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

2018中国工业互联网安全态势报告

主讲人：李江力

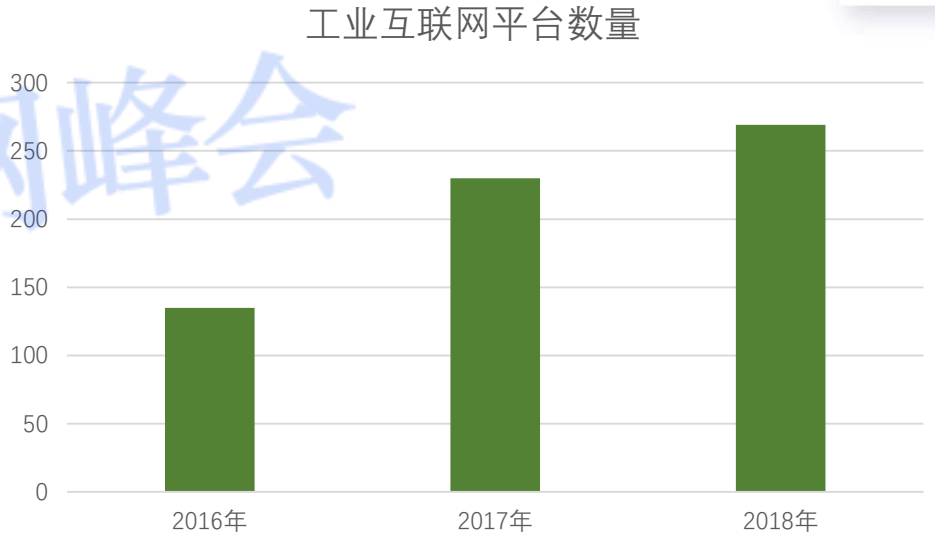
智联赋能　融通创新

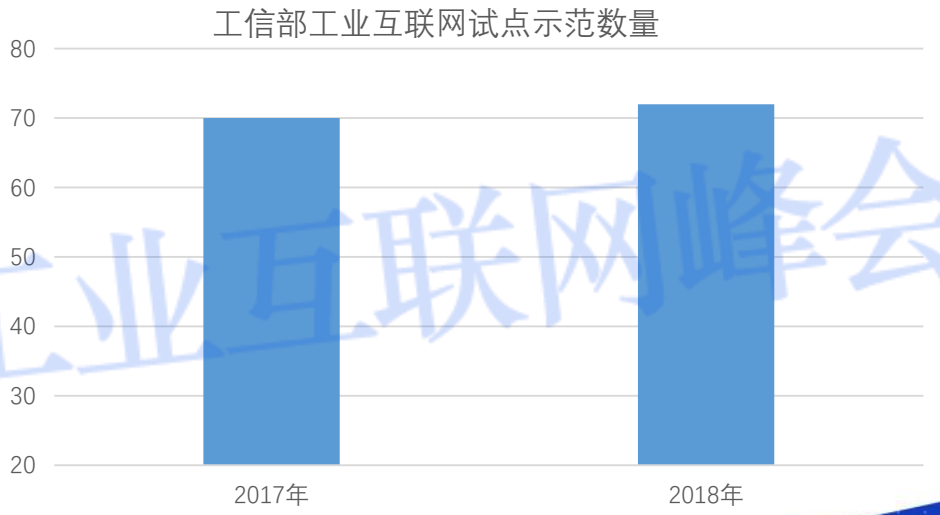
2019工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019

目录
Contents

中国工业互联网发展概述

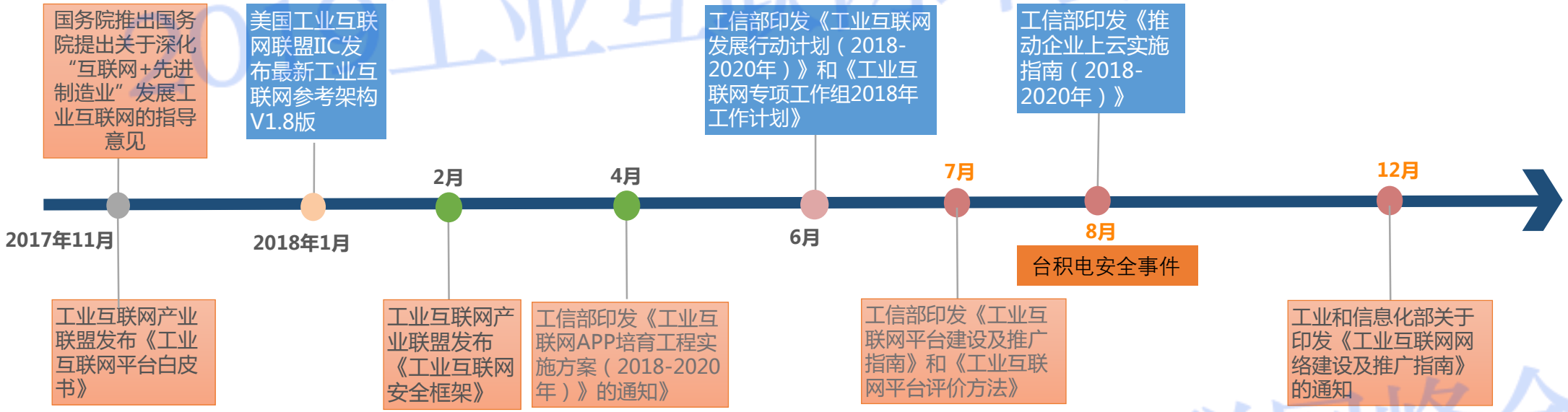
- **顶层设计基本形成**
  - 战略与政策层面，国务院《关于深化“互联网+先进制造业”发展工业互联网的指导意见》
  - 技术体系层面：实现了从三大要素（网络、数据、安全）到三大功能体系的塑造（网络、平台、安全）
- **应用实践场景丰富**
  - 构架在丰富工业场景和强劲转型需求上的应用创新和模式创新，数据驱动的初步智能化，包括逐见成效的工业和ICT（包括互联网）界的相互融合；
- **网络体系逐渐完善**
  - 网络化的补课和新体系的创新，标识解析体系。
- **平台建设快速增长**
  - 快速增长下跟随与创新的交织，极为丰富的模式创新和基础能力的综合差距（2018年已达269家）
- **安全框架形成共识，安全标准体系正在建设中。**
- **技术深层次的综合和基础差距与新技术追赶**
- **产业生态的快速形成（AII产业联盟，942家成员单位）**





注：2017年名为“制造业与互联网融合发展试点示范”

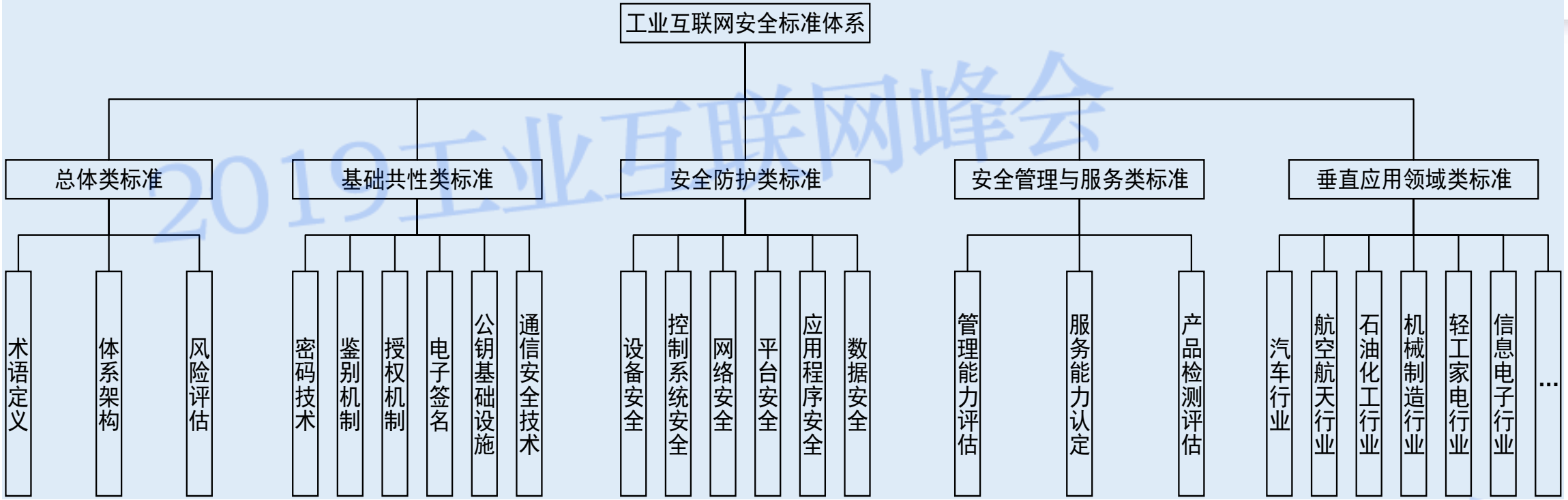
2018工业互联网安全大事记



2018各地工业互联网产业支持政策

- 2018年2月22日，湖南省经信委发布《湖南省中小企业“上云”行动计划（2018）》
- 2018年3月22日，广东省人民政府推出了《广东省深化“互联网+先进制造业”发展工业互联网的实施方案》和《广东省支持企业“上云上平台”加快发展工业互联网的若干扶持政策（2018-2020）》。
- 2018年4月9日， 浙江省信息化工作领导小组关于印发《浙江省深化推进“企业上云”三年行动计划（2018-2020年）》的通知。
- 2018年4月12日，山西省大数据发展领导小组办公室印发《山西省促进大数据发展应用2018年行动计划》的通知。
- 2018年4月18日，河南省人民政府印发《河南省智能制造和工业互联网发展三年行动计划（2018-2020年）》的通知。
- 2018年4月28日，浙江省人民政府发布了《浙江省人民政府关于深化制造业与互联网融合发展的实施意见》。
- 2018年5月16日，河南省人民政府发布了《河南省“企业上云”行动计划（2018-2020年）》。
- 2018年5月17日，重庆市人民政府印发《重庆市深化“互联网+先进制造业”发展工业互联网实施方案》的通知。
- 2018年6月14日，深圳市人民政府办公厅印发《深圳市工业互联网发展行动计划（2018-2020年）》和《深圳市关于加快工业互联网发展的若干措施》的通知。
- 2018年7月2日， 江苏省经济和信息化委员会发布《关于组织实施江苏省工业互联网创新发展“365”工程》的通知。
- 2018年7月26日，福建省工业互联网专项工作组印发《福建省工业互联网专项工作组2018年工作计划》的通知。
- 2018年7月31日，甘肃省人民政府办公厅印发《甘肃省工业互联网发展行动计划（2018-2020年）》的通知。
- 2018年8月13日，湖北省人民政府办公厅印发《湖北省工业互联网发展工作计划（2018-2020年）》的通知。
- 2018年9月5日， 重庆市人民政府办公厅发布《重庆市推进工业互联网发展若干政策》的通知。
- 2018年9月28日，天津市工业互联网专项工作组办公室印发《天津市工业互联网发展行动计划（2018-2020年）》的通知。
- 2018年11月14日，上海市经济和信息化委员会印发《上海市推进企业上云行动计划（2018-2020年）》的通知。

工业互联网安全标准体系建设



- **CCSA成立工业互联网特设组（TS8），下设安全组WG5**，正在积极推动以下标准：
  - 已送审：《工业互联网安全防护总体要求》、《工业互联网安全接入技术要求》、《工业互联网平台安全防护要求》、《工业互联网数据安全保护要求》
  - 征求意见稿：《工业互联网安全能力成熟度评估规范》、《工业互联网平台安全防护检测要求》、《工业互联网平台安全风险评估规范》、《工业互联网安全服务能力认定准则》、《工业互联网安全监测与管理系统建设要求》

- 2018年7月，**全国信息化和工业化融合管理标准化技术委员会（SAC/TC573）正式成立**

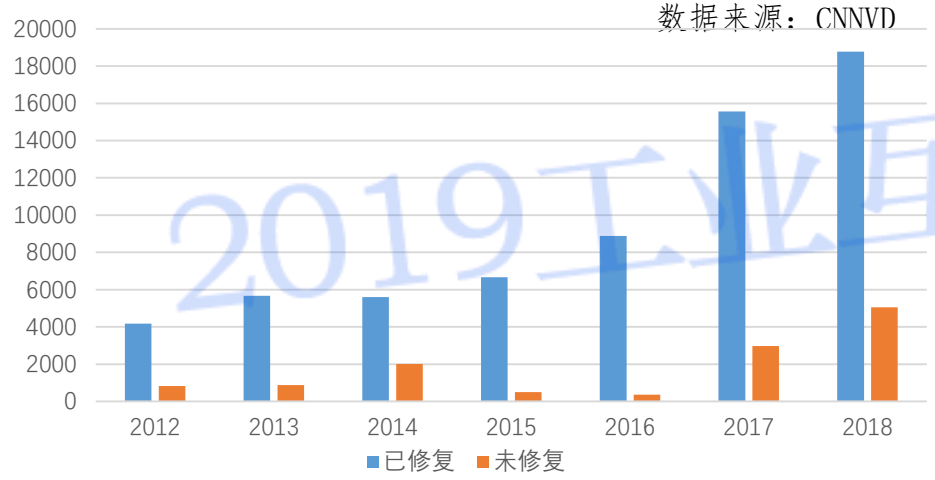
2018：工业互联网安全问题

工业终端：勒索病毒发酵	勒索病毒、挖矿木马继续发酵，工业主机终端成为安全突破口
控制系统：形势依然严峻	2018年爆多起工业控制系统有重大漏洞，影响多类生产系统
工业平台：安全方案不足	工业互联网平台方兴未艾，但其中安全防护都比较简单初级
工业APP：缺乏安全接口	工业APP形态各异、种类繁多，缺乏安全机制和标准安全API

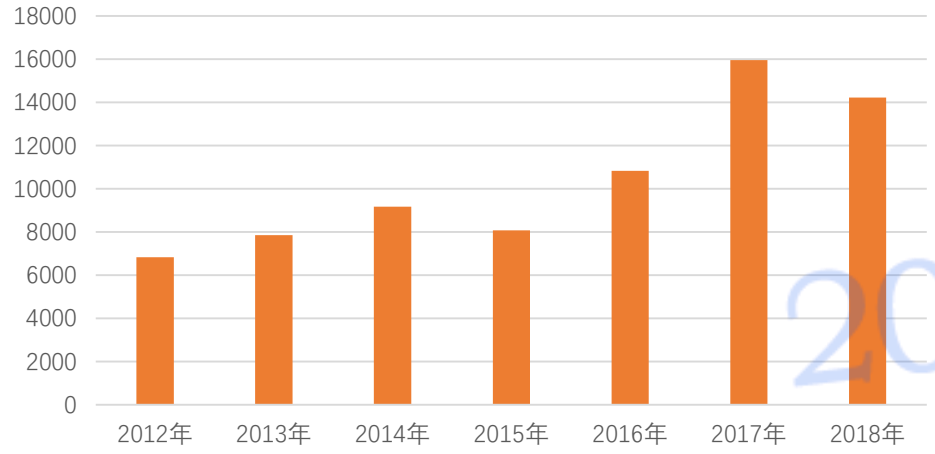
2018：互联网漏洞统计

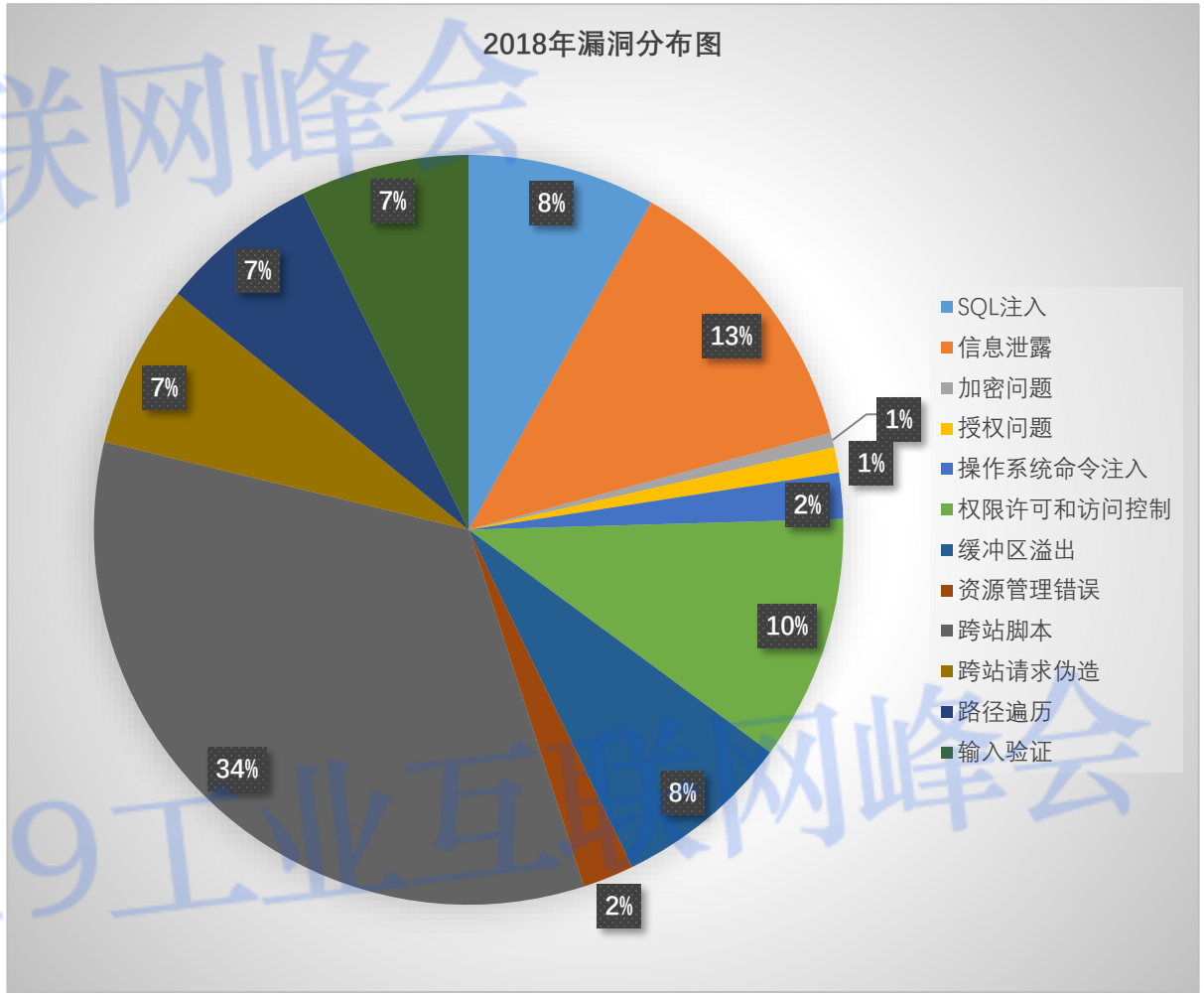
CNNVD年度漏洞分布图

数据来源：CNNVD



CNVD年度漏洞统计

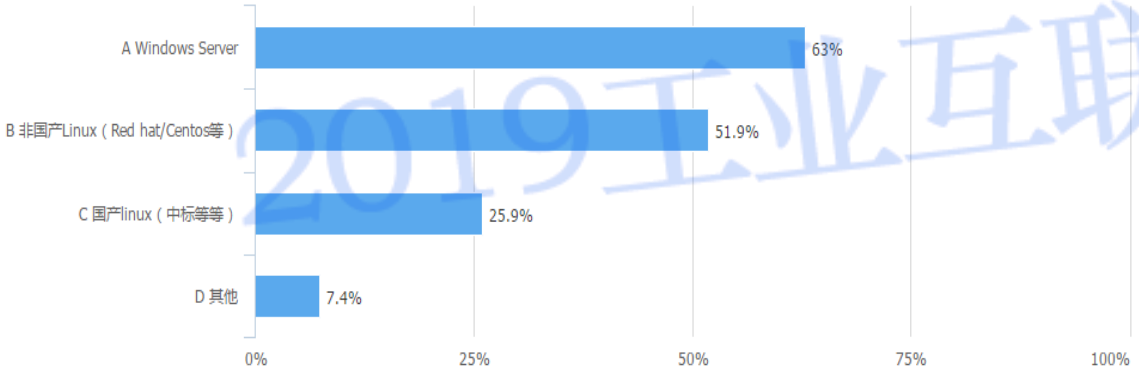




数据来源：CNNVD

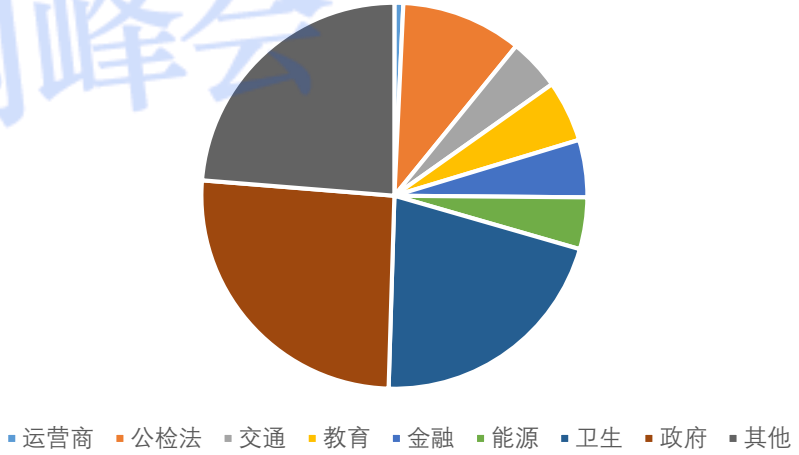
2018：工业终端安全

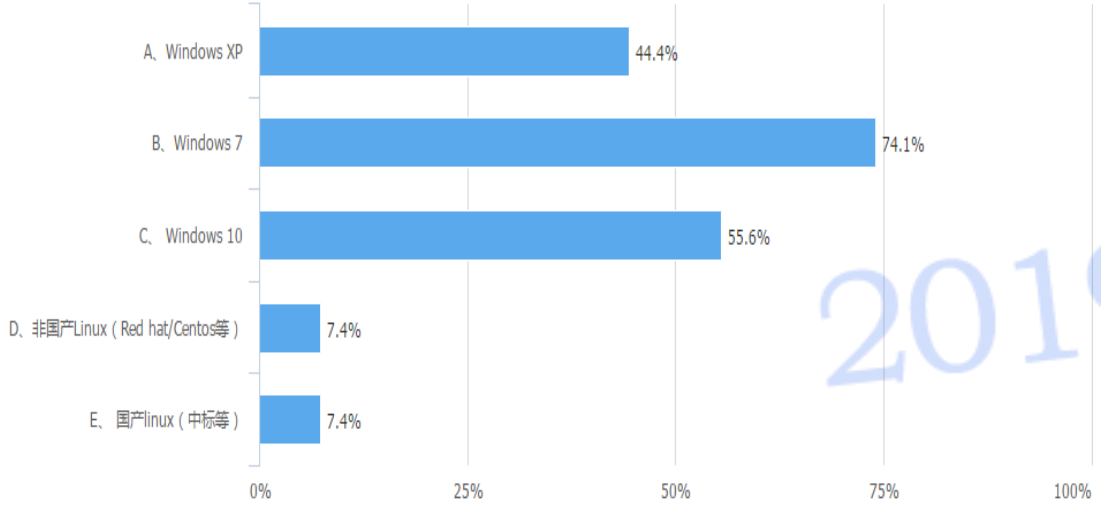
数据来源：工业互联网产业联盟



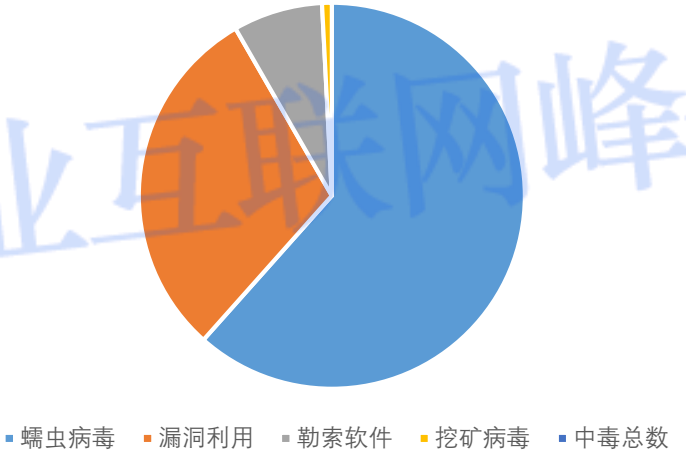
受害政企行业分布 占比

数据来源：360企业安全





受害用户感染病毒分布 占比



2018：工业终端安全

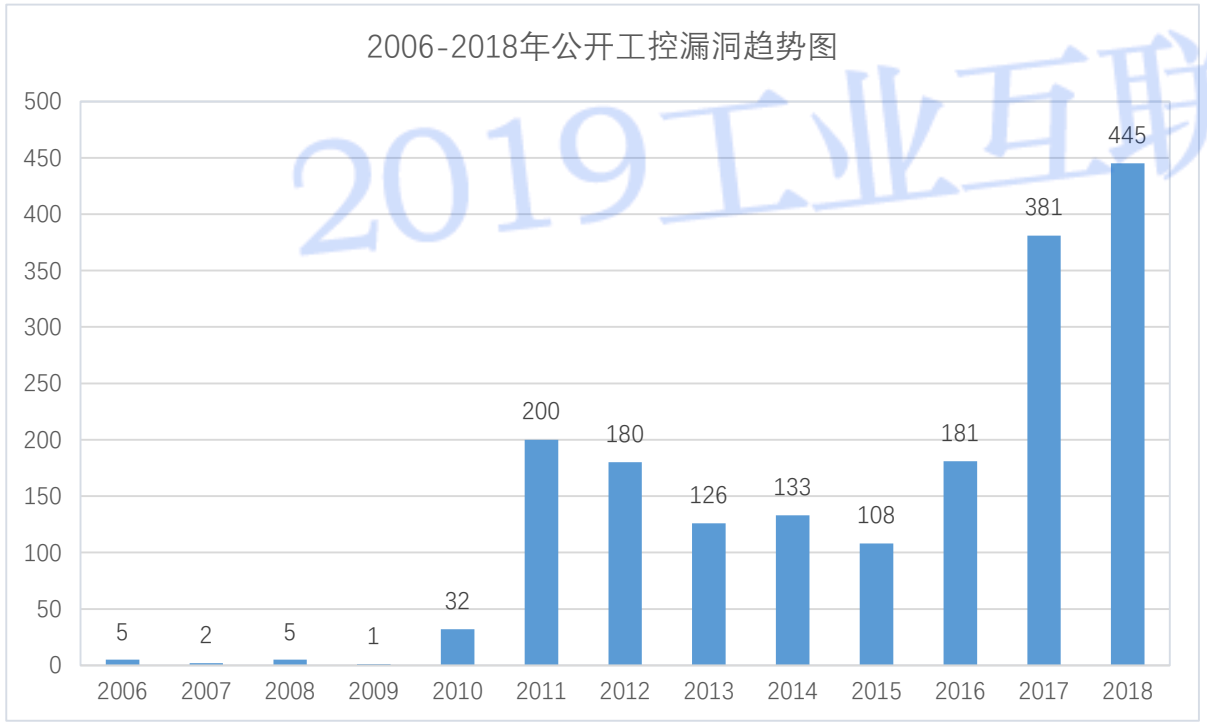
数据来源：360企业安全

数据来源：瑞星

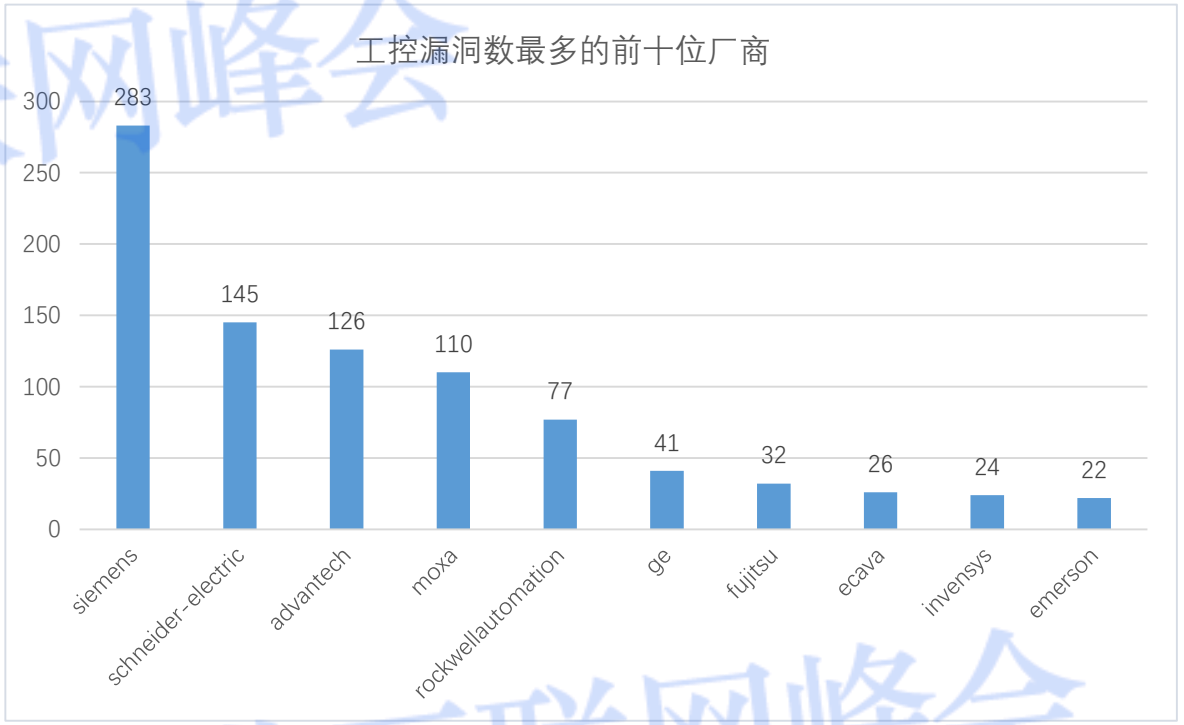
- 2018年7月，某知名汽车零部件生产企业工业生产网络遭受勒“永恒之蓝”索病毒的攻击，9月10日开始感染到多条生产线，对正常生产造成严重影响。
- 2018年8月，台积电台湾三大基地被曝遭勒索病毒入侵，生产线停摆，损失近30亿。
- 2018年11月，台湾合晶科技旗下一家工厂全线电脑感染WannaCry勒索病毒，造成产线瘫痪，工厂全部停产。
- 2018年10月，某炼钢厂工业生产网络自10月起各流程工艺主机遭受了蠕虫病毒的攻击，
- 2018年11月，某石油公司采油厂感染了一款名为Lucky的勒索病毒，业务系统受到感染，影响生产。

2018：工业控制系统漏洞统计

数据来源：CNVD



数据来源：CNVD

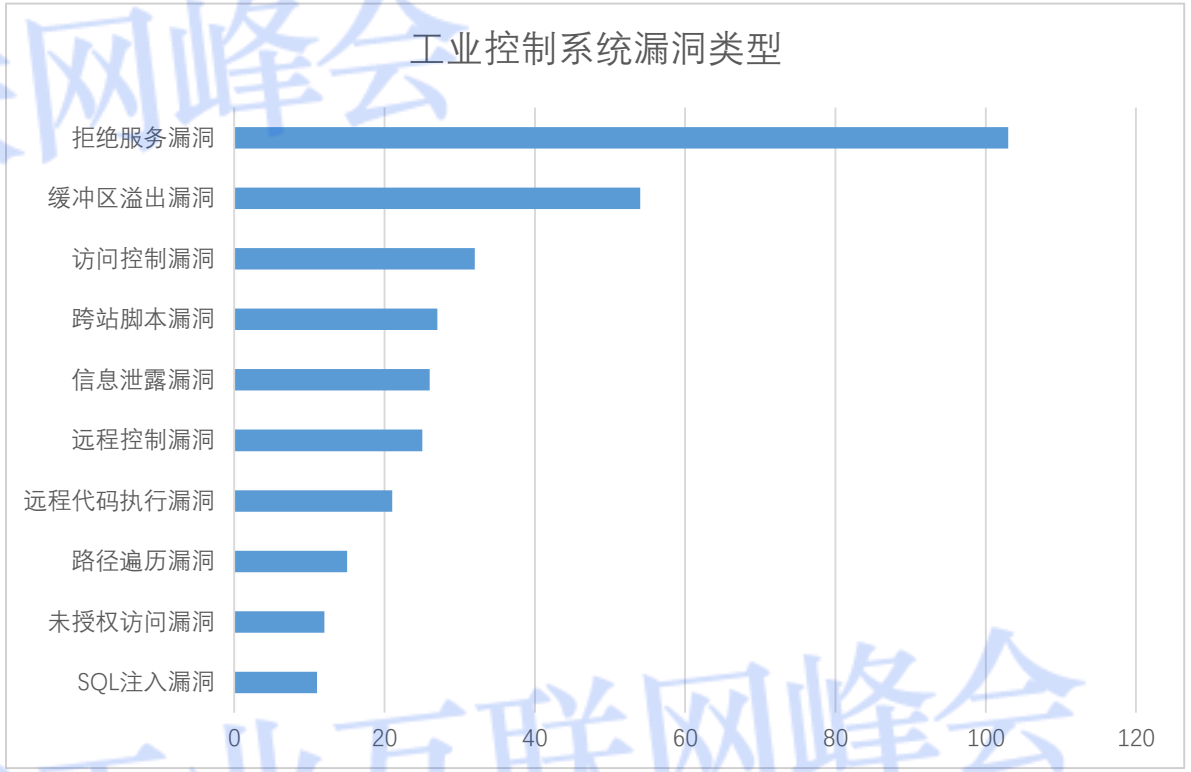


- 2018年3月，罗克韦尔PLC设被曝多项严重漏洞
- 2018年4月，西门子继电保护设备曝高危漏洞，可被用于攻击电力设施
- 2018年4月，Moxa 工业安全路由器爆多项严重漏洞
- 2018年5月，两款施耐德电气软件存在远程代码执行漏洞
- 2018年8月，西门子 WinCC 软件存在权限提升漏洞

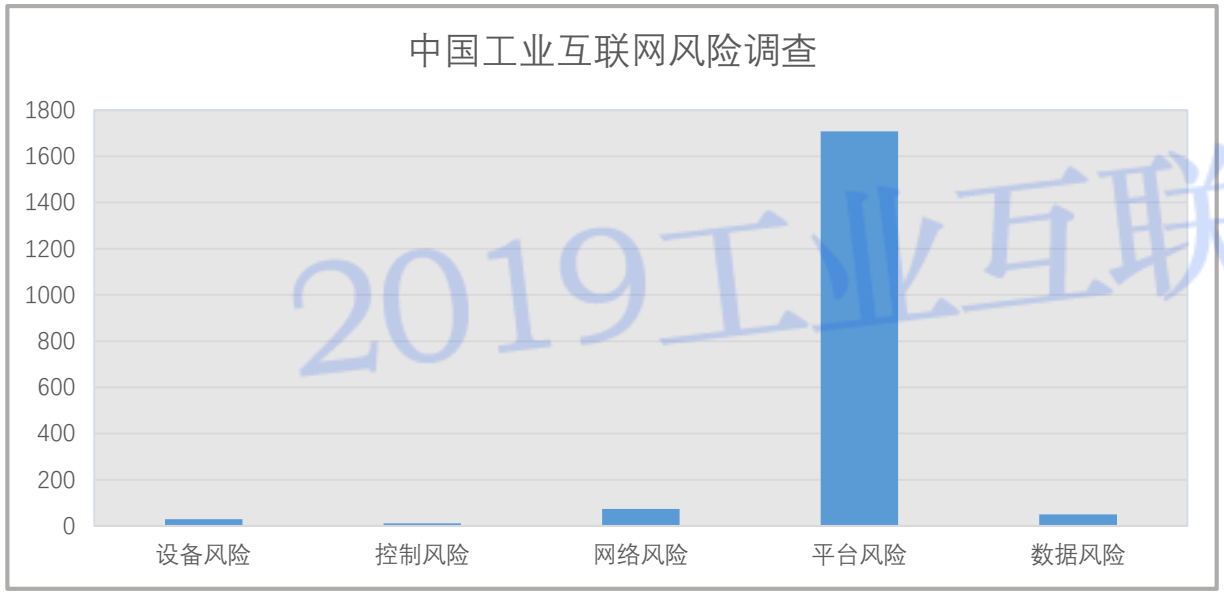
2018：工业控制系统漏洞分布

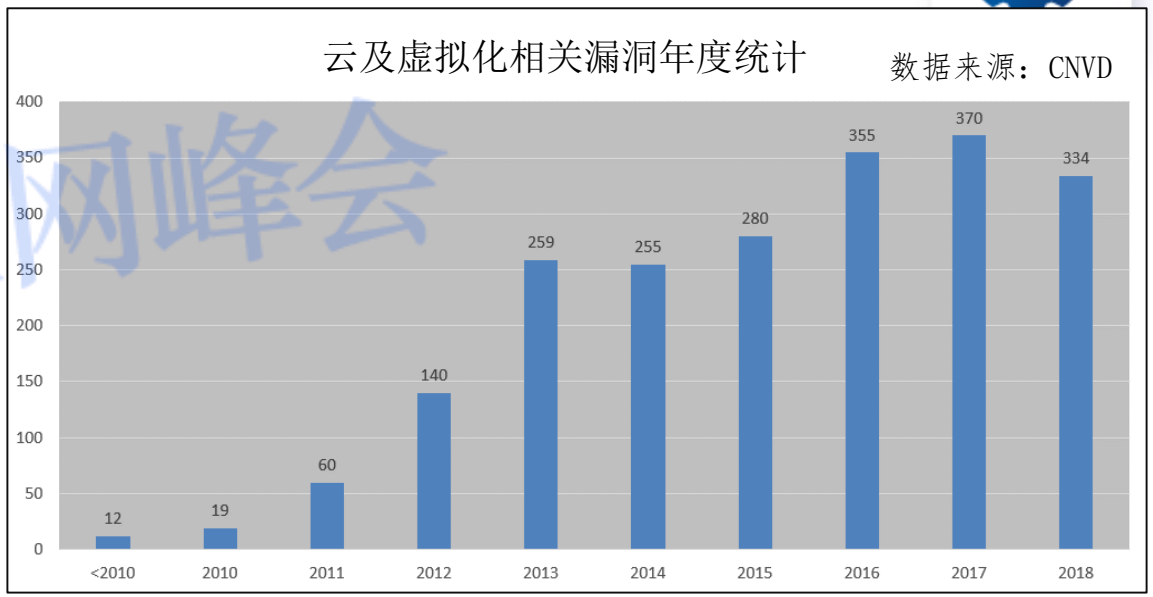
数据来源：CNVD

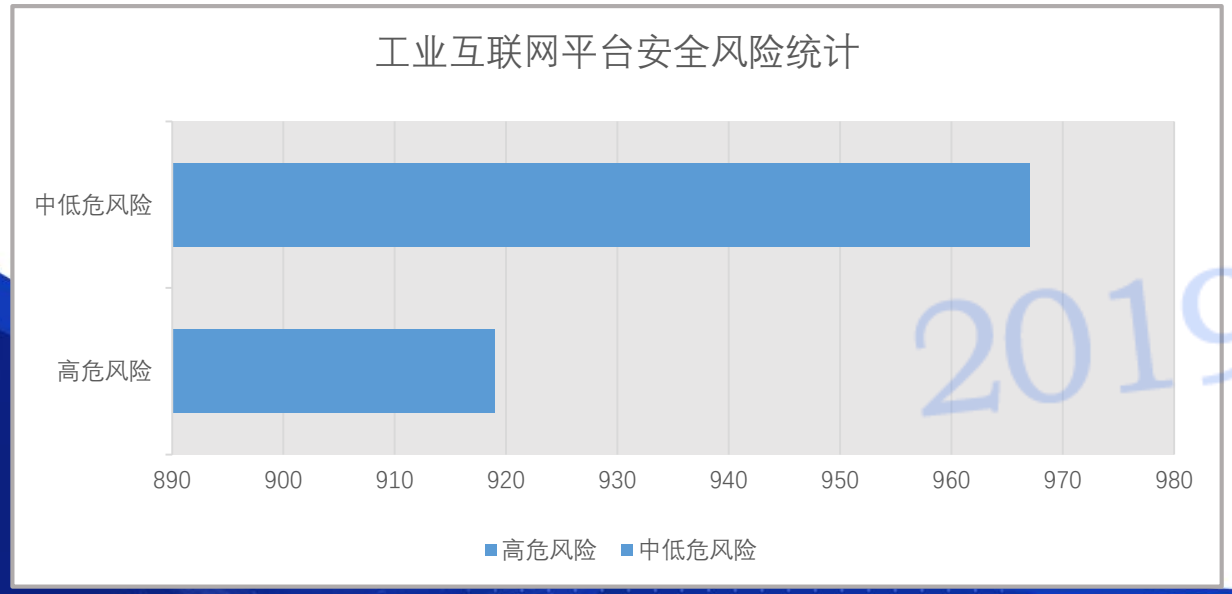
数据来源：360企业安全

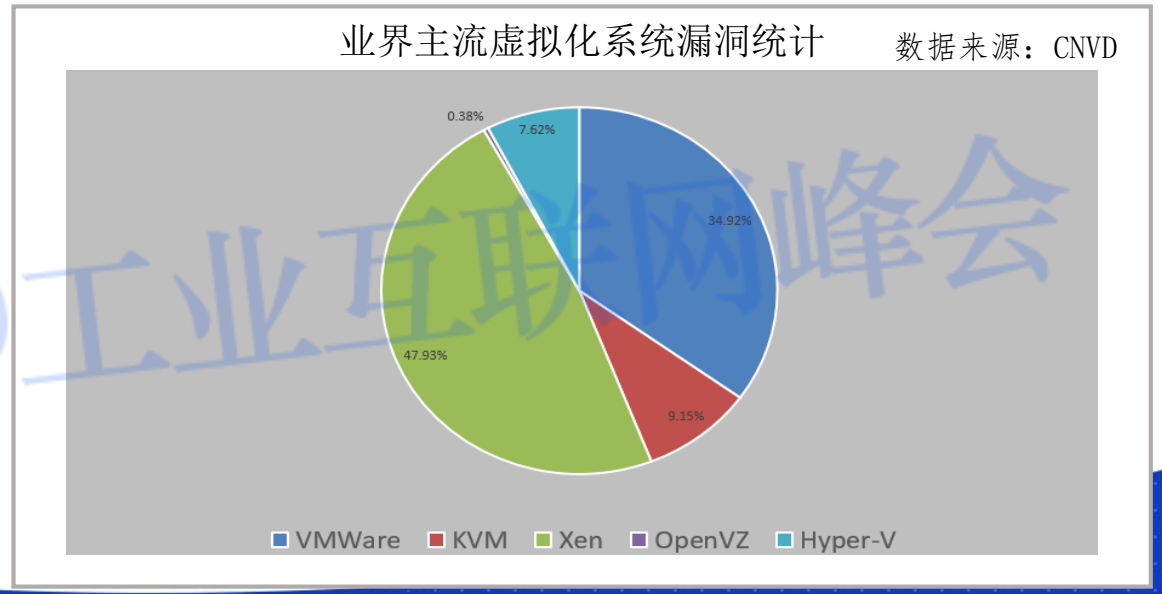


2018：工业互联网平台安全风险

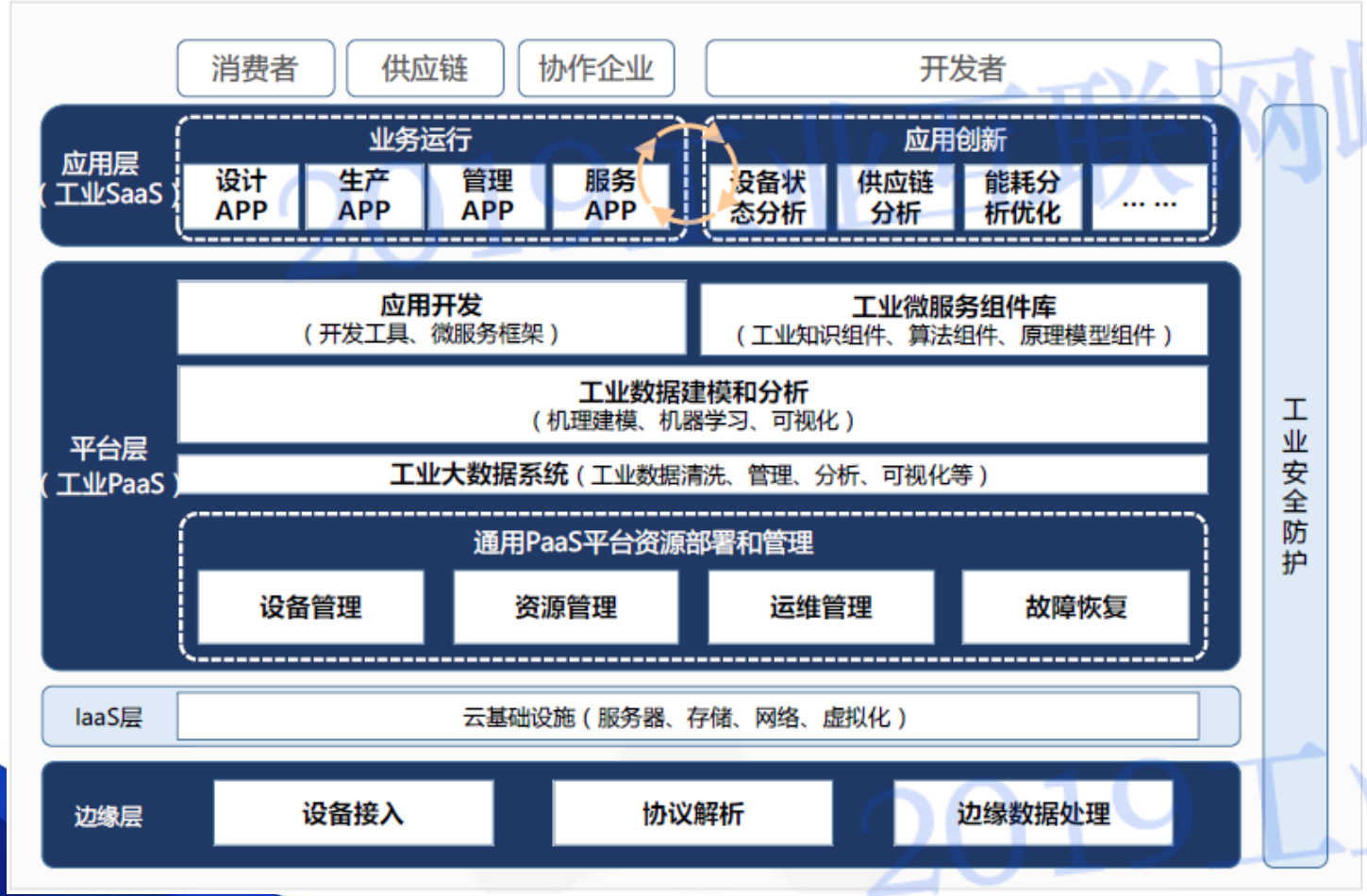








2018：工业互联网平台安全



工业互联网白皮书（2017）

安全管理制度：安全管理制度与安全应急工作有待完善，大部分企业与平台安全投入不足。

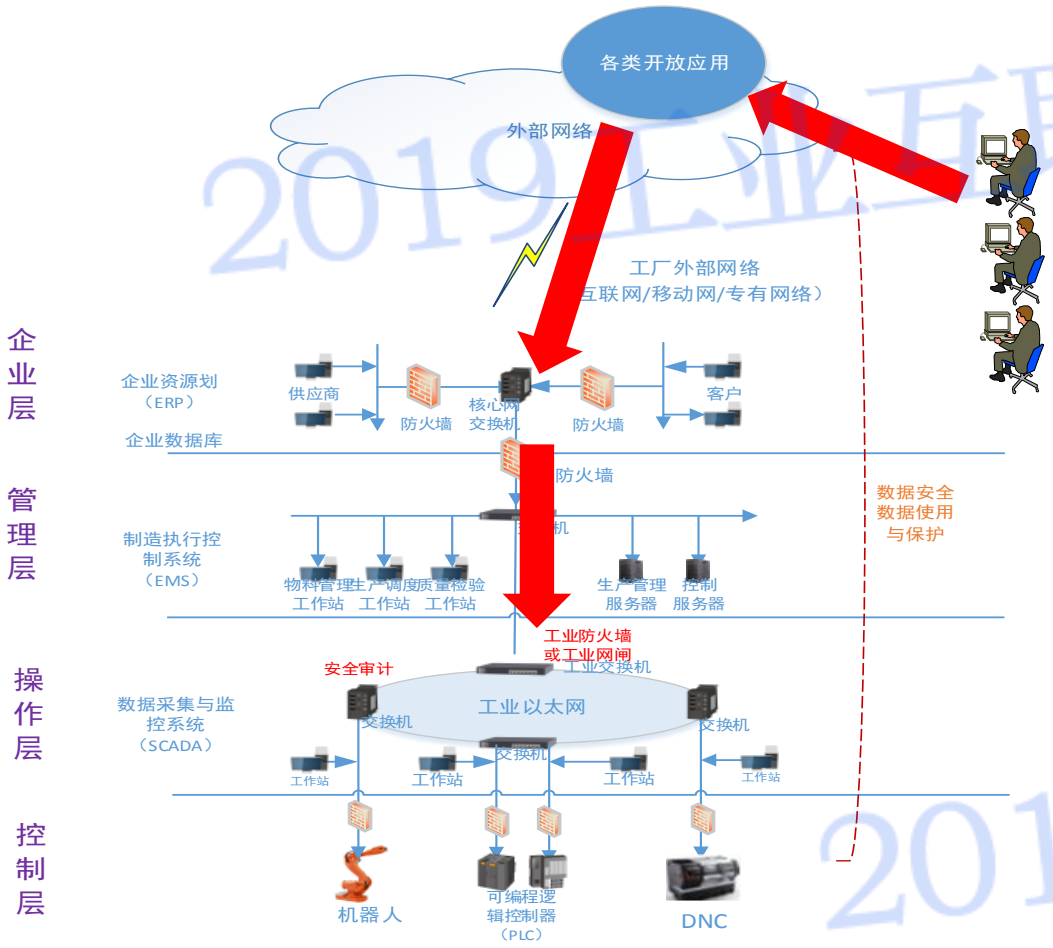
工业SaaS所面临的安全问题： SaaS的运行以互联网为基础，必将面临复杂的信息安全问题，如身份冒用、资料窃取、IP欺骗、端口扫描、数据包嗅探等，可以借助于身份认证、数据加密、入侵检测系统、防火墙、访问控制机制、数据传输控制、网络实时监控以及SQL攻击保护等手段进行安全性增强。

工业PaaS所面临的安全问题：非法窃取或访问软硬件资源、拒绝服务攻击、恶意软件植入等，此外，PaaS层本身需具备完备的安全API（如身份认证、数据加密、权限控制等等）供SaaS层调用，PaaS层安全设计的确实可能会直接造成SAAS层应用服务安全缺陷。

工业IaaS面临的安全问题：设备非法接入、恶意代码注入、会话控制和劫持、弱密码攻击、非法更改或删除平台数据、非法窃取数据或计算资源、虚拟机镜像文件非法访问和篡改、拒绝服务攻击、中间人攻击、SQL注入攻击

边缘层面临的安全问题：物理攻击；资源消耗攻击和拒绝服务攻击；数据窃取、篡改、伪造、重放等攻击；数据完整性与实时性攻击；身份认证强度低

2018：工业APP安全风险

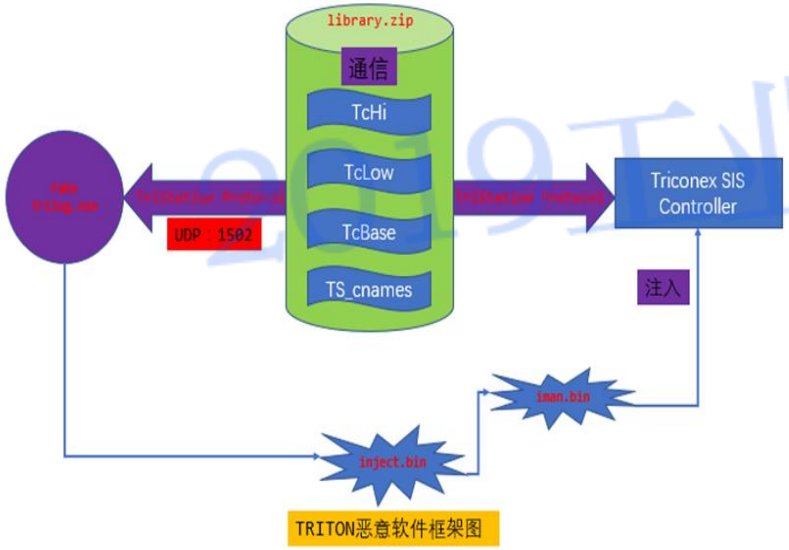


工业APP面临的安全风险

- **传统开放环境中的应用风险，工业APP都可能面对。**由于运行环境和应用组件可能由于在内存结构、数据处理、环境配置、及系统函数等各面方设计原因会导致内存溢出、敏感信息管理及封装和隐藏缺陷等问题，包括会出现其反序列化漏洞等。直接导致上层应用程序调用时出现下面的输入验证、隐藏域、漏缓冲区溢出、跨站请求伪造等问题甚至会造成软件的运行异常、数据丢失等严重问题。
- **安全机制（Security Features）不健全。**即存在身份认证、访问控制、机密性、密码使用和特权管理等方面的缺陷，PaaS层没有足够可用的安全API可以调用。
- **API误用（API Abuse)。**API是调用者与被调用者之间的一个约定，大多数的API误用是由于调用者没有理解约定的目的所造成的。当使用API不当时，也会引发安全问题。
- **时间和状态（Time and State）。**分布式计算与时间和状态有关。线程和进程之间的交互及执行任务的时间顺序往往由共享的状态决定，如信号量、变量、文件系统等。与分布式计算相关的缺陷包括竞态条件、阻塞误用等。
- **代码质量问题（Code Quality）。**低劣的代码质量会导致不可预测的行为。对于攻击者而言，低劣的代码使他们可以以意想不到的方式威胁系统。常见的该类别缺陷包括死代码、空指针解引用、资源泄漏等。

2018重点工业安全事件分析：恶意软件

TRITON



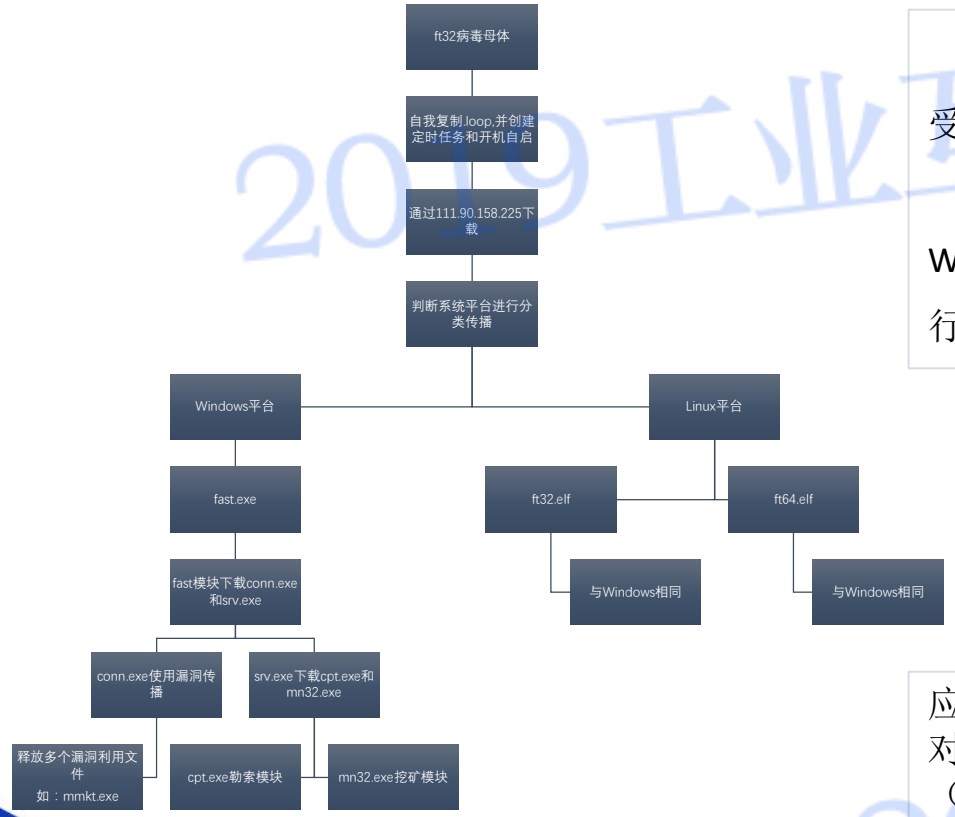
TRITON恶意软件框架图

安全仪表系统（SAFETY INSTRUMENTED SYSTEM简称SIS），又称为安全联锁系统（SAFETY INTERLOCKING SYSTEM），主要为工厂控制系统中报警和联锁部分，对控制系统中检测的结果实施报警动作或调节或停机控制，是工业企业自动控制中的重要组成部分。目前TRITON恶意软件所利用的漏洞主要影响施耐德电气TRICONEX TRICON MP3008 10.0/10.1/10.2/10.3/10.4固件版本,其他型号或者该型号的其他固件版本均不受其影响，鉴于传统工控网络系统升级困难或固件升级缓慢等因素,此恶意软件的影响还是不容小觑。

该恶意软件可以在攻陷SIS系统后，对SIS系统逻辑进行重编程，使SIS系统产生意外动作或是造成SIS系统失效，对工业设备、生产活动以及操作人员的人身安全造成巨大威胁。

- 升级固件到最新、安装对应的漏洞补丁.
- 在技术可行的情况下，将安全系统网络与过程控制信息系统网络隔离开(确保SIS处理隔离的网络中)。
- 利用提供物理控制能力的硬件功能对安全控制器进行编程
- 监控ICS网络流量，检测意外通信流量和其它异常活动。
- 对工业网络统一部署进程管理白名单产品或工业防火墙等工控安全产品。

2018重点工业安全事件分析：Lucky病毒



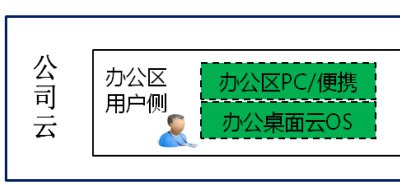
2018年11月，某石油公司采油厂感染了一款名为Lucky的勒索病毒，导致业务系统受到感染影响了生产。

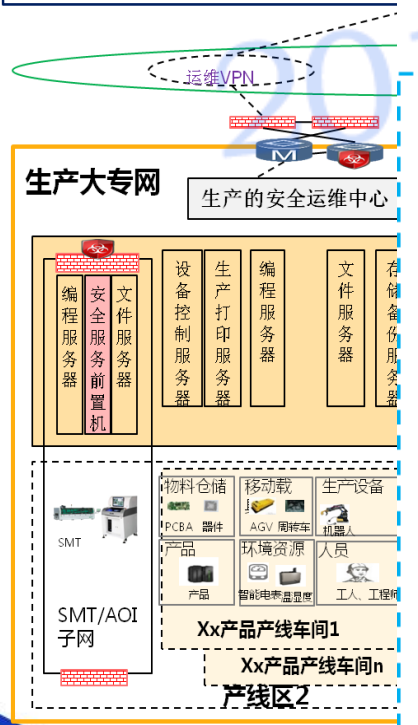
该病毒传播能力极强，可运用多种漏洞组合进行传播，同时支持感染Linux和Windows操作系统，加密文件采用高强度加密RSA+AES算法，并且还会消耗主机资源进行挖矿。

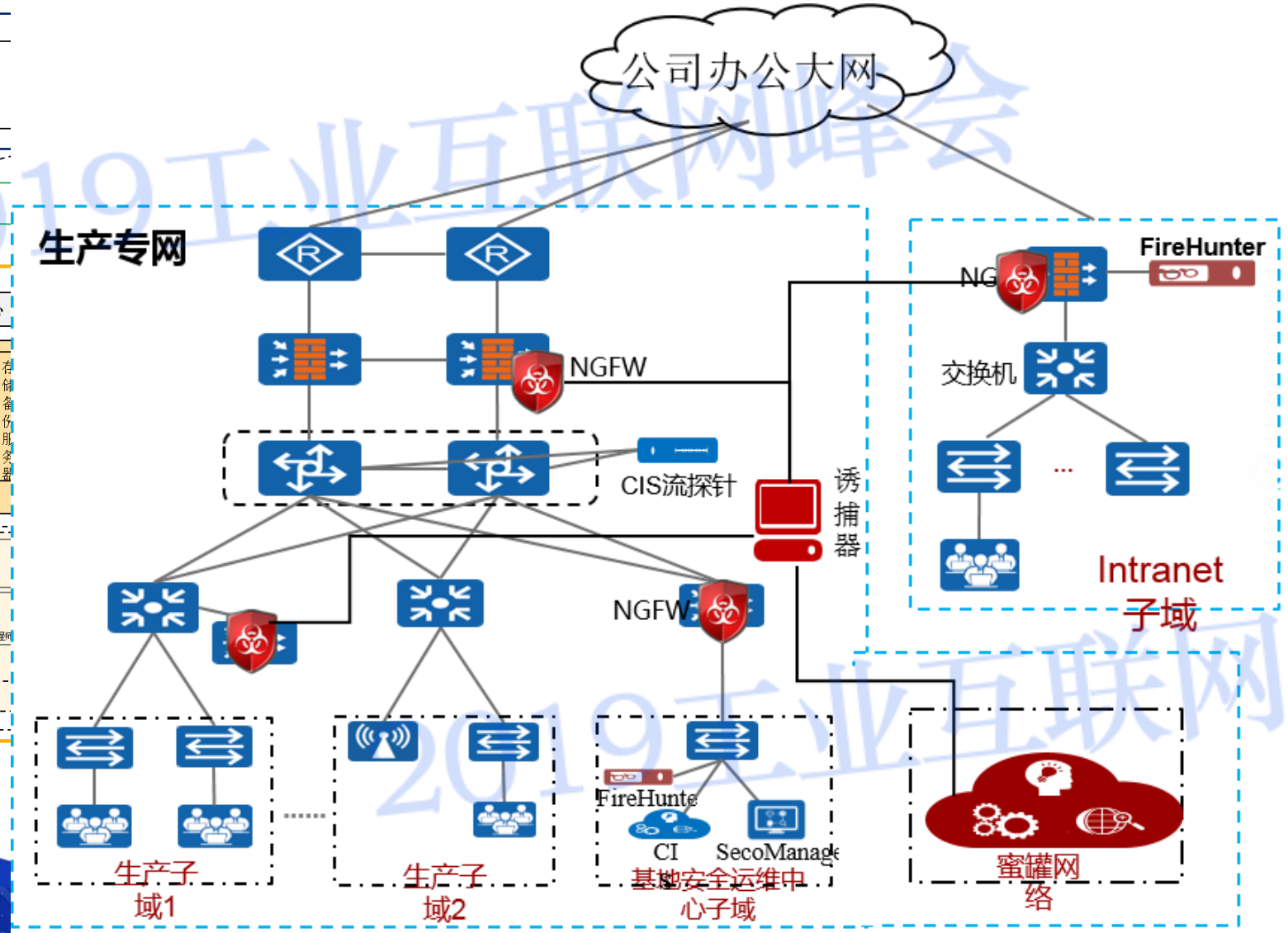
SpringDataCommons组件远程代码执行漏洞（CVE-2018-1273）
Tomcat web管理后台弱口令爆破
系统账户弱口令爆破
JBoss反序列化漏洞(CVE-2013-4810)
JBoss默认配置漏洞(CVE-2010-0738)
Weblogic WLS 组件漏洞（CVE-2017-10271）
Apache Struts2远程代码执行漏洞（S2-045）
Apache Struts2远程代码执行漏洞（S2-057）
Windows SMB远程代码执行漏洞（MS17-010）

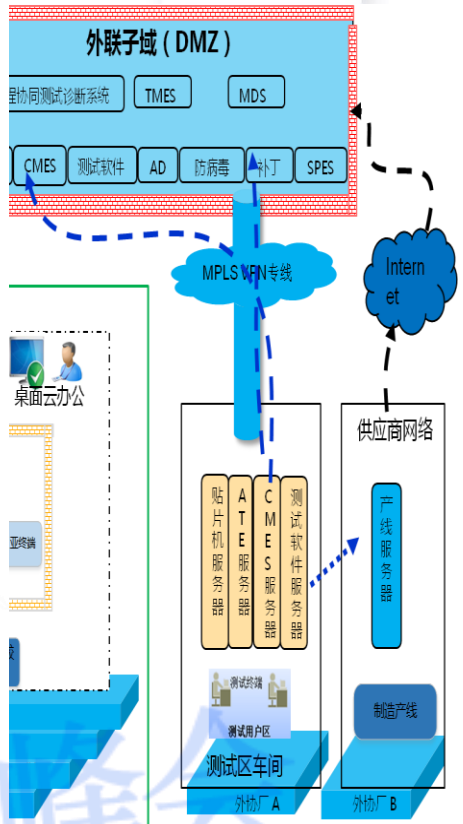
应急方案建议：
对于未中病毒的机器应采取以下措施避免受到感染：
（1）给系统和应用程序打全补丁，断绝木马传播途径。
（2）关闭局域网共享，以及非常用端口，避免遭受感染。
对于已中毒的机器应该采取以下措施阻止病毒继续传播：
（1）隔离感染主机，关闭所有网络连接，防止横向传播。
（2）使用杀毒软件全盘查杀木马。
3. 修补对应的系统或应用漏洞。

2018工业互联网安全案例：电子制造

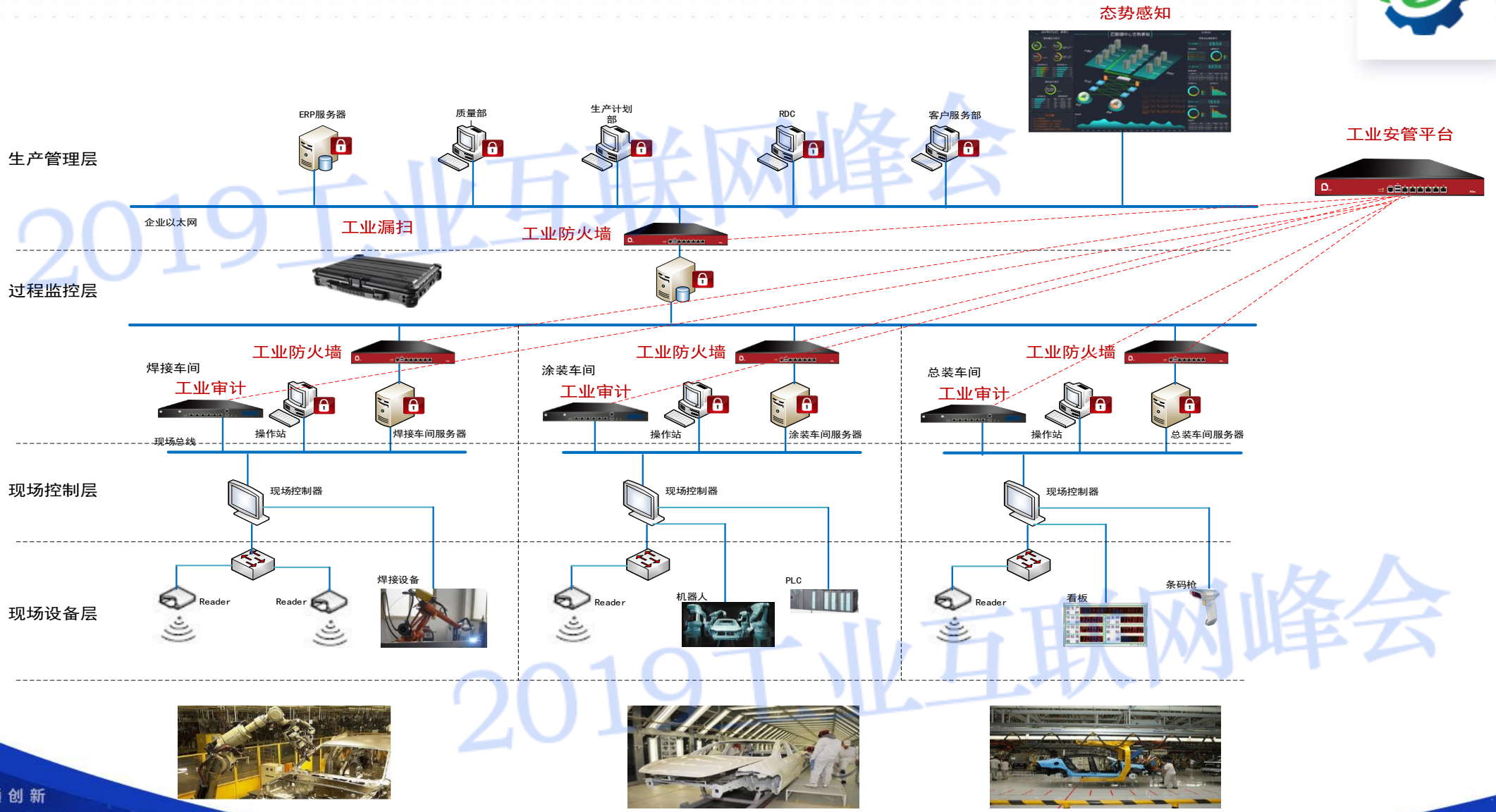








2018工业互联网安全案例：汽车制造



2019：工业互联网安全发展展望

1. *主动式、智能化的威胁检测与安全防护技术将不断发展*
2. **自主可控的工业互联网安全产品和服务体系发展和完善**
3. *工业互联网安全标准将逐步推出，并引导安全产业发展*
4. **工业互联网平台内生安全防御成为未来平台发展的重点**
5. *设备上云、数据采集与互通逐步推进，并形成安全方案*
6. **跨部门、跨行业、跨平台信息共享和联动处置机制推进**

感谢：编写组成员

《2018中国工业互联网安全报告》编写组成员：

1.	北京六方云科技有限公司	李江力、刘苏
2.	中国信息通信研究院	田慧蓉、刘晓曼
3.	360企业安全集团	陶耀东、崔君荣
4.	北京启明星辰信息技术有限公司	李转琴、刘建帅
5.	电子信息产业集团第六研究所	卢凯
6.	中国移动	张峰、马洁
7.	北京恒安嘉新科技有限公司	崔婷婷
8.	海尔集团	张海港

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

Thanks

主讲人：李江力

2018年2月22日

智联赋能　融通创新

2019 工业互联网峰会
INDUSTRIAL INTERNET SUMMIT 2019