工业互联网产业联盟
Alliance of Industrial Internet

工业互联网典型安全解决方案案例汇编V2.0

张峰
中国移动研究院安全所副所长
工业互联网产业联盟安全组副主席

智联赋能　融通创新

2019工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019

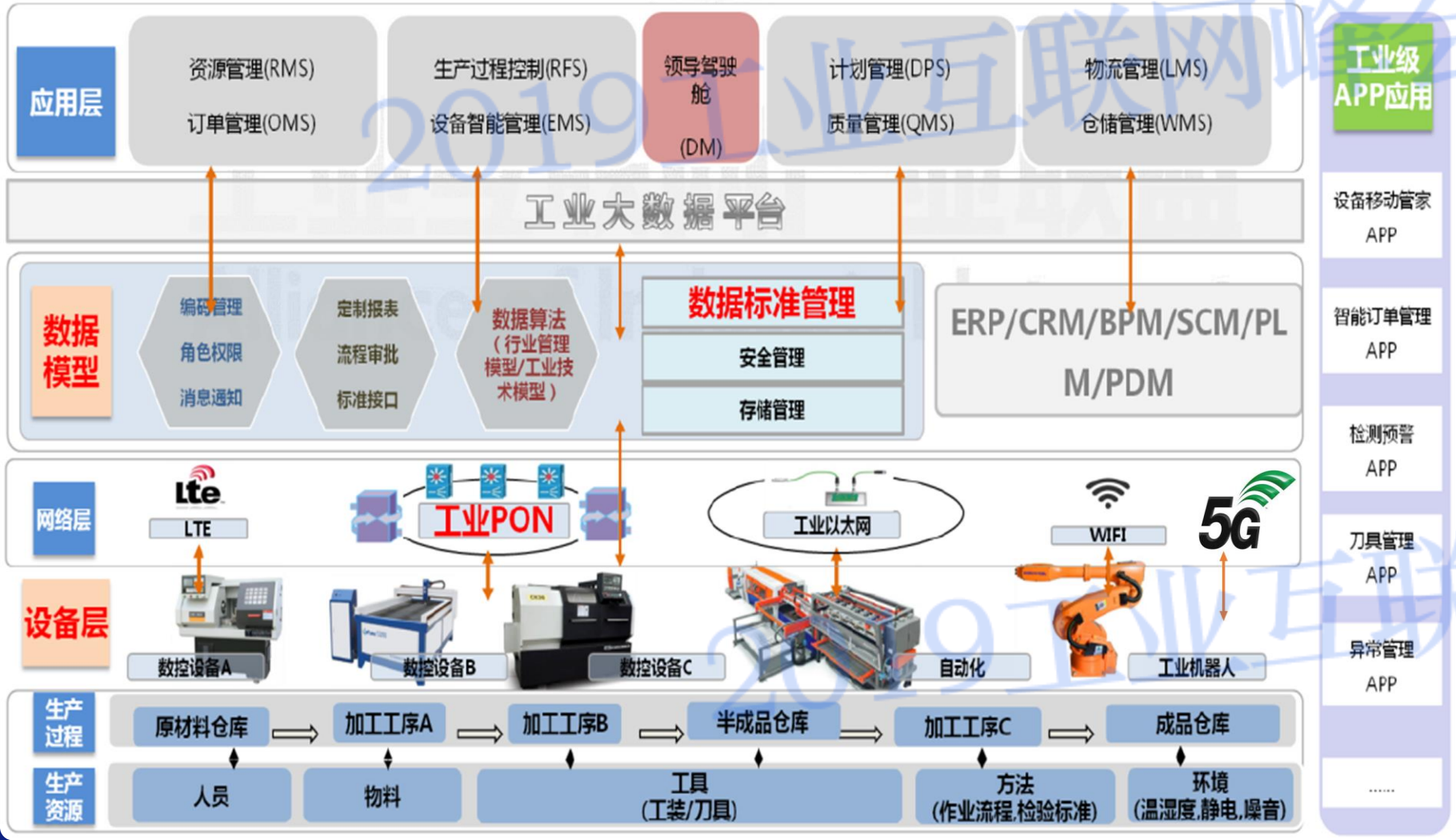
目录
Contents

工业互联网

工业互联网是构建工业环境下人、机、物**全面互联**的关键基础设施，通过工业互联网网络可以实现工业研发、设计、生产、销售、管理、服务等产业全要素的**泛在互联**。

工信部：《工业互联网网络建设及推广指南》——2019.1

工业互联网



全面互联所导致的突出安全风险：

- 设备安全
- 控制安全
- 网络安全
- 数据安全
- 应用安全

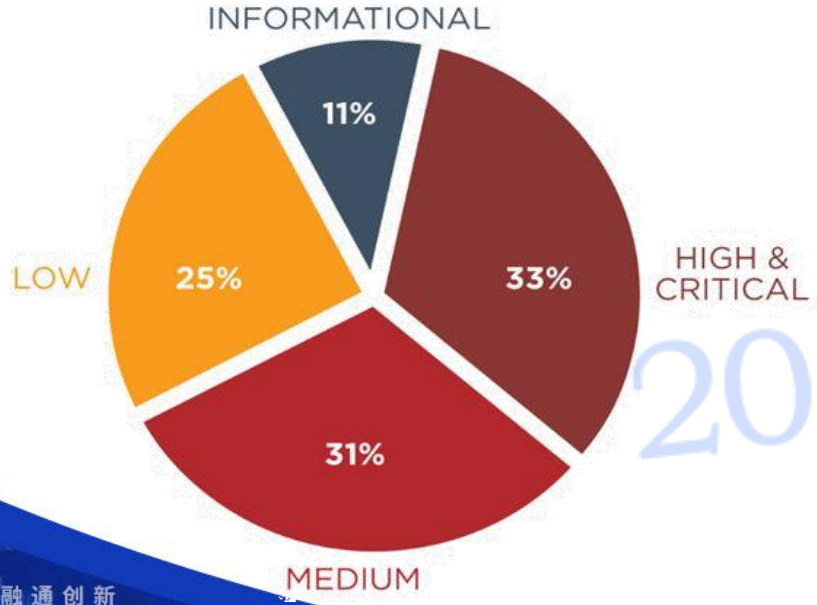
工业互联网典型安全问题

1. 设备/系统老旧，脆弱性高
2. 弱口令、默认口令、共享口令等问题
3. 不同网络域间缺少隔离措施，暴露面大
4. 病毒或恶意代码感染
5. 数据通信无加密认证
6. 违规使用移动存储设备
7. 缺乏安全审计，无法追根溯源

工业互联网安全

在企业内部，关键工业设备系统老旧，升级周期长，存在**高危**风险，工业互联网安全形势严峻。

FireEye iSIGHT Intelligence收集了大量数据，确定了工业设施中至少33%的安全问题属于高风险或严重风险。



在ICS环境中，最常见的高危风险包括已知漏洞、缺乏补丁、缺乏多因素身份认证和网络间隔离等。

HIGH-CRITICAL RISK CATEGORY	DISTRIBUTION
Vulnerabilities, Patches, and Updates	32%
Identity and Access Management	25%
Architecture and Network Segmentation	11%
Encryption and Authentication	8%
Network Management and Monitoring	7%
Insecure Services Enabled	5%
Misconfigurations	5%
Cyber Security Governance and Best Practices	4%
Other	2%

工业互联网安全

在企业外部，针对工业互联网的安全攻击事件爆发频繁，而企业的安全防护建设速度落后于网络攻击发展的速度，急需具有指导性的可落地的最佳实践为企业安全建设提供参考和示范。

Triton恶意软件感染事件

2017年12月，以施耐德电气的Triconex 安全仪表系统控制器为攻击目标的恶意软件Triton，造成中东多家能源工厂的运营中断。

台积电病毒感染事件

2018 年 8 月，台积电遭遇 WannaCry 病毒入侵，导致三大工厂生产线停摆，预估损失约 17 亿人民币。

美国天然气公司被攻击事件

2018年4月2日，美国能源公司Energy Services Group的天然气管道客户交易系统受到网络攻击，造成系统关闭数小时。

《工业互联网典型安全解决方案案例汇编V1.0》

2017年底，面向工业互联网典型行业的安全问题，联合安全研究机构、安全公司进行多方调研，完成了《工业互联网典型安全解决方案案例汇编V1.0》的编制工作，为企业安全建设提供参考和示范。

获取途径

- 在工业与信息化部官网和工业互联网产业联盟官网同步发布

案例内容

- 覆盖智能制造、智能交通、能源石化、水务电力等6个工业垂直领域
- 针对网络安全、设备安全、安全监控、安全审计、风险测评等突出安全问题
- 共遴选、汇编18个典型安全解决方案案例

重要意义

- 首次实现工业安全最佳实践方案的共享，推进工业行业整体安全发展
- 为工业互联网生态链上下游供应商、工业企业用户等在规划、建设和运营工业互联网时的安全参照。
- 促进行业内横向交流与合作

《工业互联网典型安全解决方案案例汇编V2.0》

编制目的

- 工业领域细分行业具有不同的安全需求和特性，V1.0的行业覆盖面有限，有待进一步提升；
- 2018年3月启动V2.0编制工作，进一步扩充典型案例覆盖面，增加面向工业平台安全、数据安全及安全监测等方面的先进安全解决方案；

编制流程

2018.03-06	2018.07	2018.08	2018.09-10	2018.11	2018.12
案例初稿征集	案例汇编整理	案例汇编初稿评审	案例汇编初稿修订	案例汇编终稿评审	案例汇编联盟审核

《工业互联网典型安全解决方案案例汇编V2.0》

在业内各方的共同努力下，完成了《工业互联网典型安全解决方案案例汇编V2.0》的编制工作，现已提交联盟审核。典型案例可为工业互联网垂直行业提供涵盖**横向隔离**、**纵深防御**、**统一监控**、**应急响应**、**等级保护**等全方位安全最佳实践。

- 收到27份解决方案
- 13个典型案例入选
- 9家企业参与贡献
- 覆盖5大类安全领域
  - 网络安全
  - 平台安全
  - 终端安全
  - 数据安全
  - 安全闭环管理
- 采用6+种技术手段
  - 威胁情报
  - 白名单
  - 异常行为检测
  - 智能加密
  - 无损漏洞检测
  - ……
- 应用在6大垂直行业
  - 轨道交通
  - 制造行业
  - 能源化工
  - 电力行业
  - 水务行业
  - 石油石化

汽车制造行业勒索病毒应急处理和安全解决方案

安全问题

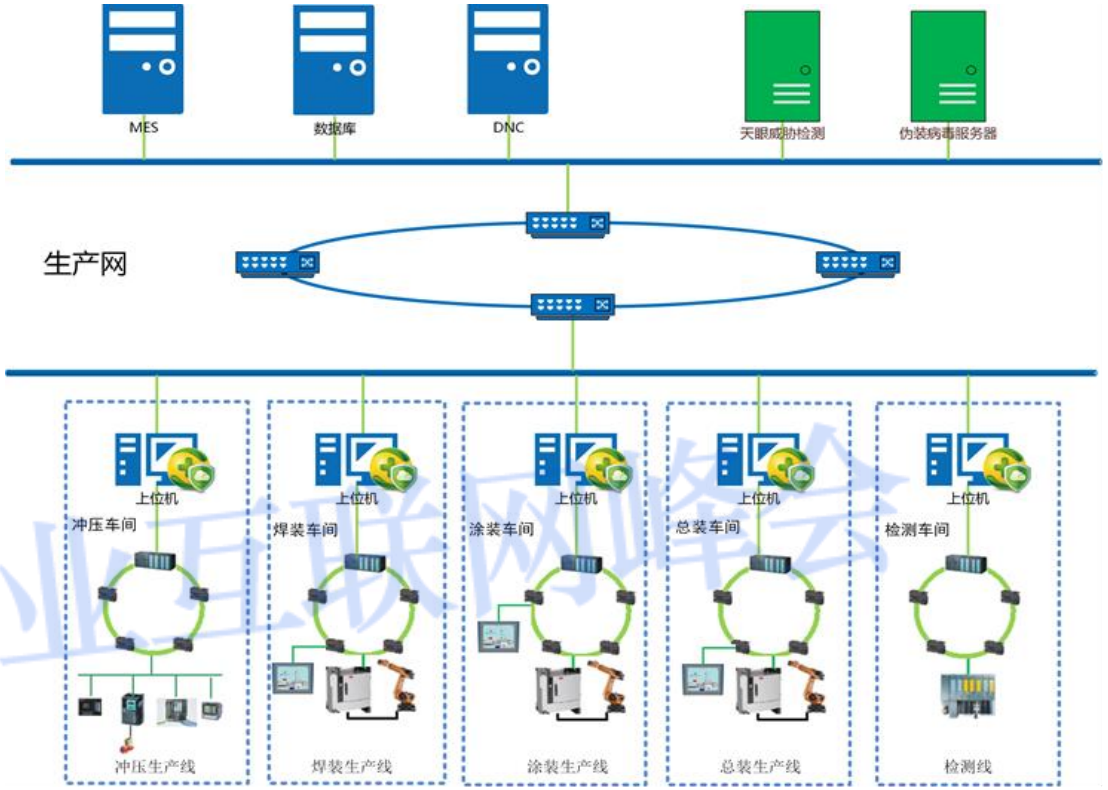
国内某汽车制造企业遭受病毒侵袭，生产制造产线几台上位机莫名出现频繁蓝屏死机现象，并迅速蔓延至整个生产园区内大部分上位机，产线被迫停止生产。

解决方案

1
- 应急处置
- 部署伪装病毒服务器，并将DNS指向此服务器，同时统计中毒终端

2
- 感染处理
- 关闭445等端口，备份数据并进行杀毒处理

3
- 安全加固
- 部署主机防护软件



某电厂信息安全监管与预警平台建设案例

安全问题

① 水电厂内各系统（各机组测温系统、厂用电系统和坝区系统等）之间未进行有效的网络隔离，可随意互访

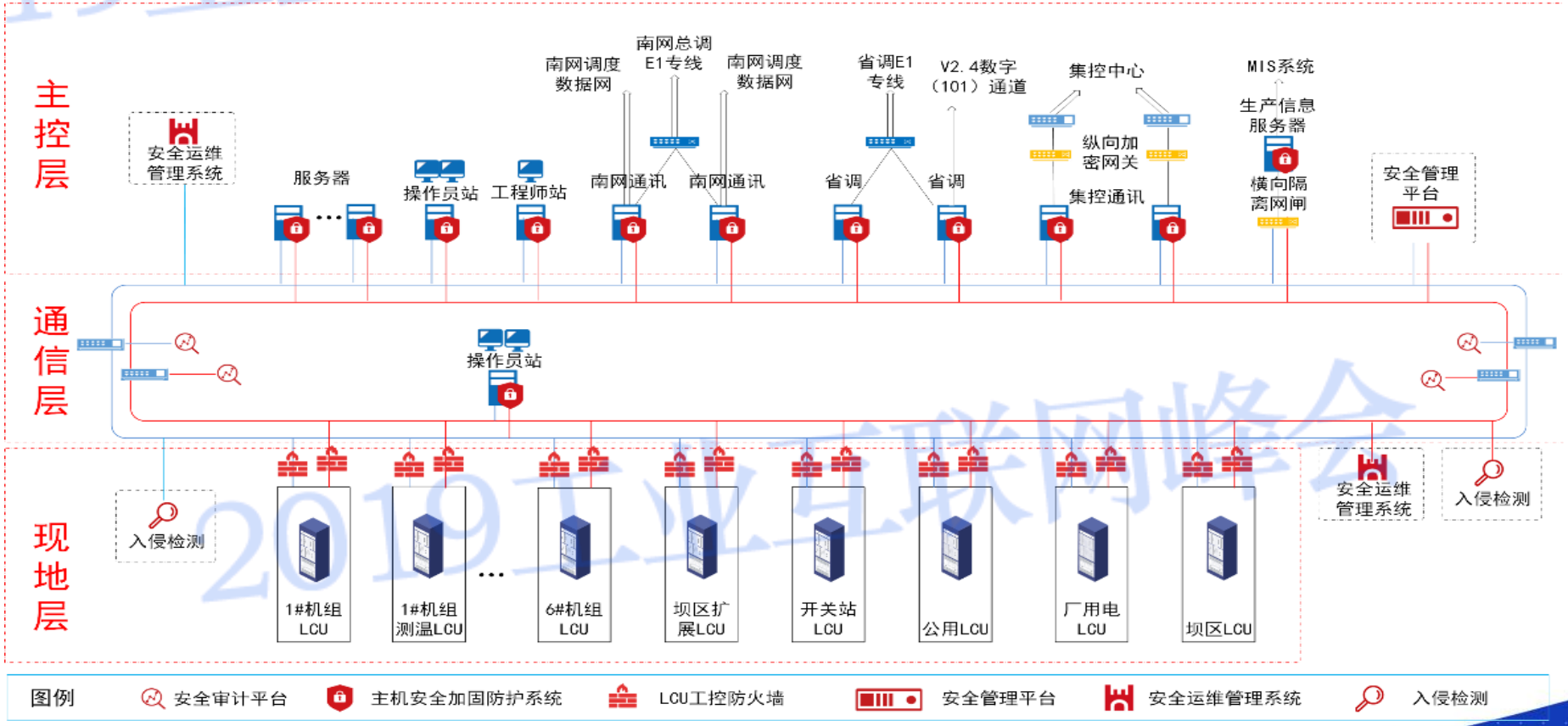
② “无人值班，少人值守”使生产控制大区遭受攻击的风险增加；

③ 需采取有效措施对移动U盘等外设的使用进行管理。

④ 需要重点管控维护过程中的关键操作行为并对所有操作行为进行取证。

解决方案

打破了传统“黑”的防护模式，打破工控安全信息孤岛，以更符合工业现场特性的防护手段，以“一个中心，三重防护”的防御体系，将传统的“被动防护”转化为“主动防御”。



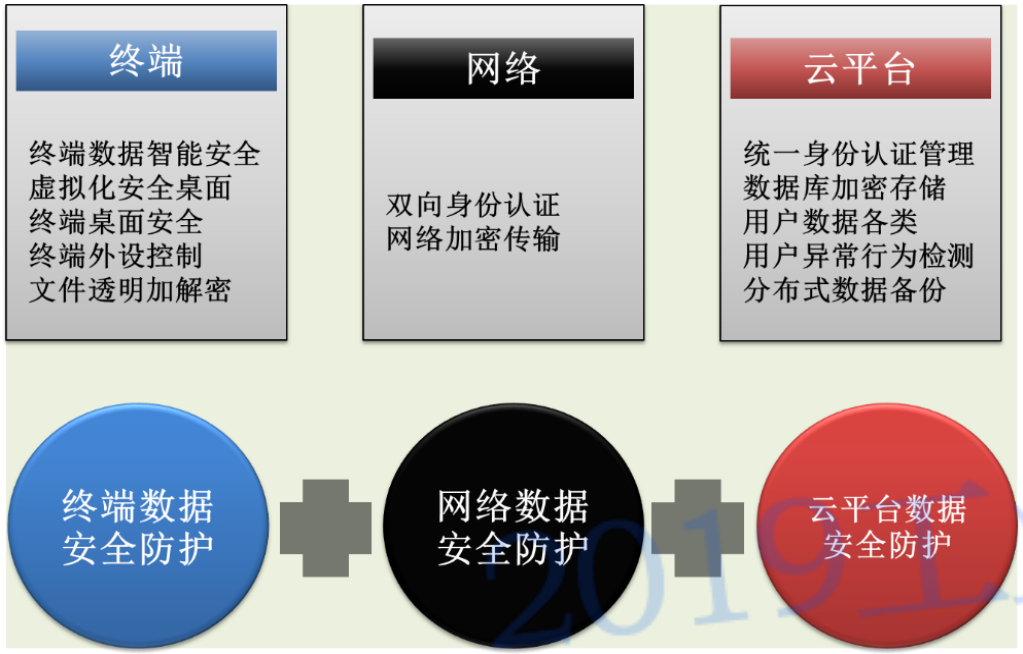
工业互联网数据安全解决方案

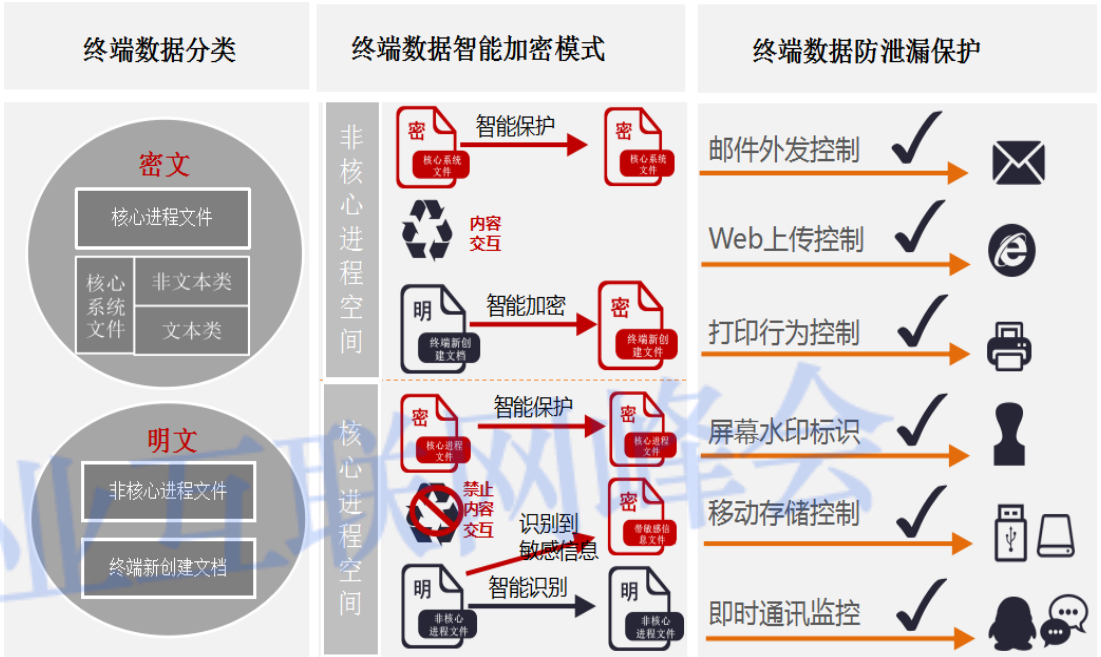
安全问题

- 商业秘密泄露
- 图纸数据随意篡改
- 电子文件残留

解决方案

面向工业设计数据全生命周期安全管理的解决方案





城市污水处理厂安全解决方案

安全问题

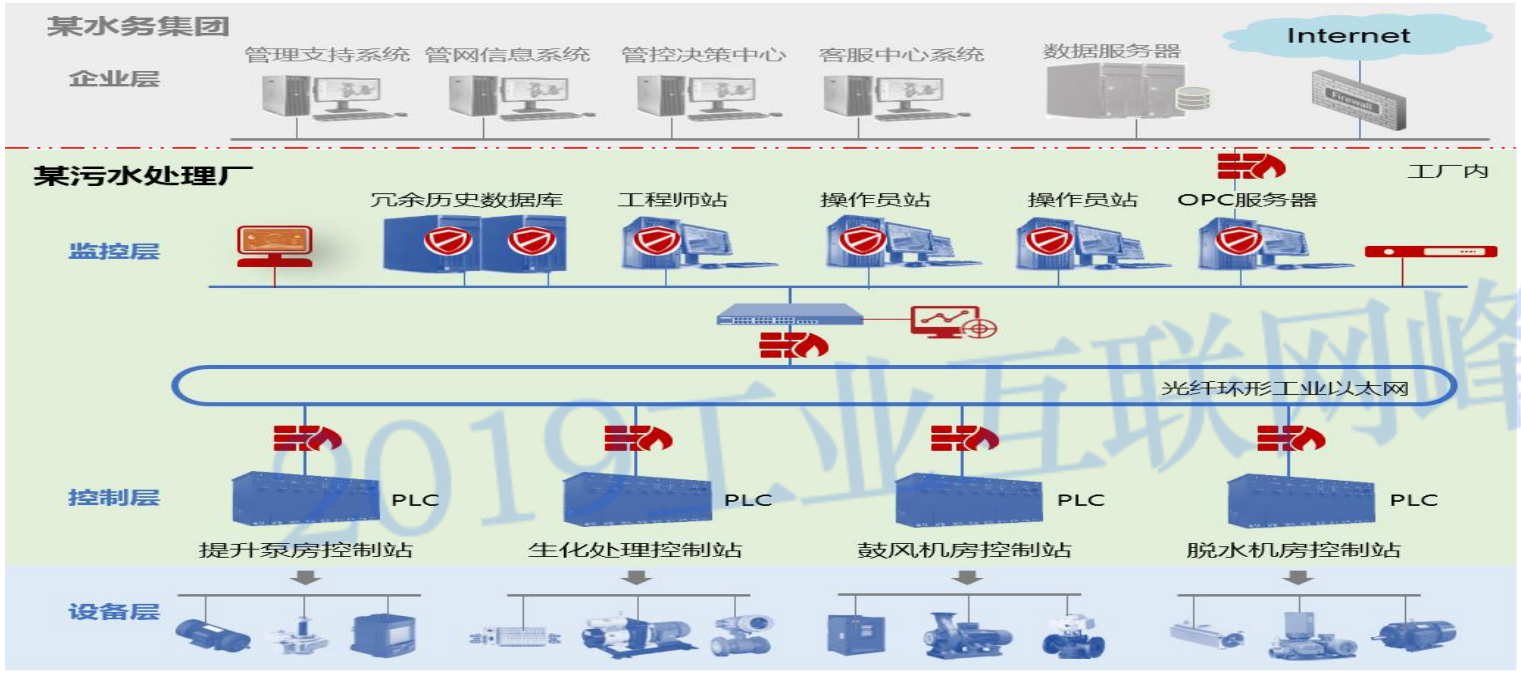
① 数据通信无加密认证机制

② 控制系统普遍存在着未设置口令、默认口令、弱口令、共享口令等问题

③ 缺乏安全日志，对已有安全日志缺乏监控审计，无法实现对整个工控系统安全的可感知与可控制。

解决方案

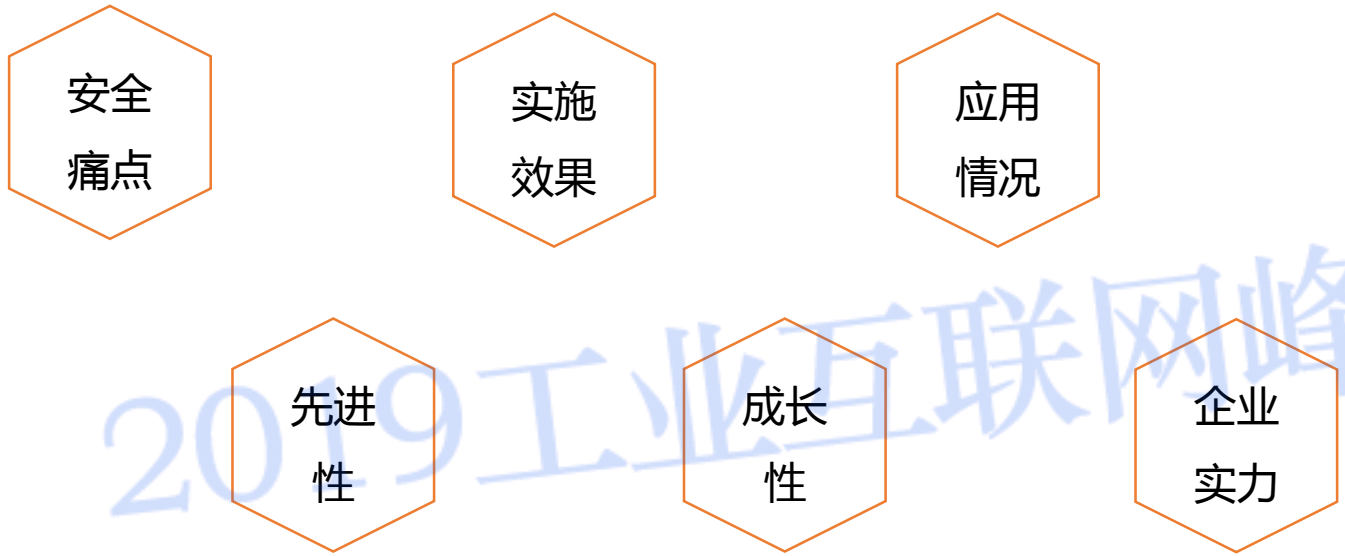
构建了覆盖控制系统基础设备安全、实时控制行为安全、业务流程作业安全的一体化深度安全防护体系，防止非授权或意外的访问、篡改、破坏和损失，确保控制系统能长期安全稳定地运行，保障城市污水处理厂出水水质的安全。



联盟评优

2019年4月，联盟将展开工业互联网优秀安全解决方案的评选工作，优秀方案从《工业互联网典型安全解决方案案例汇编V2.0》中遴选，符合评优条件且评选答辩后，综合领先的方案将被入选工业互联网产业联盟的优秀案例集，为推动工业互联网的繁荣与安全作出更大贡献。

评选要素



感谢业界各知名公司踊跃贡献最佳实践，共同促进我国工业互联网的繁荣和安全。

中国移动 China Mobile

360

北京威努特技术有限公司 Beijing Winicssec Technologies Co.,Ltd.

CEC 中国电子

Tencent 腾讯

HUAWEI

敏捷科技 agile technology

长扬科技 CHANGYANG TECH

万联网络

工业互联网产业联盟
Alliance of Industrial Internet

Thanks

智联赋能　融通创新

2019 工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019