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

构建自主可信防护体系 护航工业生产转型升级

汇报人： 和利时信息安全研究院 颜培
汇报日期： 2020年5月14日

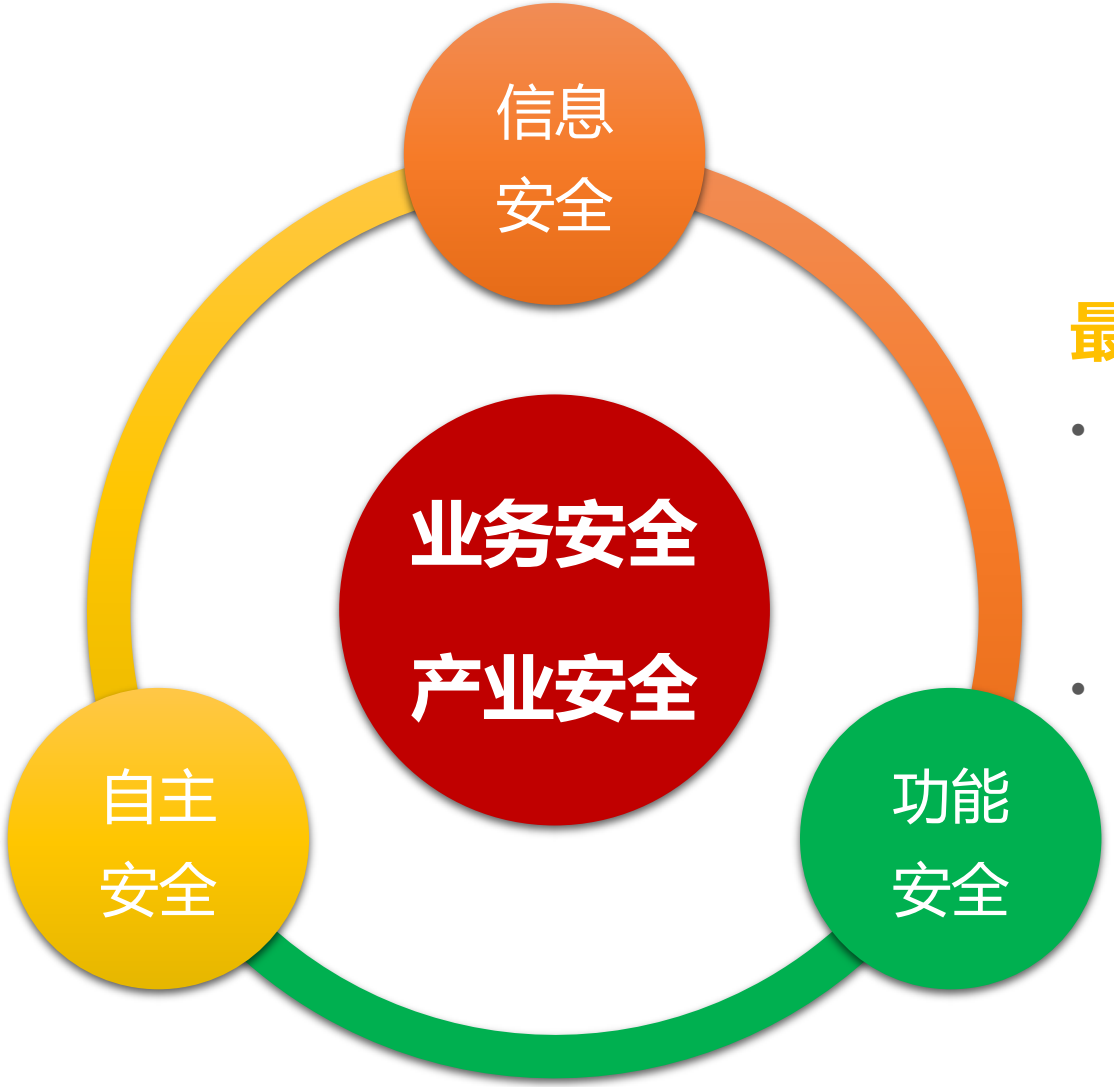
业务安全一体化的综合防护体系

纵深防护信息安全

- 多区域多边界的防护结构
- 形成控制系统的网络防护屏障

核心系统内生安全

- 基于自主的可信计算架构，构建核心工业自动化与信息系统的安全
- 自主免疫，动态防护，控制中有安全，安全中有控制



最终目标功能安全

- 信息安全主动防护体系配合功能安全系统构建全面综合防护体系
- 将控制设备安全、操作管理安全、工艺逻辑安全、网络信息安全相互融合，实现业务整体安全

等级保护2.0下的网络安全体系

适用于工业的信息安全核心技术

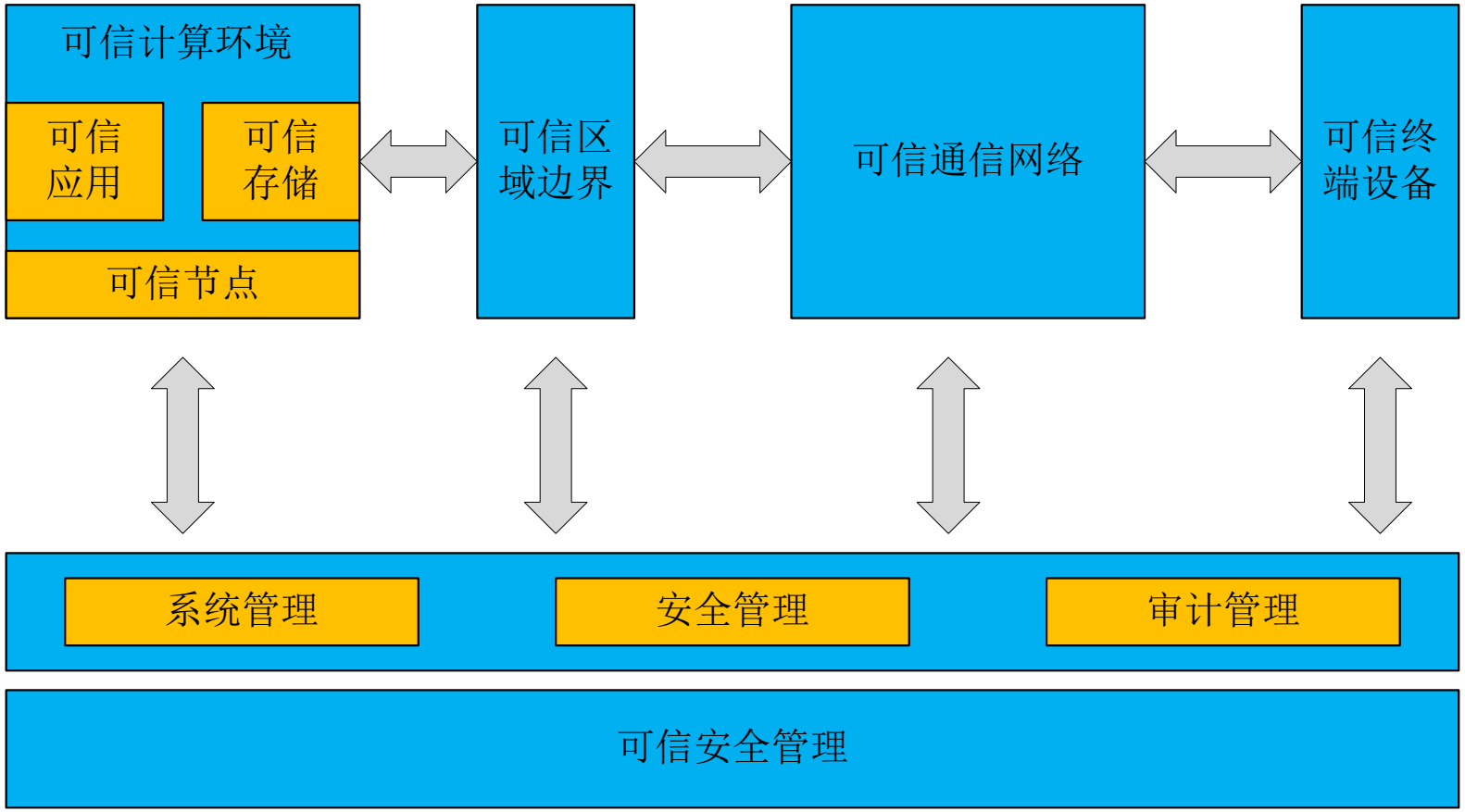
可信计算驱动的主动安全防护技术

- 传统的安全防护技术无法完全保障工业网络安全
- 基于可信计算构建的主动安全技术更适用于工业控制系统

类别	已知攻击行为				未知攻击行为	控制指令伪造行为
	拒绝服务攻击	远程代码执行	访问权限获取	信息窃取威胁		
防火墙技术	√	X	部分有效	X	X	X
入侵检测技术	√	X	部分有效	X	X	X
漏洞扫描技术	仅发现漏洞	仅发现漏洞	仅发现漏洞	仅发现漏洞	仅发现漏洞	X
可信计算主动防护技术	√	√	√	√	√	√

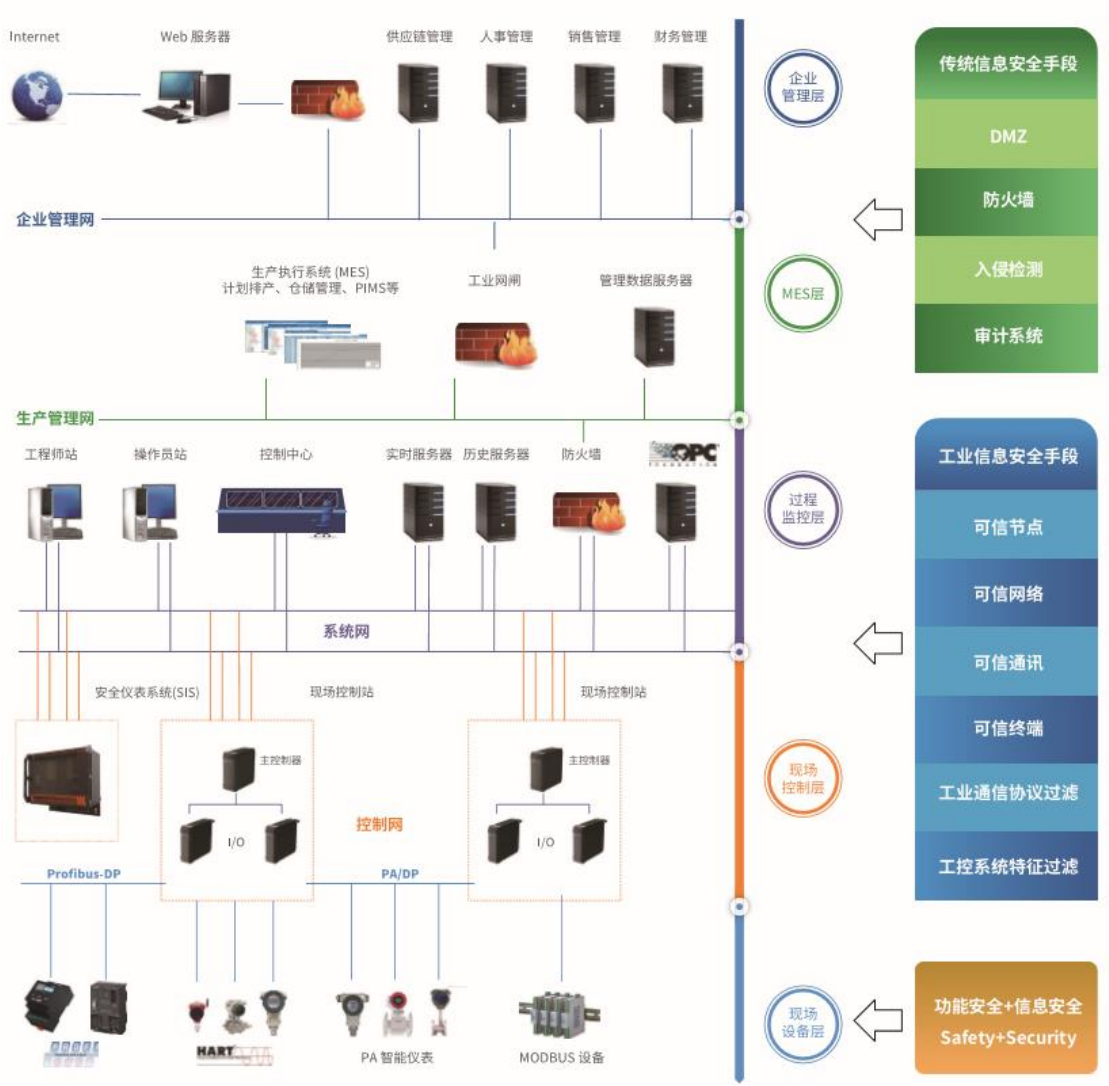
基于可信计算的主动安全免疫

主动安全免疫三重防护框架



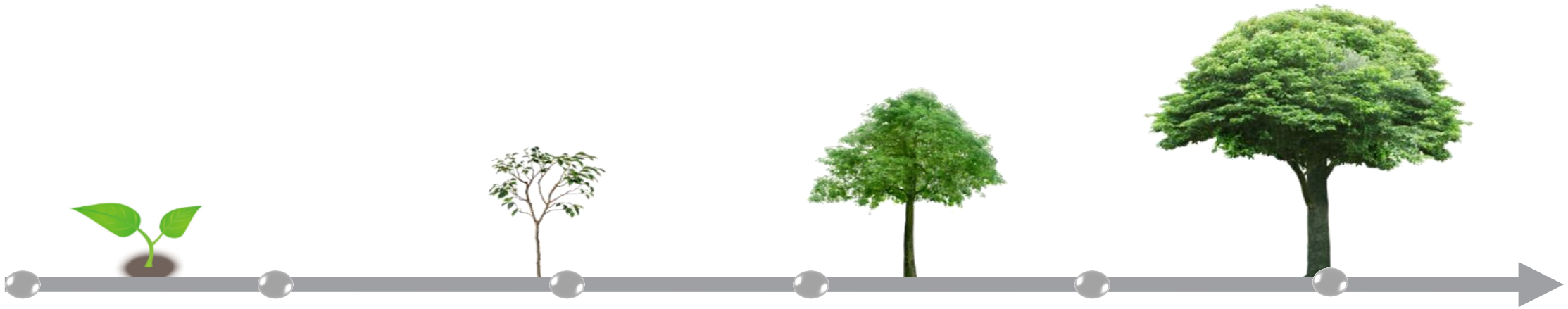
- 国密算法
- 轻量级加解密
- 数字证书体系
- 身份认证和访问控制
- 主动安全防御

工业信息安全解决方案



- 工业信息安全产品技术辅之以传统IT信息安全手段，并融合功能安全设计，通过全生命周期安全管理（产品研发、工程设计、后期服务）确保系统运行安全。
- 结合电力能源、化工石化、轨道交通、装备制造等应用场景特点的各行业综合安全建设保障整体解决方案

和利时工业信息安全发展历程



2012年

- 设立工业信息安全工作组
- 开展工业控制系统网络安全脆弱性研究

2013年

- 参与国家多项工业信息安全技术标准的制订工作
- 推出多款工业信息安全产品并批量应用

2015年

- 牵头国家科技部863项目“可编程嵌入式电子设备安全防护技术”，实现工控系统内生安全关键技术突破

2017年

- 工业通信健壮性技术取得关键突破，完成PLC、DCS、核电仪控系统等安全技术改造，陆续取得此类Achilles II级国际最高认证

2018年

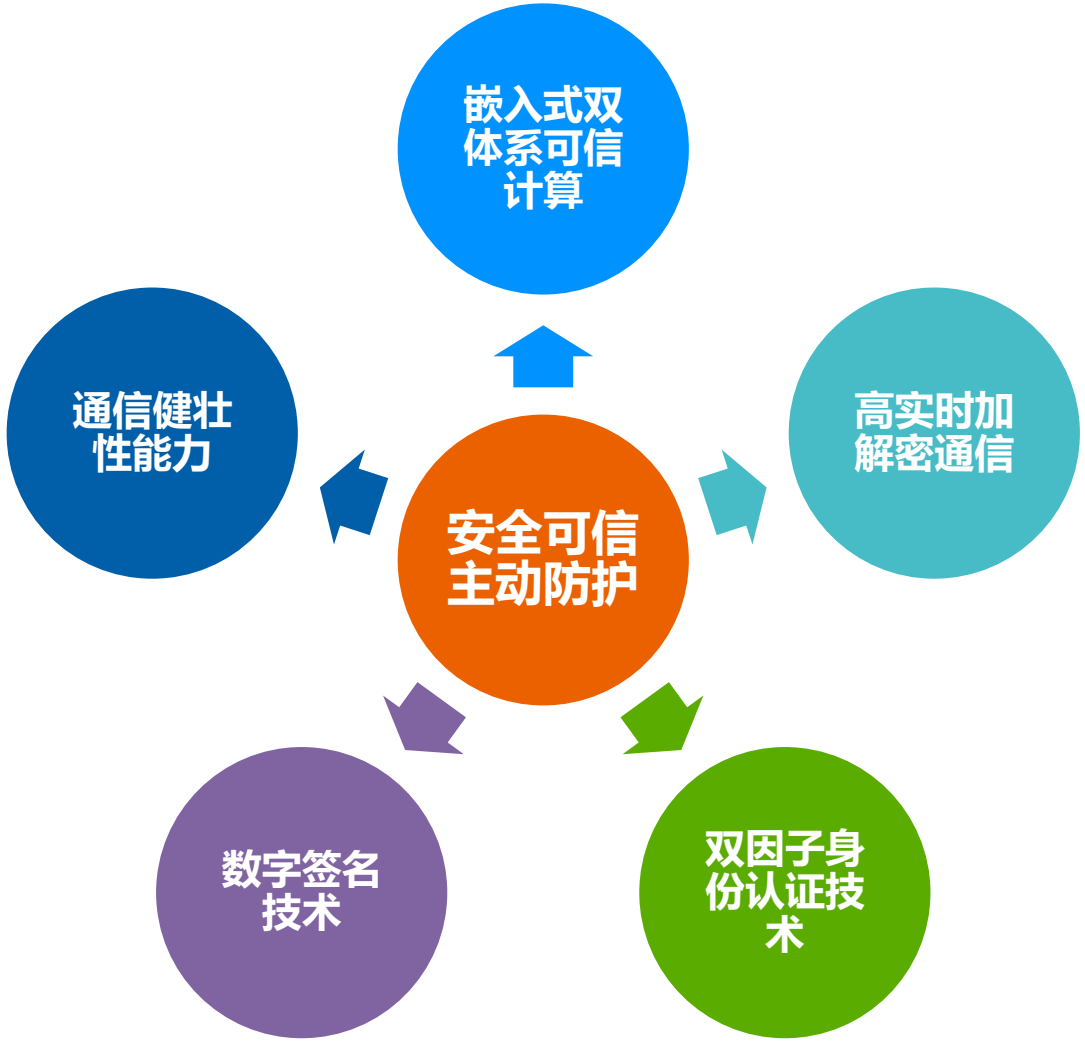
- 以内生安全工控系统为核心，形成5大类8个产品线的工业信息安全完整产品技术体系

2019年

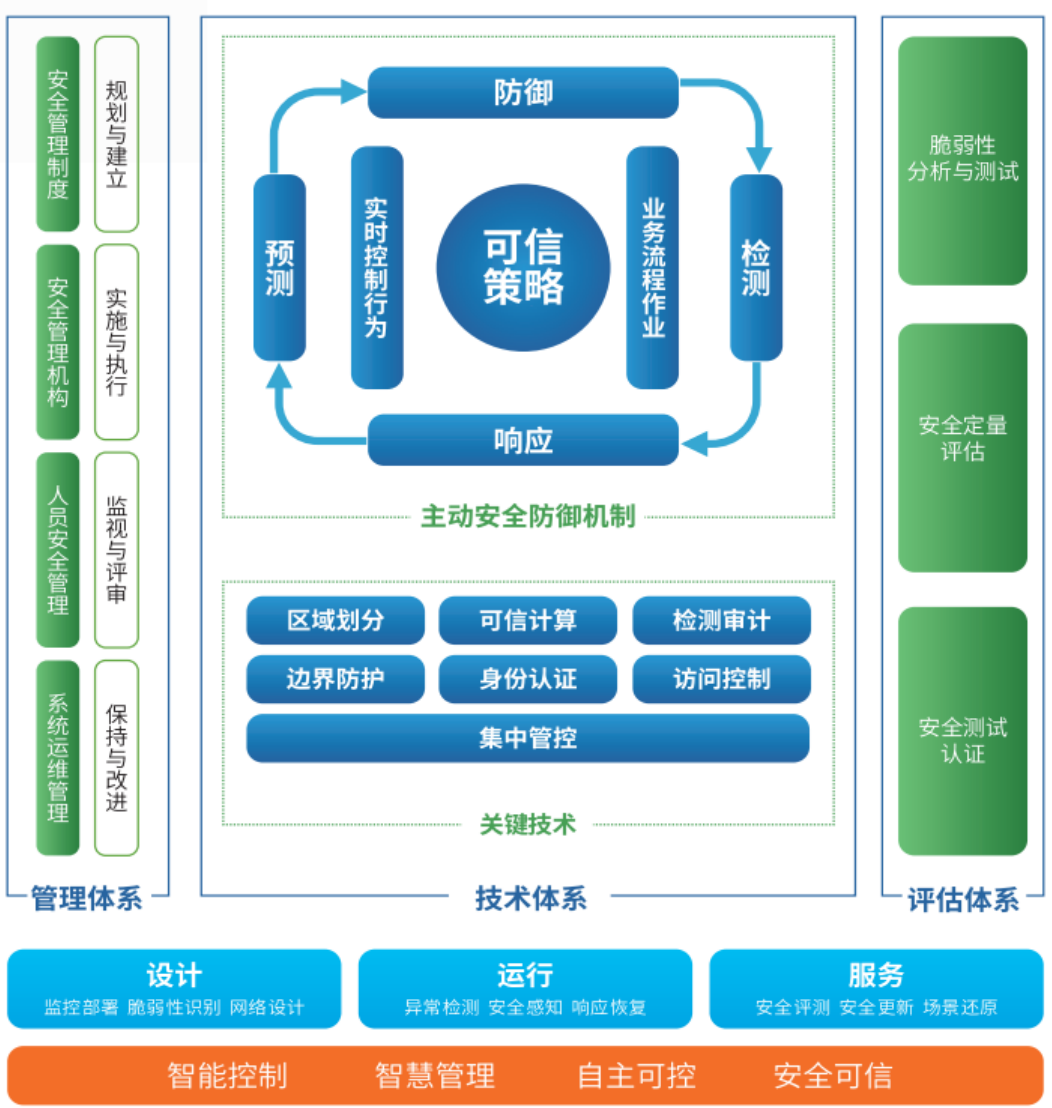
- 成立信息安全研究院，致力于工业信息安全核心技术研发，引领智能制造自主创新与安全可信的发展方向
- 累计服务各领域100多个工业信息安全建设保障项目

和利时安全可信主动防护技术积累

- **可信计算：**双体系并行可信计算3.0架构，独立安全核无扰保护，启动态和运行态全生命周期实时防护
- **通信加解密：**支持国密SM2/SM4的高实时可靠安全通信
- **双因子认证：**支持基于指纹或数字证书身份盾的权限控制
- **数字签名：**支持PKI体系和基于国密的数字签名和验签，支持对固件、接入设备的密码指纹认证
- **通信健壮性：**抗网络攻击，通过Achilles II级国际认证



和利时安全可信防御循环



国内首款主动防护可信PLC控制系统

可信计算环境

- 轻量级可信3.0技术框架
- 全生命周期动态可信验证，由内向外自主免疫
- 填补可信计算在工业嵌入式控制领域技术空白

可信网络连接

- 双向证书认证
- 高实时通信加解密
- 取得Achilles II级认证的首款国产大型PLC

多维度安全技术集成

- 强制访问控制
- 双因子身份认证
- 国密算法支撑

和利时主导和参与的标准建设

和利时主导和参与编制了超过三十余项国家与行业标准

序号	中文名称	标准组织	标准号
1	信息安全技术网络安全等级保护安全设计技术要求	国家标准(GB)	GB/T 25070-2019
2	网络安全等级保护安全设计技术要求应用指南	公安部	-
3	网络安全等级保护基本要求应用指南	公安部	-
4	工业以太网交换机技术规范	国家标准(GB)	GB/T 30094-2013
5	工业控制系统网络安全 第1部分：评估规范	国家标准(GB)	GB/T 30976.1-2014
6	工业控制系统网络安全 第2部分：验收规范	国家标准(GB)	GB/T 30976.2-2014
7	工业自动化和控制系统网络安全 可编程序控制器（PLC） 第1部分：系统要求	国家标准(GB)	GB/T 33008.1-2016
8	工业自动化和控制系统网络安全 集散控制系统（DCS） 第1部分：防护要求	国家标准(GB)	GB/T 33009.1-2016
9	工业自动化和控制系统网络安全 集散控制系统（DCS） 第2部分：管理要求	国家标准(GB)	GB/T 33009.2-2016
10	工业自动化和控制系统网络安全 集散控制系统（DCS） 第3部分：评估指南	国家标准(GB)	GB/T 33009.3-2016
11	工业自动化和控制系统网络安全 集散控制系统（DCS） 第4部分：风险与脆弱性检测要求	国家标准(GB)	GB/T 33009.4-2016
12	工业通信网络 网络和系统安全 系统安全要求和安全等级	国家标准(GB)	GB/T 35673-2017
13	信息安全技术 工业控制系统现场测控设备通用安全功能要求	国家标准(GB)	GB/T 36470-2018
14	电力监控系统网络安全防护导则	国家标准(GB)	GB/T 36572-2018
15	信息安全技术 工业控制系统网络安全防护能力评价方法	国家标准(GB)	20173583-T-469
16	信息安全技术 工业控制系统专用防火墙技术要求	国家标准(GB)	GB/T 37933-2019
17	工业过程测量和控制安全 网络和系统安全	铁路运输行业标准(TB)	JB/T 11960-2014
18	工业通信网络 网络和系统安全 术语、概念和模型	机械行业标准(JB)	JB/T 11961-2014

国家等保系列标准（设计要求、应用指南）

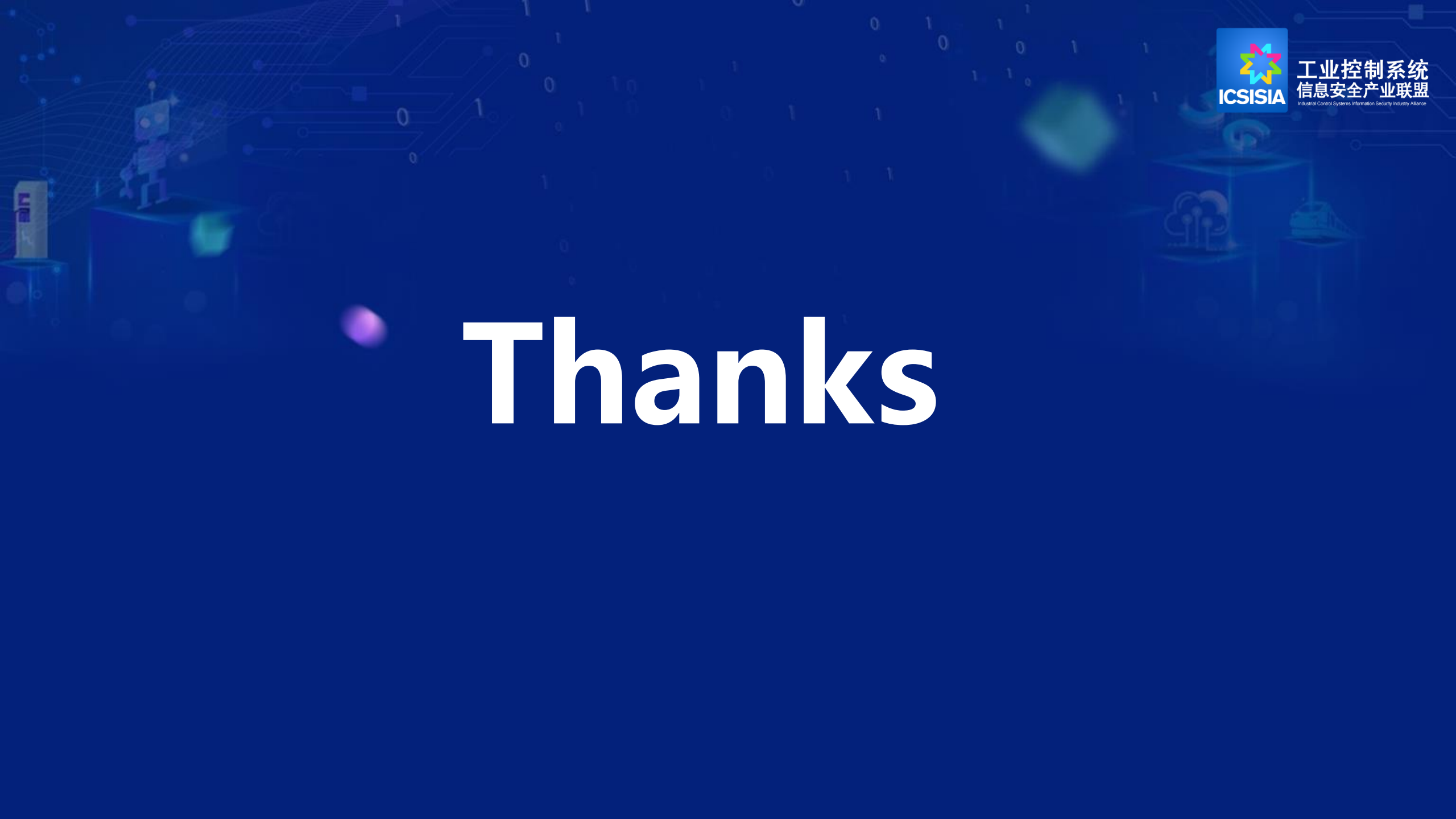
工业网络安全核心标准

电力行业标准设计主要导则

销许检测标准

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

关注工业安全产业联盟
请扫二维码



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