2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

基于商用密码的内生安全工控系统与应用实践

和利时信息安全研究院

01 工控系统安全可信技术体系

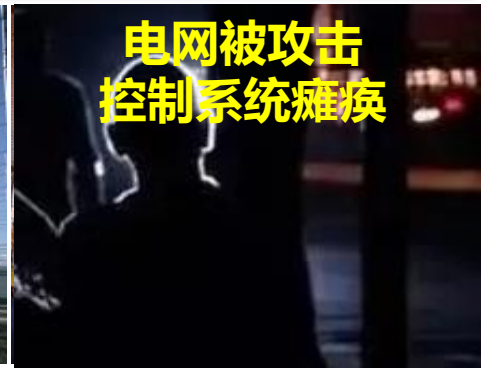
工业网络安全威胁态势

随着工业互联网、云计算等技术出现，工业控制系统已逐步从封闭隔离系统演进为开放交互系统，引入了极大的信息安全隐患。

2010年伊朗核电站"震网"事件

2012年中东石油部门"火焰"事件

2015年乌克兰电力系统"黑暗力量"事件

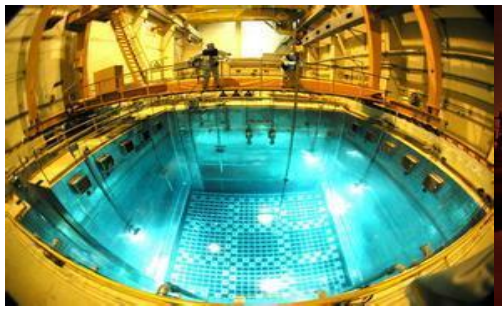


2019年委内瑞拉大停电事件

工控系统安全直接影响产业安全

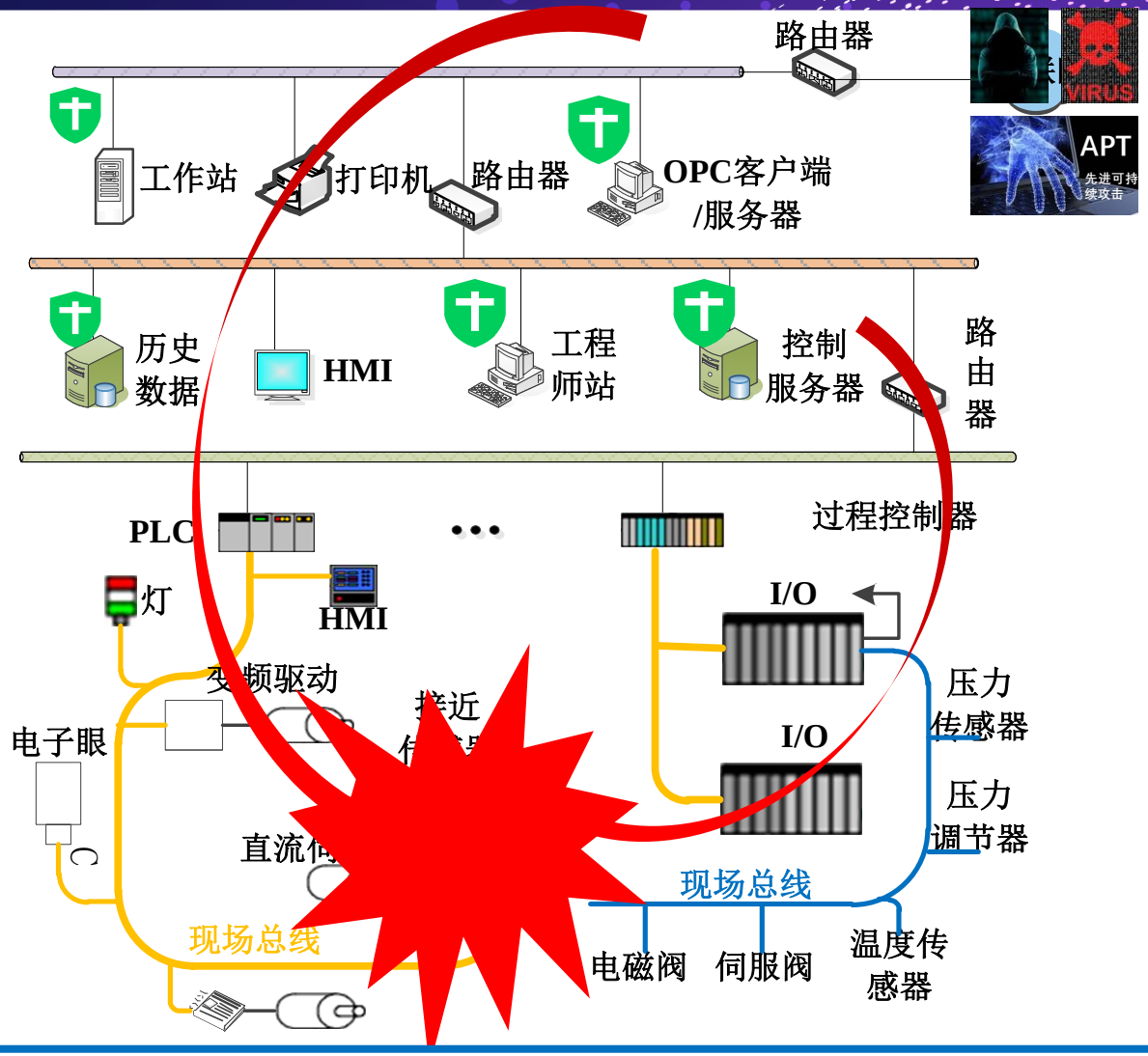







- 以PLC/DCS为代表的工业控制系统，是能源、化工、冶金等领域重大工程和装备的大脑，是实现制造业数字化、网络化、智能化的关键设备，是产业安全的基础。
- 《中华人民共和国密码法》要求使用商用密码对关键信息基础设施进行保护。
- 依据《中华人民共和国网络安全法》，国家互联网信息办公室会同工信部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录（第一批）》，PLC名列其中。

工控系统安全威胁



沿用IT领域的思路，采用防火墙、补丁等手段，在阻止、隔离和脆弱性分析基础上进行安全加固。

然而这种被动的防御方法，已很难抵挡迅猛发展的网络攻击技术及手段。各种新的和未知威胁更加剧了这种现象。

一旦入侵攻击突破传统被动防御，将严重威胁到工业控制系统的安全运行，甚至造成重特大事故。

需要基于**内生安全技术**建立涵盖控制设备安全、网络通信安全、业务流程作业安全的
工控系统主动防御体系

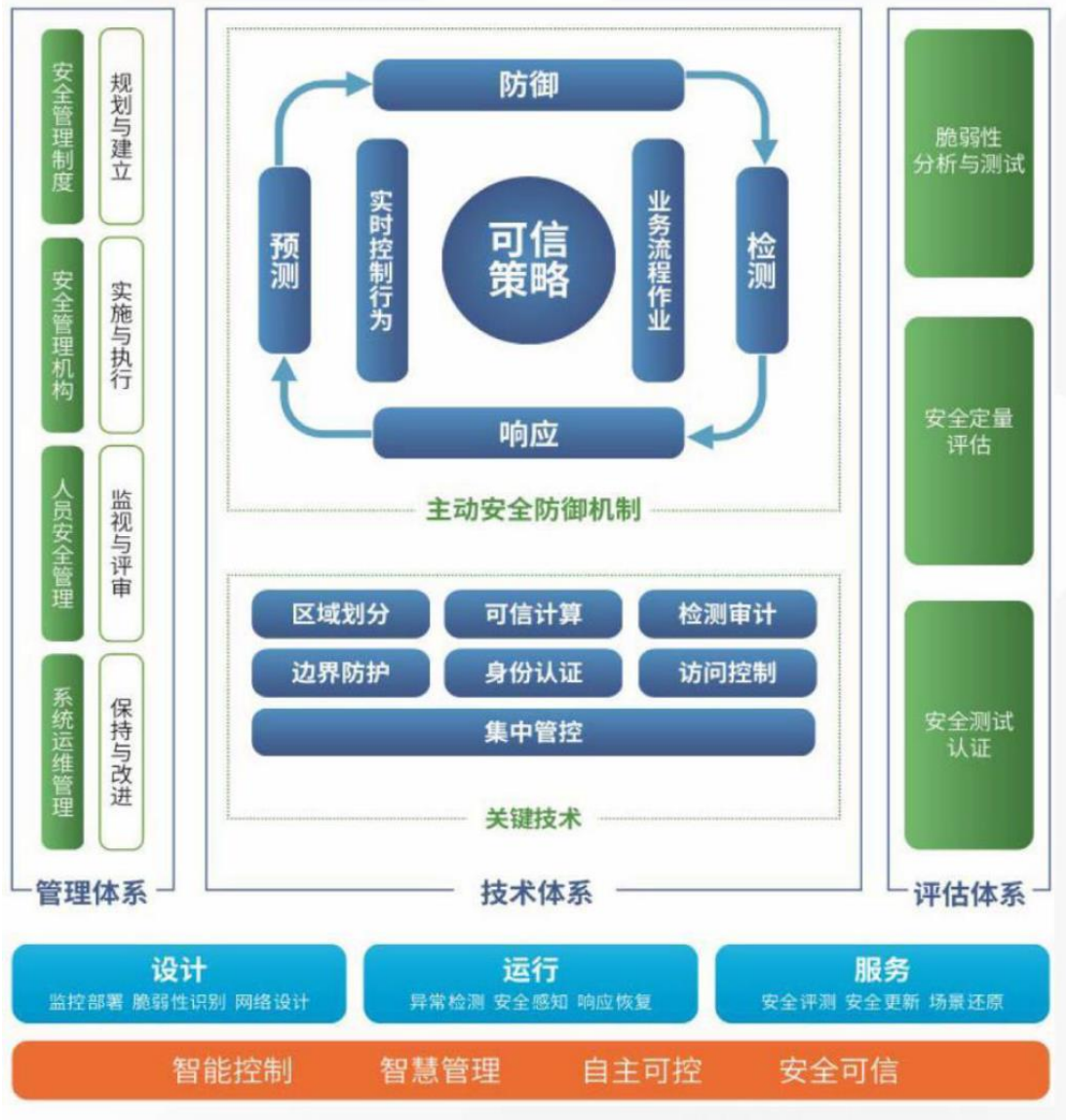
工业网络安全思考与应对

和利时致力于以“自主可控、安全可信”为业务特点，实现技术和供应链的自主可控,产品和服务的安全可信,围绕“智能控制、智慧管理”的业务核心，积极打造控制的智能化和生产管理的智慧化。

智能控制　**智慧管理**　**自主可控**　**安全可信**

和利时安全可信技术体系

基于内生安全可信，在可信策略（Trusted policy）的指导下，针对工业控制中的实时控制行为和业务流程作业，实现贯穿设计、运行、服务全生命周期的防御（Defense）、检测（Detection）、响应（Response）、预测（Prediction）的主动安全防御循环。

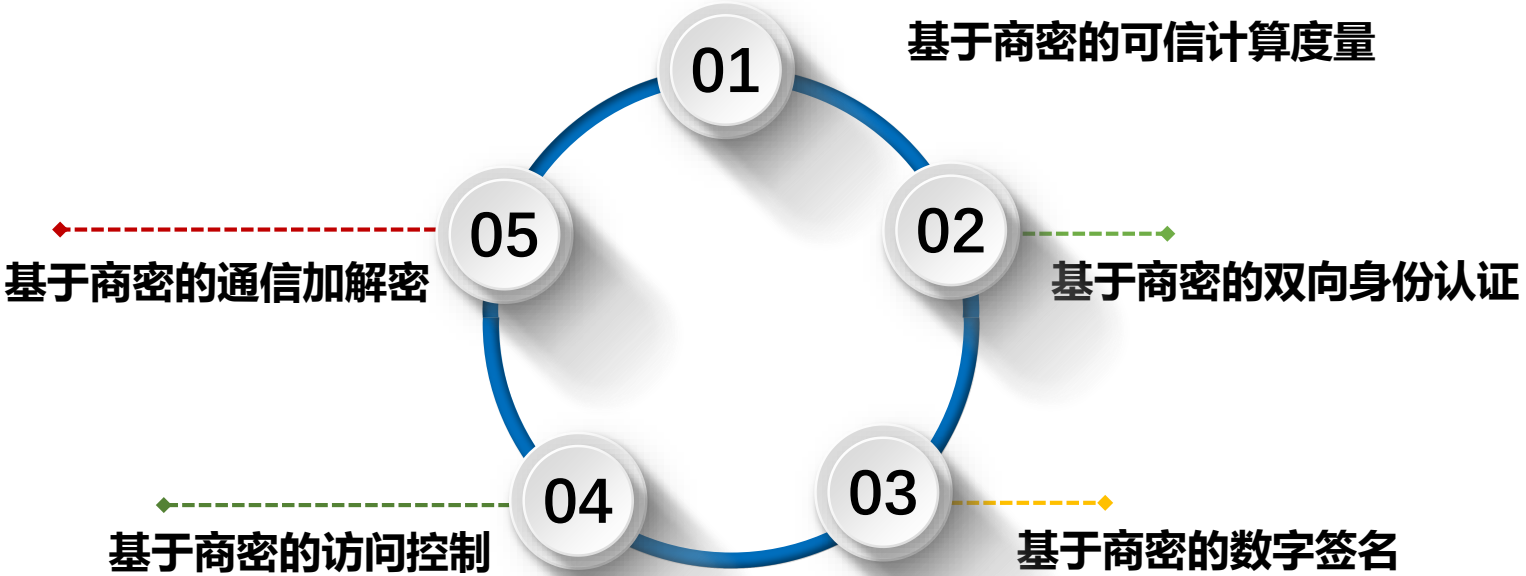


工控系统安全可信关键技术

01 安全可信控制器

02 安全可信上位机

03 安全可信管理平台



商密算法支撑

工控系统实时性、可靠性、分布式、嵌入式、轻量化应用优化

02 工控系统商密技术方案

工业控制系统商密应用方案

商密算法库 (SM2/SM3/ SM4/SM9)

- 算法软件
- 算法IP核
- 算法芯片

工控系统商密应用组件

- 双向证书认证
- 增强身份鉴别
- 数据存储保护
- 通信链路加密
- 可信计算度量
- 指令完整性验证

安全可信工业控制系统


安全可信PLC

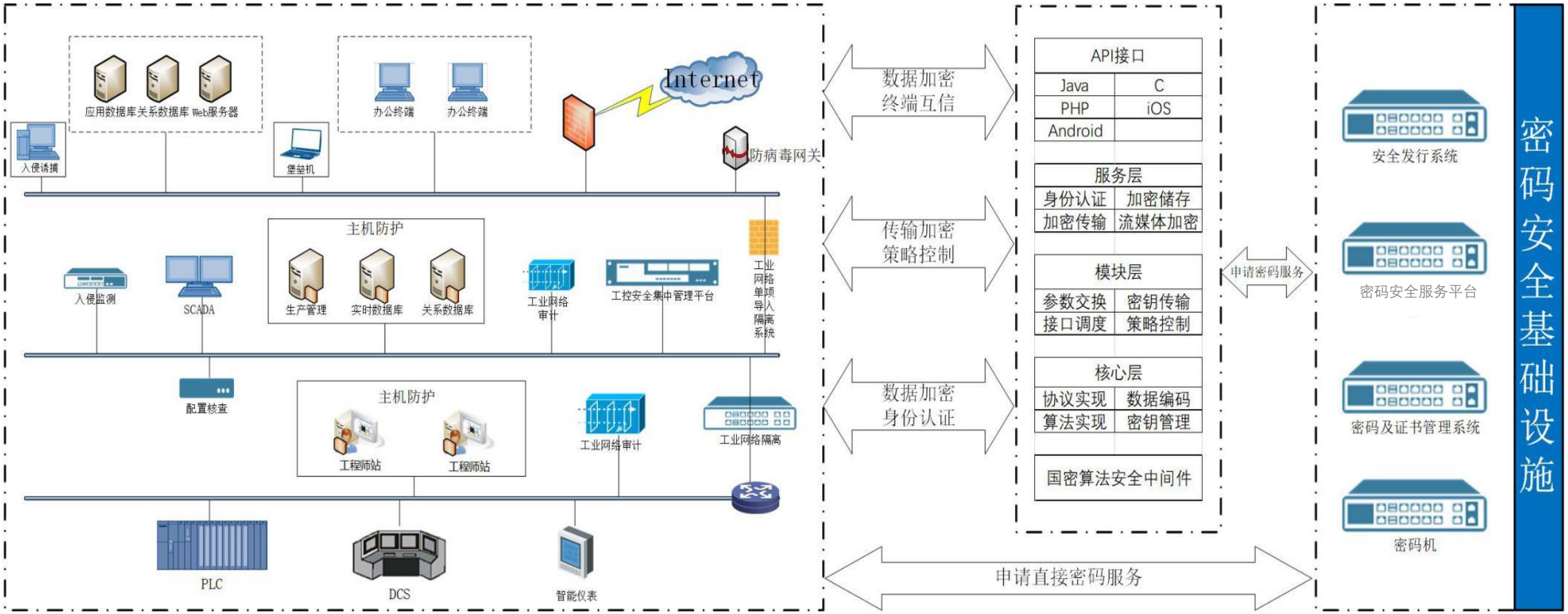

安全可信SCADA


安全可信DCS

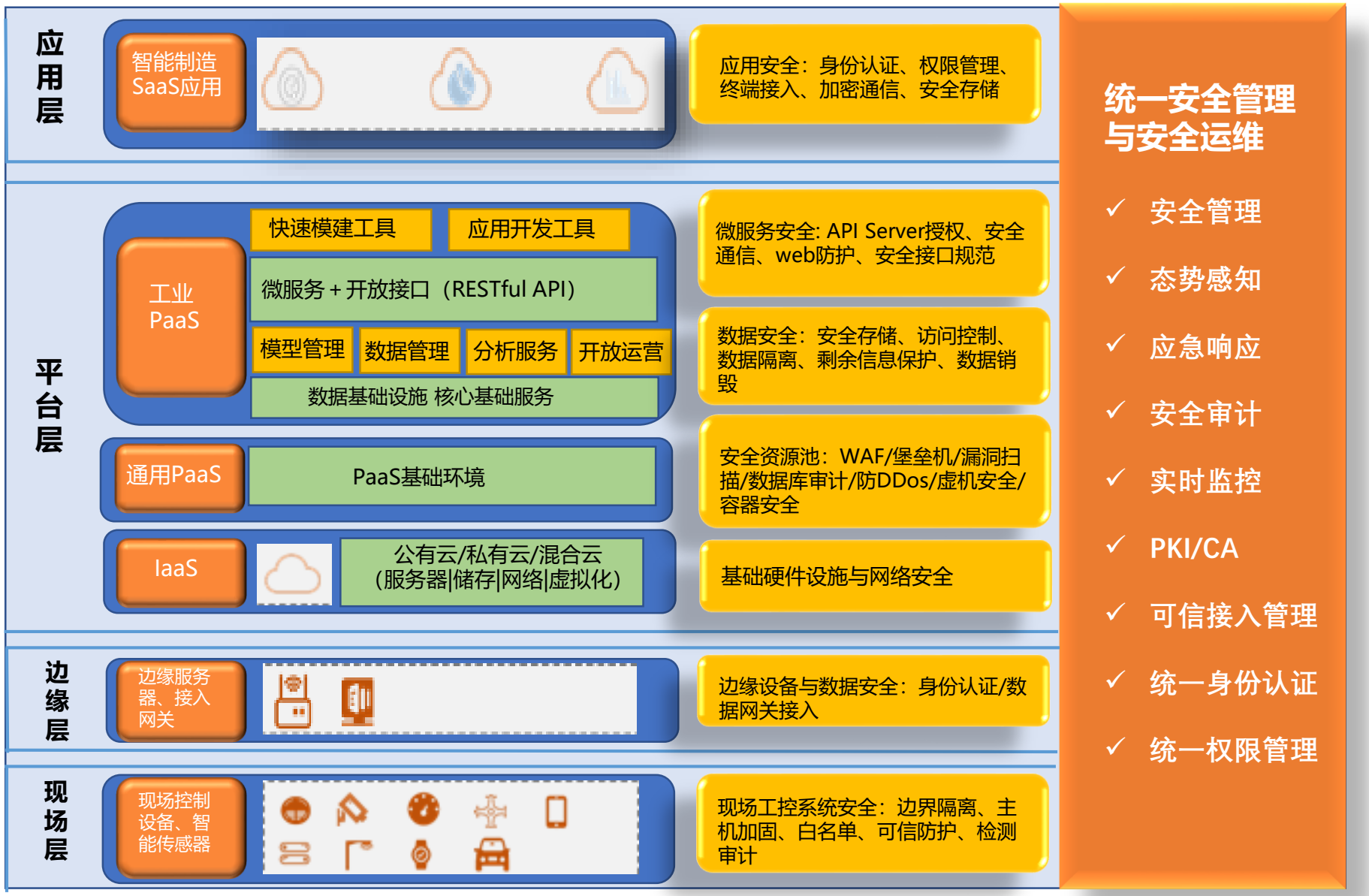

安全可信工业主机

关键信息基础设施行业应用

工业控制系统商密应用方案

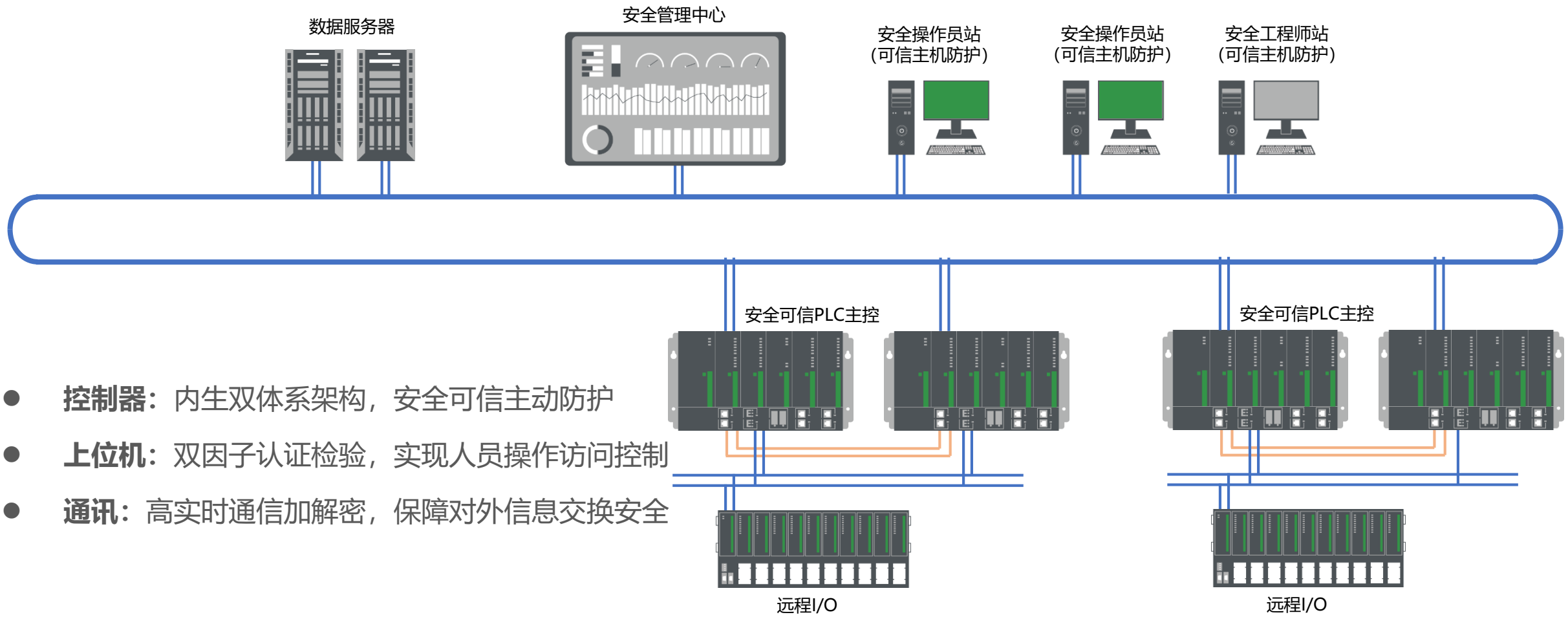


工业互联网商密应用方案



- 通过基于商密算法的内生安全主动免疫防护技术，与外围防护措施相结合，构建满足等保2.0三级要求的安全可信工业互联网平台。
- 平台通过安全资源池/安全组件/服务等形式，提供商密应用组件，形成覆盖“端、边、云”的安全防护体系。

安全可信PLC控制系统



- **控制器**：内生双体系架构，安全可信主动防护
- **上位机**：双因子认证检验，实现人员操作访问控制
- **通讯**：高实时通信加解密，保障对外信息交换安全

基于商密算法，采用国产化设计，通过双体系可信计算架构实现主动防护，满足国家关键基础设施网络安全防护需求

安全可信PLC控制系统

可信计算环境

轻量级可信计算3.0技术框架

静态启动与全生命周期动态运行可信验证

填补可信计算在工业嵌入式控制领域应用空白

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

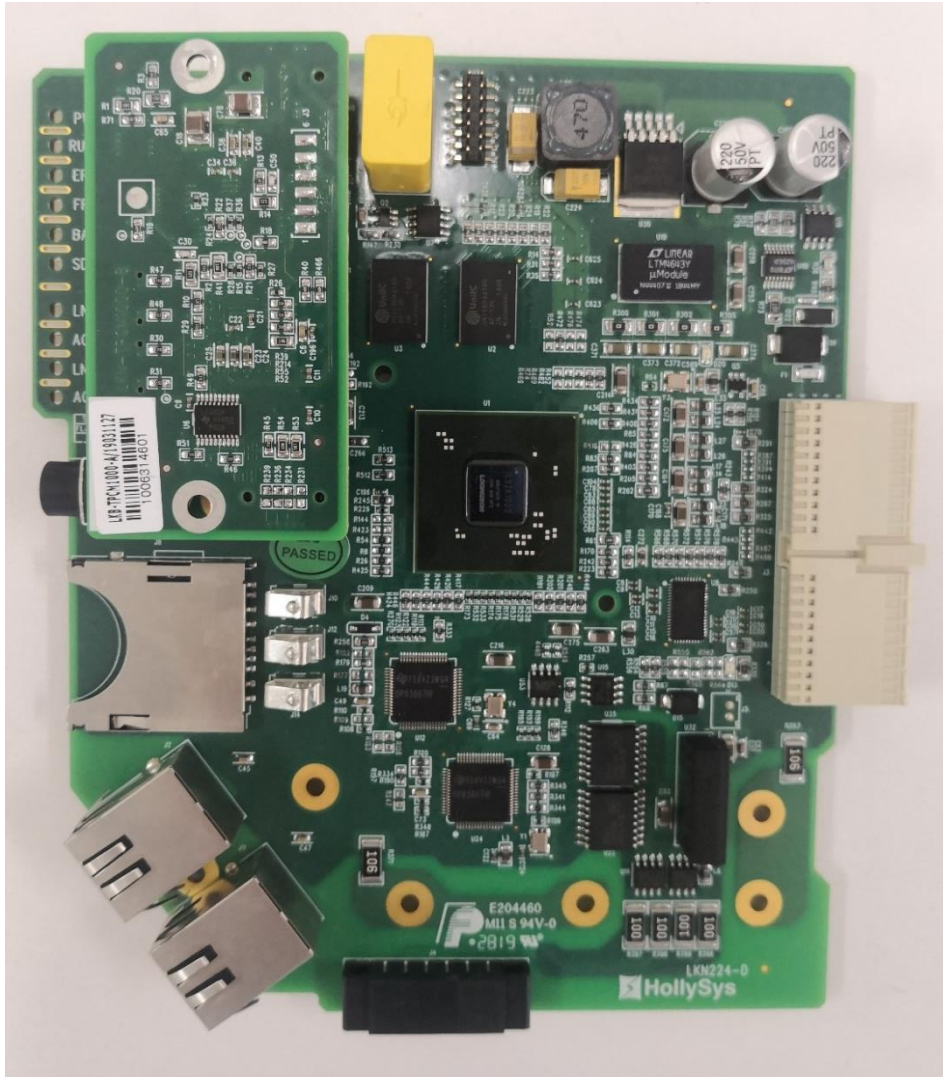
强制访问控制

双因素身份认证

关键数据区保护

安全可信PLC控制系统

- **可信芯片：**国产TCM密码芯片提供SM系列商密算法，支持可信计算与通信加解密
- **可信度量：**基于双核CPU，对系统运行进行全生命周期的无扰度量和动态监管
- **可信策略：**安全可信控制器配合可信管理平台，实现安全策略配置与度量结果呈现



基于商密的全生命周期可信度量

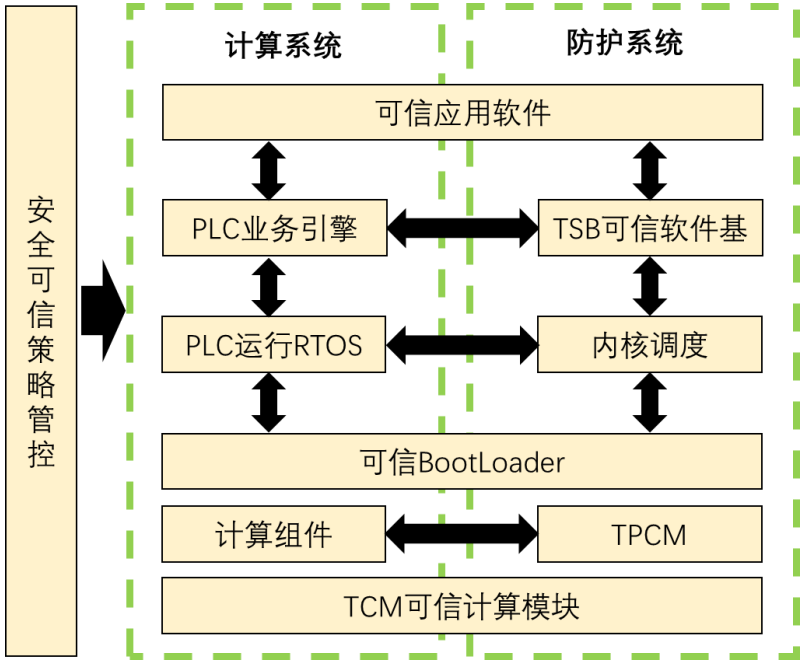
基于商密算法，在启动阶段构建可信链；在运行过程中进行全生命周期动态度量

启动时静态度量

- 双体系可信链传递
- 启动程序与文件度量

运行时动态度量

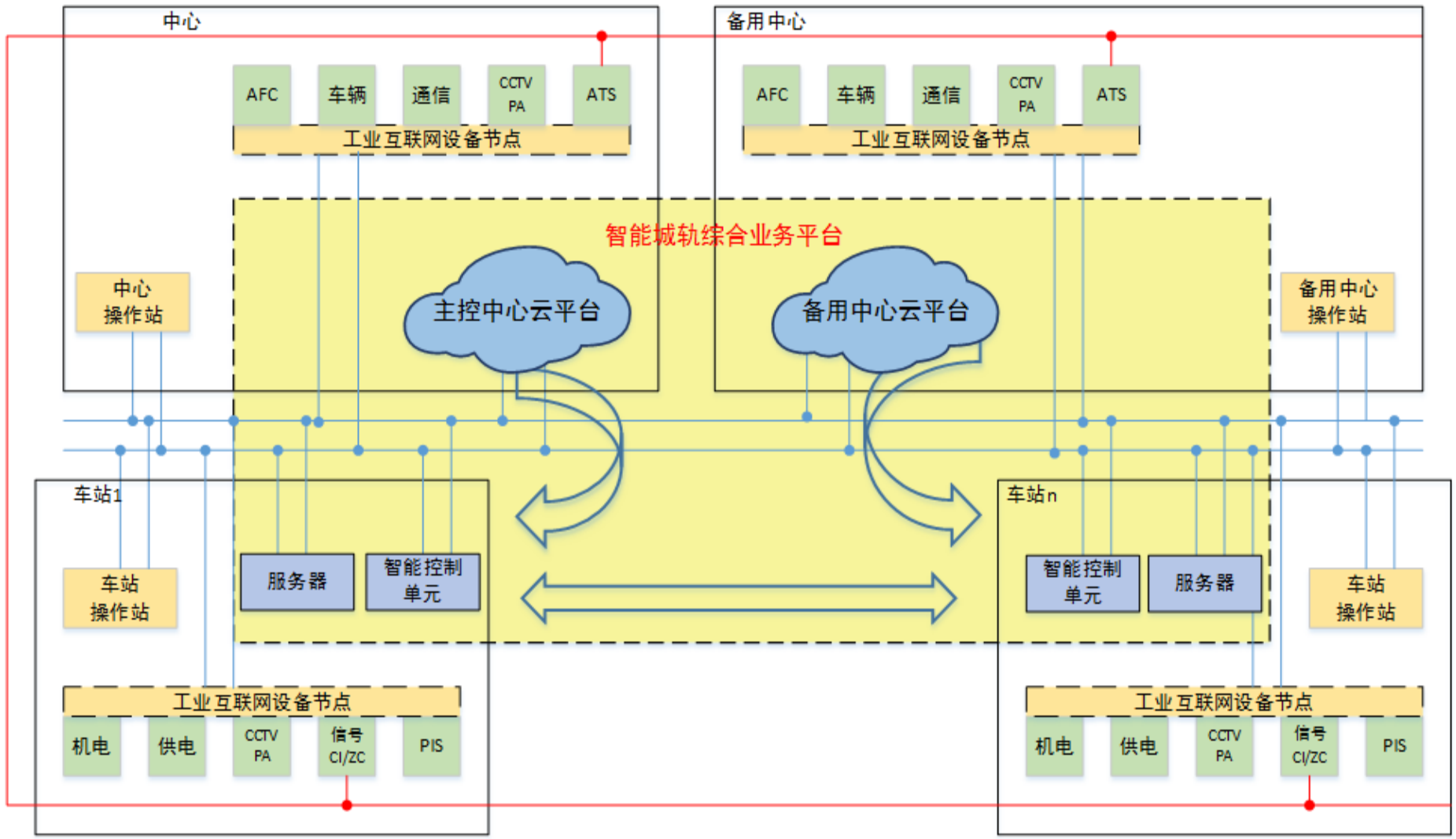
- 轻量级环境度量
- 任务四元组度量
- 业务行为度量



全生命周期可信防护

03 典型应用实践

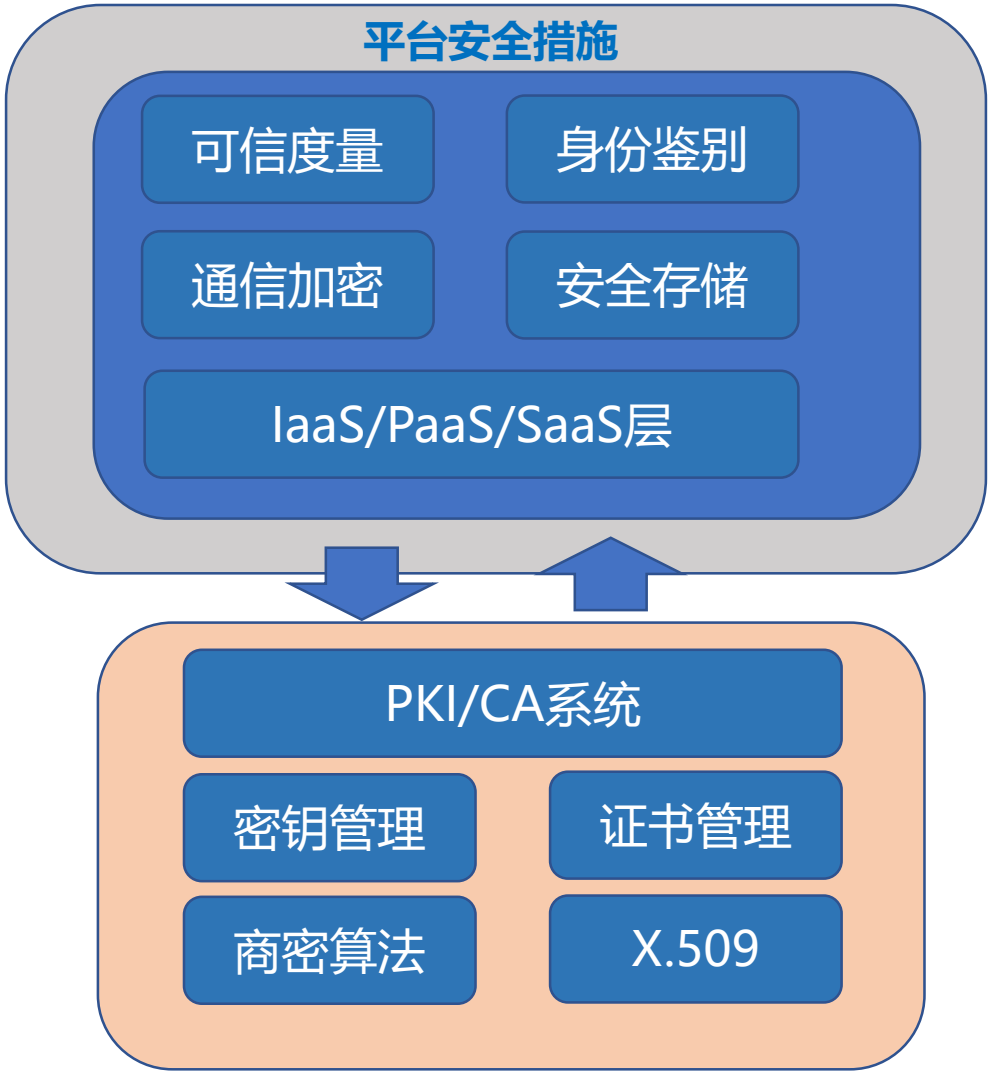
基于商密的智能城轨平台安全防护



某地铁项目基于工业互联网的智能城轨综合业务平台，创新应用同时面临着众多网络安全问题，包括：

- 平台安全问题
- 应用安全问题
- 数据安全问题
- 通信安全问题
- 访问安全问题
- 安全管理问题

基于商密的智能城轨平台安全防护



- **可信度量：**基于SM3进行系统启动时静态度量与运行时动态度量，实现从IaaS层到PaaS层的可信链传递，创建可信受控平台运行环境
- **身份认证与访问控制：**基于SM2/3与证书管理机制，实现安全增强的身份鉴别和访问控制
- **通信加解密：**基于SM2/3/4，实现重要通信数据的加密传输，通过轻量级高实时通信加解密支持HTTPS/MQTT/OPC UA等通信协议
- **存储加解密：**基于SM3/4，实现关键数据内容批量存储加解密能力

基于商密的智能城轨平台安全防护

应用情况

1. 基于商密算法的可信计算构建主动免疫内生安全机制，实现了从IaaS层、PaaS层到SaaS层的全生命周期可信度量
2. 基于商密算法的统一身份认证与访问控制服务，支撑了平台、应用和数据的访问安全
3. 基于商密算法的通信与存储过程加解密，保证了数据在传输和存储过程中的安全
4. 合规满足等保2.0三级与城轨行业标准，基于商密算法建立了“一个中心三重防护”的完整安全体系
5. 在工业互联网各层级全面应用商密算法，实现了端边云一体化防护、安全防护与城轨业务的深度融合

商密技术赋能工业网络安全

自动化控制

- 分布式控制系统DCS
- 可编程逻辑控制器PLC
- 综合监控系统SCADA
- 远程终端单元RTU

工业互联网

- 工业互联网平台
- 工业APP应用
- 工业物联网关

边缘计算

- 边缘控制器
- 智能仪表

工业大数据

- 数据接入
- 访问控制
- 数据脱敏

工业网络安全商密推广应用

围绕工业网络安全需求，建设基于商密的技术平台与组件

加快行业应用，增强关键信息基础设施系统安全

提升我国商密核心技术研发与工业网络安全综合保障能力


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音