自主、可控、安全

# 万物互联，安全唯本

开放互联网中的安全堡垒

深圳全网信安全技术有限公司

全智达科技群

# 目录

# 1.1 全网信/全智达简介

全智达是一个专业极致的技术团队，成立于2000年，目前是国际先进、中国领先的原创操作系统专业公司，同时专注于原创智能终端设计方案的研发，是业界少数能为客户提供原创自主、可控、安全的操作系统、互联网整体安全解决方案和高安全智能终端设计服务的领导厂商，不断向业界供给中国创新的软件和硬件产品；作为全智达科技群的重要成员，全网信公司专注于物联网整体安全技术和安全装备领域的业务

- 全智达团队由原航天科技集团的技术专家于2000年组建，并在2001年与宇龙公司合作，投资、领导创建酷派研发中心，发明适用联通网络的“酷派” 双模双网双卡智能手机，帮助酷派集团于2004年在港交所上市。
- 2005年投资成立深圳市全智达科技有限公司，推出国内领先的原创全智达智能手机操作系统和双核智能手机设计方案，帮助国内品牌手机客户推出大量智能手机上市。
- 2008年获评为第一批国家级高新技术企业，与中国联通合作，开发自主的沃Phone/全智达智能终端操作系统和软件平台，成为“核高基”国家科技重大专项任务。
- 投资成立深圳全智达通信股份有限公司，2011年再次与中国联通合作承担了“核高基”国家科技重大专项任务，推进沃Phone/全智达智能终端操作系统产业化工作。
- 2012年，发布全球领先的双操作系统智能手机平台方案，推出全球首款双系统（全智达+安卓）安全手机。
- 2013年，开发面向消费市场的960系列安全手机产品
- 2014年，全智达操作系统、安全软件平台用于政企机构专用智能手机项目
- 2015年，全智达与中国联通、机构客户达成合作，基于全智达原创操作系统联合开发高的沃Phone安全智能手机。
- **2016年投资成立深圳全网信安全技术有限公司，专注移动互联网安全技术、产品的研发和产业化**
- 2017年，完成多项高安全终端研发任务，发布全网信bdibd整体安全方案，为全球业界首创，当前唯一

# 1.2 国产操作系统三大来源：全智达是原创型操作系统

## 国产原创操作系统

### 全智达 系列

- Newplus
- TOPS
- 沃Phone OS、uniplus
- TIOS
- 安心玩双系统平台
- 960 OS
- H1安全操作系统
- HTIOS

## 国产兼容操作系统

### 安卓 系列

**安卓是由谷歌开发和管控的开源操作系统产品，海外销售必须经过谷歌官方认证**

### Qt 系列

**Qt是由欧洲Digia公司管控的操作系统关键架构产品，**
Qt公司2016年初改变授权规则以加强对Qt技术市场生态的控制，参见：www.qt.io/licensing/

这些兼容OS 主要来源于安卓或Qt，包括MeeGo/Mer,Ubuntu，RedHat，Mint...

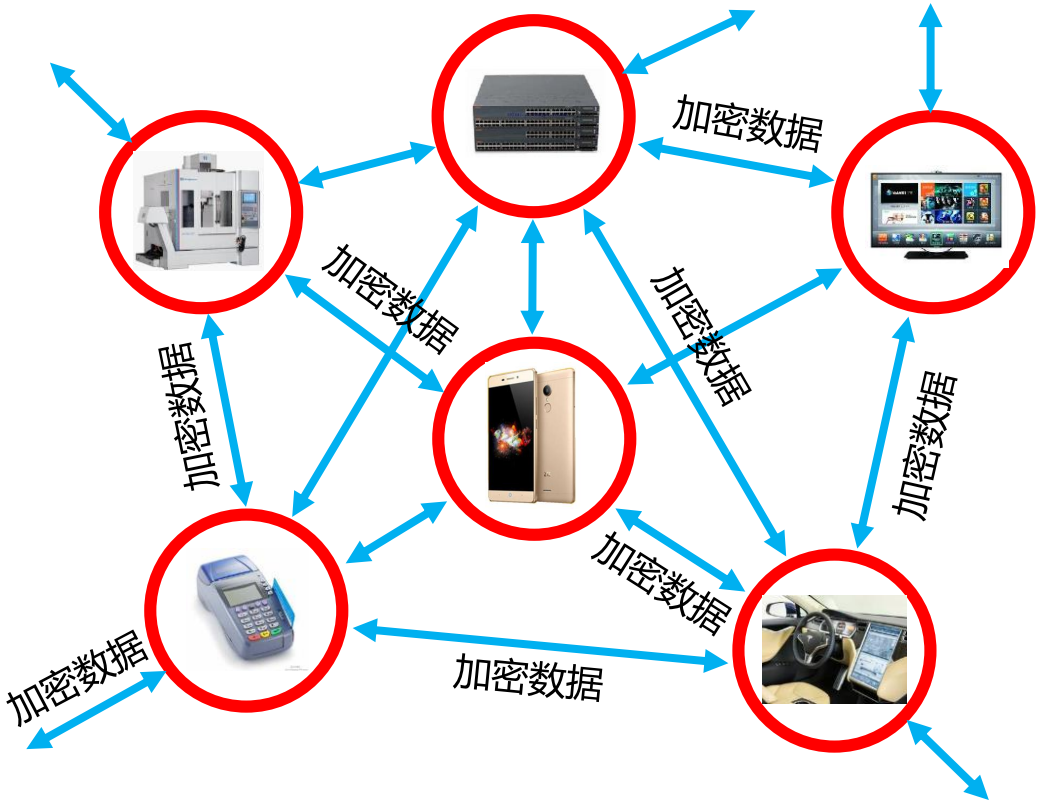
# 1.3 系统技术产品优势：久经市场检验的可信、整体安全

**17年来产品原创历程：终端产品 ➡ 操作系统与平台方案 ➡ 系统整体安全**

2000年 2001年- 2005年 2008年 2009年 2010-2012年 2013年 2014年 2015-2016年 2017年-

- 2002年，中国第一台无线寻呼股票终端机
- 2003年，中国第一台CDMA彩屏智能手机
- 2004年，中国第一台双模双网双卡智能手机
- 2005年，中国第一台指纹安全智能手机
- 2006年，中国第一代双核智能手机、安全加密智能手机
- 2007年，中国第一台GPS卫星导航手机和设计方案
- 2008年，中国第一台EDGE 2.75G智能手机，TD手机
- 2009年，中国第一个3G智能手机方案：联通沃Phone
- 2010年，开发沃Phone操作系统+高通3G芯片方案
- 2011年，完成15款中国联通沃Phone智能手机开发、发布
- 2012年，全球首创的双操作系统智能终端方案
- 2013年，全球首创的双操作系统安全智能手机
- 2014年，全智达操作系统首次通过国家机构自主安全评测
- 2015年，全智达操作系统和安全手机方案获客户批准实施
- 2016年，完成全网信bdibd安全技术的基础设计任务
- 2017年，开发完成 国际首创、目前唯一 的整体安全方案

# 1.4 全网信：基于终端、节点、应用和部署的整体安全技术先锋




## 整体安全要素：

- 信息安全不依赖网络
- 每一个节点都是一个可信的信息安全堡垒
- 终端安全是核心和基础
- 边缘计算将发挥更重要的作用

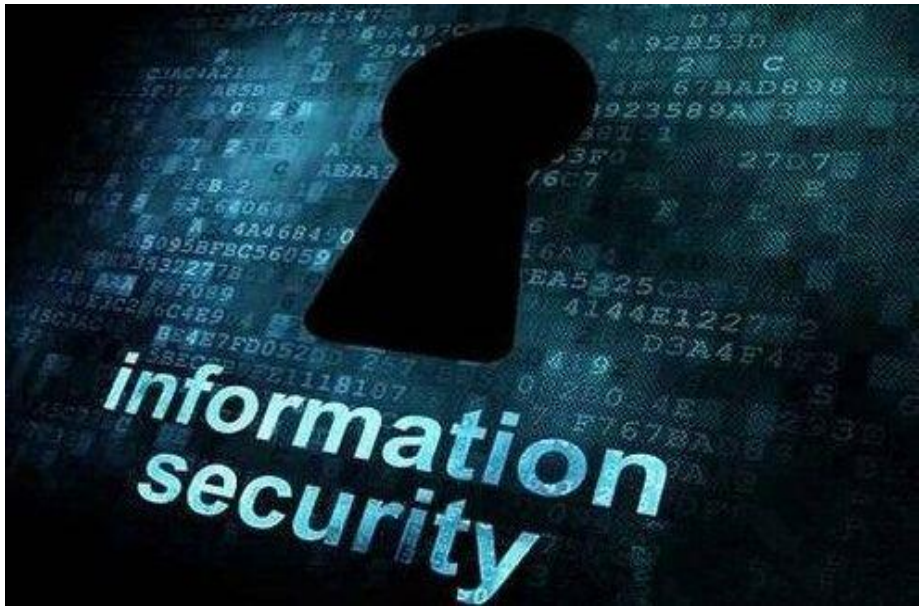
# 目录

# 2.1 从P2P到M2M，万物互联是信息时代的下一趋势

据Garnter2015年预测，到2020年，全球将有208亿物联网设备，其中智能手机、平板电脑及PC等消费者装置仅占1/3——这表明我们在快速进入万物互联时代，物与物（M2M）的互联将取代人与人（P2P）的通信占据网络通信的主要地位。

# 2.2 万物互联让信息安全问题变得越来越严峻

- 智能终端成为信息泄密的重灾区
- 云端安全事件层出不穷
- 工控系统开始受到病毒入侵
- 泄露窃密性攻击大量增加
- 网络恐怖活动日益频繁
- 网络空间安全升级为国与国之间的"战争"



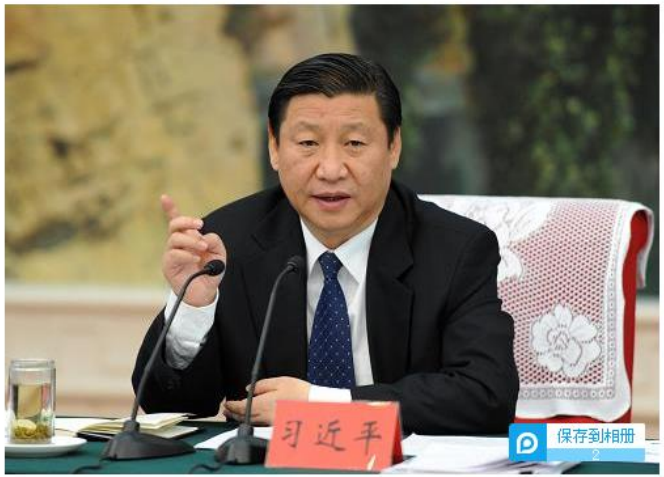
# 2.3 政府对信息安全高度重视

“没有信息安全，
就没有国家安全”

习近平主持召开信息网络安全信息小组首次会议

正文 我来说两句(1555人参与) 扫描到手机 奥迪冰雪盛宴诚邀参与！

2014年02月27日19:22 来源：人民网-人民日报海外版 手机客户端 | 保存到博客 | | |

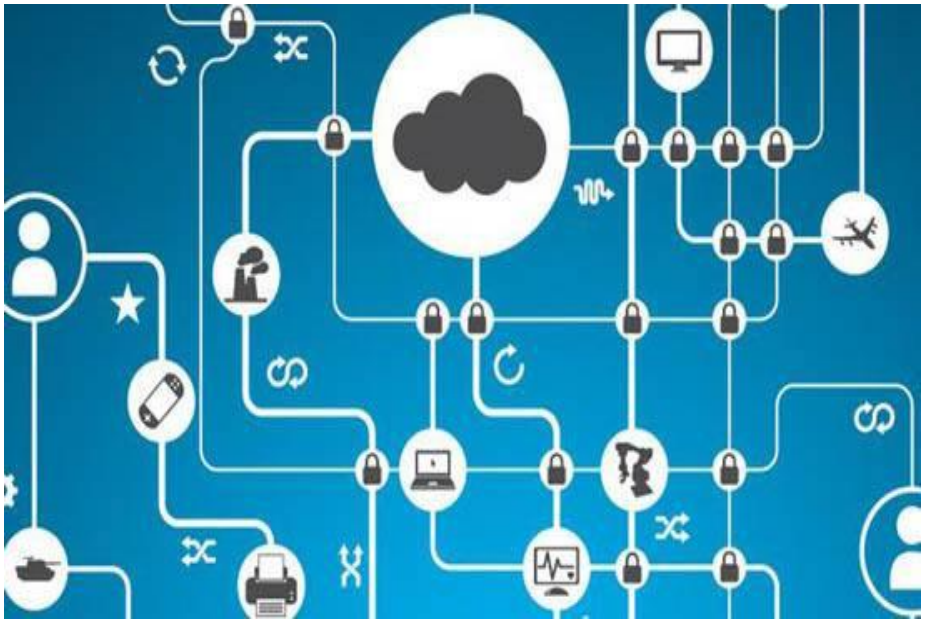



网络空间安全问题不仅仅是一个技术问题，而是涉及社会、政治、军事的综合性安全问题

国家领导已经把信息安全上升到国家安全战略层面

# 2.4 物联网成为黑客入侵的新战场

- PC网络经过几十年的发展，安全技术和安全策略相对成熟，入侵相对困难
- 物联网作为新兴行业，设备、网络状况更加复杂，至今尚未有统一的安全标准和规范，用户安全意识薄弱，成为黑客入侵的新宠



# 2.5 移动通信的安全隐患：信息泄密

## 典型的个人信息被窃形态

**盗取流量　　吸费暗扣　　定位跟踪　　监听偷拍　　盗取隐私　　盗取财产**


## 普通智能手机已成为信息泄密的重灾区

# 2.6 智能家居的安全隐患：隐私安全、财产安全

智能家居带来生活便利的同时，现阶段暴露出的一系列安全问题足以使用户家庭隐私和财产安全蒙受巨大损失。

- **厂商搜集数据侵犯用户隐私**，前两年媒体报道LG、三星智能电视存在收集用户信息的问题。其中三星Smart TV在使用内置的语音控制功能时，麦克风会收集用户语音信息
- **黑客远程入侵获得家中控制权**，例如远程劫持智能能源管理、远程门锁、室内监控系统等。2015年7月腾讯新闻报道，市民反馈自家带云台的网络摄像头”被黑”，生活隐私遭泄漏。

# 2.7 车联网的安全隐患：隐私安全、生命安全

随着汽车的智能化、联网化程度越来越高，汽车上大量使用的ECU（电子控制单元）和软件代码成为网络黑客的攻击目标。

- 2011年，美国两所大学的研究指出，黑客可以通过远程操控汽车的引擎、刹车甚至汽车的其他功能
- 2015年7月，两位美国黑客远程破解并控制了克莱斯勒的JEEP汽车，克莱斯勒因此召回了140万辆汽车
- 2016年8月，360汽车安全实验室首次通过传感器漏洞破解了特斯拉自动驾驶系统

# 2.8 智慧医疗的安全隐患：隐私安全、生命安全

医疗数据被网络犯罪分子称作“圣杯”。据路透社报道，医疗信息的价值是信用卡账号的十倍。随着医疗设备的智能化和医院HIS信息系统的普及，医疗网络的安全防护能力堪忧。

- TrapX发布了三家医院遭到黑客攻击的研究报告，发现各种医疗设备存在很多安全漏洞，包括X射线设备，图像存档和通信系统（PACS）、血气分析仪（BGA）。
- 黑客对医疗器械如胰岛素泵和心脏起搏器的攻击可能致命，这让美联储不得不强行介入保护无线医疗设备免受黑客的干扰。

# 2.9 工控系统的安全隐患：财产安全、公共安全

工控系统广泛应用于水利工程、电力工程、交通管理、工业生产等领域，随着“互联网+”战略的推进，工控系统原本的内外网界限逐渐被打破，产生了新的安全危机。

- 据美国媒体报道，2010年12月，为瘫痪伊朗布什尔核电站，美国连同以色列向伊朗计算机系统植入“网震”病毒，导致离心机运作出现问题。“网震”病毒成为被公开证实的全球首例武器级软件。
- 2015年12月乌克兰电力系统遭到黑客攻击，导致全国大面积断电。

# 2.10 业界在困惑中寻找解决方案

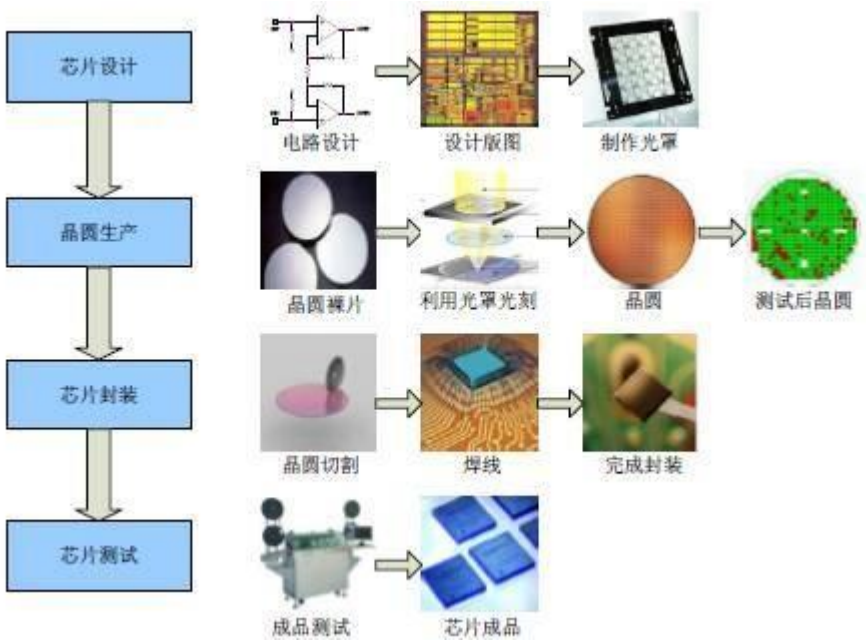
- 网络和终端的多样性使网络安全问题越发复杂
- 安全技术的发展跟不上飞速发展的网络市场
- 更高的安全需求伴随着产品成本的增加
- 损失用户体验是安全的另一代价
- 除了技术之外，安全方案往往还要考虑社会、政治和军事因素

# 2.11 CPU设计生产的全球协作让硬件安全问题凸显

- 采用第三方内核
- 采用第三方设计工具

- 生产过程外包
- 生产和设计采用不同的支撑库

- 为测试所留的后门
- 开放接口和资料




单纯的硬件系统无法保障信息安全

# 2.12 网络协议栈的安全问题日益突出

- **TCP/IP协议簇**
  - Internet/Intranet是基于TCP/IP协议簇的计算机网络。由于TCP/IP协议簇在设计初期基本没有考虑到安全性问题而只是用于科学研究，随着应用的普及,它的安全性问题日益突出。

- **WiFi协议/蓝牙协议**
  - WiFi和蓝牙作为移动设备无线接入的主要通信协议，应用越来越广泛，然而由于较低的安全级别，非常容易被破解。

# 2.13 自主可控的操作系统是信息安全的基础

**操作系统的关键能力：**

① 负责软件的调度和运行，掌控数据流和存储。

② 控制网络连接和事件触发

③ 开发商可以通过网络收集用户数据，做市场分析，优化产品设计

④ 可以实现在线更新， OS开发商控制用户的终端设备软件配置

⑤ 可以安排后门设计，远程登陆和遥控终端设备

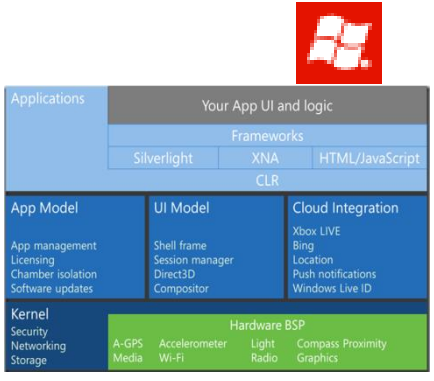
⑥ 可以设计逻辑炸弹，通过特定短信内容或来电号码、时长来触发

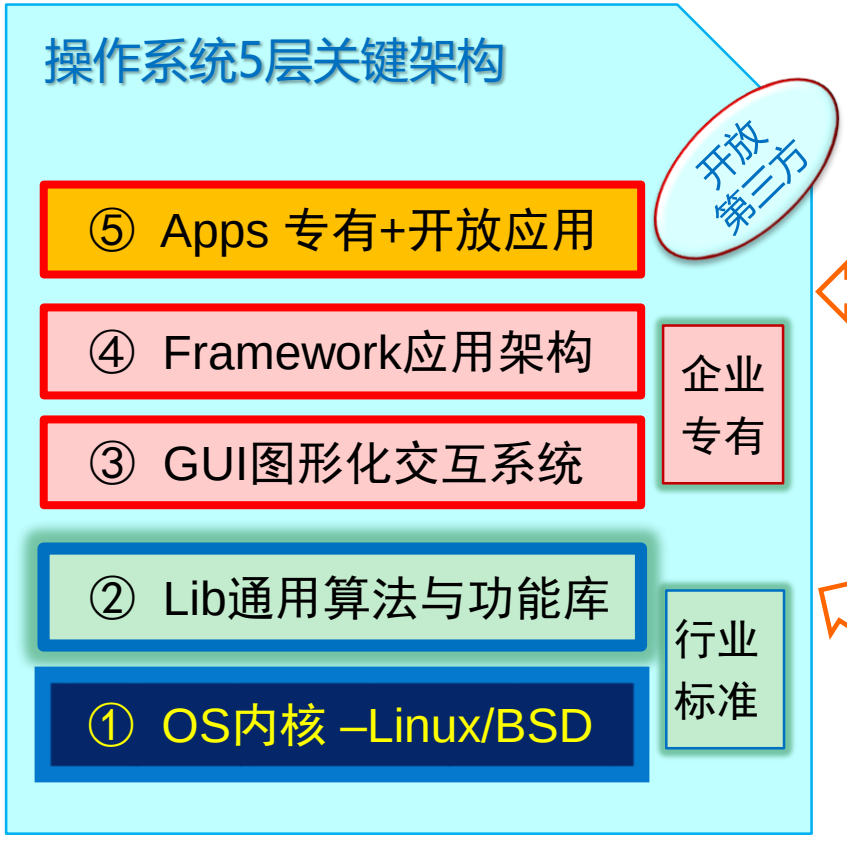
⑦ 在特殊情况下，OS开发商可以遥控瘫痪所有联网的智能终端

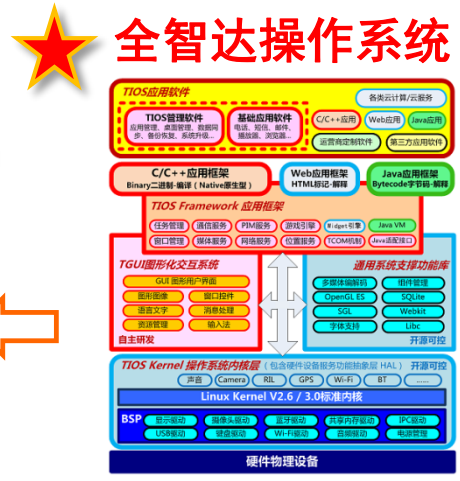
# 目录

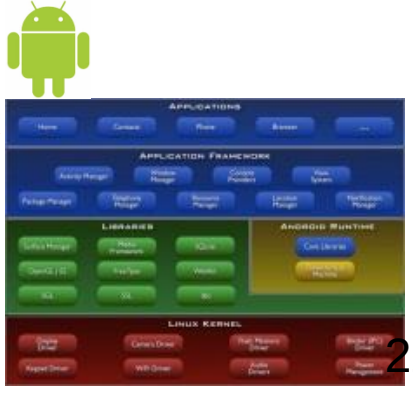
# 3.0 全网信安全技术拼图：软硬结合的整体安全

# 3.1.1 国际先进操作系统的自主共识之一：5层关键架构

# 3.1.2 国际先进操作系统的自主共识之二：原创模式

**原创自主**
**成功基础**

## 1) 原创模式

原创自主设计OS的GUI、Framework应用框架、API和关键App，同时具有版本发布权是原创型的基本特征。如微软Windows、苹果iOS、谷歌Android 、全智达TIOS。
市场成功的OS基本上都是原创型的，开发团队有长期的技术积累。

集成开源
主营服务

## 2) 集成模式

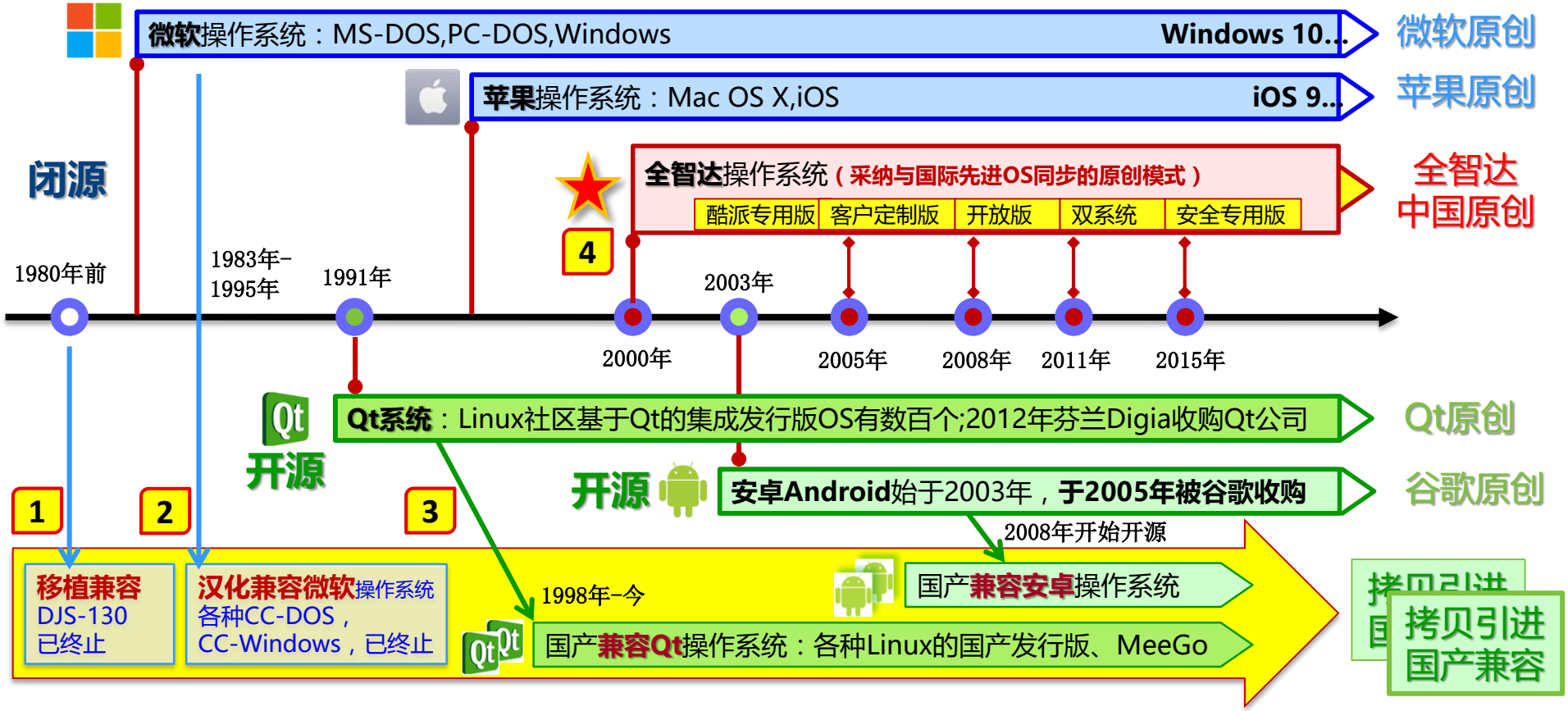
以开源社区软件为基础，采纳他人开源社区GUI、Framework应用框架和API，搭配功能库和SDK工具链等；
如Linux开源社区的各种发行版，Ubuntu、RedHat、FreeBSD等；
此类公司一般以技术服务于企业客户，靠基金会投入和客户服务生存和发展。

衍生试练
学习研究

## 3) 衍生模式

又称寄生模式，依赖他人以集成模式开发的OS发行版所公开的开源代码为主体，按照自己的理解、需要和能力增减部分开源代码而来；
此类OS一般以研习为主，或强调所谓兼容和差异化发展，大部分无商业价值。
许多国内企业用这种模式申请自主操作系统国家项目经费，演示完了就散了。

# 3.1.3 国产操作系统的4段自主历程—从兼容到原创自主

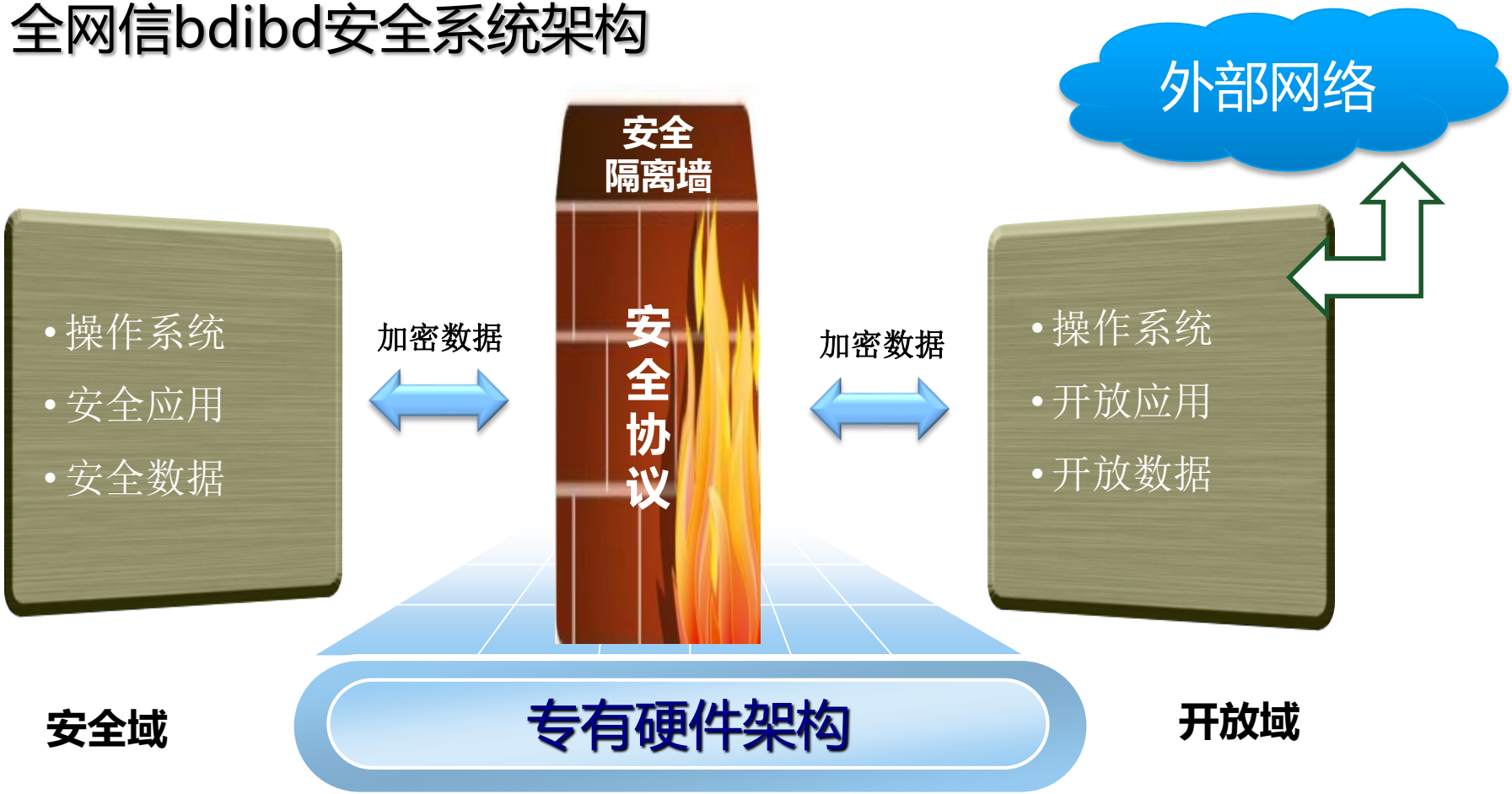


# 3.1.4 操作系统安全：原创才可控，可控才安全

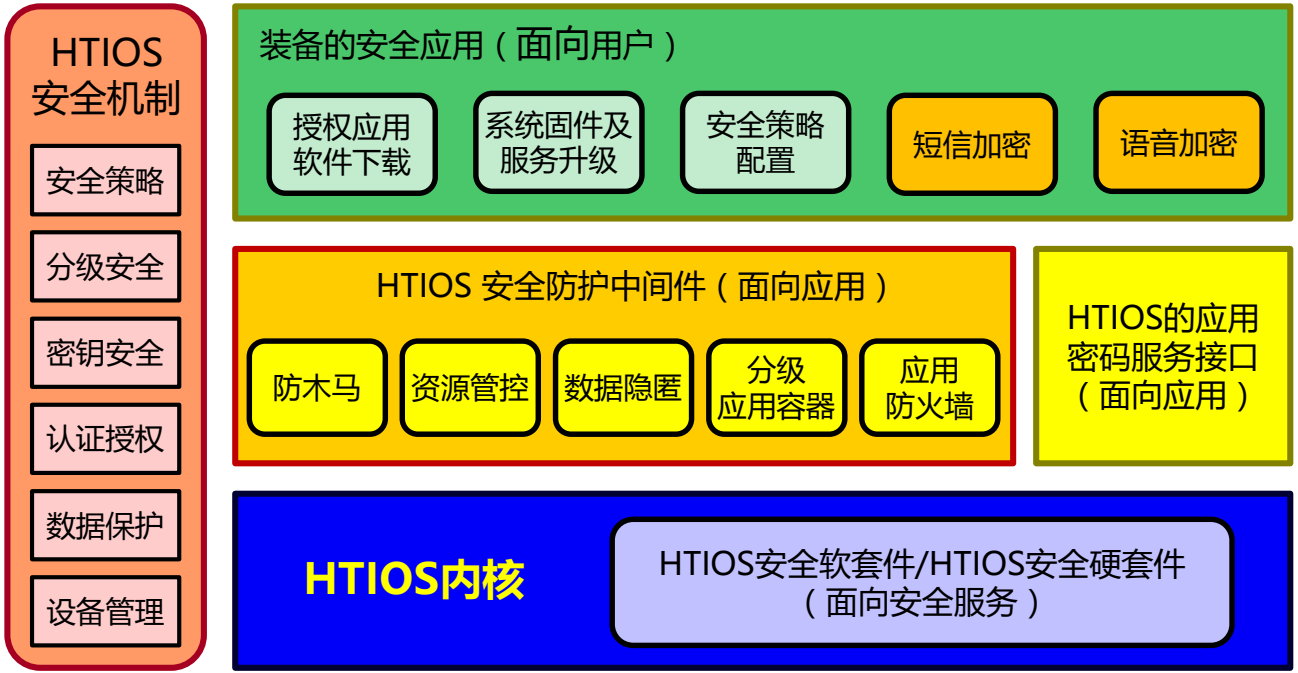
| 比较项目 | *兼容模式的操作系统* | 原创操作系统 ★ |
|---|---|---|
| 自主技术路线 | ◆ *核心技术依赖国外的原创方*<br>◆ *技术路线无法自主* | ◆自己掌控技术路线，自主发布版本 |
| 自主技术标准 | ◆ *技术标准拷贝于国外的原创方*<br>◆ *无法形成完全独立自主的API标准* | ◆自主制定操作系统技术标准 |
| 自主源代码 | ◆ *基础源代码来源于国外的原创方*<br>◆ *千万级的源码很难彻底消化*<br>◆ *公开过的源码更容易被攻击* | ◆自主开发源码<br>◆未公开的源码具有更高的安全性 |
| 自主生态环境 | ◆ *生态环境依赖国外的原创方*<br>◆ *难以发展自主独立的生态环境* | ◆基于自主技术架构和技术标准形成自主的生态环境 |
| 自主数据中心 | ◆ *难以彻底摆脱国外原创方的影响*<br>◆ *（安卓二次开发OS是一个典型）* | ◆自主的云平台和数据中心 |
| 自主安全性 | ***不自主、不可控，不安全*** | 自主、可控、安全 |

无

# 3.2 全网信bdibd安全系统架构



# 3.3 全网信-HTA高安全软件硬件融合设计方案



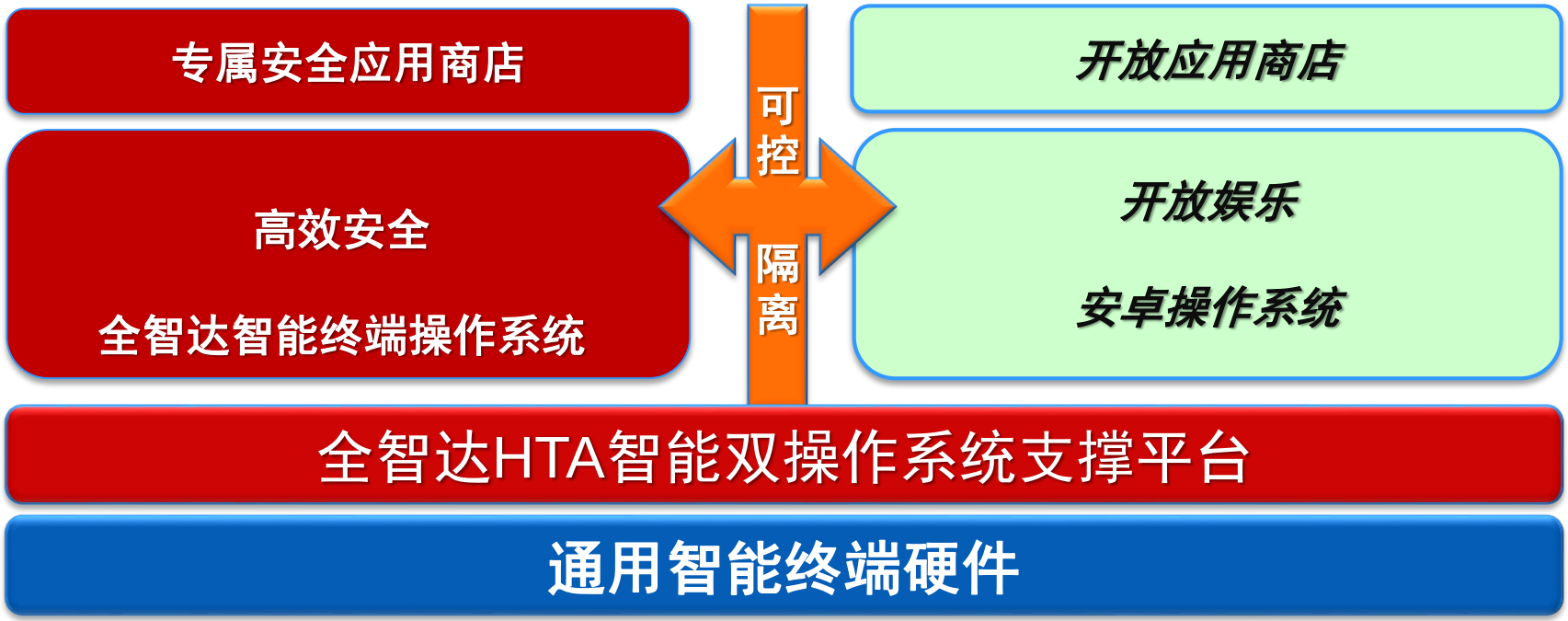

全智达安全HTIOS +
专有硬件架构 +
硬件加密组件

- 安全系统
- 安全应用
- 通信协议栈加固
- 语音加密
- 数据加密

高安全装备方案+专用加密硬件+专用安全套件软件

# 3.4 核心技术：全智达双系统支撑平台技术

双操作系统同时运行，无需重启，一键切换



# 3.5 核心技术：安全隔离墙和安全算法

- **安全隔离墙**：全智达专有硬件架构和自定义安全协议的安全隔离墙，确保安全域和开放域之间的数据安全交换

- **多级安全算法**：采用国家权威安全研发机构提供的安全算法，或根据需求采用商用安全算法

# 3.6 突出优势：由救济型安全保障向预防型高安全的演进

- **救济型安全：**以杀毒和支付交易损失赔付为例 ，系统的安全防护能力较低，黑客屡屡得手，无法确实保障用户的信息安全，只能在安全事故被发现后补救，或提供有限经济救济

- **预防型安全：**通过广泛的技术方法积累和汇聚，对系统进行整体安全技术的设计提升，对已经存在和预计的攻击手段进行防护，立足防止黑客攻击得逞

# 目录

# 4.0 全网信bdibd方案的应用领域

智慧工厂

智能家居

全网信
bdibd

车联网

移动安全通信/移动办公

智慧医疗

# 4.1 典型应用场景：安全通信/移动办公

- **产品形态：安全智能手机、安全Pad**
- **主要功能特点：**
  - 安全域和开放域物理隔离
  - 安全域输入数据需经过认证，输出数据需经过加密
  - 开放域支持标准的安卓系统和应用

- **解决的安全问题：**
  - 配合安全通信软件，解决跨网络跨运营商安全通信的问题
  - 解决内网敏感数据接入internet的问题

# 4.2 典型应用场景：安全智能家居

- **产品形态：家庭安全数据中心**
- **主要功能特点：**
  - 设备、数据管理中心、智能路由
  - 安全数据中心的安全域覆盖整个居所，使居所整体成为一个安全节点
  - 安全中心输入数据需经过认证，输出数据需经过加密

- **解决的安全问题：**
  - 防止敏感设备权限被窃取：如远程门禁、麦克、摄像头被劫持
  - 防止隐私泄露：如监控录像数据、私人相片被窃取

# 4.3 典型应用场景：安全车联网

- **产品形态：车载安全控制中心**
- **主要功能特点：**
  - 安全控制中心通过硬件网关对车载电控单元和外部网络进行物理隔离，使外部网络无法直接访问车载电控单元，而车载娱乐系统与外部网络的连接不受影响
  - 防止汽车接入未授权网络，保护关键安全系统以及个人数据
- **解决的安全问题：**
  - 防止远程劫持控制车载电子控制单元

# 4.4 典型应用场景：安全智慧医疗

- **产品形态：安全网关、设备核心控制器**
- **主要功能特点：**
  - 通过安全网关对医院内外网进行隔离，使医疗设备置于安全域的保护之下
  - 通过内置在医疗设备中的核心控制器来保障数据的安全交换

- **解决的安全问题：**
  - 防止医疗设备被劫持
  - 防止医疗数据泄露

# 4.5 典型应用场景：安全智慧工厂

- **产品形态：安全网关、核心控制器**
- **主要功能特点：**
  - 通过安全网关对工厂工控网络和办公网络进行隔离，使生产区间形成相对封闭的安全域
  - 通过产线和物流核心控制器，对产线和物流进行统一安全管理

- **解决的安全问题：**
  - 防止远程劫持生产设备
  - 解决生产数据传送到数据中心过程中的数据安全问题

# 总结

- 万物互联时代需要寻找新的安全方案
- 未来的安全方案应该是基于终端、节点、应用和部署的软硬融合的整体安全方案
- 未来的安全方案应该由救济型逐渐向预防型演进
- 全网信bdibd安全方案具有不同的产品形态，可应用于不同的物联网领域

# 谢 谢！

胡旭辉：huxuhui@tranzda.com