北京航空航天大學
BEIHANG UNIVERSITY

SafSec-IoT
物联网系统的安全问题探讨

●物联网发展 ●安全实例分析 ●安全威胁与挑战 ●应对建议

吴际
北京航空航天大学计算机学院

提纲
Agenda

01 物联网的发展

02 物联网安全实例分析

03 物联网的安全挑战

04 致力于物联网安全的建议


01
物联网的发展

一、物联网的发展

早在1990年施乐公司的网络可乐贩售机(Networked Coke Machine)就已经初步试水物联网应用。

- 1998年，美国麻省理工学院创造性地提出了当时被称作EPC系统的物联网构想；
- 1999年，建立在物品编码、RFID技术和互联网的基础上，美国Auto-ID中心首先提出了物联网的概念；
- 2005年11月17日，在WSIS会议上，国际电信联盟发布了《ITU互联网报告2005:物联网》；
- 2009年，由IBM提出智慧地球开始发展，2010年中国提出感知中国，并且首次提出物联网的中文名称。

1990
施乐公司的网络可乐贩售机最早实践

1995
比尔盖茨在《未来之路》中提及物联网

1999
MIT建立“自动识别中心”，阐明了物联网的基本含义

2003
美国《技术评论》提出传感网络技术将是未来改变人们生活的十大技术之首。

2004
日本总务省提出u-Japan计划，希望建设一个任何物体和人均可连接的泛在网络社会。

2005
国际电信联盟在WSIS上发布《ITU互联网报告2005：物联网》，引用了“物联网”概念。

2006
韩国确立u-Korea计划，旨在建设智能型网络和各种新型应用。

2008
为促进科技发展，寻找经济新的增长点，各国政府将目光放在了物联网上。

2009
欧盟执委会发表欧洲物联网行动计划，描绘了物联网技术的应用前景，促进了物联网的发展。

IBM首席执行官彭明盛首次提出“智慧地球”概念，建议政府投资新一代的智慧型基础设施。

中国无锡先建立“感知中国”研究中心，物联网被正式列为国家五大新兴战略性产业之一。

一、物联网的发展

互联互通

使用Internet来连接“物”

物物通信

“物”可自动识别，并能相互通信M2M

异构

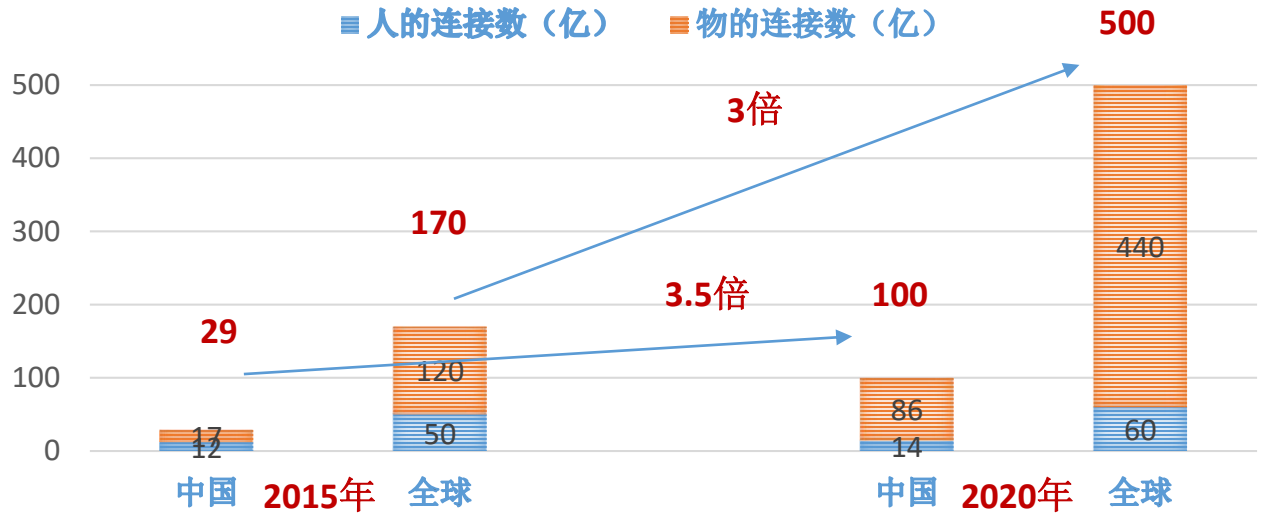
多种物理实体、多种状态

大规模并行

各种实体同时在发生状态变化和进行计算通信

一、物联网的发展

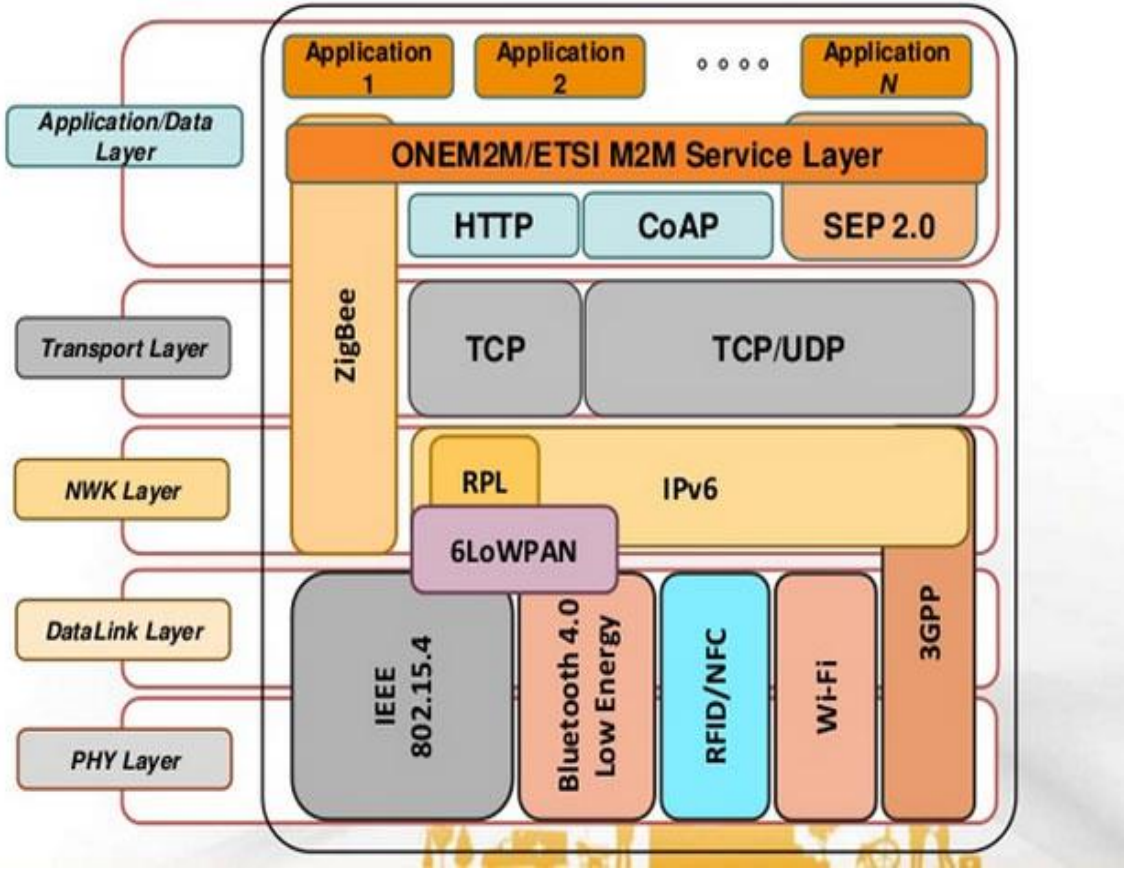
到2020年，中国将达百亿级物联网连接，产业链市场空间1万亿人民币（数据来源：麦肯锡等），至2025年，将是5-10万亿人民币。



智能家居、智能楼宇、公共事业（如抄表）、智慧城市和物流追踪这五大领域将是应用推广的重点。

5G和大数据助力IoT发展

- 丰富的协议栈，可适应多种通信场景
- 5G技术使得可以在端节点部署更强的计算能力和存储能力
- 大数据使得可以管理更多的端节点，并提供更好的BI服务
- IoT将开始由生活领域进入生产控制领域
  - 更高的实时性要求
  - 更高的安全性要求
  - 更高的智能处理要求



两种智能计算形态将并存

- **集中式智能计算** – 物端提供基础的识别能力，通过无线连接到云端，在云端集中进行数据处理与智能计算
  - 轻的端计算和存储能力
- **分布式智能计算** – 物端开展计算和智能处理，云端后期数据处理
  - 重的端计算和存储能力

02

物联网安全实例分析

终端不安全

北京时间2016年10月21 日晚间，北美地区若干重要网站无法正常访问，包括 twitter、 paypal、github等。本次安全事件是由美国知名网络域名服务提供商Dyn遭受到强力的DDoS攻击所致。

Flashpoint公司已经确认Mirai僵尸网络参与了该DDoS攻击。Mirai是一种主要感染IOT设备的僵尸程序，该僵尸程序在源码公开后，被黑客快速利用并扩散形成了大量的僵尸网络。

Mirai病毒让德国超90万台路由器遭殃。全球已有130万台以上的监控探头和摄像机等物联网（IoT）设备感染了Mirai病毒。

二、物联网安全实例分析

数据不安全

2017年3月，Spiral Toys旗下的CloudPets系列玩具遭遇数据泄露，敏感客户数据库受到恶意入侵，导致包括玩具录音、MongoDB数据、220万账户语音信息等窃取。

Spiral Toys公司使用Amazon托管服务存储客户的个人资料信息。只需要了解文件的所处位置，任何人都能够轻松获取到该数据。

2015.11，香港玩具制造商VTech遭遇入侵，近500万名成年用户和20万儿童的个人信息外泄。

2015.12，美泰公司生产的联网型芭比娃娃中存在的漏洞可能允许黑客拦截用户的实时对话……

通信协议不安全

物联网安全研究公司Armis在蓝牙协议中发现了8个零日漏洞，将影响超过53亿物联网设备。利用这些蓝牙协议漏洞，Armis发起BlueBorne攻击，可完全接管支持蓝牙的设备，传播恶意软件。

BlueBorne攻击可以服务于任何恶意目的，例如网络间谍、数据窃取、勒索攻击，甚至利用物联网设备创建大型僵尸网络。BlueBorne攻击具有穿透安全网络的能力。

NB-IoT的COAP协议目前仍然采用明文传输方式！

二、物联网安全实例分析

终端不安全导致安全事故

智能终端设备在安全防护方面的投入普遍不足。

2012 年，黑客可以在距离目标 50 英尺的范围内侵入心脏起搏器，并释放 830V 电压致人死亡。

2013 年，在黑客大会上演示如何通过攻击软件使高速行驶的汽车突然刹车。

2015 年，在Geekpwn 大会上，黑客演示了破解智能家居的过程。

GeekPwn选手曝主流智能门锁安全漏洞

2017年05月17日 16:25:38 来源： 中国网

安全极客在无需物理接触、无需拆解门锁的情况下获得果加互联网智能门锁所有的开锁密码，这是2017国际安全极客大赛GeekPwn上出现的一幕。值得一提的是，此次被选手攻破的果加智能门锁是目前中国使用量最大的智能锁品牌，被多个公寓品牌所使用。

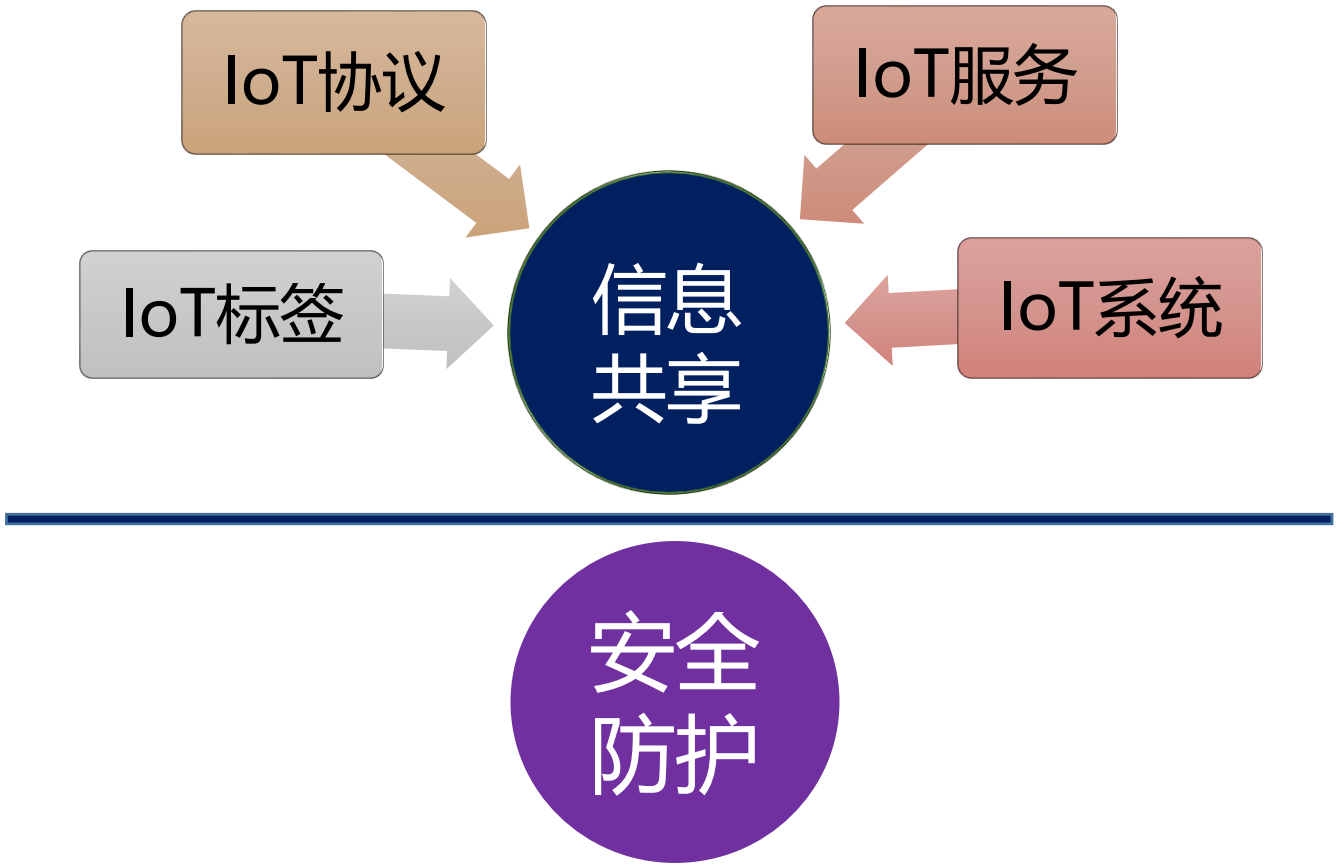
（百度安全实验室选手谢海阔、黄正）

两名黑客，打开了数百万个酒店房间

脑极体 • 2018-05-05 08:22

摘要： “漏洞即是武器”，这个网络常识正在走进我们的生活。

为什么IoT系统安全问题层出不穷?



IoT安全内涵

- Security与Safety正在融合
  - 智能汽车
  - 智能家居
  - 智慧工厂
- Security关注数据
  - 端节点
  - 网络
  - 中心节点
- Safety关注物理动作后果
  - 控制器

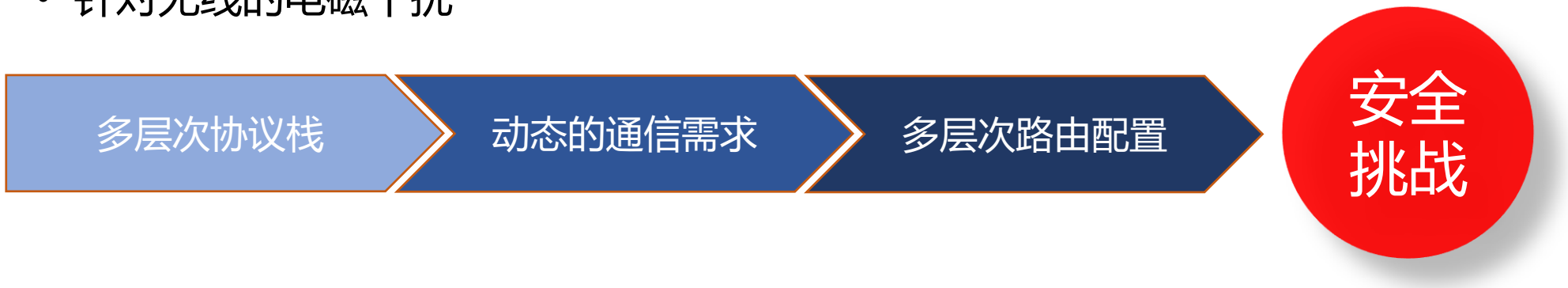

03
物联网的安全挑战

IoT端节点的安全挑战

- 连接端节点，窃取节点数据或者从IoT系统传输来的数据
- 入侵端节点，窃取节点数据并伪造数据来破坏IoT系统
- 入侵端节点，获得端节点对物理实体的控制权
- 物理或电子方式摧毁端节点，获得物理实体控制权并降低IoT系统的感知控制能力

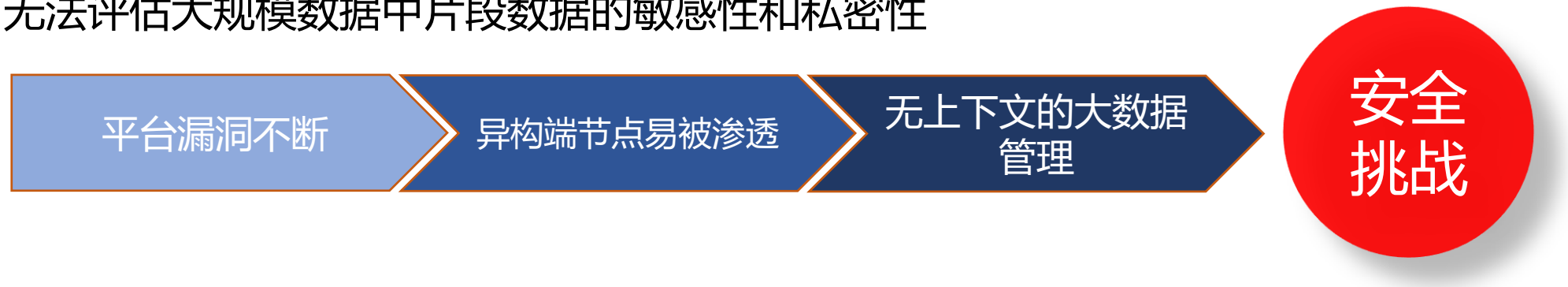
IoT网络的安全挑战

- 易被窃听消息
  - 无线方式
  - 网络监听
- 易被篡改路由
  - 跨越多层网络
- 带宽易被消耗
  - 无法甄别通信需求的真实性
- 通信稳定性已被干扰
  - 针对无线的电磁干扰



IoT中心节点的安全挑战

- DDOS
- 操作系统、服务器容器、数据库的漏洞
- 难以甄别端节点数据的完整性
- 难以确认端节点数据的合法性
- 难以获悉端节点状态的有效性
- 无法评估大规模数据中片段数据的敏感性和私密性



04

致力于物联网安全的建议

从系统开发的角度

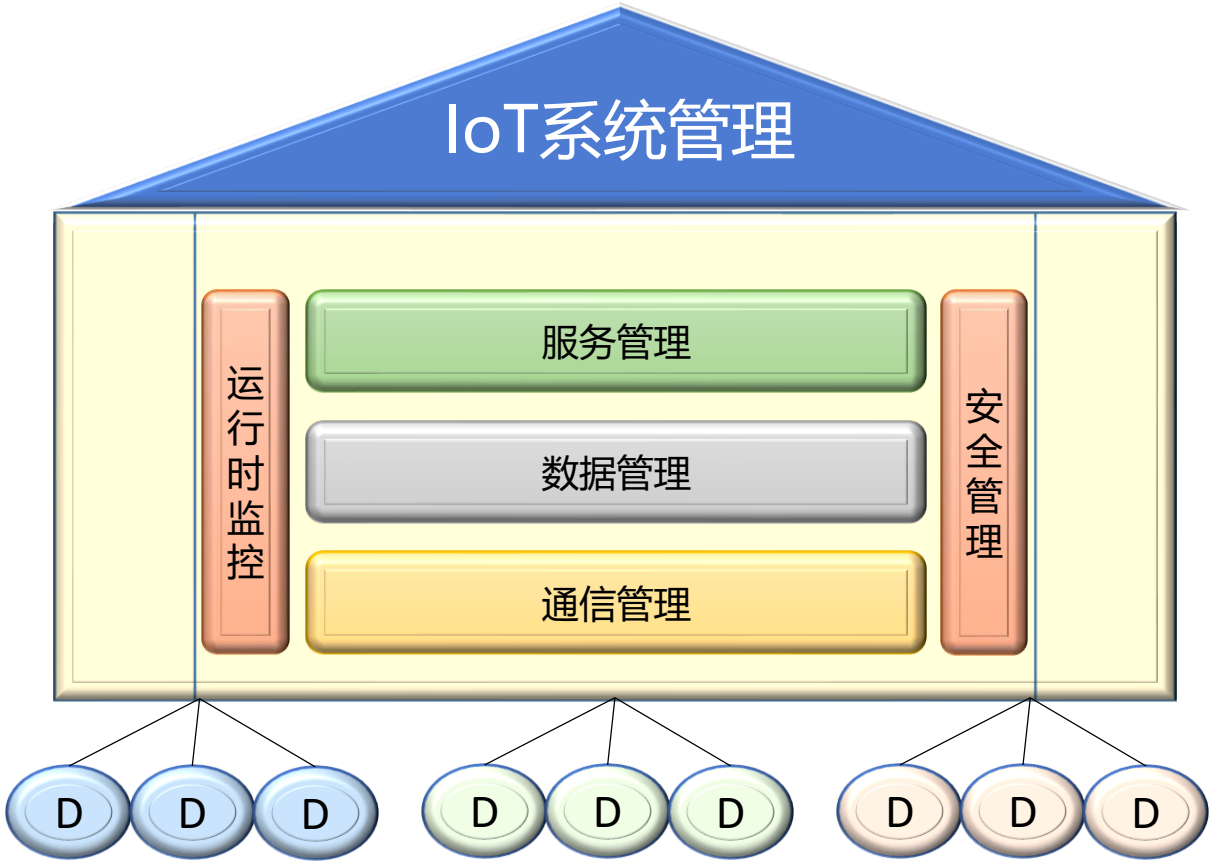
- 应用安全工程
  - Security engineering (ISO 17799)：识别vulnerability/threat，形成安全需求
  - Safety engineering (IEC 61508)：识别hazard/risk，形成安全需求
- 设计和实现全面的安全策略
  - 数据处理与通信
  - 资源访问控制
  - 加密
- 开展持续的测试
  - 端节点
  - 网络协议
  - 服务中心
- 建立安全问题库
  - 漏洞/危害管理
  - 固件升级管理
  - 防护措施管理

Safety	Security
Perform a *Hazard* Analysis	Perform a *Vulnerability* Analysis
Assess the risks associated with each *hazard*	Assess the risks associated with each vulnerability
Classify the *hazard* using Industry specific methodology	Classify the *vulnerability* using Industry specific methodology
Define *Safety* Requirements to mitigate risk	Define *Security* Requirements to mitigate risk

从系统运维的角度

- 明确端节点的数据完整性、合法性规则
- 访问控制
  - 端节点
  - 网络
  - 服务中心
- 运行时行为监测与监控
  - IDS
  - 异常状态检测
- 制定明确的安全管理策略

综合化的IOT系统架构



总结

- IoT将成为技术熔炉
  - 5G+边缘计算+大数据+AI
- 随着IoT应用的拓展，IoT面临着严峻的安全挑战
- IoT的security和safety还将继续融合
- 需要在开发阶段对安全问题进行分析，开展针对性设计和实现
- 需要综合化的系统平台来管理IoT系统技术栈的安全

微信（吴际）

电子邮箱：
wuji@buaa.edu.cn

感谢各位的聆听！