匡恩网络

工业互联网防御之道

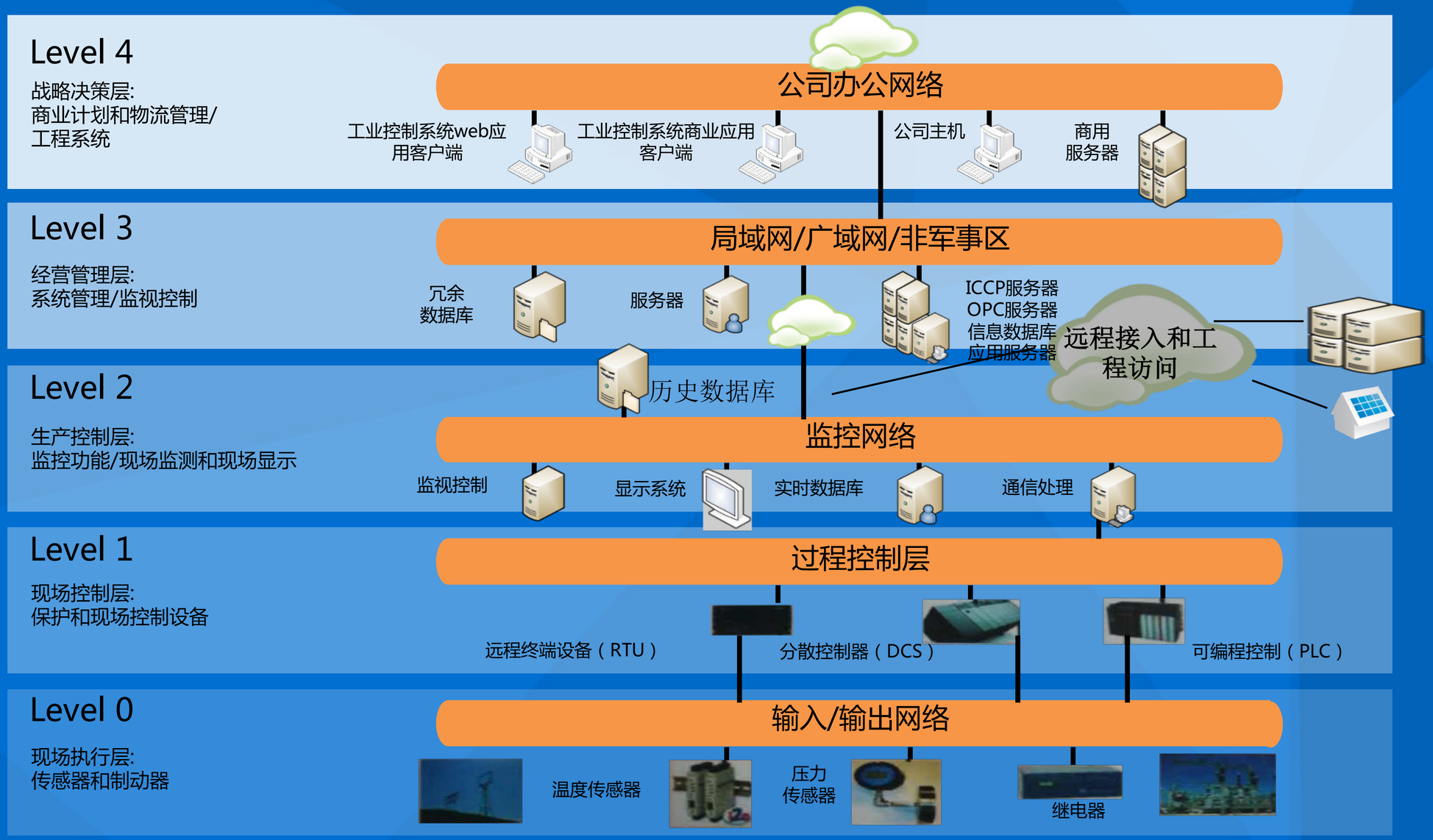
四个安全 + 时间持续

讲演者：井柯
Mail：kjing@acorn-net.net
Tel:13521526163

智能工业控制网络安全专家
北京匡恩网络科技责任有限公司

匡恩网络

工控系统网络涵盖范围



智能工业控制网络安全专家

匡恩网络

工业互联网安全防护

智能工业控制网络安全专家

匡恩网络

四个安全性

四个安全性：

一个事物的多面性；动静合一、内外兼修

结构安全性——基本概念

- **结构**

物理结构：指网络结构、生产布局的结构；
访问结构：亦即权限结构，指工控网络中不同级别的访问权限控制。

- **结构安全性**

分区隔离。当发生安全事件时，合理的结构能将威胁控制在一个范围内。
例：国家电网“横向隔离、纵向认证”。

- **入侵容忍度**

假设不能完全检测出对系统的入侵行为，当入侵和故障突然发生时，能够利用“容忍”技术来解决系统的“生存”问题，以确保系统的保密性、完整性、真实性、可用性。

本体安全性——基本概念

本体包括哪些？

即工控网络中的所有设备，除PLC、DCS等之外，还包括上位机、服务器等，也包括工控安全设备自身。

什么是本体安全性？

一个工控系统内的每一个单元和设备，自身是否有和有哪些漏洞和威胁？工业控制系统的本体安全性存在极大缺陷。

特别关注：

稳定性与安全性的区分

匡恩网络

本体安全性：设备安全、服务安全

匡恩为客户交付的两类

- 设备和服务（包括建设和运营）

自主研发和测试

- 自身安全功能设计（权限、审计、接口等）
- 自身安全防护能力（最小化、安全模型等）

专家实施和运营

- 技术和情报国内外同步
- 方案最佳实践
- 设备可信、可靠

行为安全性——基本概念

什么是行为安全性？

- 系统内部发起的行为是否具有安全隐患；
- 系统外部发起的行为是否具有安全威胁。

工控网络对行为安全性问题的处理的特殊性

- 强调减少误报：“误报等同于攻击”；
- 有一定的入侵容忍度；
- 强调白名单；
- 更重视全网的行为安全性。

匡恩网络

行为安全性：两个特质

智慧性

- 一个优势：自学习（匡恩人工智能的机器学习）
- 两个结果：用于提效减误（即人为经验）、用于决策

多样性

- 协议/流量
- 用户
- 源地址/目的地址
- 内容
- 操作动作
- 行为特征（正常、异常）

基因安全性——基本概念

什么是基因安全性？

- 既是特性，在整个生命发展周期中必须存在
- 也是原则，在整个生命迭代过程中必须遵守

- 硬件可信
- 操作系统可信
- 协议可信

- 排除恶意代码执行、植入的可能性

时间持续性——基本概念

时间持续性的内涵

- 不是一个时间点的安全，而是长期的持续的安全（运维安全）；
- 单点故障成本高，所以时间持续性要求高；
- 我们提供的解决方案，要成为系统可靠性的一部分；

涉及技术内容

- 安全咨询、安全培训、威胁评估产品、检查工具、漏洞库更新、规则库更新等。

匡恩网络

时间持续性——兼顾内外环境、实现联合防治

外界时间

- 7X24小时
- 攻击类型：有新有旧
- 攻击强度：有强有弱
- 攻击技术：有高有底
- 攻击量级：有大有小

内部时间

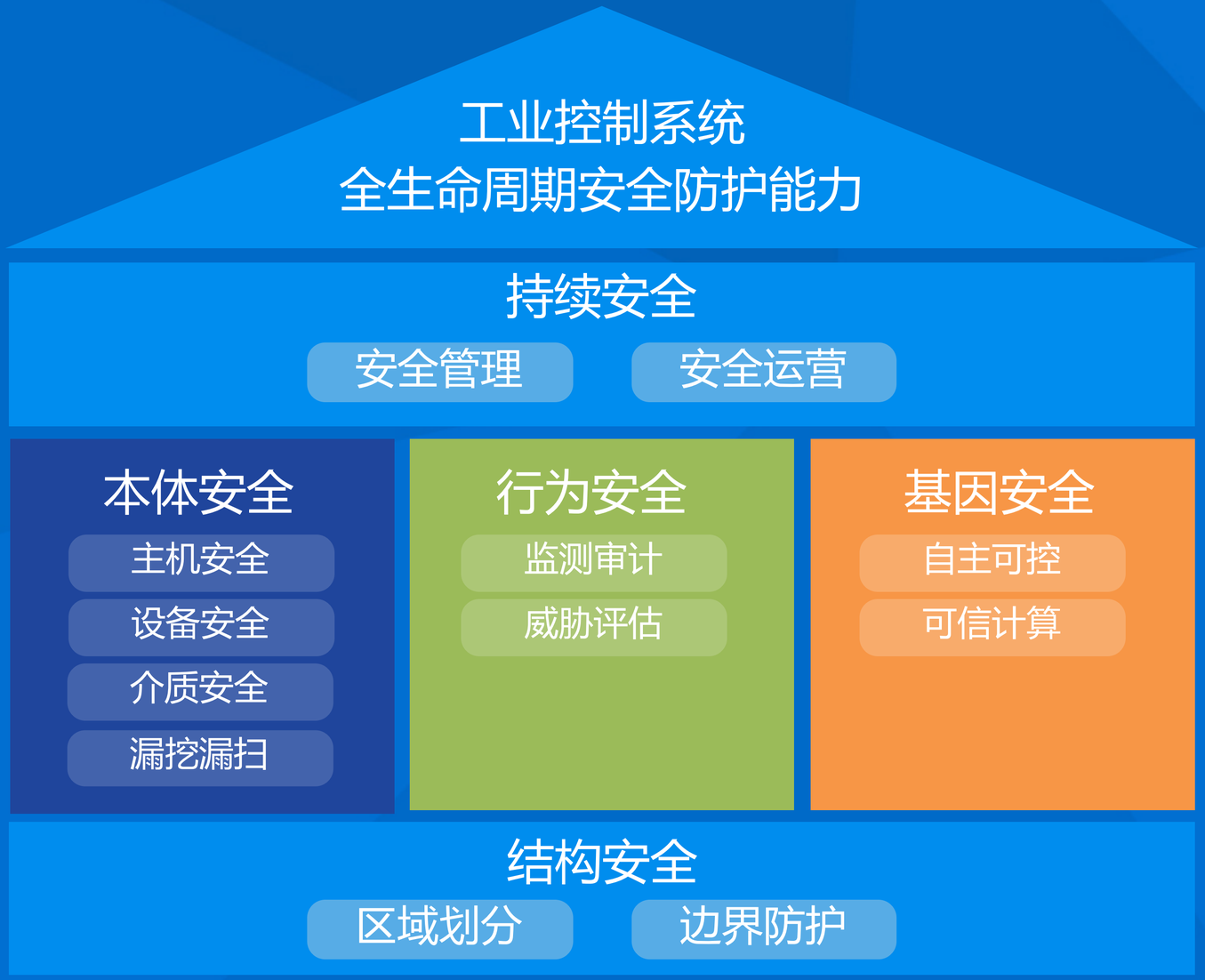
- 永续经营
- 网络、设备的变更：上线、下线、用途调整、归属调整
- 人员的变更

持续性

- 在可预见的时间内，持续不断地建设、调整和优化四个安全性，形成一个有机结合、动态适应、全面协同的安全生态环境。

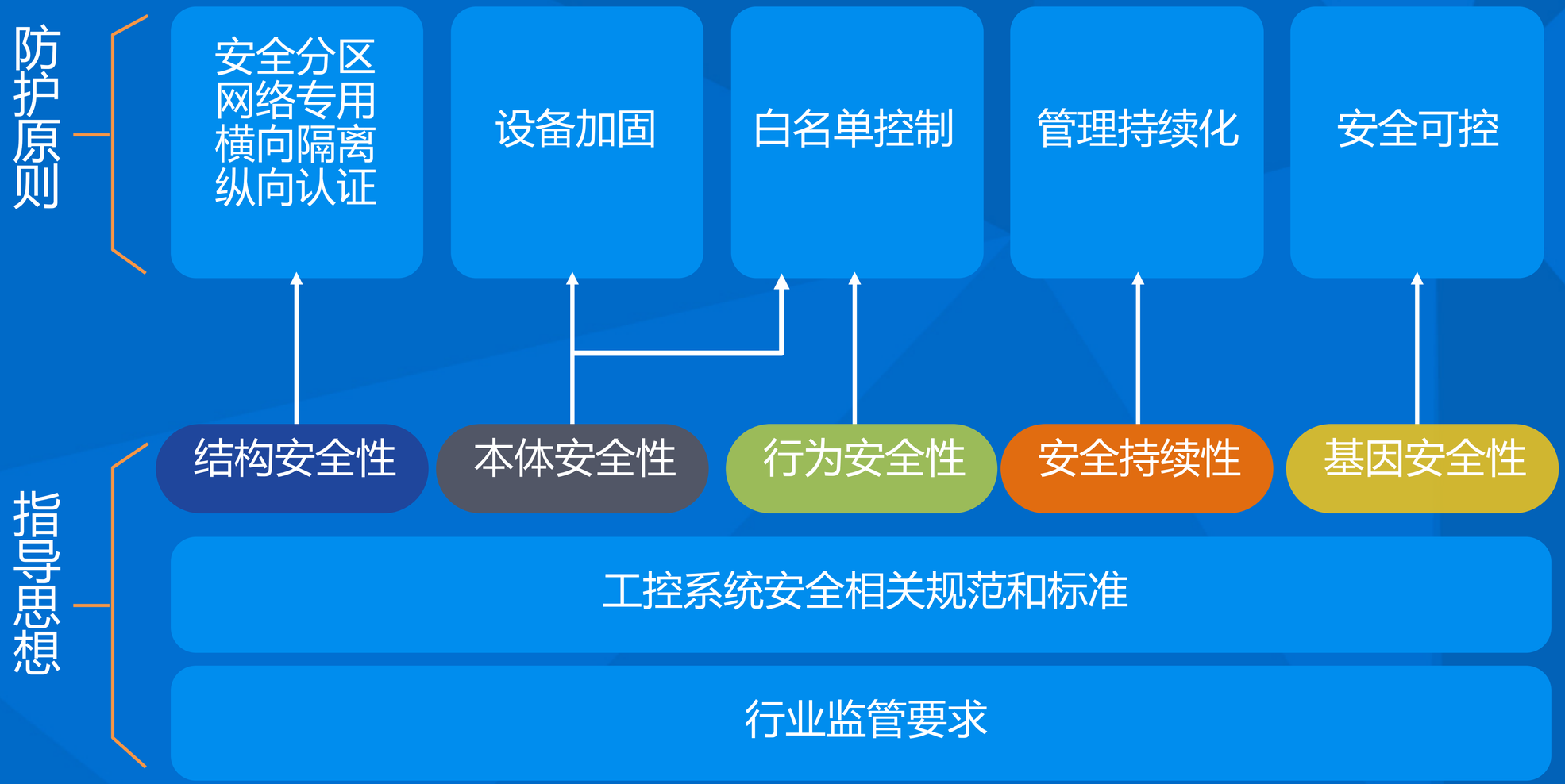
匡恩网络

解决方案整体设计



匡恩网络

解决方案对应关系



综述

结构安全性

结构安全了就解决了大部分问题。

本体安全性

- 针对工控系统的攻击，如果不能到本体安全性的层次，那它所能造成的威胁是非常有限的。

行为安全性

- 所有可能带来威胁的网络行为，最终一定要落实到某个本体上才能产生实质性后果。合理的结构和补偿性措施都是为了遏制不安全的行为。

基因安全性

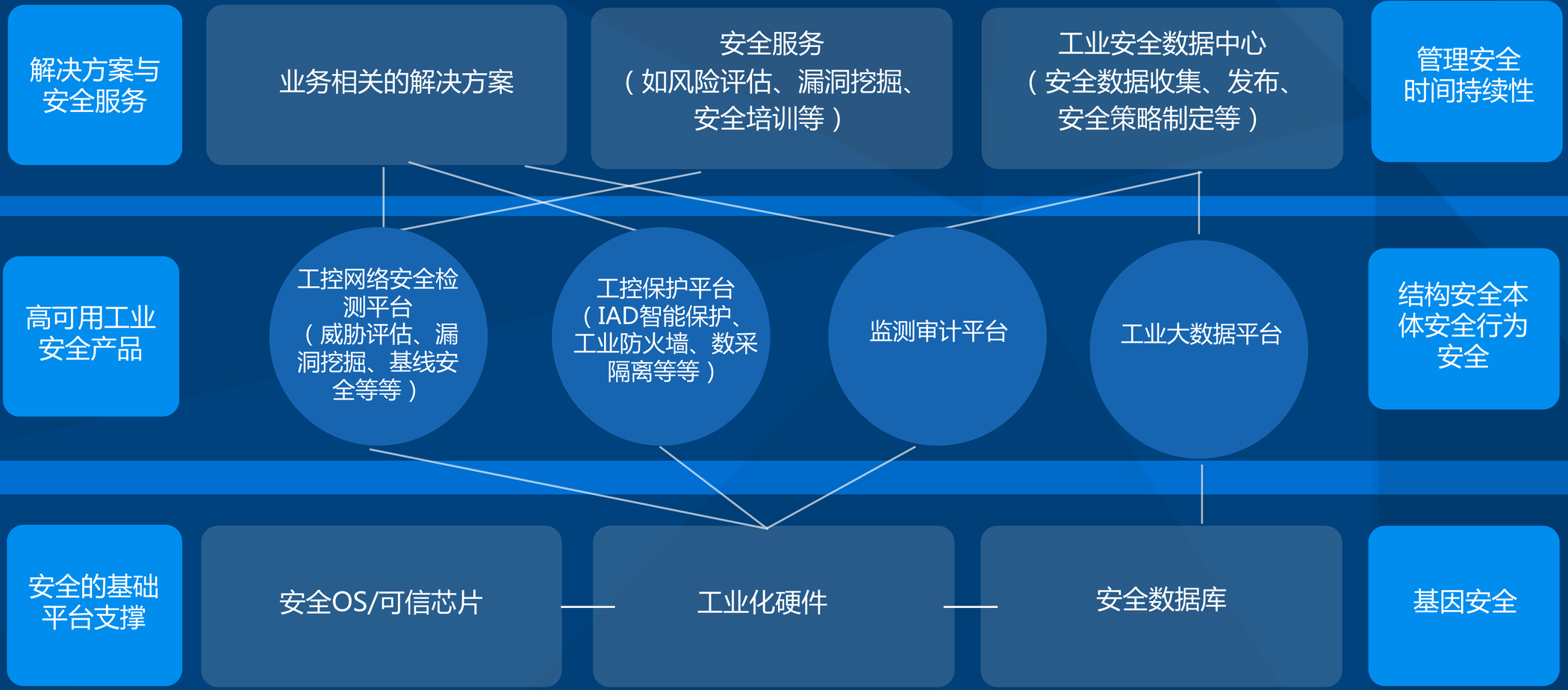
- 将本体安全性持续保持在高水平

时间持续性

- 在可预见的时间内，持续不断地建设和优化四个安全性，形成一个有机结合、动态适应、全面协同的安全生态环境。

匡恩网络

匡恩网络产品与解决方案



谢谢！

匡恩网络

北京匡恩网络科技有限责任公司

电话: (010) 5670-5608　　传真: (010) 59512799
地址：北京市海淀区知春路7号致真大厦D座13层
官网：www.kuangn.com