



工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

工业控制系统安全一体化技术

汇报人：机械工业仪器仪表综合技术经济研究所 史学玲教授
汇报日期：2019年5月9日

演讲者介绍

- 史学玲
- 国家安全生产专家组成员
- 机械工业仪器仪表综合技术经济研究所 (ITEI) 副总工程师
- IEC TC65 中国专家
- SAC/TC124/SC10 系统及功能安全标准化技术委员会副主任委员
- 全国机械安全标准化技术委员会委员
- 全国电气安全标准化技术委员会委员
- 全国电工电子可靠性与维修性标准化技术委员会委员

主要内容

一、工业安全与安全一体化

二、工业控制系统安全一体化技术

三、标准体系规划

四、成果验证

工业安全（safety）

工业：石油、化工、冶金、电力、机械、运输.....



工业是一类特殊的关键基础设施：

关键基础设施是指那些对国家来说非常重要的系统和资产，其遇到的任何瘫痪或损毁将对国家安全、国家经济安全和/或国家公众健康和安全生产产生巨大的破坏性影响

工业安全（**Safety**）：工业设施与系统没有不可接受的风险

•风险：

- 人身伤害
- 财产损失
- 环境破坏
- 声誉影响



工业安全与安全一体化

工业安全(Safety)技术发展历程



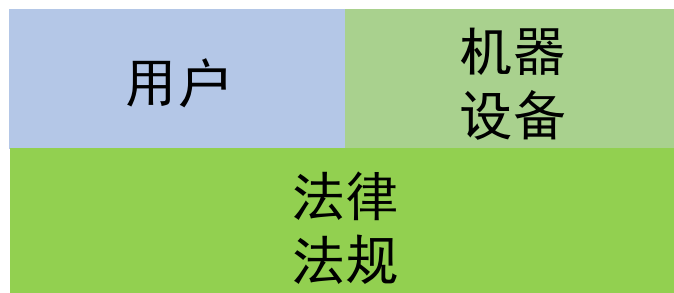
工业安全技术随着工业化进程不断更新，但安全问题极为复杂，导致安全生产事故防不胜防。

工业安全与安全一体化

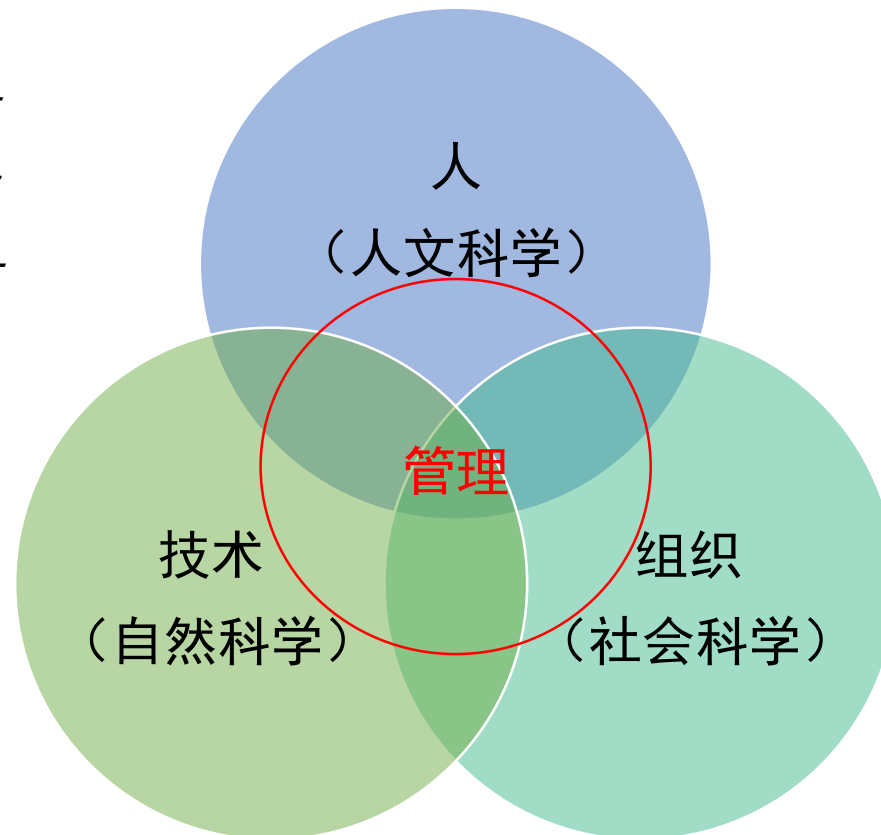
什么是工业的安全一体化？

基于人、物、环境有效协同获得的安全

能自动检测、智能识别工业生产过程中机器装备、环境的危险状态，随时掌握人的动作和能力，综合使用多个领域、多门学科技术，建立人、物和环境的协同关系，把风险控制在可容忍水平



用户在轻松愉悦的环境中获得本质安全



工业安全与安全一体化

工业的安全一体化前景

- 智能安全
- 法律法规自符合
- 环境自适应
- 动态安全距离监测
- 人员能力分级
- 设备能力分级
- 工作职责分配到每天和每个人
- 识别并控制了所有风险
- 动态的风险评估与控制

主要内容

一、工业安全与安全一体化

二、工业控制系统安全一体化技术

三、标准体系规划

四、成果验证

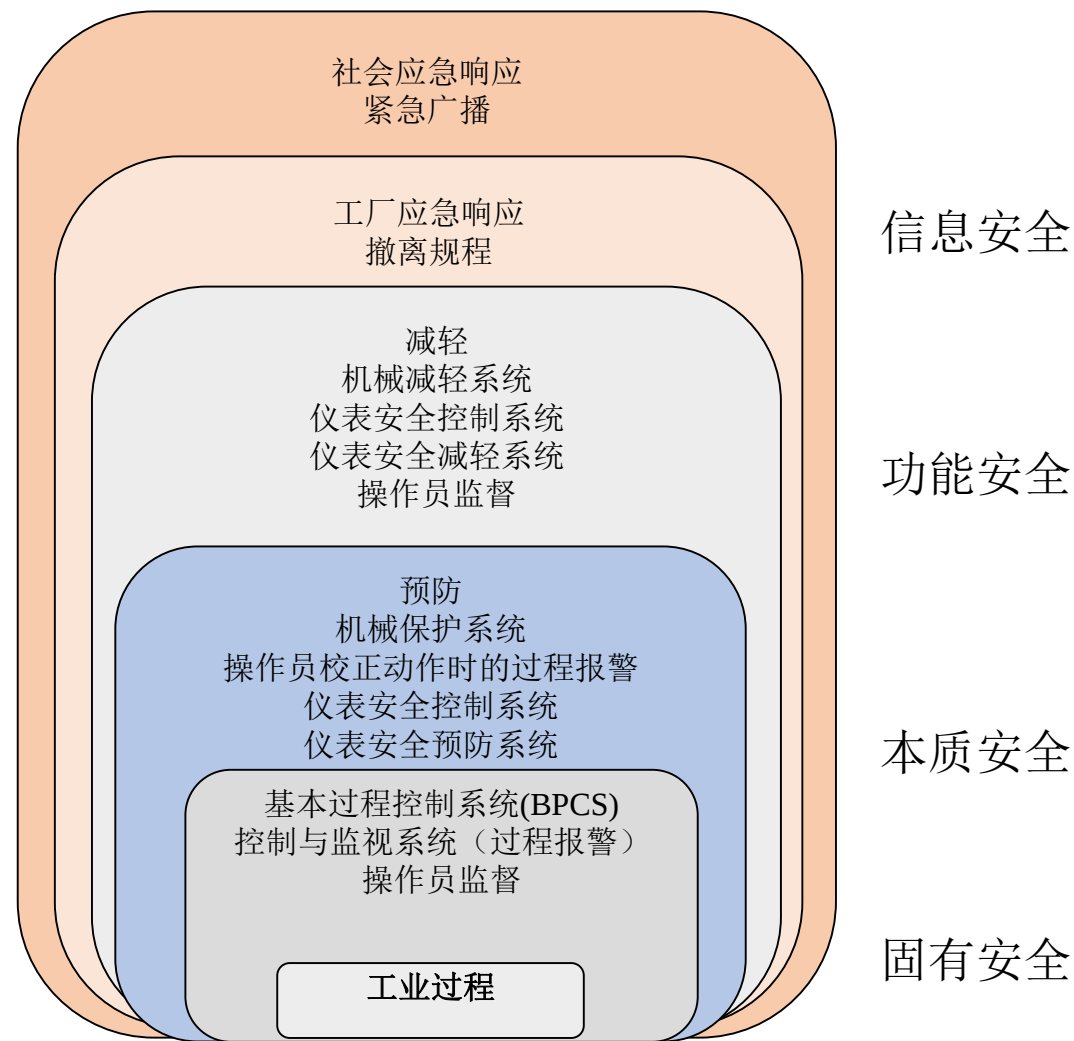
工业控制系统的安全一体化技术

工业安全（safety）与工业控制系统：

工业中使用两类不同的控制系统：

1. 工业过程控制**BPCS**
2. 功能安全防护系统
 - 预防系统
 - 减轻系统
 - 撤离系统

综合使用，实现工业生产过程本质安全



工业控制系统的安全一体化技术

- 工业控制系统的功能失效可能导致灾难
- 安全保护系统功能失效
 - 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
 - 出现事故概率很高
 - [事故案例1](#)
- 安全控制系统功能失效
 - 危险立即产生事故[案例2](#)
- 工业控制系统功能失控
 - 失控，导致 破坏、危险
 - [事故案例3](#)

事件1：2005年3月23日，BP公司在美国德州的炼油厂在开车过程中发生了多起爆炸事故，造成15人死亡，170多人受伤。
分析：事故直接原因是液位计失灵。

事件2：2017年5月17日，美国加利福尼亚州一名特斯拉Model S车主在开启了自动驾驶状态下撞上前方转弯的卡车不幸身亡。

分析：由于卡车涂装为纯白色，在强烈反光下，Tesla车载摄像头未能将这辆开车从天空背景中识别出来。

信息安全不但依赖技术，还依赖-适当的国家战略、健全的政策、全面的法律框架等。

要让技术在安全的框架内发展，必须实现功能安全

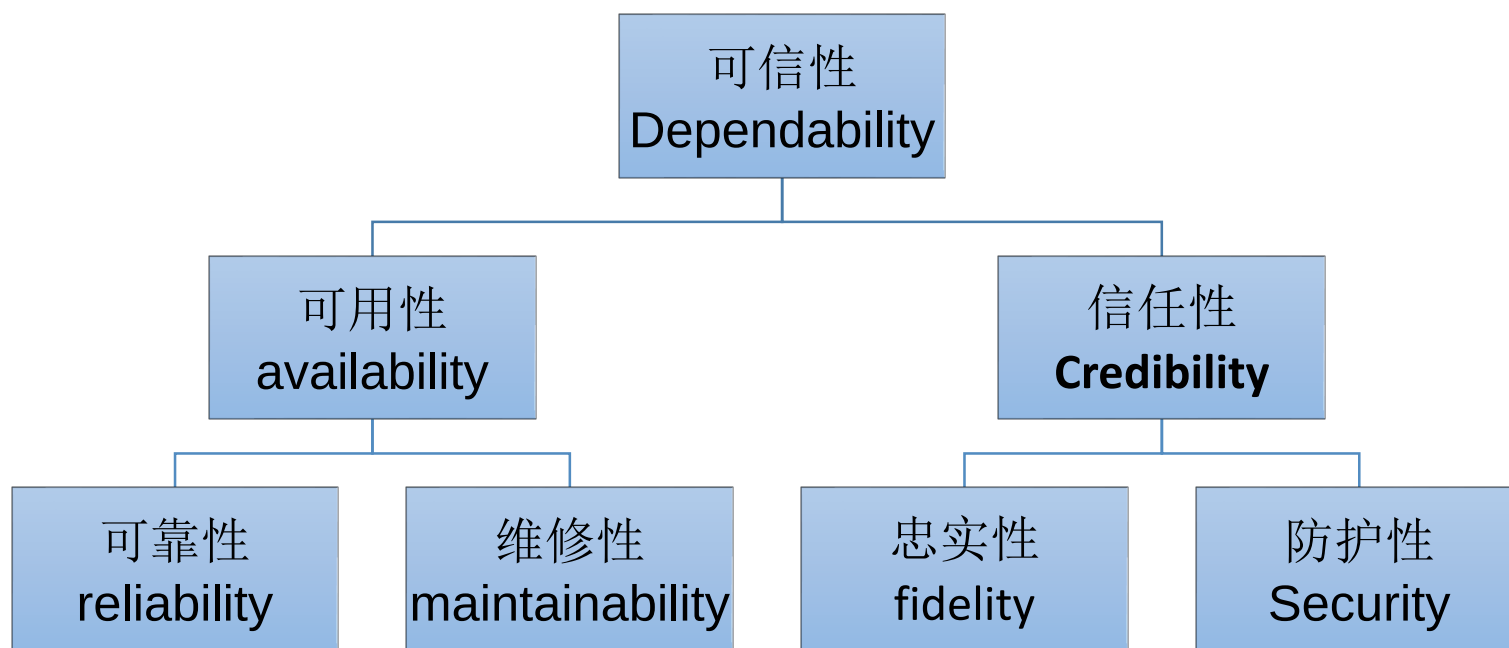
工业控制系统的安全一体化技术

- 目标:

- 正确建立系统安全功能案例4
- 用高可信的系统实现安全案例5

关键技术:

- 信息安全
- 新技术引入后的风险识别与控制
 - 大数据、大系统
 - 互联互通
 - 人工智能
- 新产品的失效模式与MTBF数据
- 复杂系统的使用维护
- 第三方监管
 - 标准与检测认证



工业控制系统的安全一体化技术

整体技术概况



证明安全的技术

- 审核
- 评估
- 验证
- 确认

标准与检测认证

组成安全的技术

- 智能设备
- 子系统
- 系统产业链

产业提升和技术进步

(IEC61882, IEC61508 (GB/T20438), IEC61511 (GB/T21109), GT/T30976, IEC62443)

主要内容

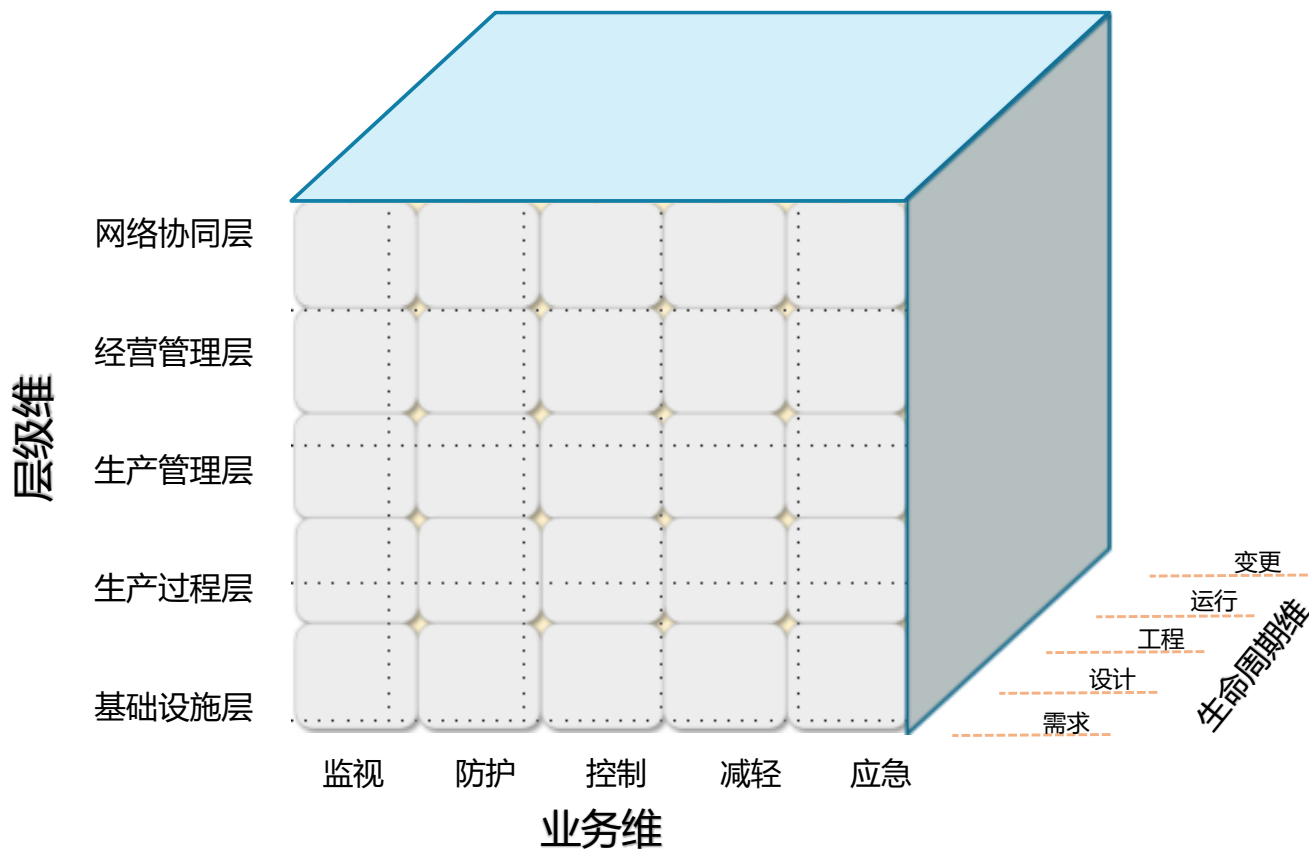
一、工业安全与安全一体化

二、工业控制系统安全一体化技术

三、标准体系规划

四、成果验证

安全一体化技术标准体系规划



《数字化车间 功能安全要求》
《数字化车间 信息安全要求》

.....

《智能工厂安全一体化 第1部分：
一般要求》

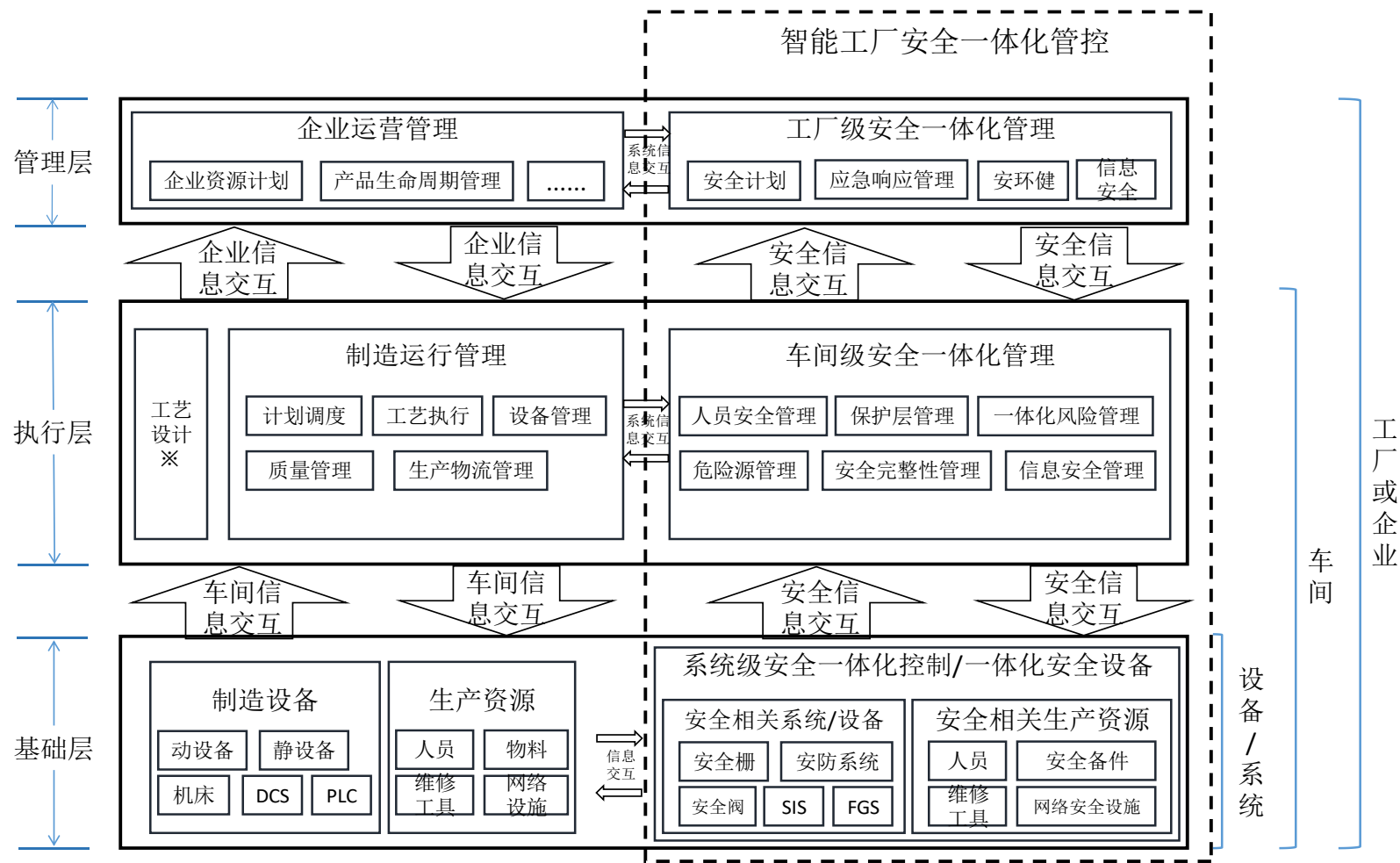
《智能工厂安全一体化 第2部分：
风险评估要求》

《智能工厂安全一体化 第3部分：
系统协同设计要求》

《智能工厂安全一体化 第4部分：
系统评测要求》

.....

安全一体化标准系列



——第1部分：一般要求

旨在定义和规范智能工厂安全一体化架构和一体化安全要素，为智能工厂一体化安全设计、实施、运行和维护提供指导。

——第2部分：风险评估要求

建立并规范智能工厂安全一体化风险评估的内容和流程。

——第3部分：系统协同设计要求

规范安全相关控制系统的信息安全设计集成应遵循的原则和具体要求。

——第4部分：系统评测要求

建立和规范安全一体化完善度指标的评测方法和流程。提出具体评测要求。

主要内容

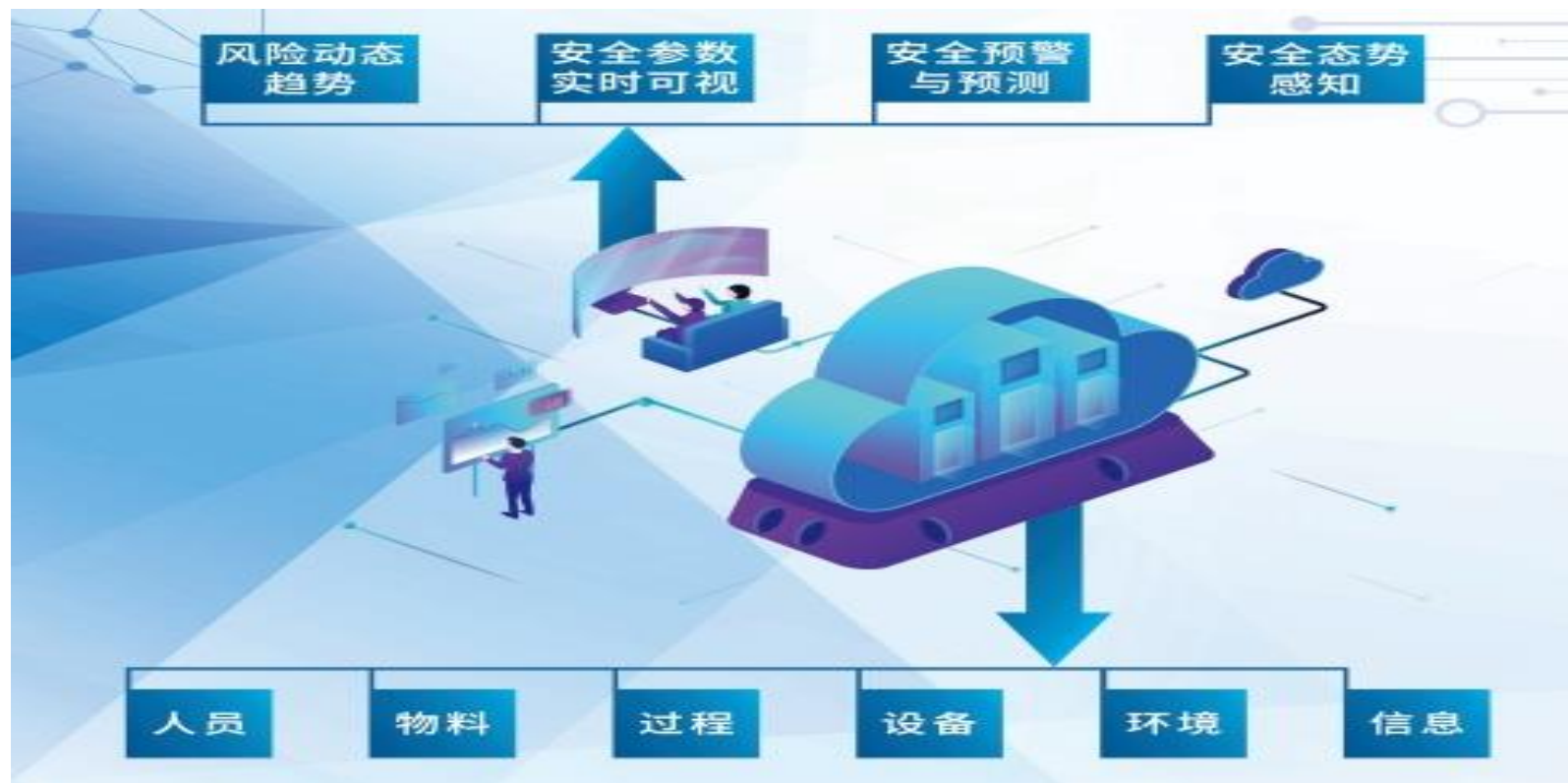
一、工业安全与安全一体化

二、工业控制系统安全一体化技术

三、标准体系规划

四、成果验证

安全一体化智能管控系统

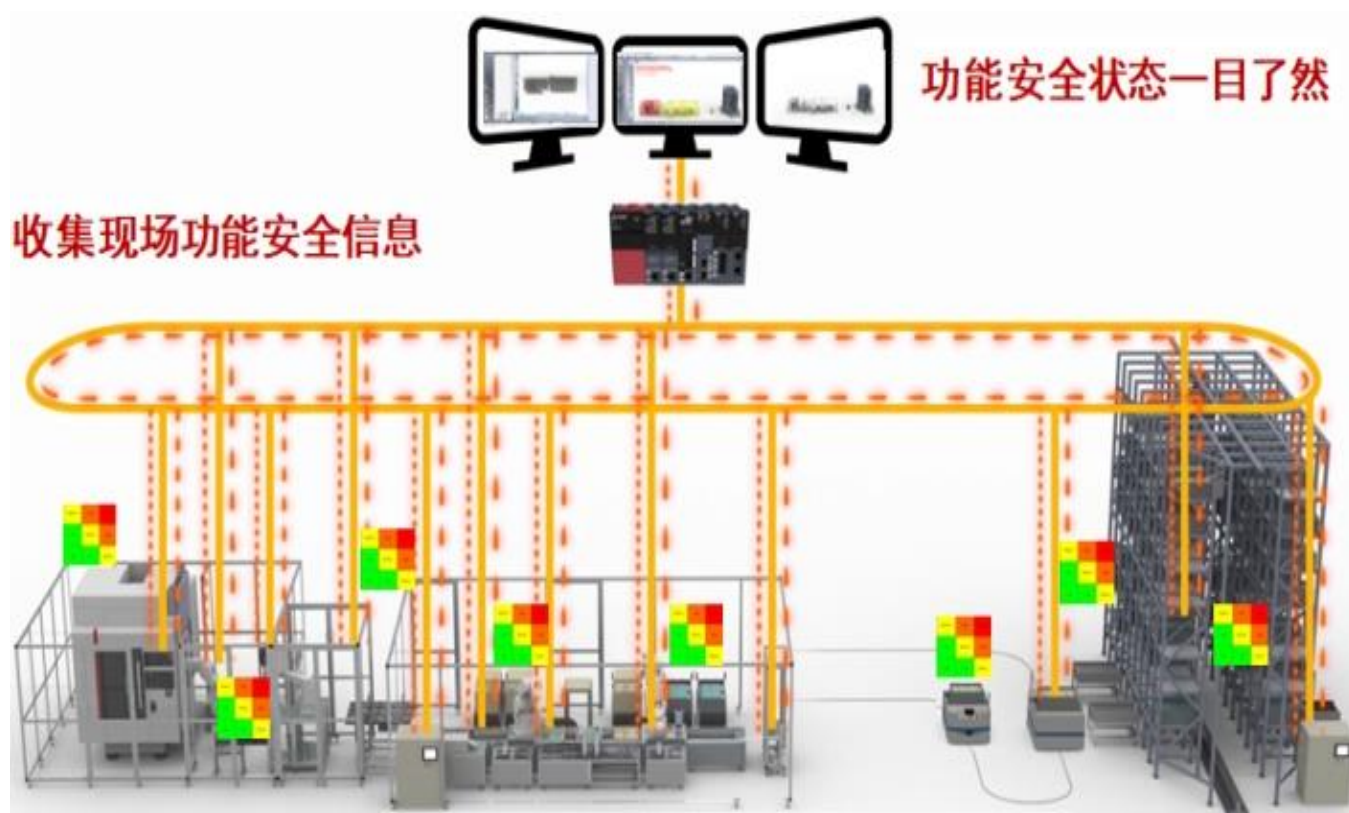


基于风险建模，将物联网的泛在感知、计算机信息技术的数据挖掘和智能分析等有机融合，构建实时、可视、可预测、可追溯、精准控制、精细管理的安全风险管控系统，实现风险管控智能化提升。

机械工业仪器仪表综合技术经济研究所
安全一体化智能管控系统

试验验证平台

安全一体化标准研究成果在机械工业仪器仪表综合技术经济研究所智能制造综合标准化试验验证平台上开展了试验验证



将信息安全态势感知与功能安全风险动态趋势结合



工业控制系统
信息安全产业联盟

Thanks