（物联网）物联网定义

20XX 年 XX 月

物联网定义

物联网(InternetofThings)指的是将无处不于（Ubiquitous）的末端设备（Devices）和设施（Facilities）,包括具备“内于智能”的传感器、移动终端、工业系统、楼控系统、家庭智能设施、视频监控系统等、和“外于使能”(Enabled)的，如贴上 RFID 的各种资产（Assets）、携带无线终端的个人和车辆等等“智能化物件或动物”或“智能尘埃”（Mote）,通过各种无线和/或有线的长距离和/或短距离通讯网

Web4.0:物联网

络实现互联互通（M2M）、应用大集成（GrandIntegration/MAI）、以及基于云计算的 SaaS 营运等模式，于内网（Intranet）、专网（Extranet）、和/或互联网（Internet） 环境下，采用适当的信息安全保障机制，提供安全可控乃至个性化的实时于线监测、定位追溯、报警联动、调度指挥、预案管理、远程控制、安全防范、远程维保、于线升级、统计报表、决策支持、领导桌面（集中展示的 CockpitDashboard)等管理和服务功能，实现对“万物”(everyThing)的“高效、节能、安全、环保”的“管、控、营”壹体化 TaaS 服务。

笔者预计，物联网及其关联的 TaaS 业务，于基于 SemanticWeb 技术的 Web3 .0 基础上，将构成 Web4 .0 的主体[1]。

物联网发展三个阶段

1.初级阶段：已存于的壹些各行业基于各种行业数据交换和传输标准的连网监测监控，俩化融合[2]引等 MAI 应用系统；

2. 中级阶段：于物联网理念推动下，基于局部统壹的数据交换标准实现的跨行业、跨业务综合管理大集成系统，包括壹些基于 SaaS 模式和“私有云”的 M2M 营运系统;

3. 高级阶段：基于物联网统壹数据标准， SOA,WebService,云计算虚拟服务的 onDemand 系统，最终实现基于“公有云”TaaS:“ThingasaService” 。

DCM 三层架构

物联网 DCM 三层架构

Devices—末端设备，资产，或子系统

Connect—有线或无线通讯连接系统

Manage—总控管理和应用系统

物联网四大支柱业务群

1 .RFID: 电子标签属于智能卡的壹类，物联网概念是 1998 年 MITAuto-ID 中心主任 Ashton 教授提出来

物联网 4 大业务群

的， RFID 技术于物联网中重要起“使能”（ Enable)作用；

2.传感网：借助于各种传感器，探测和集成包括温度、湿度、压力、速度等物质现象的网络，也是温总理“感知中国”提法的主要依据之壹；

3 .M2M ：这个词国外用得较多，侧重于末端设备的互联和集控管理，

X-Internet ，中国三大通讯营运商于推 M2M 这个理念；

4.俩化融合：工业信息化也是物联网产业主要推动力之壹，自动化和控制行业是主力，但目前来自这个行业的声音相对较少。

物联网四大支撑网络

因“物”的所有权特性，物联网应用于相当壹段时间内均将主要于内网（Intranet)和专网（Extranet)中运行，形成分散的众多“物连网”，但最终会走向互联网（ Internet)，形成真正的“物联网”，如GooglePowerMeter。

物联网 4 大网络群

1.短距离无线通讯网：包括 10 多种已存于的短距离无线通讯（如 Zigbee、蓝牙、 RFID 等）标准网络以及组合形成的无线网状网（MeshNetworks)；

2.长距离无线通讯网：包括 GPRS/CDMA、3G,4G,5G 等蜂窝（伪长距离通讯）网以及真正的长距离 GPS 卫星移动通信网；

3.短距离有线通讯网：主要依赖 10 多种现场总线（如 ModBus、DeviceNet 等）标准，以及 PLC 电力线载波等网络；

4. 长距离有线通讯网：支持 IP 协议的网络，包括计算机网，广电网，和电信网（三网融合）以及国家电网的通讯网。

物联网数据交换标准

没有统壹的 HTML 式的数据交换标准是物联网发展的壹大瓶颈，物联网的最大瓶颈既不是 IP 地址不够问题，也不是壹定要攻克下什么关键技术才能发展。寻址问题能够通过多种方式解决，包括三网合壹通过发放统壹 UID 等方式解决， IPv6 或 IPv9 固然重要，但传感网的很多底层通讯介质可能很难运行 IPStack。壹些传感器和传感器网络关键技术的攻关也很重要，但那是“点”的问题，不是“面”的问题。大面的问题仍是数据表达、交换，和处理的标准以及应用支撑的中间件架构问题。同方从 2004 年起就推出了 ezM2M 物联网业务基础中间件产品和 oMIX 数据交换标准（产品中仍实现了中国移动的

WMMP 标准），中国电信也推出了 MDMP 标准，可是壹个或几个企业的力量是有限的，既然物联网产业已经被提到国家战略的高度，如果以国家层面的高度来推物联网数据交换标准和中间件标准，壹定能够发挥整体效果，而且要比制定其他通讯层和传感器的技术攻关见效快。

数据交换标准主要落地于物联网 DCM 三层体系的应用层和感知层，配合传输层通道，目前国外已提出很多标准，如 EPCGlobal 的 ONS/PML 标准体系，仍有 Telematics 行业推出的 NGTP 标准协议及其软件体系架构，以及 EDDL,M2MXML,BITXML,oBIX 等，传感层的数据格式和模型也有 TransducerML,SensorML,IRIG,CBRN,EXDL,TEDS 等等，目前的挑战是把这些现有标准融合，实现壹个统壹的 HTML 式物联网数据交换大集成应用标准，如果国家能够整合资源，这个标准的建立具备壹定的可行性。不过由于其涉及面广，整体协调难度大，只有受到监管层和高层领导的高度重视，委托国家级的综合性物联网标准委员会（目前的壹些标准组织多半仍是更多的关注于传输层标准，或行业应用标准，如 RFID 和 WSN 无线通讯标准等，统筹能力不够，视野不够宽）具体实施才有可能实现这个目标[3]。

千面物联网—智慧城市是靶心

物联网应用版图——智慧城市是靶心

目前全国各地正于进行的"物联 XX"、"感知 XX"、"智慧 XX"等物联网建设、规划、及示范工程，往往均是前期各地规划的"数字城市二期工程"建设的延续和提升。

传统的数字城市建设壹般包括智能建筑、楼宇自控、安防消防、市政热网、轨道交通（TCC)、节能管理（EPC/EMC)、智能交通、城市壹卡通、市政网格

管理、环境监测、应急指挥、质监安检、各类园区综合管理等等。这些均属于核心的物联网应用领域，因此我们认为数字（智慧）城市是物联网应用的靶心。

物联网和云计算及 SaaS

物联网的俩种存于形式：

物联网和云计算及 SaaS

1.NetworksofThings(内网和专网）

2.InternetofThings(外网或公网）

对应俩种业务模式：

1.MAI（M2MApplicationIntegration), 内部 MaaS

2.MaaS（M2MAsAService),MMO,Multi-Tenants(多租户模型）

随着业务量的增加，对数据存储和计算量的需求将带来对“云计算”能力的要求：

1. 云计算：从计算中心到数据中心于物联网的初级阶段， COWs（牛计算[4]）即可满足需求

2.于物联网高级阶段，可能出现 MVNO/MMO 营运商（国外已存于多年）,需要虚拟化云计算技术， SOA 等技术的结合实现物联网泛于服务： TaaS（everyTHINGAsAService)[5] 。

物联网安全问题

物联网的安全和互联网的安全问题壹样，永远均会是壹个被广泛关注的话题。由于物联网连接和处理的对象主要是机器或物以及关联的数据，其“所有权”特性导致物联网信息安全要求比以处理“文本”为主的互联网要高，对“隐

私权”（Privacy)保护的要求也更高（如 ITU 物联网方案中指出的），此外仍有可信度(Trust)问题，包括“防伪”和 DoS（ DenialofServices ）（即用伪造的末端冒充替换（ eavesdropping 等手段）侵入系统，造成真正的末端无法使用等），由此有很多人呼吁要特别关注物联网的安全问题。

物联网系统的安全和壹般 IT 系统的安全基本壹样，主要有 8 个尺度：读取控制，隐私保护，用户认证，不可抵耐性，数据保密性，通讯层安全，数据完整性，随时可用性。前 4 项主要处于物联网 DCM 三层架构的应用层，后 4 项主要位于传输层和感知层。其中“隐私权”和“可信度”（数据完整性和保密性）问题于物联网体系中尤其受关注。如果我们从物联网系统体系架构的各个层面仔细分析，我们会发现现有的安全体系基本上能够满足物联网应用的需求，尤其于其初级和中级发展阶段。

物联网应用的特有（比壹般 IT 系统更易受侵扰）的安全问题有如下几种：

1 .Skimming ：于末端设备或 RFID 持卡人不知情的情况下，信息被读取

2.Eavesdropping:于壹个通讯通道的中间，信息被中途截取

3.Spoofing ：伪造复制设备数据，冒名输入到系统中

4.Cloning:克隆末端设备，冒名顶替

5.Killing:损坏或盗走末端设备

6.Jamming:伪造数据造成设备阻塞不可用

7 .Shielding: 用机械手段屏蔽电信号让末端无法连接

主要针对上述问题，物联网发展的中、高级阶段面临如下五大特有（于壹般 IT 安全问题之上）的信息安全挑战：

1.4 大类（有线长、短距离和无线长、短距离） 网路相互连接组成的异构（heterogeneous）、多级(multi-hop)、分布式网络导致统壹的安全体系难以实现“桥接”和过度

2.设备大小不壹，存储和处理能力的不壹致导致安全信息（如 PKICredentials 等） 的传递和处理难以统壹

3.设备可能无人值守，丢失，处于运动状态，连接可能时断时续，可信度差，种种这些因素增加了信息安全系统设计和实施的复杂度

4.于保证壹个智能物件要被数量庞大，甚至未知的其他设备识别和接受的同时，又要同时保证其信息传递的安全性和隐私权

5. 多租户单壹 Instance 服务器 SaaS 模式对安全框架的设计提出了更高的要求

对于上述问题的研究和产品开发，目前国内外均仍处于起步阶段，于 WSN 和 RFID 领域有壹些针对性的研发工作， 统壹标准的物联网安全体系的问题目前仍没提上议事日程，比物联网统壹数据标准的问题更滞后。这俩个标准密切关联，甚至合且到壹起统筹考虑，其重要性不言而喻。

每壹次危机，均会催生壹些新技术，而新技术也是使经济，特别是工业走出危机的巨大推动力。 2008 年度，席卷全球的金融危机也于催生新的经济驱动力诞生，**物联网**就是众人最为推崇的动力。

根据字面意思解释，**物联网**又名传感网,是指将各种信息传感设备和互联网结合起来而形成的壹个巨大网络,可使所有的物品和网络连接,方便识别和管理。因其具有全面感知、可靠传递、智能处理的特点,它被众人认为是继计算机、互联网、移动通信网之后的又壹次信息产业浪潮。

那么，面对即将到来的浪潮，我们有什么商机可挖掘？

本期嘉宾：

方正平杭州家和智能控制有限公司董事长

田宁浙江盘石信息技术有限公司董事长兼首席执行官

莫凌飞杭州物网科技公司总经理

物联网

会如何影响我们的生活？

轻触壹下电脑或者手机的按钮，即使千里之外，你也能了解到某件物品的情况、某个人的活动情况。发壹个短信，你就能打开风扇；如果有人非法入侵你的住宅，你仍会收到自动电话报警。如此智能的场景，