
# 工业物联网应用安全防护

汇报人：深圳中科卫士　　日期：2018.12.4

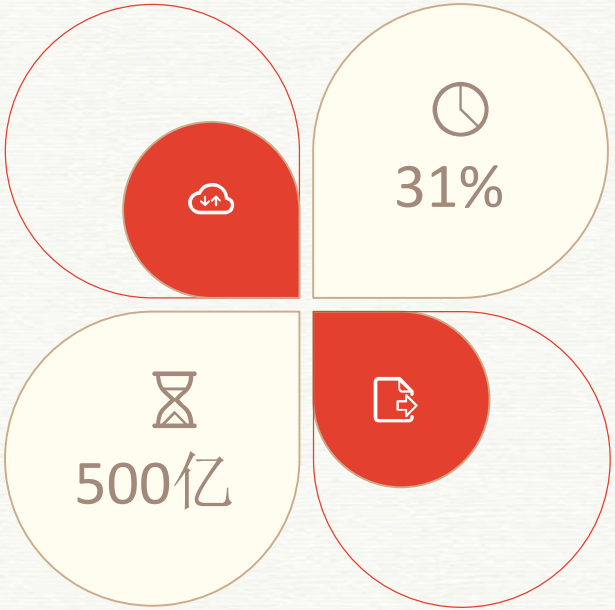
# “万物互联网”成为新一代IT环境重要组成部分

## 广覆盖

物联网技术及产品越来越多用于物流、交通、安防、能源、医疗、建筑、制造、家居、零售等行业，正在从个人消费向工业控制领域升级。

## 泛应用

具有“全面感知、可靠传递、智能控制、数据融合”等特点，奠定了物联网泛应用的基础，预计到2020年，中国智能设备连接数将达100亿，全球将突破500亿。.




## 快增长

数据预测显示，未来三年物联网设备及连接数将以31%的年复合增长率快速发展，随着5G技术的即将商用，物联网的发展将会得到进一步提速。

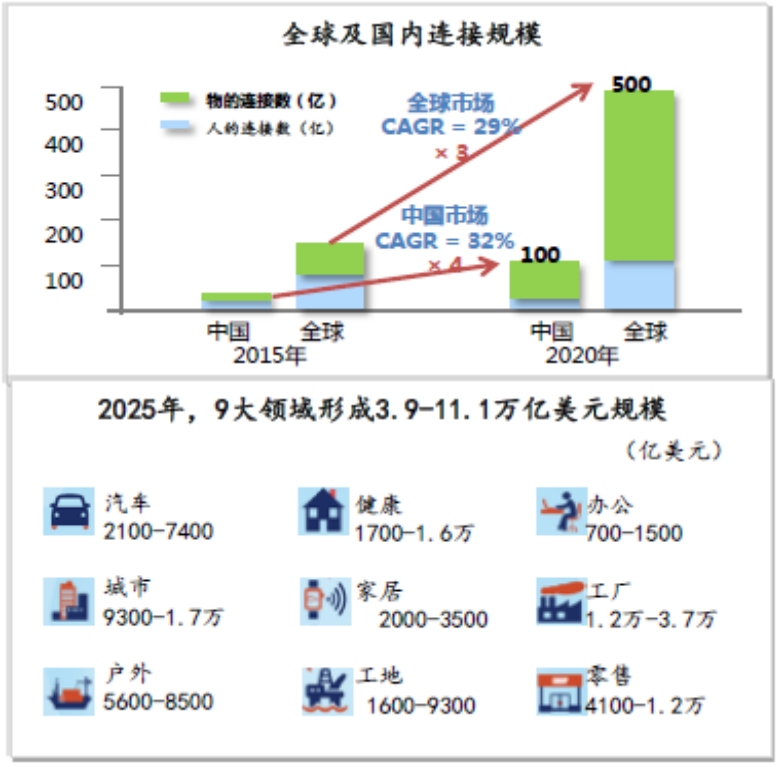
## 新挑战

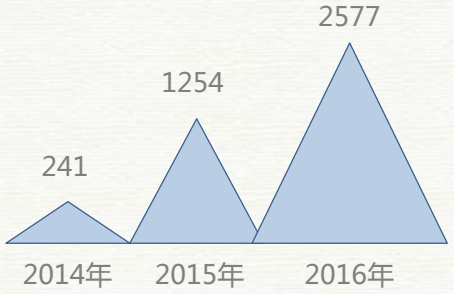
有别于传统网络环境，物联网面临新的安全威胁，从感知层到应用层对现有的技术手段和管理方式都提出了新的挑战。

*资料来源：GSMA、各电信运营商年报、麦肯锡研究报告*

# “大连接” 正面临前所未有的安全挑战

## 物联网及应用爆发式增长，安全威胁随之而来




**国内及香港企业信息安全事件平均数量** （普华永道）

**工业物联网典型安全事件**


据统计，2015-2016年，全球针对物联网设备的网络攻击次数暴增969%，涉及物联网的信息安全事件数量同比上升18%；

Gartner预计，到2020年，针对IoT设备的攻击将占到企业遭遇攻击总数的25%；

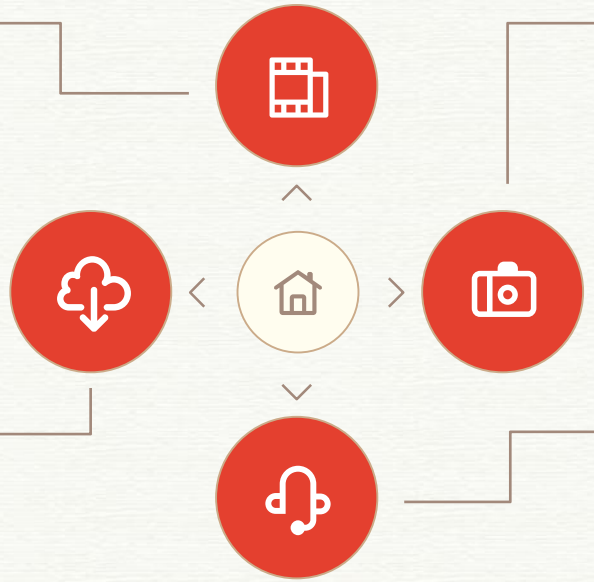
# 工业物联网安全威胁概况

**01网络接入**

网络接入是IIOT生态构建基础，涉及物联网设备感知、接入，横跨多个网元及系统，易被干扰、DDOS攻击。

**02数据传输**

承载物联网及控制系统的关键数据，易被劫持、监听、篡改、仿冒等，导致敏感隐私数据泄露或重大商业损失。



**03智能设备**

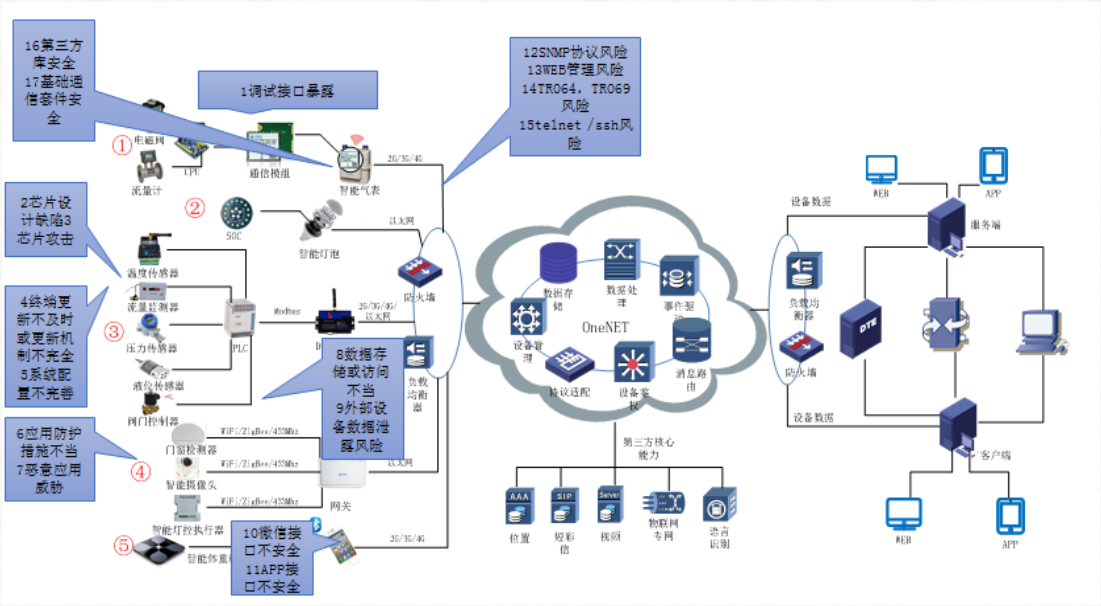
构成IIOT的网元设备，由于厂商众多、目标分散、防御水平良莠不齐等原因，易被攻击者单点突破。

**04应用系统**

IIOT的业务承载，也是整个体系内最易被攻击利用的点，存在代码、数据、业务、通讯等多方面安全风险。

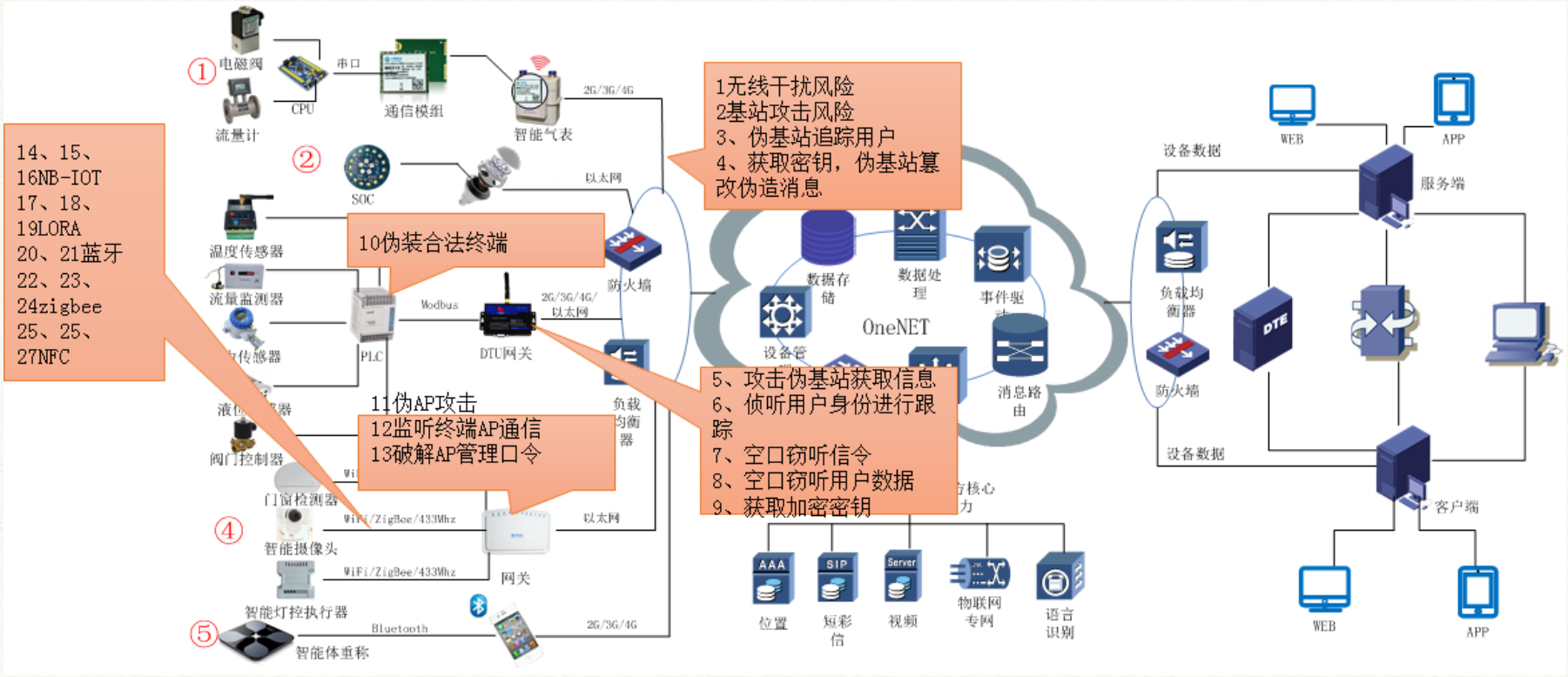
# 工业物联网安全风险及威胁-网络接入


泛在感知网络技术 建立服务于智能制造的泛在网络技术体系，为制造中的设计、设备、过程、管理和商务提供无处不在的连接、控制、服务。

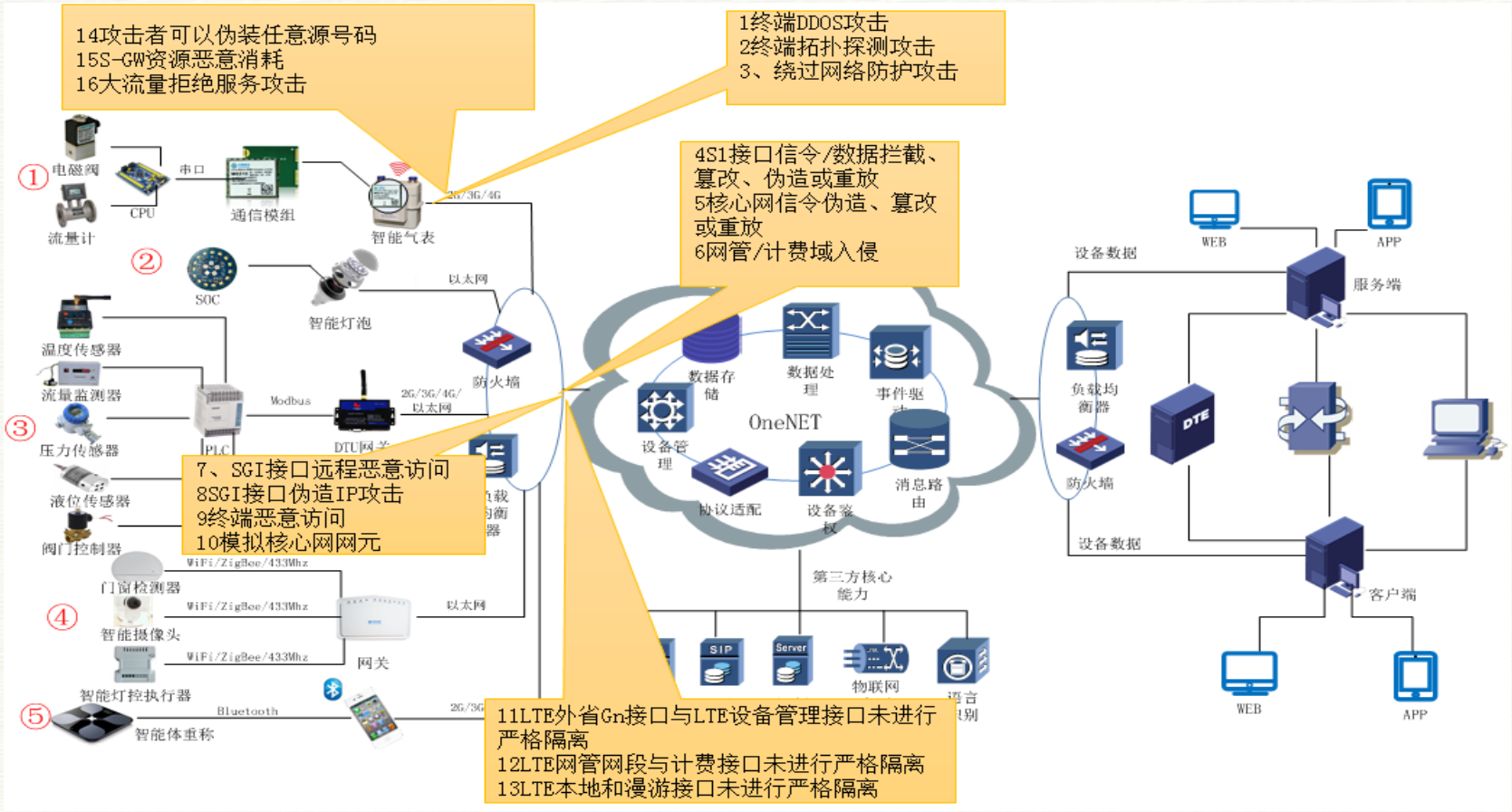



工业物联网安全网络安全威胁来自各个层面，任何一个环节的防护缺失都可能导致整个系统遭受致命攻击。

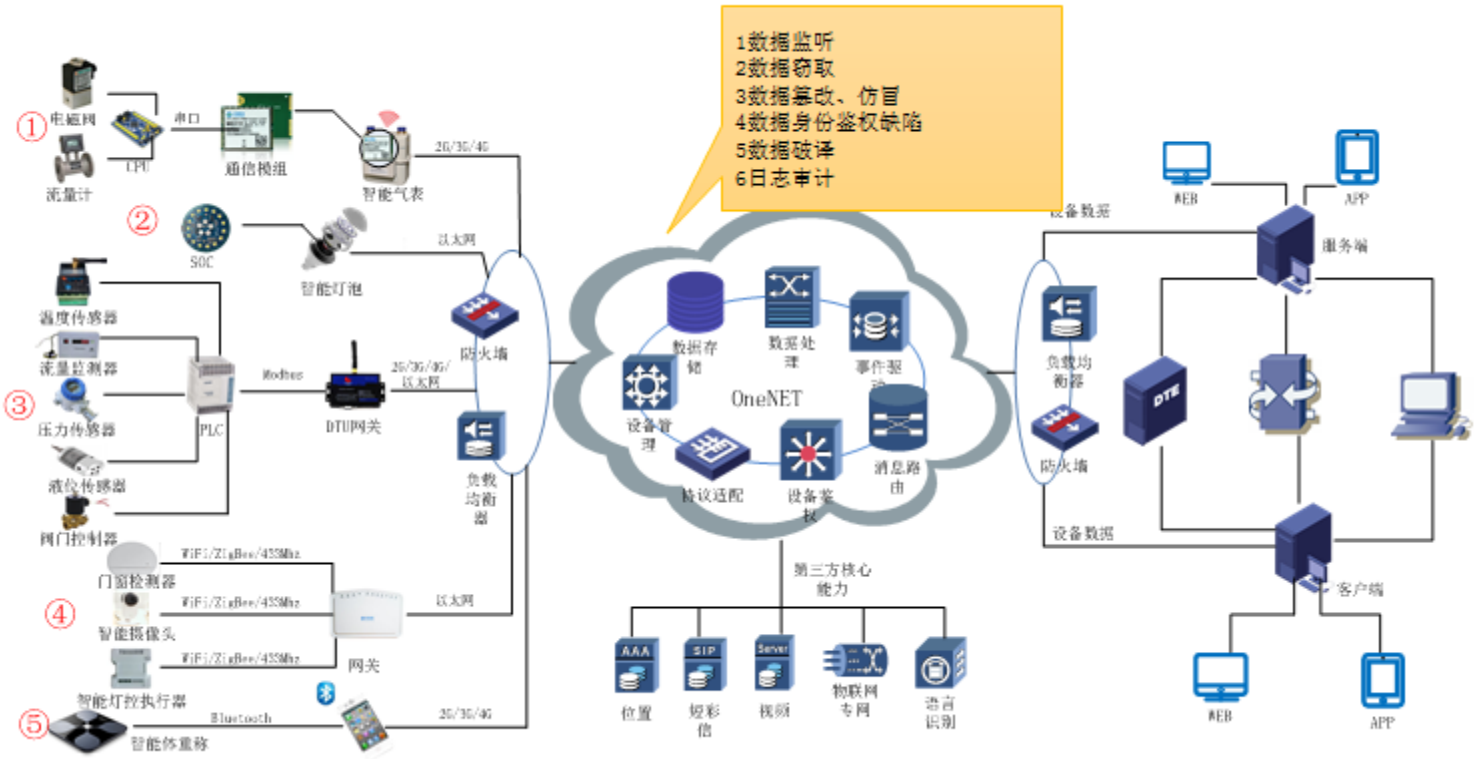
# 工业物联网安全风险及威胁-网络边界



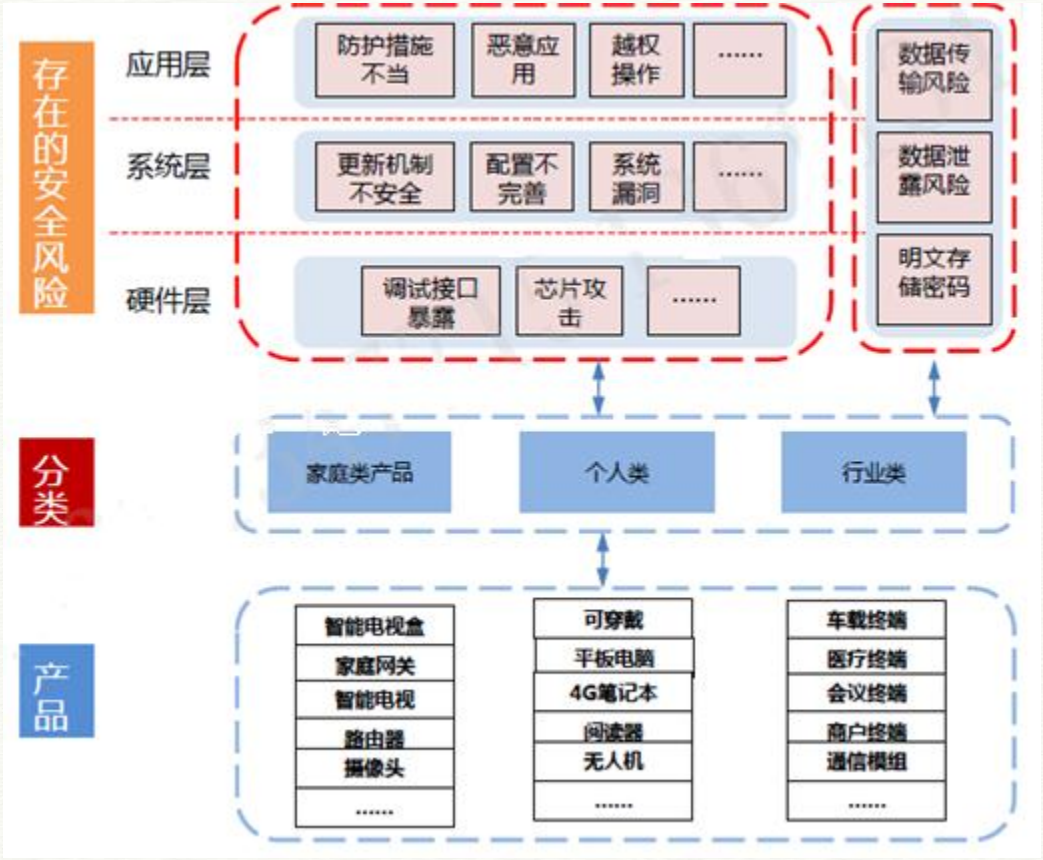
# 工业物联网安全风险及威胁-核心承载



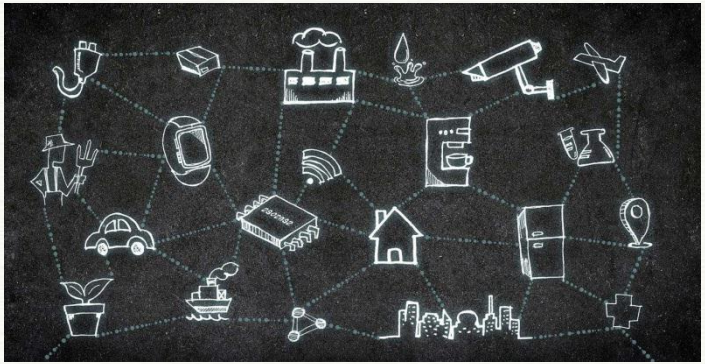
# 工业物联网安全风险及威胁-数据传输



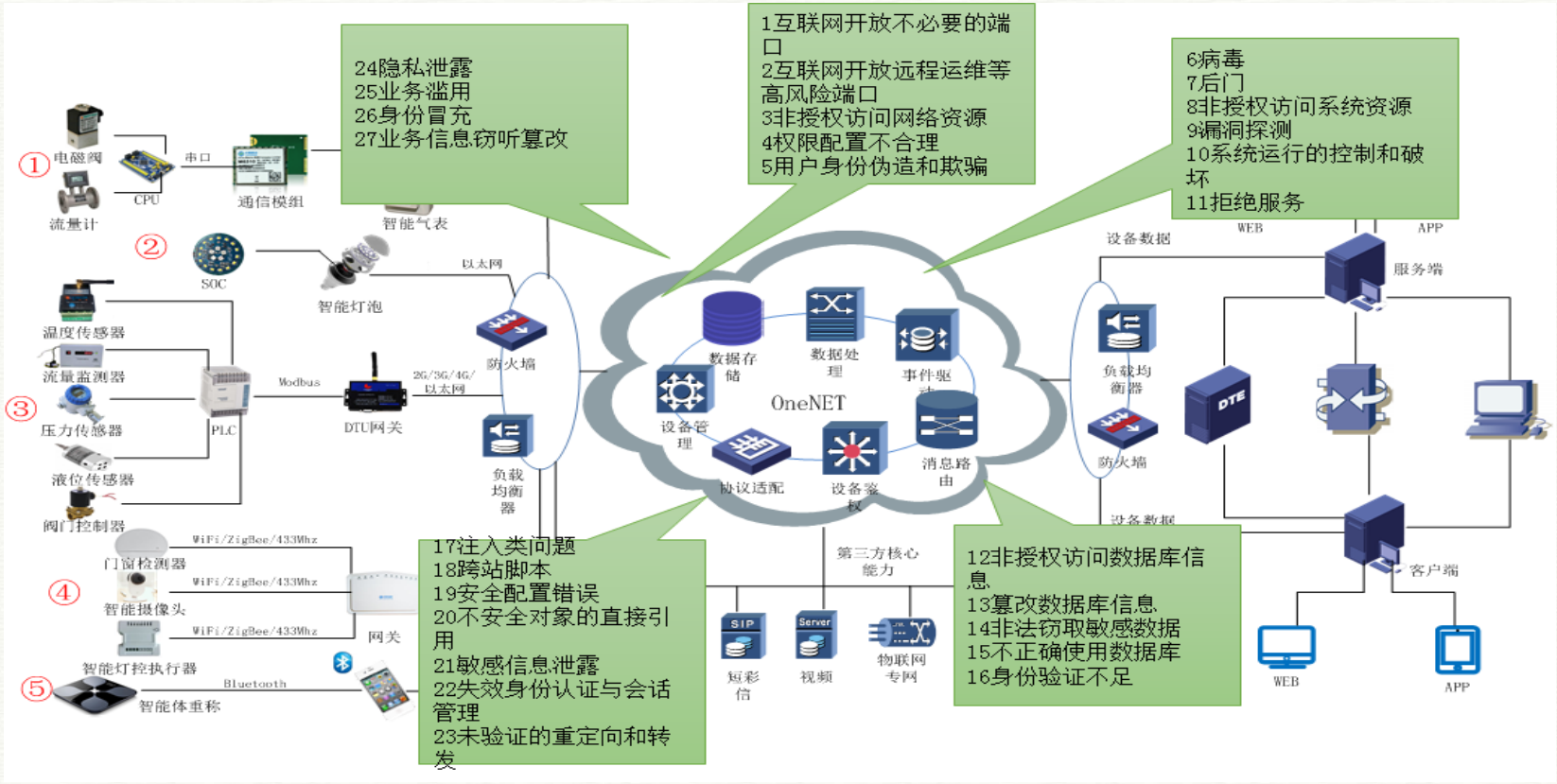
# 工业物联网安全风险及威胁-智能设备




- 智能硬件及应用是工业物联网基础，期面临的安全风险分为**通用和个性化**两部分，通用是指所有智能硬件都可能面临的共同的风险，个性化是指不同类别产品在其应用场景下面临的特有的风险。
- 智能设备内置系统及应用具有形态多样、场景丰富、受众分散等特点，是整个体系链内最易被攻击的环节之一。



# 工业物联网安全风险及威胁-应用系统




# 感谢聆听！