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

工业互联网安全框架（2018）

主讲人：田慧蓉

创新引领 融通发展

2018 工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2018

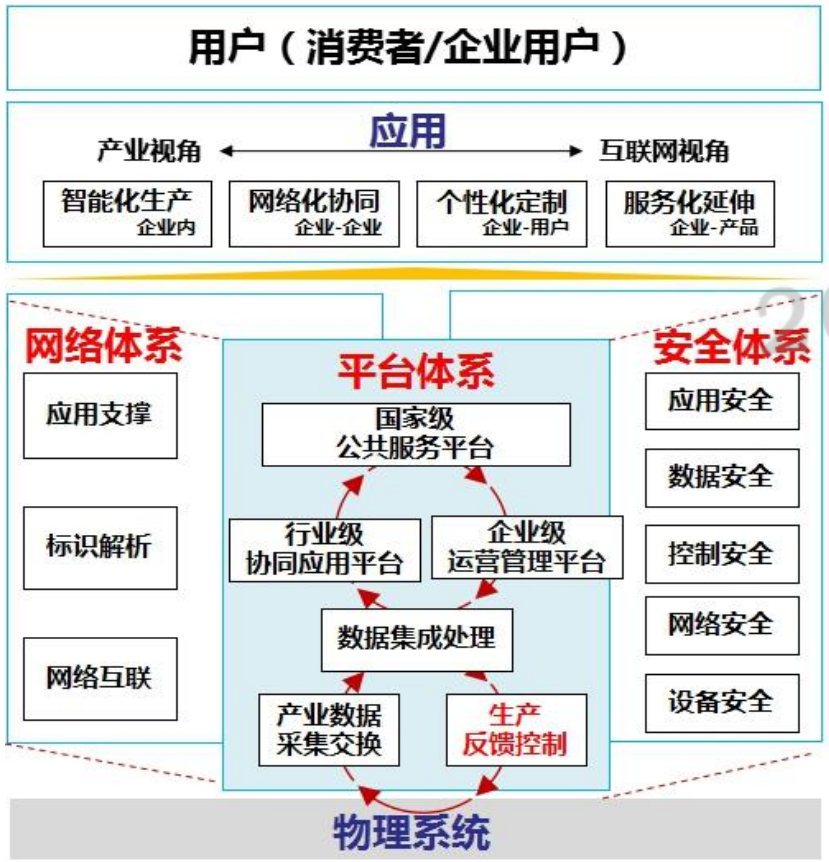
联合发布单位

- 中国信息通信研究院
- 北京奇虎科技有限公司
- 中国电子信息产业集团有限公司第六研究所
- 北京神州绿盟信息安全科技股份有限公司
- 中国移动通信集团公司
- 华为技术有限公司
- 富士康科技集团
- 北京匡恩网络科技有限责任公司
- 中国科学院沈阳自动化研究所
- 中国电信集团有限公司
- 思科系统（中国）网络技术有限公司
- 杭州安恒信息技术有限公司
- 大唐高鸿数据网络技术股份有限公司
- 北京安点科技有限责任公司

目录
Contents

（一）工业互联网发展具有重大意义

工业互联网是满足工业智能化发展需求，具有低时延、高可靠、广覆盖特点的关键网络基础设施，是新一代信息通信技术与先进制造业深度融合所形成的新兴业态与应用模式。



工业互联网深刻变革传统工业的创新、生产、管理、服务方式，催生新技术、新模式、新业态、新产业

繁荣数字经济	创新网络国际治理	统筹两个强国建设
新基石	新途径	新引擎

（二）工业互联网的三大体系

网络体系是基础

将连接对象延伸到工业全系统、全产业链、全价值链：

- 全要素：人、物品、机器、车间、企业等
- 各环节：设计、研发、生产、管理、服务
- 实现泛在深度互联

平台体系是核心

工业智能化发展的核心载体：

- 海量数据汇聚与建模分析
- 制造能力标准化与服务化
- 工业知识软件化与模块化
- 各类创新应用开发与运行
- 支撑生产智能决策、业务模式创新、资源优化配置、产业生态培育

安全体系是保障

工业智能化的安全可信环境：

- 建设满足工业需求的安全技术和管理体系
- 增强设备、网络、控制、应用和数据的安全保障能力
- 识别和抵御安全威胁
- 化解各种安全风险

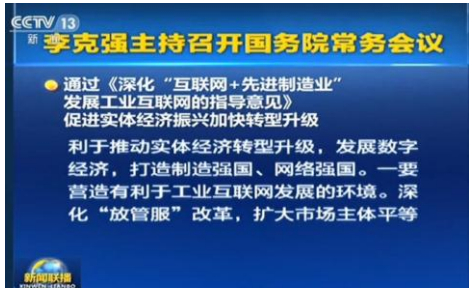
（三）国家高度重视工业互联网发展，安全成为工业互联网关键要素

十九大报告

- ✓ 加快建设制造强国，加快发展先进制造业，推动互联网、大数据、人工智能和实体经济深度融合
- ✓ 推动新型工业化、信息化、城镇化、农业现代化同步发展

《深化“互联网+先进制造业”发展工业互联网的指导意见》

- ✓ 促进实体经济振兴、加快转型升级
- ✓ 引导企业**提高网络安全防护能力**…围绕汽车、电子、能源、航空航天等重点制造领域**建设网络和平台安全保障管理与技术体系**



● 苗圩部长解读十九大报告

- ✓ 实施工业互联网创新发展战略，加快构建新一代信息基础设施，打造网络、平台、**安全**三大体系，抢占数字经济发展主动权和话语权

● 苗部长部署2018年工业和信息化工作

- ✓ 深入实施工业互联网创新发展战略，开展工业互联网发展“323”行动，实施工业互联网三年行动计划…**实施工业互联网安全防护提升工程**

（四）工业互联网安全框架的重要性

联盟已发布的《工业互联网体系架构（版本1.0）》

工业互联网安全体系

设备　　控制　　应用　　网络　　数据

明确5大安全防护对象

工业互联网安全框架

内容聚焦**网络安全**，主要解决工业互联网面临的网络攻击等**新型风险**，同时**考虑与功能安全和物理安全的关系**

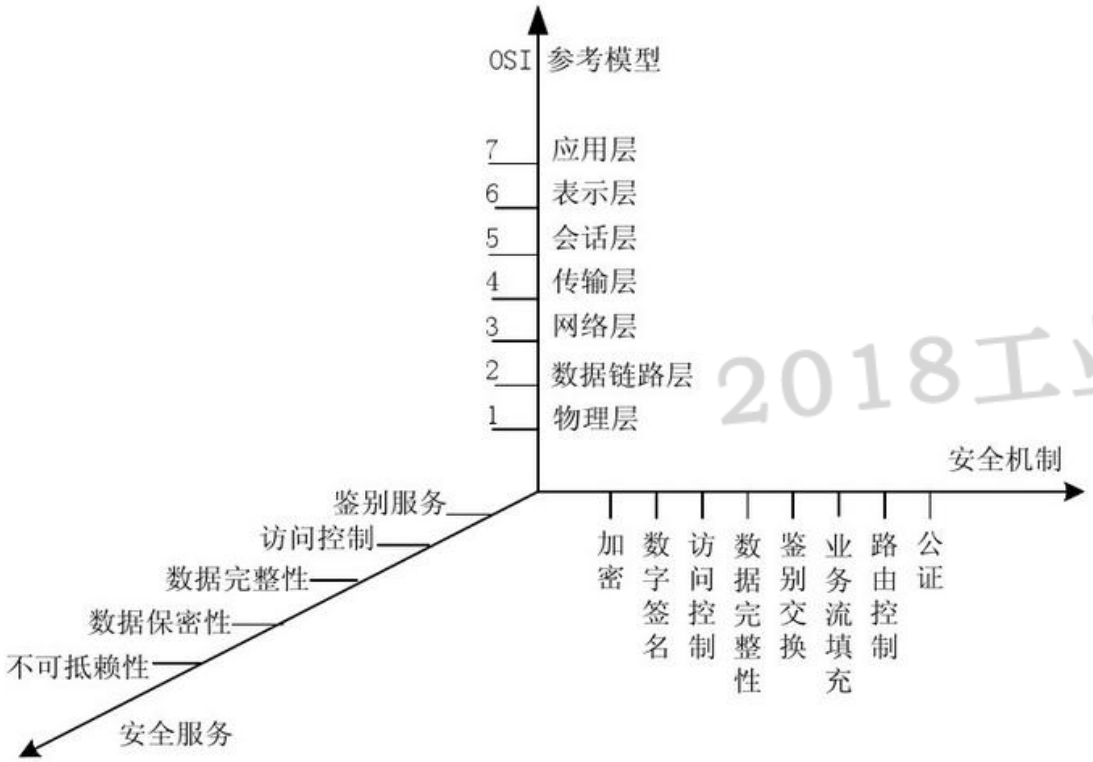
指导工业互联网相关企业部署安全措施

提升安全能力

目录
Contents

（一）传统网络安全框架分析——OSI安全体系结构

OSI安全体系结构定义了5大类安全服务和8类安全机制，可根据具体系统适当地配置于OSI模型的七层协议中。



■ **突出特点：**采用了**分层**的思想，层与层间相互独立，具有很好的**灵活性**。

■ **局限性：**只专注于网络通信系统和静态防护技术，**对于持续变化的内外部安全威胁缺乏足够的监测与应对能力**，因而**无法满足更复杂更全面的信息保障的要求**。

（一）传统网络安全框架分析——P2DR模型

P2DR模型引入动态安全的理念，将网络安全的实施分为防护、检测和响应三个阶段。在整体安全策略的指导下部署安全防护措施。

防护Protection
部署防护手段阻止安全威胁

响应Response
发现并及时截断可疑数据并启动相关报警信息

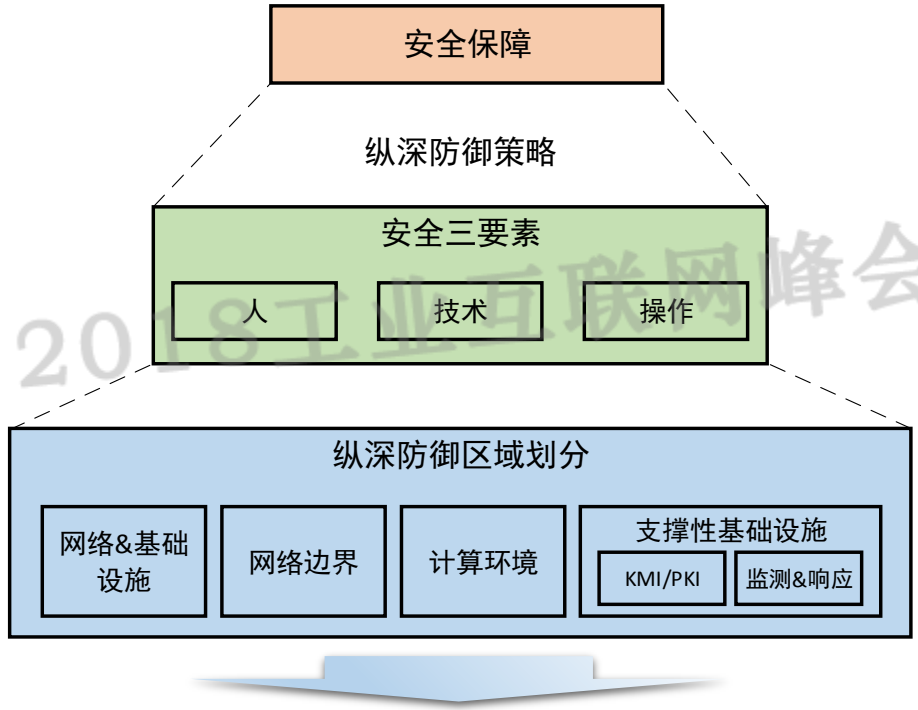
检测Detection
对网络进行实时监测和定期检查，建立完善的审计系统

■ **突出特点：**基于**闭环控制**的**动态安全模型**。适用于需要长期持续安全防护的系统。

■ **局限性：**局限于从技术上考虑网络的安全问题，**忽视了管理对于安全防护的重要性**。

（一）传统网络安全框架分析——IATF

IATF提出保障信息系统安全应具备的三个核心要素：即人、技术和操作。同时，将网络系统的安全防护分为网络和基础设施防御、网络边界防御、计算环境防御和支撑性基础设施防御四部分。



- **突出特点**：通过对四个部分分别部署安全保障机制，形成对网络系统的**纵深防御**，最大限度降低安全风险，从而保障系统的安全性。
- **局限性**：实现的都是对网络系统的静态安全防护，**并未对网络系统部署动态持续的安全防护措施**。

（一）传统安全框架分析——IEC62443

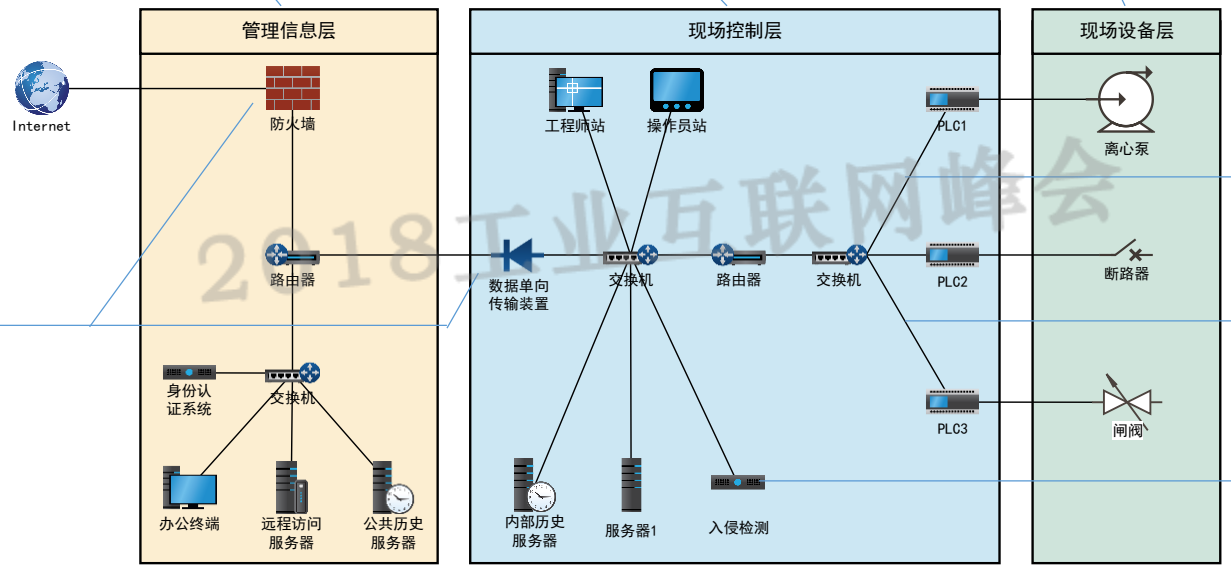
IEC62443将工业控制系统按照控制和管理的等级划分成相对封闭的区域，区域之间的数据通讯通过管道进行，通过在管道上安装信息安全管理设备来实现分级保护，进而实现控制网络的纵深防御。

区域划分

按照业务不同划分安全区域

边界隔离

加入防火墙、单向传输等装置实现对网络边界的隔离防护



链路防护

构建VPN等安全传输通道，实现对链路传输数据的安全防护

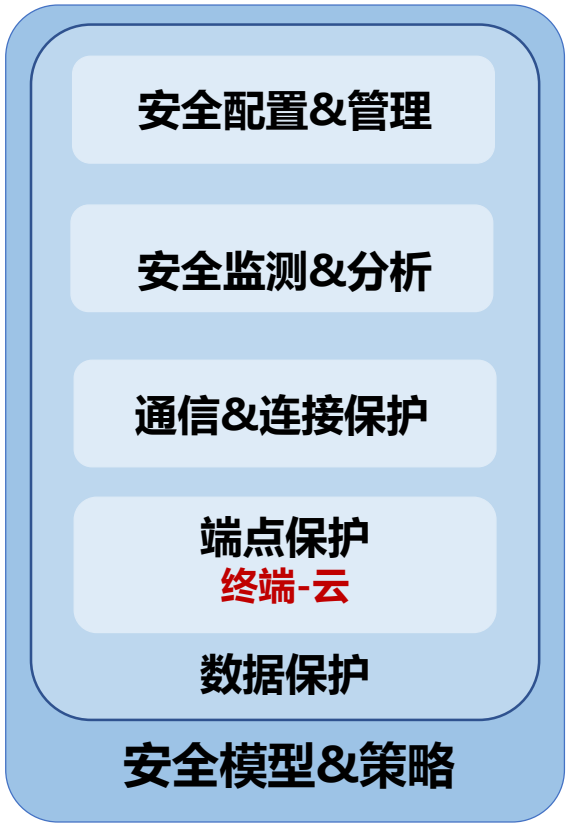
通信管控

基于协议深度解析，实现对通信内容的全面管控

- **突出特点**：采用**纵深防御**的安全防护策略，将**技术与管理有机结合**。
- **局限性**：实现的是静态安全防护，没有考虑动态安全防护的思路。

（二）美国IIC工业互联网安全框架分析

美国IISF从实施视角出发，以安全模型和策略作为总体指导，部署通信、端点、数据、配置管理、监测分析等方面的安全措施。



- **安全模型&策略**

数据保护安全策略 终端安全策略 安全策略通信&连通性 安全策略监测&分析 ...

- **安全配置&管理**

终端识别管理 终端配置&管理 终端监测&分析 通信配置&管理 ...

- **安全监测&分析**

数据保护的监测&分析 监测的安全模型&策略 ...

- **通信&连接保护**

网络配置&管理 网络监测&分析 通信终端保护 连通性的物理安全 ...

- **端点保护**

终端标识 终端信任根 终端物理安全 终端数据保护 ...

- **数据保护**

静态数据 动态数据 使用数据 ...

突出特点：美国IISF**聚焦于IT安全，侧重于安全实施，明确了具体的安全措施。**

（二）德国工业4.0架构中的安全

德国工业4.0并未专门针对安全提出相应的安全架构。安全作为新的商业模式的推动者，在RAMI 4.0中起到了承载和连接所有结构元素的骨架的作用。

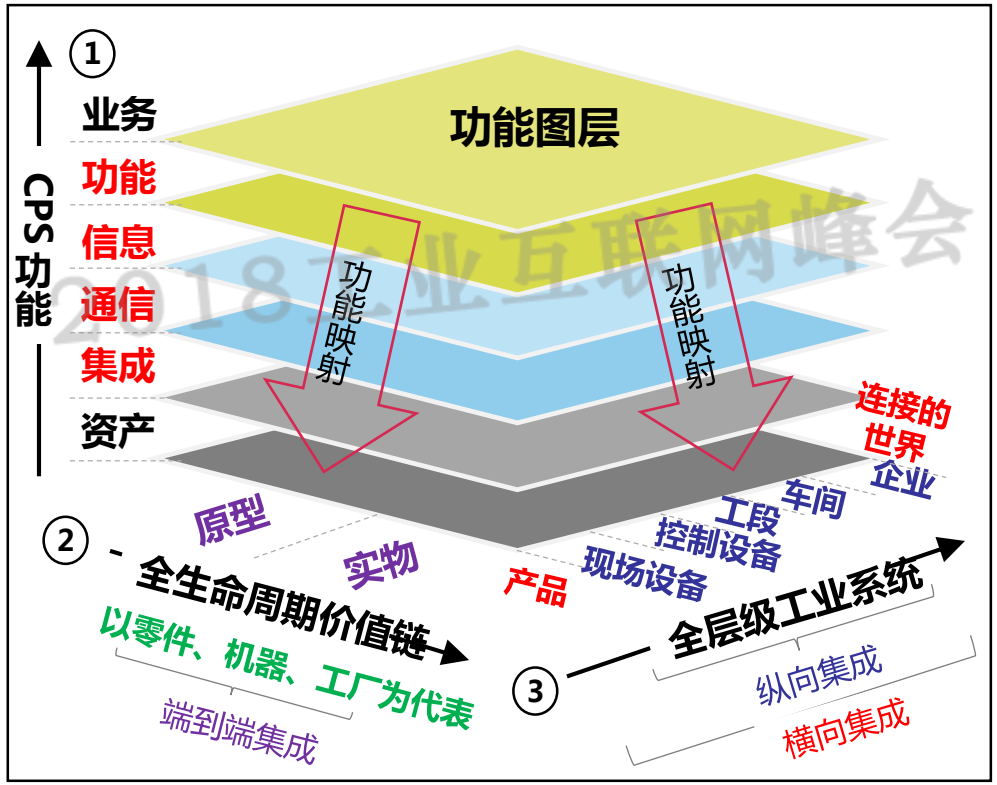
工业4.0参考架构（RAMI 4.0）

1、CPS功能视角

安全应用于**所有不同层次，**安全风险必须做整体考虑。

2、价值链视角

对象的所有者必须考虑其整个**生命周期的安全性。**



3、工业系统视角

所有对象/资产需要**安全方面的考虑**（风险分析），并需要对象/资产所有者提供其对象/资产相关的**安全特性，**来对其实时保护措施。

突出特点：德国RAMI 4.0采用了**分层**的基本安全管理思路，**侧重于防护对象的管理。**

（三）共性分析及经验借鉴

1 分类别部署安全防护措施

根据安全需求确定具体分类标准：

✓安全防护对象（OSI安全体系结构，美国IIC工业互联网安全框架，德国工业4.0安全框架）；

✓安全防护流程（P2DR模型）；

✓安全区域（IATF、IEC62443）；

2 动态安全模型成为主流

相对安全观已成为共识，为应对不断变化的安全风险，工业互联网安全框架应是动态的、持续的：

✓P2DR模型，美国IIC工业互联网安全框架，德国工业4.0架构中的安全

3 “技术手段+管理手段“相结合

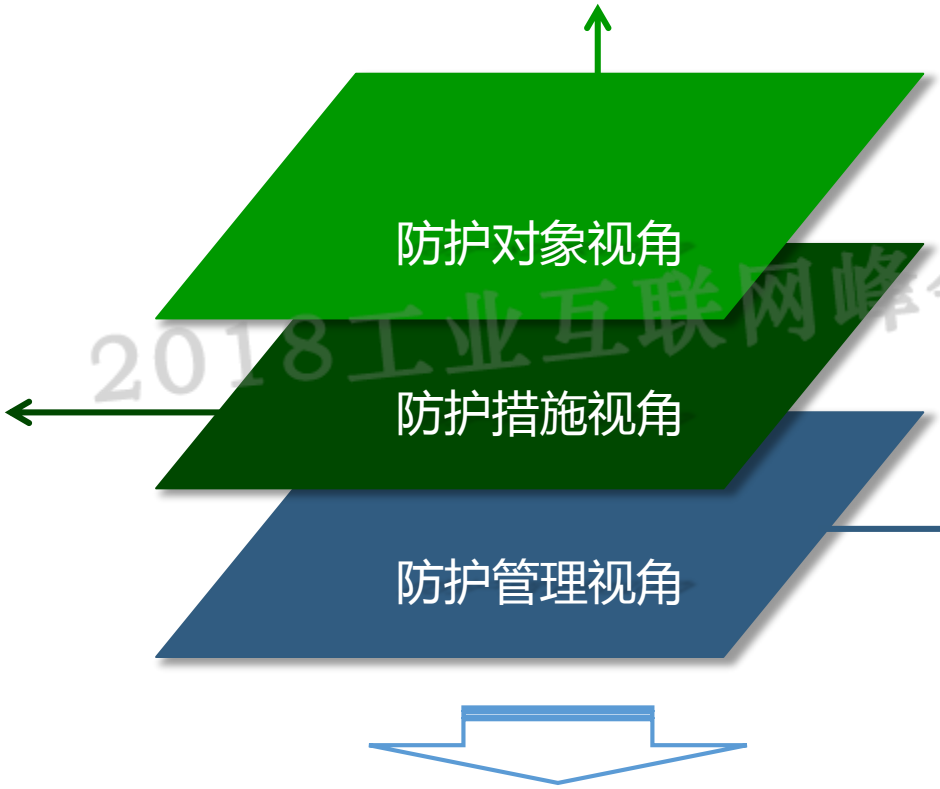
在安全模型中融入完善的安全管理机制能够更好的发挥模型的安全保障能力：

✓IATF、IEC62443、美国IIC工业互联网安全框架

目录
Contents

（一）工业互联网安全框架设计思路

防护对象视角：明确安全防护对象是前提。



防护措施视角：部署安全防护措施是关键。

防护管理视角：落实安全防护管理是重要保障。

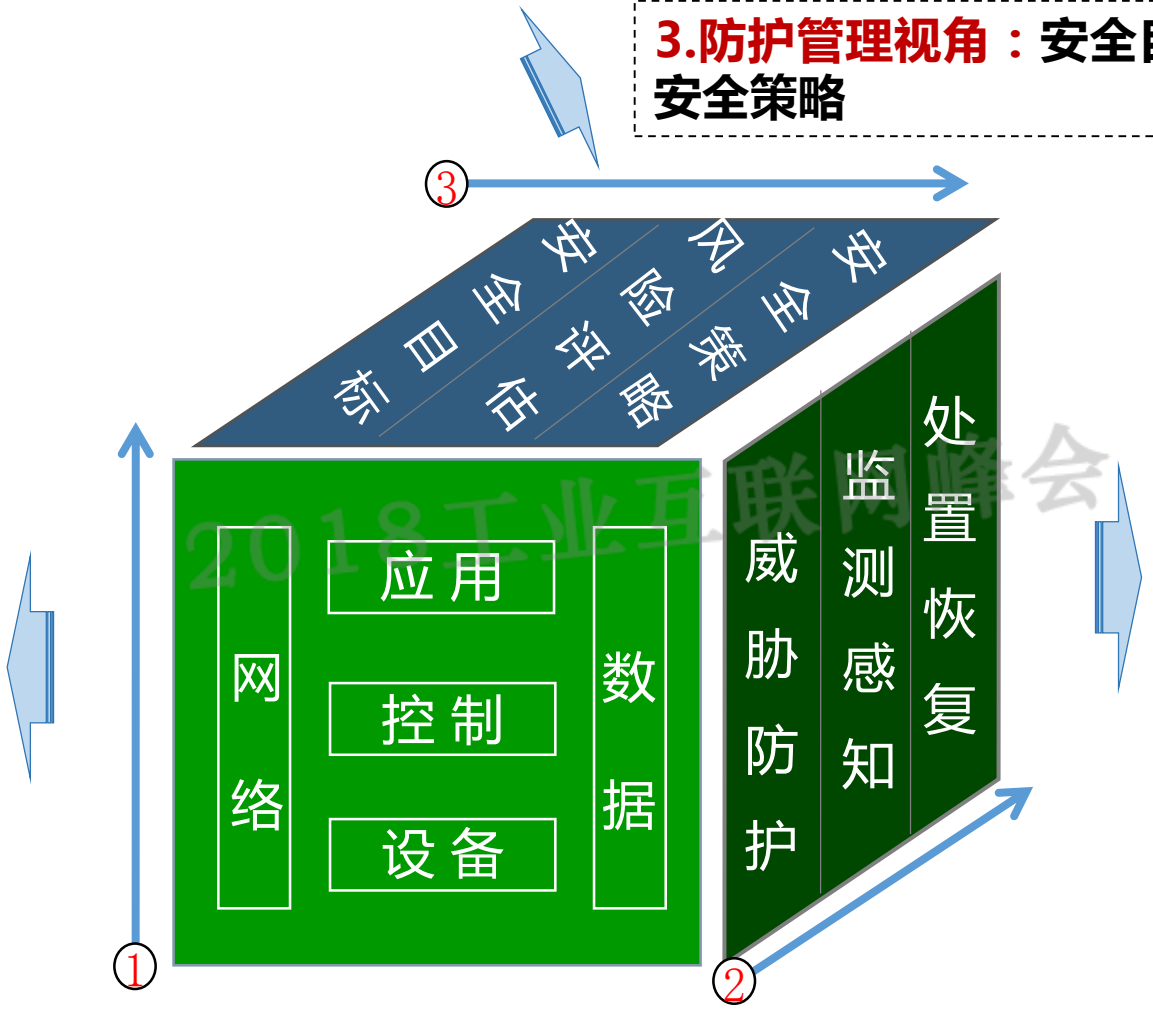
需从**防护对象视角、防护措施视角**及**防护管理视角**三大视角出发构建工业互联网安全框架，引导企业全面部署安全防护措施。

（二）从三个视角构建工业互联网安全框架

3.防护管理视角：安全目标、风险评估、安全策略

1.防护对象视角：

- ✓设备
- ✓控制
- ✓网络
- ✓应用
- ✓数据

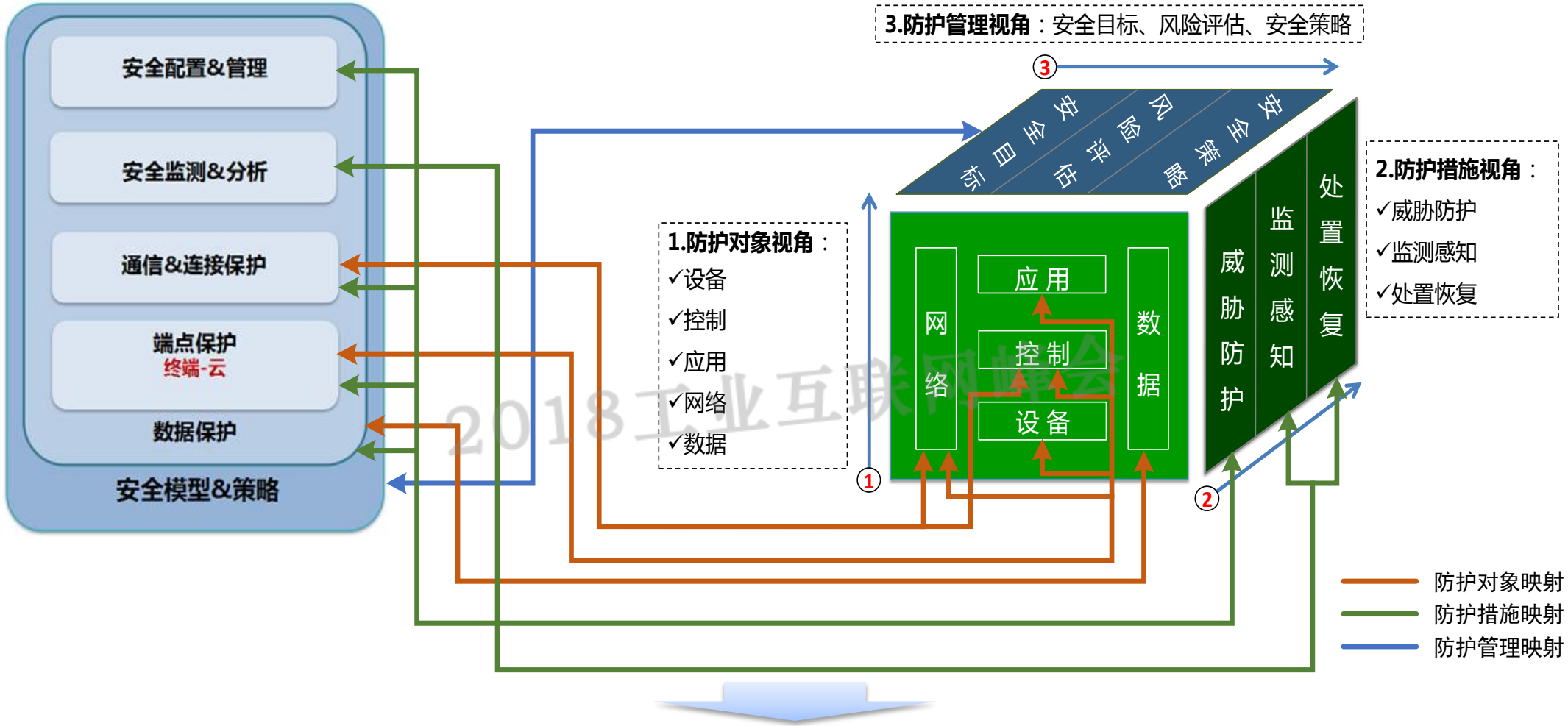


2.防护措施视角：

- ✓威胁防护
- ✓监测感知
- ✓处置恢复

工业互联网安全框架的三个防护视角之间相对独立，又相辅相成、互为补充，形成一个完整、动态、持续的防护体系。

（三）中美工业互联网安全框架对比分析



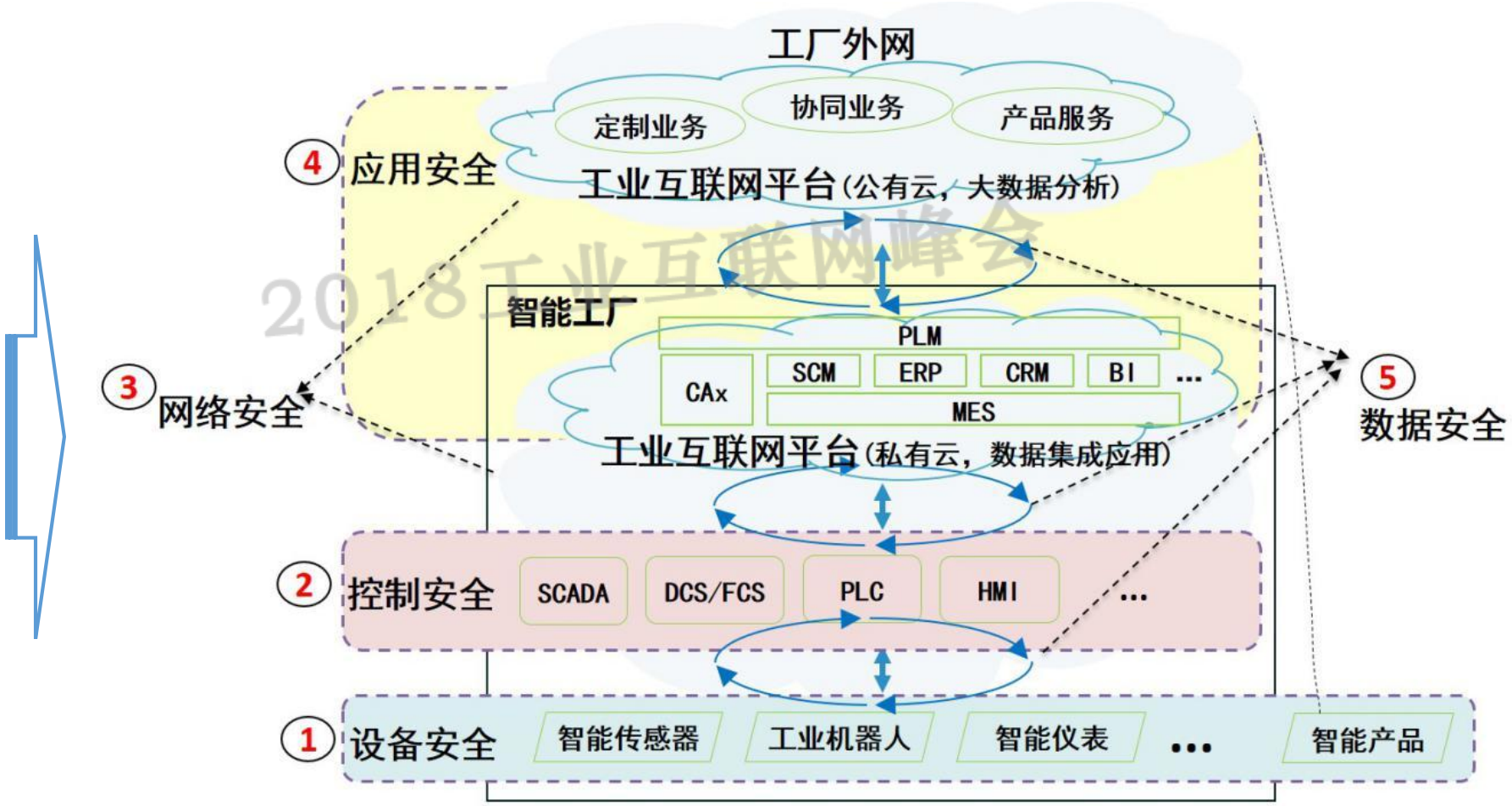
中美工业互联网安全框架虽呈现视角有不同，但两者设计思路趋于一致，在防护内容上也具有一致的对应关系。均从指导企业部署工业互联网安全实施角度出发，强调技管结合、动静互补，全面持续提升工业互联网安全防护能力。

（四）工业互联网安全框架分析—防护对象视角

中国工业互联网产业联盟（AII）发布《工业互联网体系架构（版本1.0）》，提出工业互联网安全体系架构，聚焦设备、控制、网络、应用、数据五大安全重点。

安全防护对象

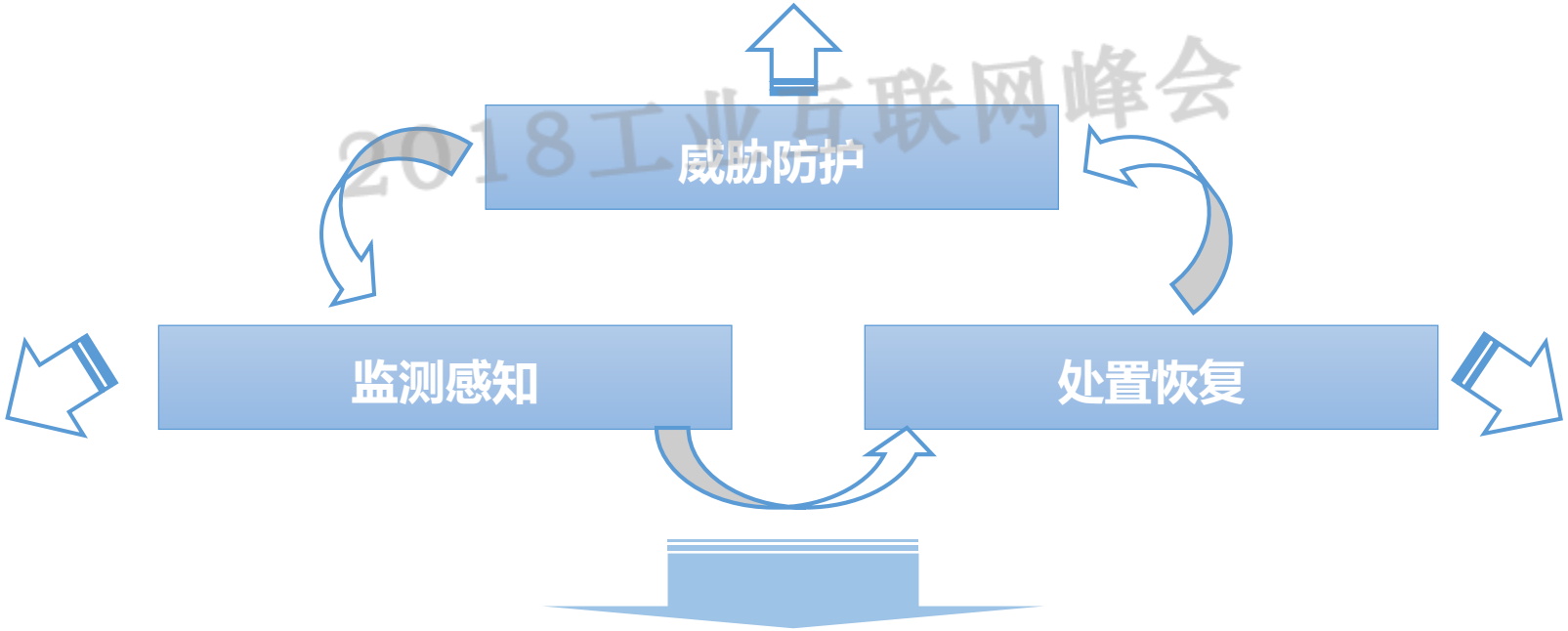
1. 设备安全
2. 控制安全
3. 网络安全
4. 应用安全
5. 数据安全



（五）工业互联网安全框架分析—防护措施视角

为应对工业互联网所面临的各种安全威胁，主要从**威胁防护、监测感知和处置恢复三大环节**构建防护措施视角。

针对五大防护对象，部署主被动防护措施，阻止外部入侵，构建安全运行环境，消减潜在安全风险。



部署相应的监测措施，实时感知内部、外部的安全风险。

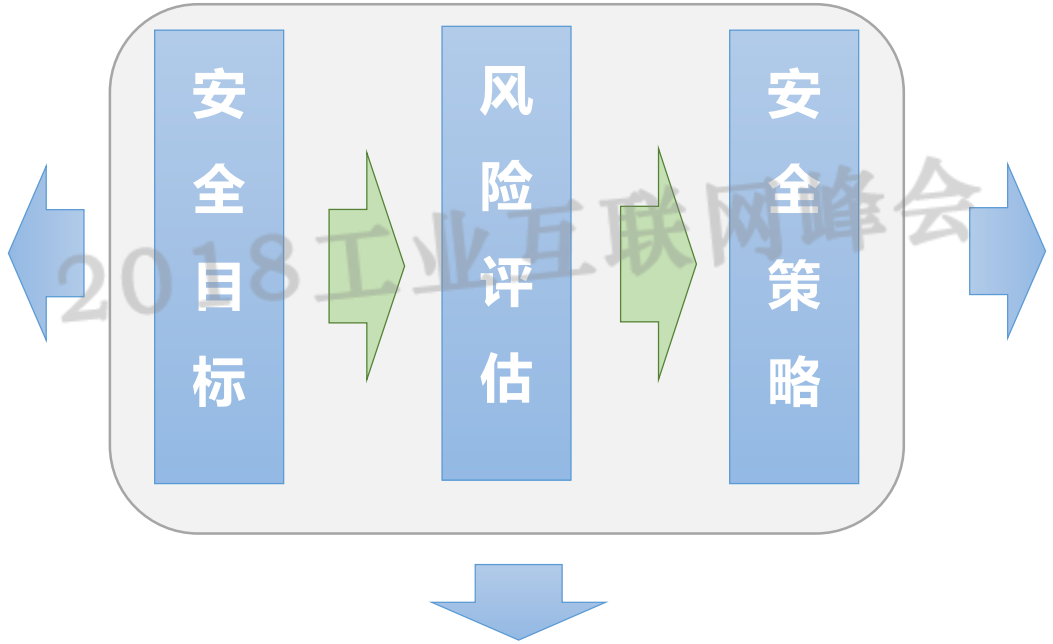
建立响应恢复机制，及时应对安全威胁，并及时优化防护措施，形成闭环防御。

防护措施视角从**生命周期、防御递进角度**明确安全措施，从而实现**动态、高效的防御和响应**。

（六）工业互联网安全框架分析—防护管理视角

防护管理视角的设立，旨在**指导企业构建持续改进的安全防护管理方针**，在明确防护对象及其所需要达到的**安全目标**后，对于其可能面临的**安全风险进行评估**，找出当前与安全目标之间存在的差距，制定相应的**安全防护策略**，提升安全防护能力，并在此过程中不断对管理流程进行改进。

- 保密性
- 完整性
- 可用性
- 可靠性
- 弹性
- 隐私安全



从工业互联网总体安全考虑，定义保证工业互联网正常运行的指导方针及安全模型，结合安全目标以及风险评估结果，明确当前工业互联网各方面的安全策略，并不断进行完善。

分析工业互联网系统的资产、脆弱性和威胁，明确风险处置措施，确保工业互联网数据安全性、设备接入安全性、平台安全性等，并最终形成风险评估报告。

目录
Contents

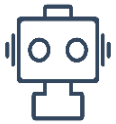
（一）工业互联网安全防护措施实施—设备安全

工业互联网安全框架实施过程中的重点包括：针对工业互联网五大安全防护对象面临的安全风险采取的相应安全防护措施，以及贯穿工业互联网全系统的监测感知与处置恢复两大类防护措施。

设备变化

机械化 → 高度智能化

嵌入式操作系统
+
微处理器
+
应用软件

智能机器

安全风险分析

- **攻击直达设备**

控制系统→智能设备

- **攻击范围扩大**
- **扩散速度增加**
- **漏洞影响扩大**

特定型号设备→海量通用设备

设备安全防护措施

操作系统/应用软件安全

- 固件安全增强
- 漏洞修复加固
- 补丁升级管理

硬件安全

- 硬件安全增强
- 运维管控

（二）工业互联网安全防护措施实施—控制安全

控制变化

分层封闭局部 → 扁平开放全局

控制环境：

IT与OT融合

封闭到开放

工厂控制：

局部到全局

控制监测上移

实时控制下移

安全风险分析

➢攻击从IT层渗透到OT层

OT层环境：可信→不可信

➢攻击从工厂外渗透到工厂内

工厂内环境：封闭→开放

➢攻击难度大大降低

IT和OT隔离（OT环境可信）

控制协议、软件安全机制缺失

↓

IT和OT融合（OT环境不可信）

控制协议、软件脆弱性暴露

➢信息安全与功能安全问题交织

信息安全问题→功能安全失效

信息安全防护→功能安全能力下降

控制安全防护措施

控制协议安全

- 身份认证
- 访问控制
- 传输加密
- 健壮性测试

控制软件安全

- 软件防篡改
- 认证授权
- 恶意软件防护
- 补丁升级更新
- 漏洞修复加固
- 协议过滤
- 安全监测审计

控制功能安全

- 物理安全环境防护
- 兼容性验证
- 工艺流程安全防护
- 提升人员安全意识
- ……

（三）工业互联网安全防护措施实施—应用安全

应用变化

设计协同
+
供应链协同
+
制造协同
+
服务协同
+
用户全流程参与
+
产品服务延伸

安全风险分析

➢安全保护需求不同

不同业务平面有不同的服务安全需求

Eg. 航天二院导弹协同设计 VS 潍柴动力全球协同设计

➢网络安全隔离能力要求高

支持百万级VPN隔离及用户量增长

➢业务应用安全保障能力要求高

百级业务平面安全服务保障

应用安全防护措施

平台安全

安全审计　认证授权　DDOS防护
安全隔离　安全监测　补丁升级
……

工业应用程序安全

代码审计　人员培训　漏洞发现
审核测试　行为监测和异常阻止
……

（四）工业互联网安全防护措施实施—网络安全

网络变化

异构刚性局部 → 统一灵活全局

工厂内网：

以太网IP化

无线化

灵活组网

全局组网

工厂外网：

IT与互联网融合

OT与互联网融合

企业专网与互联网融合产品服务与互联网融合

安全风险分析

- **攻击门槛降低**

专有协议→以太网/IP协议

- **易受DDOS攻击**

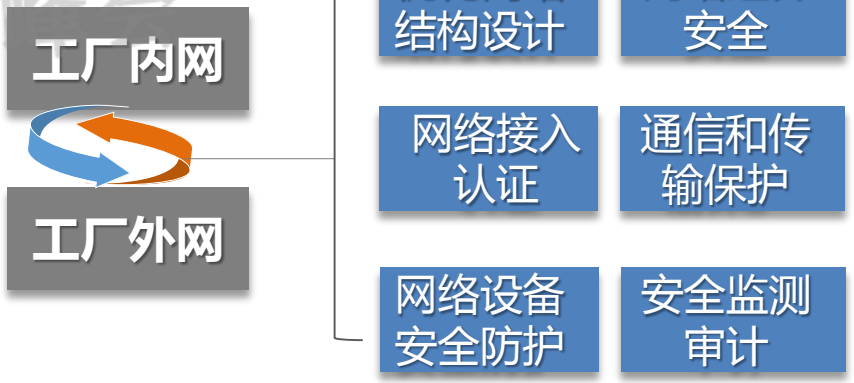
现有10M/100M工业以太网交换机性能低，难以抵抗广播风暴等DOS攻击

- **安全策略面临挑战**

静态→动态

- **无线网络风险**
- **5G/SDN等新技术风险**
- **工厂内外网互联互通风险**

网络安全防护措施



（五）工业互联网安全防护措施实施—数据安全

数据变化

少量 单一 单向 → 大量 多维 双向

体量大、种类多
+
结构复杂
+
IT和OT双向流动
+
厂内外双向流动

安全风险分析

➢数据泄露风险增大

生产数据从OT→IT，从厂内→厂外

➢数据保护难度增大

体量大、种类多、保护需求不同、流动方向和路径复杂

➢大数据分析催生价值保护需求

生产数据价值低→大数据分析产生价值（推断出工艺、导弹射程等敏感信息）

➢用户隐私数据泄露风险

工厂外个性化定制、服务化转型涉及大量用户隐私数据

数据安全防护措施

- 数据收集
- 数据传输
- 数据存储
- 数据处理

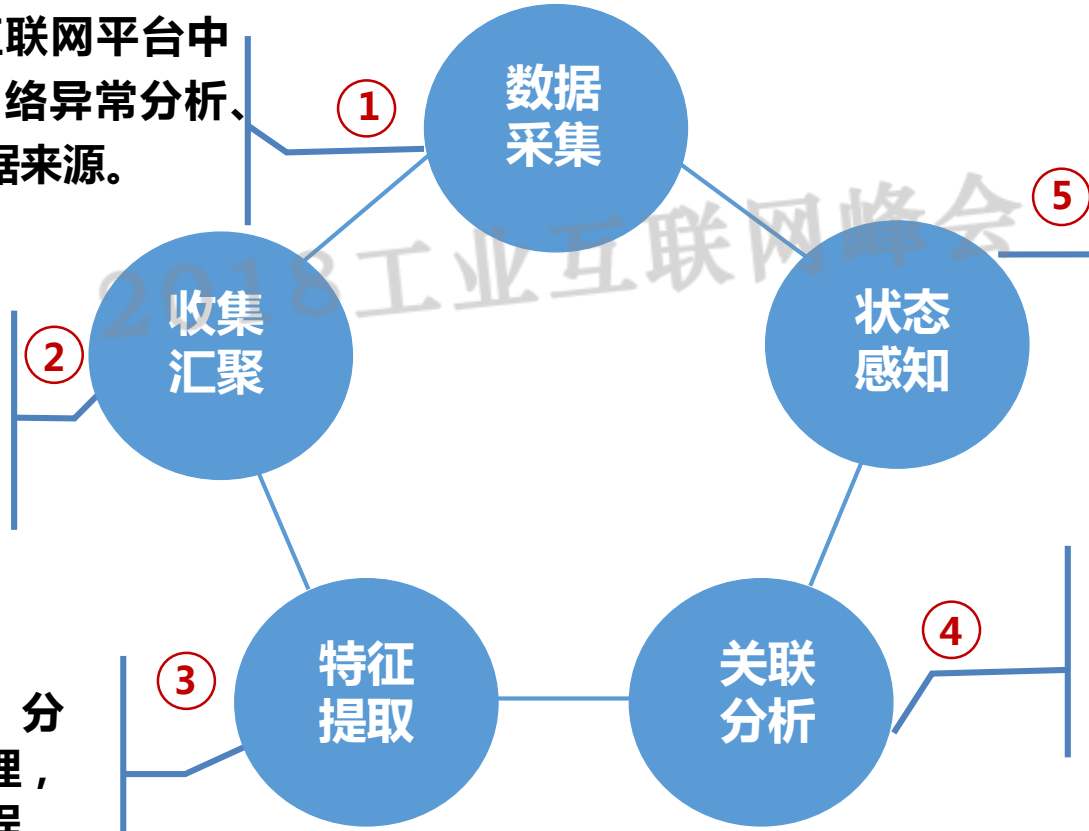
→

- 明示用途
- 数据加密
- 访问控制
- 业务隔离
- 接入认证
- 数据脱敏
- ……

（六）工业互联网安全防护措施实施—监测感知

监测感知是指部署相应的监测措施，主动发现来自系统内外部的安全风险，具体措施包括数据采集、收集汇聚、特征提取、关联分析、状态感知等。

- 对工业现场网络及工业互联网平台中各类数据进行采集，为网络异常分析、设备预测性维护等提供数据来源。



- 对工业控制系统及应用系统所产生的关键工业数据进行汇聚
- 对全网流量进行监听与存储

- 对数据特征进行提取、筛选、分类、优先级排序、可读等处理，实现从数据到信息的转化过程

- 基于关联分析过程，实现对企业工业互联网运行规律、异常情况、安全目标、安全态势、业务背景等的认知

- 将运行机理、运行环境、操作内容、外部威胁情报等有机结合，基于大数据进行横向大数据分析和多维分析，判断设备或网络的安全情况

（七）工业互联网安全防护措施实施—处置恢复

处置恢复机制是落实工业互联网信息安全管理，保障工业互联网系统与服务持续运行的有力保障。处置恢复机制主要包括响应决策、备份恢复、分析评估等。

处置恢复

响应决策

- 处置恢复组织架构
- 灾难风险分析与管理
- 灾难数据监测
- 灾难恢复决策
- 灾难恢复响应
- …

备份恢复

- 备份能力等级定义
- 备份能力需求确立
- 备份恢复策略制定
- 灾难备份中心建设、运行与维护管理
- 处置恢复预案演练与管理
- …

分析评估

- 风险分析
- 风险定义与预案制定
- 处置恢复效果评估
- 处置恢复方案改进
- …

目录
Contents

工业互联网安全框架将不断丰富和完善

工业互联网安全防护作为未来工业互联网发展的一个重点关注方面，要求工业互联网安全框架在工业互联网快速发展中不断更新与完善。未来工业互联网安全防护工作有以下几个方面值得关注：

1. 安全防护智能化将不断发展
2. 工业互联网平台安全地位日益凸显
3. 工业互联网大数据安全防护成为热点
4. 安全监测与威胁处置要求越发迫切
5. 安全信息共享和联动处置机制呼声日高

未来，需紧密结合工业互联网安全发展的五大趋势，重点聚焦防护措施视角和防护管理视角，不断进行丰富和完善。

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

THANKS

主讲人：田慧蓉

2018年2月2日