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

360 企业安全 安全第一

工业互联网安全体系建设与实践

主讲人：陶耀东 博士

AII安全组执行主席

360工业控制系统安全国家联合实验室 主任

创新引领 融通发展

2019 工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019

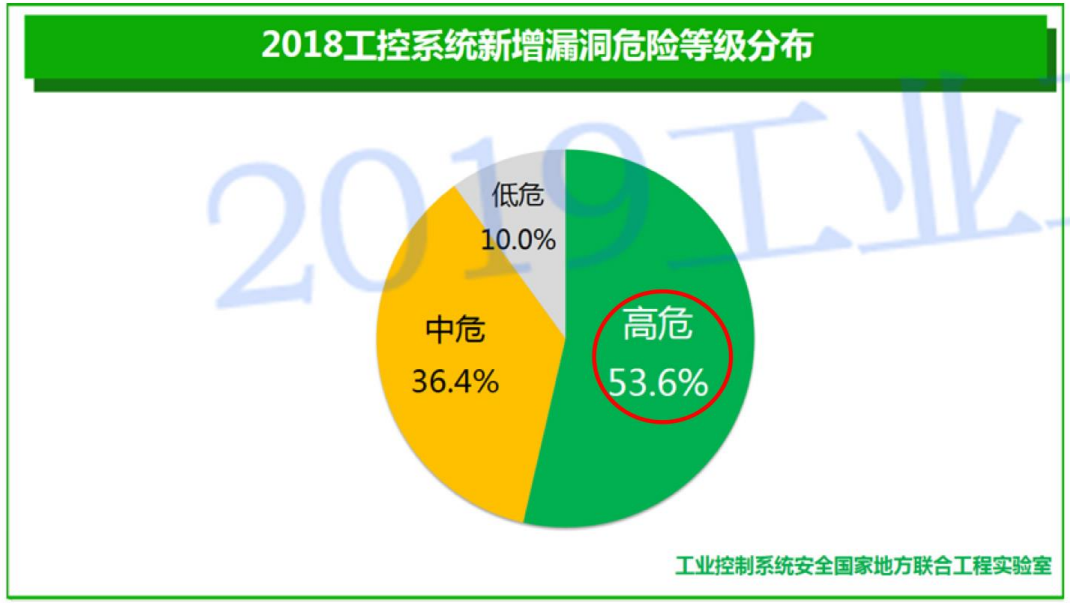
目录
Contents

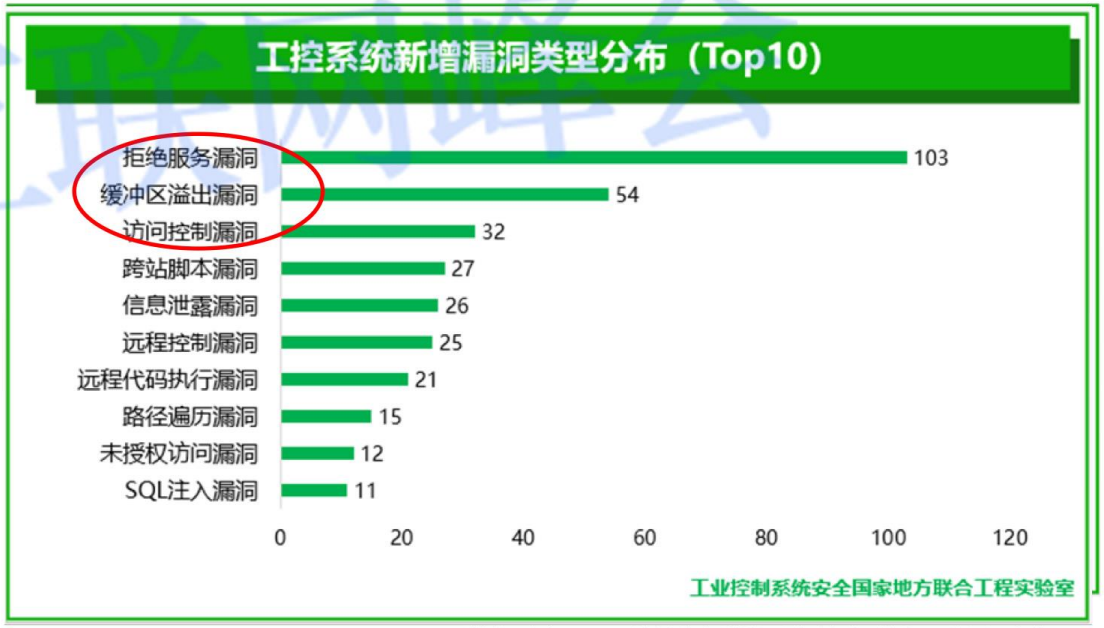
现状一：工业互联网安全风险突出

安全漏洞数量快速增长，高危漏洞呈高发态势，漏洞涉及行业广泛

2018年全年，CNVD新增工控漏洞达到442个，创历史新高。高危漏洞数量占比最高，达到53.6%

2018制造业漏洞占比达到30.6%
拒绝服务、缓冲区溢出、访问控制漏洞数量较多，



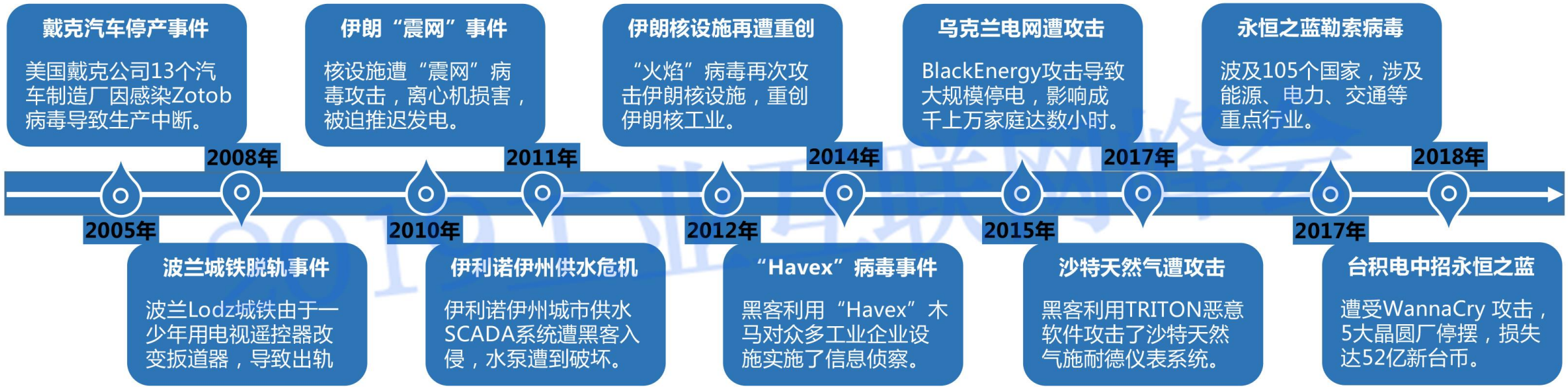


数据来源：工业控制系统国家地方联合工程实验室

工业互联网安全风险突出，整体形式严峻

2019工业互联网峰会

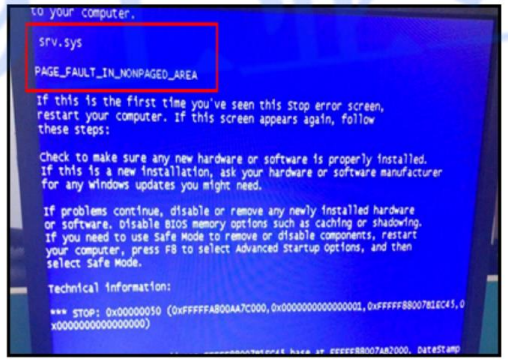
现状二：国内外工业互联网安全事件层出不穷



现状二：国内外工业互联网安全事件层出不穷

近几年360企业安全集团处理过的网络攻击事件，涉及汽车生产、智能制造、电子加工、烟草、电力、能源等

行业**几十余家企业**，大多数都导致了**工业主机蓝屏，文件加密，生产停工**



某汽车模具厂，停产 2017.05

某冷轧钢板厂，停产 2018.07

某炼钢厂，停产 2018.10

某关键IC厂，停产 2019.01

“永恒之蓝及挖矿变种”成为工业企业安全事件最主要原因之一

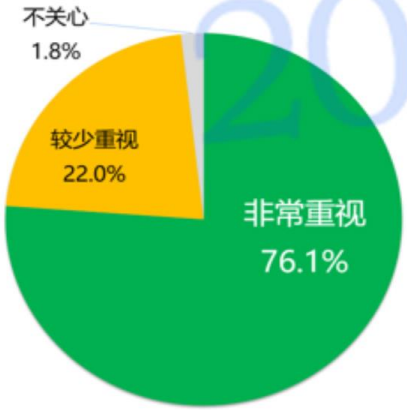
现状三：国家高度重视，工业安全防护体系推进中

机构	时间	政策文件	政策说明
全国人大	2017.06	● 《中华人民共和国国家安全法》	第三十一条　国家对公共通信和信息服务、**能源、交通、水利、**金融、**公共服务、**电子政务等重要行业和领域 … **关键信息基础设施**，在网络安全等级保护制度的基础上，实行**重点保护**。
国务院	2017.11	● 《关于深化“互联网+先进制造业”发展工业互联网的指导意见》	建立“**工业互联网安全保障**体系、提升安全保障能力”发展目标。
工信部	2011.10	● 《关于加强工业控制系统信息安全管理的通知》（451号）	… 加强重点领域**工控信息系统安全管理措施**，特别提到了与国计民生紧密相关领域的控制系统，如**核设施、电力、天然气、铁路、城市轨道交通、民航、城市供水**等
工信部	2016.10	● 《工业控制系统信息安全防护指南》（338号）	工业企业开展**工控安全防护**工作的**整体性指导文件**。
工信部	2017.06	● 《工业控制系统信息安全事件应急管理工作指南》（122号）	指导做好**工业控制系统信息安全事件应急管理**相关工作，保障工业控制系统信息安全。
工信部	2017.08	● 《工业控制系统信息安全防护能力评估工作管理办法》（188号）	检验338号文的实践效果，**综合评价工业企业工业控制系统信息安全防护能力**。
工信部	2017.12	● 《工业控制系统信息安全行动计划（2018-2020）》（316号）	为全面落实国家安全战略，**提升工业企业工控安全防护能力**，促进工业信息安全产业发展，加快我国工控安全保障体系建设，制定本**行动计划**。
工信部	2018.05	● 《工业互联网发展行动计划（2018-2020年）》	工业互联网安全指导性文件，明确并**落实企业主体责任**，… 建立针对**重点行业、重点企业的监督检查、信息通报、应急响应**等管理机制。
网信办	2017.07	● 《关键信息基础设施安全保护条例（征求意见稿）》	第十八条　…应当纳入关键信息基础设施保护范围： （一）政府机关和**能源**、金融、**交通**、**水利**、卫生医疗、教育、社保、环境保护、公用事业（**供水、供热、燃气**）等行业领域的单位；
公安部	2018.08	● 《网络安全等级保护条例（征求意见稿）》	第三十四条 … 应当按照网络安全等级保护制度要求，采取措施，管控云计算、大数据、人工智能、物联网、**工控系统**和移动互联网等新技术、新应用带来的安全风险，消除安全隐患。

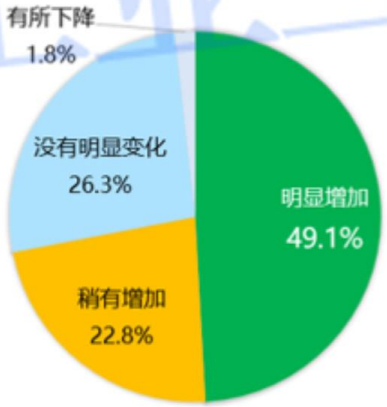
趋势一：企业对安全重视程度提高，投入增加

- 用户对安全的重视程度明显提高，有76.1%的工业用户非常重视工业互联网安全的建设
- 未来两年，近50%工业企业在安全方面的投入有明显增加趋势，22.8%企业投入的资金稍有增加。总体来看，工业互联网企业对安全的投入有一个良好的趋势
- 66.7%企业认为安全建设投入应占工业互联网投入的5%-10%

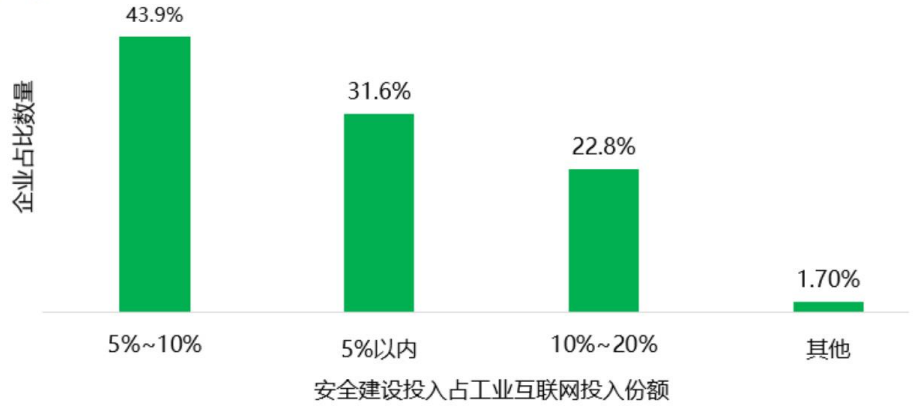
企业对工业互联网安全重视程度



未来两年，工业企业对工业互联网安全投入的预期



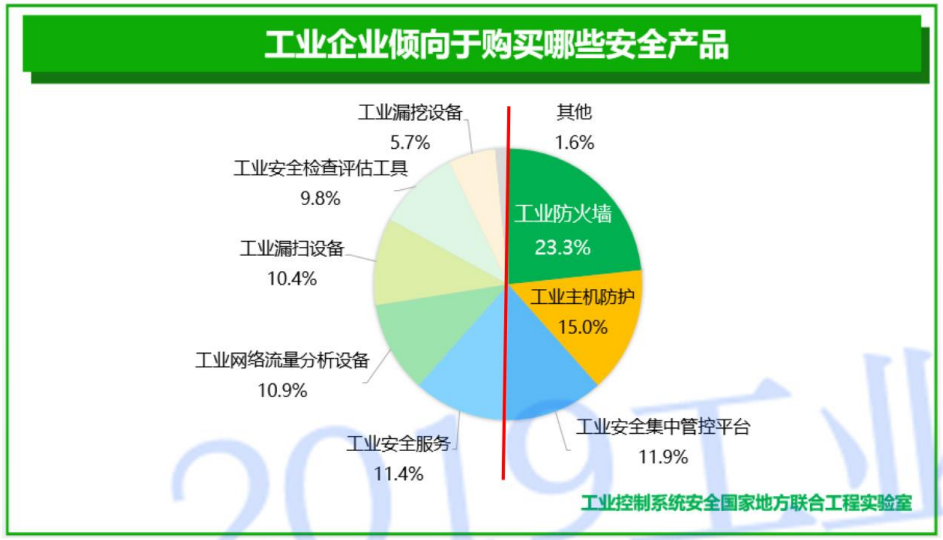
工业互联网安全建设投入占工业互联网投入份额



工业控制系统国家地方联合工程实验室

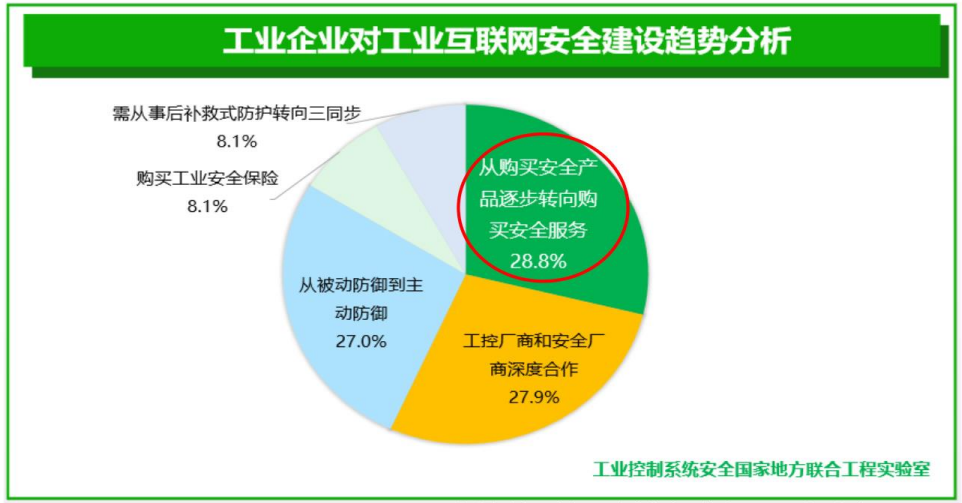
数据来源：对AII联盟工业互联网企业的调研

趋势二：防护产品需求高，其他产品呈多样化趋势



- 工业防火墙、工业主机防护、工业安全集中管控平台三个产品所占比例高达50%
- 安全检测类、安全评估类、安全服务类、安全研究类产品需求发展平衡，工业安全产品和服务体系日益完善

- 从购买安全产品逐步转向购买安全服务占比达到28.8%，安全服务市场扩大
- 工控厂商和安全厂商深度合作占比达到27.9%，多方协作趋势明显，构建产业协同的联合防御体系
- 技术层面深度创新

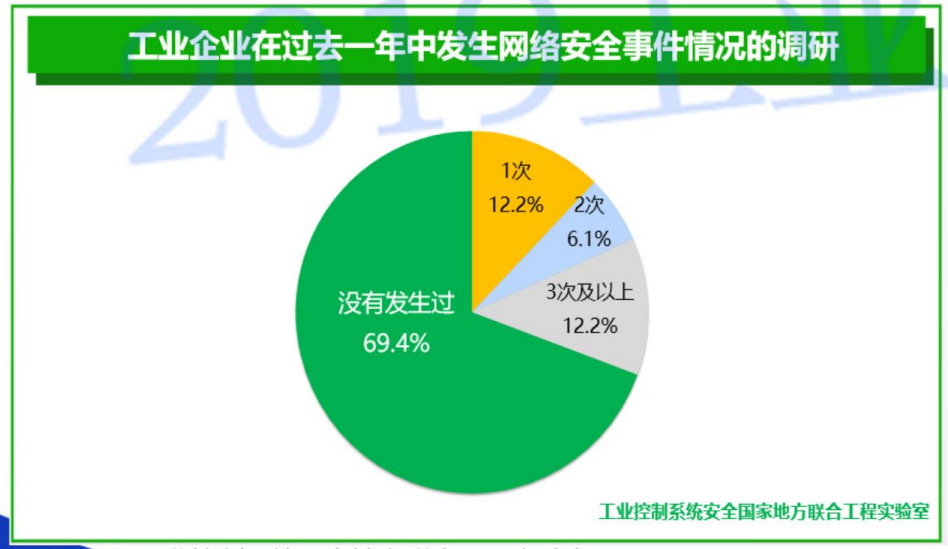


数据来源：对All联盟工业互联网企业的调研

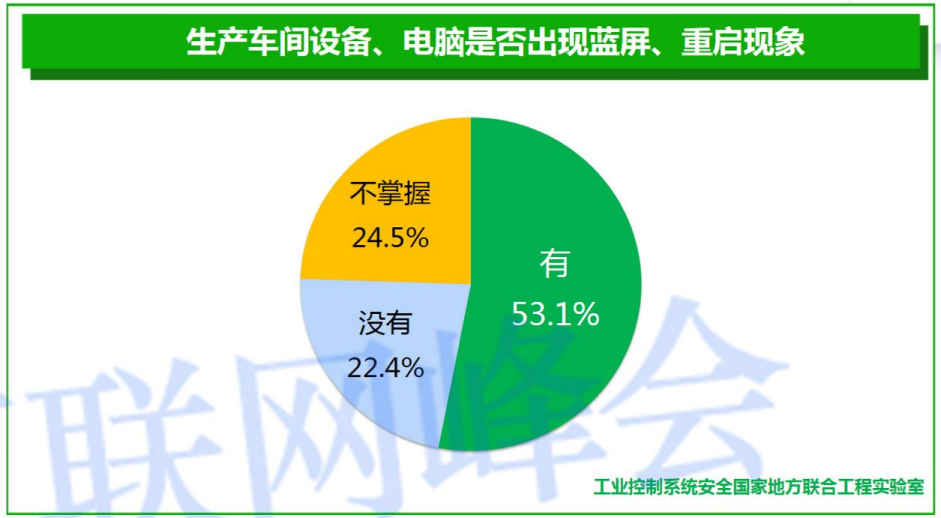
2019工业互联网峰会
工业控制系统国家地方联合工程实验室
创新引领 融通发展
2019工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019

趋势三：企业对自身面临安全风险的感知较弱

- 超过53%的企业遭受过生产设备安全故障问题
- 另有约1/4的企业对此问题表示 “不掌握”相关情况
- “不掌握”也就意味着企业其实并没有部署足够的网络安全监测措施以实时了解其工业系统的网络安全状况



工业控制系统国家地方联合工程实验室



工业控制系统国家地方联合工程实验室

- 69.4%企业表示在过去一年没有发生过网络安全事件
- 当企业内部电脑出现大量蓝屏、重启等现象时，往往意味着企业已经遭到了攻击，但企业管理者未作为安全事件来进行响应和调查，错过处置最佳时机

数据来源：对All联盟工业互联网企业的调研

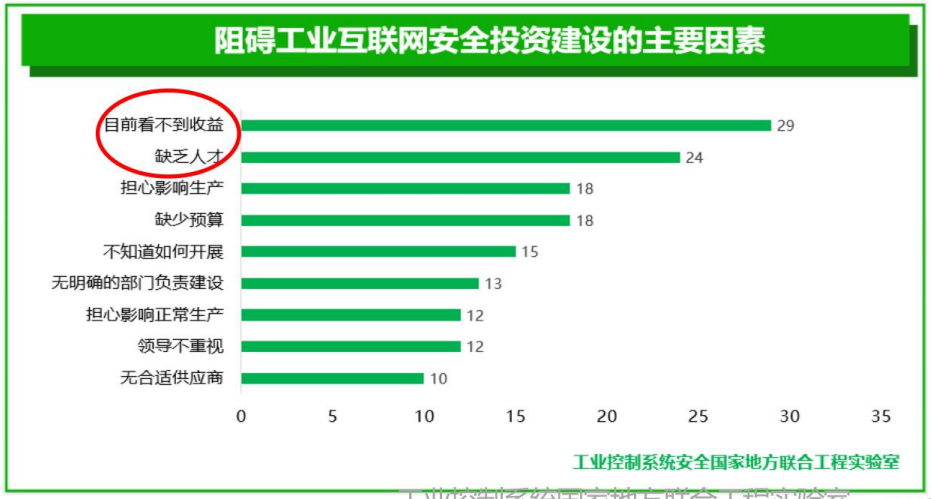
2019工业互联网峰会

趋势四：收益不明/人才缺乏为阻碍安全建设主因

工业控制系统国家地方联合工程实验室

- 人才缺乏是影响工业互联网建设的首要因素，占比最高
- 值得注意的是信息安全和资金不足占据相同的比例，可见信息安全在工业互联网投资建设中影响越来越大。

- 目前看不到收益、人才缺乏是阻碍安全投资建设的重要因素
- 工业互联网安全建设最大的难处在于没有造成安全事故，企业高层较难理解安全建设短时间内给企业带来的收益，工业互联网安全建设不被工业企业理解。



工业控制系统国家地方联合工程实验室

数据来源：对All联盟工业互联网企业的调研

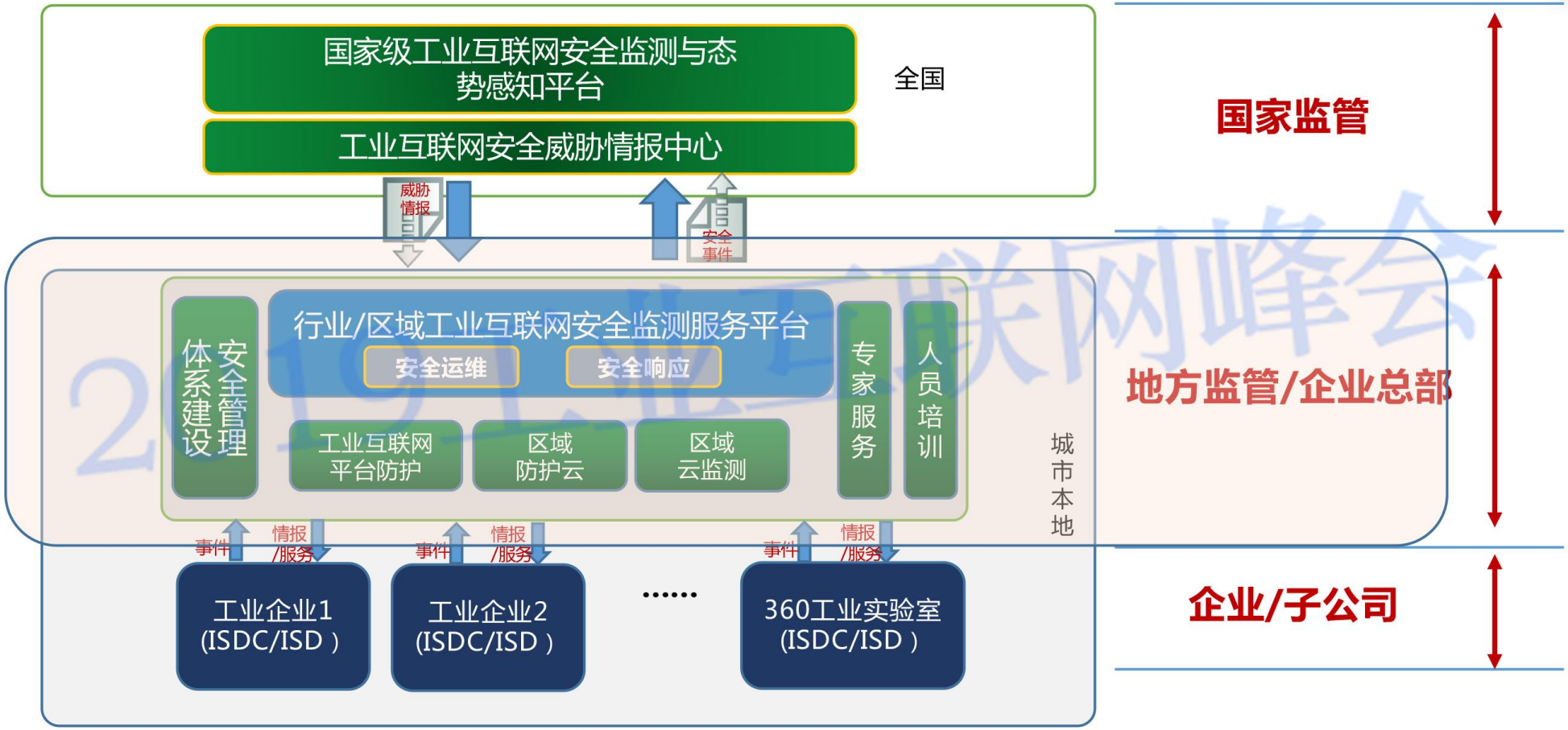
2019工业互联网峰会
创新引领 融通发展
INDUSTRIAL INTERNET SUMMIT 2019

目录
Contents

数据驱动安全理念，协同联动防护体系

2019工业互联网峰会

工厂-集团-监管机构 多级安全服务体系



监管的痛点 /政府监管/企业总部-监测平台建设思路

- 家底摸不清
- 互联网上无监测
- 安全态势难感知
- 事前无预警
- 事后难处置
- 业务管理无系统

◆ **突出重点**

将重点放在**工业互联网企业和**关系国计民生**工控企业**上，进行重点防护

◆ **摸清家底**

通过专业工具和技术，摸清辖区内工业企业工业资产，建立工业企业的资产列表

◆ **持续监测**

对辖区内工业互联网开展主动实时持续监测，及时发现企业的安全风险

◆ **预警通报**

建立动态的风险预警和预警通报机制，提高监管部门的监督管理和应急处置能力

◆ **情报共享**

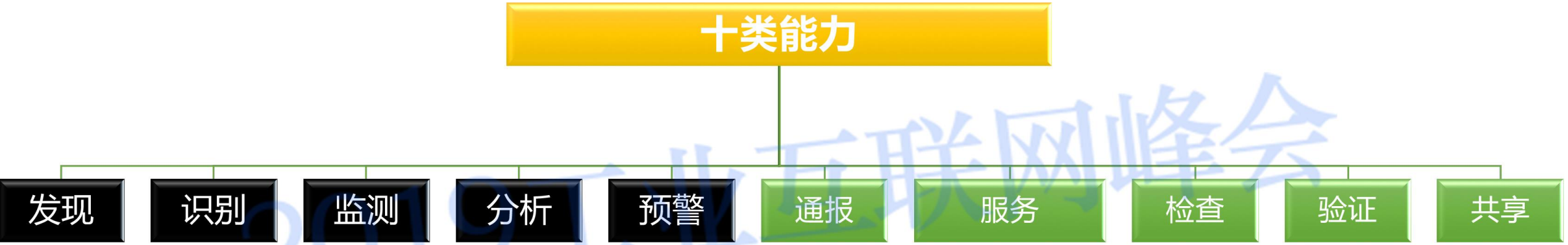
同工信部、临近的省市和辖区内工业企业共享工业信息安全情报

◆ **支持经办**

将安全培训、事件上报、事件处置、现场检查、企业自查、企业整改等日常工作进行业务流程化定义，通过应用系统来辅助、支持工信监管部门的日常业务处理

2019工业互联网峰会

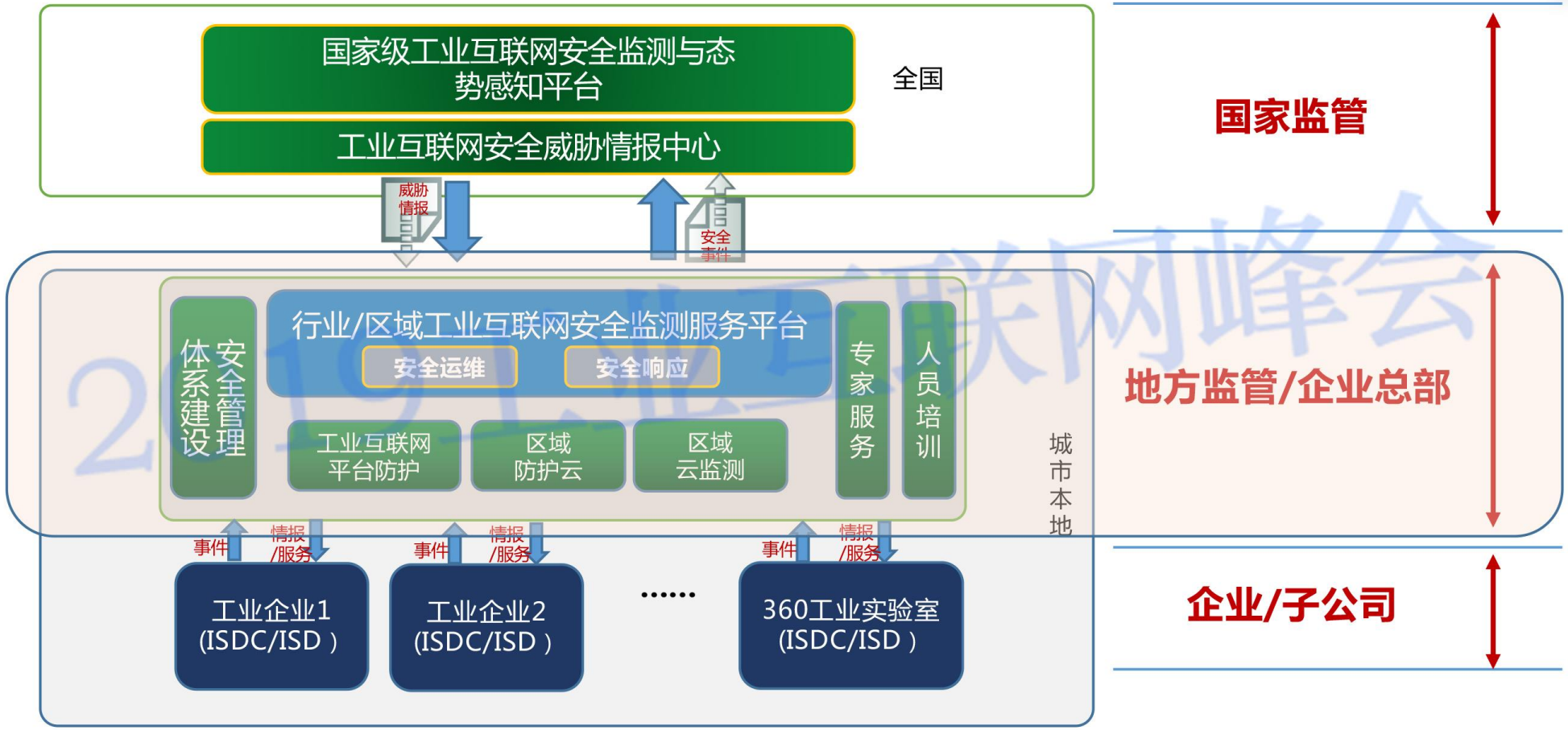
工业互联网安全监测服务平台10大能力



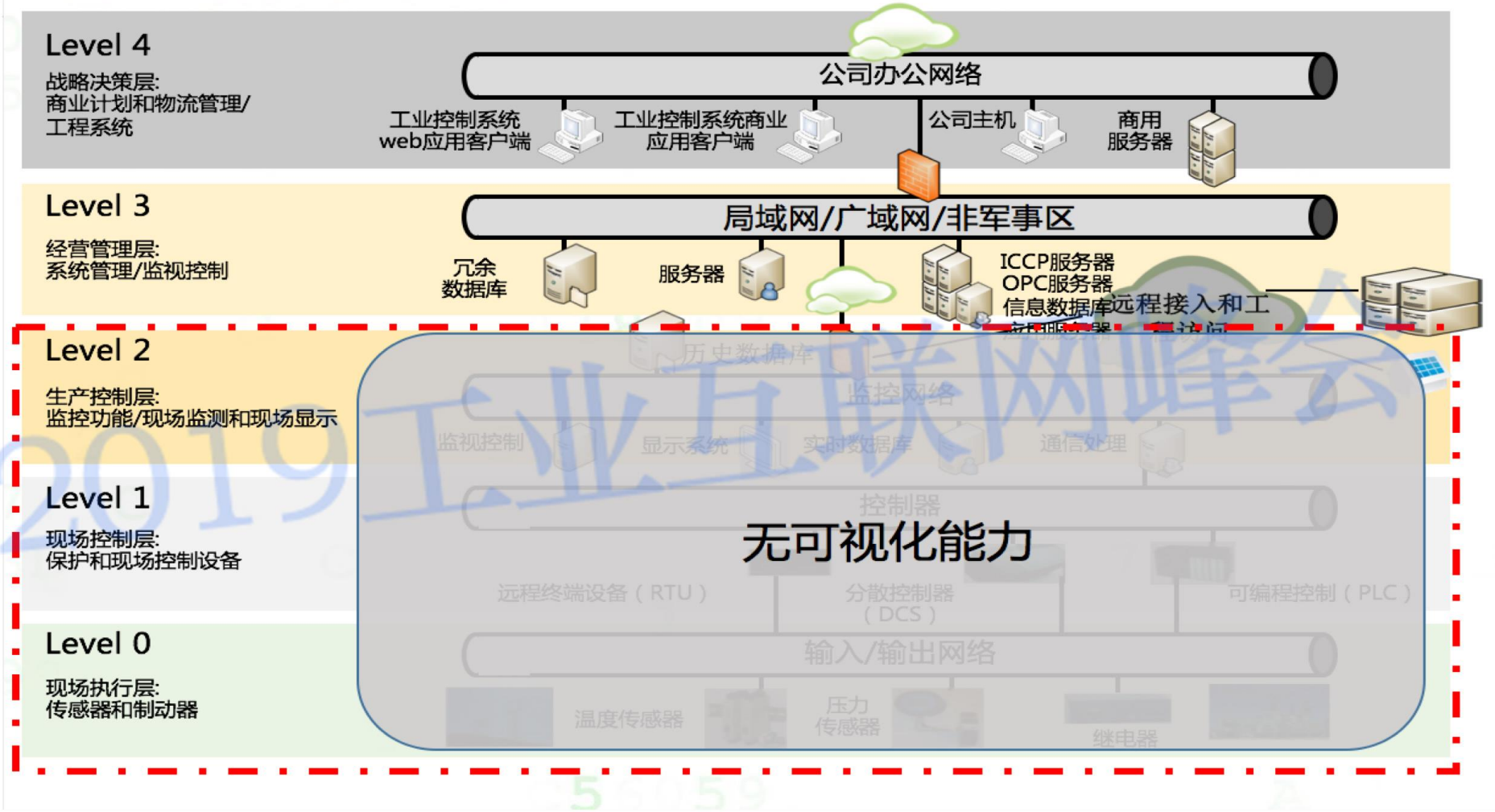
2019工业互联网峰会

可发现识别、可预警通报、可检查整改、可对外服务、可日常运营

工厂-集团-监管机构 多级安全服务体系



工业企业痛点：工业企业工业网络安全几乎空白



- 企业内网缺少可见性
- 企业公网缺少监测能力
- 企业出现安全事件平均解决时间长，损失大

工业企业-工业互联网安全防护

01 资产发现及梳理（asset）

工业安全服务 services

资产发现和梳理；
流量分析，威胁发现；
工控安全体系化设计；
模拟环境渗透测试；
对安全事件响应演练；
安全意识培训；

工业安全检查评估工具 Tools

威胁情报匹配；
异常行为和未知威胁检测；
工控资产发现与漏洞扫描；
工控合规检查及报告生成；
工控协议解析、流量分析；
行为日志、项目管理等；

02 安全隔离与防护 (Isolation and protection)

工业安全主机防护（Endpoint Protect）

智能机器匹配白名单生成
多种模式一键切换；
外部设备安全管控；
针对wannacry防御技术；
支持多种操作系统；
工业主机统一管理；

工业控制安全网关（Gate）

工控协议的深度解析；
IT、OT一体化安全防护；
白名单智能学习；
入侵防御、病毒等威胁检测；
全面风险信息展示及分析；
高可靠的传输加密；

03 安全监控与审计 (Monitoring and auditing)

工业安全监测系统

工控网络异常检测；
工控关键事件检测；
工控关键业务中断检测；
工控网络流量审计；
支持协议规约检测；
支持基线检测功能；

04 安全管理与运营（Management and operation）

工业安全监测控制台

企业级工业安全运营平台
应急响应平台与可视化
基于威胁情报的攻击发现
工控关键操作监测
流量监测、异常行为监测
关键资产管理、日志采集与管理
上报风险事件、响应处理

工业安全管理系统

工控安全设备和系统管理;
统一配置和运维;
实现策略配置下发;
网络流量分析;
工业控制网络运行实时掌握;

05 工业态势感知 (Situation Awareness)

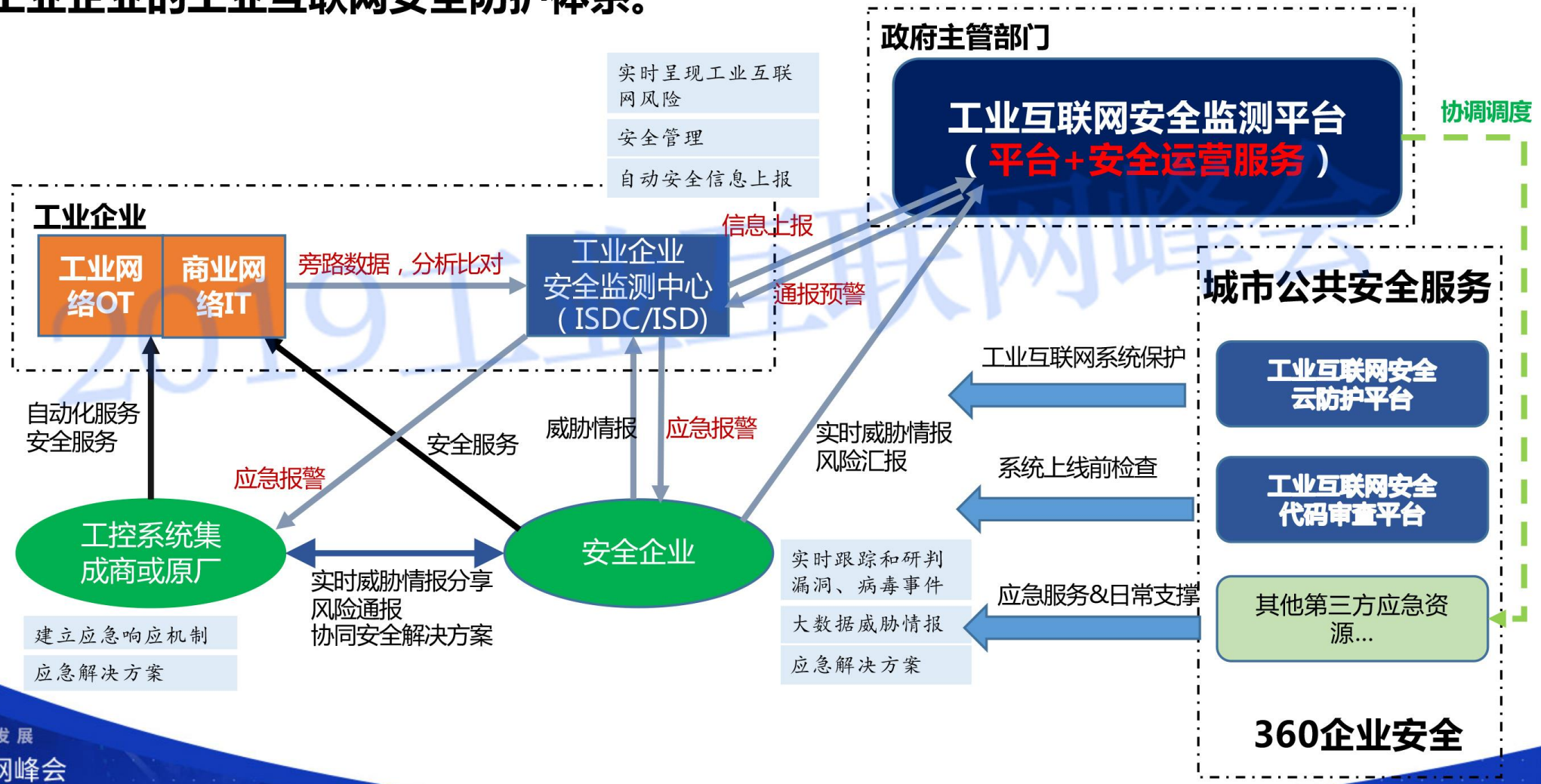
工业态势感知

区域行业威胁风险和事件感知
工业安全监测系统
预警通报系统
事件处置系统
情报信息系统
综合管理系统

2019工业互联网峰会

工业互联网安全防护体系——运营体系

建立以内外网监测为基础，以协同联动和信息共享为驱动，以安全运营为中心，以业务服务为目标的面向工业企业的工业互联网安全防护体系。



实践一：比亚迪17000台工业主机安全防护

背景需求

- 比亚迪生产制造产线遭受**“永恒之蓝”勒索病毒**侵袭
- **场景复杂**：电池、手机、笔记本、汽车电子、配件、整车组装等各类车间，涉及电子制造、汽车制造场景，工业软件众多。
- **适配复杂**：工业主机多样，硬件配置多样，操作系统有WinXP、Win7、Win8、Win10等，各种汽车的测试板卡、数据采集卡适配

方案效果

- **应用规模巨大**

37个工业园区，**17000台**工业主机

- **实施复杂度高**

场景复杂：**10+种**工业制造场景

操作系统：**15种**

应用复杂：**100+**工业软件适配

实施复杂：**非停产实施**

项目入选工信部工业互联网安全优秀应用案例

2019工业互联网峰会

实践二：海尔智能工厂工业安全监测（ISD/ISDC）

360企业安全 安全第一

Haier

背景需求

- 海尔是智能制造行业的标杆企业，为加强工业安全管理，希望发现潜在的生产安全隐患，及时处置，保障生产连续性
- **厂区监测**：涉及到沈阳、天津、青岛、郑州、佛山5座城市的8家智能工厂，覆盖空调、洗衣机、电冰箱三大产线
- **全网感知**：掌握各厂区的工业资产家底和生产安全整体状况

方案效果

- 在8个厂区部署工业安全监测系统ISD
  - 获取完整资产清单
  - 发现生产安全漏洞
  - 监测工控系统异常
- 集团总部工业安全监测系统控制台ISDC
  - 汇总分析各厂区数据
  - 大屏集中展示全网安全态势

该案例是海尔COSMOPlat生态体系安全防护的重要部分

2019工业互联网峰会

实践三：某城市工业互联网安全监测服务平台

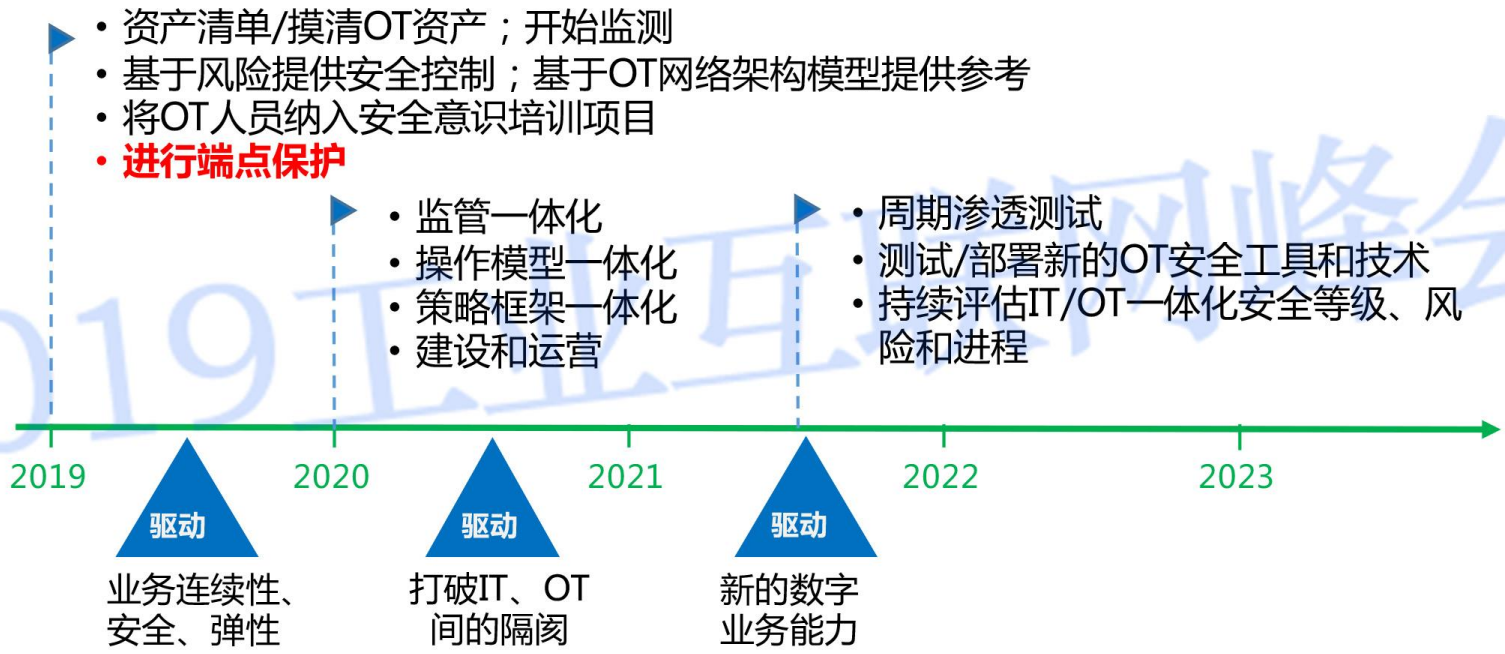
- 对XX市全域内41万个IP地址风险监测
- 发现应用站点84个新增，工控系统31个，物联网系统16个
- 工控漏洞25个、物联网漏洞4个、应用站点漏洞723个
- 通过平台向19个工业重点企业发出了预警信息

总体安全态势为中等风险

目录
Contents

工业互联网安全战略推进时间表

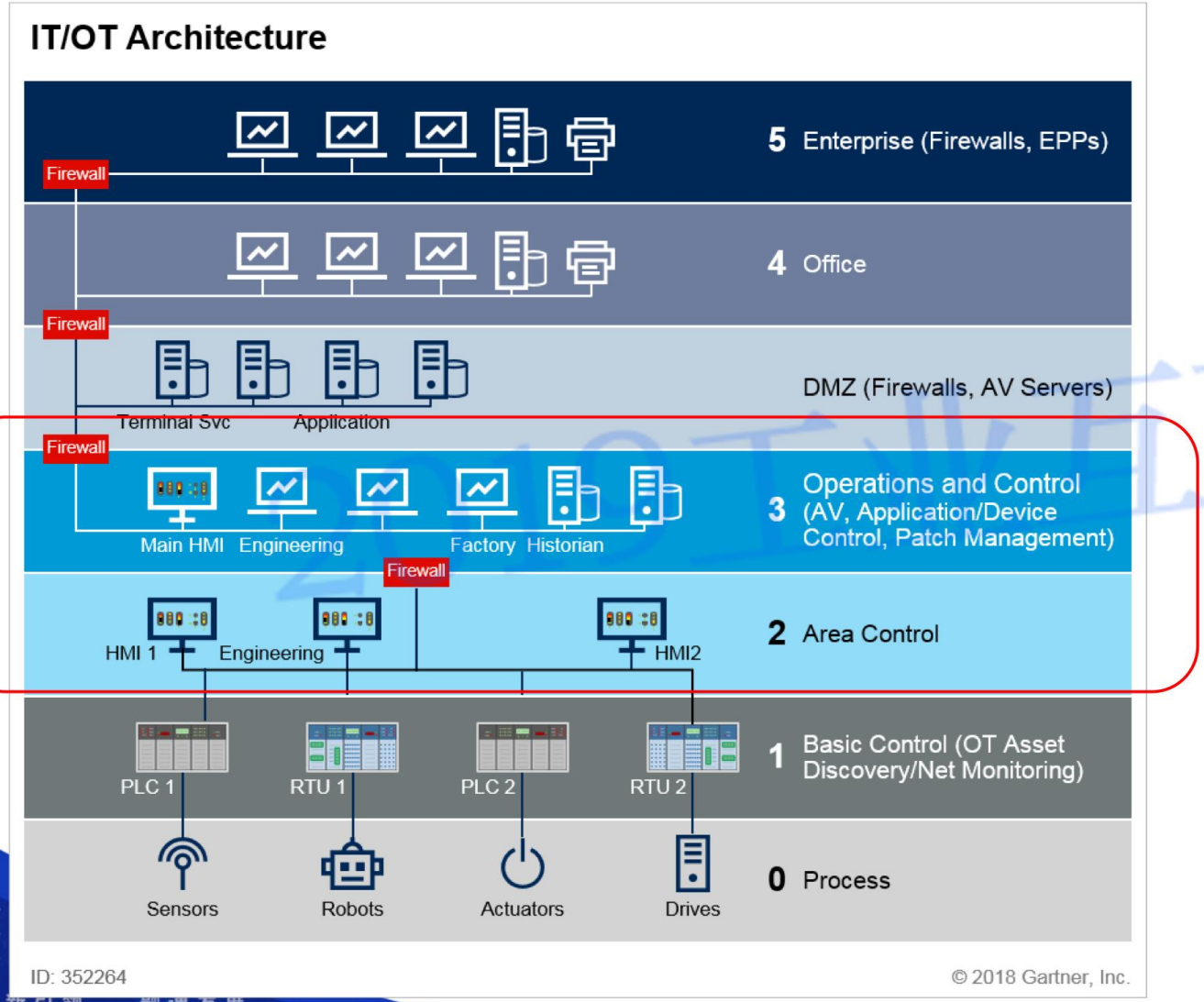
安全治理是长期且复杂的过程，难以一蹴而就，需要循序渐进

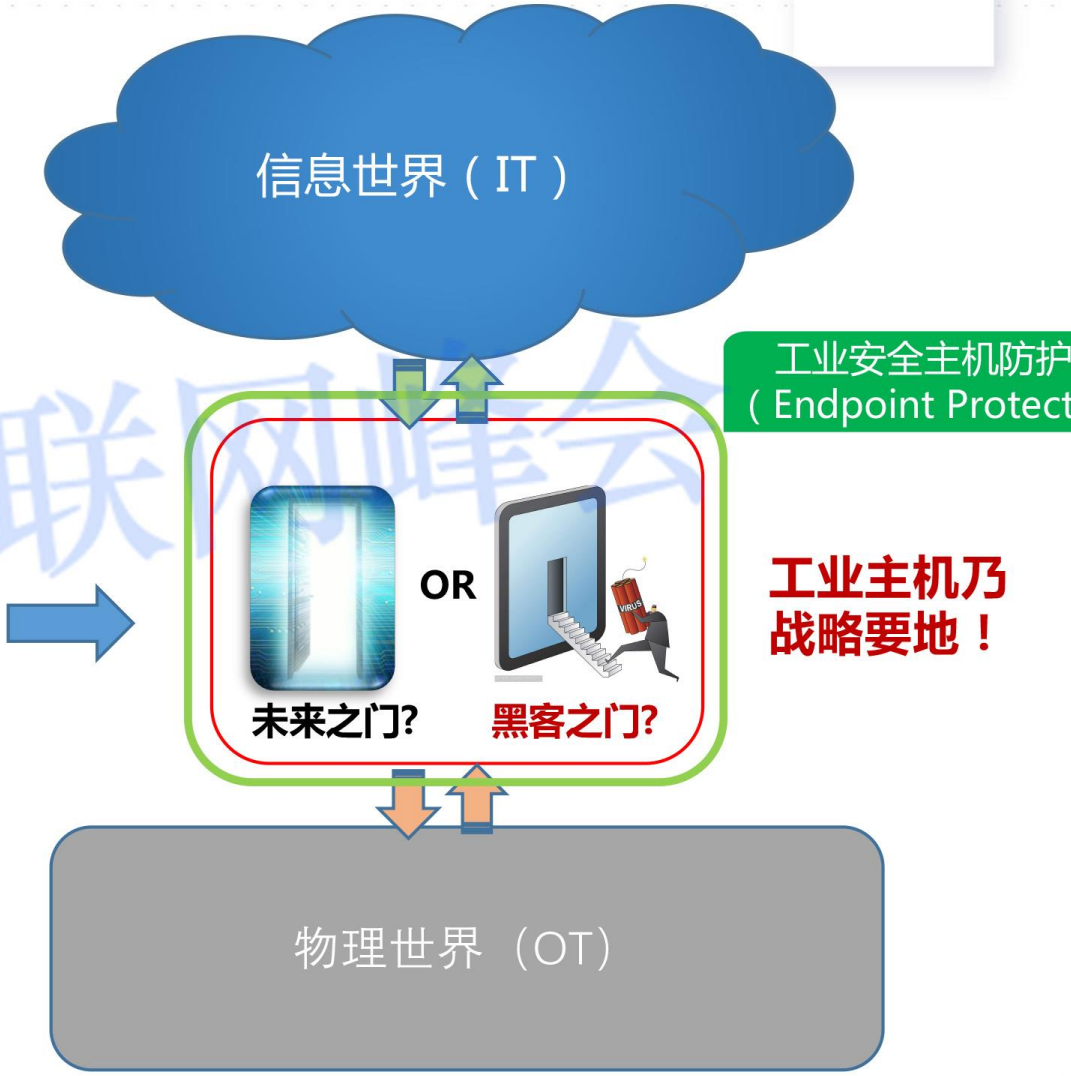


战略路线图时间表

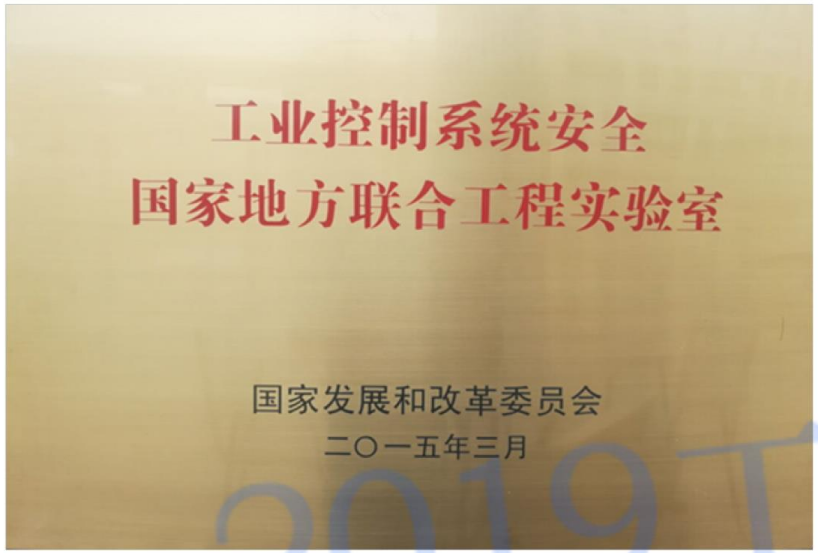
2019工业互联网峰会

工业主机（安全之门）——战略要地

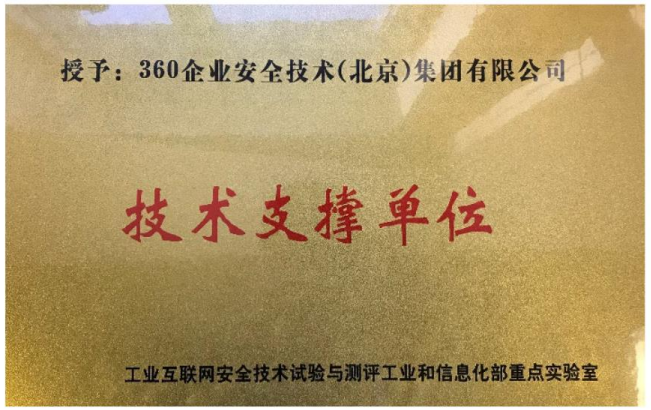




360在工业互联网安全领域已开展工作



- 国家发改委——工业控制系统安全国家地方联合实验室
- 中国工业互联网产业联盟——副理事长、安全组组长
- 工业控制系统信息安全产业联盟——副秘书长单位
- 中国边缘计算产业联盟-安全组组长
- 国家工业信息安全产业发展联盟—风险通报与应急服务组 副组长
- 中关村网信产业联盟——智能制造信息安全专委会 副主任理事



独家技术支持工信部“首届工业信息安全技能大赛”，参与制定工业安全相关重要国家标准

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

Thanks

主讲人：陶耀东

2018年2月21日

创新引领　融通发展

2019工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019