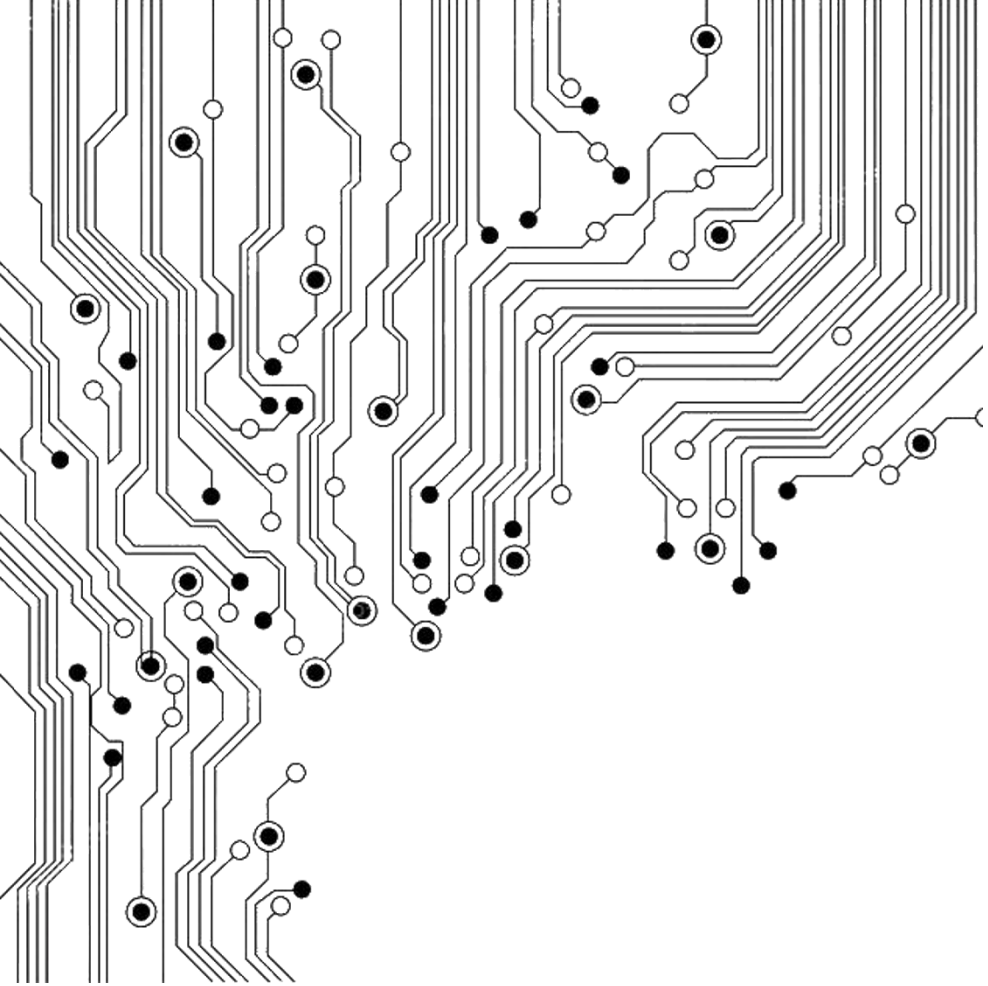


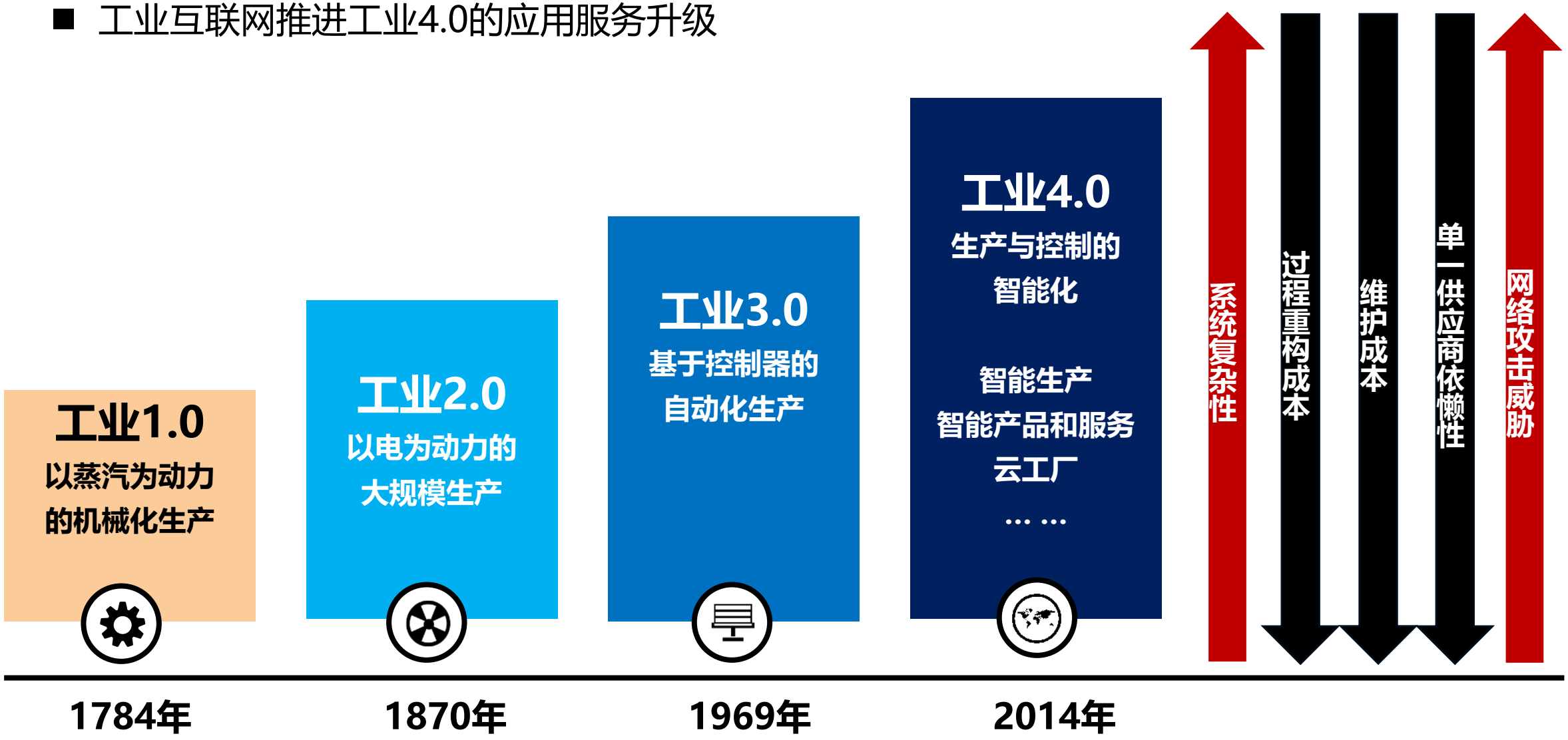
工业互联网信息安全
拓展知识

华东师范大学
刘虹

目录

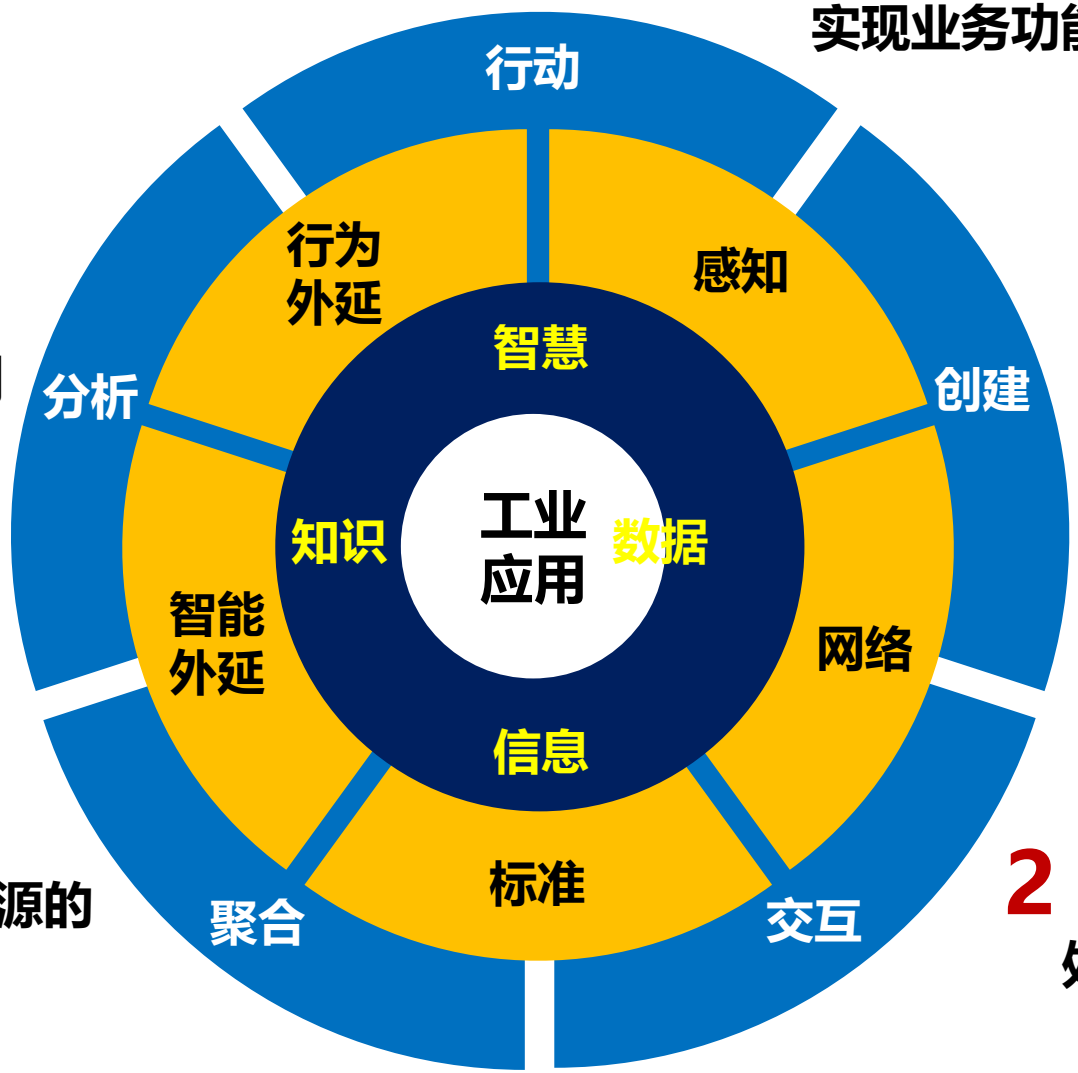
工业革命的演进

- 工业互联网推进工业4.0的应用服务升级



工业互联网的信息链

5 促使工业设备触发特定行为，
实现业务功能调整或优化



4 分析数据和信息，
通过解释原因，实现预测

1 通过传感器监控设备行为，
并产生数据和信息

3 将来自不同来源的
信息进行聚合

2 数据和信息通过网络传输到
处理中心，通过标准化实现交互

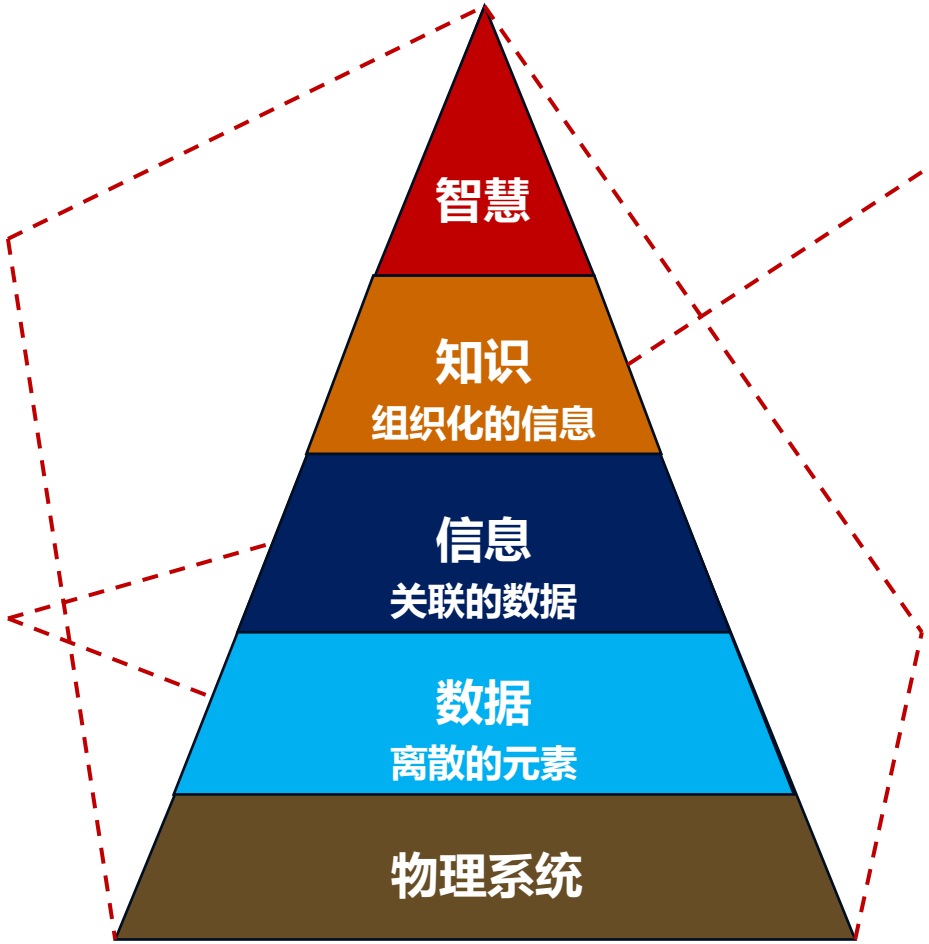
工业互联网的信息链

挑战1

OT和IT跨界协作需要建立
物理网络空间联接融合

挑战2

超过40种工业总线，
协议专用私有，
数据和信息流通难度大



挑战3

信息不精确、非完整，
知识模型构建难度大

挑战4

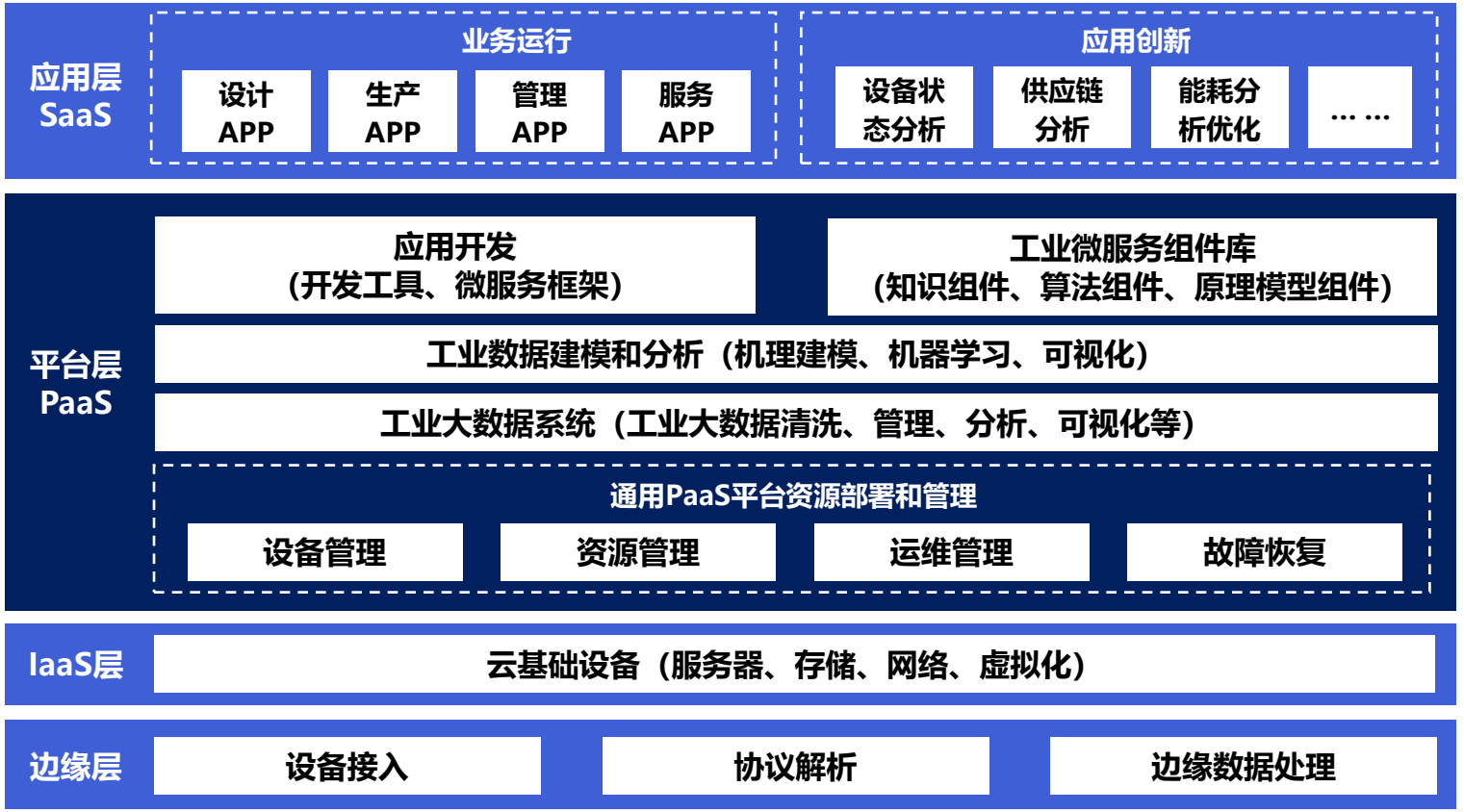
产业链变长，
全生命周期数据集成，
增加端到端协作难度

工业互联网平台

■ 工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析和服务体系。

- 边缘数据是基础
- 工业IaaS是支撑
- 工业PaaS是核心
- 工业APP是关键

数据+模型=应用



参考《工业互联网平台白皮书》

工业互联网平台

- 工业互联网平台：数据+模型=应用

工业数据

物理终端

业务流程

研发工具

生产工艺

代码化
参数化
图形化

分析模型

业务逻辑模型 “因果”

理论模型　逻辑模型　部件模型
工艺模型　故障模型　仿真模型

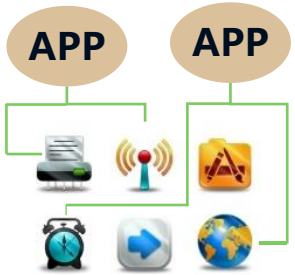
数据驱动模型 “相关”

数据挖掘　机器学习　控制模型
聚类分析　关联分析　回归预测

应用服务

整体式架构

微服务架构



状态感知

实时分析

科学决策

精准执行

工业互联网平台的核心

■ 工业互联网平台的核心是在工业技术原理、行业知识、基础工艺、研发工具规则化、模块化、软件化基础上形成的数字化模型。

从哪来

物理设备

业务流程逻辑

研发工具

生产工艺

怎么建

代码化编程
参数化编程
图形化编程

MATLAB

python™

Java™

是什么

机理模型“因果”

理论模型　逻辑模型　部件模型
工艺模型　故障模型　仿真模型

数据驱动模型“相关”

数据挖掘　机器学习　控制模型

什么样

整体式架构

微服务架构

怎么用

状态感知　实时分析　科学决策　精准执行

描述
诊断
预测
决策

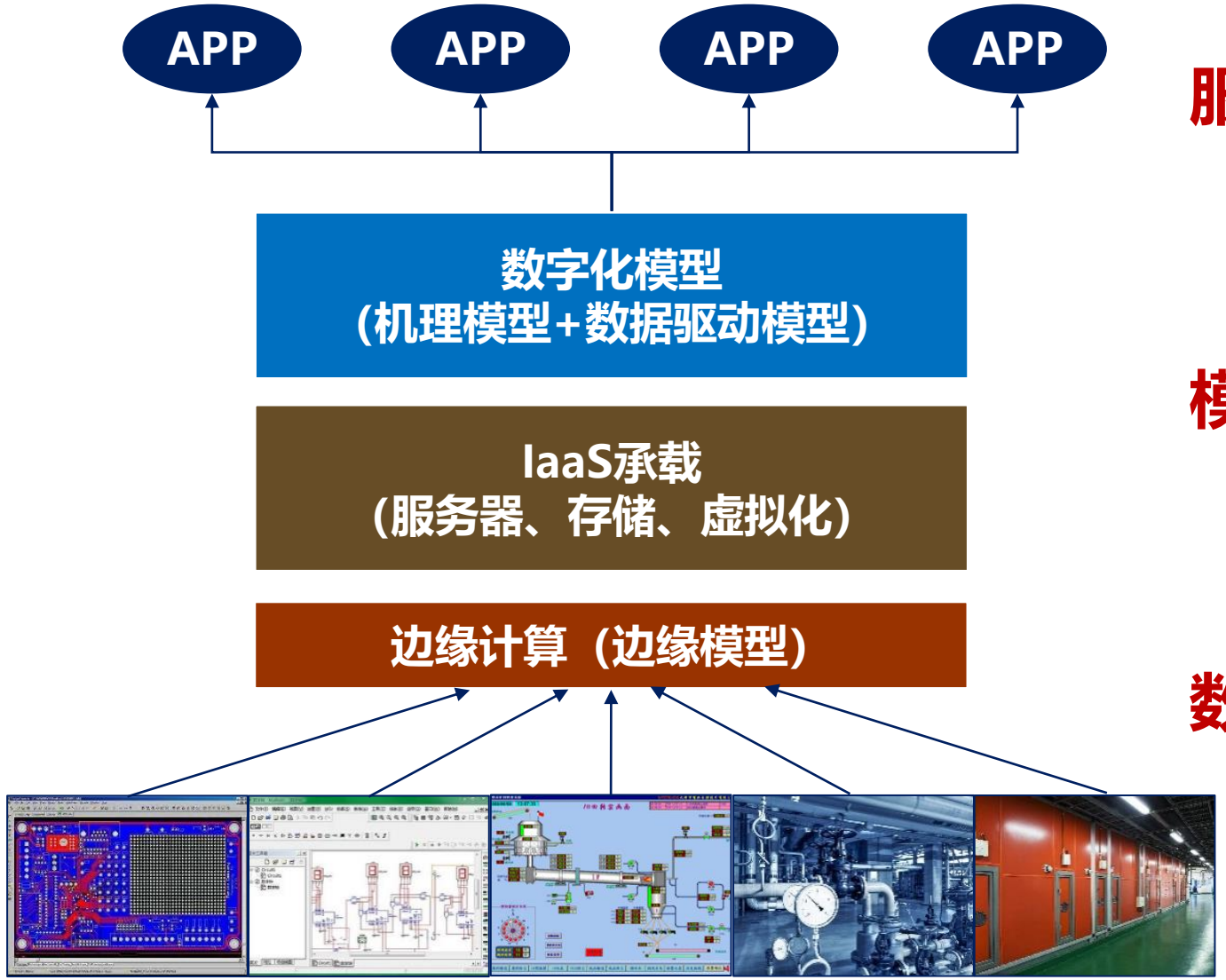
工业互联网平台的“变与不变”

■2个没变：解决的核心问题没有变、解决问题的逻辑没有变

工业互联网平台的“变与不变”

6个变了：

- 数据从哪来
- 数据到哪去
- 模型在哪部署
- 模型怎么部署
- 资源优化深度
- 资源优化广度



服务 = 模型 + 数据

工业互联网的特点

- 主要特点和要求
  - 可靠部署：复杂环境中的工业感知控制设备
  - 安全加固：通用软硬件平台和网络通信协议
  - 稳定运行：异构边缘节点计算节点
  - 灵活服务：工业互联网微服务架构

终端智能化

网络泛在化

计算边界化

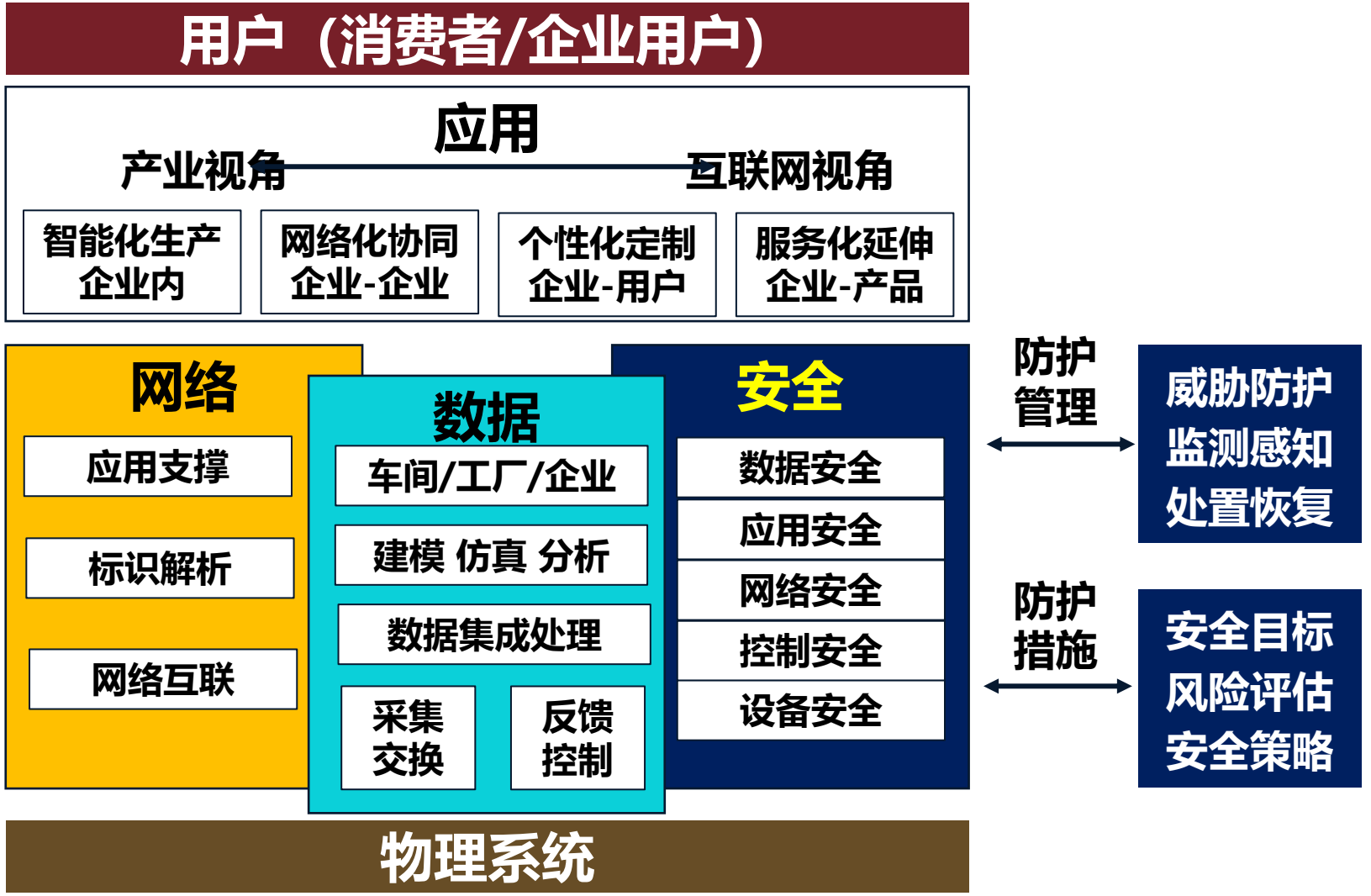
网络扁平化

服务平台化

目录

工业互联网安全

- 工业互联网安全
  - 设备安全
  - 控制安全
  - 网络安全
  - 应用安全
  - 数据安全



参考《工业互联网平台白皮书》

工业互联网的安全视角

- 边缘层：物理空间隐性数据在信息空间的显性化

数据采集

数据不足：部署传感器进行数字化改造，支持设备数据感知和互联

协议转化

数据杂乱：协议识别解析，支持TCP/IP、Modbus、Profinet等主流通信协议

边缘智能

数据计算：数据本地存储、分发和预处理

数据**不敢**传

数据**不能**传

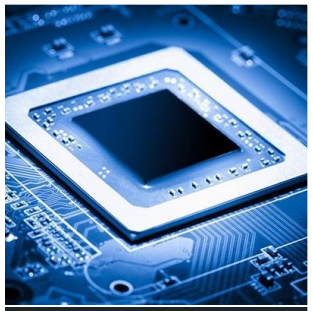
数据**不必**传

网络延迟
协议适配
数据泄漏

资源功耗
负载均衡
离线处理

工业互联网的安全视角

- 边缘层：工业嵌入式系统基础软硬件安全测试和缺陷发现



安全可信验证实时操作系统

FreeRTOS　SafeOS

Windows Server　WIND

安全核心器件（芯片/控制器）

设备数据接入与控制
对云端数据上传和控制接收
边缘端智能分析服务

嵌入式C程序单元测试

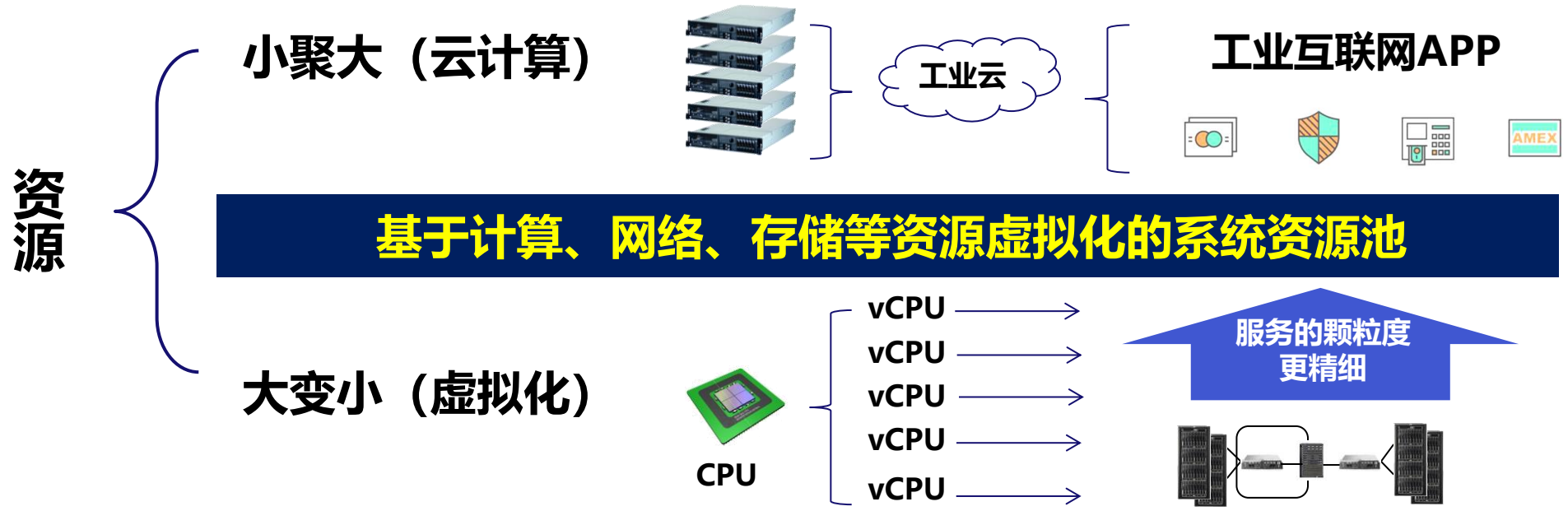
- 最高等级动态测试要求语句、分支及MC/DC覆盖达到100%
- 符合IEC 61508等功能安全标准

代码运行时动态缺陷检查

- 动态符号执行求解引擎
- 防止内存泄露、内存重复释放
- 防止除零、空指针、数组/指针越界
- 代码签名，保障运行代码授权

工业互联网的安全视角

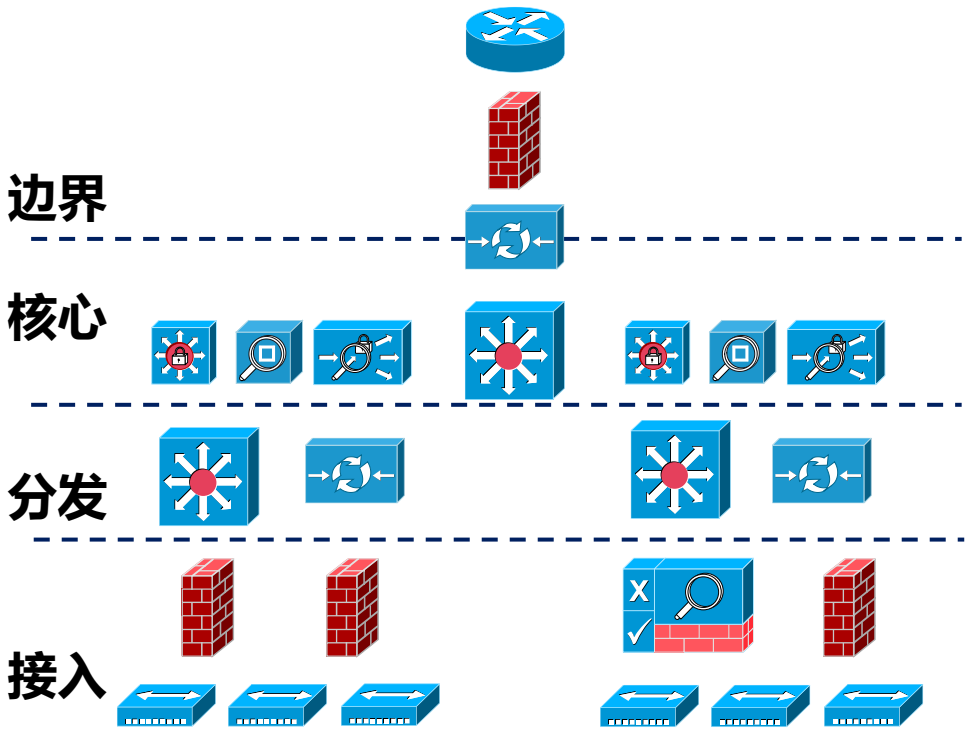
- IaaS层：基于计算、网络、存储等资源虚拟化的系统资源池
  - 支撑工业数据“采集、存储、应用、共享”全生命周期
  - 支持数据聚合和基础设施复用，从烟囱式分散平台向融合式集中平台演进



工业互联网的安全视角

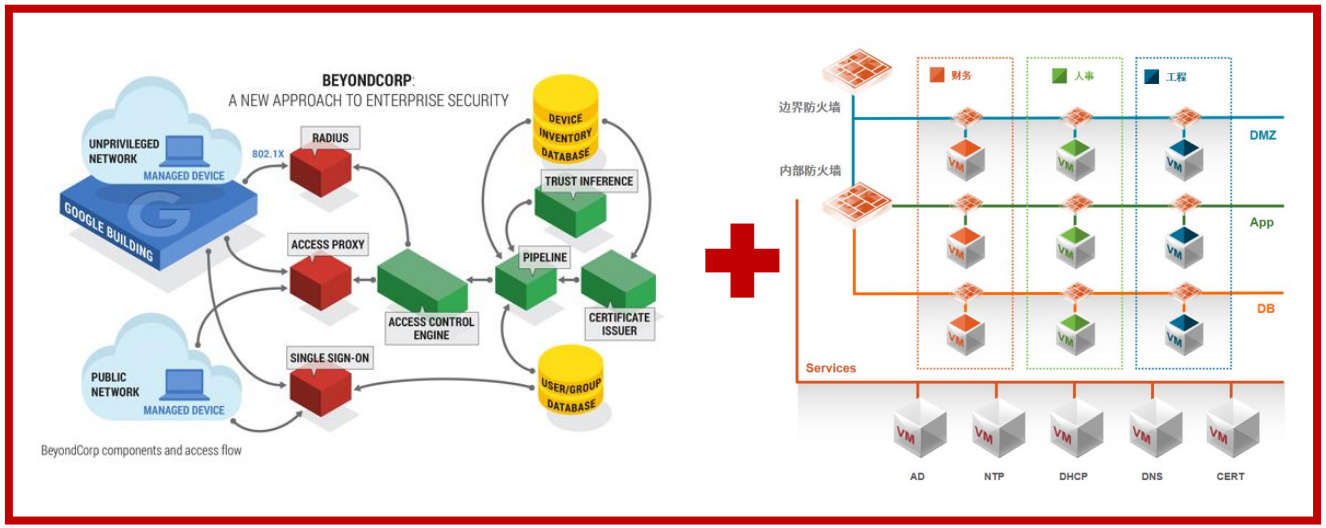
- IaaS层：基于零信任和微分段的软件定义安全策略

安全叠加：隔离+并行+中心化



谷歌BeyondCorp

限制并严格执行访问控制
接入验证所有数据来源
监控审计网络流量日志

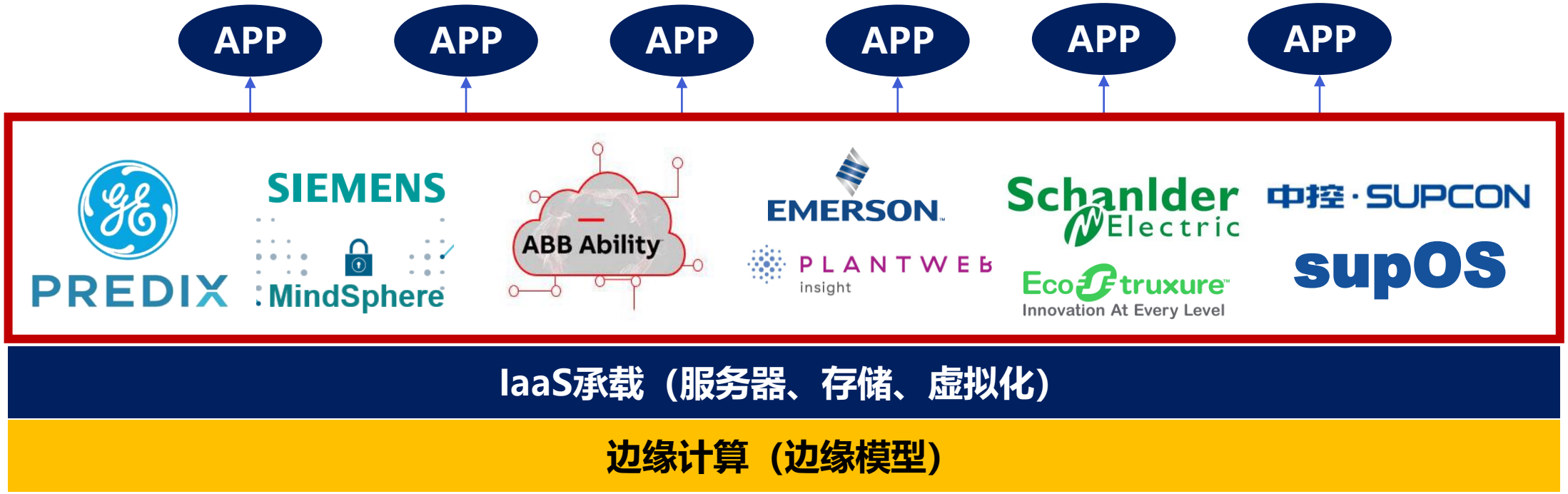


VMWare NSX

利用微分段在
数据中心内部
对虚机进行隔离

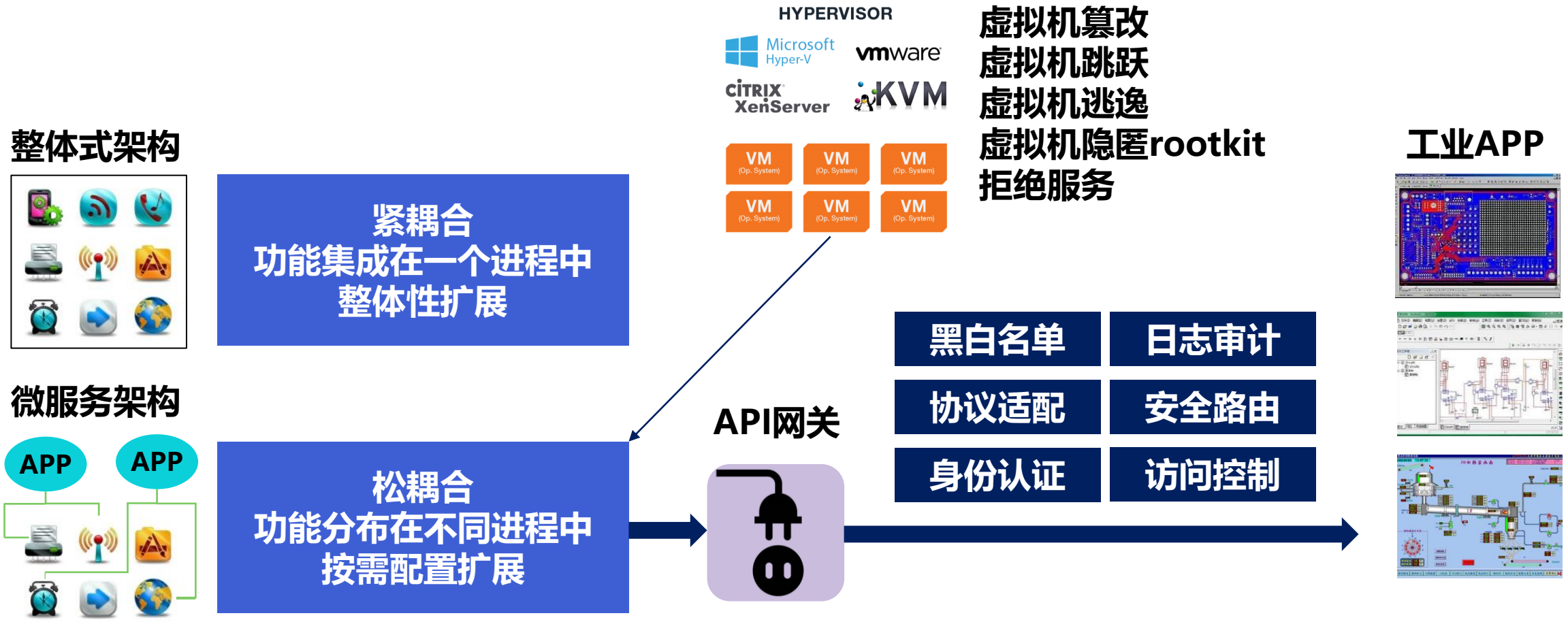
工业互联网的安全视角

- PaaS层：基于云基础设施的工业互联网操作系统
  - 向下调试设备、业务系统等软硬件资源
  - 向上承载工业APP等应用服务



工业互联网的安全视角

- PaaS层：提供工业APP创建、测试和部署的安全开发环境



工业互联网的安全视角

- SaaS层：面向特定行业、特定场景的应用解决方案
  - 服务于研发、生产、管理、服务全过程
  - 全产业链+产品全生命周期

云化：传统软件云化改造
（研发设计、经营管理、生产制造）

云生：新型工业APP
（状态监控、故障诊断、监测预警）

设备性能优化
工业流程优化

深度

广度

单元级
系统级
平台级

+

状态感知
实时诊断
分析预测
科学决策

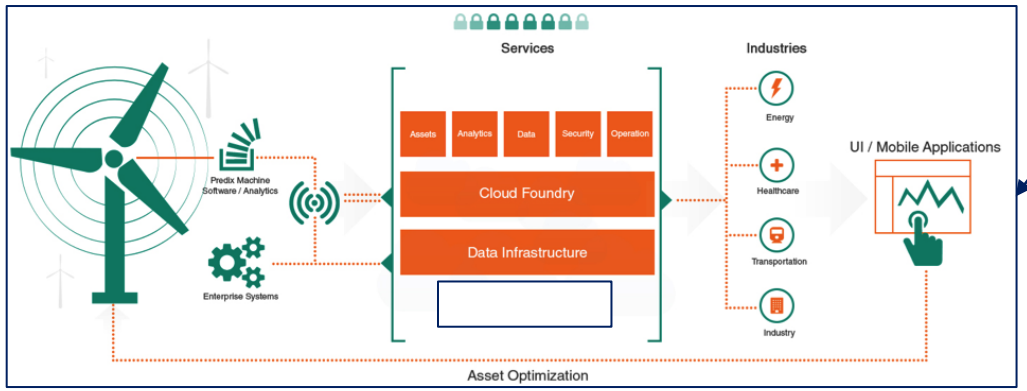
工业互联网的安全视角

- SaaS层：支持代码审计的已知漏洞分析和未知漏洞发现

云化APP

云生APP

基于微服务固化的工业APP：开放、通用



软件成分分析及漏洞扫描
- 源代码和二进制文件扫描
- 漏洞关系网
- 开源许可证合规性

安全传输
- 基于证书的安全链接
- 端到端的安全通道
- 提供接口供APP调用

安全存储
- 密钥保护
- 加密数据存储

代码保护
- 代码混淆
- 机密数据保护
- 预防代码提取和篡改

设备指纹
- 通过手机特定的软硬件标识生成设备指纹

工业互联网安全需求

基于硬件的信任根

单纯软件防护对高安全设备是不够的，硬件防护可以检测并减缓物理攻击，防止攻击者重复使用某攻击手段

最小化的可信计算基础

可信计算基础的最小化在保证安全操作环境外，暴露给高攻击者的机会大大减少

纵深安全防御

防御必须是深度多样化的，同时对攻击造成的伤害必须可以采取减缓措施

分区化安全防护

分区是有硬件强制提供边界防护，以防止一个软件分区中的缺陷或漏洞传播到系统中其他软件分区

证书化的身份验证

证书使用私钥签名并使用公钥验证的身份和授权声明，证书难以被窃取、伪造或者假冒

可更新的安全措施

在设备受到安全威胁后，可以通过自动更新功能达到更安全状态

可审计的安全设施

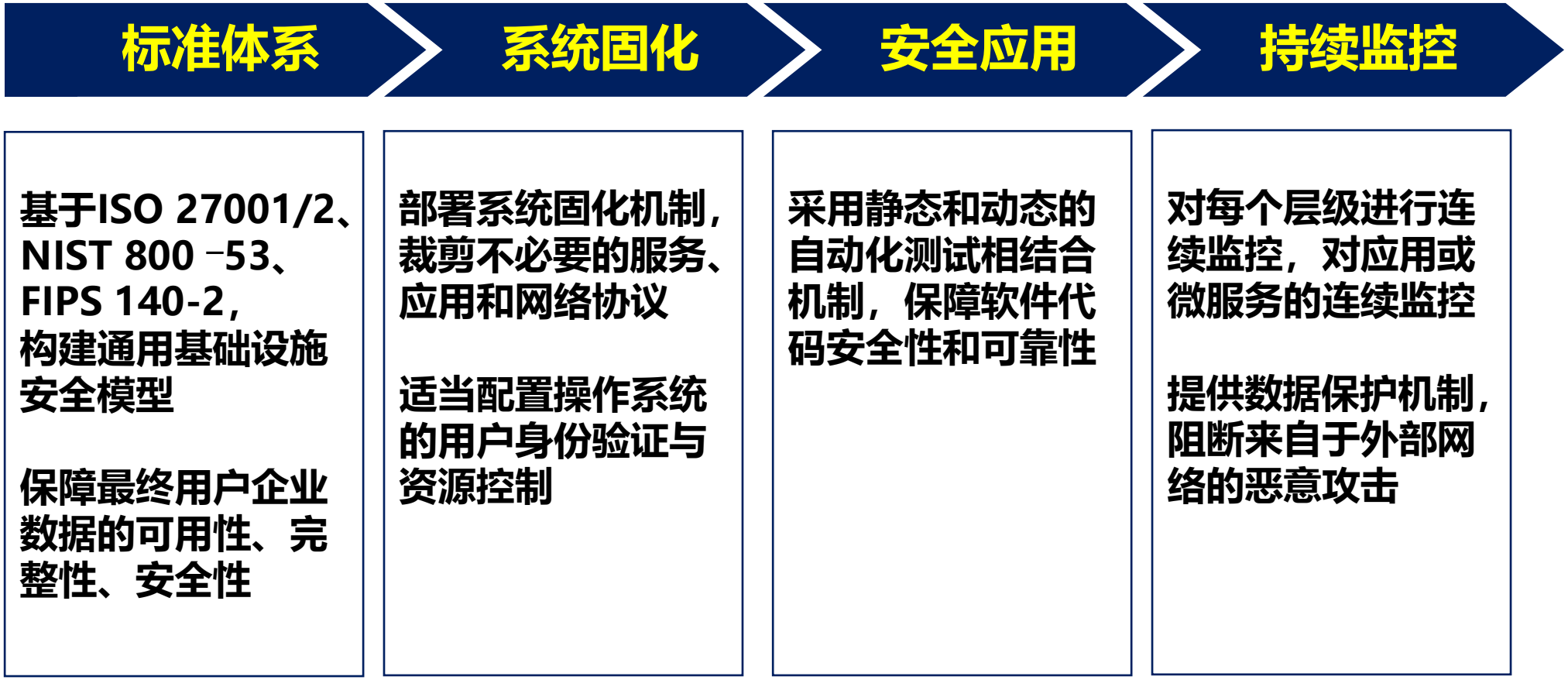
攻击过程和破坏结果是可以记录、追踪，达到事后审计效果

不可克隆的系统镜像

系统不被克隆机制可以用来防止攻击者采用重复的方法获取系统信息，同时也防止系统被篡改

工业互联网的安全趋势

- 构建端到端信任、动静检测监测的内生式工业级安全体系



目录

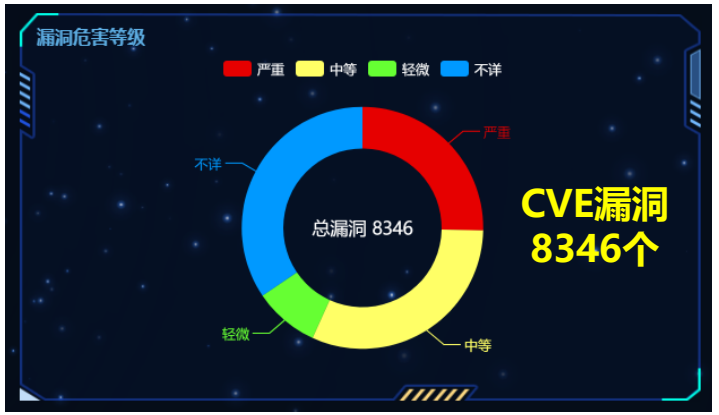
战略背景

■ 工控系统是“制造强国”和“网络强国”战略重要保障，是国家关键基础设施的重要组成部分，是汽车电子、轨道交通、能源电力重点领域的“神经中枢”。

工控信息安全问题凸显：公安部18个重点领域工控系统安全检查：

- 28个省所辖104个地市的451家单位的工控系统现场抽查
- 西门子等国外工控设备存在漏洞，占比93%
- 硬件系统漏洞1.5万个，操作系统漏洞4.7万个，急危和高危漏洞达50%
- 工控威胁事件中，**高危占比58%，中危占比37%**

数据来源：《工业控制网络安全态势报告》



背景现状

- 工控系统安全主要包括**功能安全**（Safety）和**信息安全**（Security）

1. 安全防护薄弱、运行阶段风险高

工控系统在设计、研发和集成阶段未充分考虑安全问题，导致进入运行阶段风险极高，必须贯彻全生命周期安全理念。

2. 国外设备为主，运行受制于人

超过85%存量工控设备被西门子、施耐德等垄断；存在“设备不能碰、配置不能改、账户不能管”，必须坚持自主可控的国产化替代路径。

3. 自主可控关键技术储备不足

工控安全技术原创性不足，缺乏整体技术布局。安全检测评估、监测预警、应急响应等服务能力不足。

4. 行业应用广泛，安全问题复杂

城市基础设施和重点制造行业运行大量工控系统，不同行业工控系统门类复杂，差异显著；同一行业不同装置间系统各不相同，须分类施策。

5. 融合趋势明显，风险交织渗透

随着工业互联网发展，工控安全和互联网安全交织；功能安全和信息安全密切相关，必须整体统筹考虑。

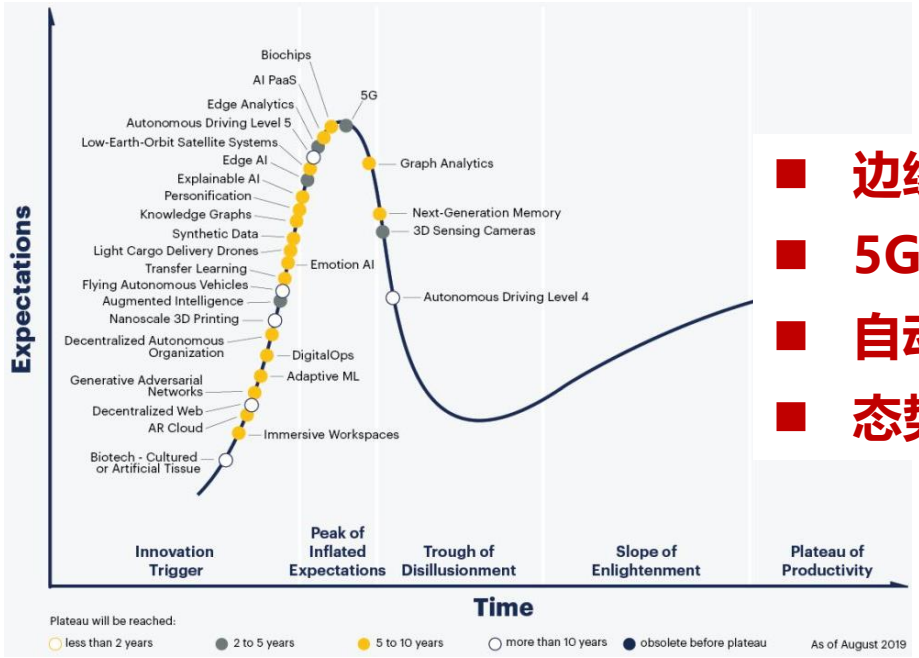
政策方面：国家政策法规

- 法律
  - 2016年《中华人民共和国网络安全法》
  - 2019年《中华人民共和国密码法》
  - 2020年《中华人民共和国数据安全法（草案）》
- 公安部：
  - 2019年**《信息安全技术 网络安全等级保护基本要求》（等保2.0）**
- 网信办：
  - 2017年**《关键信息基础设施安全保护条例（征求意见稿）》**
- 工信部：
  - 2016年《工业控制系统信息安全防护指南》
  - 2017年《工业控制系统信息安全事件应急管理工作指南》
  - 2017年《工业控制系统信息安全防护能力评估工作管理办法》
  - 2017年《工业控制系统信息安全行动计划（2018-2020年）》
  - 2018年《工业互联网发展行动计划（2018-2020年）》
  - 2019年《加强工业互联网安全工作的指导意见》
  - 2020年《工业互联网企业网络安全分类分级指南》
  - 2020年**《“工业互联网+安全生产”行动计划(2021~2023年)》**

技术方面：国外

- 工控安全呈现功能和信息融合化、纵深防御主动化、威胁数据共享化等趋势

单一方式、无延续性的直接性破坏式攻击	简单→复杂	多方式、持续性的深层次隐蔽性攻击
主要采用专用的硬件、软件和通信协议	专用→通用	逐渐采用通用的硬件、软件和通信协议
面向已知恶意代码、威胁、漏洞	已知→未知	面向未知恶意代码、威胁、漏洞
工控安全事件“事中审计、事后溯源”	事中、事后→事前	工控安全事件的“事前态势感知”



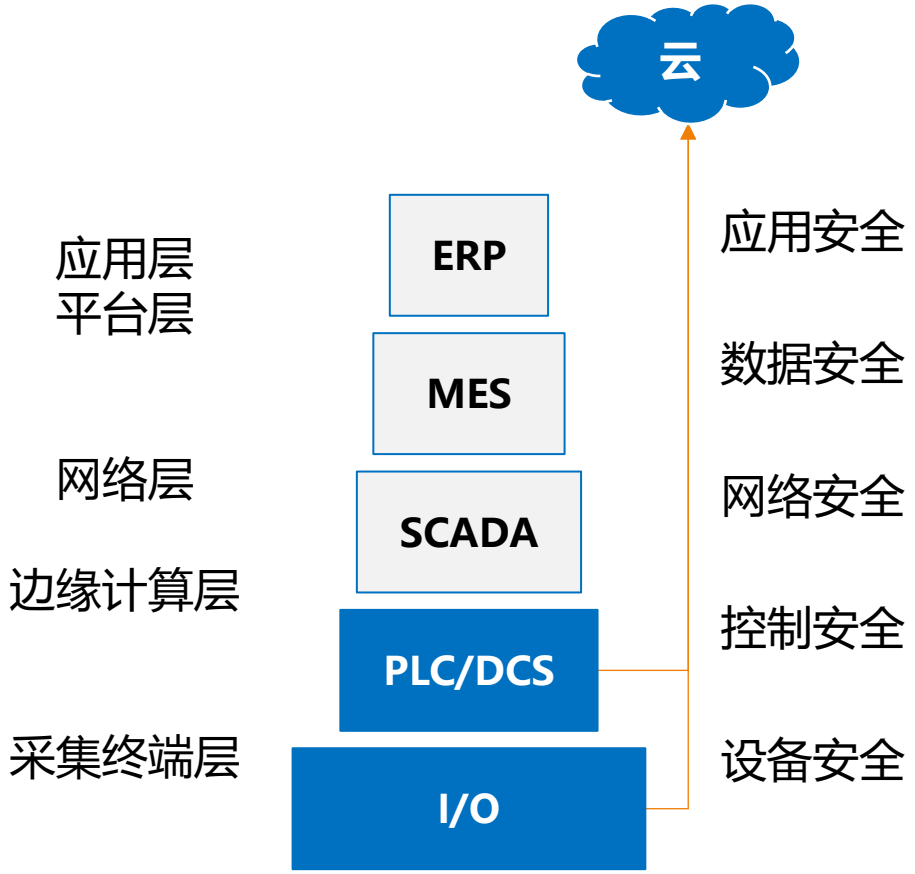
- 边缘计算
- 5G通信
- 自动驾驶
- 态势感知

新一代工控系统安全框架

数据层 应用层	业务应用			
	隐私保护			
	用户隐私保护	企业敏感数据保护		
通信层	保密性	完整性	可用性	
	通信保密性	通信完整性	通信可用性	
	数据保密性	数据完整性	数据可用性	
	信息保密性	信息完整性	信息可用性	
设备层	可靠性			
	设备硬件可靠性	软件功能可靠性	数据分析可靠性	人身安全可靠性
	物理资产			

技术方面：国内

- 面向“云管边端”的接入安全、数据安全、平台安全融合技术趋势



标准方面：国外

- 代表性国际标准：
  - IEC 62443《工业过程测量、控制和自动化网络与系统信息安全》系列标准
  - NIST SP800-82《工业控制系统安全指南》

标准方面：国内

■ 国内工控安全标准体系逐渐完善，正在全面推进标准草案编制工作

工控功能安全标准

汽车电子

- GB/T 18384-1-3

轨道交通

- GB/T 28808
- GB/T 28809
- GB 24339.1-2

电力

- GB/T 12788-2000
- GB/T 13629-2008
- EJ/T 1058-2005
- EJ/T 1223-2007
- NB/T 20055-2011

标准方面：国内相关标准列表

■ 工控信息安全标准列表（TC260单独归口）

序号	标准名称	所出状态
1	《信息安全技术 工业控制系统安全控制应用指南》GB/T 32919-2016	已发布
2	《信息安全技术 工业控制系统安全管理基本要求》GB/T 36323-2018	已发布
3	《信息安全技术 工业控制系统信息安全分级规范》GB/T 36324-2018	已发布
4	《信息 安全技术 工业控制系统风险评估实施指南》GB/T 36466-2018	已发布
5	《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》GB/T 36470-2018	已发布
6	《信息安全技术 工业控制系统安全检查指南》GB/T 37980-2019	已发布
7	《信息安全技术 工业控制系统信息安全防护建设实施规范》	送审稿
8	《信息安全技术 工业控制系统安全防护技术要求和测试评价方法》	送审稿
9	《信息安全技术 工业控制系统网络审计产品安全技术要求》GB/T 37941-2019	已发布
10	《信息安全技术 工业控制系统专用防火墙技术要求》GB/T 37933-2019	已发布
11	《信息安全技术 工业控制网络监测安全技术要求及测试评价方法》GB/T 37953-2019	已发布
12	《信息安全技术 工业控制系统漏洞检测产品技术要求及测试评价方法》GB/T 37954-2019	已发布
13	《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》GB/T 37934-2019	已发布
14	《信息安全技术 工业控制系统产品信息安全通用评估准则》GB/T 37962-2019	已发布
15	《信息安全技术 数控网络安全技术要求》GB/T 37955-2019	已发布
16	《信息安全技术 可编程逻辑控制器（PLC）安全技术要求和测试评价方法》	送审稿

主要任务：信息安全+功能安全+共性支撑

- **信息安全：工控安全防护系统**
  - 计算环境、通信网络、区域边界等
- **功能安全：高可信工业控制器**
  - DCS、PLC、SCADA、ECU等核心器件
- **共性支撑：行业共性基础设施**
  - 工具链、试验床、标准规范、知识库等

<table>
<tr><th colspan="6">③ 共性支撑</th></tr>
<tr><th colspan="2">安全工具链</th><th>行业试验床</th><th>标准规范</th><th colspan="2">工控知识库</th></tr>
<tr><td>需求分析工具</td><td>系统测试工具</td><td>车载ECU攻防演练试验床</td><td rowspan="2">面向行业的工控系统
功能安全和信息安全兼容性</td><td colspan="2">工控协议库</td></tr>
<tr><td>概要设计工具</td><td>集成测试工具</td><td>轨道交通列控系统试验床</td><td colspan="2">工控漏洞库</td></tr>
<tr><td>建模仿真工具</td><td>单元测试工具</td><td>电力安全攻防演练试验床</td><td rowspan="2">典型工控系统
安全技术要求和
测试评价方法</td><td colspan="2">设备指纹库</td></tr>
<tr><td colspan="2">代码生成工具</td><td>其他行业试验床</td><td colspan="2">IP信誉库</td></tr>
<tr><th colspan="3">① 功能安全</th><th colspan="3">② 信息安全</th></tr>
<tr><th>基础软硬件</th><th>通信设备</th><th>工控核心器件</th><th>计算环境安全</th><th>通信网络安全</th><th>区域边界安全</th></tr>
<tr><td rowspan="2">高实时
总线芯片</td><td rowspan="2">私有通信协议</td><td>SCADA</td><td>可信验证</td><td>加密通信</td><td rowspan="2">工业网闸</td></tr>
<tr><td>DCS</td><td>主机加固</td><td>安全网关</td></tr>
<tr><td rowspan="3">高实时
高安全
操作系统</td><td rowspan="3">边缘计算
安全网关</td><td>PLC</td><td>资产扫描</td><td>异常检测</td><td rowspan="3">工业
防火墙</td></tr>
<tr><td>安全仪表</td><td>代码审计</td><td>安全审计</td></tr>
<tr><td>行业专用器件</td><td>漏洞挖掘</td><td>态势感知</td></tr>
</table>

技术图谱：信息安全

■ 高安全工控防护系统：国产化自主可控架构，融合AI安全算法应用、国密算法

区域边界安全

工业网闸	■ 麒麟OS、鲲鹏、兆芯CPU等
工业防火墙	■ SCADA、DCS、PLC、RTU

通信网络安全

加密通信	**安全网关**	**态势感知**	
■ 支持国密SM1/2/4	■ 支持工业协议识别		■ 蜜罐诱捕 ■ AI攻击画像 ■ 指令识别 ■ 内容检测
异常检测	**安全审计**		
■ 未知攻击识别检测	■ AI安全行为基线		

计算环境安全

可信验证	■ 硬件安全可信信任根，国密算法	
主机加固	■ 操作系统加固+基于AI的白名单自学习	
资产扫描	**代码审计**	**漏洞挖掘**
■ 全网无损探测 ■ 网络拓扑测绘	■ 代码漏洞关联分析 ■ 恶意代码基因分析	■ 基于AI的未知漏洞模糊测试

威努特 WINICSSEC　6cloud 六方云

Venus　金电网安 GOLDEN SECURITY NET

三零卫士　观安

傲密信息 CHINASORT　云联接 CloudConnect

PENGYUE 上海鹏越惊虹

格尔软件 KOAL　TrustKernel 上海瓶钵信息科技有限公司

INGEEK 银基　SEARI 上电科

技术图谱：功能安全

■ 高可信功能安全的工控核心器件：融合功能安全通信协议、安全可信硬件模块

工控核心器件

数据采集与件事控制系统 SCADA	■ 支持异常故障报警和动态预警
分散型控制系统 DCS	■ 支持功能安全标准工控通信协议 ■ 软硬件设计考虑信息安全功能
可编程逻辑控制器 PLC	■ 支持安全可信处理芯片
安全仪表系统	■ 支持多重化冗余表决组件

工控通信协议

私有通信协议	■ IEC61508 SIL3级TCP/IP协议栈 ■ 支持国密、3DES开放网络加密 ■ 支持HDLC、TCP/UDP、CAN
边缘计算安全网关	

工控基础软硬件

高实时总线芯片	**高实时、高安全操作系统**
■ 基于高实时总线芯片的工控通信协议栈和总线通信板卡 ■ 支持自动检错和纠错 ■ 支持非对称加密	■ 工业高实时应用和非实时应用的工业级操作系统 ■ 支持X86、ARM、龙芯CPU架构 ■ 支持SIL3级TCP/IP协议栈组件

宝信软件 BAOSIGHT
HTE 海得控制
新华控制 XINHUA CONTROL
上海自动化仪表有限公司 SHANGHAI AUTOMATION INSTRUMENTATION CO., LTD.
SEARI 上电科 上海电器科学研究所(集团)有限公司 Shanghai Electrical Apparatus Research Institute (Group) Co., Ltd.
国核自仪系统工程有限公司 STATE NUCLEAR POWER AUTOMATION SYSTEM ENGINEERING COMPANY, LTD.
INESA INSTRUMENT 仪电科学仪器
威尔泰 WELL TECH

CETC 中国电子科技集团公司第三十二研究所
S²C 中标软件 STANDARD SOFTWARE
CETC 普华基础软件股份有限公司

NXP 恩智浦半导体
KYLAND
SiboTech®
雷卯电子
上海贝岭
上海复旦微电子 FM
AisinoChip

技术图谱：共性支撑

■ 行业共性基础设施：自主可控安全工具链，面向行业的精细化、兼容性测评

安全工具链

需求分析工具	系统测试工具
■ Doors ■ Stimulus	■ Tessy/Testbed ■ Vector/ETAS ■ Cybellum
概要设计工具	**集成测试工具**
■ Rhapsody ■ Symatvison	■ Testbase ■ Hinates
建模仿真工具	**单元测试工具**
■ Simulink	■ Tessy/Testbed ■ QAC
代码生成工具	
■ Simulink Coder/Targetlink	

行业试验床

车载ECU攻防演练试验床
■ VCU、BMS、T-box、IVI ■ CAN/CANFD/以太网
轨道交通列控系统试验床
■ 自动无人驾驶CBTC系统 ■ 自动列车监控ATS系统
电力安全攻防演练试验床
■ 核电蜜罐攻击诱捕系统
其他行业试验床
■ 数字孪生+控制系统靶场

标准规范

面向行业的工控系统 功能安全和信息安全兼容性
■ 轨交列控系统 ■ 核电DCS系统
典型工控系统安全技术要求和测试评价方法
■ PLC、DCS（已立项） ■ 行业专用控制系统

工控知识库

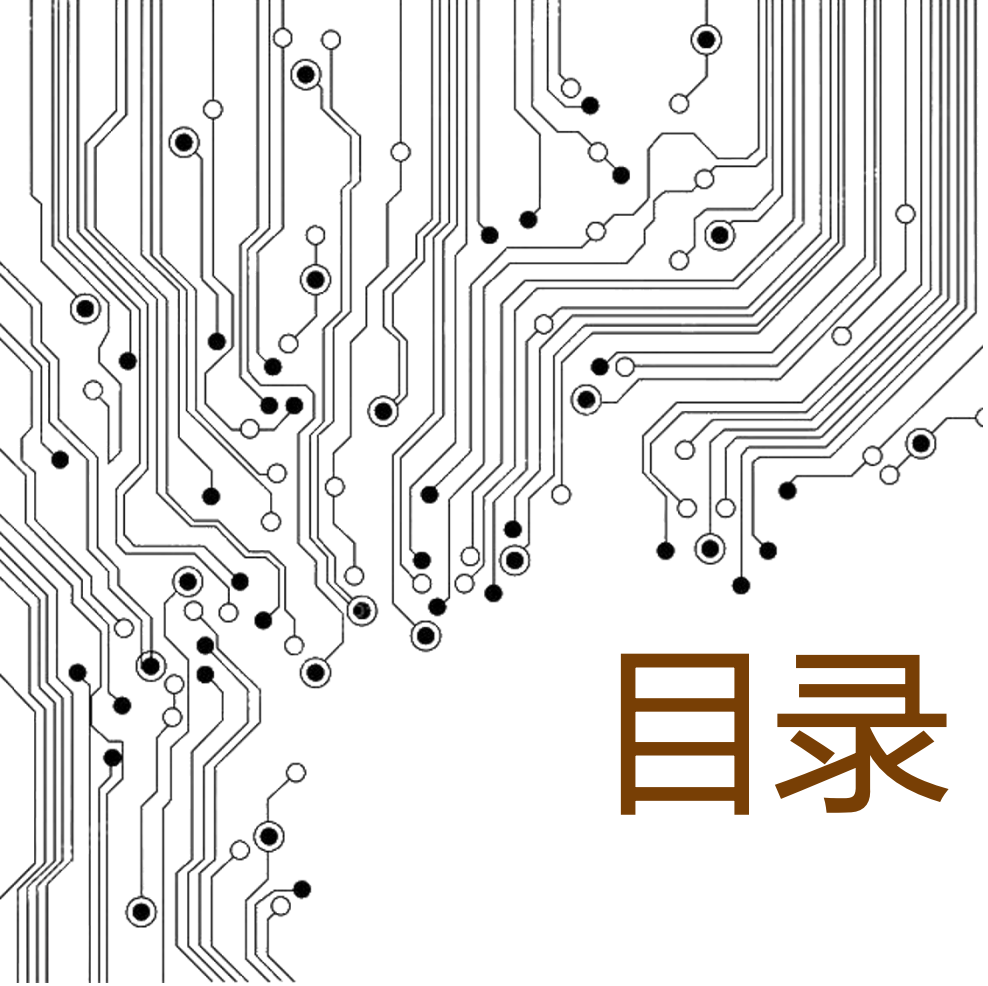
工控协议库
Modbus、IEC104、IEC61850、DNP3、BACnet、Profinet、S7，Crimson V3、FINS、PCWorx、ProConOS等
工控漏洞库
CVE+CNVD
设备指纹库
西门子、施耐德、罗克韦尔、三菱、南瑞、四方、ABB、研华、中控、和利时等
IP信誉库
态势感知+蜜罐+威胁情报

国家政策对产业的影响：工业互联网、自主可控、国密算法

政策	产业现状	安全需求
《中华人民共和国网络安全法》 《网络安全等级保护基本要求》（等保2.0） 《中华人民共和国密码法》	■工控设备缺乏信息安全设计，存在大量安全漏洞，高中危产比超过90%； ■电力行业信息安全先行：“**安全分区、网络专用、横向隔离、纵向认证**”。	■工控系统在**设计、研发和集成阶段**考虑功能安全和信息安全及其融合问题 ■**国密算法**全面支撑工控信息安全产品及应用。
《工业控制系统信息安全防护指南》 《工业控制系统信息安全事件应急管理工作指南》 《工业控制系统信息安全防护能力评估工作管理办法》 《工业控制系统信息安全行动计划（2018-2020年）》	■工控系统行业差异性显著，需求复杂多样； ■**态势感知、安全防护、应急处置**信息安全能力不足。	■在线监测网络，应急资源库，仿真测试、信息共享、信息通报平台（**一网一库三平台**）。
《工业互联网发展行动计划（2018-2020年）》 《加强工业互联网安全工作的指导意见》	■“工控系统安全”升级为“**工业互联网安全**”战略。	■**设备、控制、网络、应用、数据**等五个安全维度。
信息技术应用创新工作委员会	■超过85%存量国外垄断“**设备不能碰、配置不能改、账户不能管**”，自主可控国产化需求。	■**自主可控**：高可信工控系统、基于国产CPU和OS的高安全工控防护系统。

行业政策对产业的影响：功能安全和信息安全融合

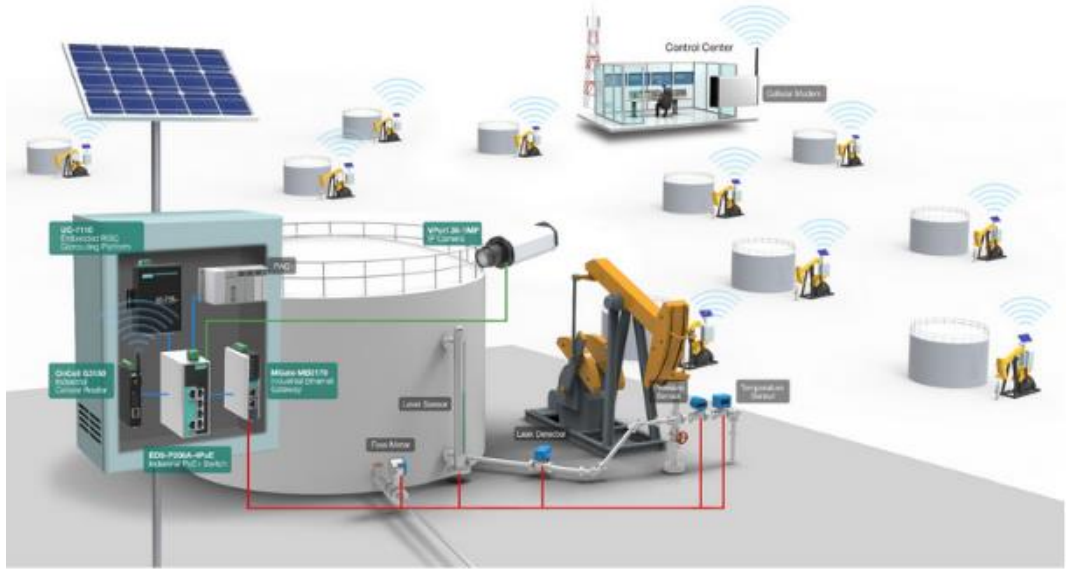
政策	产业现状	安全需求
国家第六阶段机动车污染物排放标准（国6） 《车联网（智能网联汽车）产业发展行动计划》	■需要构建自动驾驶L3及以上**安全可信的软硬件**集成与应用能力； ■重型车远程排放监管系统，提出**车载终端安全**技术强制要求。	■基于AutoSar和ISO26262整车控制器**功能安全**设计； ■汽车电子控制器、CAN/车载以太网安全**渗透测试**； ■结合**国密算法和安全加固**，开展车联网及车载ECU通信安全、车机应用安全、数据安全和用户隐私保护。
《智慧城市轨道交通信息技术架构及网络安全规范》 《轨道交通CBTC信号系统互联互通建设指导》 《城市轨道交通云平台网络拓扑架构技术规范》 《城市轨道交通信息化设计规范》	■等保2.0驱动的列车自动控制系统等保三级要求； ■生产网和管理网**单向隔离**；功能和信息安全**相对割裂**。	■轨交云平台信息安全防护； ■**国密算法**及国产化需求； ■高安全等级SIL4级以上信号系统的功能安全和信息安全**兼容性测试**。
《泛在电力物联网白皮书2019》 国家能源局关于加强电力行业网络安全工作的指导意见	■99%工控安全采用硬件隔离设备；尚未解决电力资产运行中的安全监测、智能感知、主动防御能力。	■工控系统**内生安全**设计； ■功能安全监测评估、信息安全主动防御； ■功能安全和信息安全兼容性，信息安全产品对工控系统可靠性的影响。



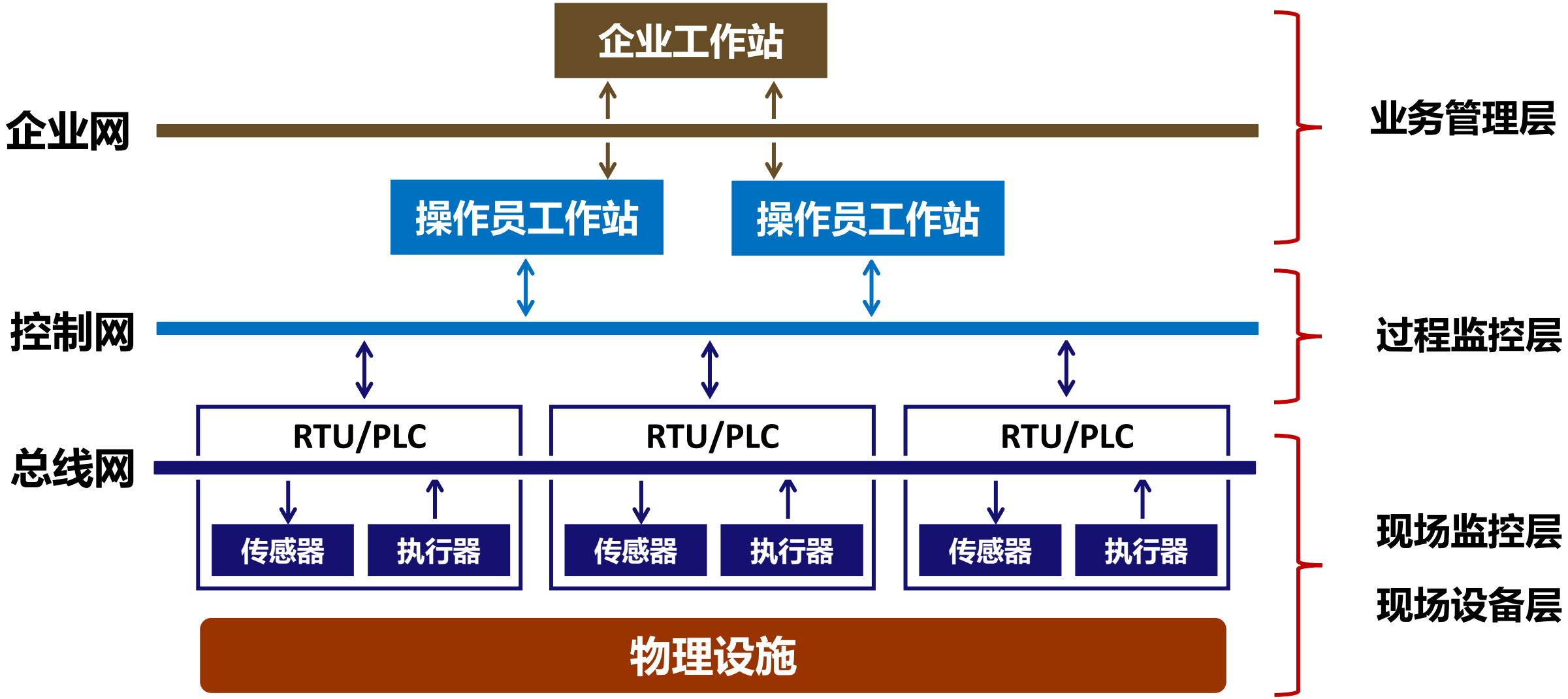
目录

工控系统的主要组件

- 工控系统由一系列自动化控制组件以及对实时数据采集监测的过程控制组件构成，从封闭隔离系统，演进为开放交互系统。
  - 监控和数据采集系统（SCADA）
  - 过程控制系统（PCS）
  - 分布式控制系统（DCS）
  - 可编程逻辑控制器（PLC）
  - 远程终端（RTU）

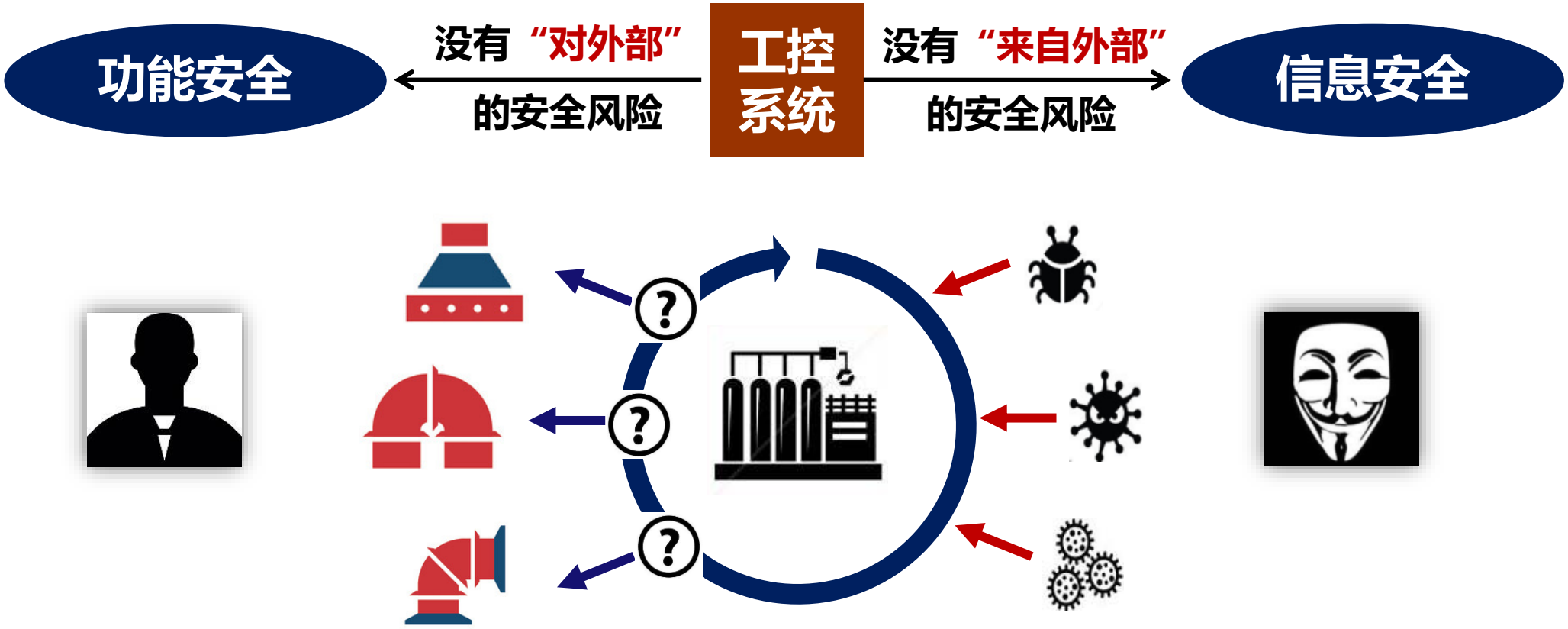


工控系统的典型网络


企业工作站
企业网
操作员工作站
操作员工作站
控制网
RTU/PLC
RTU/PLC
RTU/PLC
总线网
传感器
执行器
传感器
执行器
传感器
执行器
物理设施
业务管理层
过程监控层
现场监控层
现场设备层

工控系统的安全范畴

- 工控系统是功能安全Safety和信息安全Security的融合体



工控安全的总体框架

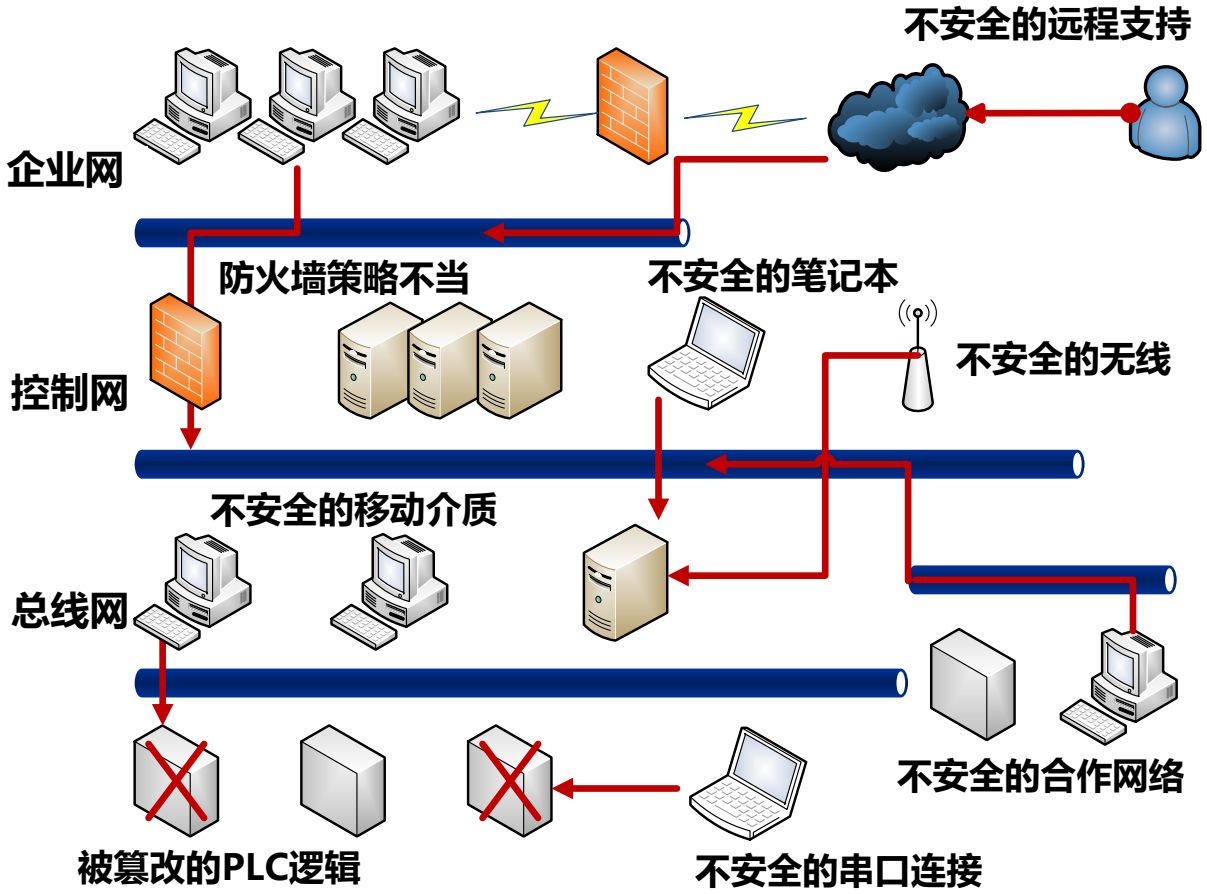
- 工控系统安全技术体系

设计	工控系统功能安全设计
使用	工控系统功能安全防护
认证	工控系统功能安全标准认证

攻击前	工控安全威胁态势感知
攻击中	工控系统信息安全防护
攻击后	工控系统应急处置

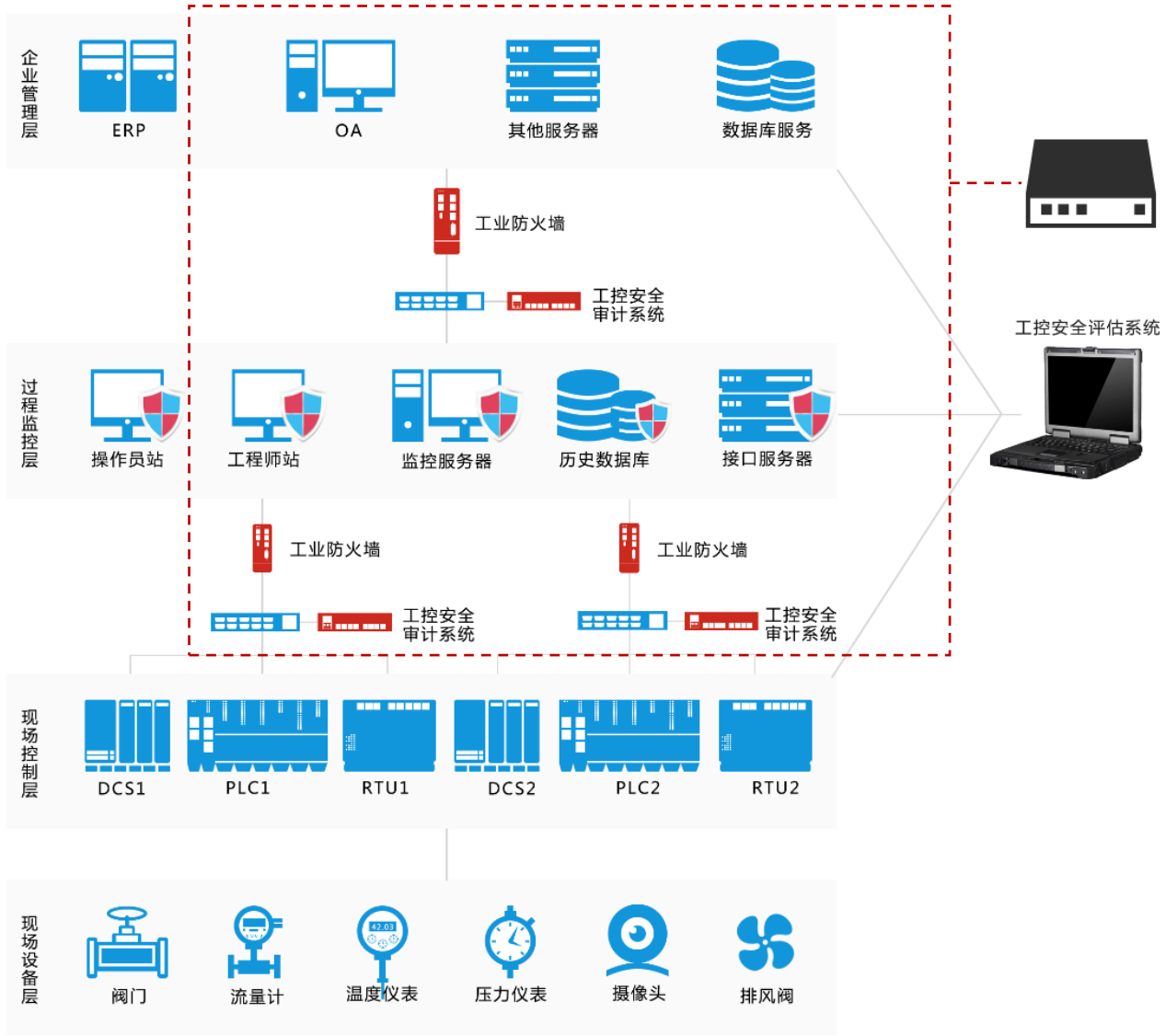
工控信息安全隐患

- 操作系统漏洞和杀毒软件升级
  - 工控系统通常不对操作系统打补丁，不安装或不升级杀毒软件。
- 远程接入支持
  - 对远端工控设备进行检测或升级过程。
- 防火墙策略
  - 不符合安全策略的非法数据流通过防火墙。
- U盘摆渡、笔记本和串口
  - 设备维修时笔记本电脑的随便接入。
- 无线网络和合作网络
  - 无线通信链路的开放性以及合作网络的不确定性。



工控信息安全防护

- 典型工控信息安全产品
  - 终端安全卫士
  - 工业防火墙
  - 工控安全审计系统
  - 工控安全评估系统
  - 工控安全管理平台



工控信息安全防护思路

攻击方式	单一方式、无延续性的直接性破坏式攻击	简单→复杂	多方式、持续性的深层次隐蔽性攻击
安全隐患	主要采用专用的硬件、软件和通信协议	专用→通用	逐渐采用通用的硬件、软件和通信协议
安全机制	工业防火墙、网关等逻辑隔离 资源受限设备的固定式安全加固	逻辑→物理	工控防火墙、网闸等物理隔离 内核和外围的弹性式安全加固
	已知恶意代码查杀、已知威胁入侵检测 已知漏洞扫描、已知异常流量监测	已知→未知	未知恶意代码查杀、未知威胁入侵检测 未知漏洞挖掘、未知攻击行为检测
	工控安全定性风险评估	定性→定量	工控安全定量风险评估
攻击应对	攻击事件的“事中审计、事后溯源”	防御→防疫	攻击事件的“事前态势感知、动态预测”

工控信息安全防护思路

■ 呈现功能和信息融合化、纵深防御主动化、威胁数据共享化等趋势

单一方式、无延续性的直接性破坏式攻击	简单→复杂	多方式、持续性的深层次隐蔽性攻击
主要采用专用的硬件、软件和通信协议	专用→通用	逐渐采用通用的硬件、软件和通信协议
面向已知恶意代码、威胁、漏洞	已知→未知	面向未知恶意代码、威胁、漏洞
工控安全事件“事中审计、事后溯源”	事中、事后→事前	工控安全事件的“事前态势感知”

■ 功能和信息安全融合 **硬件+软件+安全**

将信息安全融入到产品功能安全设计、研发、制造、应用全生命周期

■ 纵深安全防御主动化 **边界隔离→多重关卡→主动防御→以攻为守**

以美国火眼公司为代表的APT攻击主动防御，面向未知漏洞、木马、后门的监测预警

■ 威胁情报数据共享化 **信息孤岛→数据共享**

美国率先发布CybOX、STIX、TAXII等威胁情报感知共享规范。

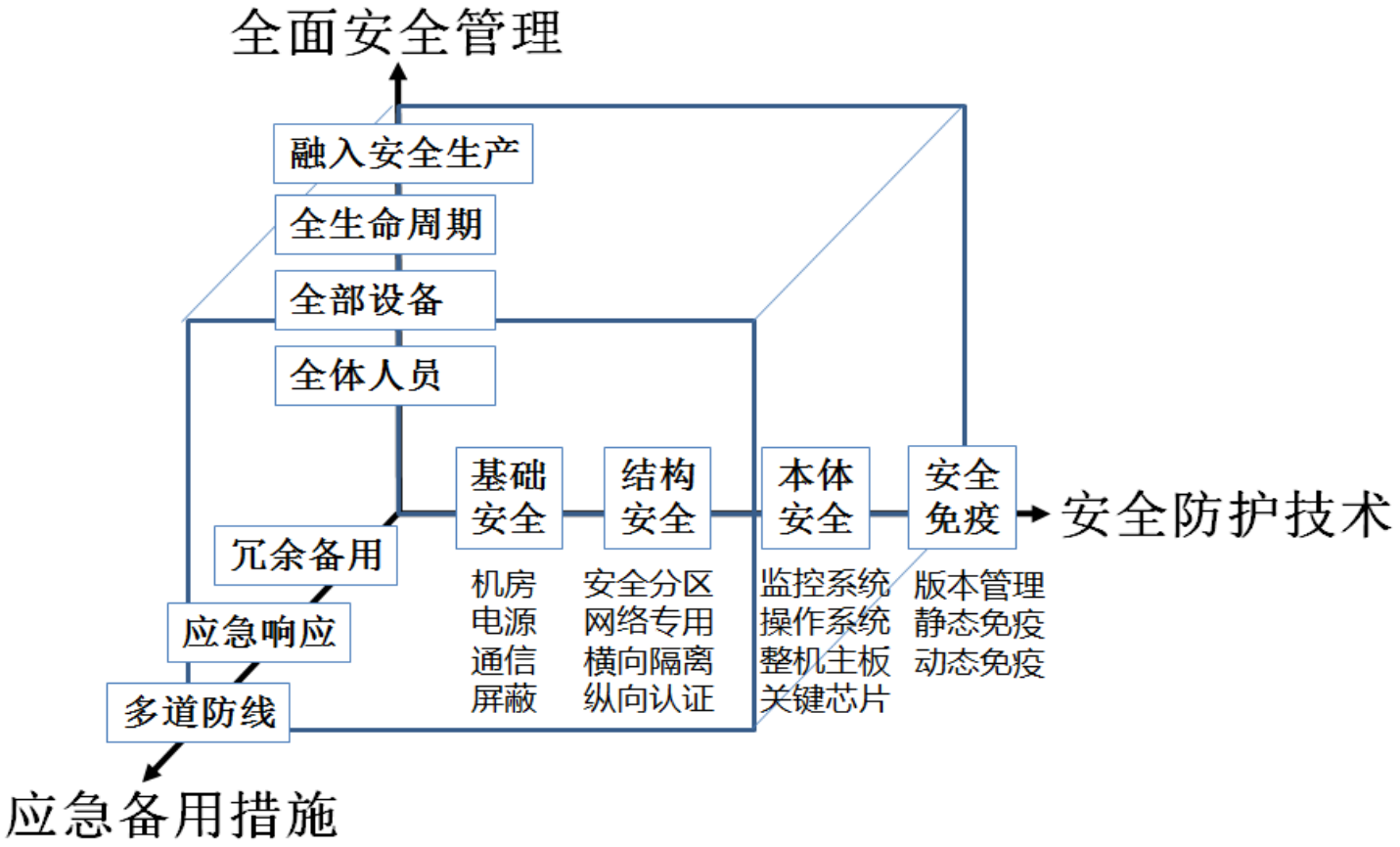
目录

电力系统安全统防护体系

■ 安全防护体系维度叠加补强——**硬件面向集群、软件面向服务**

安全防护技术

基础安全	■ 机房、电源、通信 ■ 屏蔽、密码、认证
结构安全	■ 业务系统应分区分级 ■ 关键业务应网络专用 ■ 横向边界应单向隔离 ■ 纵向边界应加密认证
本体安全	■ 监控系统无恶意软件 ■ 操作系统无恶意后门 ■ 整机主板无恶意芯片 ■ 主要芯片无恶意指令
安全免疫	■ 可信计算安全免疫



现有物联网防护方案

- 面向“云-管-端”的纵深安全防护体系
  - 终端防御
    - **弱终端**：数据传输层加密，安全启动、安全FOTA升级、设备标识组合引擎DICE
    - **强终端**：安全证书、入侵检测、加密认证、可信计算平台模块TPM/可信平台控制模块TPCM
  - 管道保障
    - 恶意行为检测与隔离
  - 云端保护
    - 态势感知、数据安全和隐私保护

面向技术、运维、管理
侧重网络流量异常分析

T：安全技术族，M：安全运维与管理

现有物联网防护方案

- 面向平台和服务的安全防护体系
  - 物联网嵌入式操作系统
  - 物联网开发平台
  - 物联网安全服务

侧重密码算法实现安全防护

- 多安全等级
- 跨平台支持
- 一机/次一密
- 离线认证
- 国密算法

设备认证	数据保护	安全监控与态势感知
一机一密	数据加密	
一次一密	数据防篡改	
动态密钥更新	数据完整性校验	
数字签名：防止身份伪装	敏感数据防提取	
动态认证：防止重复攻击	安全固件升级	
双向认证：防止会话劫持	程序可信启动	
可信信任根（SE、TEE、软加固）		

现有物联网防护方案

- 面向平台和服务的安全防护体系

云

物理环境安全	主机安全
数据安全	应用安全

云端安全

机房安全	账号管理	WAF
网络隔离	反DDoS	入侵检测
访问控制	漏洞扫描	数据加密
身份认证	日志监控	数据脱敏

管

应用协议安全
设备接入与认证安全
应用层协议安全

通信安全

WiFi安全	移动通信安全	HTTPS安全
BLE安全	设备ID	MQTT安全
ZigBee安全	双向认证	COAP安全
LoRaWAN安全	通信加密	

边/端

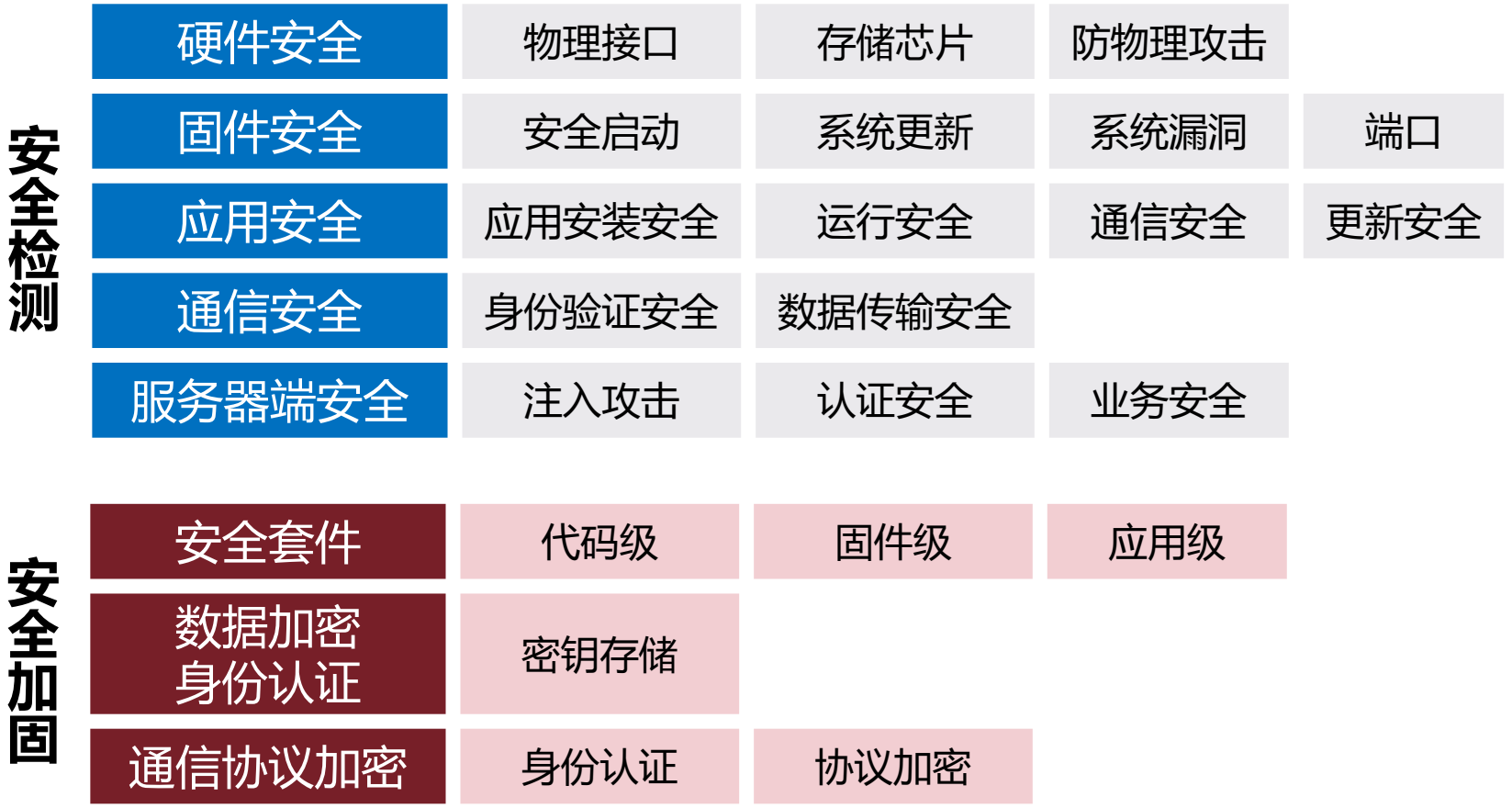
硬件安全		软件安全
物理安全	PCB安全	系统安全
传感器安全	芯片安全	应用安全

边缘/终端安全

物理防护	SE和TEE	代码安全
PCB安全	可信启动	安全SDK
传感器安全	系统加固	日志安全
芯片安全	安全OTA	

现有物联网防护方案

- 面向物联网全系统、全生命周期的安全防护方案
  - 安全检测
  - 安全加固
  - 态势感知
    - 终端运行状态监控
    - 终端漏洞和封校感知
    - 终端异常和威胁发现
    - 终端更新修复



现有物联网防护方案

- 面向物联网全系统、全生命周期的安全防护方案
  - 云平台安全
  - 传输安全
  - APP安全
  - IoT设备安全

- **侧重安全检测服务**
- **侧重安全加固服务**
- **侧重系统安全漏洞**

云平台安全
身份鉴别漏洞、访问控制漏洞、SQL注入漏洞、入侵管理后台

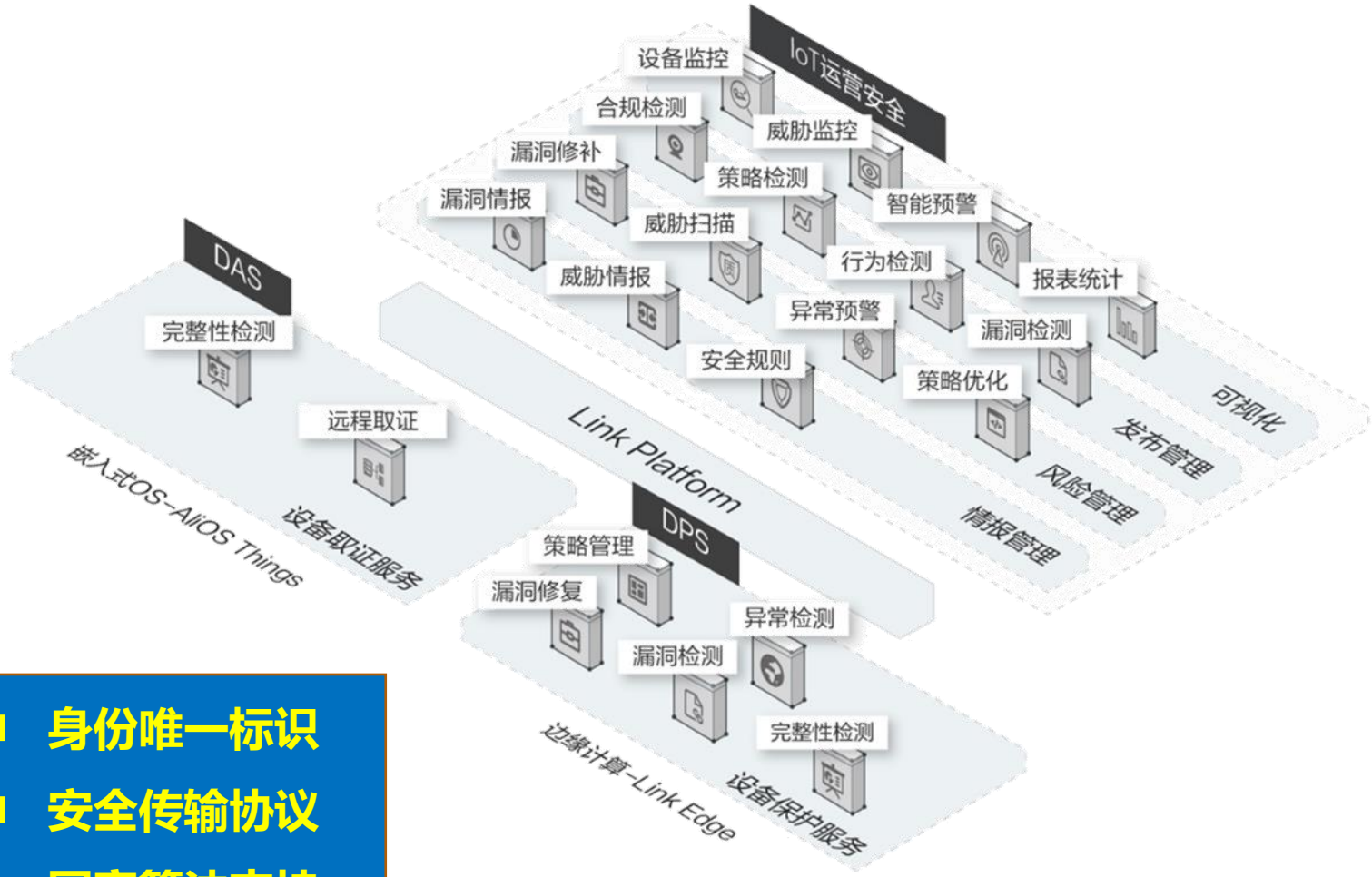
网络传输安全
明文传输密码、设备信号重放、无线信号拦截、OTA固件更新拦截

APP安全
获取加密密钥、伪造控制指令、逆向分析

IoT设备风险
硬件提权、逆向固件、密钥窃取、漏洞利用

现有物联网防护方案

- 安全运营中心
  - 安全检测与评估
  - 漏洞扫描和修复
  - 威胁感知和阻断
  - 安全运营托管
- IoT设备身份认证
- IoT固件安全检测



- **身份唯一标识**
- **安全传输协议**
- **国密算法支持**

现有物联网防护方案

■ 现有物联网安全防护思路

面向云	态势感知，威胁情报，监测预警 安全审计，流量分析，恶意代码检测 身份认证，访问控制
面向管	安全边缘计算网关 基于密码算法的加密传输协议TLS
面向端	固件漏洞挖掘，固件安全检测 固件安全加固，安全加密芯片

现有物联网防护方案

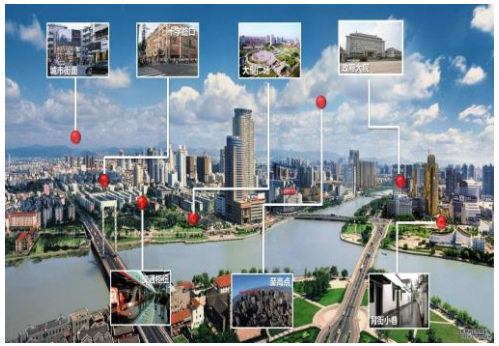
■ 现有方案的不足之处：

- 侧重**软件完成开发后**的测试和加固，忽略**软件开发过程中**的功能安全和信息安全
- 侧重**基于网络流量分析**的监测预警，忽略**基于人员行为和业务逻辑**的安全可信基线
- 侧重**基于IP黑白名单**的安全策略配置，忽略**基于应用白名单**的未知恶意进程拦截

面向软件测试和加固	■发现问题难以有效整改 ■软件缺陷导致安全危害 ■软件漏洞导致安全风险
基于网络流量分析	■难以识别合法用户违规操作 ■难以识别业务逻辑错误 ■难以实现实时性阻断
基于IP黑白名单	■仅依赖IP五元组识别异常流量 ■仅依赖应用协议解析识别异常应用

面向软件全生命周期 (需求→研发→测试→响应)	■构建安全开发环境 ■建议安全编码规范 ■建立威胁建模和风险评估 ■支持软件开源漏洞持续分析
基于人员行为 基于业务逻辑	■基于用户行为画像 ■基于设备行为画像 ■基于特定攻击场景
基于应用白名单	■仅可信主体（合法用户、合法设备）允许访问特定资源（包括应用程序、文件系统、API接口、外设等）

工业互联网面临的挑战



海量异构物联感知终端

安全服务能力不足

物联网安全隐患突出

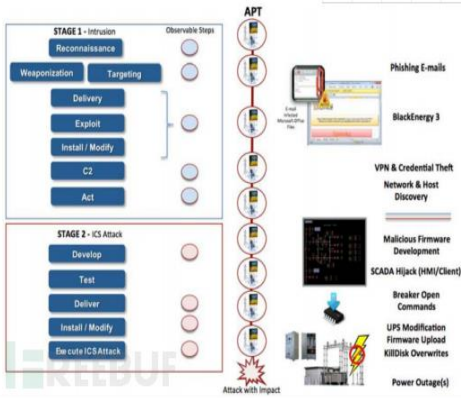
资源整合利用程度不够

物联网运营有待加强

- **边界模糊，防护失效**。随着泛在物联、云大物移智的发展，传统边界模糊不清，数据沉淀边缘；
- **品牌众多，安全薄弱**。物联终端品牌类型多，安全薄弱，通信协议碎片化，安全防护困难重重；
- **户外暴露，监控困难**。户外部署，物理安全难保证，准入控制手段缺乏，边缘侧安全问题严峻；
- **传统技术，难以落地**。传统网络访问控制方法粒度过粗，策略不够灵活，难以适应物联网环境；
- **点多面广，管理困难**。物联终端广泛分布在路边、楼宇、车站等场所，难以进行统一集中管理。

工业互联网典型安全事件

近年来，包括工业互联网在内的关键基础设施已经成为全球网络攻击的重点目标，面临的安全形势日趋严峻。随着电力系统逐渐由封闭走向开放、共享，呈现出网络结构复杂化、边界模糊化和威胁形态多样化的特点，随之带来了更多的网络安全问题，给整体的网络安全防护带来了严峻挑战。



2015年12月，乌克兰国家电力部门遭受恶意代码攻击导致断电

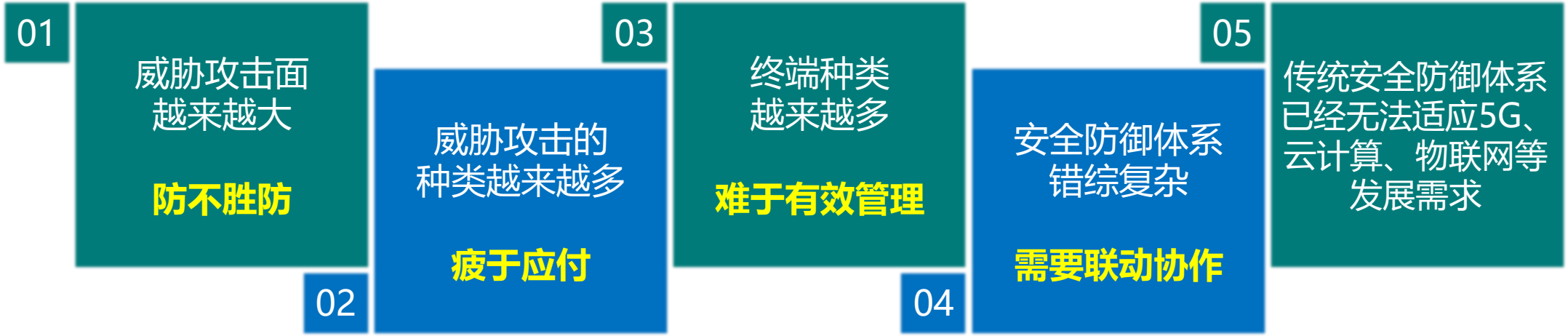
2019年3月，委内瑞拉电力系统遭受网络攻击导致大面积停电

2021年5月9日，美国最大燃油管道遭网络攻击 多州进入紧急状态

能源基础设施网络攻击事件逐年上升，不逐一列举

安全现状

- 数字化转型发展推动网络安全问题加剧，攻击的数量、多样性以及损害的程度大幅提升。
- 新兴技术如云计算和物联网等推动保护对象进一步拓展。
- 政策的发展与逐步完善对企业提出更高要求

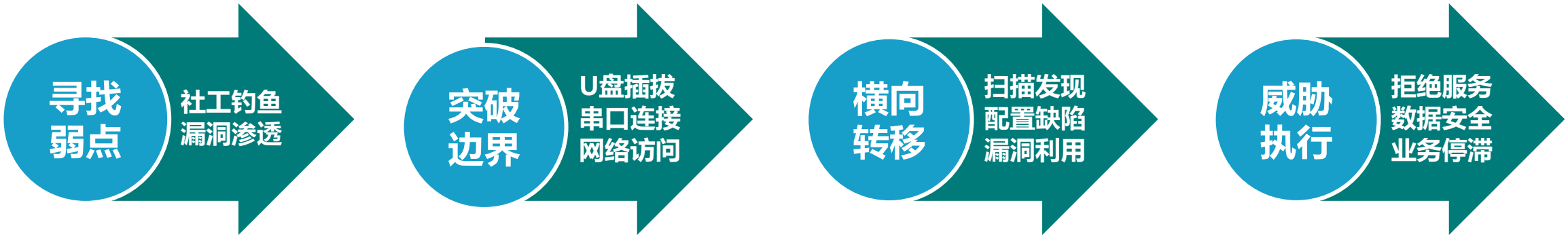


工业互联网面临的挑战

■ 分散的边缘运维难以集中防护

- 变电站、配电房等边缘侧环境中，安全防护主要依赖物理隔离和边界防护。一障。
- 配电柜、户外台区本质上没有物理安全。
- 二次设备1多为专用系统，关注功能较多，安全测试不充分，设备自身可能存在
- 运维/检修人员分布广，电脑数量大，且安全管理难。

- CNVD-2018-12361： 四方某型号（用于110kv及以上变电站）测量控制装置IP协议分片存在拒绝服务漏洞。攻击者通过发送非法的IP分片报文，可导致设备的网络功能进入不稳定状态，进而导致设备异常并进入间歇性网络服务中断状态。
- CNCERT：《2019年上半年我国互联网网络安全态势》表明，在某次安全测试中，在涉及28个厂商、70余个型号的六大类产品（测控装置、保护装置、智能远动机、站控软件、PMU、网络安全态势感知采集装置，）中均发现了中、高危漏洞，可能产生的风险包括拒绝服务攻击、远程命令执行、信息泄露等。
- 2015/2016年，俄罗斯黑客先利用社工攻陷乌克兰电网运维人员PC，再横向移动，利用IEC 60870-5-101，IEC 60870-5-104、EC 61850等协议，试图攻击继保设备和SCADA系统。

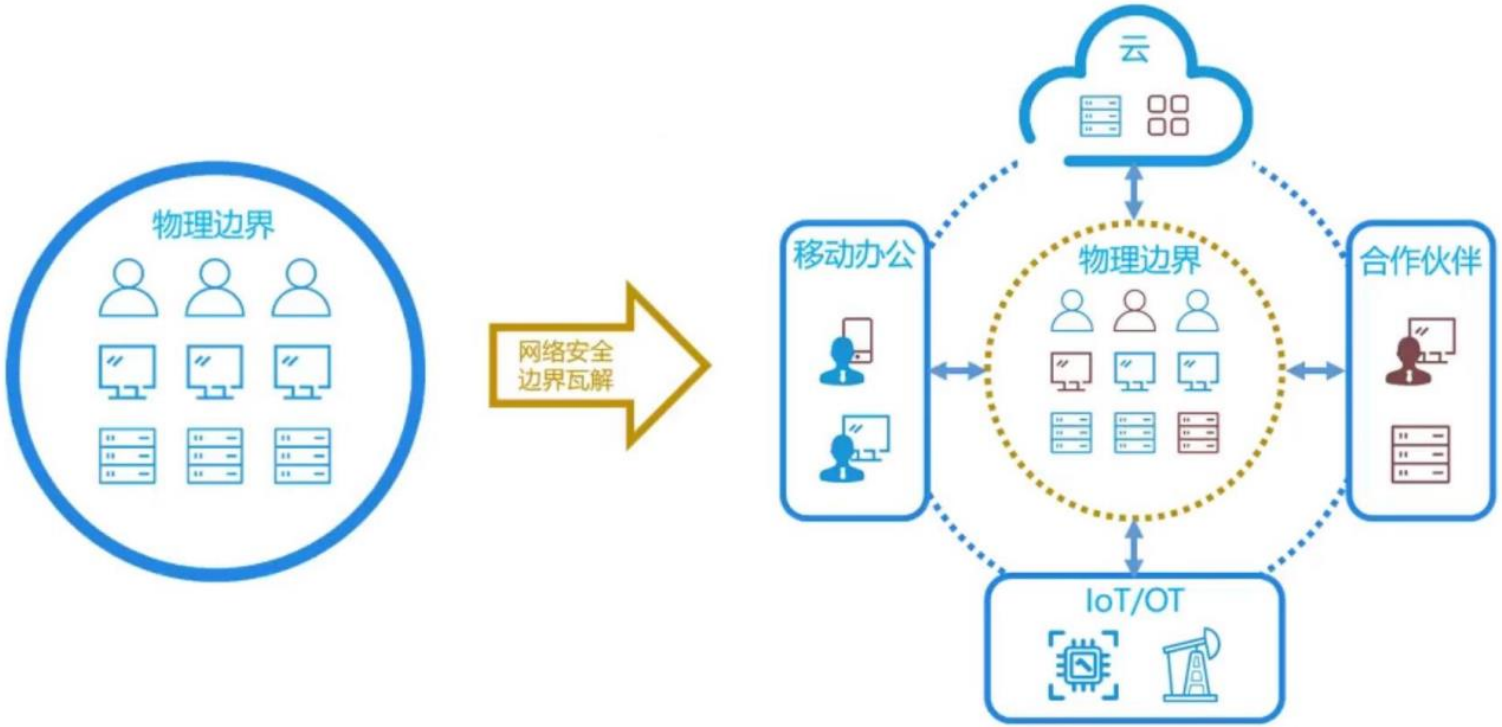


传统的安全防御体系局限性

- 传统的安全防御体系已经无法适应5G、云计算、物联网等发展需求
  - 传统的安全架构以”纵深防御+边界防御“为主。
  - 企业在成长过程中，安全边界逐步被打破、并彻底走向模糊化，基于边界的安全防护体系逐渐失效，已经难以适应企业的快速成长，难以应对业务的变化。

网络边界的变化，
万物互联时代网络边界已经模糊

传统以网络边界为核心，
现代安全要求以身份为核心



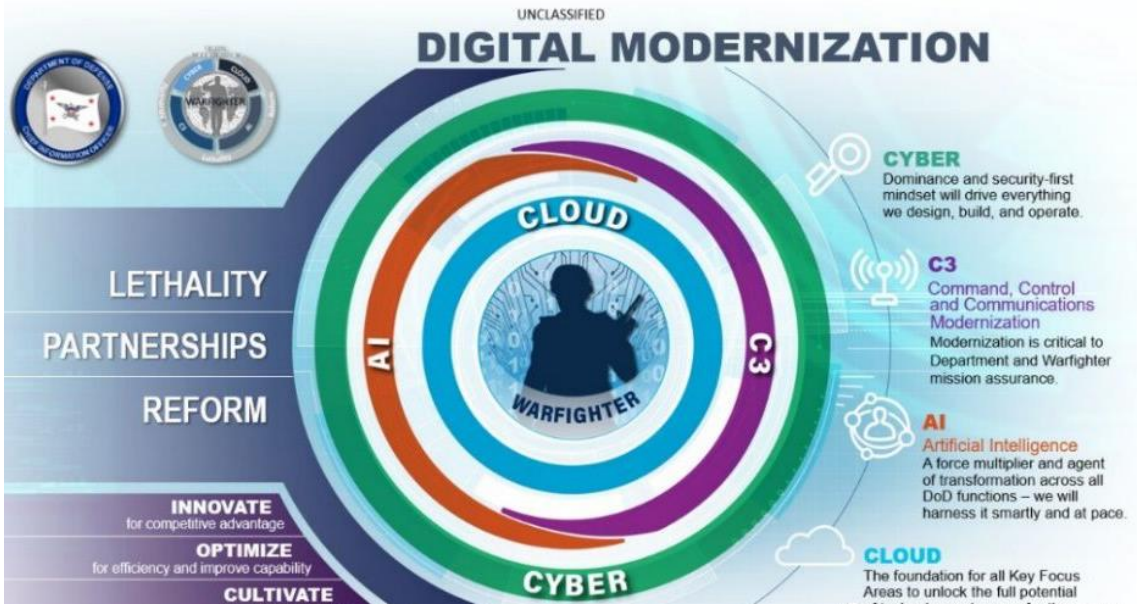
工业互联网安全要求

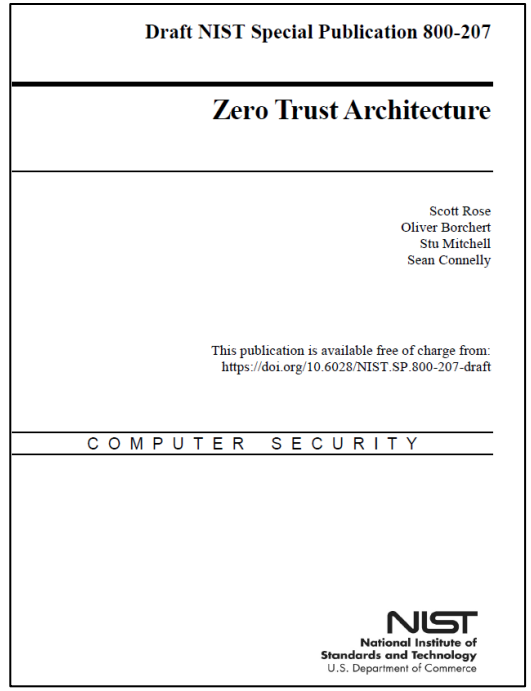
- 实现对海量终端的安全防护，杜绝僵尸网络等攻击事件发生，实现“工业互联网终端不发生大面积被控”，确保不对外系统造成影响。
- 实现对全域物联网大平台的安全保障红线，实现“单点入侵不影响物联网大平台安全”。
- 实现对涉及电网安全稳定运行的关键业务系统的底线保护，实现“工业互联网采集监测不影响大电网运行安全”，确保万无一失。

零信任安全技术成为美国国家级网络安全战略

2019.7，美国《国防部数字现代化战略：国防部信息资源管理战略规划（2019财年-2023财年）》，**零信任安全列为优先发展技术 。**

2020.8，美国国家标准技术院NIST发布**《零信任架构》安全标准**正式版。




Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

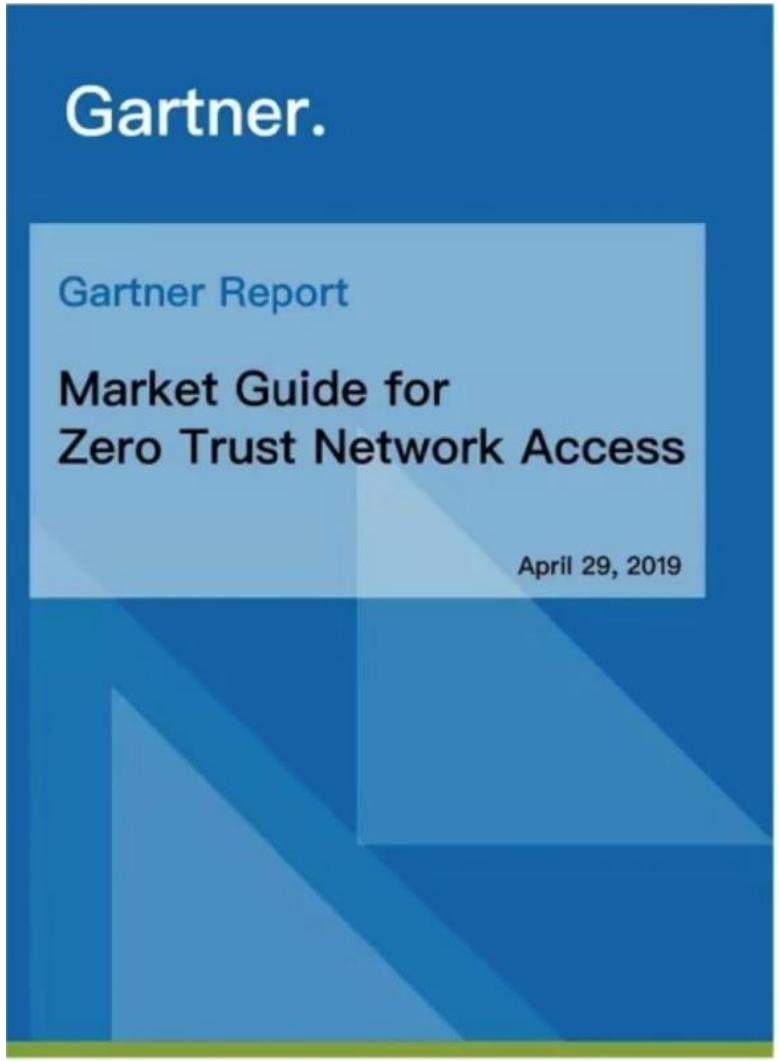
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

2021.5，美国总统拜登签发了行政命令（EO），**强制推行零信任架构。**

Gartner零信任行业报告



- Gartner 最新行业报告《Market Guide for Zero Trust Network Access》
- 《零信任网络访问ZTNA市场指南》 2019-04-29
  - 2020年，面向生态系统台作伙伴开放的80%的新数字业务应用程序将通过零倍任网络访问（ZTNA）进行访问。
  - 2023年，**60%的企业将淘汰大部分远程访问虚拟专用网络（VPN）转而使用ZTNA**。40%的企业将采用零信任网络访问用于报告中描述的其他使用场景。

零信任技术的国家政策

2019.9 工信部《关于促进网络安全产业发展的指导意见》：

2025年网络安全规模超过2000亿，"零信任安全"为"网络安全关键技术"。

邮箱登录 | 移动版网站 | 工信微报

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

看新闻 找文件 查办事 提意见 查数

工业和信息化部 新闻动态 信息公开 政务服务 公众参与 工信数据 专题专栏

首页 > 工业和信息化部 > 机关司局 > 网络安全管理局 > 工作动态 > 正文

公开征求对《关于促进网络安全产业发展的指导意见（征求意见稿）》的意见

发布时间：2019-09-27 来源：

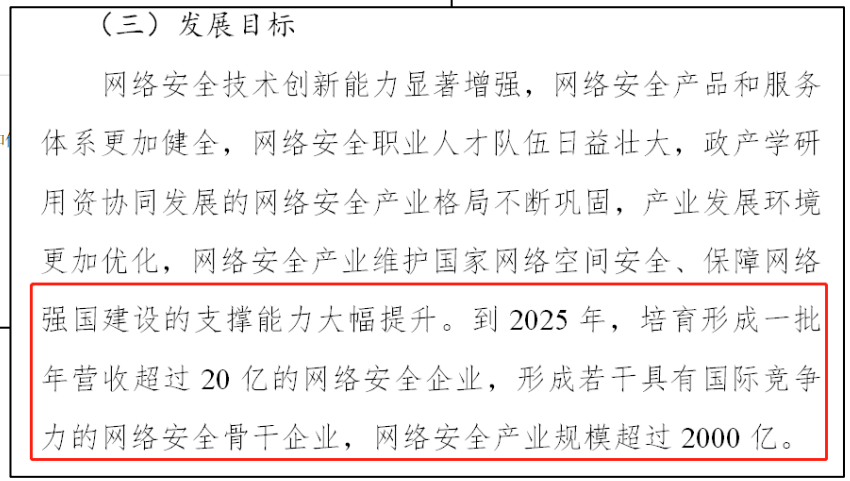
为贯彻落实《中华人民共和国网络安全法》，积极发展网络安全产业，工业和
导意见（征求意见稿）》（见附件），现面向社会公开征求意见。如有意见或建议，

联系电话：010-66022774

传　　真：010-66022774

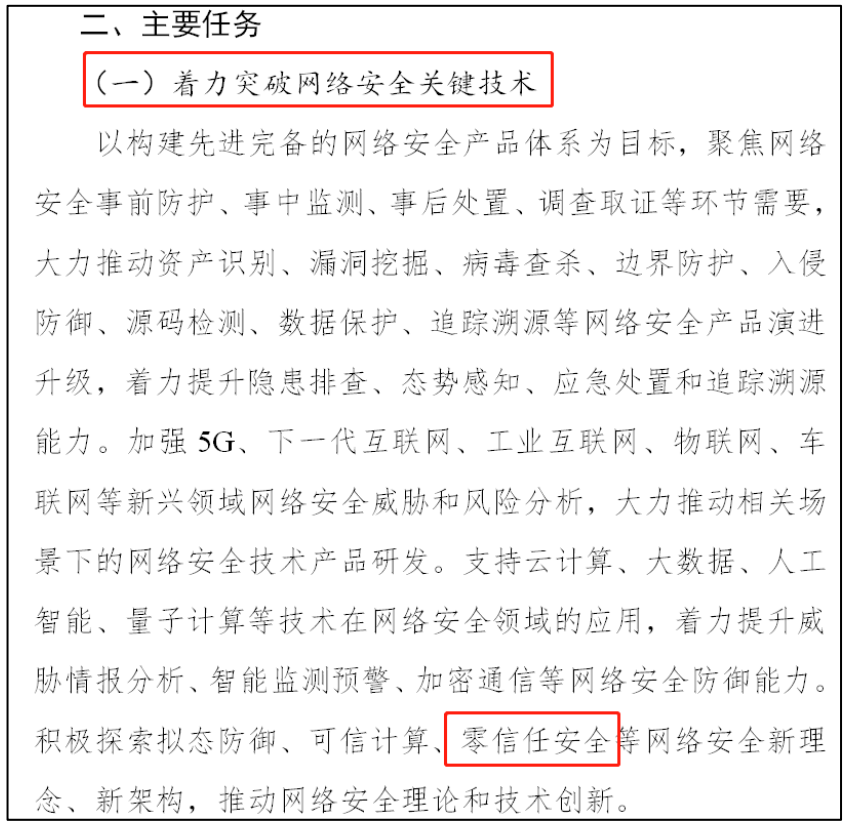
邮　　箱：wangmeifang@miit.gov.cn

附件：关于促进网络安全产业发展的指导意见（征求意见稿）



（三）发展目标

网络安全技术创新能力显著增强，网络安全产品和服务体系更加健全，网络安全职业人才队伍日益壮大，政产学研用资协同发展的网络安全产业格局不断巩固，产业发展环境更加优化，网络安全产业维护国家网络空间安全、保障网络强国建设的支撑能力大幅提升。到 2025 年，培育形成一批年营收超过 20 亿的网络安全企业，形成若干具有国际竞争力的网络安全骨干企业，网络安全产业规模超过 2000 亿。



二、主要任务

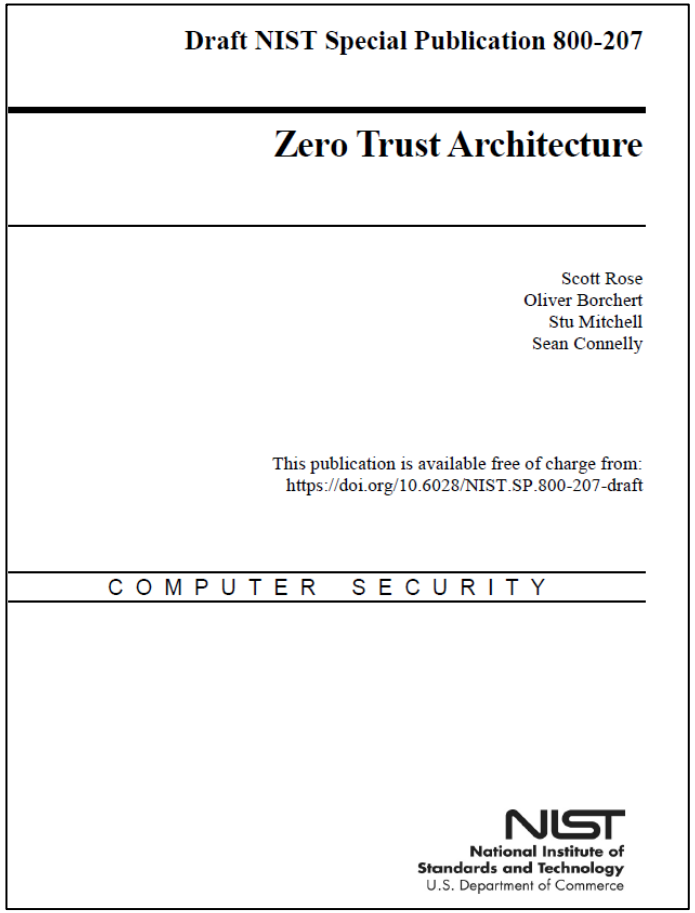
（一）着力突破网络安全关键技术

以构建先进完备的网络安全产品体系为目标，聚焦网络安全事前防护、事中监测、事后处置、调查取证等环节需要，大力推动资产识别、漏洞挖掘、病毒查杀、边界防护、入侵防御、源码检测、数据保护、追踪溯源等网络安全产品演进升级，着力提升隐患排查、态势感知、应急处置和追踪溯源能力。加强 5G、下一代互联网、工业互联网、物联网、车联网等新兴领域网络安全威胁和风险分析，大力推动相关场景下的网络安全技术产品研发。支持云计算、大数据、人工智能、量子计算等技术在网络安全领域的应用，着力提升威胁情报分析、智能监测预警、加密通信等网络安全防御能力。积极探索拟态防御、可信计算、零信任安全等网络安全新理念、新架构，推动网络安全理论和技术创新。

NIST SP800-207白皮书的定义

- 零信任(Zero Trust, ZT)
  - 一系列概念和观念，被设计用于降低执行中的不确定性
  - 信息系统和服务所在的网络被视为已沦陷
  - 精确的访问决策，且对每个请求都单独进行
- 零信任架构(Zero Trust Architecture, ZTA)
  - 企业的网络安全计划
  - 利用零信任概念，包括组件关系、工作流规划和访问策略

零信任企业是指企业部署的网络基础设施
和运行策略基于零信任架构设计


Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

安全设计要求

以**安全资源管理**为依托，**安全服务**为目标，**安全运营**为核心，实现海量异构终端设备安全**可视可管可控**的目标。推动构建“状态风险监测、环境风险分析、安全风险管控”一体化的物联网**零信任安全防护**生态体系，提升工业互联网安全的**可预测性、可验证性、可解释性。**

□ 全面检测预警实现终端安全感知

监测终端安全态势，获取物联终端行为信息，充分利用大数据深度挖掘技术，实现安全态势感知。

□ 保护边缘物联设备的本体安全

在TEE基础上构建安全的、适配物联网嵌入式环境的本体安全防护，实现新型工业互联网的全链条安全可信。

□ 边缘设施安全可信接入促进云端安全

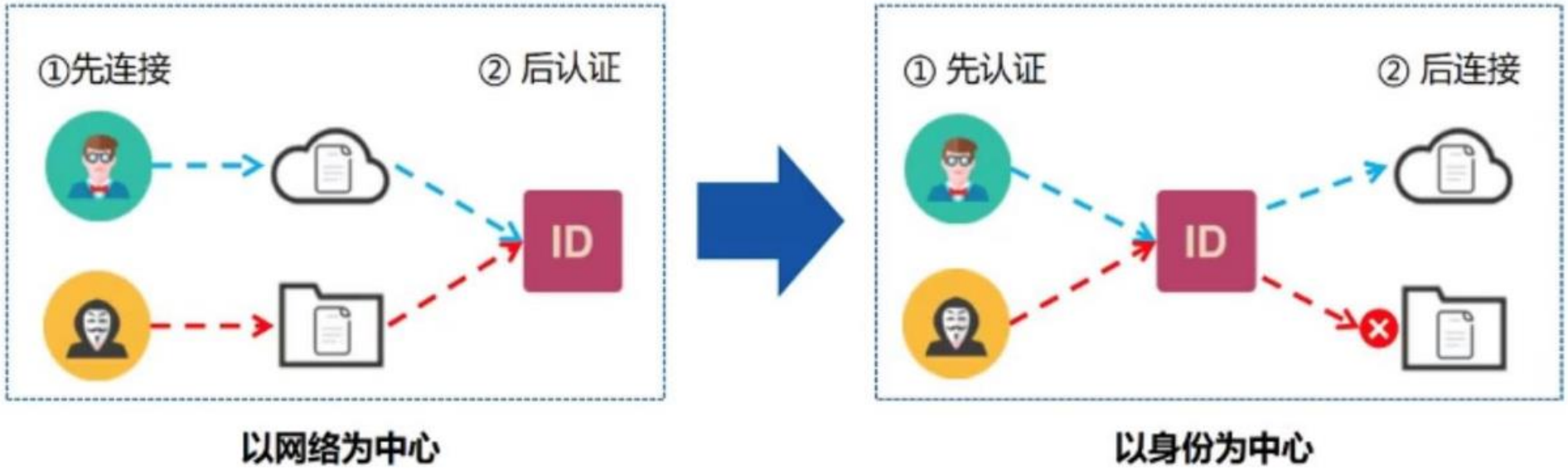
建立智能设备合法性验证机制，构筑云边协同的安全防护技术体系，促进云端安全

零信任网络假定

零信任网络五个基本假定：

- 网络无时无刻不处于危险的环境中。
- 网络中自始至终存在外部或内部的威胁。
- 网络的位置不足以决定网络的可信程度。
- 所有的设备、用户和网络流量都应当进过认证和授权。
- 安全策略必须是动态的，并基于尽可能多的数据源计算而来。

零信任核心概念



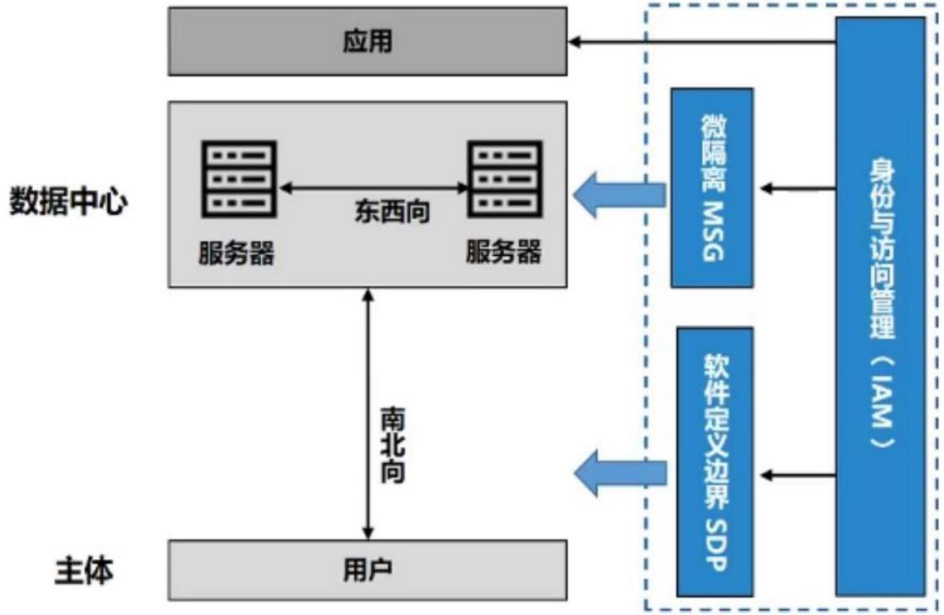
- 零信任架构理念的核心是将传统以网络为基础的信任，变为以身份为信任的机制

  ——“永不信任，始终验证”

- 通过身份治理，实现设备、用户、应用等实体的全面身份化，从零开始构筑基于身份的信任体系，建立企业全新的身份边界。

零信任实践技术架构

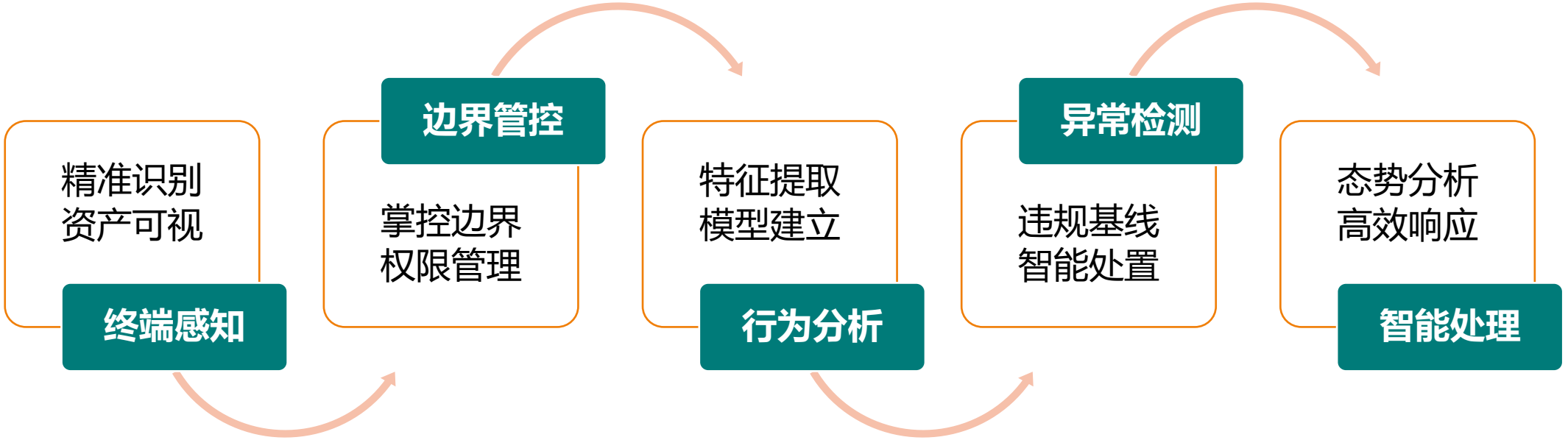
- **南北向流量：**
  - 指用户到服务器的流量（Client-To-Server），通常由“软件定义边界”技术来实现南北向零信任安全。
- **东西向流量：**
  - 指服务器到服务器的流量（Server-To-Server），通常由“微隔离”技术来实现东西向零信任安全。
- **身份安全：**
  - “身份与访问管理”为用户身份信息的输入，实现身份认建以及应用内用户权限的管理。



身份与访问管理（Identity and Access Management，IAM）——
组织信息化的顶层设计以及信息化管理的重要支撑部分，也是零信任架构的支撑。

安全持续监测系统

■ 搭建一站式、流程化、标准化、可视化、透明化的安全体系，通过单一平台即可实现边缘侧终端设备持续感知、接入安全管控、访问行为安全分析、违规异常检测预警、安全态势智能处置等复杂组合场景安全持续监测能力。



零信任预期效益

■ 通过对零信任安全防护体系建设，以动态信任评估体系为核心将安全技术和安全设备融为统一技防体系，结束基于边界的拼凑式防御；

■ 零信任“永不信任，持续认证，最小特权”的理念，不再执拗与空间和时间，以身份为中心为业务与数据提供全方位持续防护，在保证安全性的同时为业务创新提供强有力的网络架构支撑。

降低安全风险

取代传统基于静态边界防护的访问控制策略，建立以身份为核心的动态访问控制策略，实现了访问控制策略由静到动的能力提升，使网络安全风险感知更加敏锐，安全响应更加迅速，并在一定程度上避免供应链安全风险；

增强终端防护

通过研究终端本体的安全防护技术，适配终端TEE（安全可信执行环境）agent，以软件形式灵活实现主流终端接入加密与终端安全监测，形成电力终端本体、环境、行为统一的安全防护能力，从而提升电力终端在新型业务场景下的安全防护能力；

赋能业务发展

采用零信任防护体系，支持各种新增业务模式，基于虚拟化部署的零信任网关可在业务需求时快速弹性扩容，支持5G新业务终端的大规模安全接入，同时防护架构的演变将促进整体公司业务管理转向以身份和权限为核心的管理模式，促进业务整体发展；

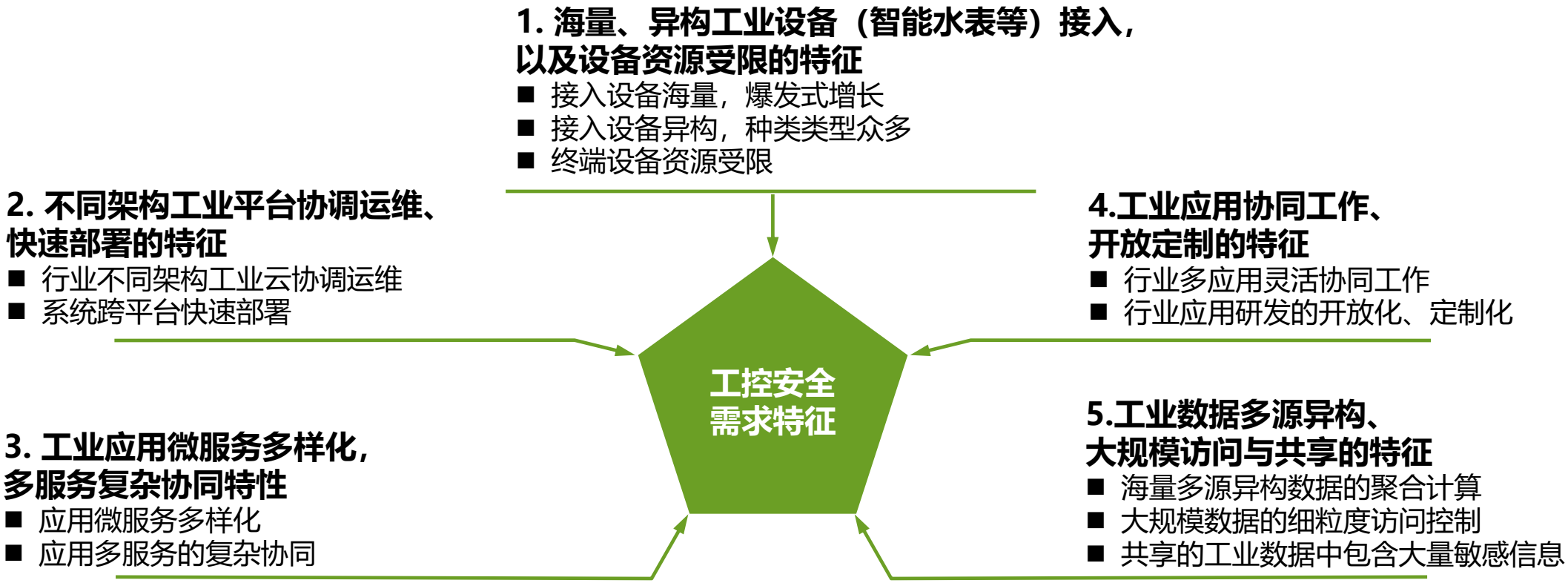
释放数据潜能

零信任防护体系下，使办公、运维及各类终端接入更加便捷，提升了业务的速度与敏捷性，业务数据交互的便利性，更能挖掘数据价值，释放数据潜能。

目录

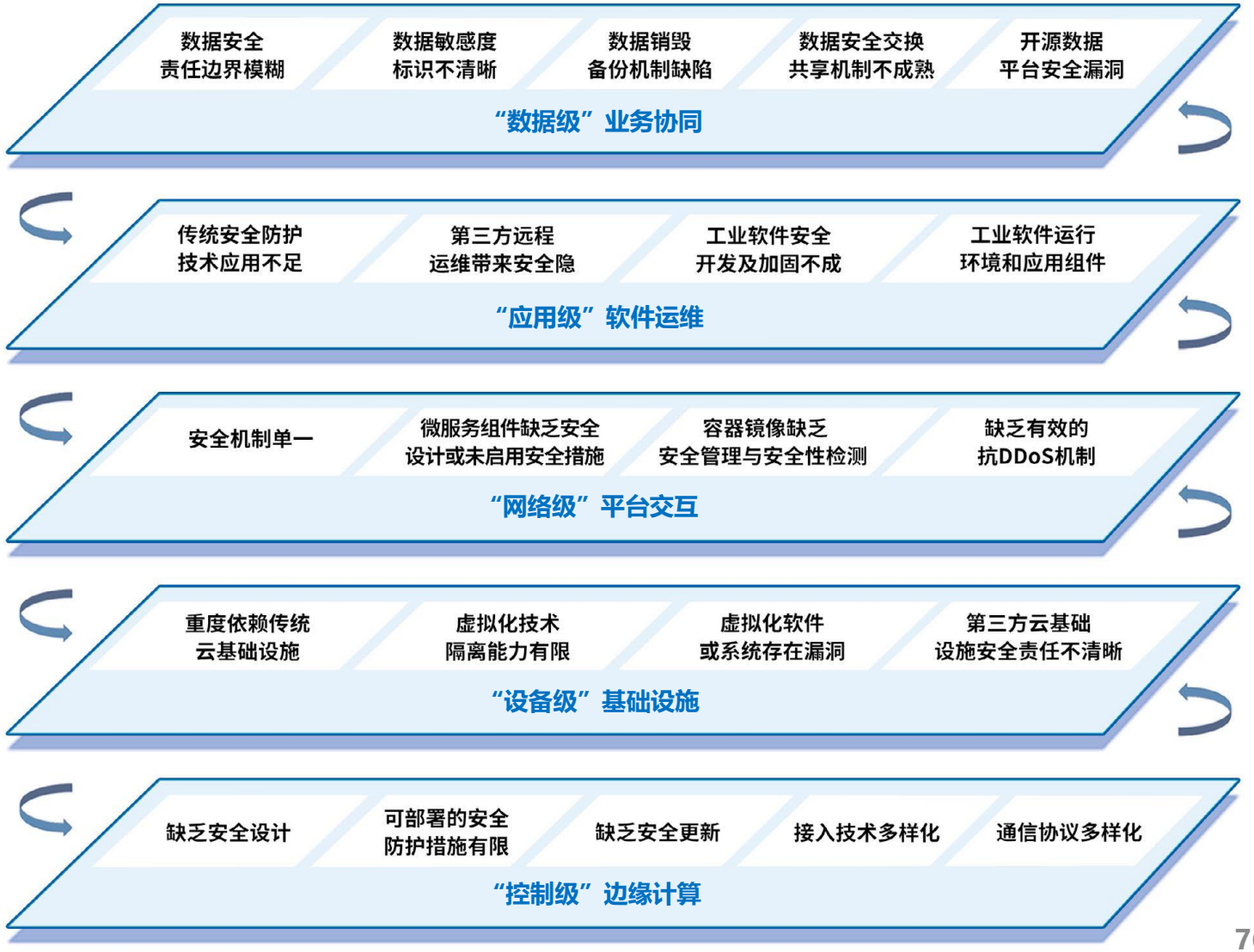
工控安全需求

- 5G边缘计算、工业互联网、人工智能新兴技术驱动下的工控安全新需求



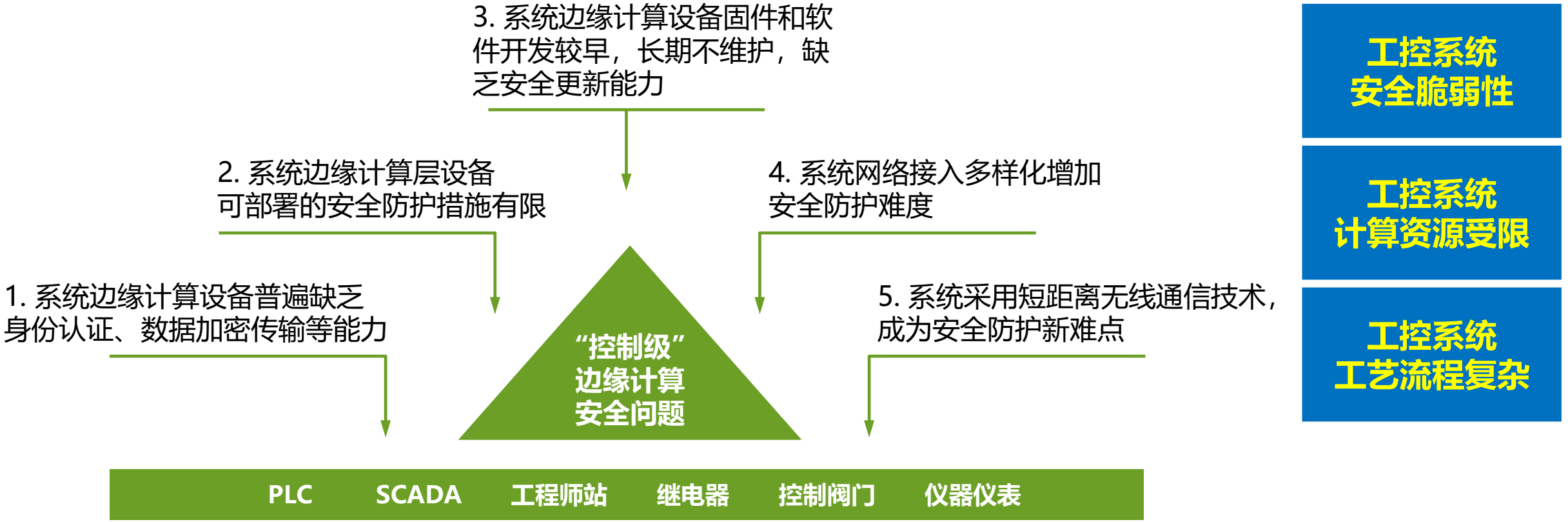
工控安全问题及薄弱点

- 工控安全维度及延伸范畴
  - **“控制级”**边缘计算
  - **“设备级”**基础设施
  - **“网络级”**平台交互
  - **“应用级”**软件运维
  - **“数据级”**业务协同



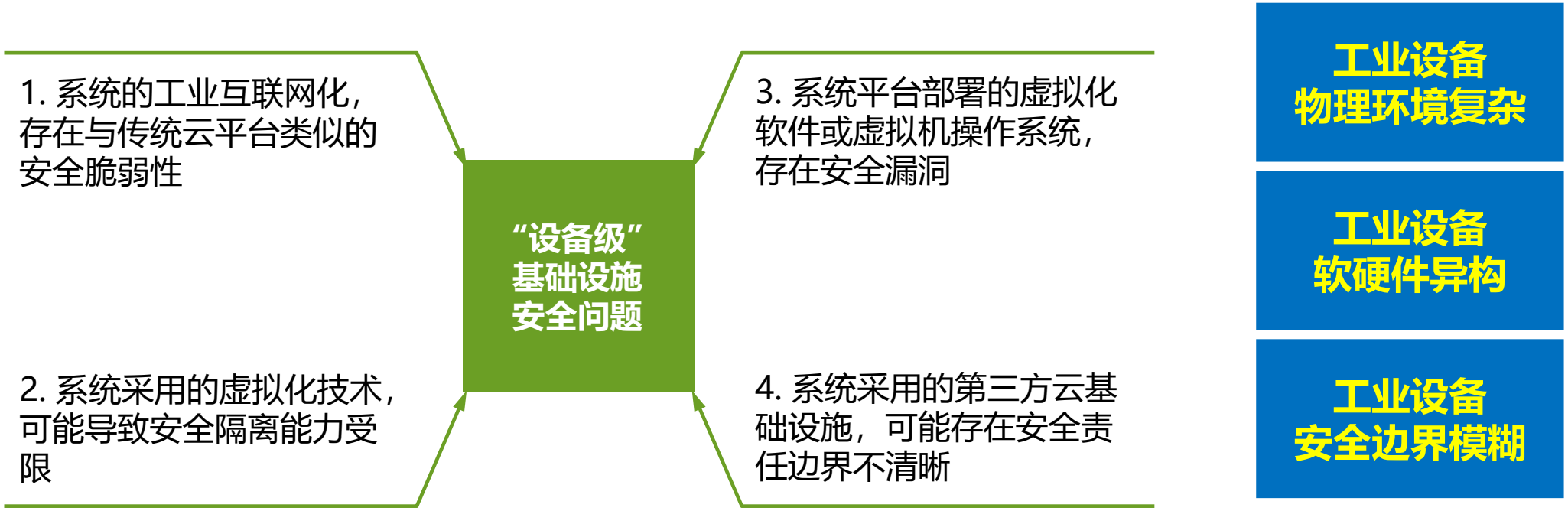
工控安全问题清单

■ 工控安全维度及延伸范畴——“控制级”边缘计算导致的安全问题



工控安全问题清单

■ 工控安全维度及延伸范畴——“设备级”基础设施导致的安全问题



工控安全问题清单

■ 工控安全维度及延伸范畴——“网络级”平台交互导致的安全问题

“网络级”平台交互安全问题

1

传统安全防护手段无法满足
系统平台服务安全要求.

应用远程开发、配置、
部署、运行和监控安全新需求

2

系统平台化发展趋势，
使得微服务组件缺乏安全设计
或未启用安全措施。

微服务组件与外部组件之间的
应用接口缺乏安全认证、
访问控制等安全设计

3

系统采用云平台
架构及容器镜像模式，
缺乏安全管理及安全性检测

4

系统平台缺乏有效的
抗缓冲区溢出、抗拒绝服务攻击等
防御机制，

可能导致工控及业务系统的
资源耗尽和网络瘫痪

工控安全问题清单

■ 工控安全维度及延伸范畴——“应用级”软件运维导致的安全问题

工控软件可靠性要求高

工业应用微服务部署

工业软件开发设计缺陷

工控安全问题清单

■ 工控安全维度及延伸范畴——“数据级”业务协同导致的安全问题

1 数据安全防护责任边界模糊

工业行业数据体量大、种类多、关联性强，在采集、传输、存储、处理、使用等环节责任边界模糊

2 敏感数据标识及保护技术待完善

研发、生产、运维、管理等数据敏感程不同，需要数据分级分类实现数据细粒度标识

3 数据销毁及备份机制存在缺陷

系统平台数据资源的重新分配，存在用户数据泄露风险

4 数据安全共享交换机制尚不成熟

行业数据分析决策，需要多方数据计算或训练模型，安全共享交换机制尚未成熟

5 开源数据平台存在安全漏洞

行业数据分析系统主要基于开源软件（存储和计算框架）部署，存在安全漏洞

行业数据多源异构

行业数据共享交互需求

行业数据智能算法应用

THANK YOU

聚焦行业痛点　赋能内生安全