# 智能制造安全一体化设想

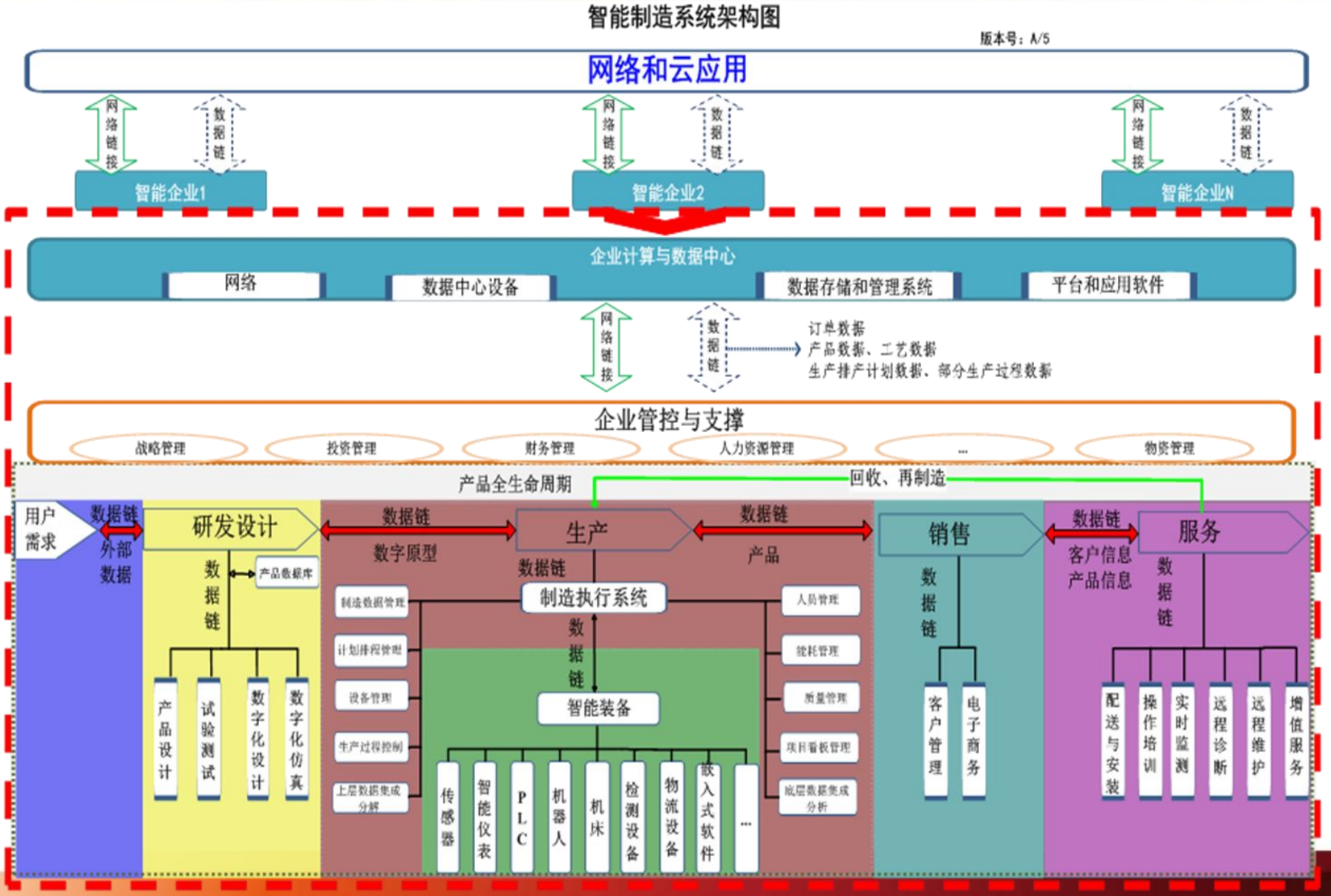
梅恪

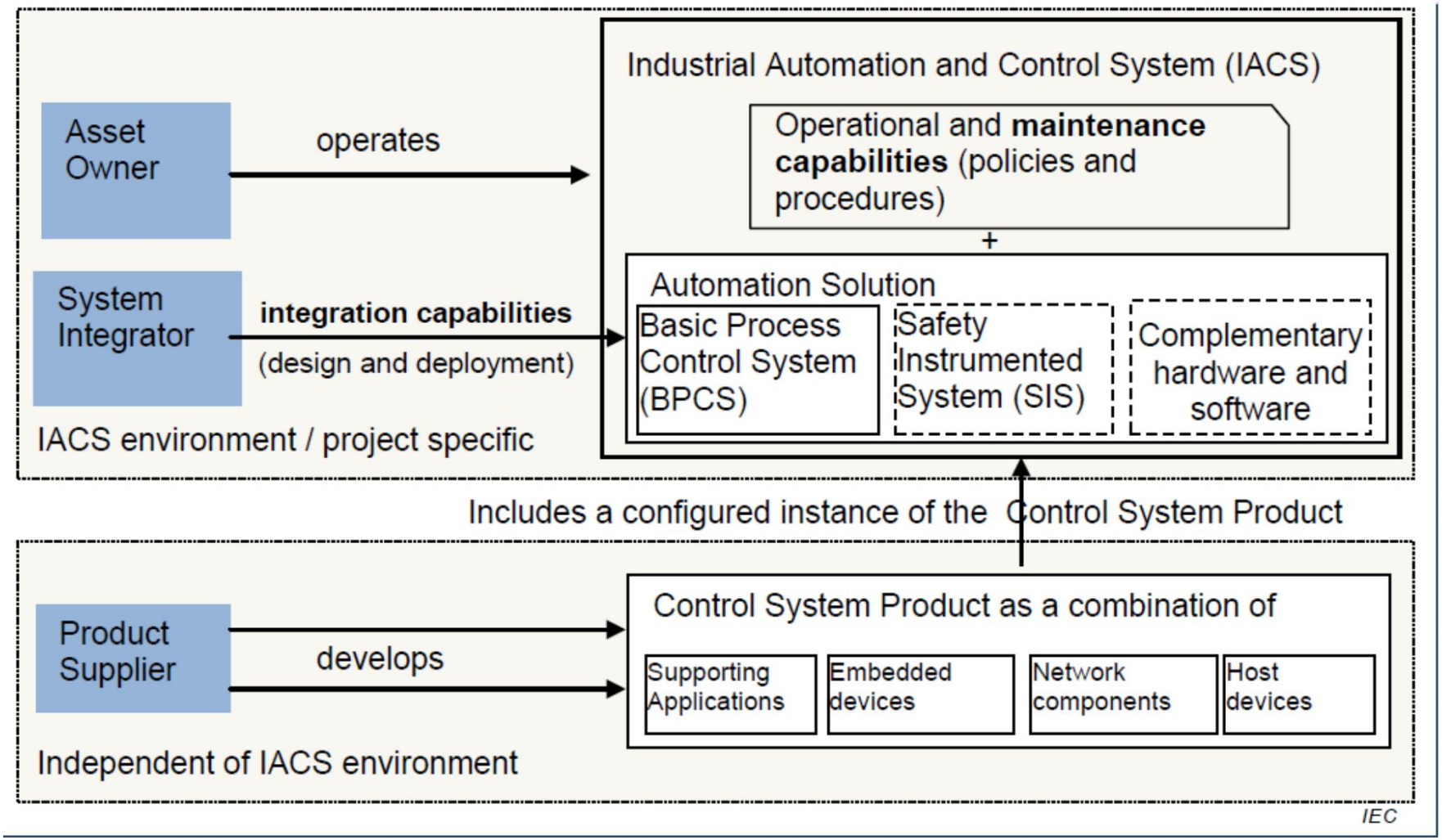
机械工业仪器仪表综合技术经济研究所（ITEI）
全国工业过程测量与控制标准化技术委员会（SAC/TC124）

一、企业安全实践

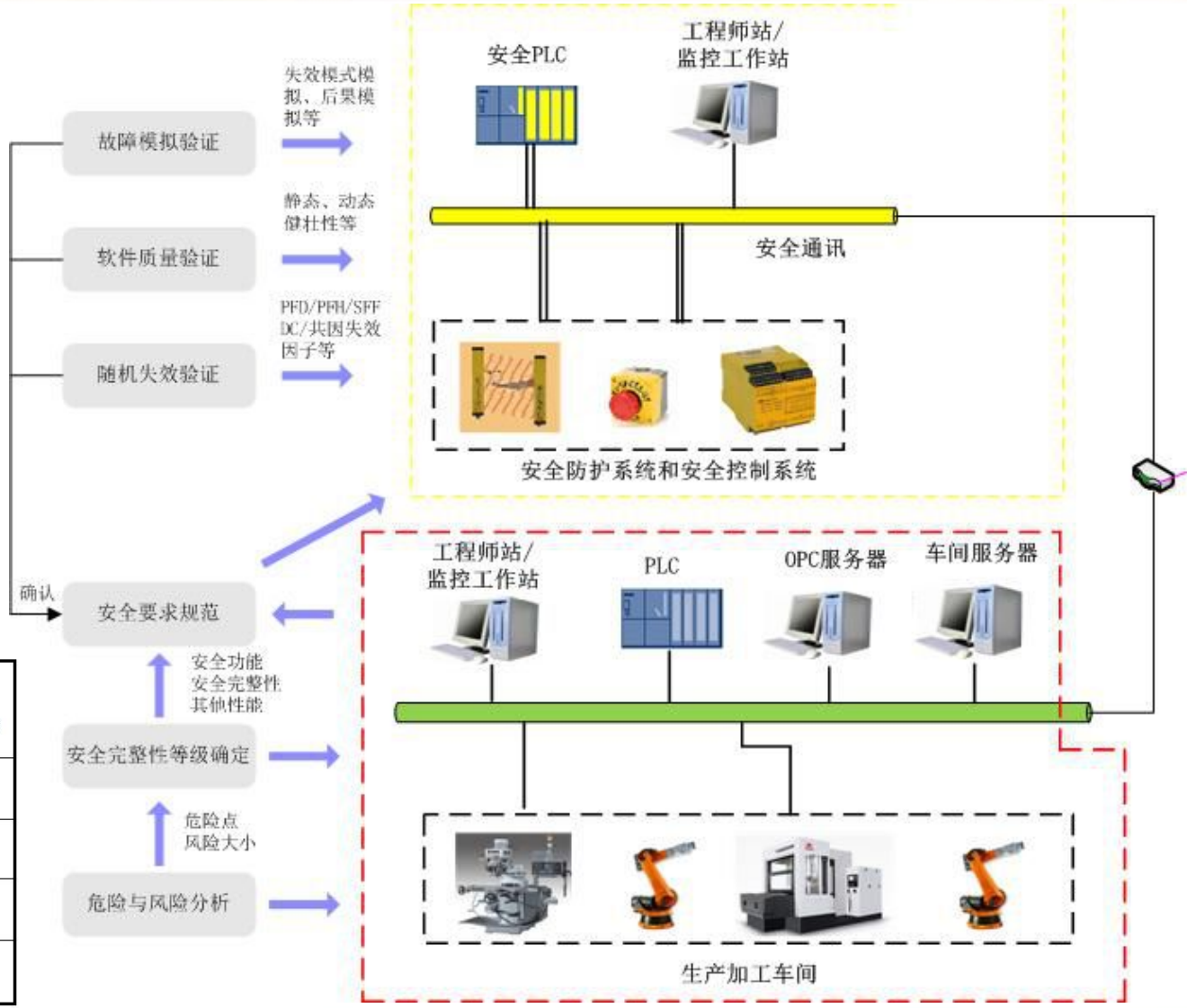
二、全安全特性

三、安全一体化思考


智能制造系统架构图
版本号：A/5
网络和云应用
网络链接
数据链
智能企业1
智能企业2
智能企业N
企业计算与数据中心
网络
数据中心设备
数据存储和管理系统
平台和应用软件
订单数据
产品数据、工艺数据
生产排产计划数据、部分生产过程数据
企业管控与支撑
战略管理
投资管理
财务管理
人力资源管理
...
物资管理
产品全生命周期
回收、再制造
用户需求
外部数据
研发设计
产品数据库
产品设计
试验测试
数字化设计
数字化仿真
数字原型
生产
制造执行系统
制造数据管理
计划排程管理
设备管理
生产过程控制
上层数据集成分解
人员管理
能耗管理
质量管理
项目看板管理
底层数据集成分析
智能装备
传感器
智能仪表
PLC
机器人
机床
检测设备
物流设备
嵌入式软件
...
产品
销售
客户管理
电子商务
客户信息
产品信息
服务
配送与安装
操作培训
实时监测
远程诊断
远程维护
增值服务


Industrial Automation and Control System (IACS)
Asset Owner
operates
Operational and maintenance capabilities (policies and procedures)
+
System Integrator
integration capabilities
(design and deployment)
Automation Solution
Basic Process Control System (BPCS)
Safety Instrumented System (SIS)
Complementary hardware and software
IACS environment / project specific
Includes a configured instance of the Control System Product
Product Supplier
develops
Control System Product as a combination of
Supporting Applications
Embedded devices
Network components
Host devices
Independent of IACS environment
IEC

- 功能安全设计




| Safety Integrity Level (IEC 61508) | Probability of dangerous failure per hour | Probability of dangerous failure per year |
|---|---|---|
| **SIL 1** | $<10^{-5}$ | $<10^{-1}$ |
| **SIL 2** | $<10^{-6}$ | $<10^{-2}$ |
| **SIL 3** | $<10^{-7}$ | $<10^{-3}$ |
| **SIL 4** | $<10^{-8}$ | $<10^{-4}$ |

- 运维诊断设计

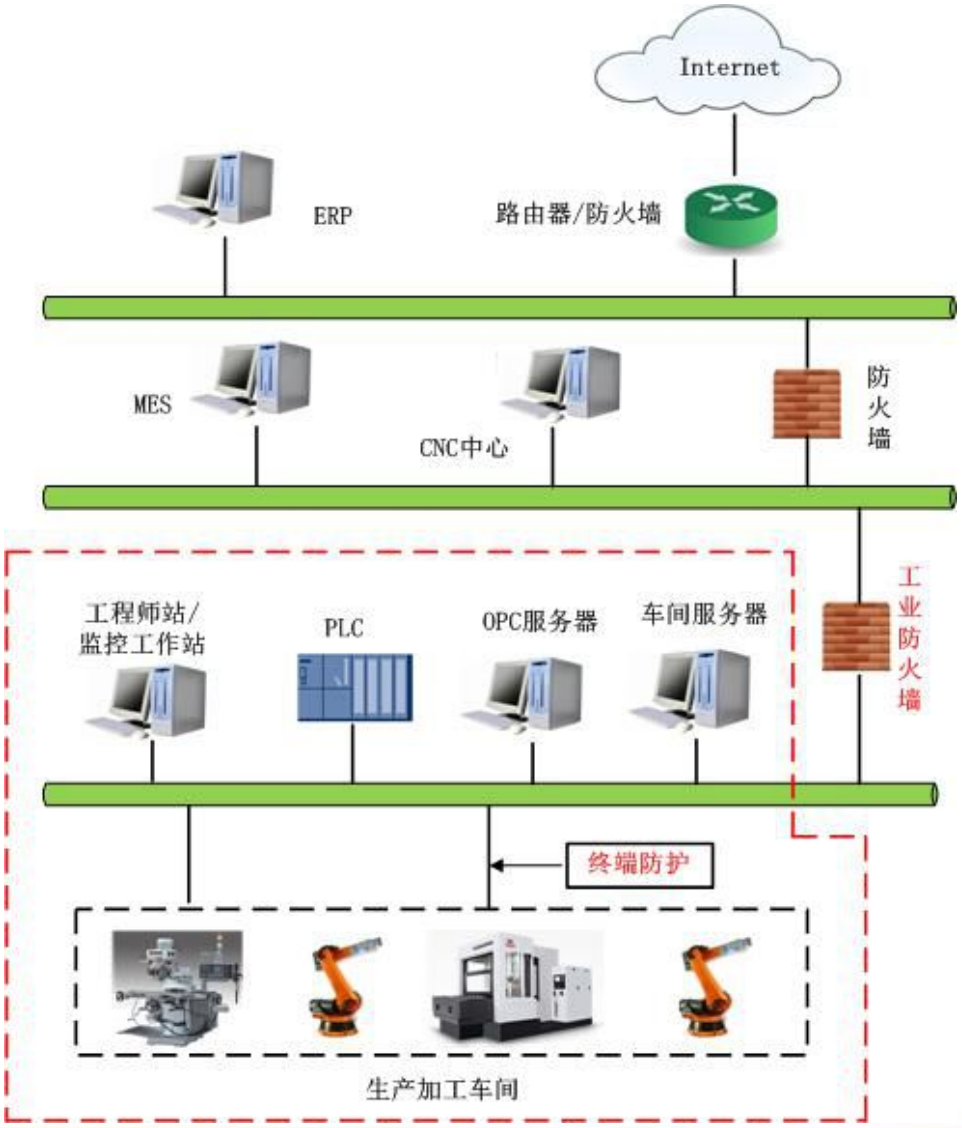

拓扑结构
网络性能
信息安全
系统脆性
系统弹性
运行质量评估与预测
硬件特性
运行状态
编码正确性
功能正确性
可靠性
可用性
可维护性
可测试性
安全性
综合保障性
运维诊断
系统仿真测试功能
环境模拟测试功能
过程仿真测试功能
PROFI BUS
PROFI NET
DeviceNet
EtherCAT
EtherNet/IP

- 信息安全设计

$R=\{D_{PLANT}+P_{FILED}+T_{IACS}+V_{IACS}\}$

其中：R风险评估结果；$D_{PLANT}$自动化程度；$P_{FILED}$工艺特性；$T_{IACS}$威胁；$V_{IACS}$脆弱性

工控信息安全风险分析结果除了依赖于IT信息安全熟知的威胁与脆弱性因素之外，还制约于工厂自动化应用水平和领域工艺特性。生产工艺流程的特性直接决定了可能发生的危险事件类型（爆炸、漏液、释放有毒气体等）；工厂自动化应用水平（全自动化、半自动化或颗粒自动化）决定了可能造成的影响的范围；威胁决定了事件发生的可能性；脆弱性决定了漏洞被利用的可能性。



# 案例1：铁岭钢厂钢包脱落事故

## Case1: Ladle fall off accident of Tieling steel mill

2007年4月18日，铁岭钢铁厂。脱落钢水包口直对着工人开会的小屋，很多钢水被灌入小屋，32名工人死亡 。事故直接原因：功能失效

# 案例2 Case 2

- 2015年6月29日， 德国汽车制造商大众位于保纳塔尔的工厂发生意外，一名22岁的工人被机器人抓住，挤向了一块金属板，不幸身亡。

# 案例3 伊朗核设施受攻击事件

- 2010年9月，Stuxnet（震网）病毒攻击伊朗重要工业设施，包括布什尔核电站

安全保护功能失效

- 形成第二类危险源
- 实际风险超过可接受风险，出现“不安全”状态。

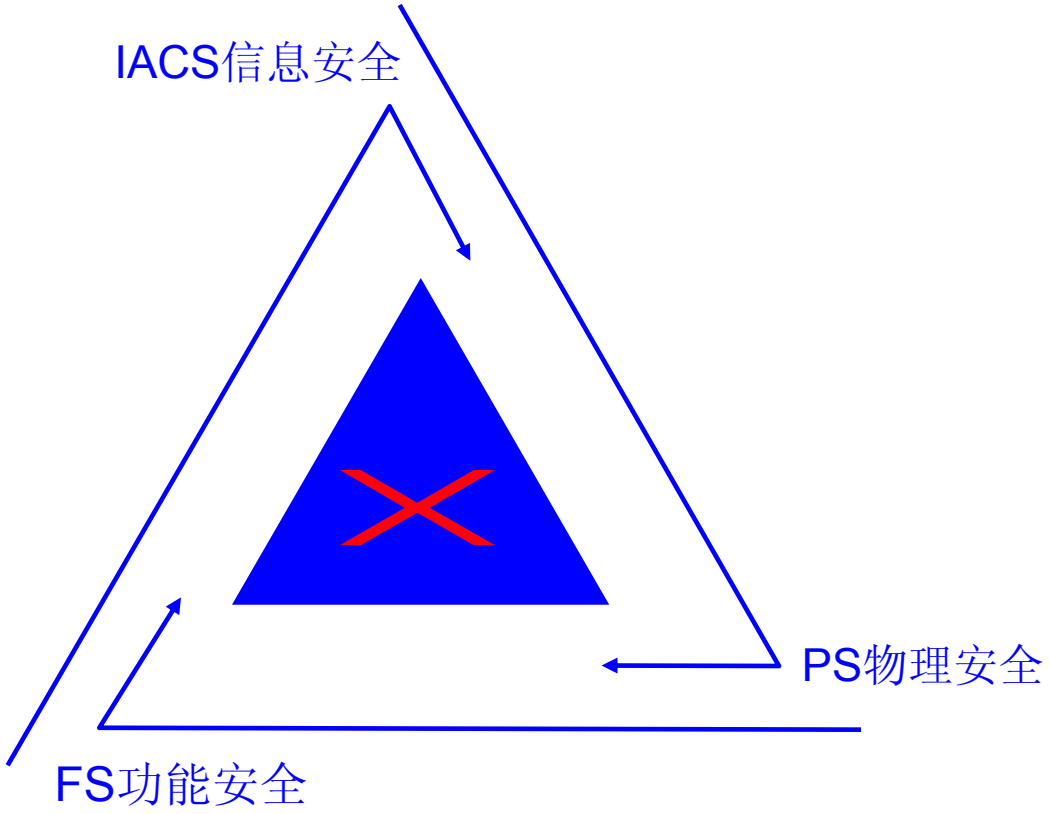
安全控制功能错乱

- 危险立即产生事故。

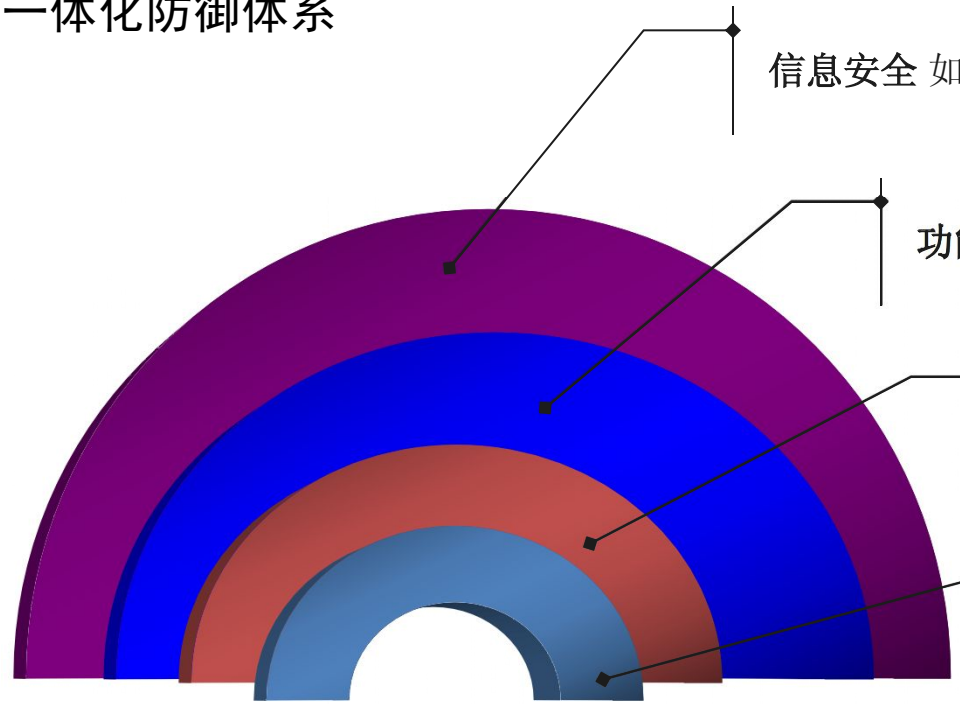
控制功能失控

- 失控，导致 破坏、危险。

在企业安全框架内，必须保证系统功能不会失效（失控）


IACS信息安全
PS物理安全
FS功能安全

# 一体化防御体系

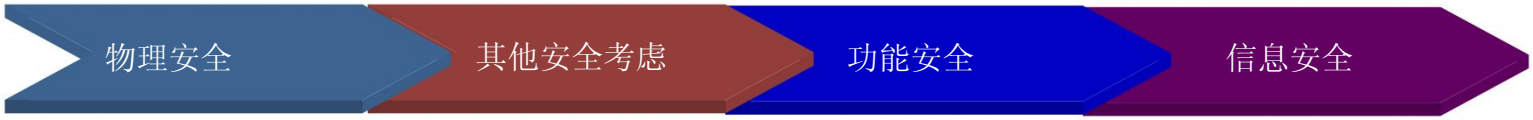


**信息安全** 如：CSMS、探测与防护.

**功能安全** 如：安全联锁、SIS

**其他安全** 如：防爆.

**物理安全** 如：电气、机械、火焰.




# 安全一体化


安全一体化产品

智能安全传感

智能安全执行

智能安全控制

防火墙

网闸

……

安全一体化系统集成和应用

安全一体化集成系统

智能安全防护系统

智能安全控制系统

智能安全检测系统

智能安全监视系统

安全一体化应用单元

设备状态检测与预警

智能巡检

应急联动

……

安全一体化运维管理

产品级安全运维管理

系统级安全运维管理

车间/厂级安全运维管理

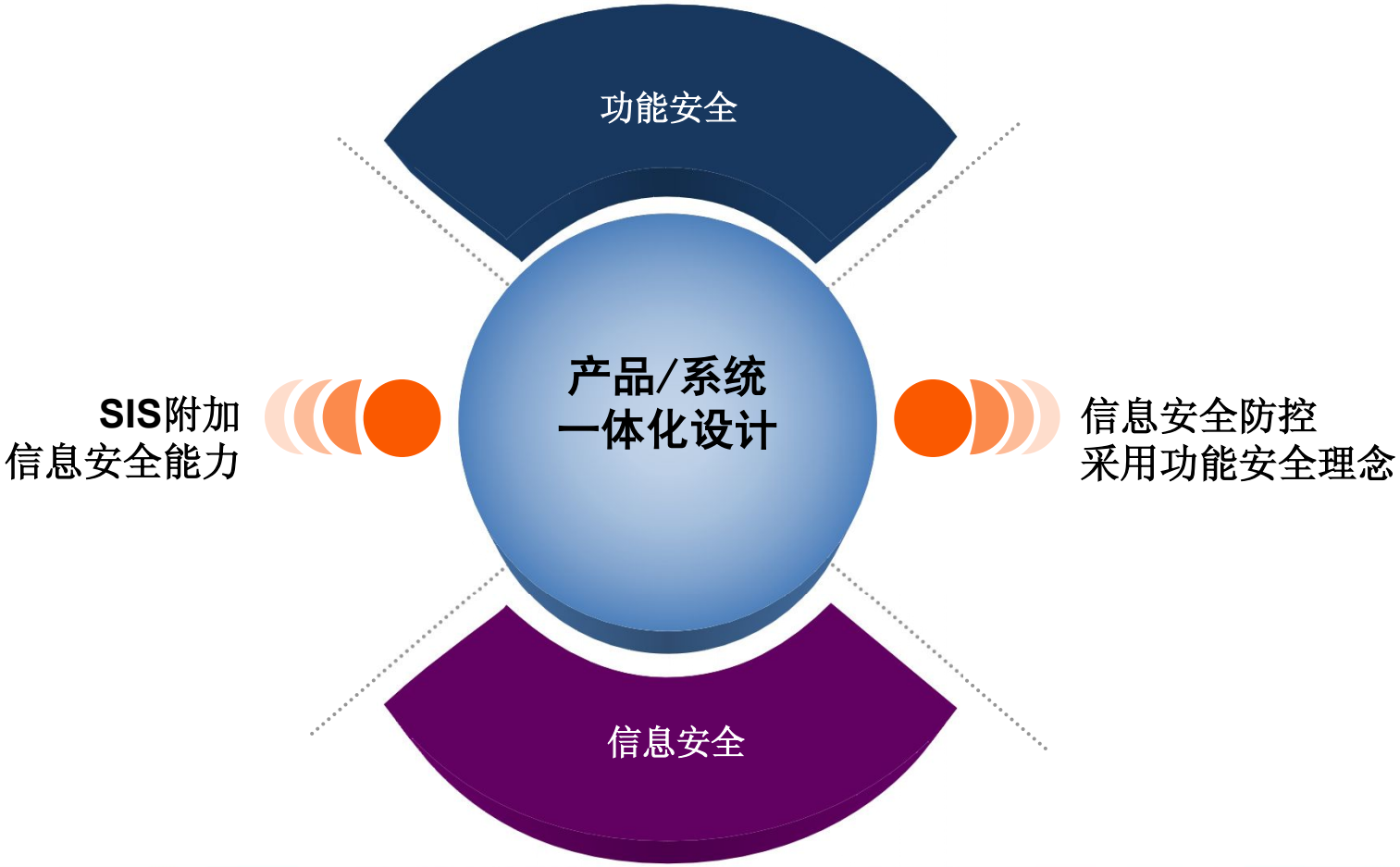
安全一体化测评

产品安全性能测评

集成系统的安全能力测评

运维管理体系安全有效性评估

# 产品/系统设计理念



# 谢 谢

# Thanks