报警 (Stale Alarms)
7. 报警泛滥 (Alarm Floods)
8. 无预案报警
9. 报警优先级设置不对
10. 随意屏蔽和变更报警

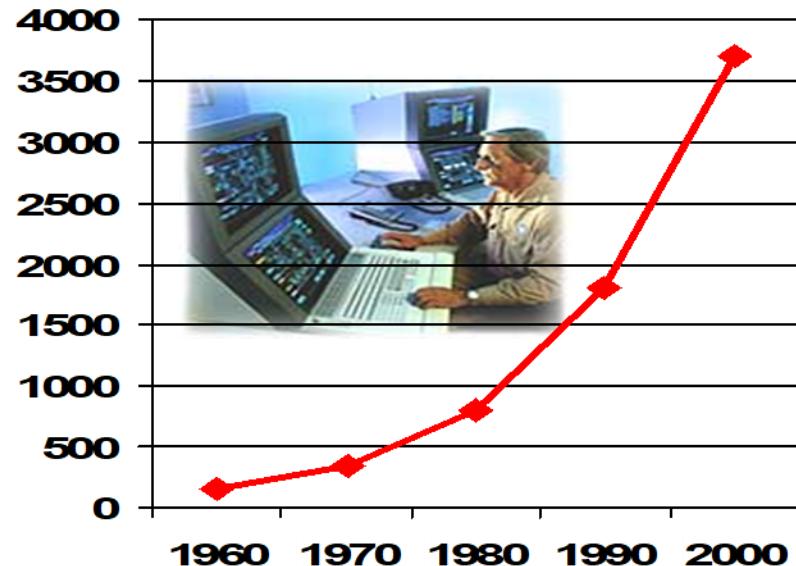




安彦咨询

一. DCS等控制系统廉价普遍应用带来的报警问题：数量急剧增加

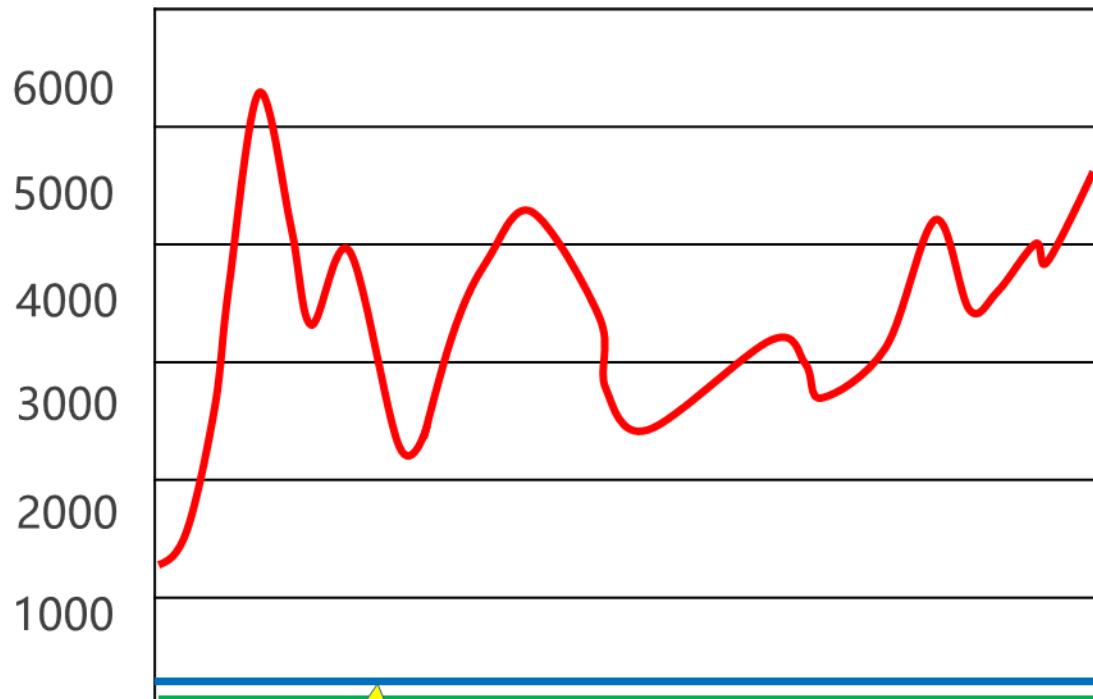
组态的每个操作员处理的报警个数



操作员不可能评估成千上万个报警事件!

哪些报警是安全的、操作员可以不管?

记录的报警
最多可处置的报警数量 (300)
可接受的报警数量 (150)



操作员处置能力



报警管理不善现象

“化危为安” 线上讲堂

安彦咨询

一、DCS等控制系统廉价普遍应用带来的报警问题：数量急剧增加

工艺过程波动异常时的报警泛滥，大量溢出的报警占据控制系统报警汇总画面，造成操作员手足无措，无法及时发现关键工艺设备异常状态，给安全生产造成极大的威胁！



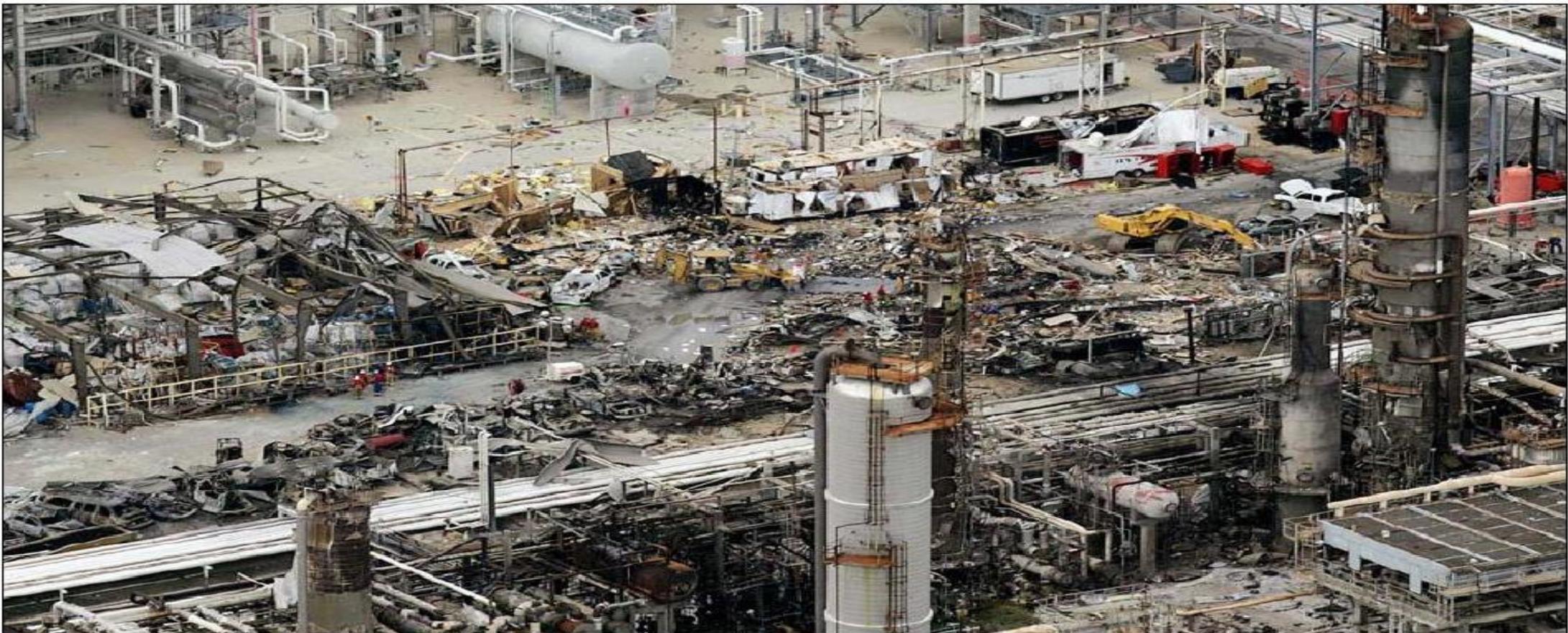


工业事故案例

“化危为安” 线上讲堂

安彦咨询

2005年3月23日，BP石油公司在美国德克萨斯的一家炼油厂发生爆炸事故，美国OSHA调查认为报警管理不善是造成事故的一个主要原因，在爆炸发生前一小时内，操作台上的报警数量有130多个，操作员无法发现关键异常工况并及时响应。



2005年BP德克萨斯炼厂爆炸事故-15人死亡，170伤



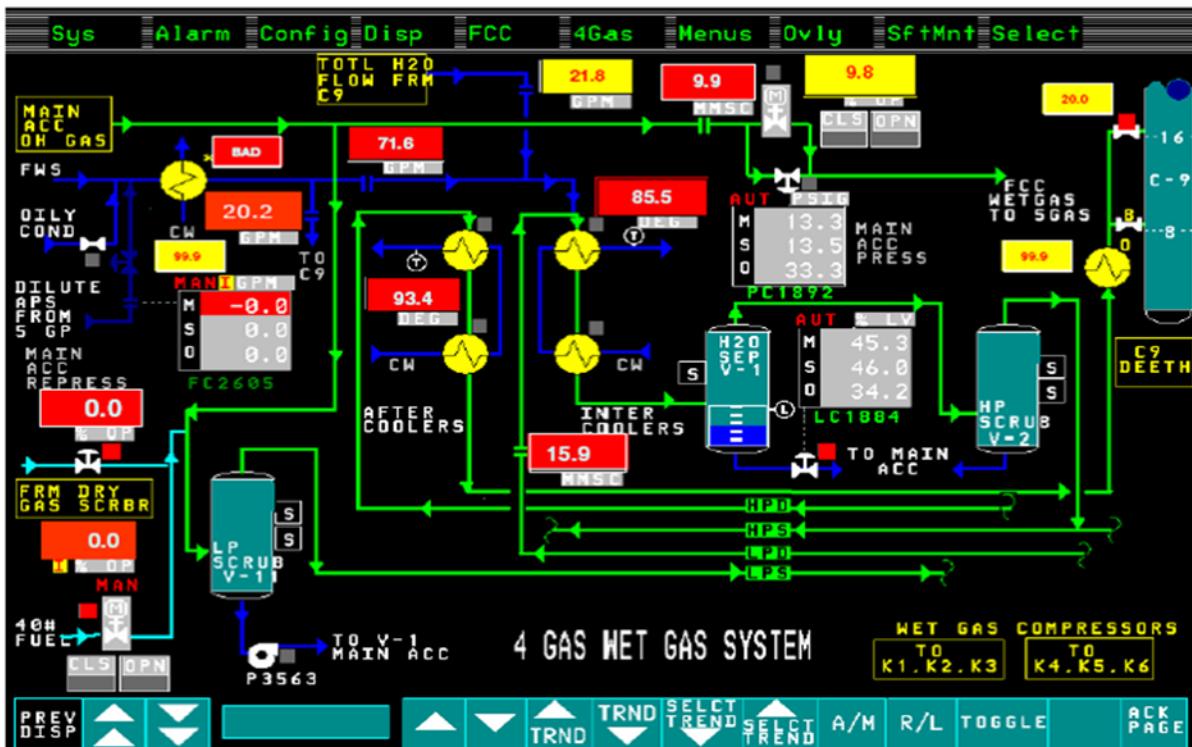
报警管理不善现象

“化危为安” 线上讲堂

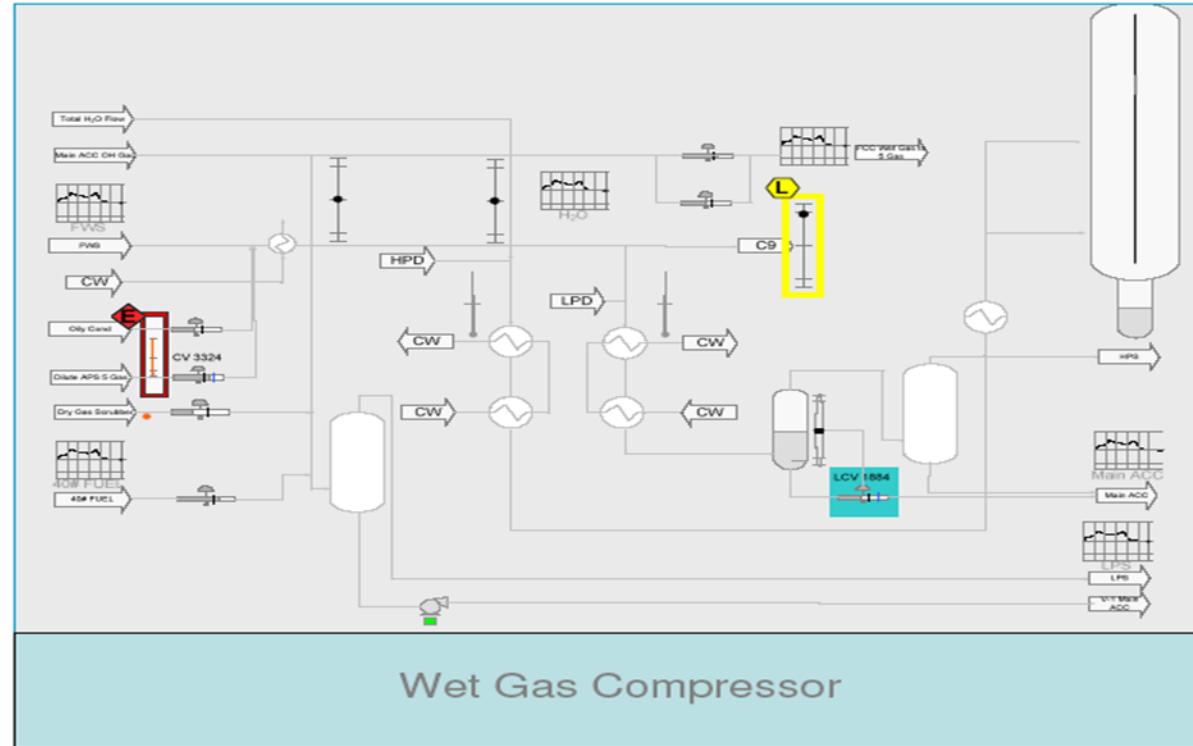
安彦咨询

二、DCS等控制系统人机界面复杂、不清晰，无法给操作员提供快速和正确的指引，及时发现和处置各类工艺设备异常工况。

不良的报警界面设计



良好的报警界面设计





安彦咨询

1. 企业对报警系统缺乏系统和规范的全生命周期管理

为什么我们的控制系统先进了，而工艺过程却不稳定了，什么地方出了毛病？

模量控制盘

1. 单个的、固定的、相互邻近的控制盘
2. 可以全览整个工艺过程
3. 工艺过程紊乱的早期模式识别
4. 直接、快速地用控制器进行控制
5. 一个控制盘有50到150个报警



CRT控制台

1. 4-6 屏幕、50-100个显示画面
2. “显示内情的” 工艺过程画面
3. 过程紊乱事件识别
4. 通过多次键击才能访问控制器
5. 一个控制台有2,000到4,000个报警





安彦咨询

“化危为安” 线上讲堂



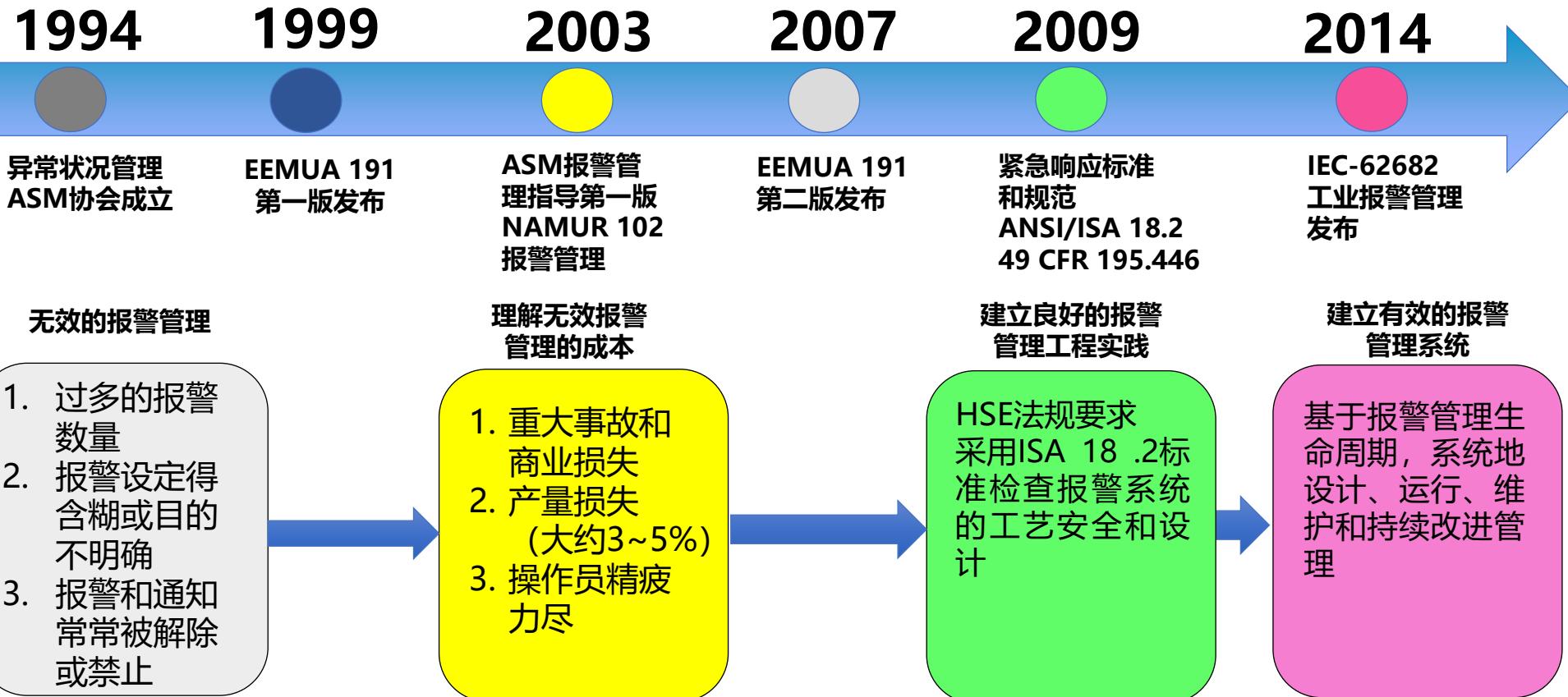
报警管理标准和规范



报警管理标准和规范

“化危为安” 线上讲堂

安彦咨询



EEMUA = Engineered Equipment and Materials Users Association
工程设备和材料用户协会

ASM = Abnormal Situation Management Consortium
异常工况管理协会





报警管理标准和规范

“化危为安” 线上讲堂

安彦咨询

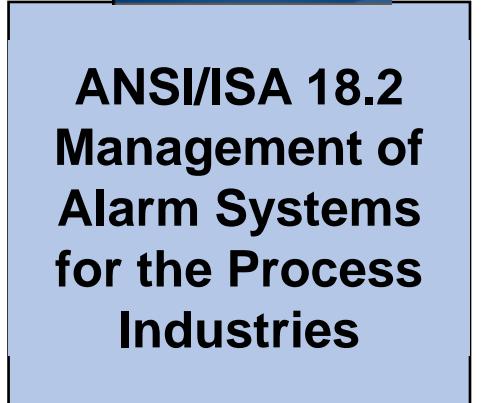
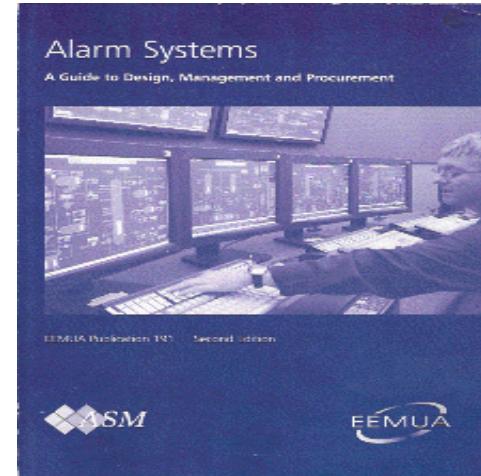
EEMUA-191 《报警系统-设计、管理和采购导则》 - 2013

ANSI/ISA-18.2 《过程工业报警系统管理》 -2016

IEC 62682 《过程工业报警系统管理》 -2014

通用核心管理要求：

1. 生产人员专注于最重要的报警
2. 根据需要抑制没有意义的报警
3. 根据清楚、简洁和全面的报警和指引信息了解当前生产状况
4. 准确获得关于生产状况可能的原因以及建议的纠正措施
5. 评估系统和操作人员的行为和绩效



ANSI- American National Standards Institute
美国国家标准协会

ISA – US Instruments, Systems Association
美国仪器、系统和自动化协会



安彦咨询 各行业报警统计与EEMUA和ISA报警管理绩效KPI指标

KPI指标	石油 天然气	石油 化工	发电	其他	EEMUA 标准	ISA 标准
平均每天报警数	1200	1500	2000	900	150-300	150-300
平均驻留报警数	50	100	65	35	<10	<5
每10分钟内报警峰值	220	180	350	180	<=10	<=10
平均每10分钟报警数	6	9	8	5	1-2	1-2
报警级别分布比例 (百分比 低/中/高)	25/40/35		25/40/35		80/15/5	80/15/5

数据来源：Matrikon公司



安彦咨询

“化危为安” 线上讲堂



报警全生命周期管理



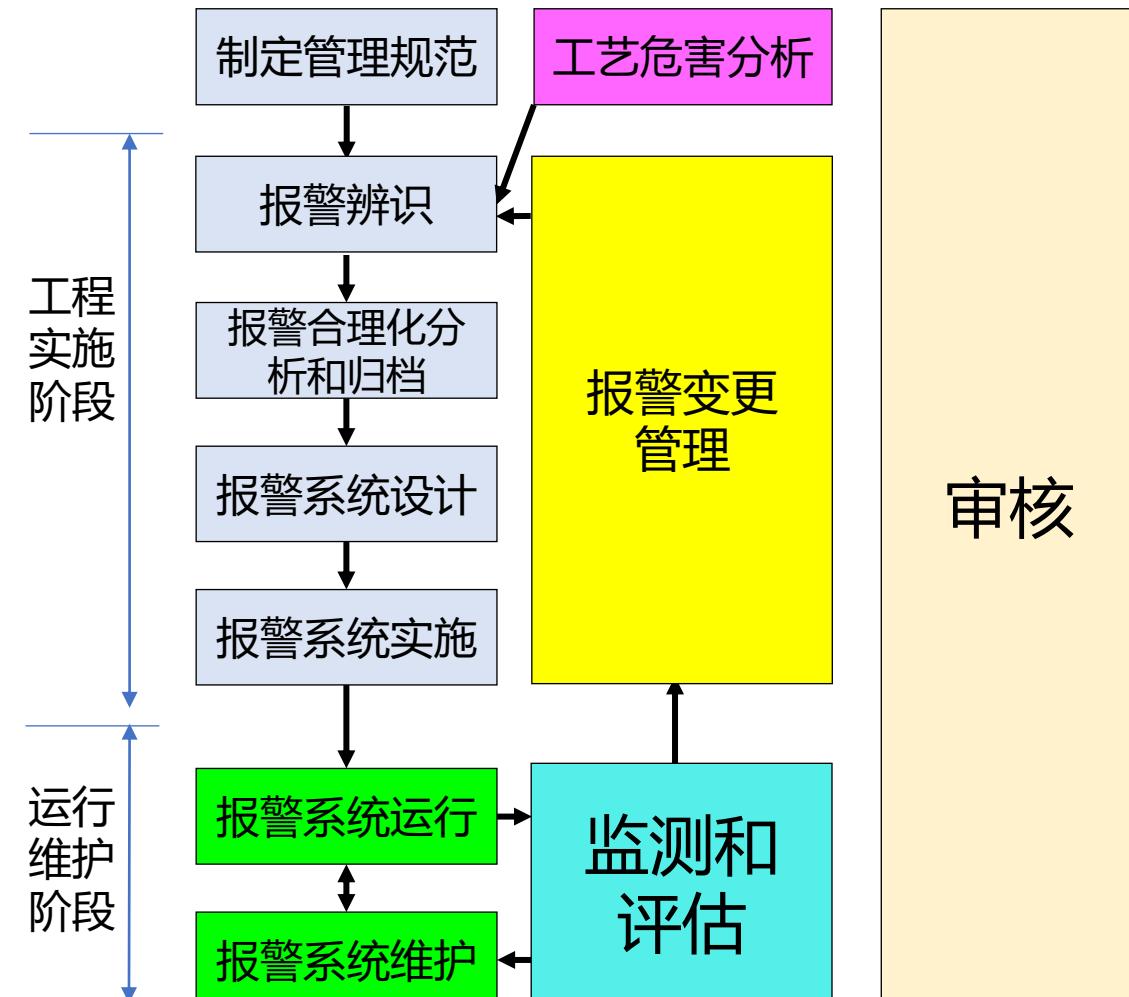
报警全生命周期管理

“化危为安” 线上讲堂

安彦咨询

根据ANSI/ISA18.2规范定义的报警管理生命周期活动包含10个步骤，包括：

1. 两个阶段：
 - ✓ 工程实施
 - ✓ 运行维护
2. 适用于新装置和在役装置报警管理与优化
3. 基于ASM和EEMUA标准
4. 包括解决报警设计、运行问题和持续改进的最佳实践





报警全生命周期管理要点

“化危为安” 线上讲堂

安彦咨询

报警管理规范主要内容

1. 报警管理职责
2. 设置报警系统的目的
3. 报警分级标准
4. 报警人机界面设计
5. 报警阈值设定原则
6. 报警日常管理
7. 报警绩效标准
8. 报警统计分析与改进
9. 报警屏蔽和变更管理
10. 报警绩效评估与考核

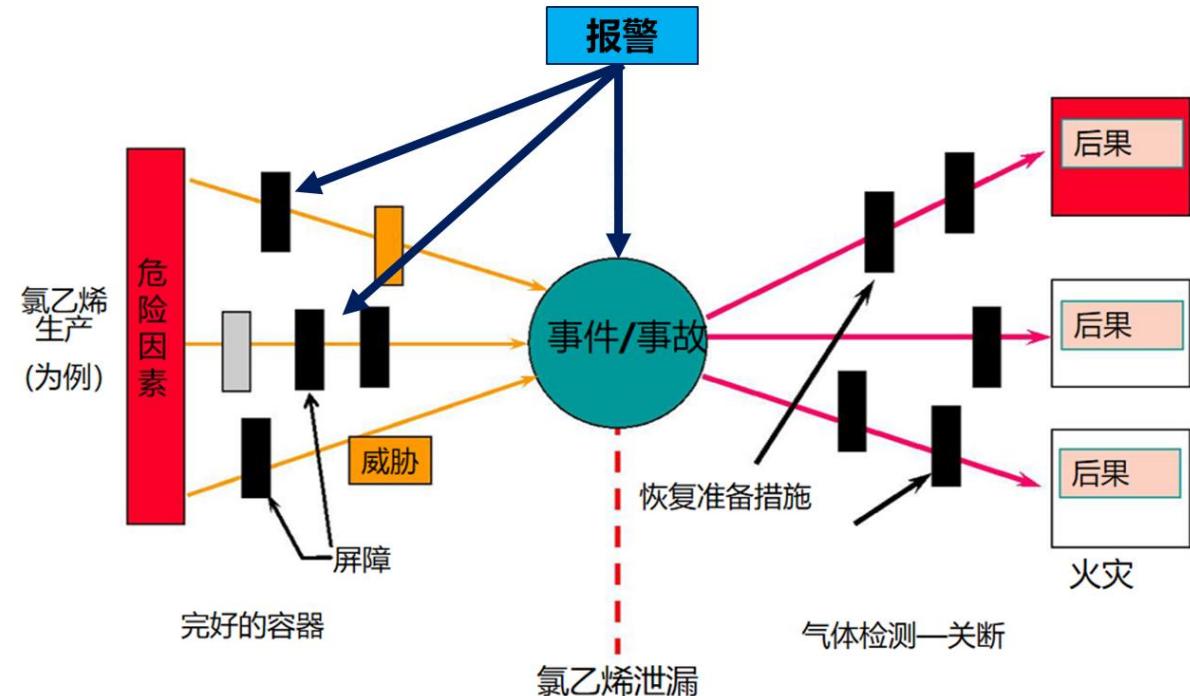




报警辨识

报警辨识是对可能设置的报警和报警变更进行定义的阶段，通过报警辨识确定要设置的报警作为报警归档和合理化分析的输入信息，报警设置识别途径：

1. 工艺设计数据
2. 工程标准规范安全控制要求
3. P&ID审核
4. **工艺危害PHA和LOPA分析报告**
5. 操作规程审核
6. 事故调查报告
7. 关键设备可靠性管理
8. 质量管理审核
9. 控制系统硬件完整性





通过HAZOP分析识别和完善报警功能

节点	偏差	原因	后果	可能 性	后 果 等 级	风 险 等 级	安全措施	可能 性	后 果等 级	风 险 等 级	建议措施
1.聚合 反应釜	反应釜 压力 PI200 过低	静密封 点泄漏	介质泄漏着 火，造成人员 伤亡	4	5	20	1. 可燃气体报警器 AI200A/B/C 2. PI200压力低报警及操作员响应 3. PSL200低低联锁 4.应急处置源	2	5	10	1.增加LI200 液位低报警， 以便及时发现 反应釜液位下 降
			内外冷管破裂 可能引起二次 伤害	3	5	15	1. 可燃气体报警器 AI200A/B/C 2. PI200压力低报警及操作员响应 3. PSL200低低联锁 5.应急处置源	1	5	5	



报警合理化分析和归档

报警归档和合理化分析是定义报警和报警优先级的主要方法：

1. 在报警辨识的基础上，对所有产生报警的位号点都应经合理化分析确定，在报警合理化分析过程中，所有控制系统的报警点都应逐个分析
2. 确定每个报警的类型、设定值、优先级和分类
3. 报警后的行动和不响应后果的分析
4. 可能需要对某些报警进行逻辑配置（状态报警）
5. 编制装置报警文档清单

TICA-100			
位号	反应器温度控制器		
PVHHTP	125	PVHHPR	EMERGENCY
PVHITP	105	PVHIPR	HIGH
PVLOTP	80	PVLOPR	LOW
PVLLTP	70	PVLLPR	HIGH
OPHITP	--	OPHIPR	--
OPLOTP	--	OPLOPR	--
		BADPVPR	HIGH
高报警原因	1. 助催化剂量加入过多，反应过于剧烈 2. 冷却水调节阀TV-100故障 3. 冷却水泵故障PP-100不上量		
处置措施	1. 降低助催化剂流量设定值FIC-109 2. 现场检查调节阀TV-100 3. 现场检查冷却水泵PP-100		

有效报警三个原则：**目的、响应、充足的时间**

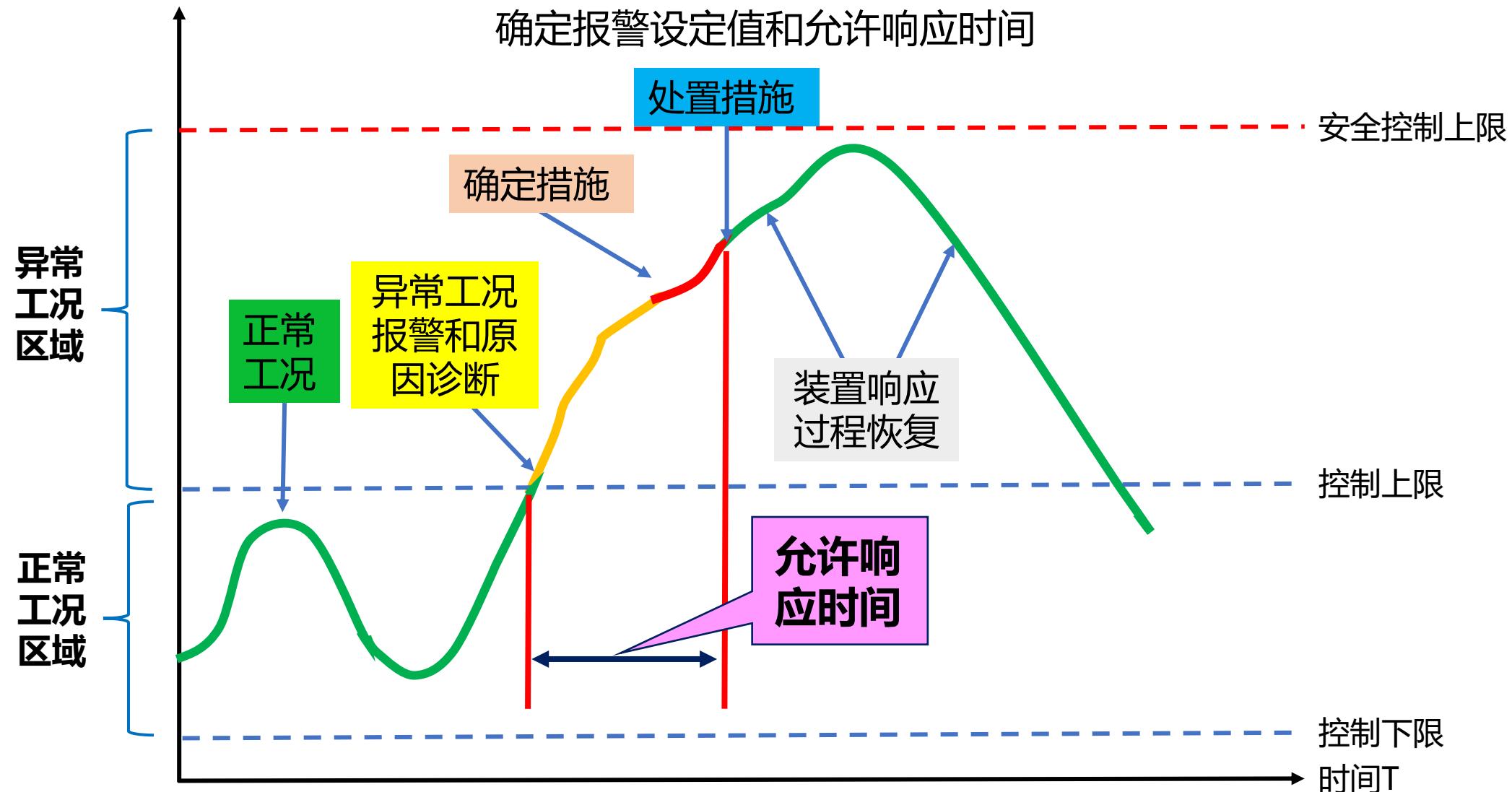


报警全生命周期管理要点

“化危为安” 线上讲堂

安彦咨询

报警合理化分析和归档





报警合理化分析和归档

报警级别设置矩阵范例

安全	1人救治	1人或以上轻伤	1人或多人重伤	1人死亡
环境	微量泄漏或排放	少量泄漏或排放	大量泄漏或排放	排放影响到社区
财产损失	<5万元	5到20万元	20到100万元	>100万元
声誉	当地媒体报道	市级媒体报道	省级媒体报道	国家媒体报道
后果程度	轻微	中等	严重	极其严重
立刻 (<10分钟)	中	中	高	紧急
迅速 (10-30分钟)	低	中	高	紧急
尽快 (30-60分钟)	低	低	中	高

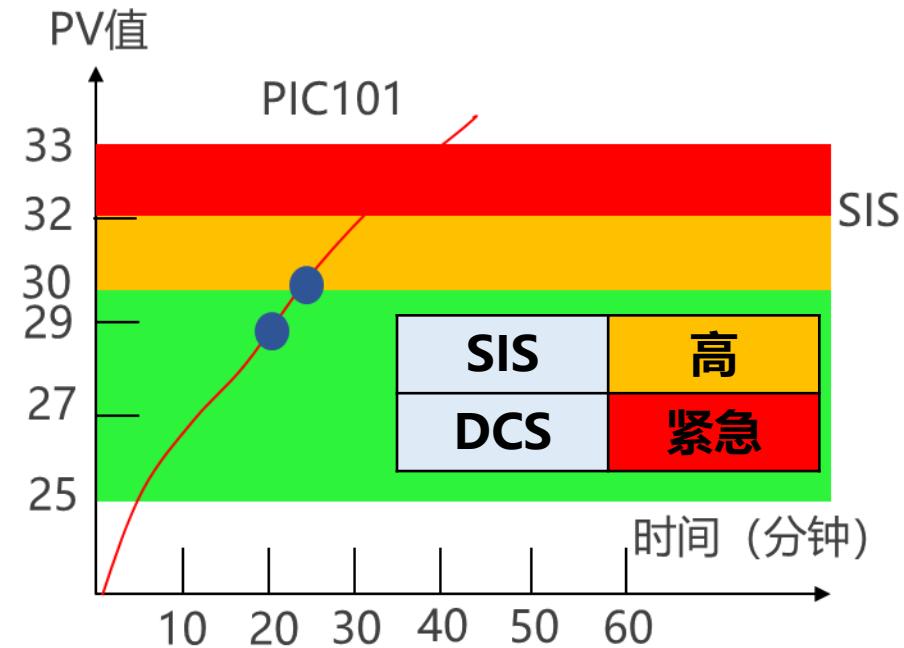
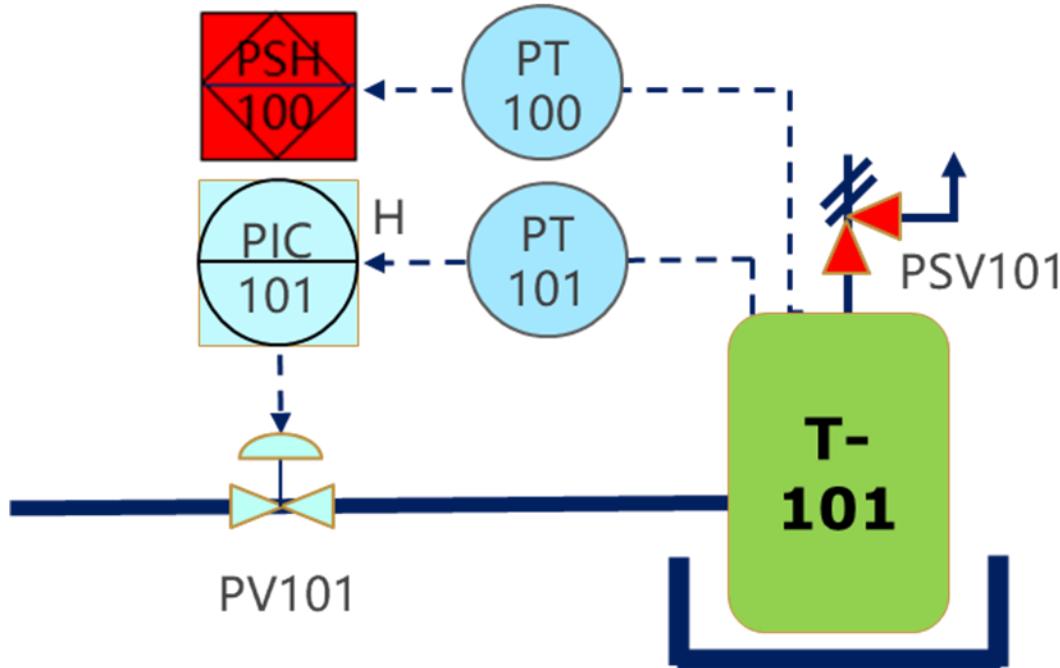
优先级不同，报警的声音和颜色不同



报警设定值范例

“化危为安” 线上讲堂

安彦咨询



参数	偏差	原因	后果	L	S	R	安全措施	L	S	R
压力	压力高	PIC101回路故障	T101 储罐超压，导致破裂，物料泄漏导致人员中毒、火灾爆炸	4	5	20	1.PIC101设计有压力高报警 2.设计有安全阀PSV101 3.设计有SIS联锁PSH100	1	5	5
		操作失误全开PV101		4	5	20	1.PIC101设计有压力高报警 2.设计有安全阀PSV101 3.设计有SIS联锁PSH100	1	5	5



报警系统设计

报警设计原则:

1. 报警要涵盖所有的重要工况的异常情况
2. **符合相关工程标准和规范**
3. 每一个报警都有相应的响应
4. 能给操作员一定的操作指引
5. 能给操作员充足的时间响应报警
6. 设计一个**主报警监控系统**

1. 报警系统的设计应符合 HG/T 20511 的要求;
2. 火灾自动报警系统的设计应符合 GB 50116 的要求;
3. 可燃和有毒气体报警的设计应符合 GB/T 50493 的要求。

详细设计包括三方面:

1. 基本报警设置：包括报警类型、设定值、死区和延时设置
2. 人机接口设置：包括画面显示和报警汇总画面
3. **先进报警功能AAS设计**：包括报警统计、变更管理、抑制和屏蔽功能



报警系统设计

基本报警设计原则-集中管理，人机界面清晰，易导航至操作画面，异常工况报警及时显示和声音提醒响应

横河DCS报警参数一览表

HH 上上限报警
HI 上限报警
LO 下限报警
LL 下下限报警
IOP 输入开路
OOP 输出开路
DV- 负偏差报警
DV+ 正偏差报警
ANS+ 回讯不正常 (MV =2,PV#2)
ANS- 回讯不正常 (MV =0,PV#0)
CAL 校验状态
MHI 阀门输出上限
MLO 阀门输出下限报警

NR 正常
HALM 高优先级报警
MALM 中优先级报警
LALM 低优先级报警
RALM 记录级报警
CNF 仪表连接错误报警
AOF 仪表报警旁路
TRIP 热断路报警
VEL+ 正变化率报警
VEL- 负变化率报警
PERR 回讯恢复正常
PERR 回讯恢复正常



报警全生命周期管理

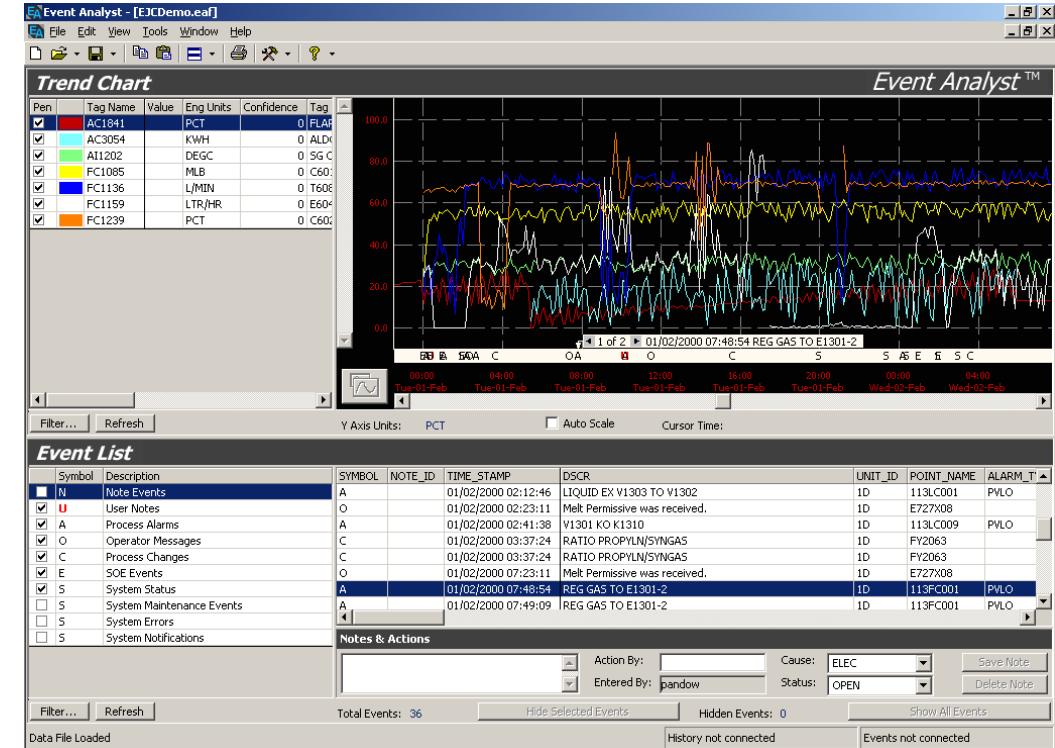
“化危为安” 线上讲堂

安彦咨询

报警系统运行

将报警系统投入使用，按照报警管理规范执行，持续改进报警管理水平，运行过程包括：

1. 报警系统处于使用状态
2. 操作人员报警管理培训
3. 建立报警管理台账和记录
4. 报警记录和分析（如高优先级报警）
5. 根据需要抑制和移除滋扰或高频报警
6. 检查和监督操作人员对报警的响应和处置



操作人员要熟悉报警系统功能使用和工艺设备报警的响应处置措施！



报警系统绩效监测与评估

设定报警管理绩效指标

基于EEMUA191报警KPI指标

主要考核指标	指标量度	报警绩效指标				
		预测	高效	稳定	被动	过量
每个小时平均报警数量	报警动态指标	<6	<60	<60	<600	>600
10分钟内最大报警数量	报警溢出程度	<10	<100	<1000	>1000	>1000
10分钟内包含30个报警以上的百分比	报警溢出频率	<1%	<5%	<25%	<50%	>50%
前10个最多报警占总报警数量百分比	报警改善空间	<1%	<5%	<10%	<25%	>25%
在任何情况下保持持续报警数量	报警静态指标	<5	<10	<50	<100	>100
陈旧报警数量 (辅助指标)		0	<5	<10	<20	>20
操作员抑制的报警 (辅助指标)		<5	<10	<15	<50	>50



报警全生命周期管理

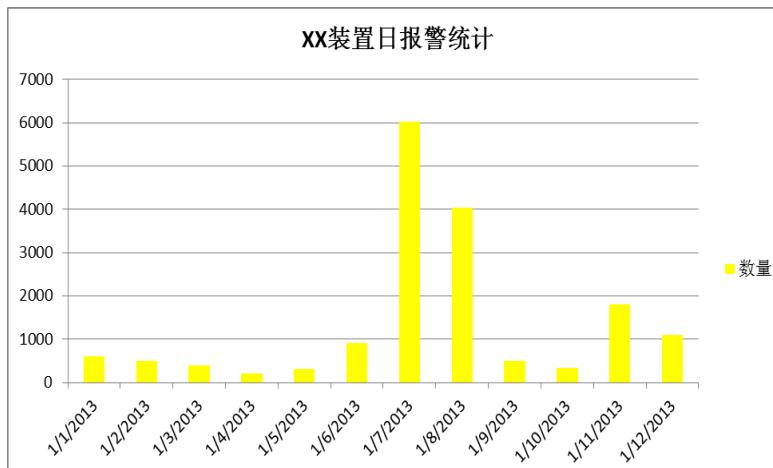
“化危为安” 线上讲堂

安彦咨询

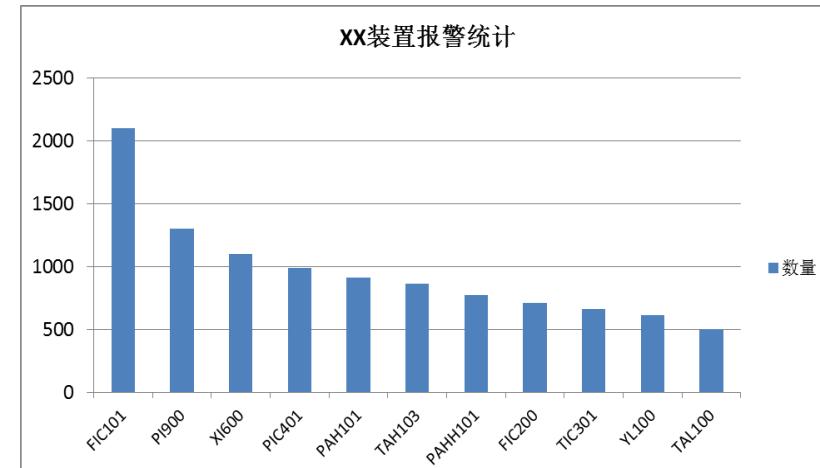
报警系统绩效监测与评估

- 定期收集DCS等系统中报警和历史事件日志中的报警活动数据，利用诊断工具对收集到报警数据进行统计分析，确定报警绩效等级。
- 重点对高频和高优先级报警进行根源分析，查找工艺设备及操作异常情况，并回顾工厂历史上发生的事故事件情况，确定整改和优化措施。

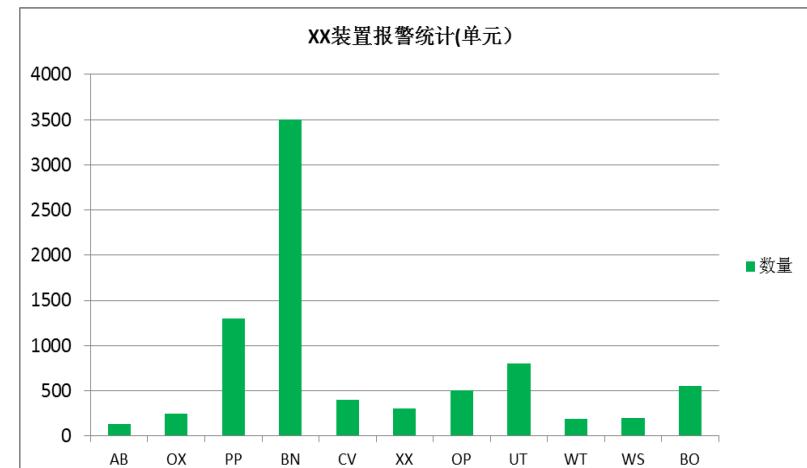
报警数量统计（日报警）



报警数量统计（位号）



报警数量统计（操作单元）



报警统计报表范例



报警全生命周期管理

“化危为安” 线上讲堂

安彦咨询

报警系统优化策略和实施

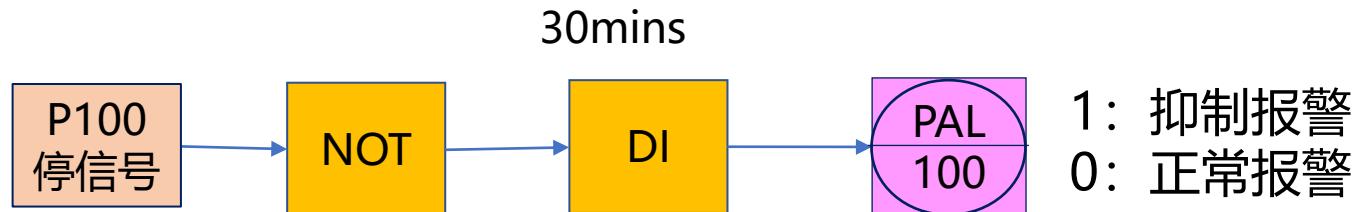
动态报警管理：基于状态报警设计，消除驻留报警

范例-设备状态报警

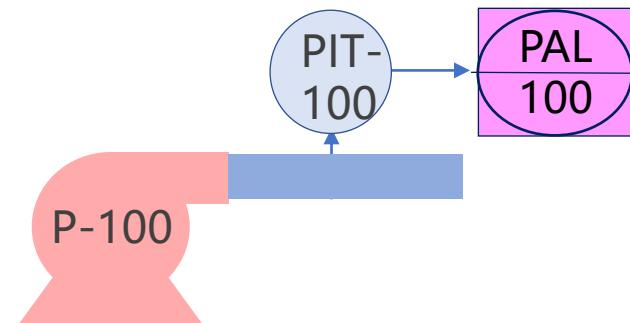
问题：P100泵开车阶段运行，负荷正常后停止产生驻留报警

解决方法：P100停止运行后30分钟，自动抑制PAL100的报

警，报警不再DCS汇总画面清单显示，重新运行时，报警功能立刻恢复，可应用在正常切换备用设备等工况。



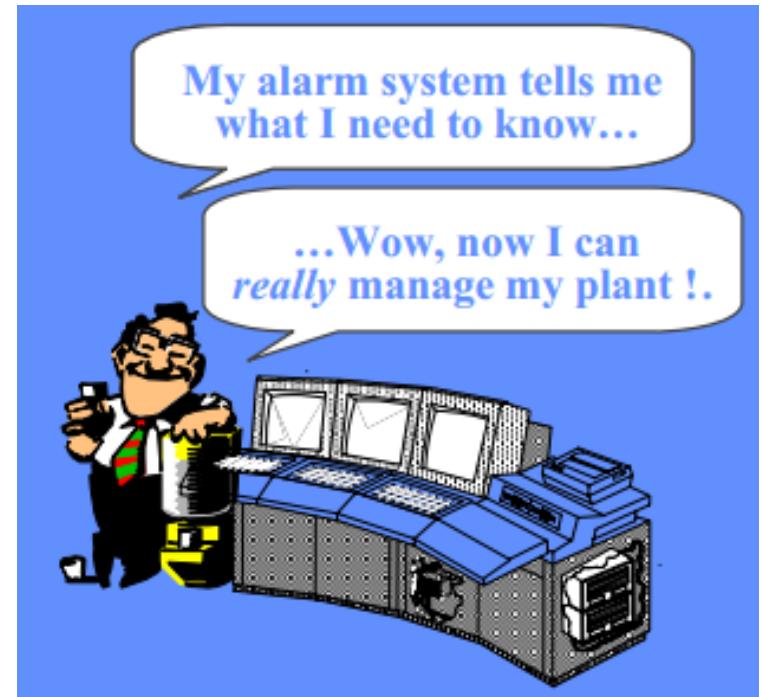
标志	报警时间	位号	测点说明
SYS	2021/04/19 08:24:47.827	P20106A	二塔进料泵A电流
SYS	2021/04/14 08:05:35.483	SY580MNA	80号操作站A网
SYS	2021/04/14 08:05:35.483	SY580SD80	80号操作站
SYS	2021/04/14 08:05:33.971	SY580MNB	80号操作站B网
SYS	2021/04/14 08:04:17.471	SY580S80	80号操作员在线
SYS	2021/03/01 08:48:20.775	FIC6601	醋酸罐回流调节
SYS	2021/02/28 09:30:33.218	LI1285	V10115二反异构计量泵液位
SYS	2021/02/28 09:28:50.217	2PI1208	P10111A异构计量泵出口压力
SYS	2021/02/23 13:48:11.649	SB10111A	P10111A异构计量泵工作频率
SYS	2021/02/23 13:48:11.649	IB10111A	P10111A异构计量泵工作电流
SYS	2021/02/23 13:48:04.145	SB10111B	P10111B异构计量泵工作频率
SYS	2021/02/23 13:48:04.145	IB10111B	P10111B异构计量泵工作电流
SYS	2021/02/01 14:29:48.799	SB10106B	P10106B醋酸罐工作频率
SYS	2021/02/01 14:29:48.799	IB10106B	P10106B醋酸罐工作电流
SYS	2020/10/15 12:01:04.237	PN12_AJX	备用
SYS	2020/09/28 16:08:15.484	PN12_AKF	备用
SYS	2020/09/07 06:59:30.797	PN12_AMR	备用
SYS	2020/09/03 10:29:08.177	FIO13_52	13.52_SM432
SYS	2020/09/03 10:29:08.177	FIO13_51	13.51_SM432
SYS	2020/09/03 10:29:08.177	FIO13_50	13.50_SM432
SYS	2020/09/03 10:29:08.177	FIO13_49	13.49_SM432
SYS	2020/09/03 10:28:54.321	TR1287	V10117二反后缓冲罐温度
SYS	2020/09/03 10:28:54.321	TR1286	V10116二反前缓冲罐温度
SYS	2020/09/03 10:28:54.321	TR1285	V10115二反前缓冲罐温度
SYS	2020/09/03 10:28:54.321	TR1284	V10109后缓冲罐温度
SYS	2020/09/03 10:28:54.321	TR1282	V10108C甲醇缓冲罐温度
SYS	2020/09/03 10:28:54.321	PN13_AHB	





报警系统运行与维护

1. 把不同工艺单元的报警组态在不同的操作区域，使相关操作区域操作员只能接受本区域的报警。
2. 对报警设定值重新评估设定-操作员有足够时间处理报警。
3. 调整和优化报警值的死区-0.5~3%之间
4. 删减重复的报警功能-如PID控制器的重复报警
5. 删减没有任何工艺异常情况时发生的报警
6. 删减那些发生报警而操作员没有任何响应的报警。
7. 修改/扩大仪表量程，消除超量程报警。
8. 及时处理仪表故障消除DCS IOBAD报警。
9. 优化PID参数，调整工艺操作消除控制回路波动报警。
10. 严格管控报警屏蔽和变更管理





安彦咨询

“化危为安” 线上讲堂



联锁和联锁管理定义



吉化双苯厂硝基苯装置爆炸事故

“化危为安” 线上讲堂

安彦咨询

2005年11月13日，中石油吉林石化分公司双苯厂硝基苯精馏塔发生爆炸，造成8人死亡，60人受伤，直接经济损失6908万元，并导致了一起跨省、跨国界的重大环境污染事件。

事故直接原因：

外操人员违反操作规程使预热器及管线的法兰松动、密封失效，空气吸入系统，由于摩擦、静电等原因，导致硝基苯精馏塔发生爆炸，并引发其它装置、设施连续爆炸。



事故教训：

1. 人员违章操作导致事故
2. 本质安全设计不足：危险工艺过程没有设计SIS联锁系统作为安全保护层



安彦咨询

联锁 Interlock

是指为了防止工艺或设备参数超限造成产品质量、设备、安全生产事故而设置的**保护**设施及功能，用于生产装置（或独立单元）过程参数超出安全操作范围、机械设备故障、系统自身故障或物料、能源中断时，自动（必要时也可以手动）产生的一系列预先定义**动作**，使操作人员和生产装置处于**安全状态**的系统。

联锁系统 Interlock System

当过程参数超限、设备异常以及操作员输入信号时，执行预先预定要求的系统。

联锁系统分为**安全联锁系统**和**非安全联锁系统**。

联锁系统可由传感器/或发讯器、逻辑控制器、最终元件及相关软件组成。

--HG/T 20511-2014 《信号报警及联锁系统设计规范》

联锁分类

工艺联锁、设备联锁、安全环保联锁、机械联锁、电气联锁等。



安彦咨询

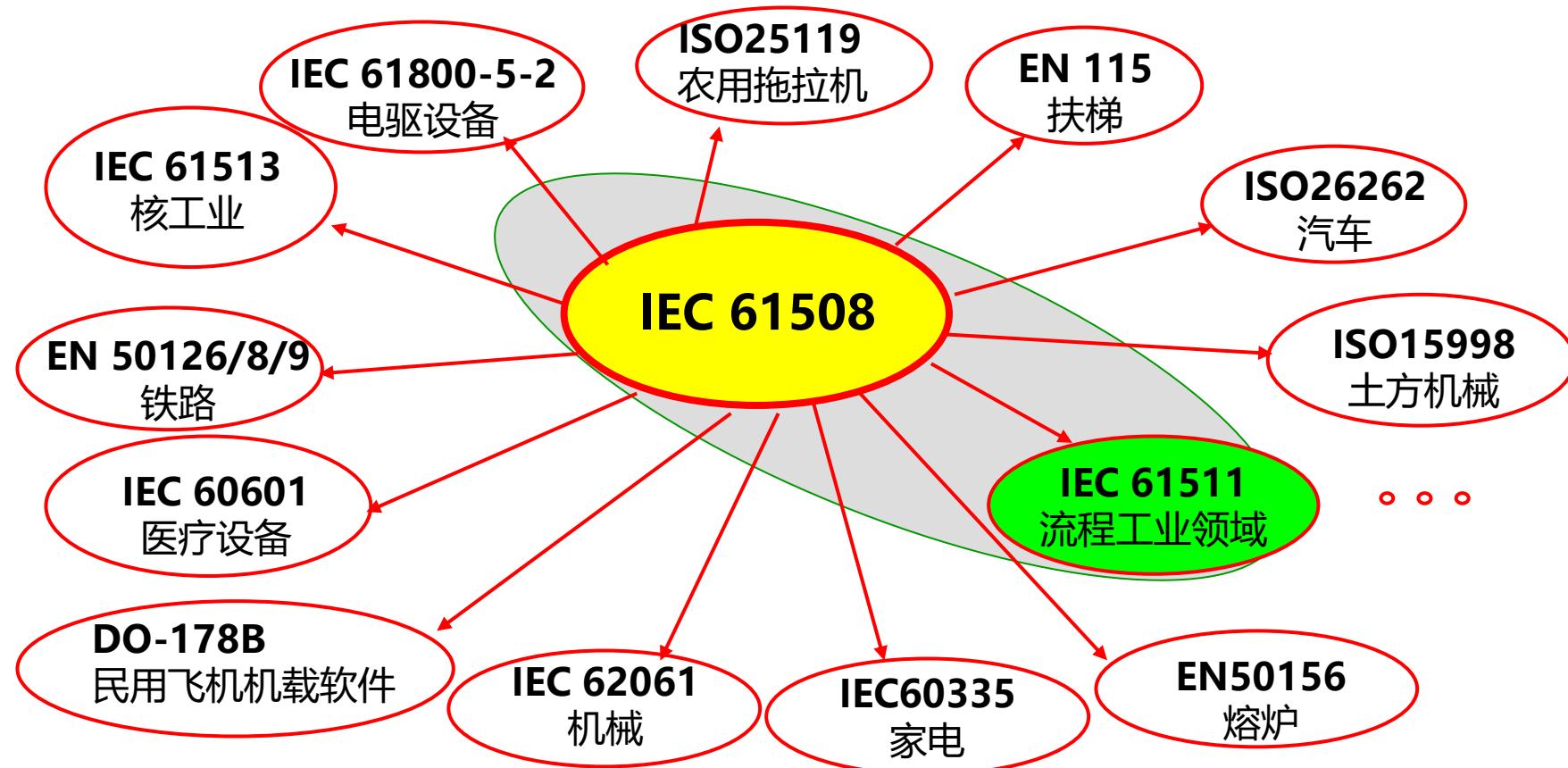
1. SHB-Z06-1999 《石油化工紧急停车及安全联锁系统设计导则》，采用了IEC标准中的一些理念
2. SY/T10045-2003 《工业过程中安全仪表系统的应用》国家经济贸易委员会发布，作为石油天然气行业标准。等同采用ISA84.01-1996
3. SH/T3012-2003 《石油化工安全仪表系统设计规范》，国家发改委颁布实施了石油化工行业标准
4. GB/T20438.1-2006 《电气/电子/可编程电子安全相关系统功能安全》，IEC61508完整转换，2106年进行升级
5. GB/T21109.1-2007 《过程工业领域安全仪表系统的功能安全》由IEC61511完整转换，于2007年10月11日发布，2007年12月1日实施
6. GB/T50770-2013 《石油化工安全仪表系统设计规范》，标准引入安全生命周期概念
7. HG/T20511-2014 《信号报警及联锁系统设计规范》



安彦咨询

两个重要的功能安全标准体系（安全仪表系统SIS）

IEC61508-电气/电子/可编程电子安全相关系统的功能安全





两个重要标准

“化危为安”线上讲堂

安彦咨询

ICS
N 10



中华人民共和国国家标准

GB/T 20438.1—2017/IEC 61508-1:2010
代替 GB/T 20438.1—2006

电气/电子/可编程电子安全相关系统的
功能安全 第1部分:一般要求

Functional safety of electrical/electronic/programmable electronic safety-related
systems—Part 1: General requirements

(IEC 61508-1:2010, IDT)

**IEC61508 1998年发布, 2010年升级
GB/T20438 2007年实施, 2017年升级**

2017-12-29 发布

2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会发布

ICS
N 10



中华人民共和国国家标准

GB/T 21109.1—2007/IEC 61511-1:2003

过程工业领域安全仪表系统的功能安全
第1部分:框架、定义、系统、硬件和
软件要求

Functional safety—Safety instrumented systems for the process
industry sector—Part 1: Framework, definitions, system,
hardware and software requirements

(IEC 61511-1:2003, IDT)

**IEC61511 2003年发布, 2016年升级
GB/T21109 2007-12-01实施**

2007-10-11 发布

2007-12-01 实施



中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会发布



安彦咨询

“化危为安” 线上讲堂



联锁全生命周期管理



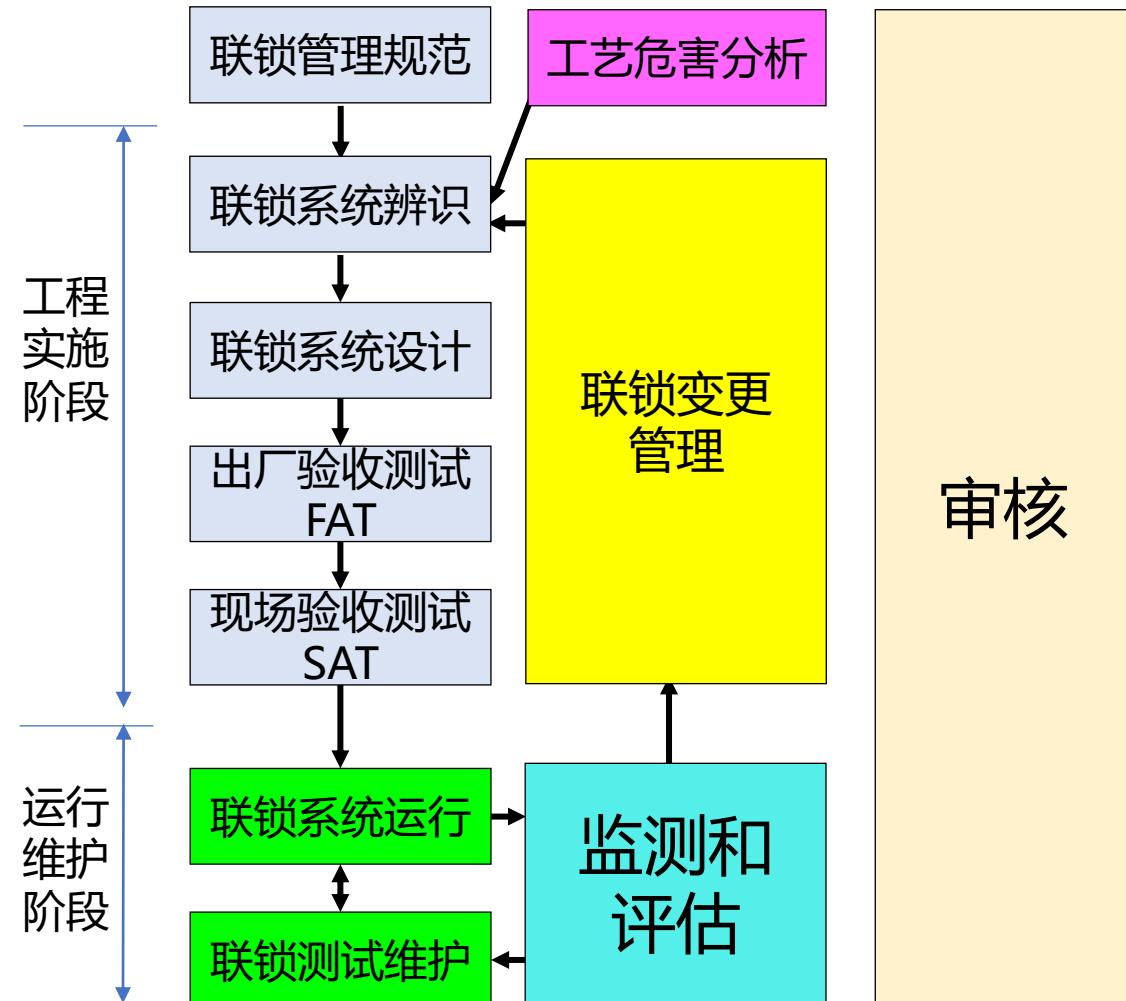
联锁全生命周期管理

“化危为安” 线上讲堂

安彦咨询

联锁管理生命周期活动包含10个步骤，包括：

1. 两个阶段：
 - ✓ 工程实施
 - ✓ 运行维护
2. 适用于新装置和在役装置联锁系统管理与优化
3. 包括解决联锁系统设计、运行问题和持续改进的最佳实践





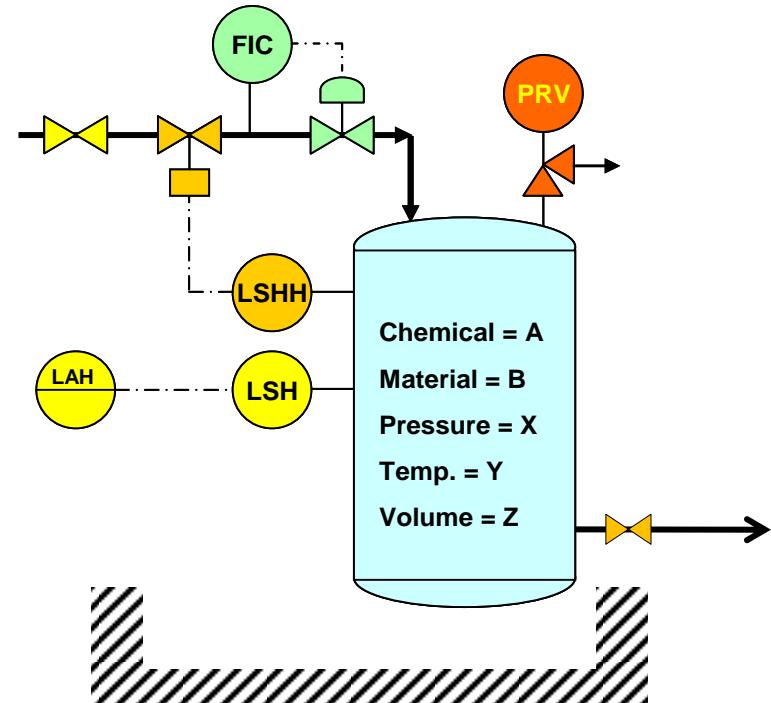
联锁全生命周期管理要点

“化危为安” 线上讲堂

安彦咨询

联锁管理规范主要内容

1. 联锁管理职责
2. 联锁分级管理要求
3. 新建、改建、扩建等项目中的联锁系统风险分析管理要求
4. 联锁系统设计技术要求
5. 联锁系统选型、采购、安装、调试和投用管理
6. 联锁系统档案与记录
7. 联锁保护系统日常维护、故障处理和检修具体要求
8. 联锁系统和应用软件备份管理
9. 联锁变更与解除管理
10. 联锁系统故障排查、记录与整改
11. 联锁系统管理检查与审核





安彦咨询

联锁辨识-工程规范

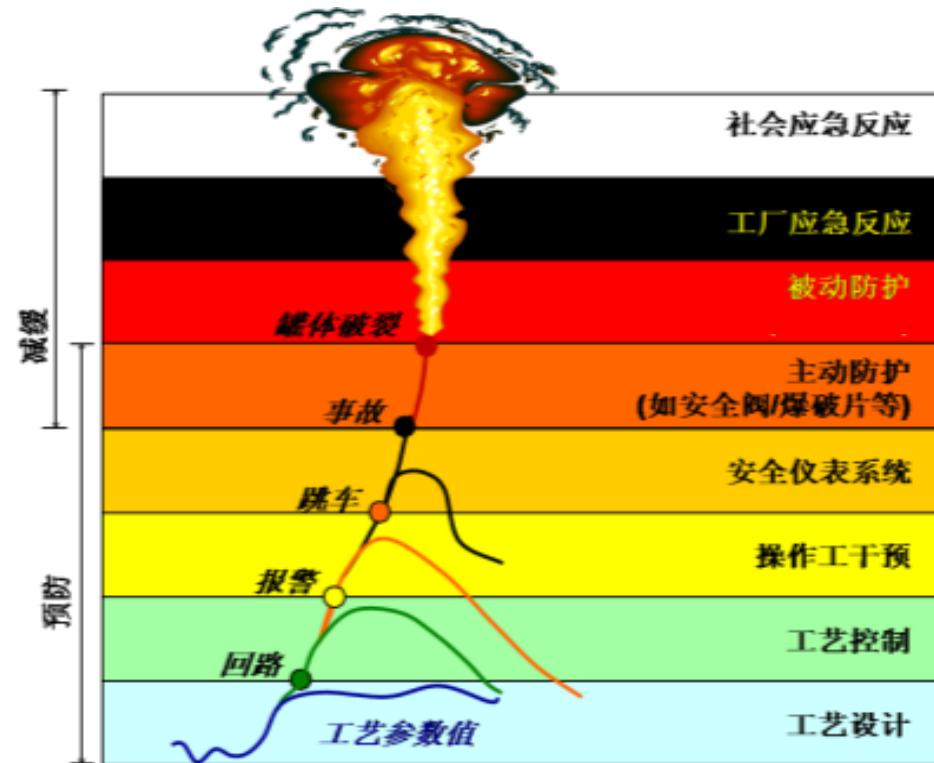
1. **《国家安全监管总局关于进一步加强化学品罐区安全管理的通知》** (安监总管三〔2014〕86号) (一) 根据规范要求设置储罐高低液位报警, 采用超高液位自动联锁关闭储罐进料阀门和超低液位自动联锁停止物料输送措施。大型、液化气体及剧毒化学品等重点储罐要设置紧急切断阀。
2. **《危险化学品重大危险源监督管理暂行规定》** (国家安全生产监督管理总局令 第40号) 第十三条 (三) 对重大危险源中的毒性气体、剧毒液体和易燃液体等重点设施, 设置紧急切断装置; 毒性气体的设施, 设置泄漏物紧急处置装置。涉及毒性气体、液化气体、剧毒液体的一级或者二级重大危险源, 配备独立的安全仪表系统 (SIS)。
3. **《化工和危险化学品生产经营单位重大生产安全事故隐患判定标准 (试行) 》** (安监总管三〔2017〕121号) 五、构成一级、二级重大危险源的危险化学品罐区未实现紧急切断功能; 涉及毒性气体、液化气体、剧毒液体的一级、二级重大危险源的危险化学品罐区未配备独立的安全仪表系统。
4. **《石油化工企业设计防火标准》** GB 50160-2008 (2018年版) 6.2.23 可燃液体的储罐宜设自动脱水器, 并应设液位计和高液位报警器, 必要时可设自动联锁切断进料设施。



安彦咨询

联锁辨识与分级

基于工艺危害分析PHA、工程规范等，识别联锁功能并确定等级，确保人员安全和关键工艺设备有足够的保护层。



联锁分级范例

联锁保护系统按其重要性分为三级

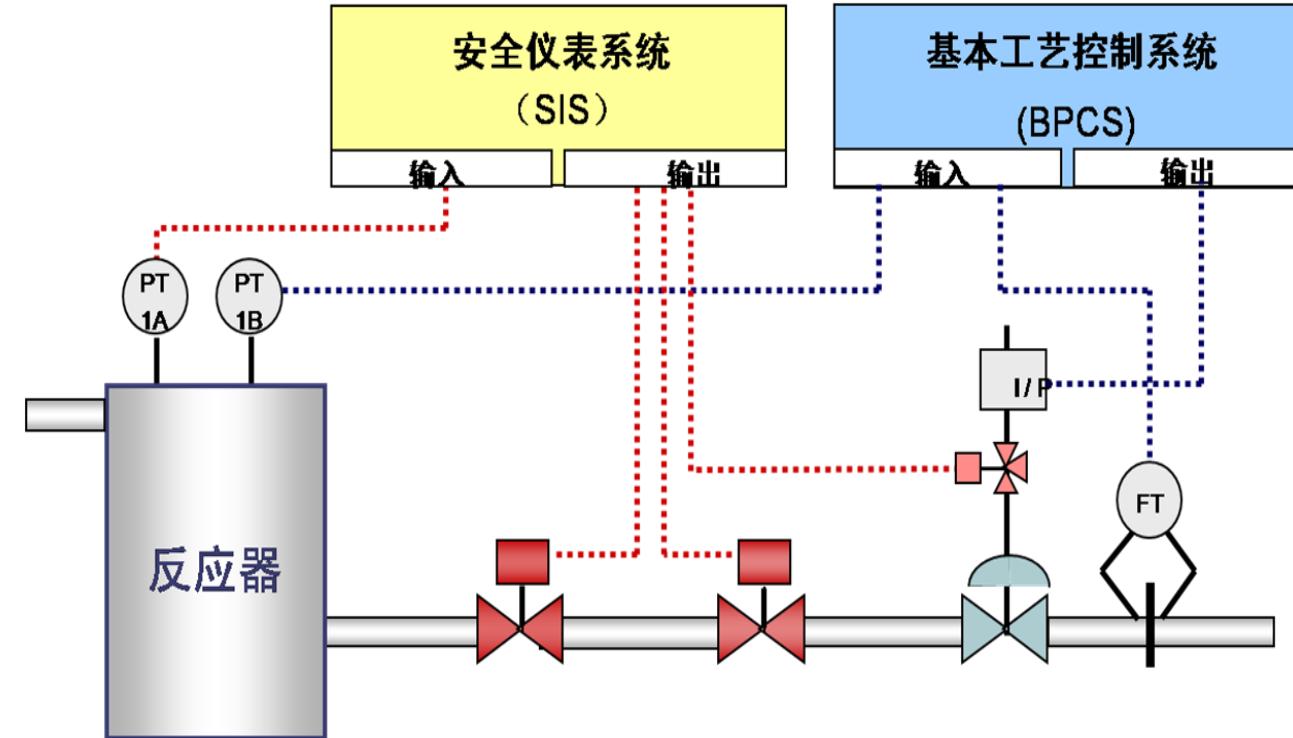
- 1. A级（工厂级）**：联锁动作造成单套或多套装置停车、关系到重大人身、设备安全和产品质量的仪表联锁回路；
- 2. B级（部门级）**：联锁动作造成装置局部或单个工段、单元停工，其影响面次于A级联锁的联锁回路；
- 3. C级（车间级）**：联锁动作造成装置工段、单元内局部停工或单台设备停车，其影响面次于B级联锁的联锁回路。



安彦咨询

联锁系统的设计原则

1. 独立设置原则（传感器和执行元件）
2. 中间环节最少原则
3. 采用冗余容错结构
4. 故障安全原则
5. 风险分配原则
6. 采用连续测量仪表代替开关类仪表
7. 紧急停车按钮应设可靠的护罩
8. 具备报警和SOE功能

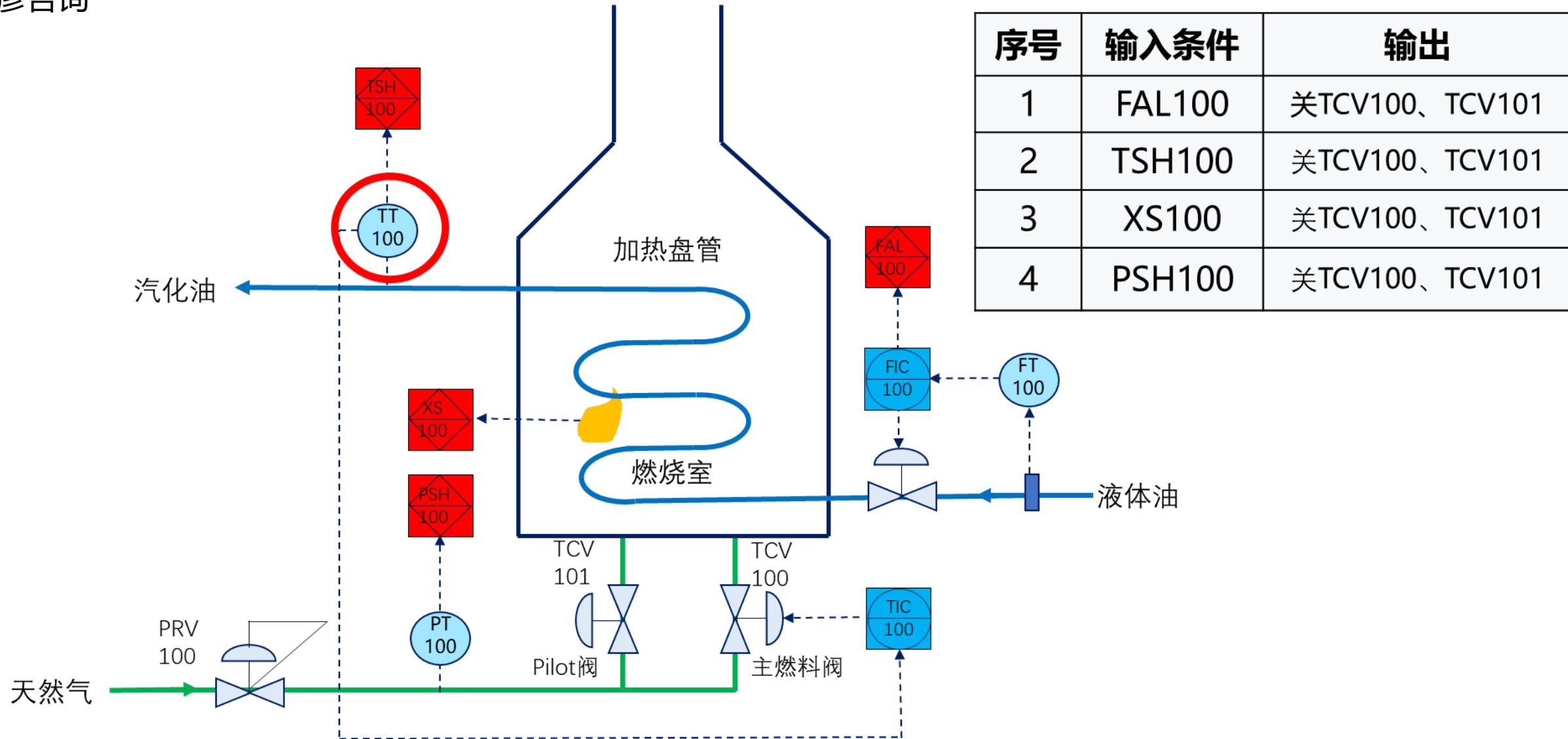




联锁设计范例

“化危为安” 线上讲堂

安彦咨询





冗余逻辑的表决方法及其与安全性、可用性的关系

表决方法	隐故障概率 (拒动)	显故障概率 (误动)	允许	不允许	安全性	可靠性
一选一	0.02 (短路的概率)	0.04 (开路的概率)		存在隐故障和显故障	差	差
二选一	0.0004 (两个均短路的概率)	0.08 (只要有一个开路的概率)	其中之一存在隐故障 (仍可安全停车)	其中之一存在显故障 (将误停车)	最好	最差
二选二	0.04 (只要有一个短路的概率)	0.0016 (两个均开路的概率)	其中之一存在显故障 (不会误停车)	其中之一存在隐故障 (该停拒停)	最差	最好
三选二	0.0012 (三个中两个均短路的概率)	0.0048 (三个中两个均开路的概率)	其中之一存在隐故障或显故障	其中两个存在隐故障或显故障	较好	较好



联锁全生命周期管理要点

“化危为安” 线上讲堂

安彦咨询

FAT与SAT管理

组织管理

1. FAT和SAT人员由用户、工程公司（设计院）、供应商三方技术人员组成。
2. 编制和审核FAT和SAT测试计划和方案。

文档检查

1. 工程文件、软件文件和制造商标准文件。

测试项目

1. 系统硬件和软件型号配置、冗余容错、报警、IO精度、网络、联锁功能、操作画面、自诊断、SOE功能、控制器负荷、系统可维护性、在线组态修改、编译和下装等。

测试记录与报告

ICS 25.040, 40
N 10



中华人民共和国国家标准

GB/T 25928—2010/IEC 62381:2006

过程工业自动化系统
出厂验收测试(FAT)、现场验收
测试(SAT)、现场综合测试(SIT)规范

Automation systems in the process industry—
Factory acceptance test (FAT),
site acceptance test (SAT), and site integration test (SIT)

(IEC 62381:2006, IDT)



2011-01-14 发布

2011-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会发布



联锁全生命周期管理要点

“化危为安” 线上讲堂

安彦咨询

联锁台账建立-通常在PSSR（启动前安全检查）阶段完成

- 1. 联锁逻辑图
- 2. PHA报告(HAZOP)
- 3. P&ID图



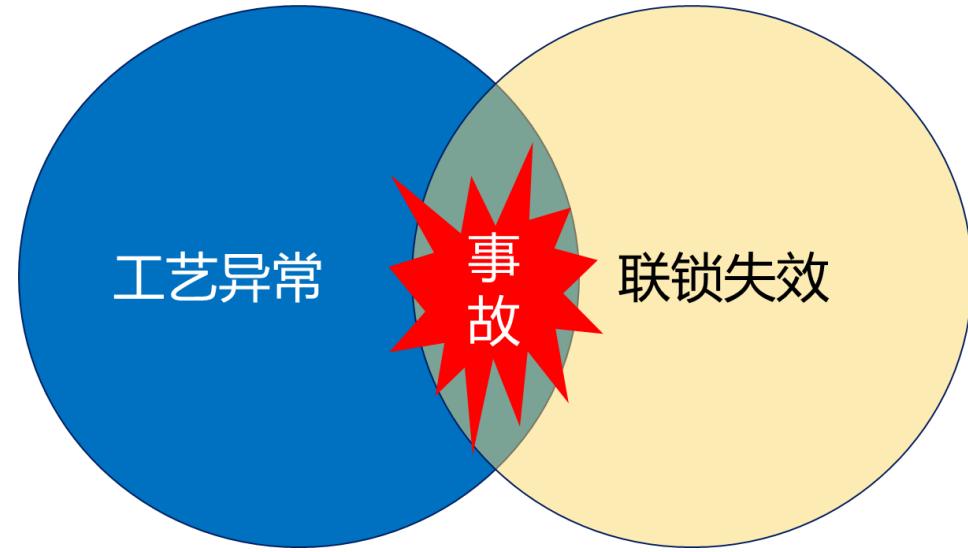
序号	联锁回路名称	联锁回路位号 (一次仪表位号)	联锁形式	测量内容 (具体内容)	测量设备名称	联锁系统	联锁动作值	联锁动作设备位号	联锁动作设备名称	联锁动作内容	联锁等级
1	循环气压缩机C-100安全保护联锁	PT100	三取二	C-100润滑油总管压力低低	压力变送器	SIS TRICON-TMR	≤ 0.15MPa	C-100	压缩机	停C-100	B
		PT101		C-100润滑油总管压力低低	压力变送器	SIS TRICON-TMR	≤ 0.15MPa				
		PT102		C-100润滑油总管压力低低	压力变送器	SIS TRICON-TMR	≤ 0.15MPa				
2		VT100	二取二	压缩机轴振动高高	振动探头	SIS TRICON-TMR	≥ 18mm/s	C-100	压缩机	停C-100	B
		VT101		压缩机轴振动高高	振动探头	SIS TRICON-TMR	≥ 18mm/s				
3		PT103	单点联锁	C-100润滑油总管压力正常	压力变送器	SIS TRICON-TMR	≤ 0.25MPa	C-100油泵	辅油泵	开辅油泵	B



安彦咨询

联锁失效的原因分析与整改

1. 硬件故障：传感器、逻辑运算单元或执行元件故障。
2. 管理因素：
 - ◆ 随意变更联锁逻辑或设定阈值；
 - ◆ 随意解除联锁保护功能；
 - ◆ 未及时恢复解除的联锁回路。
3. 设计失误：功能错误或不足未实现设计安全保护功能。



业界不乏类似惨重事故教训

重大工艺安全隐患：

目前有的企业一些联锁未投用或处于旁路状态，且联锁摘除期间缺乏有效管控措施！



日常维护-联锁功能安全与可靠的保证





联锁的变更和解除管理

关键：联锁的变更和解除必须得到审核及批准！！！

联锁变更

1. 设定新的联锁阈值
2. 增加或减少联锁回路
3. 逻辑功能或算法改变等

以下情形应视为联锁切除

1. 控制系统上联锁的切除
2. 给检测元件加入假信号代替实际测量值
3. 使用跨接线将检测元件旁路
4. 使用管道将现场动作执行元件旁路
5. 为了达到无法触发联锁的目的而改变联锁阈值

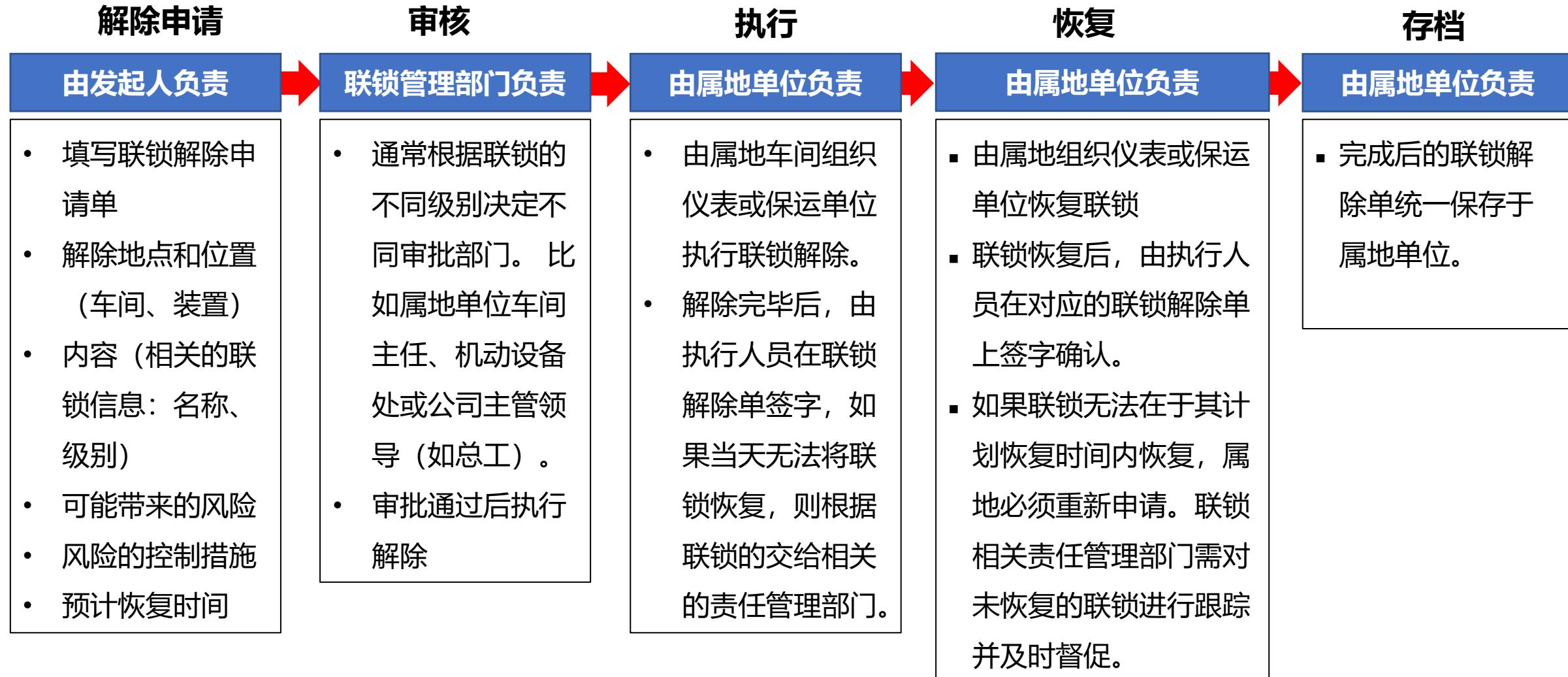
实施前应对照工艺危害分析PHA报告(HAZOP/What-If) 的相关内容，将解除联锁后可能导致的风险和应急预案进行阐述。

如无法找到工艺安全评估报告中的相关内容，则应从以下几个方面对风险进行评估：

- ✓ 可能导致的人员伤害严重程度（单人医疗事故 -> 多人死亡）
- ✓ 可能导致的环境影响(公司内 -> 周边社区或区域)
- ✓ 可能受到影响的上下游装置和工艺



安彦咨询 联锁的变更和解除管理



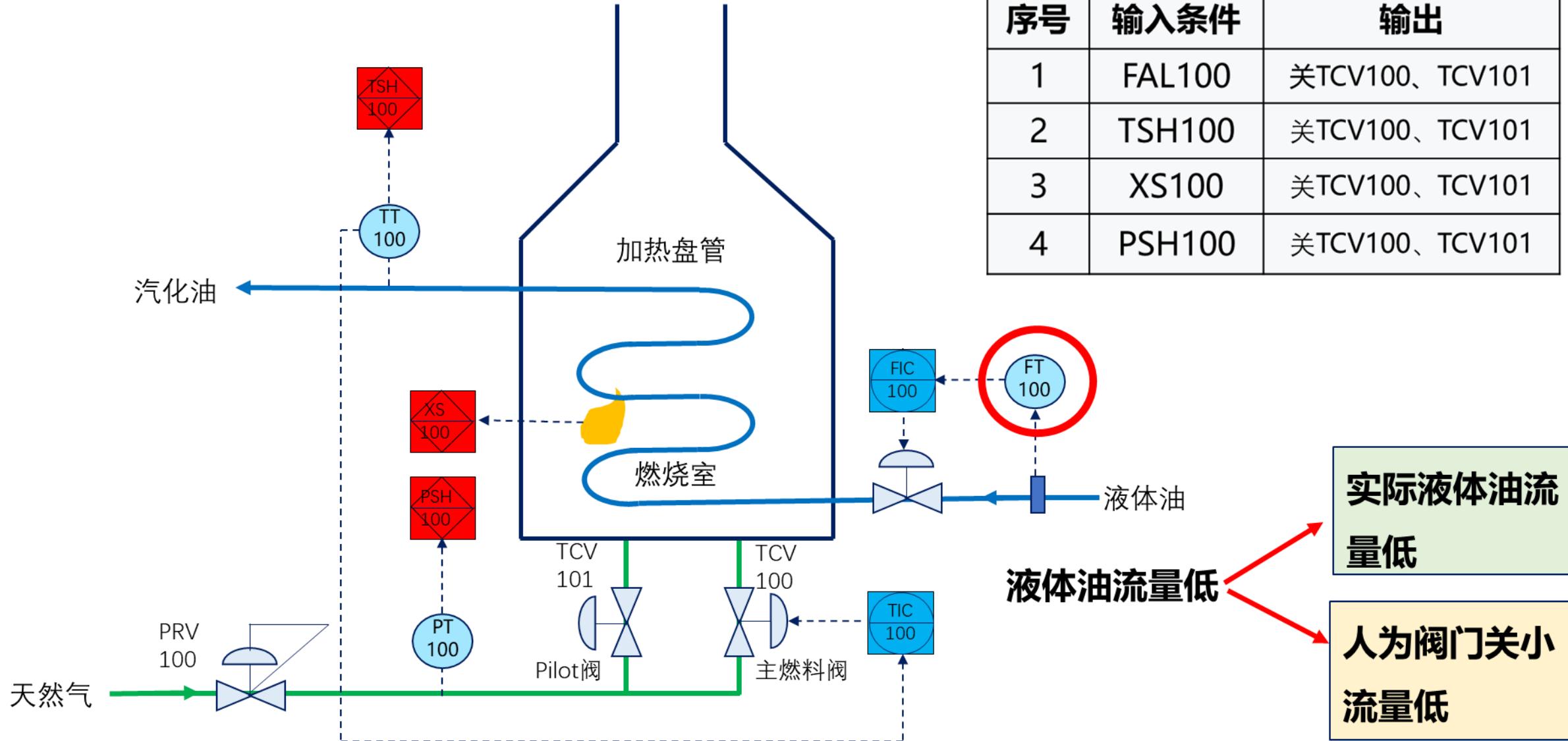


联锁解除风险分析范例

“化危为安” 线上讲堂

安彦咨询

FT100故障无法投入运行，需旁路此联锁





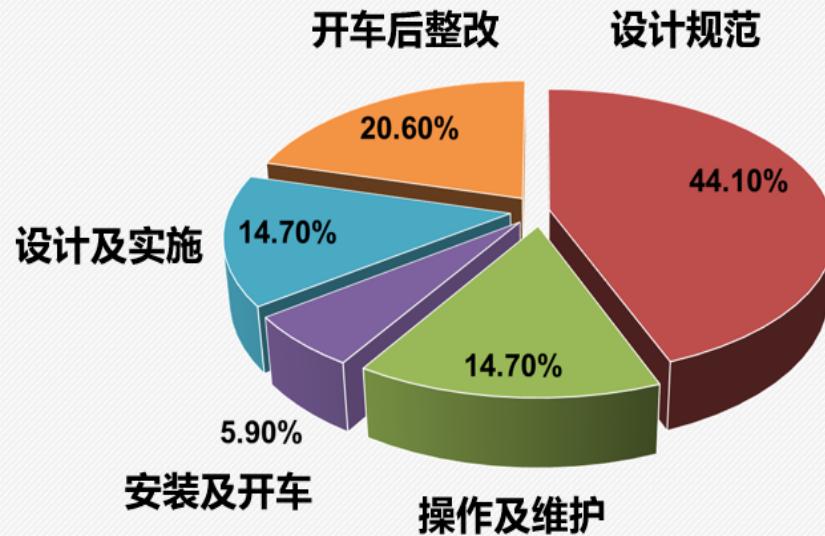
联锁管理绩效指标

安彦咨询

主要考核指标	指标量度	联锁绩效指标
月度联锁投用率	总体联锁管理	100%
年度联锁故障数量	联锁可靠性	0
联锁摘除变更管理符合性	联锁变更管理	100%
1. 月度联锁投用率=联锁投用回路数量/总联锁回路数量 $\times 100\%$ 2. 年度联锁故障数量=测试时发现的联锁故障回路数量 + 运行时的联锁不正常动作次数（误动和拒动）		

“化危为安” 线上讲堂

与安全仪表系统相关的事故统计图



摘自<Health & Safety Executive HSE-UK>



安彦咨询

“化危为安” 线上讲堂



基于6西格玛的报警联锁管理改进

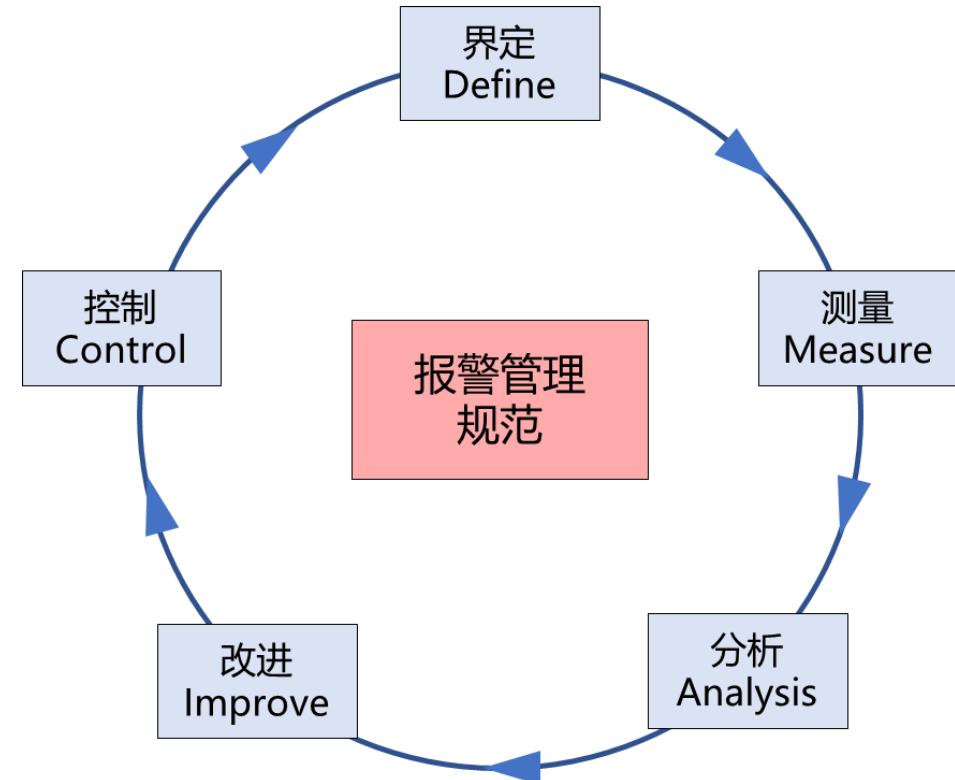


基于6西格玛报警管理改善途径

“化危为安” 线上讲堂

安彦咨询

1. 界定：制定报警管理规范和管理标准
2. 测量：收集和评估现有报警系统绩效
3. 分析：报警绩效基准分析，找出差距
4. 改进：制定报警系统优化措施和实施
5. 控制：持续维护和改进报警系统管理



6西格玛管理原理

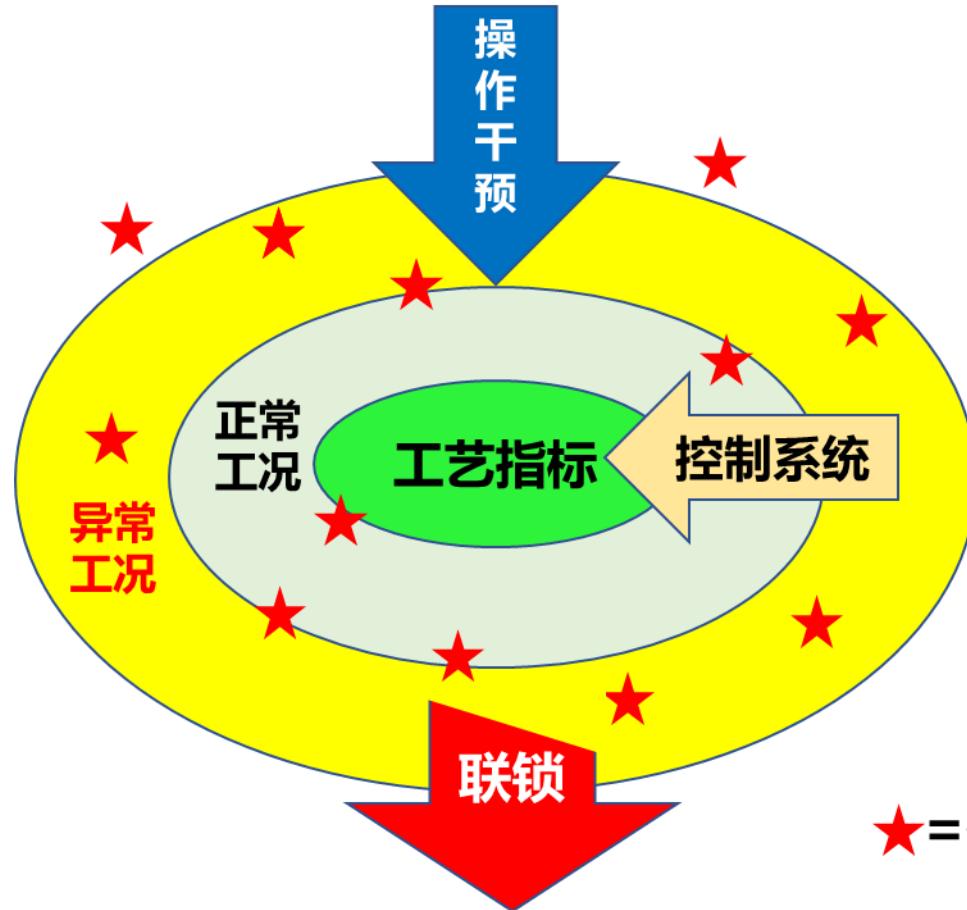


报警管理改善流程

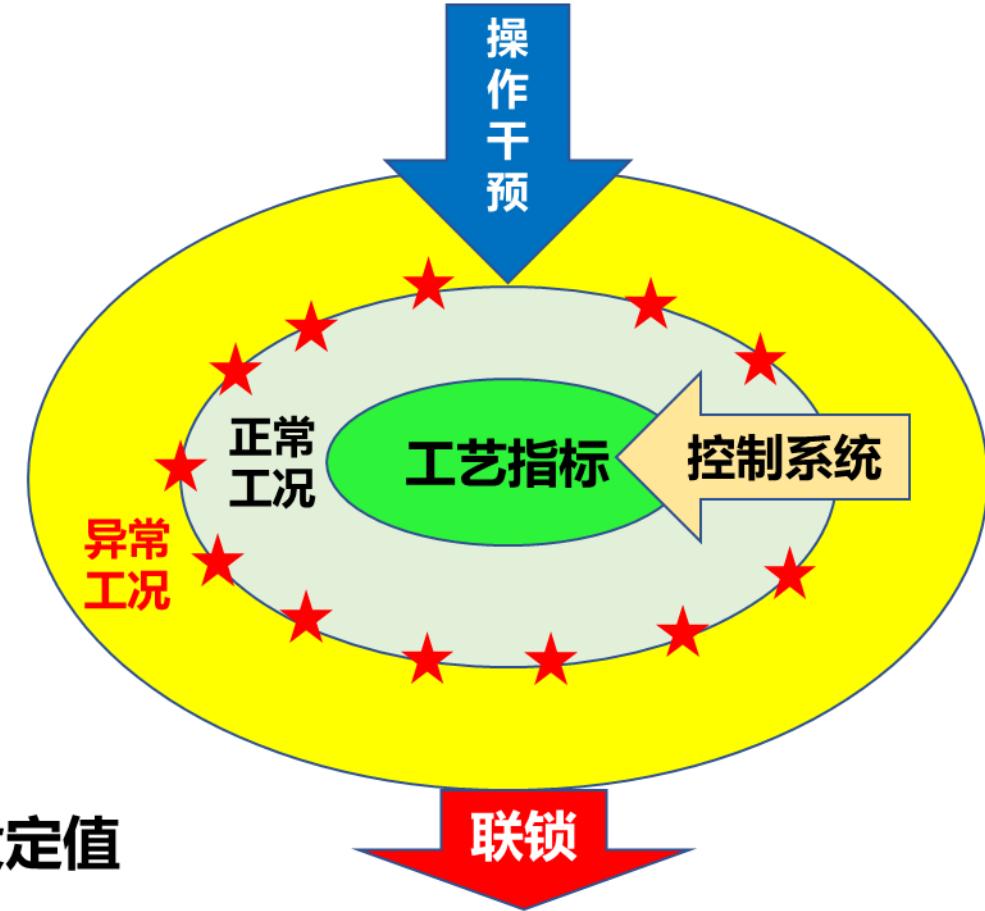
“化危为安” 线上讲堂

安彦咨询

目标：建立安全和高效的报警系统



低效的报警和联锁设计



高效的报警和联锁设计

★=报警设定值

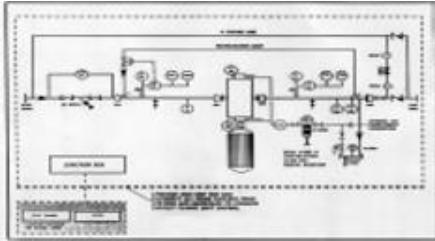


报警管理改善流程

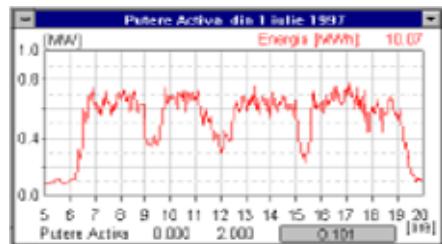
“化危为安” 线上讲堂

安彦咨询

组建报警改善团队，收集资料和数据进行统计分析



P&ID



历史数据



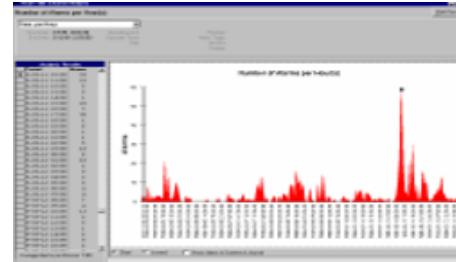
PHA/HAZOP报告

报警系统优化需要的资源

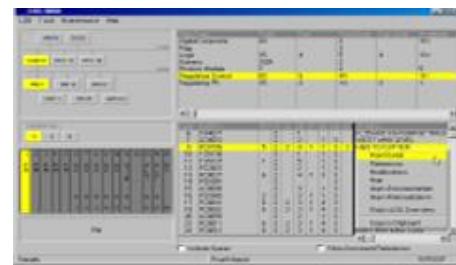


装置知识和经验
工艺、设备
操作规程、程序

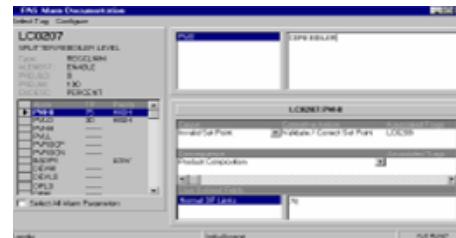
- ✓ 操作员
- ✓ 工艺和控制工程师
- ✓ HSE人员
- ✓ 生产和维修工程师



报警数据分析



位号组态数据



专业优化软件



报警管理改善流程

“化危为安” 线上讲堂

安彦咨询

报警绩效基准分析，找出差距

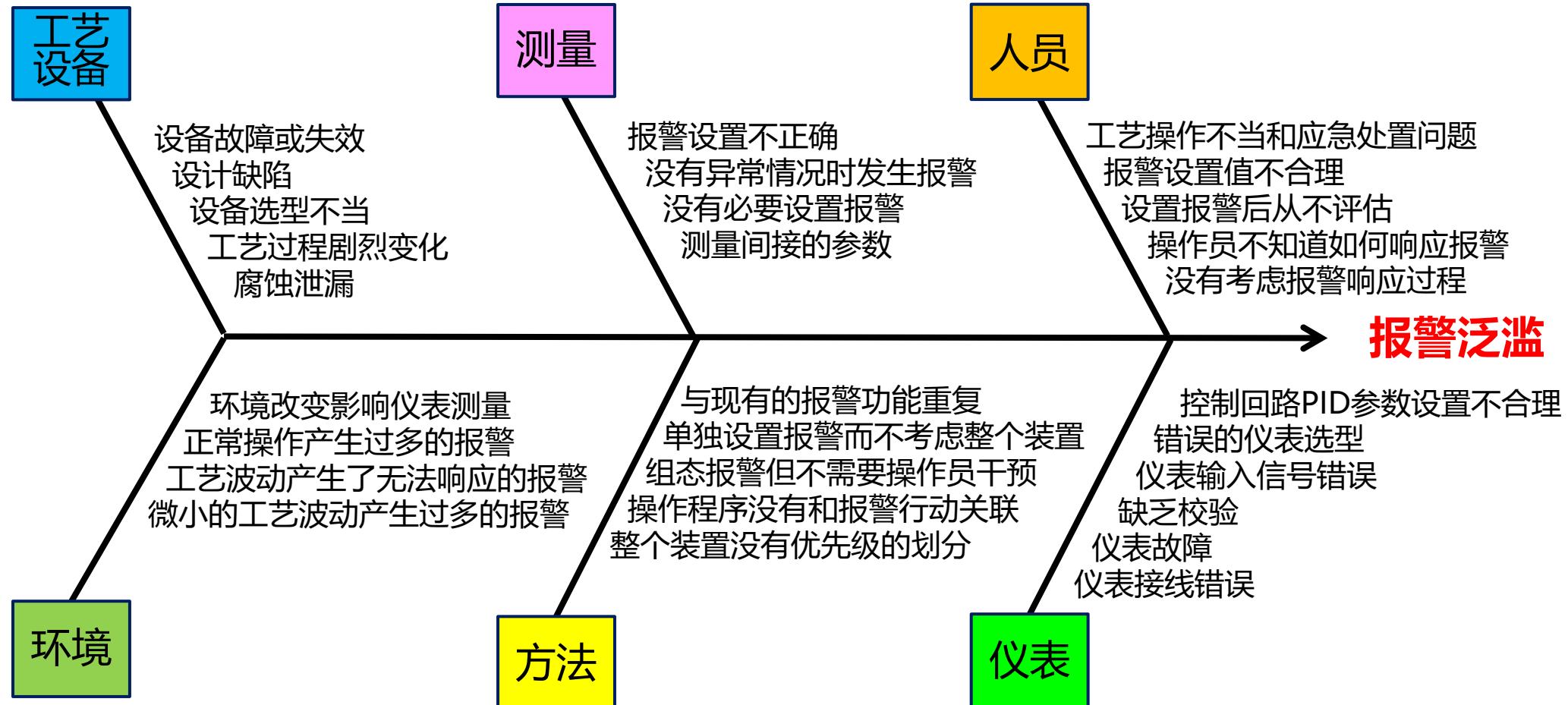
EEMUA191报警KPI指标

主要考核指标	指标量度	报警绩效指标				
		预测	高效	稳定	被动	过量
每个小时平均报警数量	报警动态指标	<6	<60	<60	<600	>600
10分钟内最大报警数量	报警溢出程度	<10	<100	<1000	>1000	>1000
10分钟内包含30个报警以上的百分比	报警溢出频率	<1%	<5%	<25%	<50%	>50%
前10个最多报警占总报警数量百分比	报警改善空间	<1%	<5%	<10%	<25%	>25%
在任何情况下保持持续报警数量	报警静态指标	<5	<10	<50	<100	>100
陈旧报警数量 (辅助指标)		0	<5	<10	<20	>20
操作员抑制的报警 (辅助指标)		<5	<10	<15	<50	>50





报警绩效基准分析，找出差距



报警泛滥原因鱼骨分析图

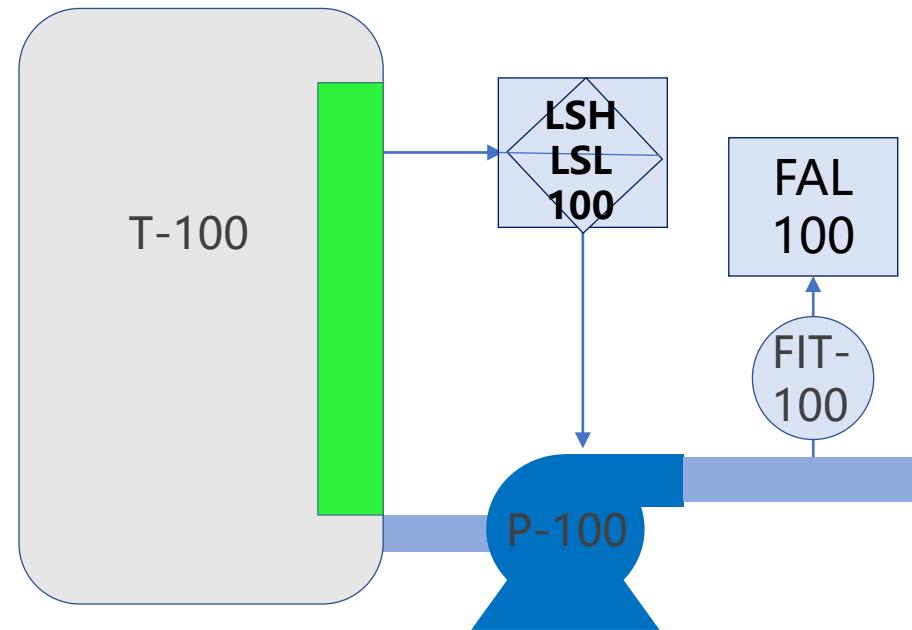
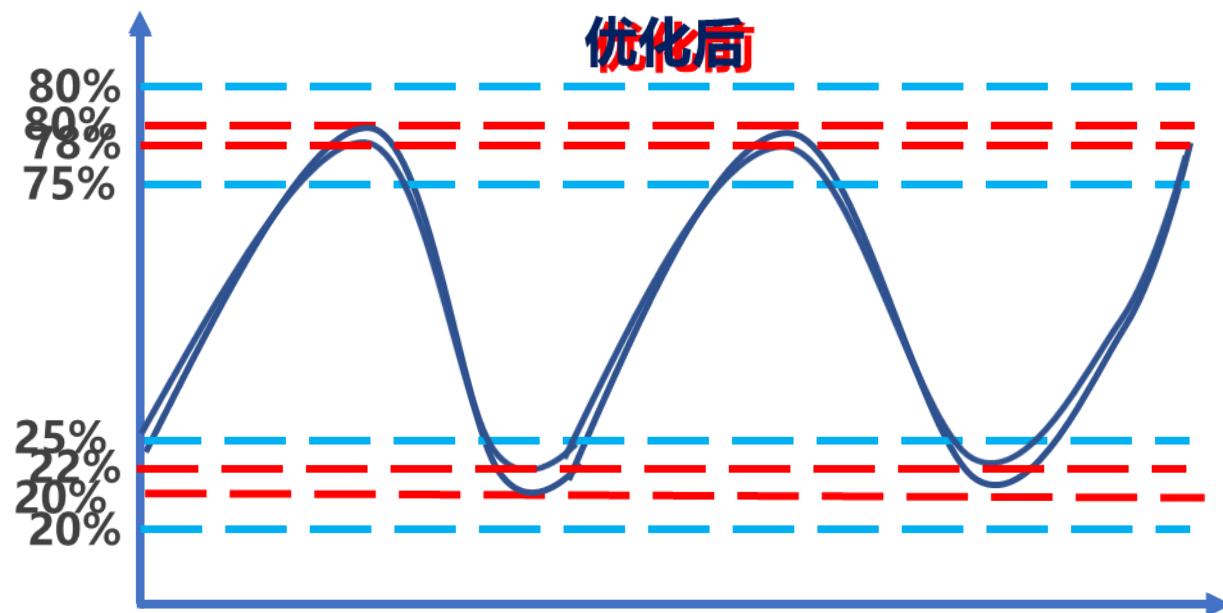


安彦咨询

改进：制定报警系统优化策略和实施

范例：优化控制逻辑

T-100液位LI100超过75%DCS高报警，当超过80%后在DCS高高报警，同时P-100泵自动启动运行，当液位低于25%时低液位报警，当低于20%时同时自动停P-100泵，导致DCS上出现大量报警。



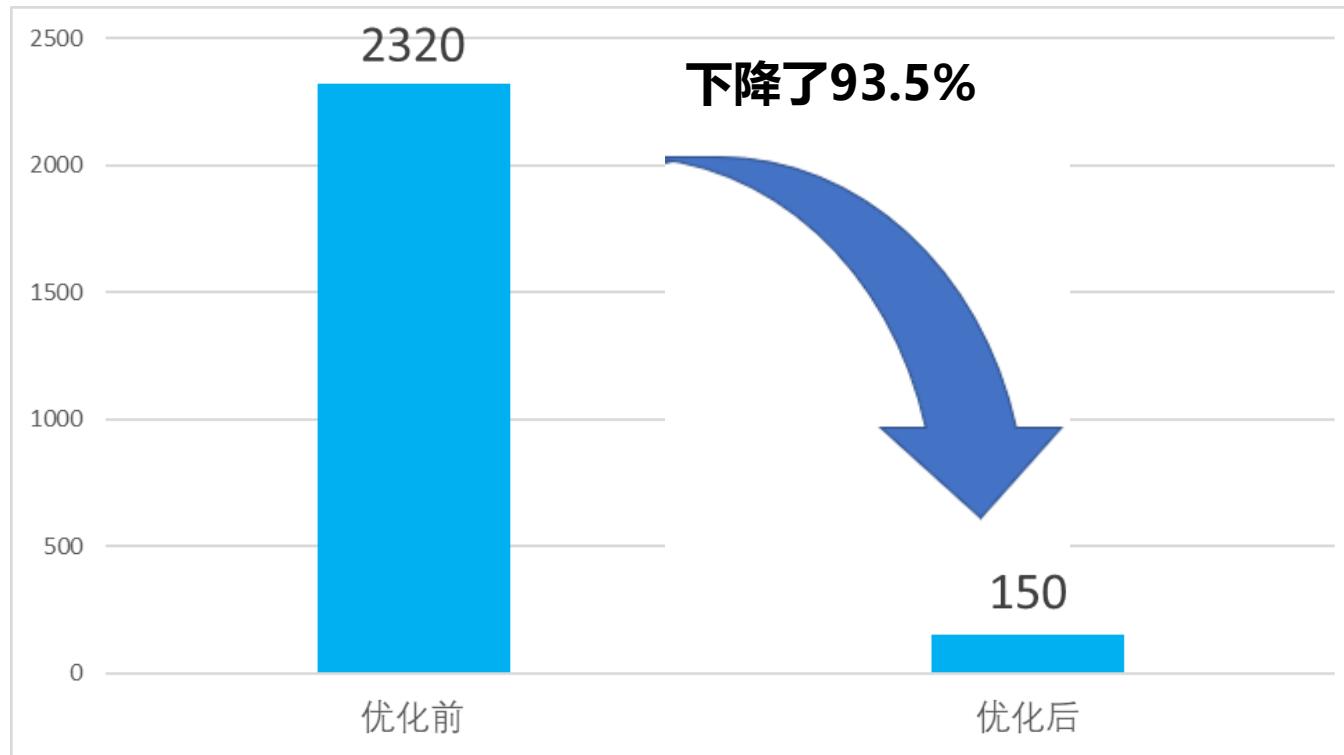


安彦咨询

制定报警优化措施和实施

通过调整和优化工艺设备操作、修复故障设备和仪表、优化工艺控制方案、工艺技术改造人员培训等措施，持续数据收集与分析，将工艺过程报警降低到合理可控水平。

报警管理改善前后对比范例（个/天）





报警管理改善流程

“化危为安” 线上讲堂

安彦咨询

持续维护和改进报警系统管理

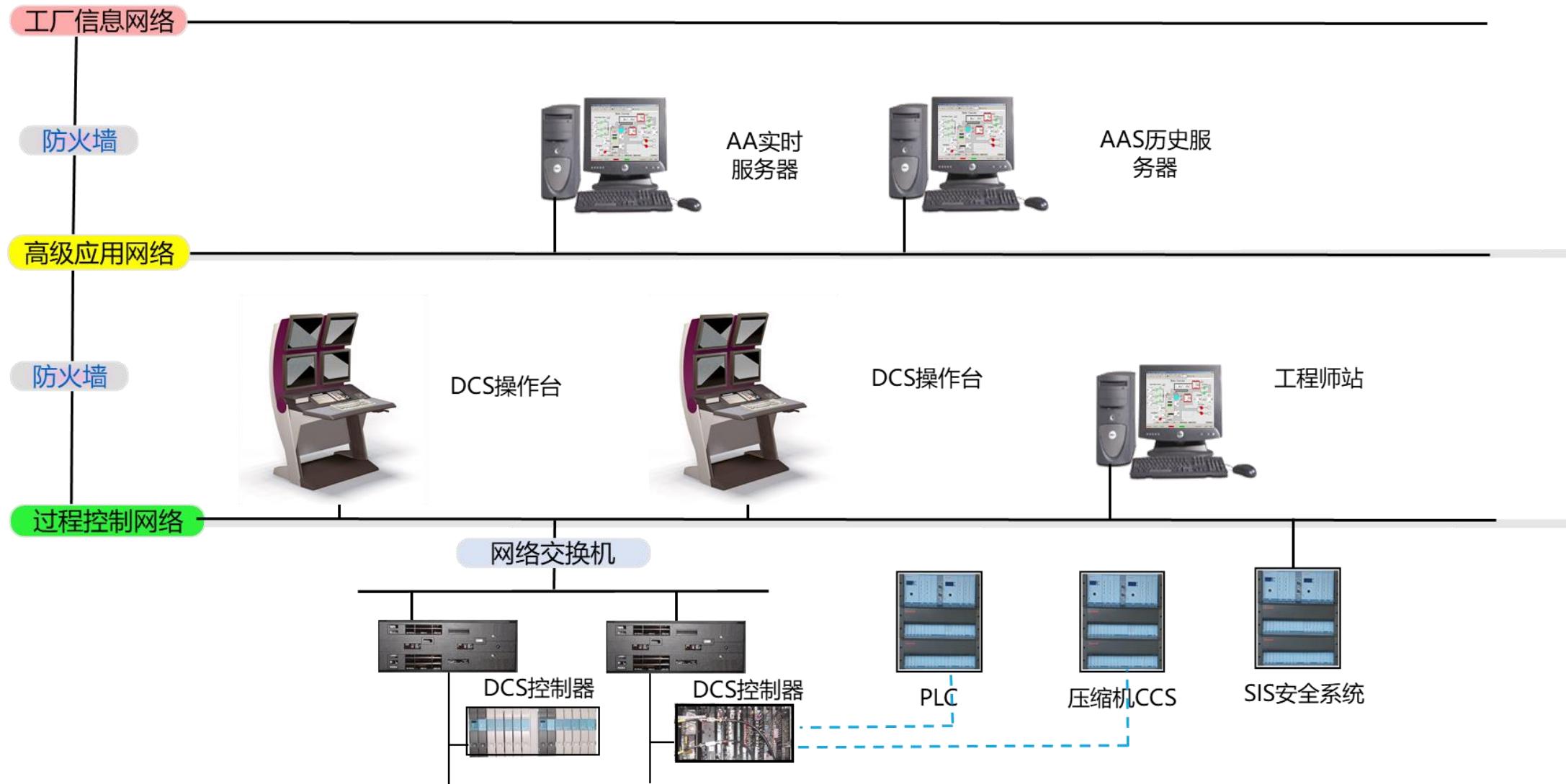
使报警系统成为操作人员可信赖的保护层，及时预警各类工艺设备异常工况，操作员快速和有效处置，杜绝重大工艺安全事故的发生。

位号	TICA-100		
描述	反应器温度控制器		
PVHHTP	125	PVHHPR	EMERGENCY
PVHITP	105	PVHIPR	HIGH
PVLOTP	80	PVLOPR	LOW
PVLLTP	70	PVLLPR	HIGH
OPHITP	--	OPHIPR	--
OPLOTP	--	OPLOPR	--
		BADPVPR	HIGH
高报警原因	1. 助催化剂量加入过多，反应过于剧烈 2. 冷却水调节阀TV-100故障 3. 冷却水泵故障PP-100不上量		
处置措施	1. 降低助催化剂流量设定值FIC-109 2. 现场检查调节阀TV-100 3. 现场检查冷却水泵PP-100		





先进报警系统AAS设计





总结

“化危为安” 线上讲堂

安彦咨询

1. 以生产技术人员为主，多专业参与报警和联锁管理改善；
2. 以重大工艺设备风险管控为核心，结合 PHA 和 HAZOP 分析技术，确保报警和联锁保护层的合理性和可靠性；
3. 规范制度标准，强化本质安全设计和运行维护管理；
4. 持续收集数据分析和改进，严格绩效考核和管理审核；
5. 工程和管理措施改进相结合，通过技术和管理措施将报警和联锁系统改造为和潜在工艺设备事故、隐患和事件密切相关的，能够提供有效信息和保护功能的可以信赖的系统。





联系信息

安彦咨询 珠海安彦企业管理咨询有限公司

联系电话：18826213299（微信同号）

地址：广东省珠海市香洲区南屏珠海大道华发新城1栋401室

邮箱：annyan@vip.126.com

网址：www.anyanzixun.cn



“化危为安”线上讲堂





安彦咨询

“化危为安”线上讲堂



“化危为安”线上讲堂



协会微信公众号



谢谢观看