边缘计算信息安全架构分析与技术展望

中国科学院沈阳自动化研究所
尚文利

提 纲

1. 边缘计算技术的产生
2. OFC、IIC安全参考架构
3. ECC安全参考架构建议
4. 安全创新技术展望

一个万物感知、万物互联、万物智能的智能社会

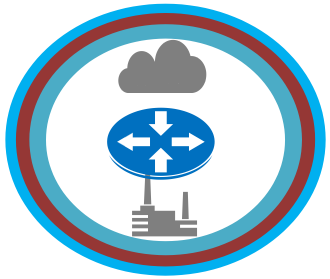
 … people	新增40亿互联网用户
 …cities	27座城市超过1000万人口
 …devices	80亿智能手机在使用
 …connectivity	联接数将达1000亿
 …content	人均日消费1.7GB数据
 …usage	3万亿美元移动支付市场

到2025年

行业数字化转型是构建智能社会的支柱

边缘计算（EC-IOT）的定义与发展三阶段

边缘计算（Edge Computing）是在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力的开放平台，就近提供边缘智能服务，满足行业数字化在敏捷联接、实时业务、数据优化、应用智能、安全与隐私保护等方面的关键需求。



联接

统一　安全　易集成

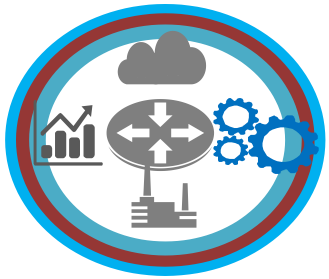
50B
设备

85%
未连接

智能

数据分析　数据可视化　实时决策

50%
数据需要在边缘分析，处理



自治

自决策　自响应　自优化

微网格

提 纲

1. 边缘计算技术的产生
2. OFC、ICC安全参考架构
3. ECC安全参考架构建议
4. 安全创新技术展望

现阶段安全技术架构

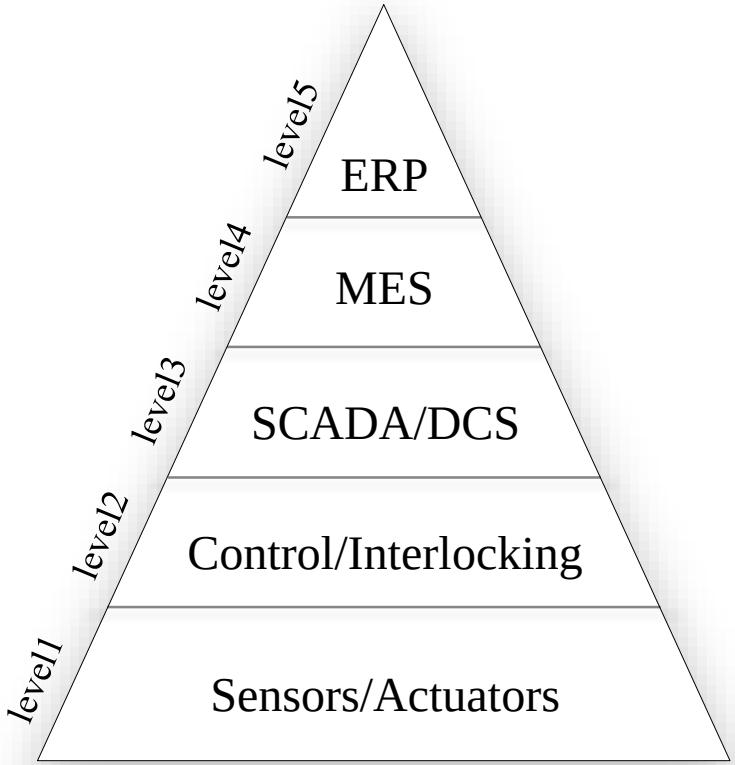
- 基于标准指南，ICS安全技术是 **“纵深防御”体系，**针对网络的安全控制提供被动防御，体现为区域隔离、防火墙、入侵检测、漏洞挖掘等方面。

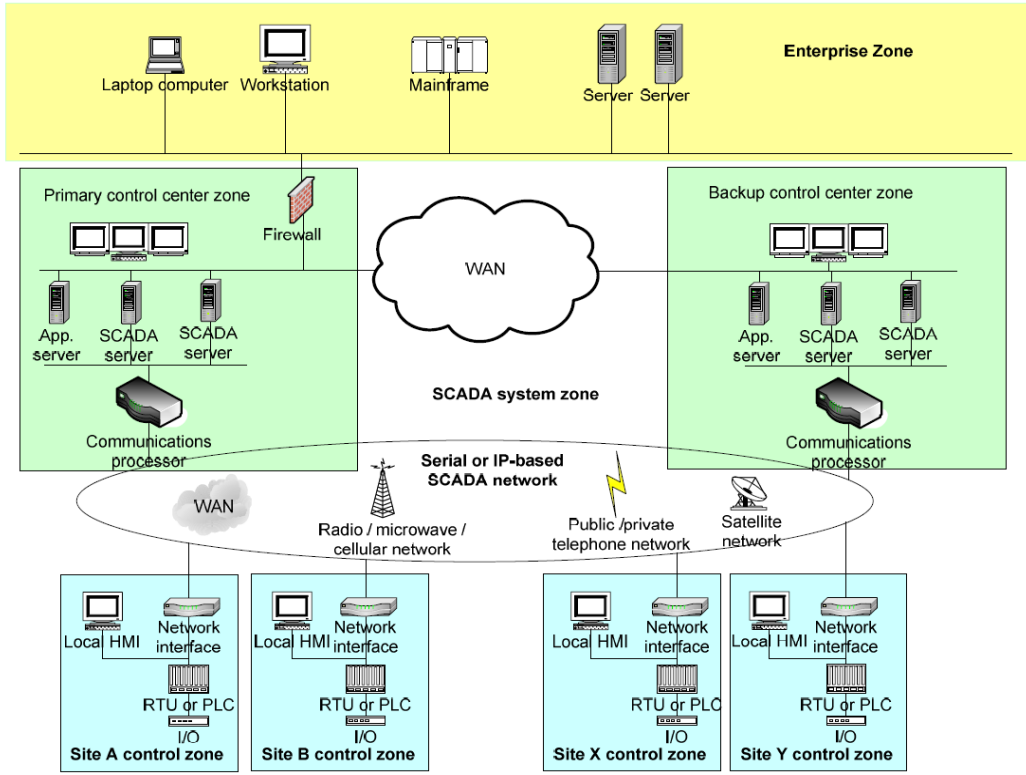
IEC 62443

Industrial communication networks — Network and system security

NIST SP800-82

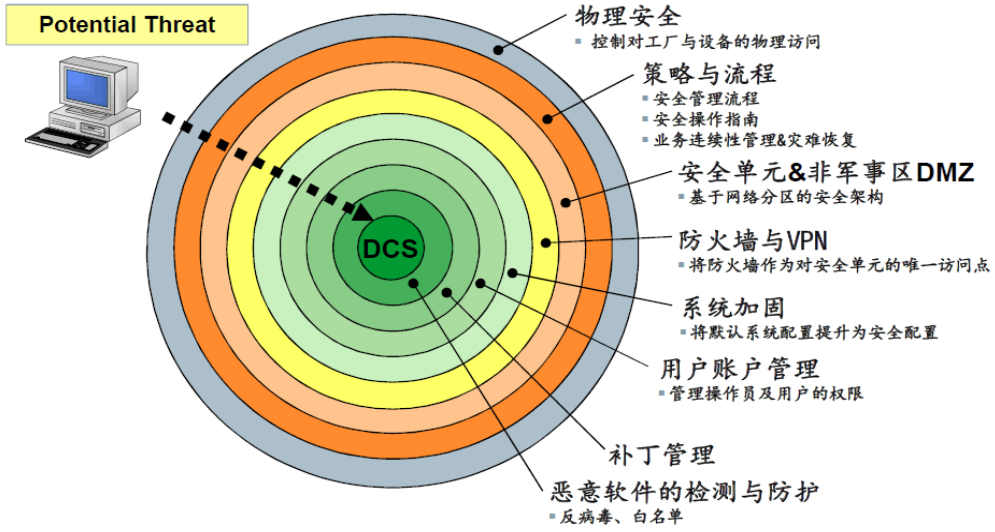
Guide to Industrial Control Systems Security

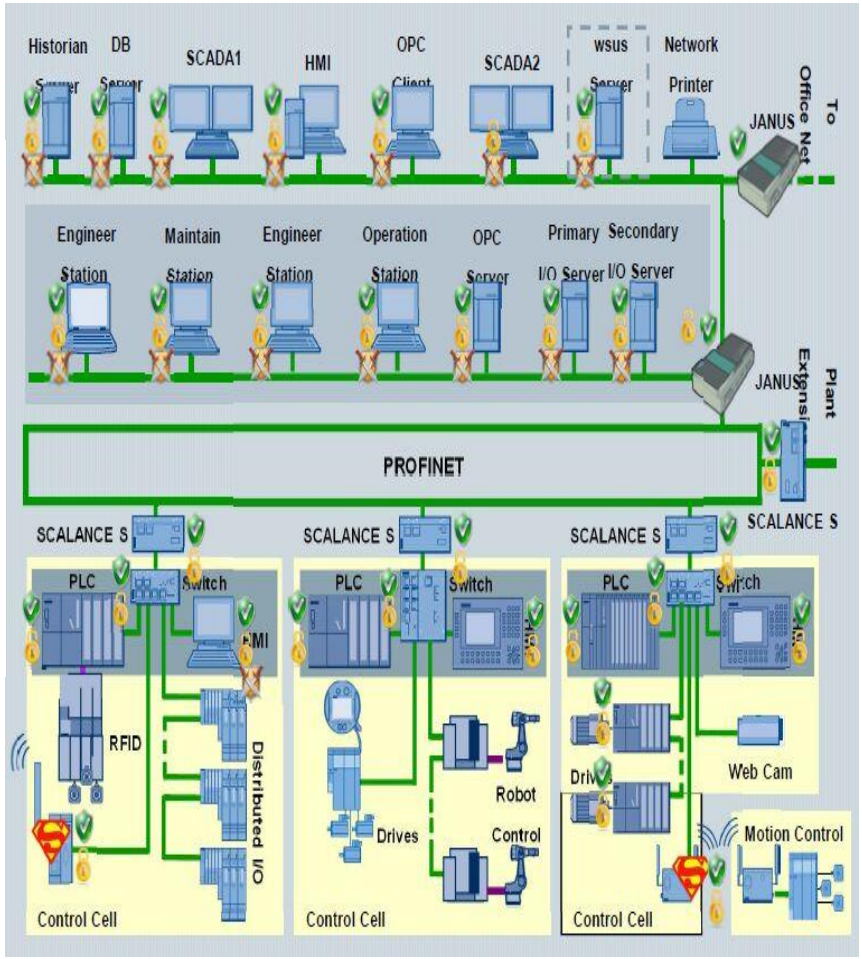




西门子工业安全技术架构

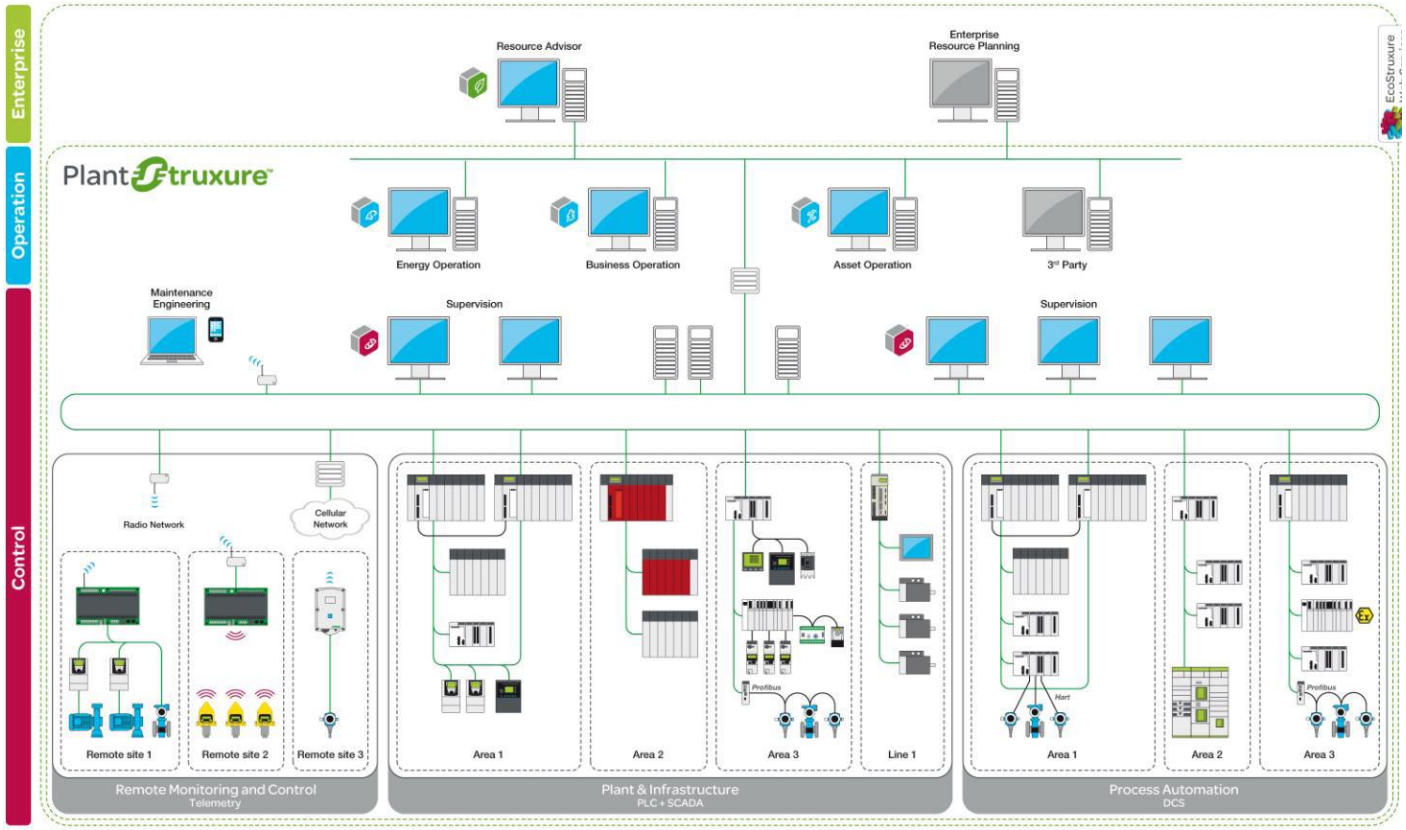
基于纵深防御理念的安全工控系统





施耐德工业安全技术架构

“自下而上”的三级防护体系，设备级防护是核心，减少发生概率，降低危害程度。



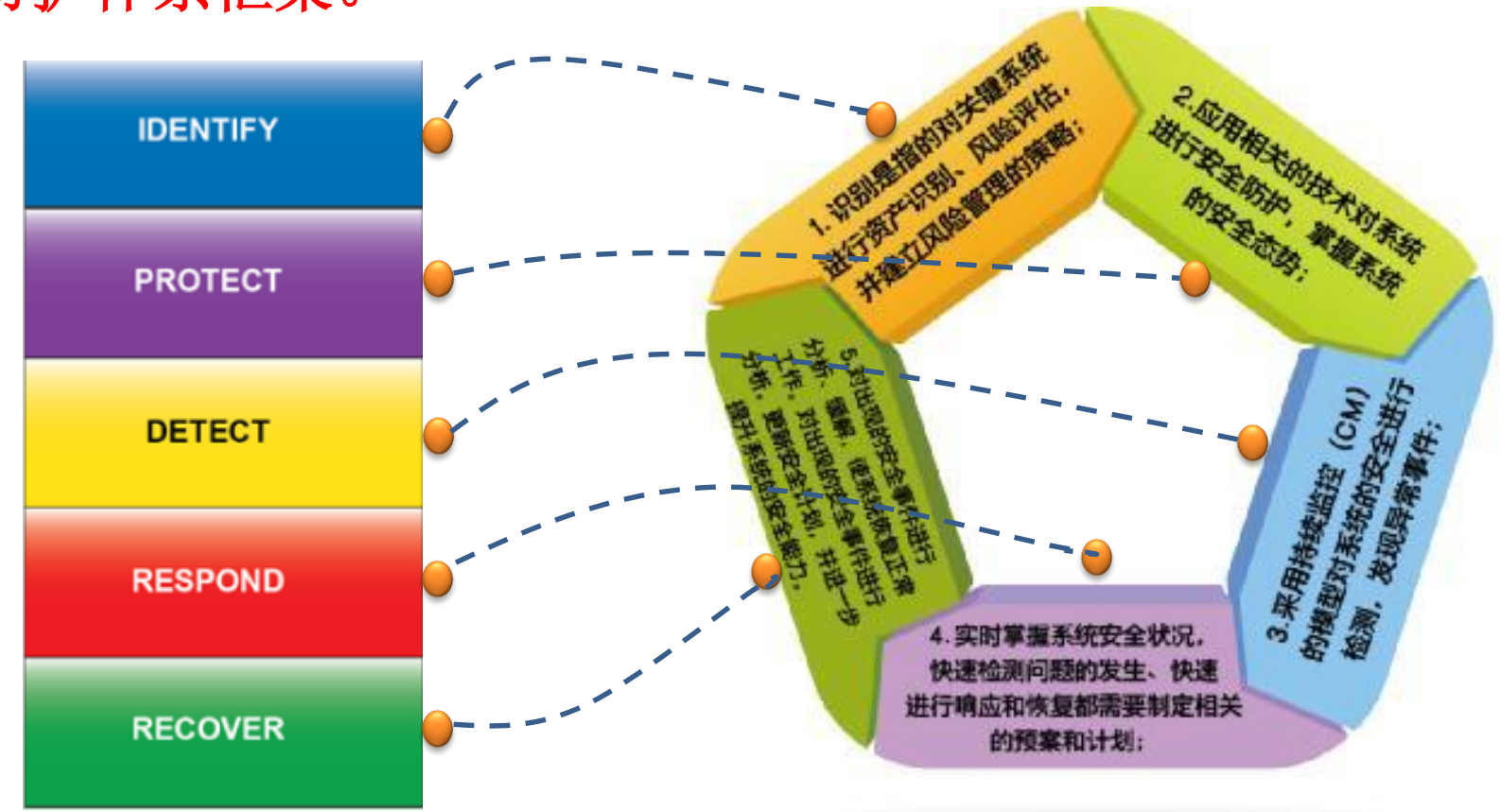
管理级

系统级

设备级

NIST关键基础设施的安全框架

基于识别、保护、检测、响应和恢复五个层面的安全防护体系框架。

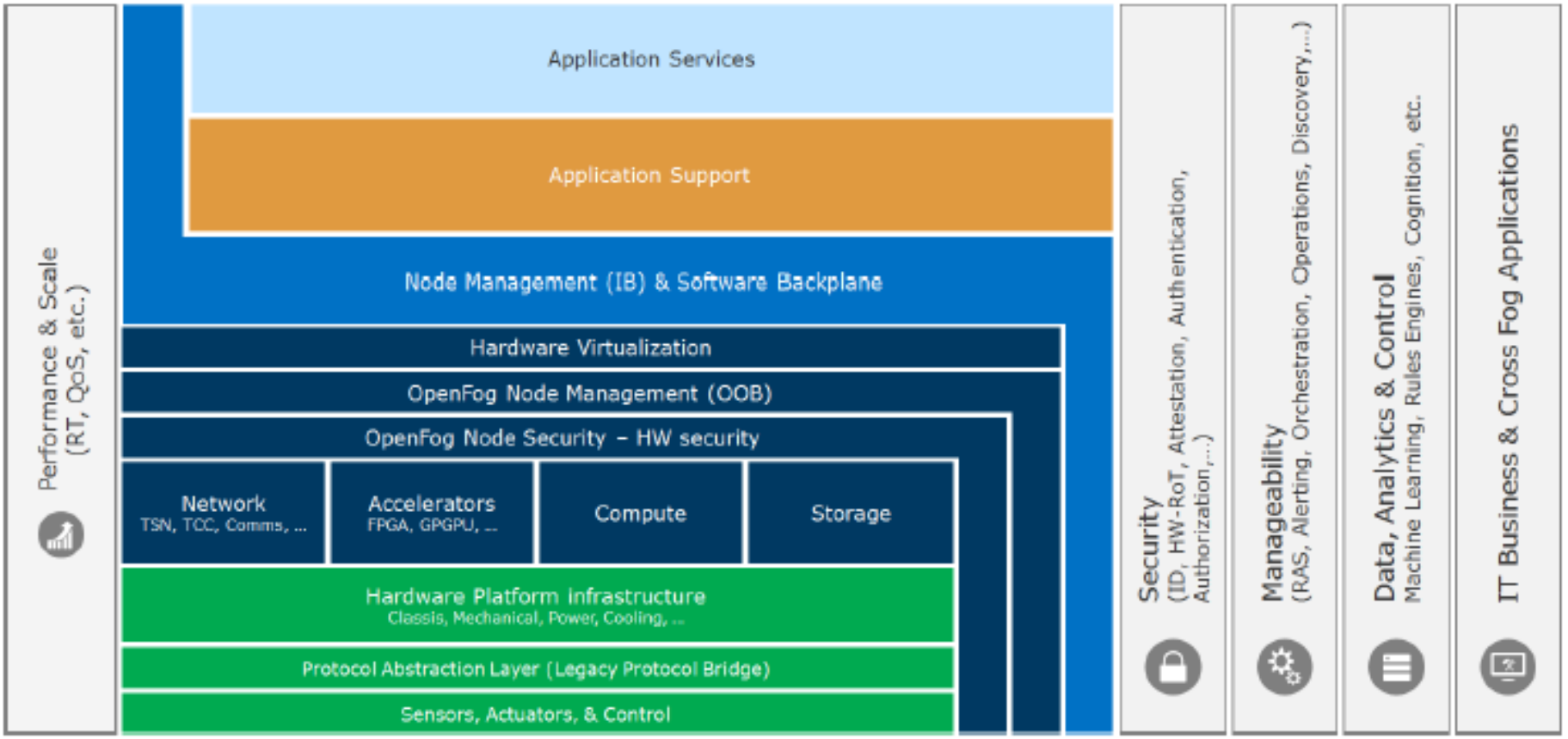


OFC安全参考架构

- 2015年11月19日，ARM、思科、戴尔、英特尔、微软和普林斯顿大学Edge Laboratory等物联网(IoT)领导者成立了OpenFog Consortium（开放雾联盟）。
- 2017年2月9日，美国加州弗里蒙特，OpenFog Consortium宣布发布OpenFog参考架构(RA)，旨在支持物联网(IoT)、5G和人工智能(AI)应用的数据密集型需求的通用技术框架。
- OFC给出雾计算的定义为“雾计算是一种靠近云物连接用户侧的，具有分布式计算、存储、控制和网络功能的水平系统级架构”。

OFC安全参考架构

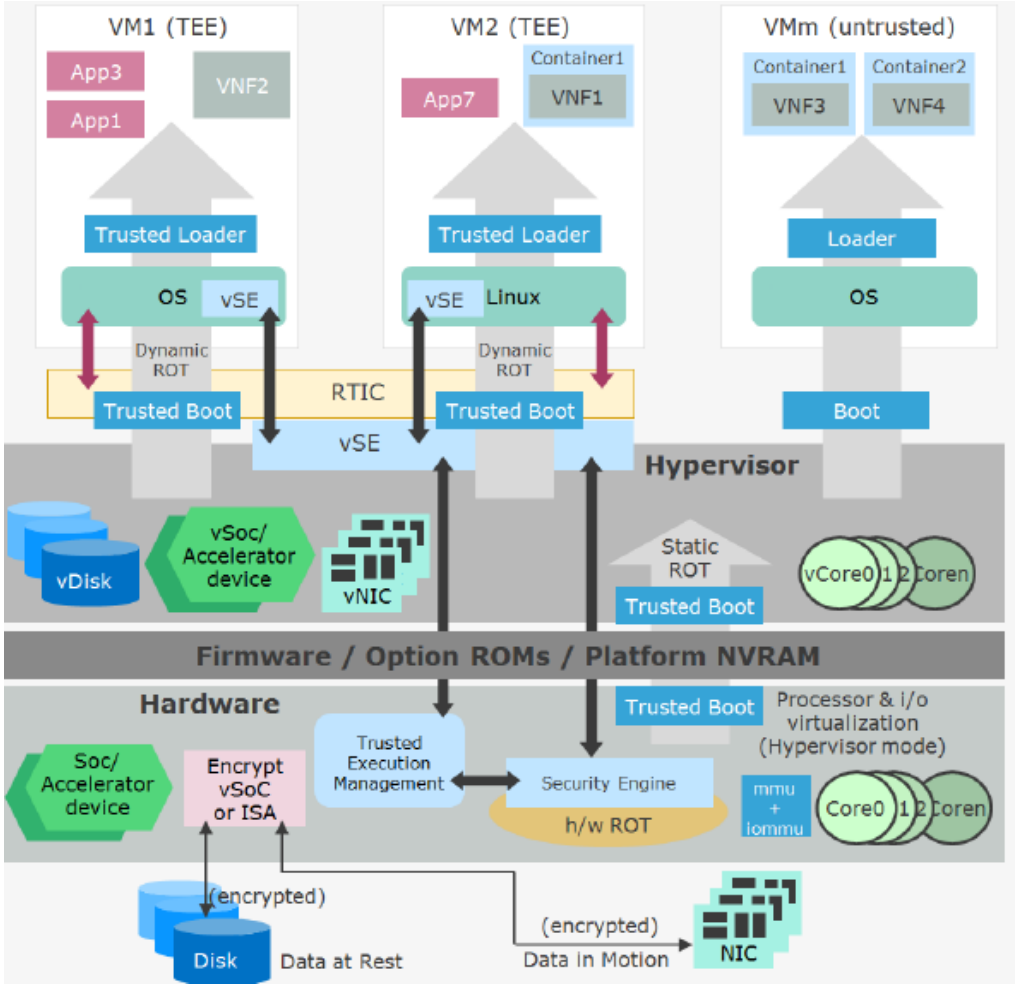
- OFC参考架构贯穿节点、网络、数据、应用等等。



强调End-to-End security的实现

OpenFog Node Security

- 物理安全机制
  - ✓ 针对物理特征（外壳，封装或螺丝）的检测、响应
- 可信机制
  - ✓ 可信根、可信启动过程、身份证明、认证过程
- 虚拟化技术
  - ✓ 在有能力或重要的主节点实现任务的虚拟化，可隔离病毒发生



Network Security

- 通信安全机制
  - ✓ 机密性、完整性、认证性、不可抵赖性，并且在设计时能耗、复杂性、安全性要求不同

    - Node-to-Cloud Secure Communication Pathways
    - Node-to-Node Secure Communication Pathways
    - Node-to-Device Secure Communication Pathways

- 访问控制、入侵检测、异常行为分析等防护技术
- 协议安全

Layers	Protocols
PHY & MAC Layer	• WLAN: 802.11 • WPAN: 802.15 • PLC: PRIME • Automation: CIP
Wireless Protocol Stacks	• WiFi • Bluetooth • ZigBee
Adaptation Layer	• WLAN/WPAN: 6LowPAN • PLC: PRIME IPv6 SSCS • Automation: EtherNet/IP
Transport/Network Layers	• UDP over IPv6 • TCP over IPv6 • uIPv6 Stack
Application Layer (Publish-Subscribe Messaging)	• CoAP • MQTT • AMQP • RTPS
Routing	• RPL • PCEP • LISP (Cisco)
Security	• 802.1AR – Secure Device Identity • 802.1AE - Media Access Control (MAC) Security • 802.1X – Port-Based (Authenticated) Media Access Control • IPsec AH & ESP, Tunnel/Transport Modes • (D)TLS – (Datagram) Transport Layer Security

Data Security

- Data in Use
  - ✓ 访问权限、内存保护、机密性使用、调试接口访问限制等
- Data at Rest
  - ✓ 全磁盘加密、文件系统或数据库加密、访问权限等
- Data in Motion （transit）
  - ✓ VPN或SSL方式、连接加密、文件/数据加密

Security management

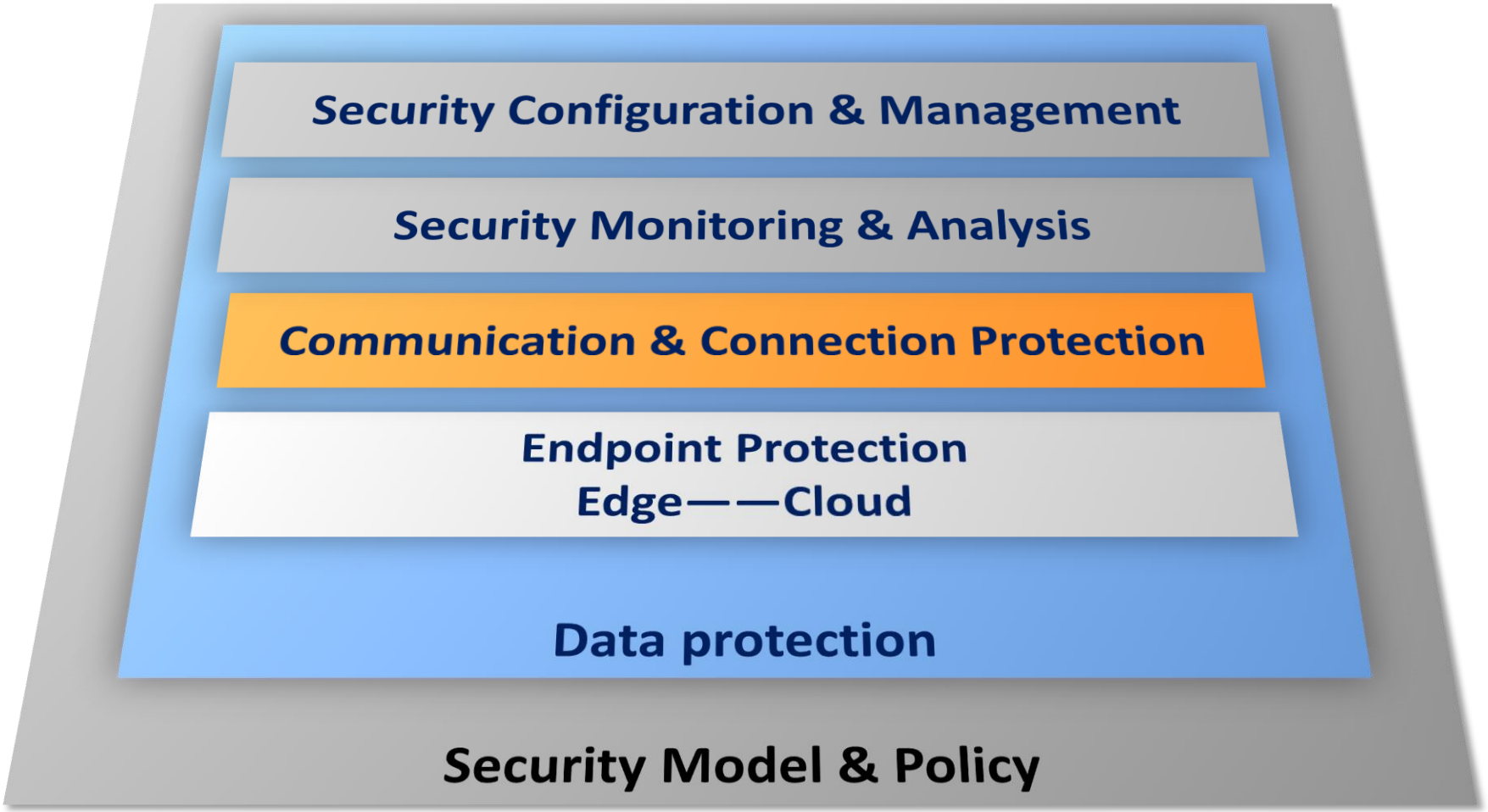
- key management
- crypto suite management
- identity management
- security policy management.

IIC安全参考架构

- 美国GE提出并主导的工业互联网联盟（IIC，Industrial Internet Consortium）
- 2016年09月，发布了《工业物联网安全框架》，一份旨在解决工业物联网(IIoT)及全球工业操作运行系统相关安全问题，从多个角度解决安全、可靠性和隐私问题。

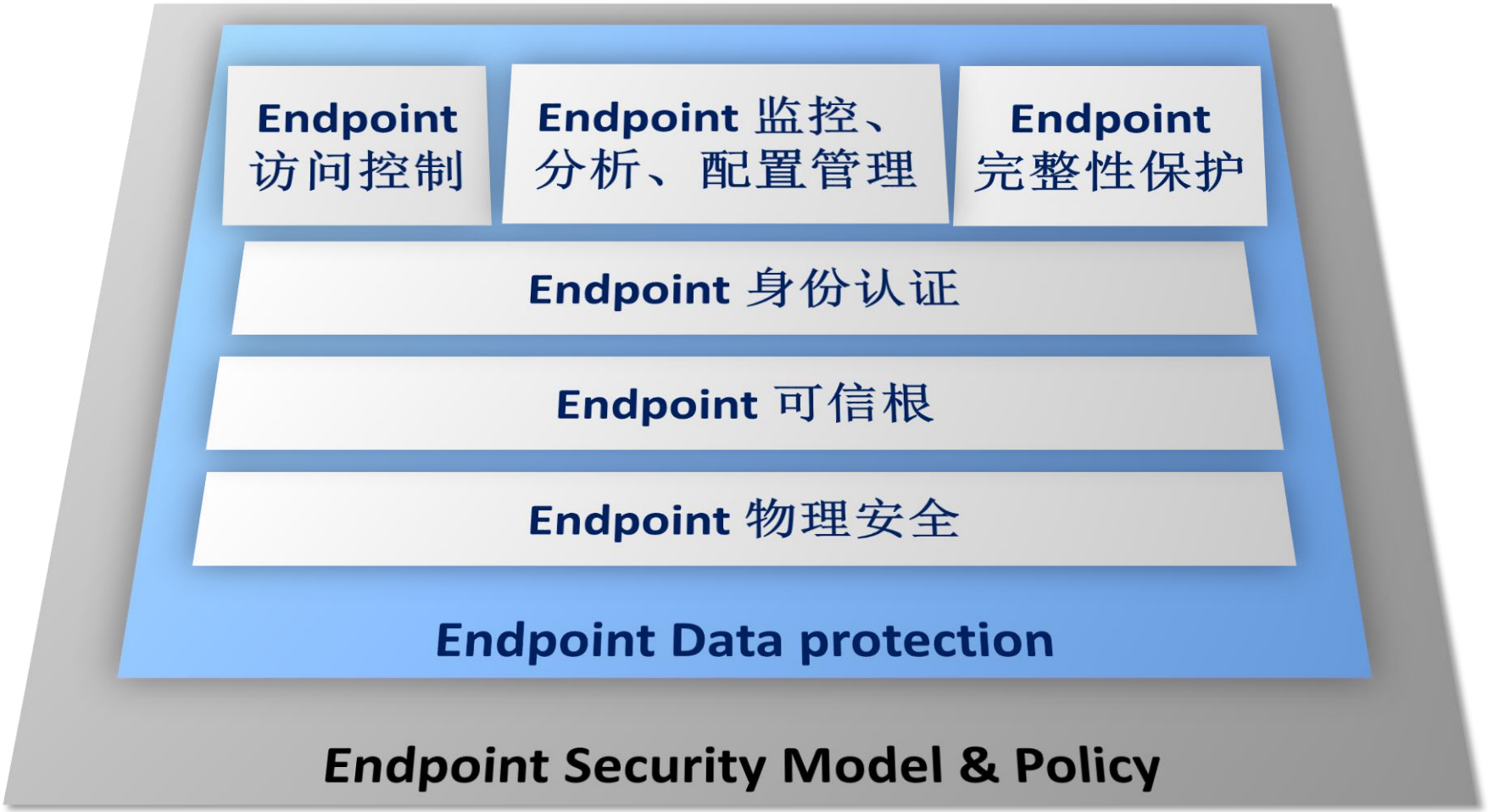
IIC安全参考架构

- 三个层次视角解析安全架构



IIC安全架构剖析参考

- **Endpoint Protection:**可用性>机密性>完整性

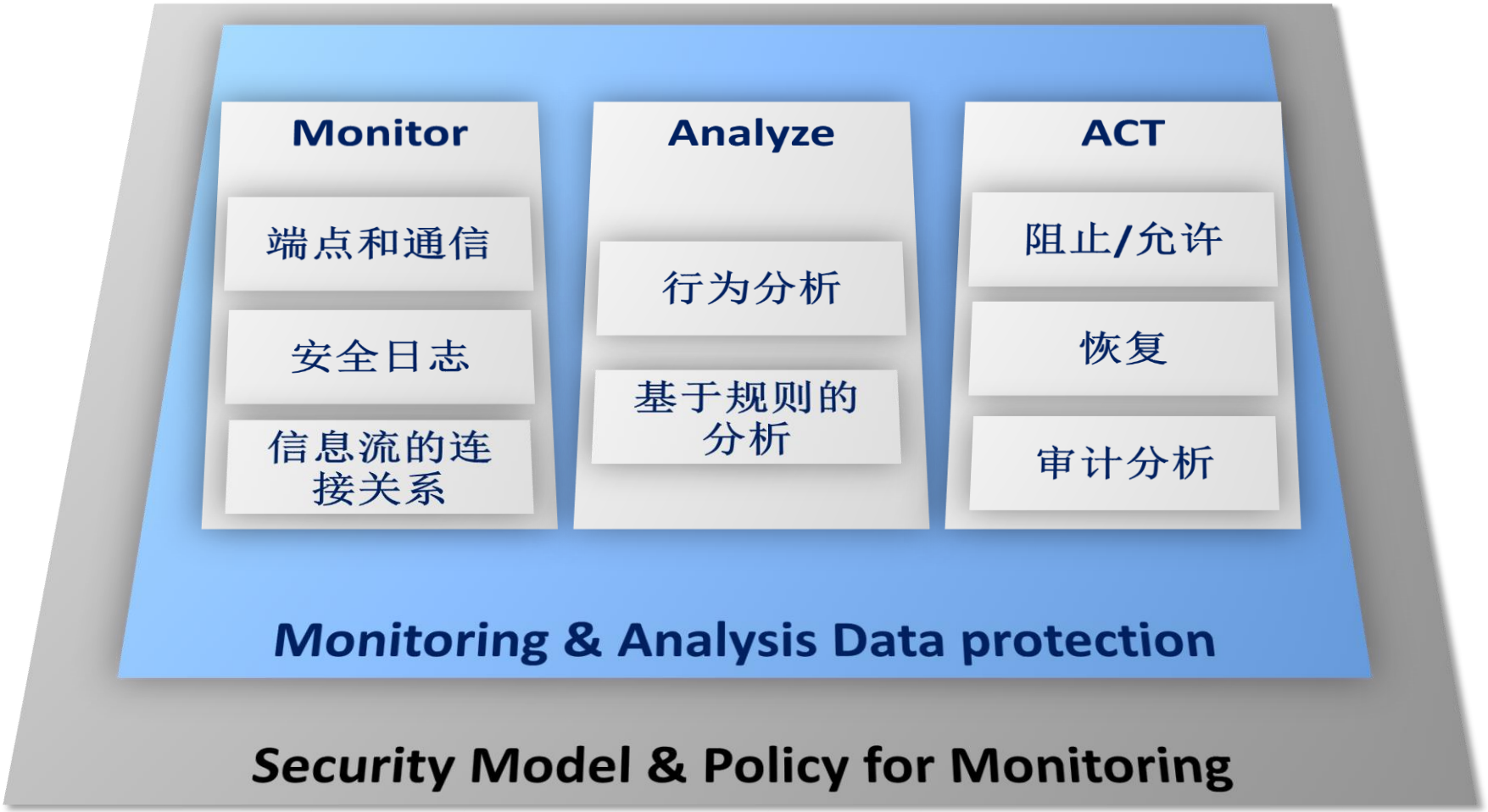


IIC安全架构剖析参考

- **Communication & Connection Protection**

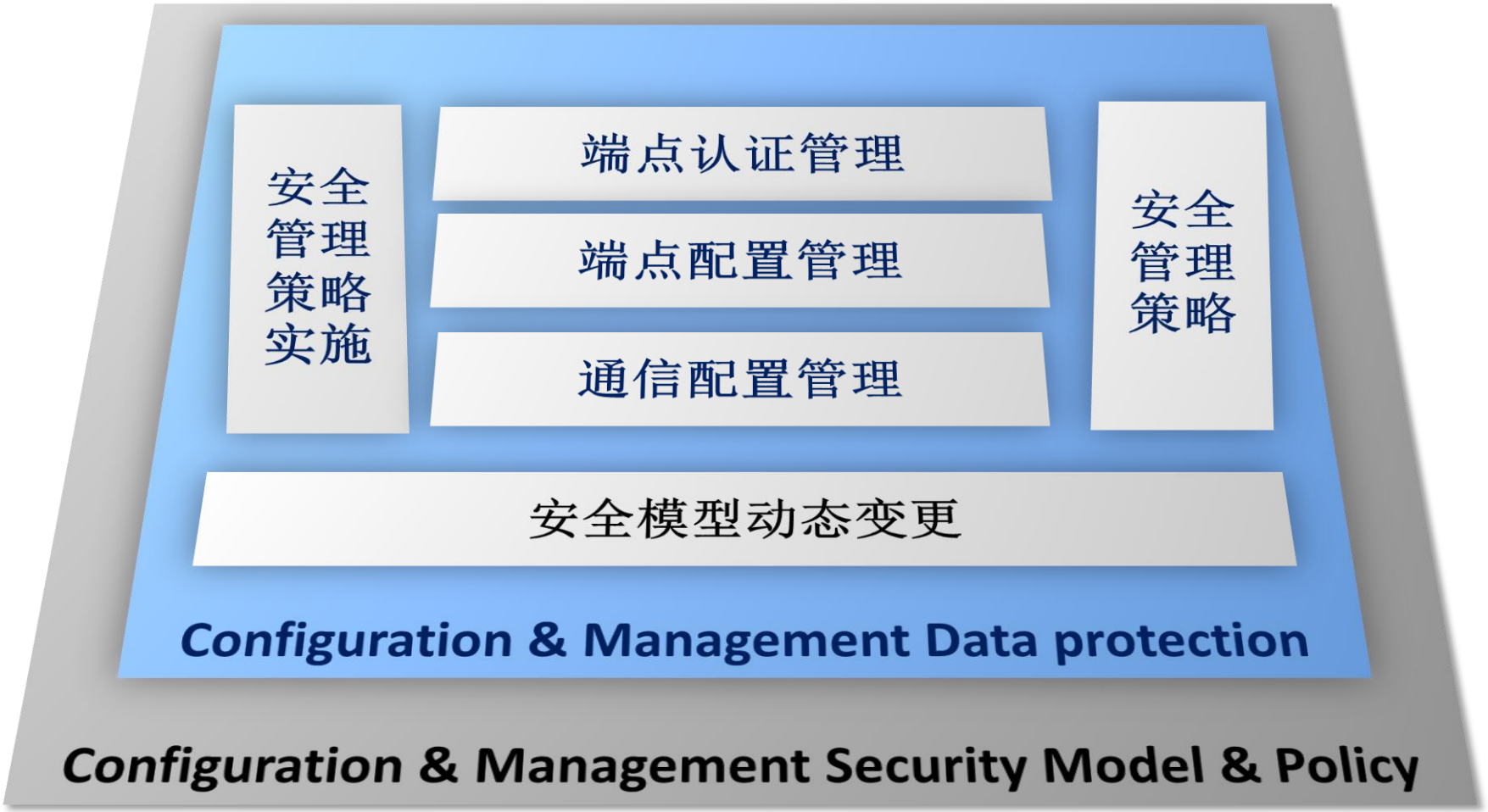
IIC安全架构剖析参考

- **Security Monitoring & Analysis**



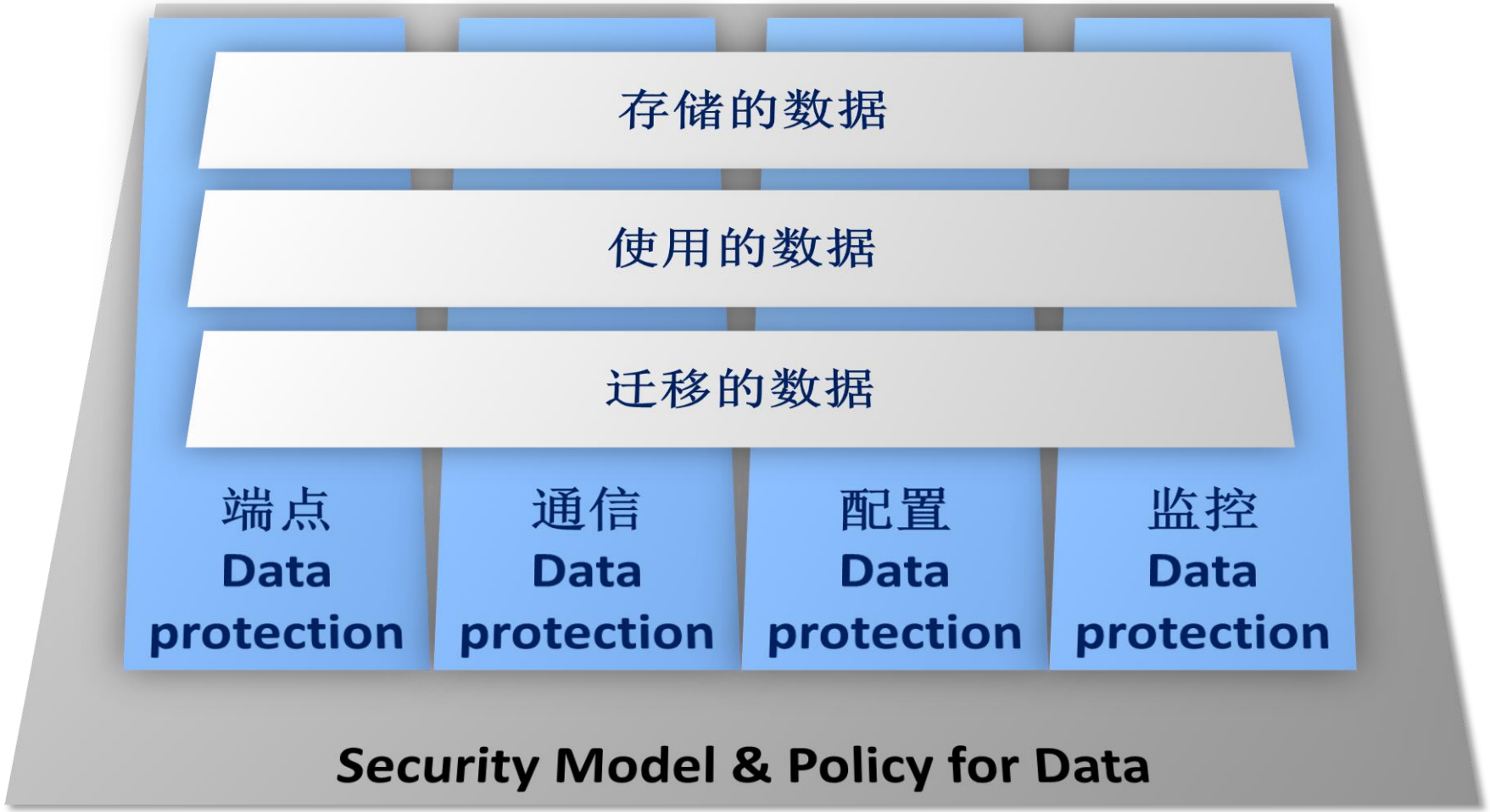
IIC安全架构剖析参考

- **Security Configuration & Management**



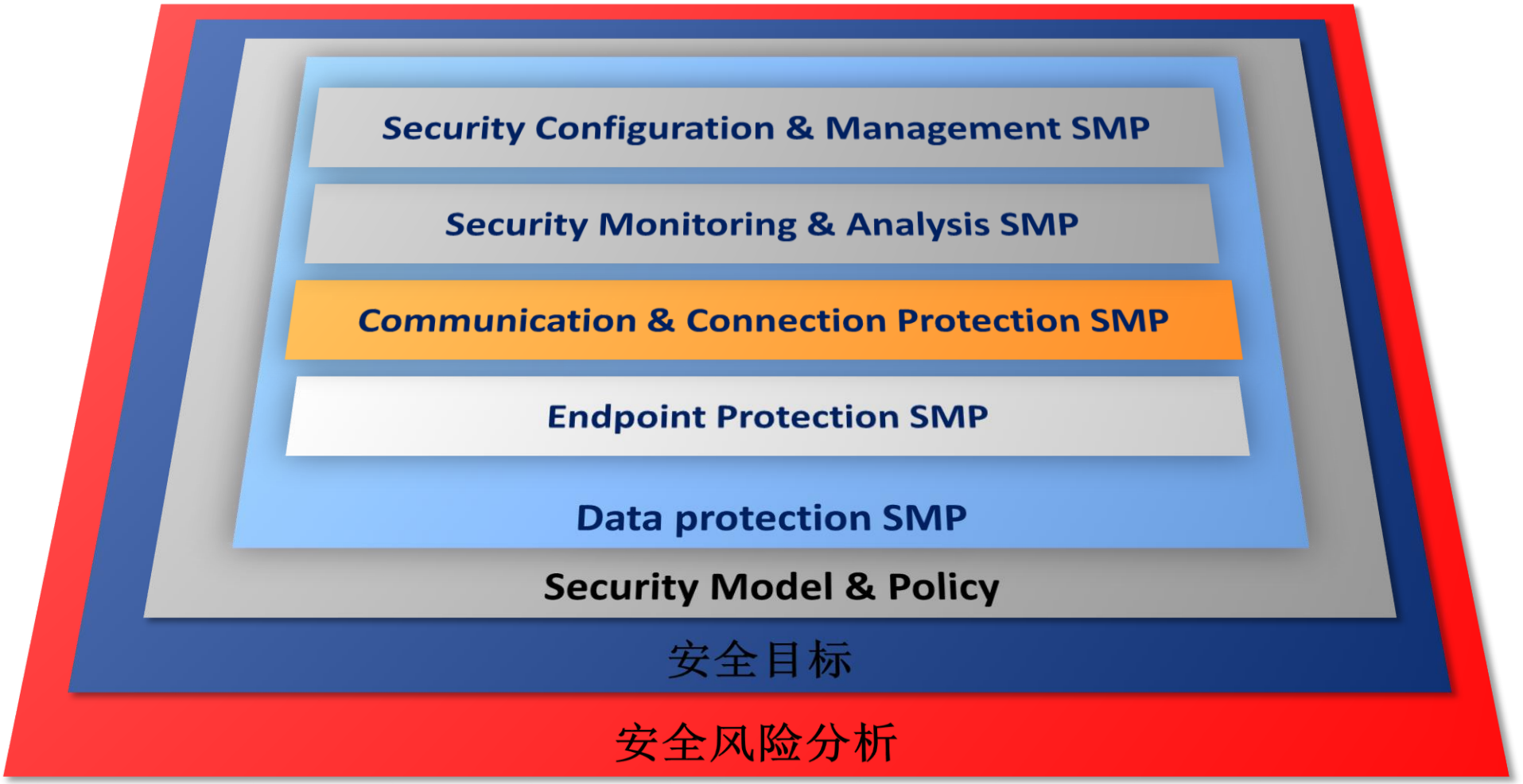
IIC安全架构剖析参考

- **Data protection**



IIC安全架构剖析参考

- **Security Model & Policy（SMP）**



提 纲

1. 边缘计算技术的产生
2. OFC、ICC安全参考架构
3. ECC安全参考架构建议
4. 安全创新技术展望

工业领域的边缘计算参考架构映射

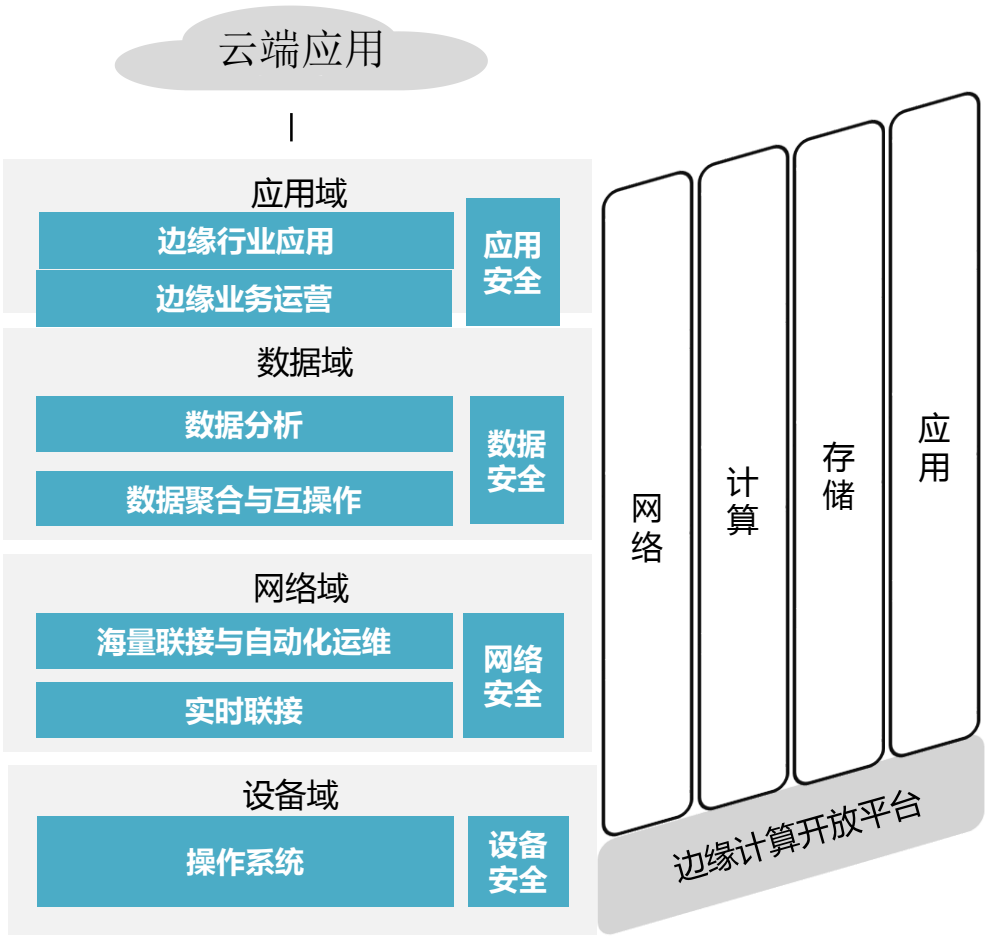
美国国家标准与技术研究院（NIST）给出了云计算的定义为“云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问， 进入可配置的计算资源共享池（资源包括网络，服务器，存储，应用软件，服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。”

除“云”之外皆是“边缘”

边缘计算中的“边缘”，是指从数据源到云计算中心路径之间的任意网络和计算资源。

边缘计算参考架构安全问题

边缘计算参考架构



- **应用域**
  实现边缘行业应用，支撑边缘业务运营；
- **数据域**
  数据全生命周期服务，并保障数据的安全与隐私性；
- **网络域**
  为系统互联、数据聚合与承载提供联接服务；
- **设备域**
  支撑现场设备实现实时的智能互联及智能应用。

提 纲

1. 边缘计算技术的产生
2. OFC、ICC安全参考架构
3. ECC安全参考架构建议
4. 安全创新技术展望

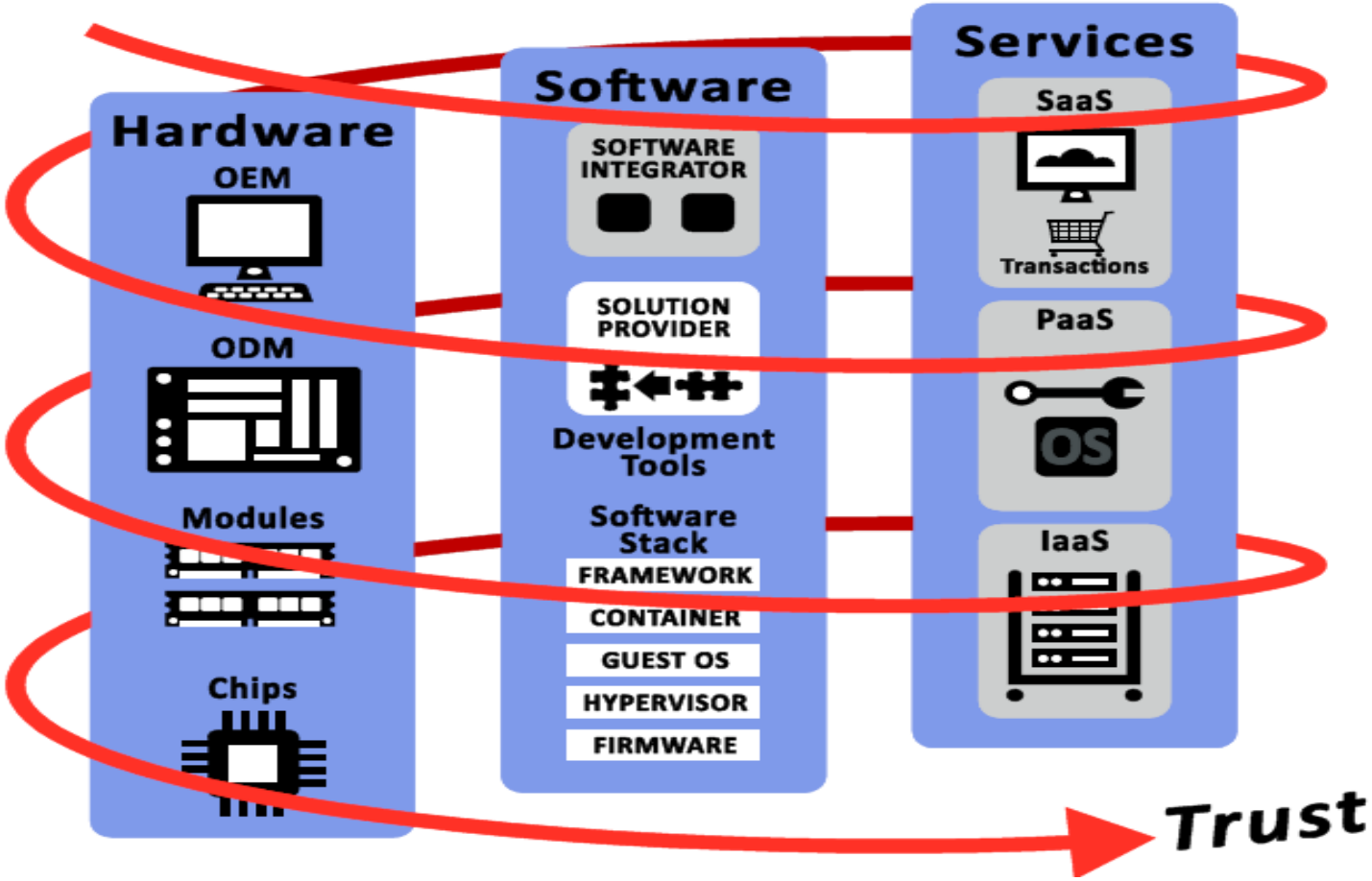
网络安全

形成下一代工业防火墙作为ECC边界防护的有利支持

- 针对通信网络层的攻击，研究下一代工业防火墙（集成多种安全功能于一体，实现安全功能软件化的自由配置，简化网络部署并能动态调节安全功能。

应用安全

- 跨域信任服务体系——区块链技术



已有研究-工业防火墙

防护模型

基于“区域”与“管道”的安全防护模型

深度防御

Modbus/TCP、Modbus/UDP、OPC 等工控协议应用数据的深度解析

访问控制

基于规则策略的动态包过滤和 Syslog 的实时报警技术

冗余电源设计

电源采用 12VDC 电压冗余供电，提高硬件可靠性

工业级设计

低功耗无风扇，双散热面，工业级防腐设计，导轨式安装

兼容性设计

兼容所有 PLC、HMI、RTU 等工业控制设备

高可用性

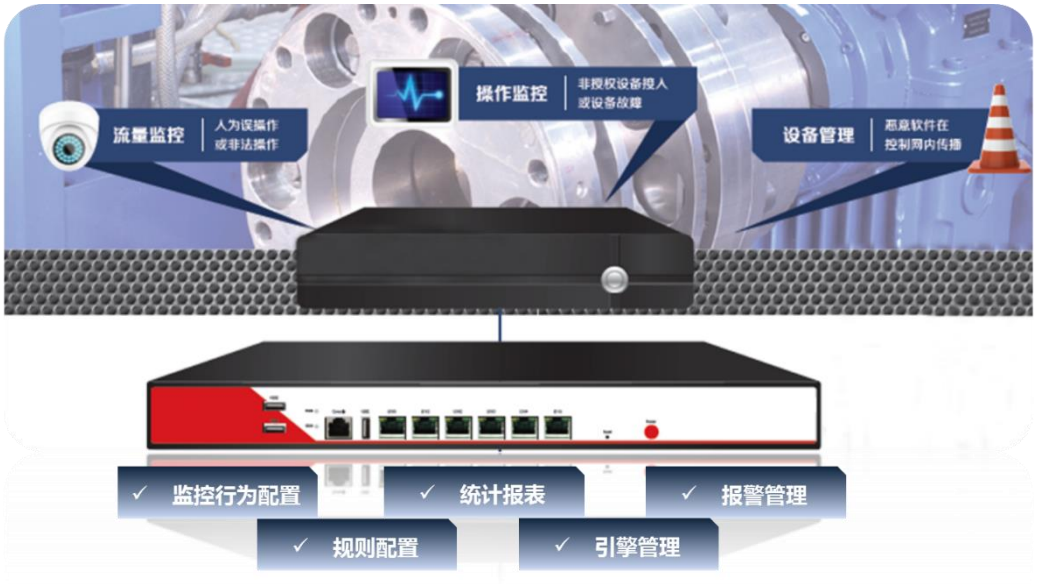
支持时间同步，重启自动加载规则，console 口配置

多模式运行

包括直通、管控和自学习模式，适应多种网络拓扑结构

已有研究-网络监测

研究面向工业通信协议的网络安全监测技术，为安全态势感知提供基础分析数据。



敬请批评指正！