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

自主可信的工业信息安全防护体系建设

汇报人：和利时信息安全研究院 刘伟
汇报日期： 2019年5月9日

工业控制系统发展趋势

工业控制系统变革由封闭走向开放

物联网

工业云

工业控制系统信息安全事件频发

2012年

中东石油部门
“火焰” 病毒感染事件

2015年

乌克兰电力系统
受到BlackEnrgy攻击，造成
大面积停电

2017年

“WannaCry”
勒索病毒入侵
石油公司加油站支付系统

2018年

“WannaCry”
勒索病毒变种入侵
台积电

工业信息安全-国家战略

HollySys

工控安全事关国家之战略安全

掌握核心关键技术是立足之本

工业控制系统是现代工业装备、国家重大工程及关键基础设施的枢纽和运行中心

工控信息安全防护体系演变

信息安全防护体系发展方向

- 基于纵深防护的信息安全体系

构建以边界防护为主体的信息安全防护体系架构

- 信息安全主动防护体系

以深度融合信息安全防护技术，以可信计算为基础的主动防护体系

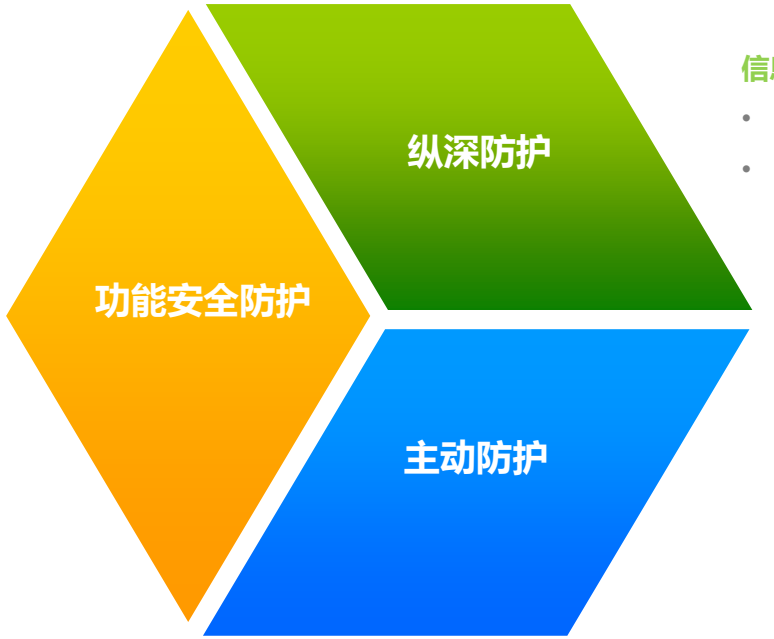
- 综合防护体系

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

信息安全综合防护体系

功能安全防护

- 保护控制系统的功能安全
- 外围防护被突破后避免事故发生
- 工控系统最终防护屏障



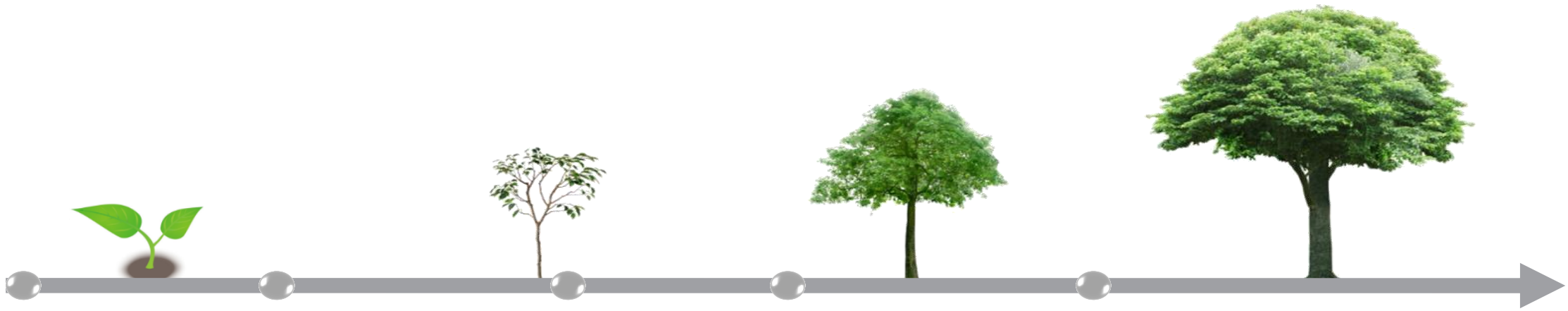
信息安全纵深防护

- 多区域多边界的防护结构
- 形成控制系统的信息安全防护屏障

信息安全主动防护

- 基于可信计算体系构建控制系统对网络威胁的自免疫能力

和利时工业信息安全发展历程



2012年

- 技术中心组建成立工业信息安全工作组
- 开展工业信息安全研究和技术推动工作

2013年

- 参与多项国家工业信息安全技术标准的制订工作
- 开展工业控制系统信息安全脆弱性研究

2015年

- 牵头科技部863项目-可编程嵌入式电子设备的安全防护技术及开发工具

2017年

- 可信计算和信息安全关键技术实现突破，完成国内首个具备可信计算能力的PLC产品
- 通信健壮性技术取得关键突破，相继完成包括PLC、DCS、核电仪控系统的技术改造，产品陆续取得此类安全能力的国际最高认证。

2018年

- 建成包括5大类10个产品线的信息安全完整产品族
- 累计服务100多个信息安全改造和新建项目

2019年

- 和利时信息安全研究院成立，致力于推动工业信息安全核心技术创新和研究，引领关键工业控制设备自主可控和安全可信的发展方向

信息安全主动防护技术积累

- **抗网络攻击能力**
  - 抵御网络风暴
  - 抵御网络洪涝攻击
  - 抵御重放攻击
  - 抵御畸形报文攻击
  - 处理超长合规报文

- **网络健壮性能力（阿基里斯2级国际认证）**


Certificate Of Compliance

This is to certify that the:
K-CU03 K Series High-Performance Controller Module
Model Number: K-CU03
Hardware Version: K-CU03-A
Software Version: K-CU03-B1
Category: Embedded Device

Manufactured by:
Hangzhou HollySys Automation Co. Ltd.

Is in compliance with the requirements set forth by:
Achilles Level II Certification

CERTIFICATE 390-011718

Felicia Nicastro
Senior Cyber Security Director

cchilles


Certificate Of Compliance

This is to certify that the:
LK Series
Model Number: LK225-A01
Hardware Version: LK225-A
Firmware Version: LK225-A01
Category: Embedded Device

Manufactured by:
Beijing HollySys Co., Ltd.

Is in compliance with the requirements set forth by:
Achilles Level II Certification

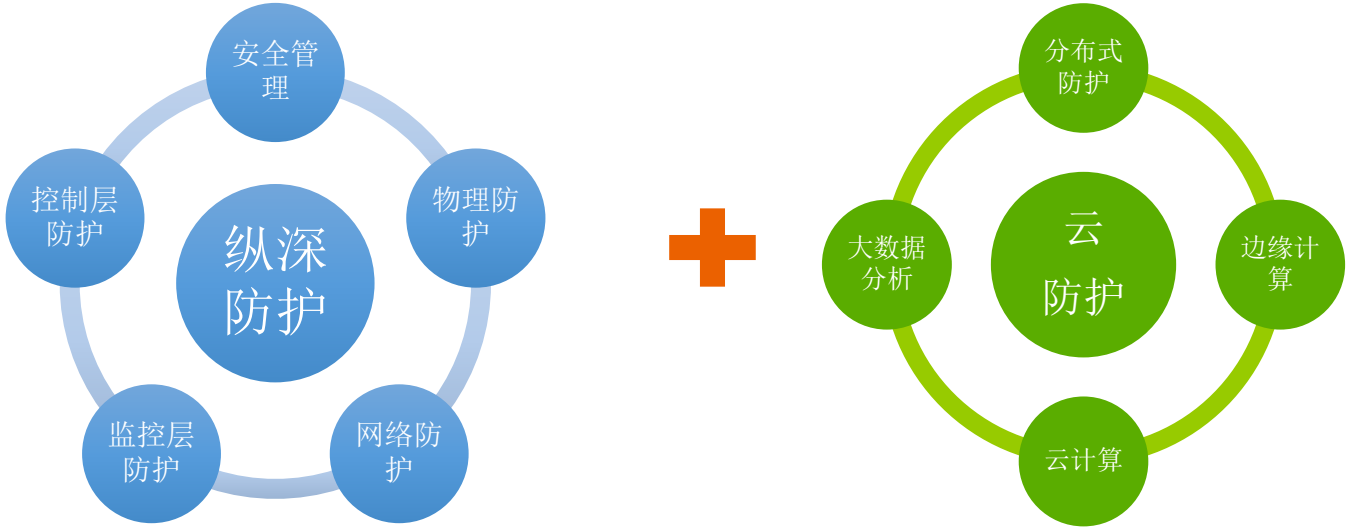
CERTIFICATE-411-091018

Felicia Nicastro
Senior Cyber Security Director

cchilles

信息安全防护体系能力突破

纵深防护-云防护体系融合



被动防护-主动防护技术融合

“三大突破”助力提升工控系统核心安全能力

HollySys

提高工业控制系统核心安全能力

工控系统双体系可信计算

为控制系统核心控制器和计算机构建自主免疫的可信安全环境，基于可信计算技术建立自主免疫系统，包括可信芯片、可信平台、可信软件基、可信网络连接、可信管理支持。

控制&安全一体化解决方案

依托和利时完整的安全产品族和在工业控制系统专用网络和通信的技术积累，将传统边界防护解决方案与控制系统网络和数据特点有机融合，定制化开发对控制逻辑和控制网络数据有效监管和防护的整体解决方案，实现安全中有控制，控制中有安全的突破性解决方案。

信息、功能、业务安全融合

通过对工业控制系统业务监管、功能监管、控制逻辑监管赋能三位一体的工业信息安全新理念。将控制层设备安全、业务操作安全、控制逻辑安全等信息与网络信息安全构成安全新集合。

和利时信息安全防护体系

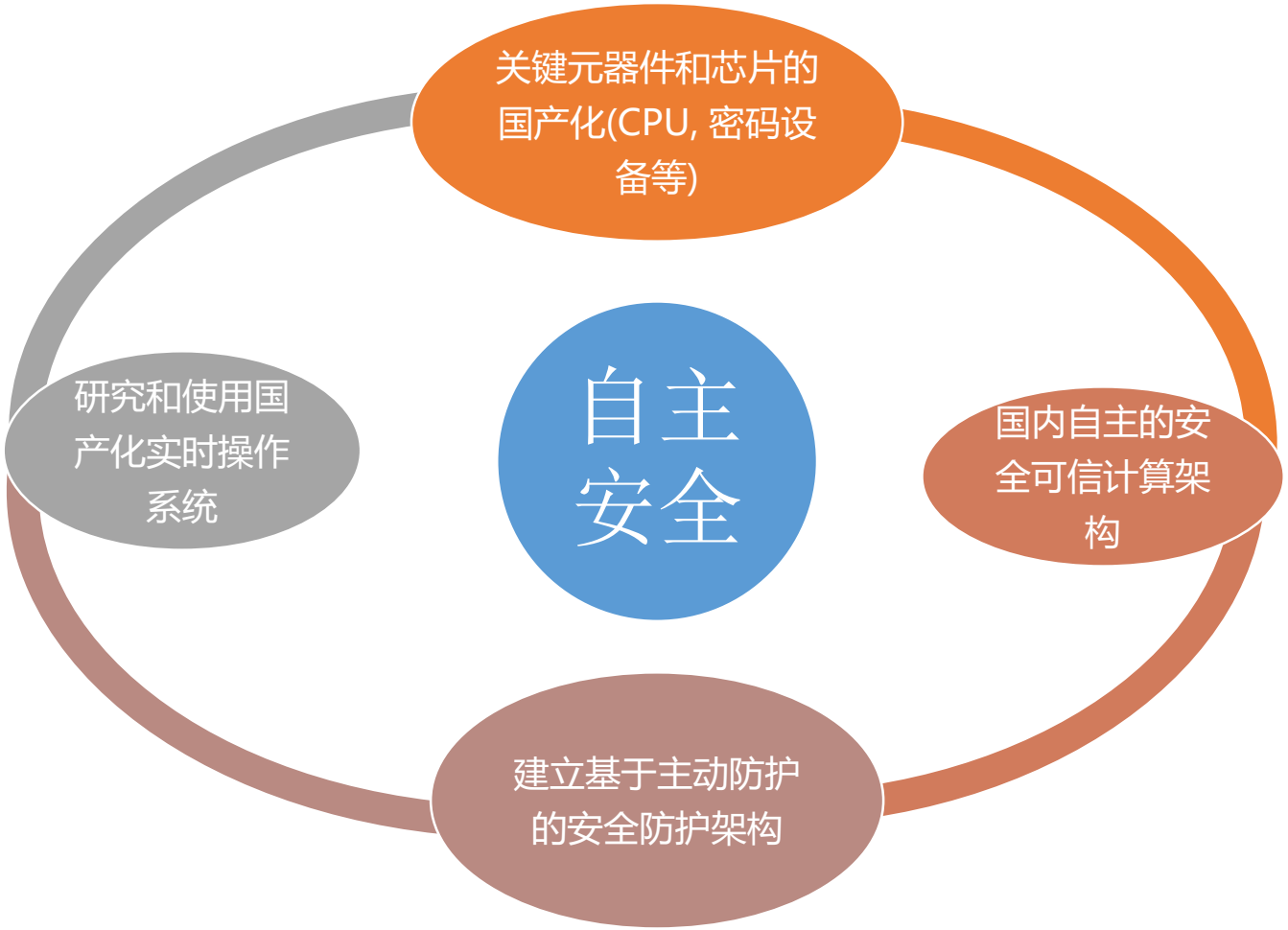
核心思想：

以整体围绕可信计算的内生防护为基础，通过纵深防护体系的边界防护理念构建外围防线

GB/T 22239-2018 信息安全技术 网络安全等级保护基本要求

满足等保的需求的基础上，在本质上增强控制系统的核心防护能力。

自主安全原则


关键元器件和芯片的国产化(CPU, 密码设备等)
国内自主的安全可信计算架构
建立基于主动防护的安全防护架构
研究和使用国产化实时操作系统
自主安全

和利时信息安全防护体系

防护层级设计：

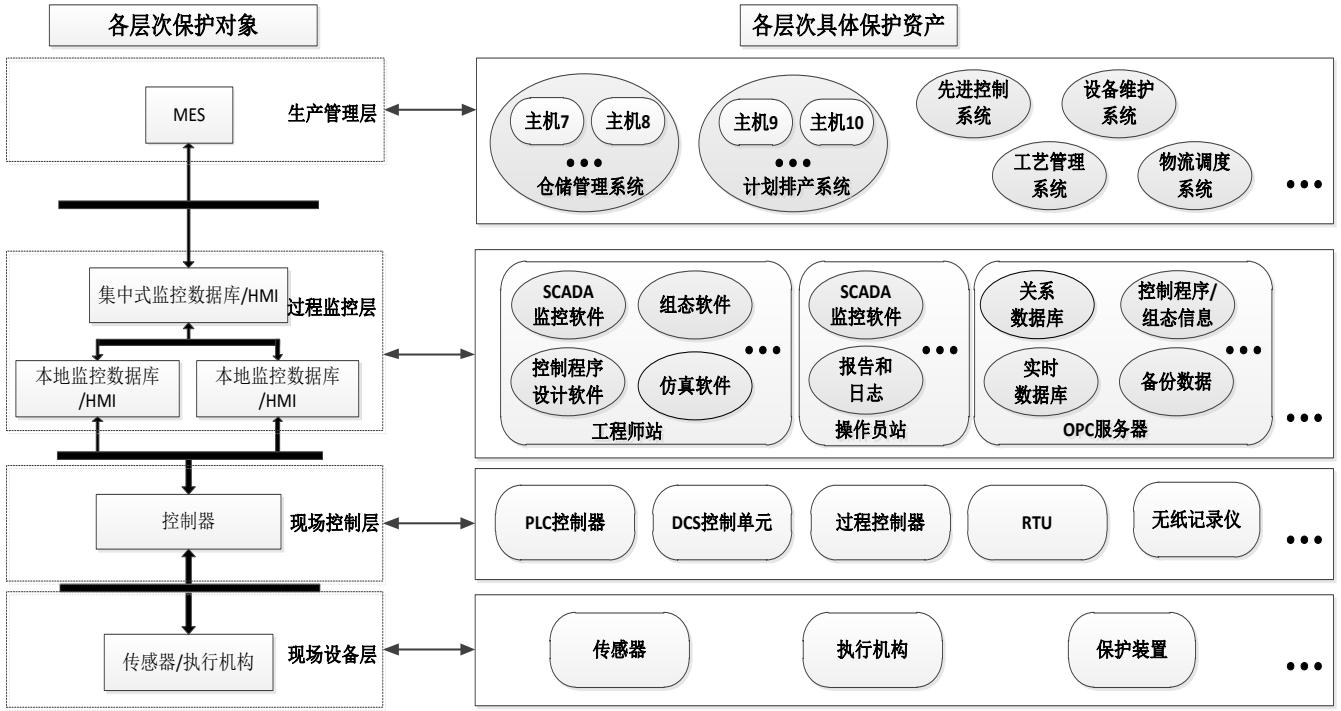
根据GB/T 22239.5-2018 信息安全技术 网络安全等级保护基本要求-第5部分 工业控制系统安全扩展对系统层级划分的规则将控制系统划分为四个层级，针对每一层级明确被保护的资产对象。

生产管理层：MES、APS、WMS等；

过程监控层：工程师站、操作员站、服务器、上位机软件等；

现场控制层：PLC控制器、DCS控制器等；

现场设备层：传感器、仪器仪表等。



和利时信息安全防护体系

基本防护策略：

- 区域划分隔离：根据等级保护要求的区域划分原则将控制系统按照不同的功能、控制区、非控制区进行区域划分。
- 网络节点保护：对各安全区域的边界节点进行隔离防护，并对各安全域内的关键通信节点配置防护策略。
- 主机安全防护：主机加装防病毒软件及主机加固软件保证主机设备安全。
- 通信数据保护：控制系统的关键数据如下装数据、身份验证数据等进行通信加密和加密存储。
- 集中审计管控：在安全管理区配置集中审计和管理平台，对系统安全策略统一管理并集中收集分析各层级的安全审计内容。

和利时信息安全防护体系

安全产品部署：

- **边界隔离设备：工业防火墙**（依照特定的规则，允许或是限制传输的数据通过）、**工业安全网闸**（通过切断由外部发起的连接保护内部网络）
- **入侵检测系统：**对网络传输数据进行即时监视，在发现可疑流量时发出警报或者采取主动反应措施
- **审计设备：**对安全设备、网络设备、主机系统进行日志数据采集、解析和分类，并生成各类分析报告、以及对网络设备、主机、通信链路进行监控

终端防护：

- **终端防护（主机加固软件、工控主机卫士）、工业白名单软件**

系统内的主机终端进行主机操作系统安全加固时应从配置管理、网络管理、接入管理、安全审计、恶意代码防范等几个方面进行

和利时信息安全防护体系

安全管理平台：

- **工业安全管理平台**

对工业控制系统的网络设备、安全设备（工业防火墙、工业安全网闸、工业入侵检测、工业安全审计等）、主机防护设备等进行统一安全管理，实现工控网络及各类设备进行可用性与性能的监控、事件的分析审计预警、风险与态势的度量与评估、工控网络信息流行为的合规分析等。

应用安全设计：

- **主控制器、上位机软件**

进行应用安全设计时应从身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错、资源控制等几个方面进行。主要针对主控制器及上位机组态软件。

“1+4+5”工业信息安全设计理念

和利时信息安全设计：

一个原则

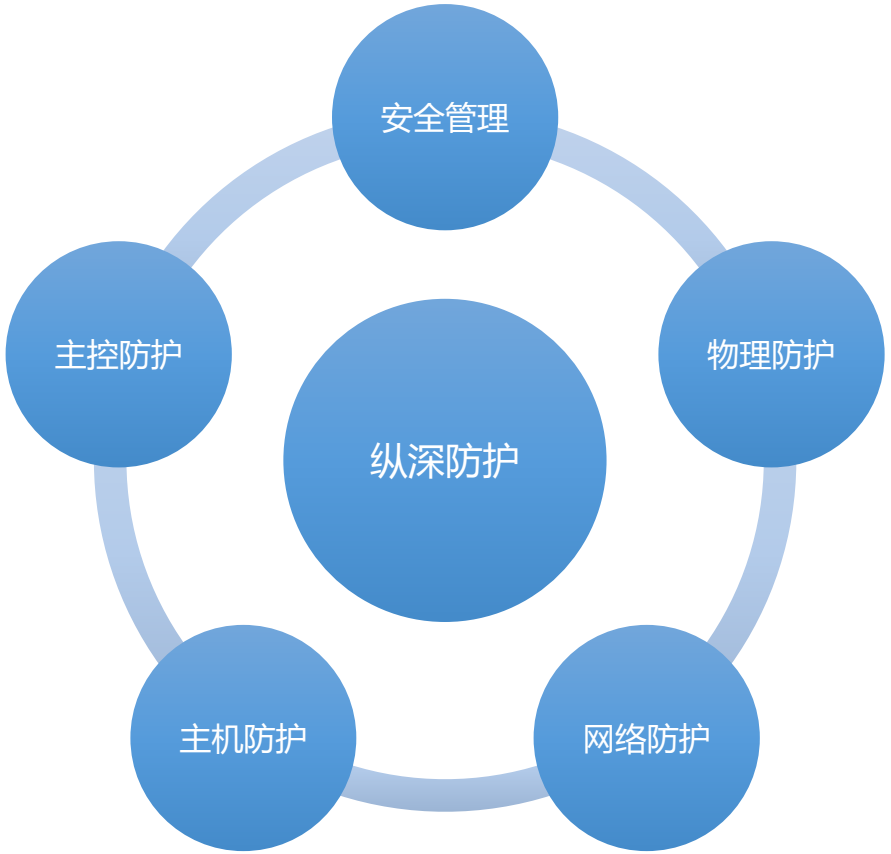
- 纵深防护原则

四个层面：

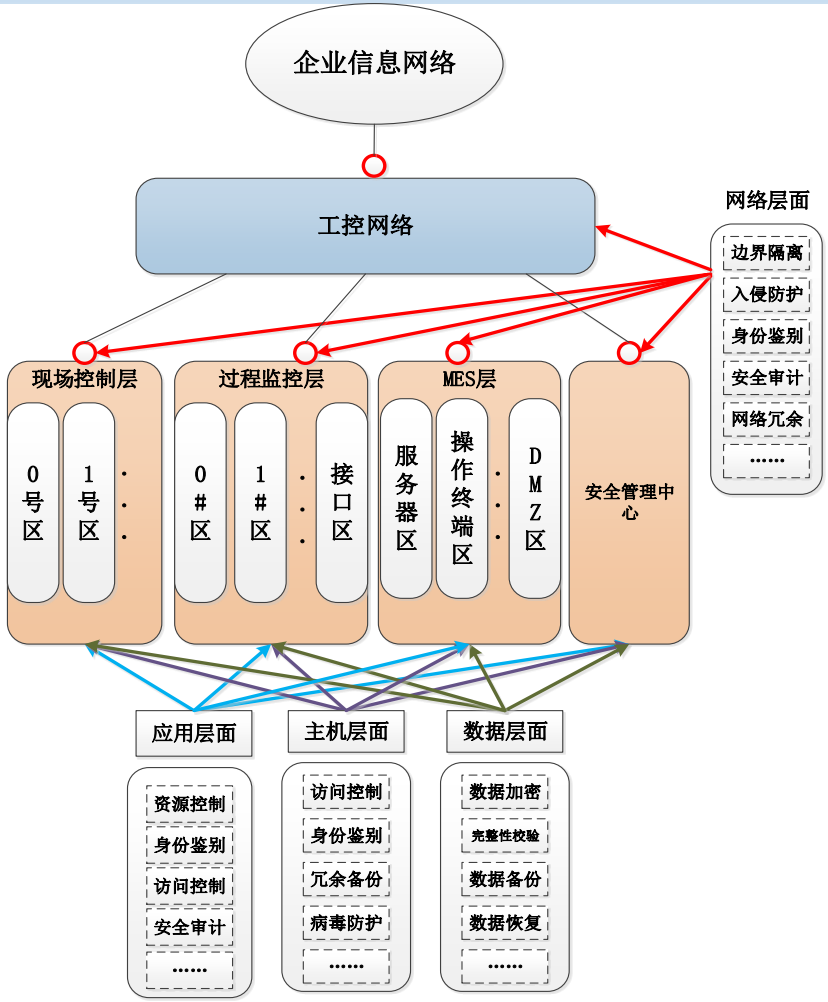
- 数据层面
- 网络层面
- 主机层面
- 应用层面

五类防护策略：

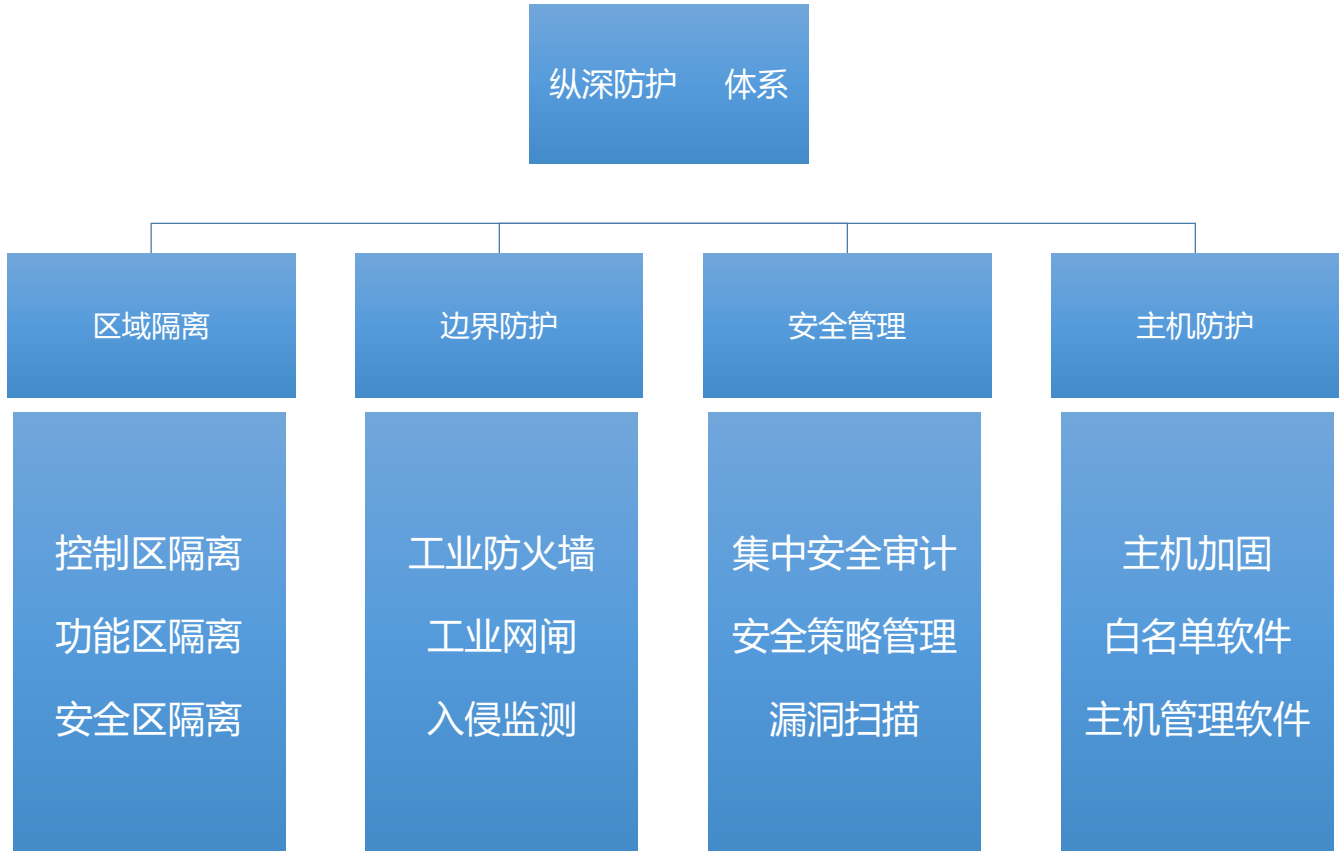
- 区域划分隔离
- 网络节点保护
- 主机安全防护
- 通信数据加密
- 集中审计管控



工业控制系统信息安全纵深防护



信息安全纵深防护结构


纵深防护 体系
区域隔离
边界防护
安全管理
主机防护
控制区隔离
功能区隔离
安全区隔离
工业防火墙
工业网闸
入侵监测
集中安全审计
安全策略管理
漏洞扫描
主机加固
白名单软件
主机管理软件

信息安全综合防护体系部署

- 分区分域
- 优化网络结构

网络加固

- 安全防护产品

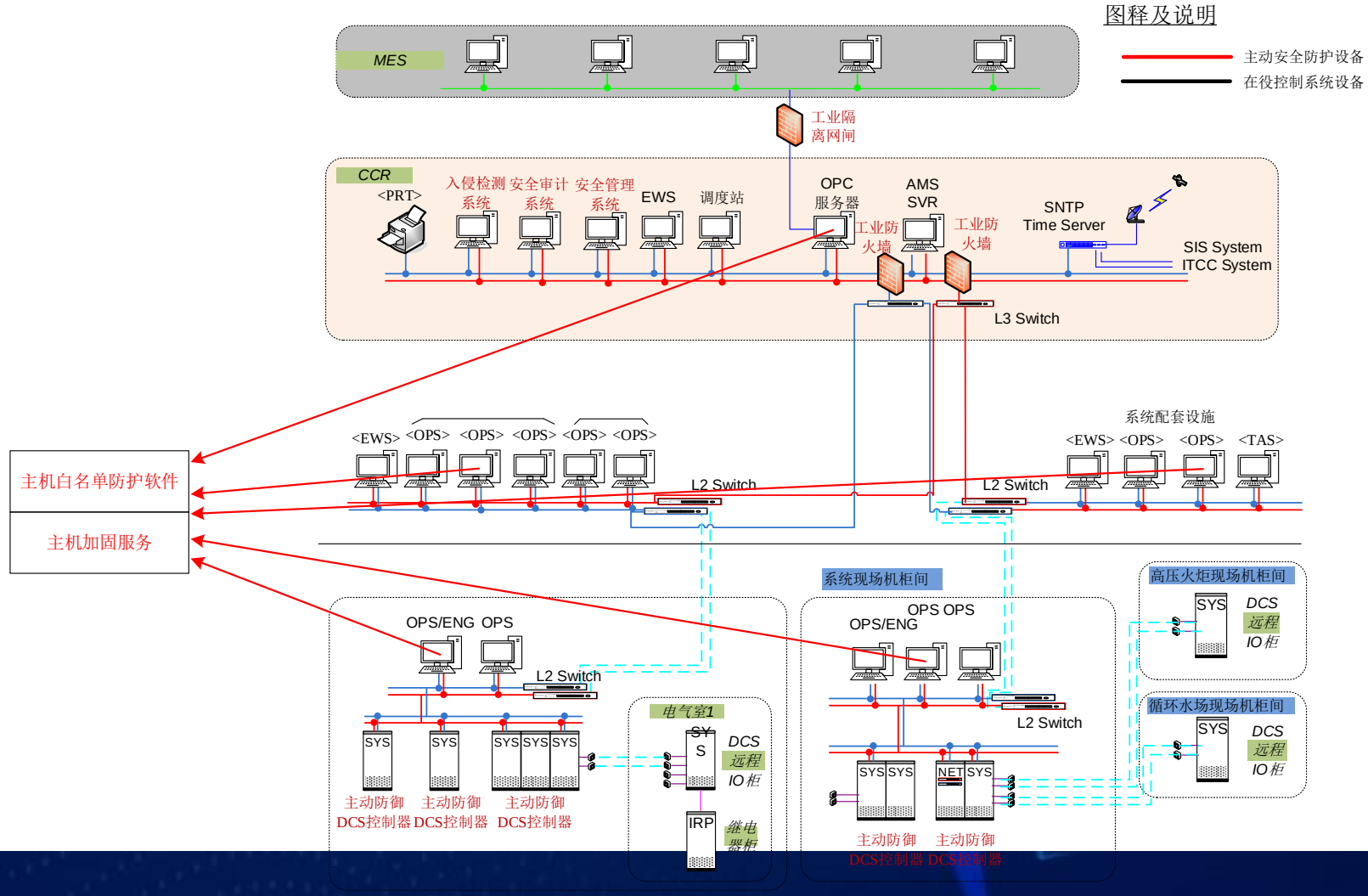
边界抵御

- 业务流程审计
- 操作运维审计
- 网络流量审计

一体化审计

- 网络健壮性能力
- 可信计算平台

内生安全



和利时工业信息安全产品谱系

基于嵌入式可信计算的主动防护

HollySys

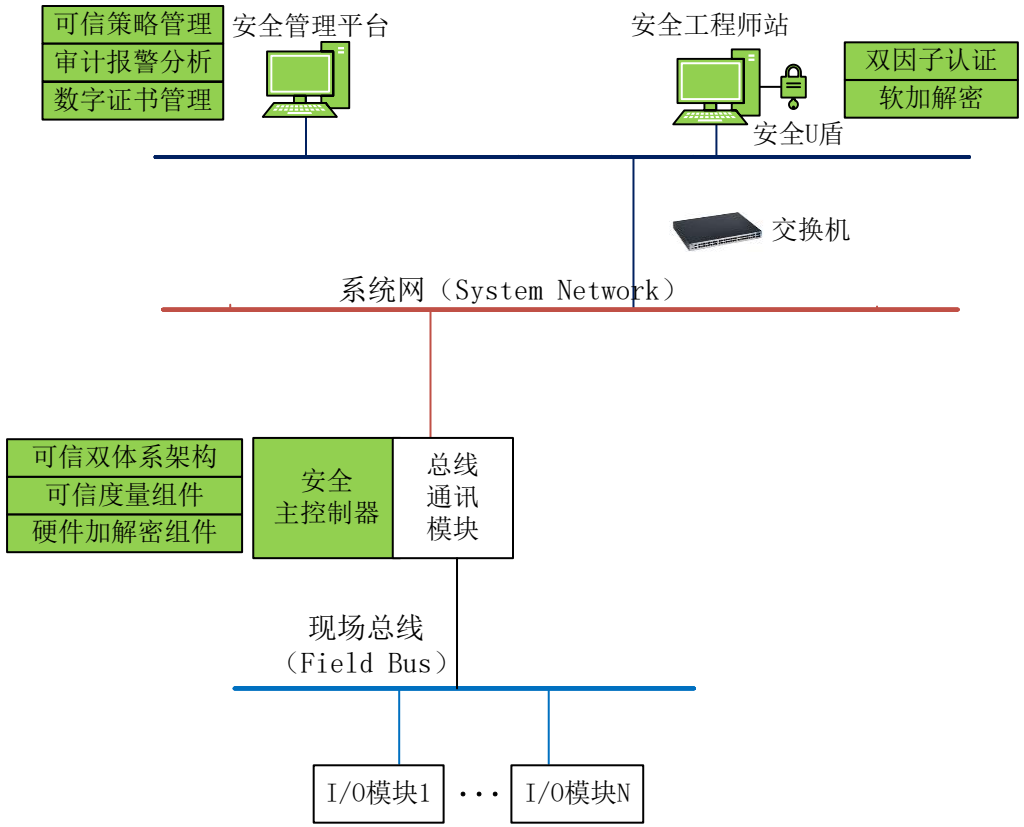
运算与保护并行-主动免疫

可信计算体系结构-上层应用进行透明可信支撑

安全可信策略管控-识别可信和非可信的成分，保障应用执行环境和网络环境安全

应用于嵌入式环境下，满足工业嵌入式应用场景的高实时性、高可靠性、分布式、自主化需求

自主可信控制系统

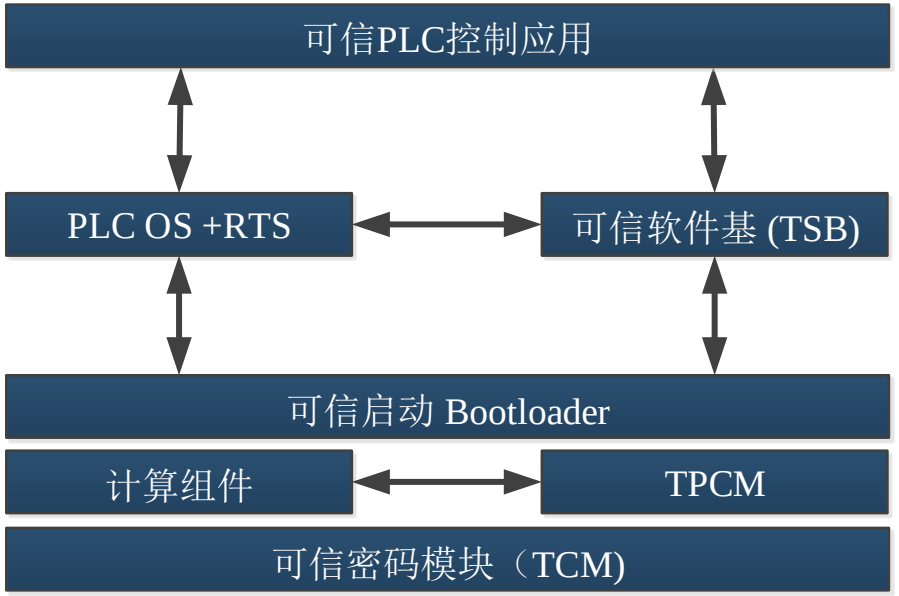


结合自主可控PLC，实现控制器主动防御及配套信息安全防护，满足国家关键设施应用需求，树立国内领先技术优势：

- 系统：产品组件与核心技术-全国产化自主可控
- 控制器：内生双体系可信架构，主动防御安全可信
- 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

自主可信控制系统

- **安全主控制器的双体系结构：**
  - TCM: 为可信计算提供国密运算支持。
  - TPCM：实现对Bootloader和OS内核的可信度量，控制嵌入式设备硬件启动引导，控制安全核（core0）操作系统启动引导。
  - TSB：在控制器运行状态下对PLC功能进行可信度量，并将度量结果以报警方式上传至管理平台。



自主可信控制系统

和利时LK可信PLC控制系统选用国产加解密芯片作为硬件基础，采用轻量级双体系可信计算技术，填补了可信计算在工业嵌入式可编程控制器领域的技术空白。

LK可信PLC实现了工业控制系统由内向外的主动防护，保证了信息安全关键技术和算法的自主可控，并且是首个在通信防护能力取得Achilles II级认证的国产PLC系统，整体信息安全防护能力达到国际领先水平，目前已成功应用电力、化工、热网、隧道管廊等多个行业。

信息安全行业解决方案

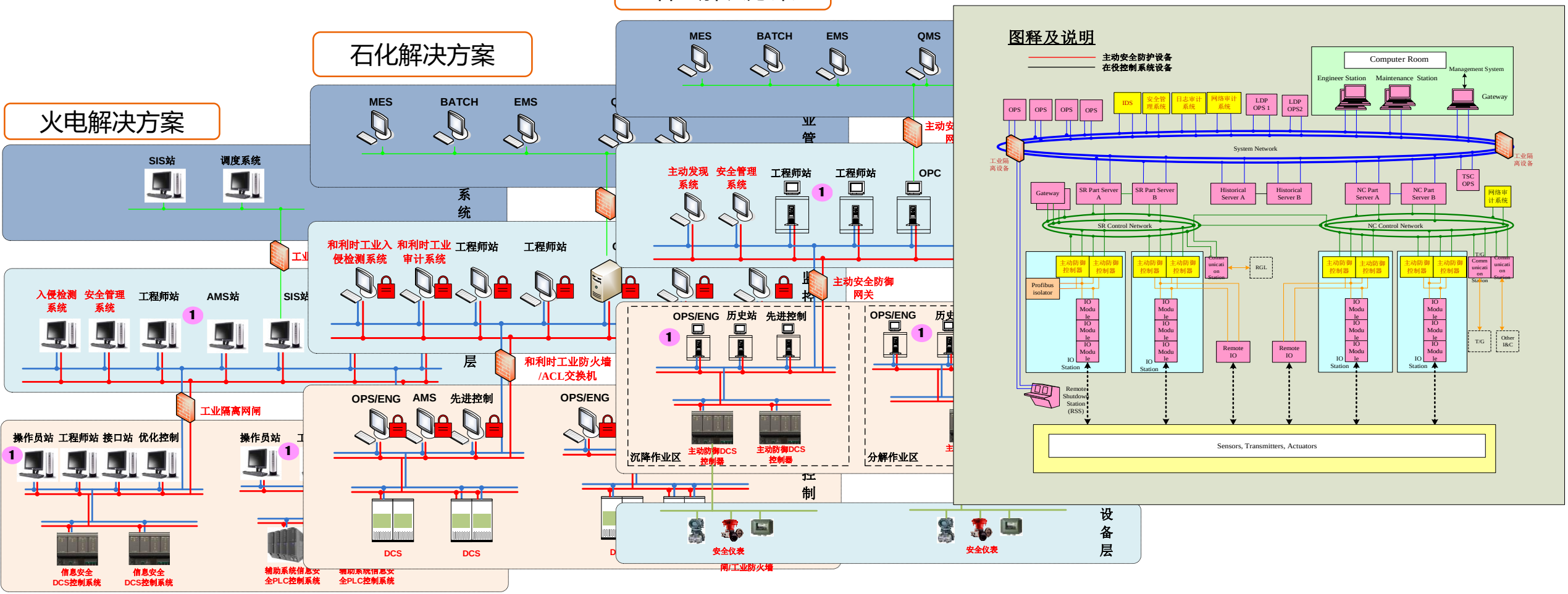
HollySys

火电解决方案

石化解决方案

冶金解决方案

核电解决方案



Thanks

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