ISC 2019 第七届互联网安全大会

用可信计算3.0筑牢网络安全防线

国家集成电路产业发展咨询委员会委员
国家信息化专家咨询委员会委员
国家三网融合专家组成员
沈昌祥 院士

第七届互联网安全大会 360互联网安全中心

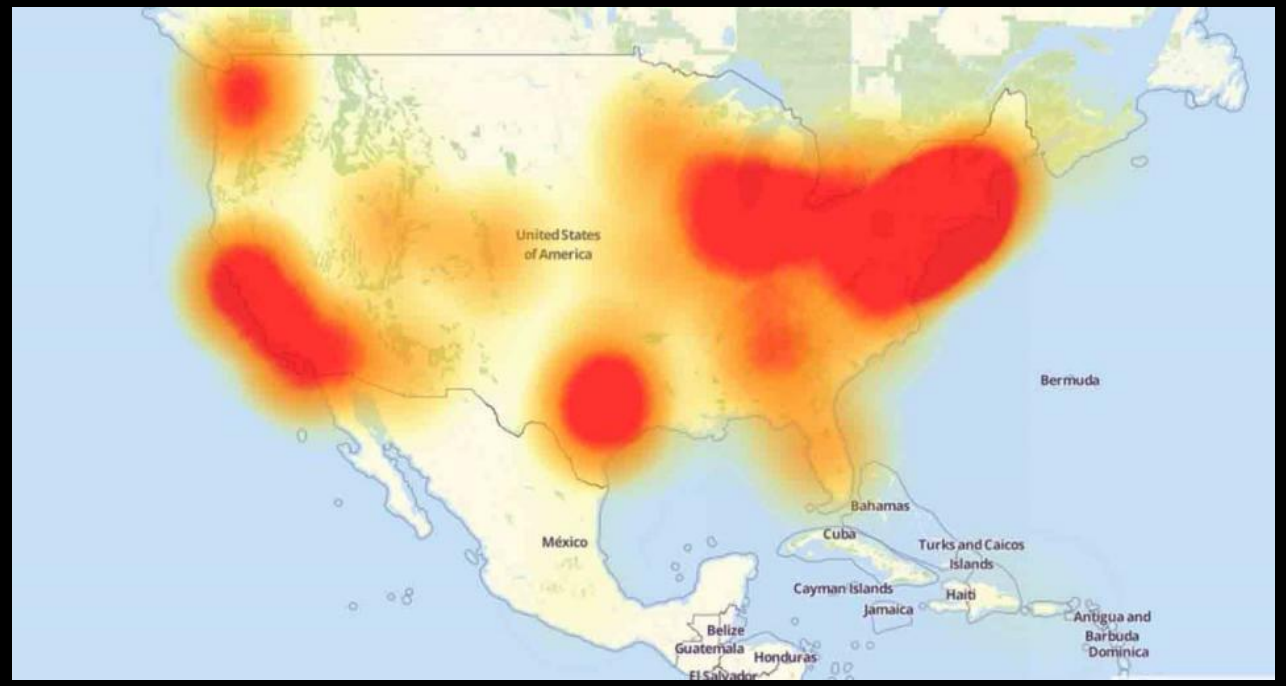
1 PART

科学的网络安全观

“没有网络安全就没有国家安全，没有信息化就没有现代化”

安全是发展的前提，发展是安全的保障。没有网络安全，信息社会将成为黑暗中的废墟。

案例一： 2016年10月21日，美国东海岸（世界最发达地区）发生世界上瘫痪面积最大（大半个美国）、时间最长（6个多小时）的分布式拒绝服务（DDoS）攻击。



“物联网破坏者”（“Mirai”未来）劫持网络摄像头（**杭州制造**），让上百万摄像头同时请求访问互联网，造成网络堵塞瘫痪。更有进一步攻击，升级为PDoS（永久拒绝服务攻击），清除设备里的所有文件。

案例二： 2017年5月12日爆发的“WannaCry”的勒索病毒，通过将系统中数据信息加密，使数据变得不可用，借机勒索钱财。病毒席卷近150个国家，教育、交通、医疗、能源网络成为本轮攻击的重灾区。

2018年8月3日，台积电遭到勒索病毒入侵，几个小时之内，台积电在中国台湾地区的北、中、南三个重要生产基地全部停摆，造成约十几亿美元的营业损失。最近的5.4侠盗版危害极大。

《网络安全法》

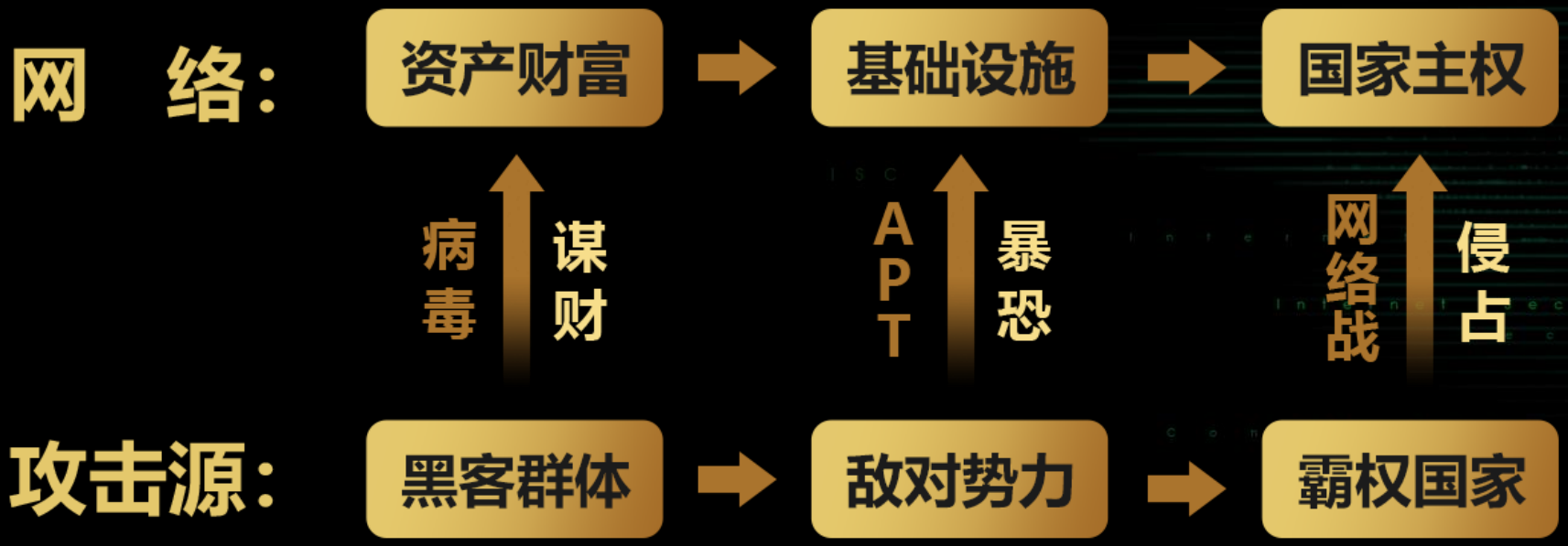
第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，**推广安全可信的网络产品和服务**，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

《国家网络空间安全战略》提出的战略任务“夯实网络安全基础”，强调“尽快在核心技术上取得突破，**加快安全可信的产品推广应用**”。

网络安全等级保护制度2.0标准要求全面使用**安全可信的产品和服务**来保障关键基础设施安全。

1、网络威胁是永远的主题

网络空间极大威胁：有利可图、全方位攻击



2、网络空间极其脆弱

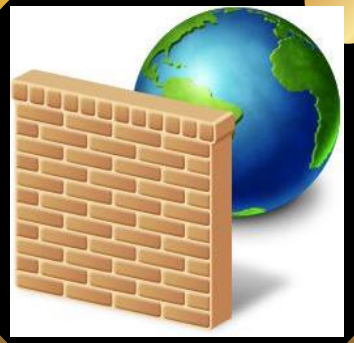

网络空间极其脆弱
是
计算科学问题
图灵计算原理
（少攻防理念）
体系结构问题
冯诺伊曼架构
（缺防护部件）
计算模式问题
重大工程应用
（无安全服务）

3、安全风险的实质

设计IT系统不能穷尽所有逻辑组合，必定存在逻辑不全的缺陷。利用缺陷挖掘漏洞进行攻击是网络安全永远的命题。

主动免疫的安全目标：确保为完成计算任务的逻辑组合不被篡改和破坏，实现正确计算。

传统“封堵查杀”已过时



防火墙

病毒查杀

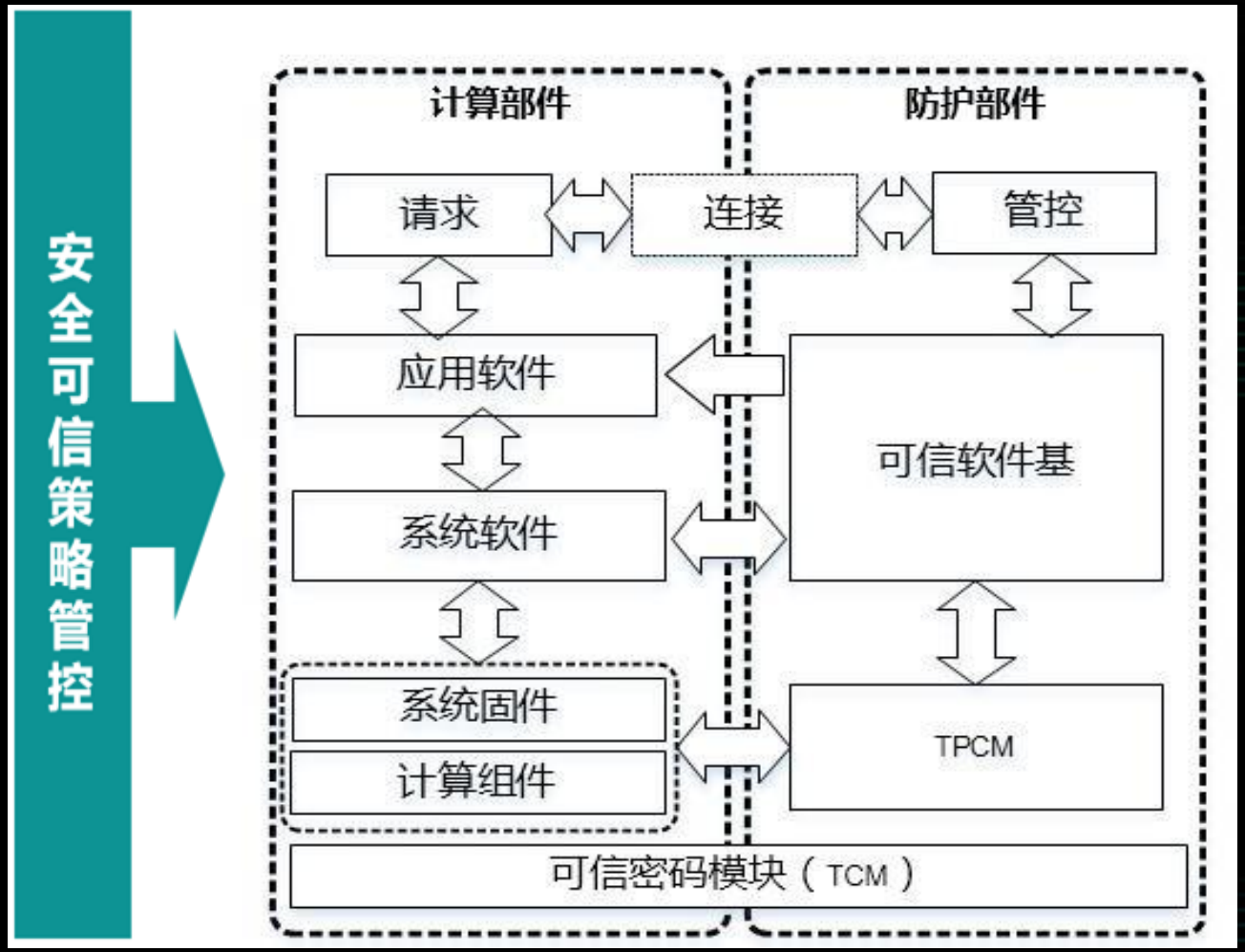
入侵检测

杀病毒、防火墙、入侵检测的传统“老三样”难以应对人为攻击，且容易被攻击者利用，找漏洞、打补丁的传统思路不利于整体安全。

4、主动免疫可信计算

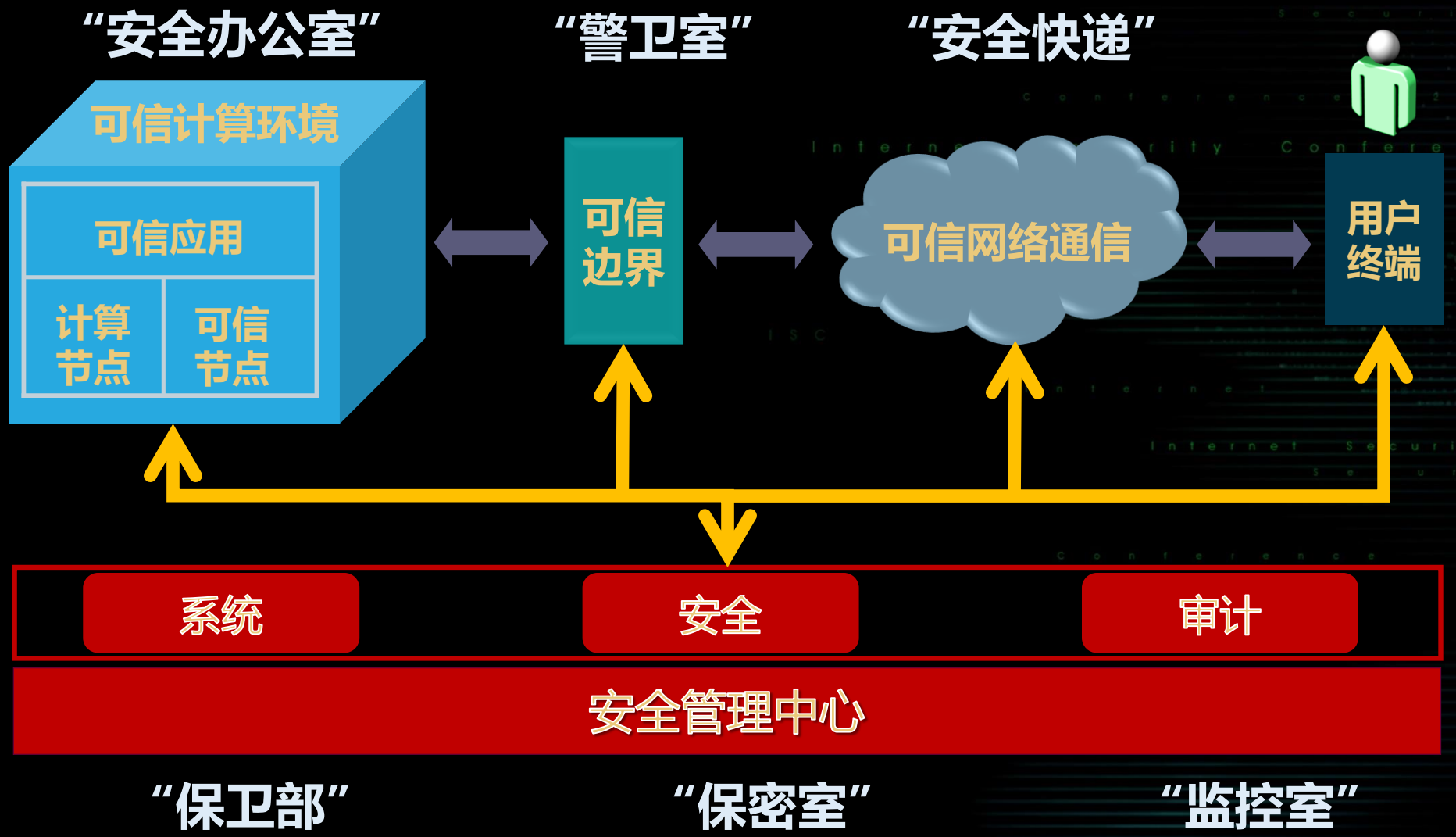
主动免疫可信计算是指计算运算的同时进行安全防护，**以密码为基因**实施身份识别、状态度量、保密存储等功能，及时识别“自己”和“非己”成分，从而破坏与排斥进入机体的有害物质，相当于为网络信息系统培育了免疫能力。

安全可信的计算节点双体系（计算+防护）结构



建立免疫 反腐败子系统

可信安全管理中心支持下的主动免疫三重防护框架



安全防护效果：

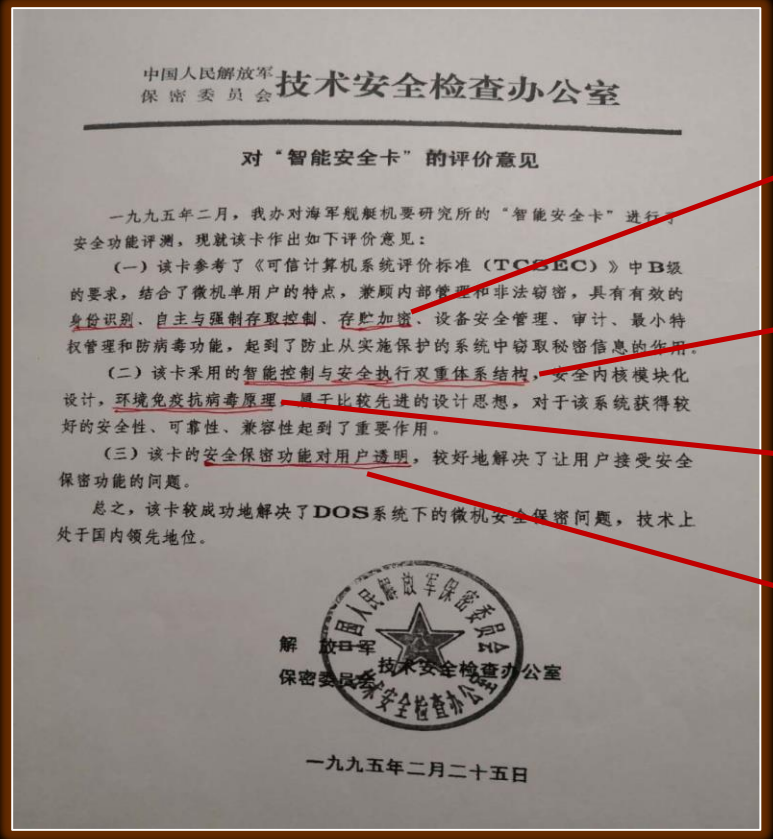
“WannaCry”、“Mirai”、“黑暗力量”、“震网”、“火焰”、“心脏滴血”等不查杀而自灭

ISC 2019 第七届互联网安全大会

2 PART

中国可信计算革命性创新

中国可信计算源于1992年立项研制的**可信计算综合安全防护系统（智能安全卡）**，于1995年2月底通过测评和鉴定。经过长期军民融合攻关应用，形成了自主创新安全可信体系，开启了**可信计算3.0时代。**



中国人民解放军保密委员会技术安全检查办公室

对“智能安全卡”的评价意见

一九九五年二月，我办对海军舰艇机要研究所的“智能安全卡”进行了安全功能评测，现就该卡作出如下评价意见：

（一）该卡参考了《可信计算机系统评价标准（TCSEC）》中B级的要求，结合了微机单用户的特点，兼顾内部管理和非法窃密，具有有效的身份识别、自主与强制存取控制、存贮加密、设备安全管理、审计、最小特权管理和防病毒功能，起到了防止从实施保护的系统中窃取秘密信息的作用。

（二）该卡采用的智能控制与安全执行双重体系结构，安全内核模块化设计，环境免疫抗病毒原理，是一比较先进的设计思想，对于该系统获得较好的安全性、可靠性、兼容性起到了重要作用。

（三）该卡的安全保密功能对用户透明，较好地解决了让用户接受安全保密功能的问题。

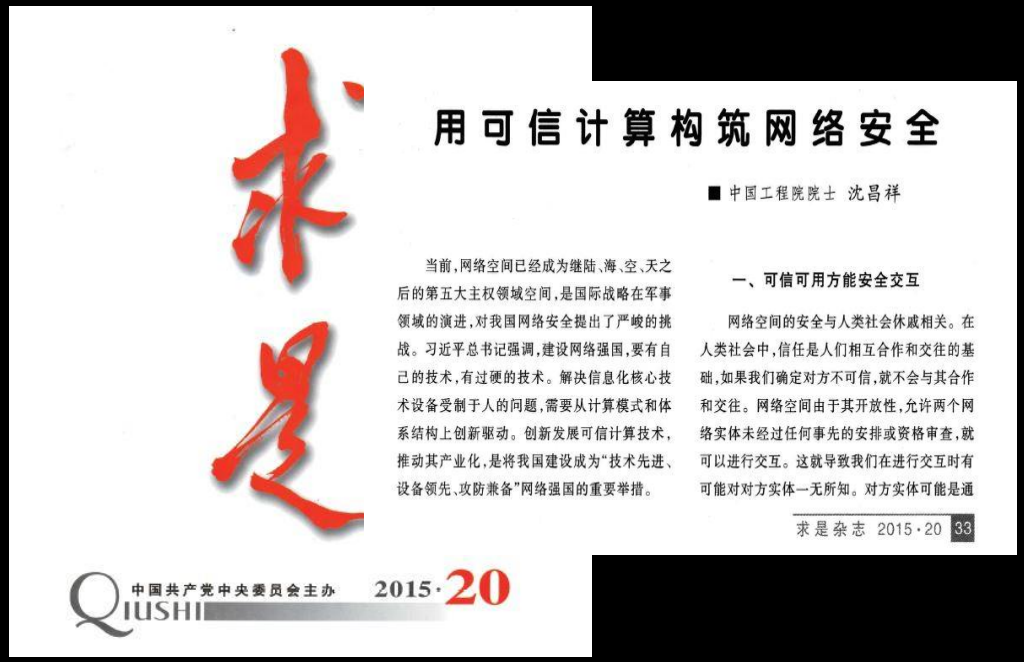
总之，该卡较成功地解决了DOS系统下的微机安全保密问题，技术上处于国内领先地位。

解放军保密委员会技术安全检查办公室

一九九五年二月二十五日

- 公钥密码身份识别、对称密码加密存储
- 智能控制与安全执行双重体系结构
- 环境免疫抗病毒原理
- 数字定义可信策略对用户透明

开创可信计算3.0时代


求是

用可信计算构筑网络安全

■ 中国工程院院士 沈昌祥

当前，网络空间已经成为继陆、海、空、天之后的第五大主权领域空间，是国际战略在军事领域的演进，对我国网络安全提出了严峻的挑战。习近平总书记强调，建设网络强国，要有自己的技术，有过硬的技术。解决信息化核心技术设备受制于人的问题，需要从计算模式和体系结构上创新驱动。创新发展可信计算技术，推动其产业化，是将我国建设成为“技术先进、设备领先、攻防兼备”网络强国的重要举措。

一、可信可用方能安全交互

网络空间的安全与人类社会休戚相关。在人类社会中，信任是人们相互合作和交往的基础，如果我们确定对方不可信，就不会与其合作和交往。网络空间由于其开放性，允许两个网络实体未经过任何事先的安排或资格审查，就可以进行交互。这就导致我们在进行交互时有可能对对方实体一无所知。对方实体可能是通

求是杂志 2015·20 33

中国共产党中央委员会主办 QIUSHI 2015·20


解读品牌竞争力 新华通讯社主管

CHINA TOP BRANDS 中国名牌

可信计算：网络安全的主动防御时代

沈昌祥：可信计算让信息系统国产化真正落地

Shen Changxiang: Trusted Computing Ensure That The Information System Localization Takes Effect

本刊记者 / 杨侠 摄影 / 王楚天

Windows系统升级的背后，有着怎样的可信计算机制较量？可信计算究竟是怎样的一种信息安全保障模式，在自主可控信息系统国产化战略中又能起到怎样的作用？带着这些问题，记者特别专访了信息

的密码就相当于人体的基因，对于“基因”的变异可用编码原理检验其有无变化。可信计算的免疫功能就像人体的免疫功能一样，是一个动态的支撑体系，可独立成为一个循环系统，进行完整性检查，换言之，

中国工程院院士沈昌祥（左）讲述对可信计算的研究与应用

◆可信可用方能安全交互

◆主动免疫方能有效防护

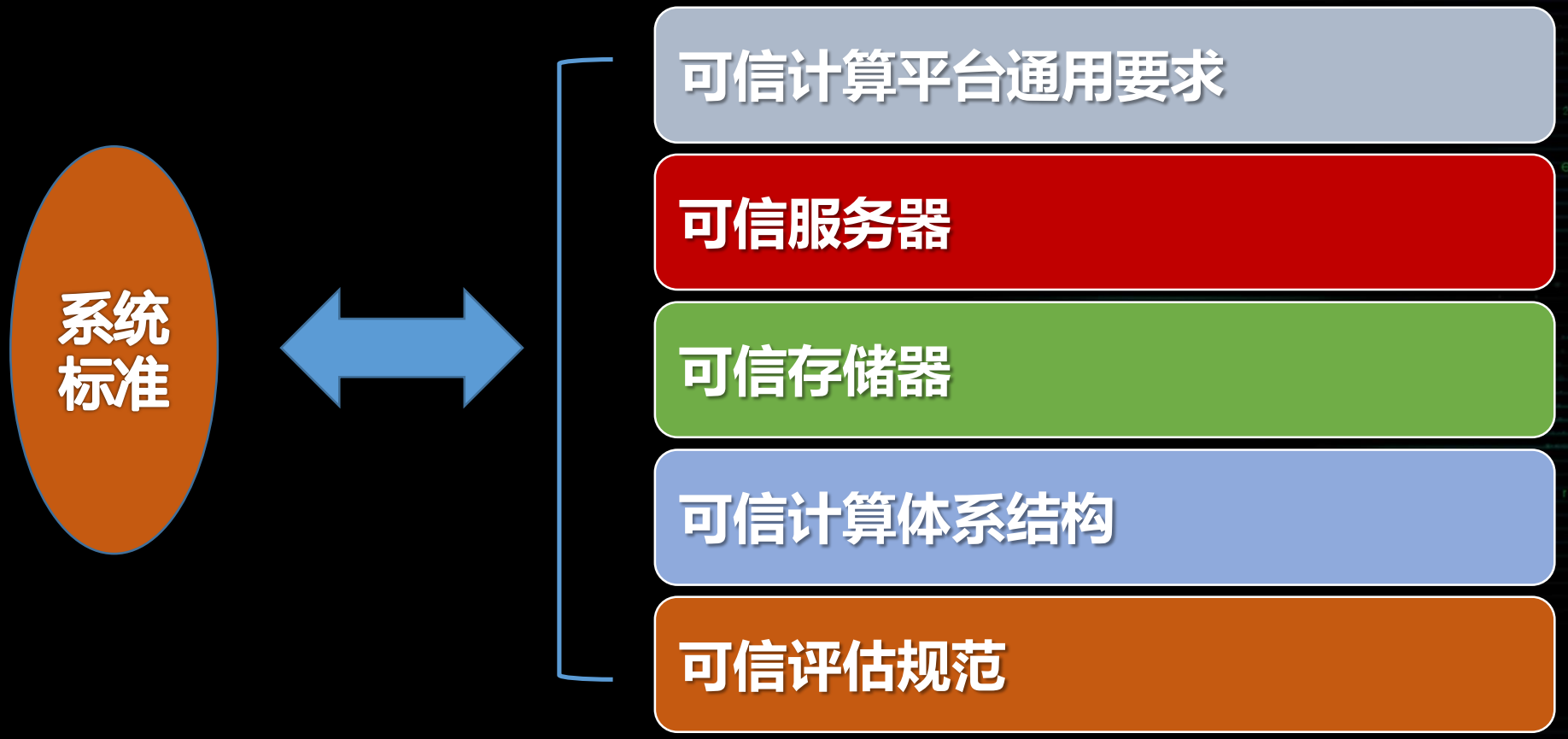
◆自主创新方能安全可控

新华社 《中国名牌》

可信计算：网络安全的主动防御时代

1、创新可信计算标准体系

我国2010年前完成了核心的9部国家标准和5部国军标的研究起草工作。截至目前，已发布国家标准3部、国军标3部，即将发布国家标准2部，已发布团体标准（中关村可信计算产业联盟标准）4部。授权专利百余项。


系统标准
可信计算平台通用要求
可信服务器
可信存储器
可信计算体系结构
可信评估规范

2、创新可信密码体系

密码机制创新

采用对称与公钥密码相结合体制，提高了安全性和效率

密码算法创新

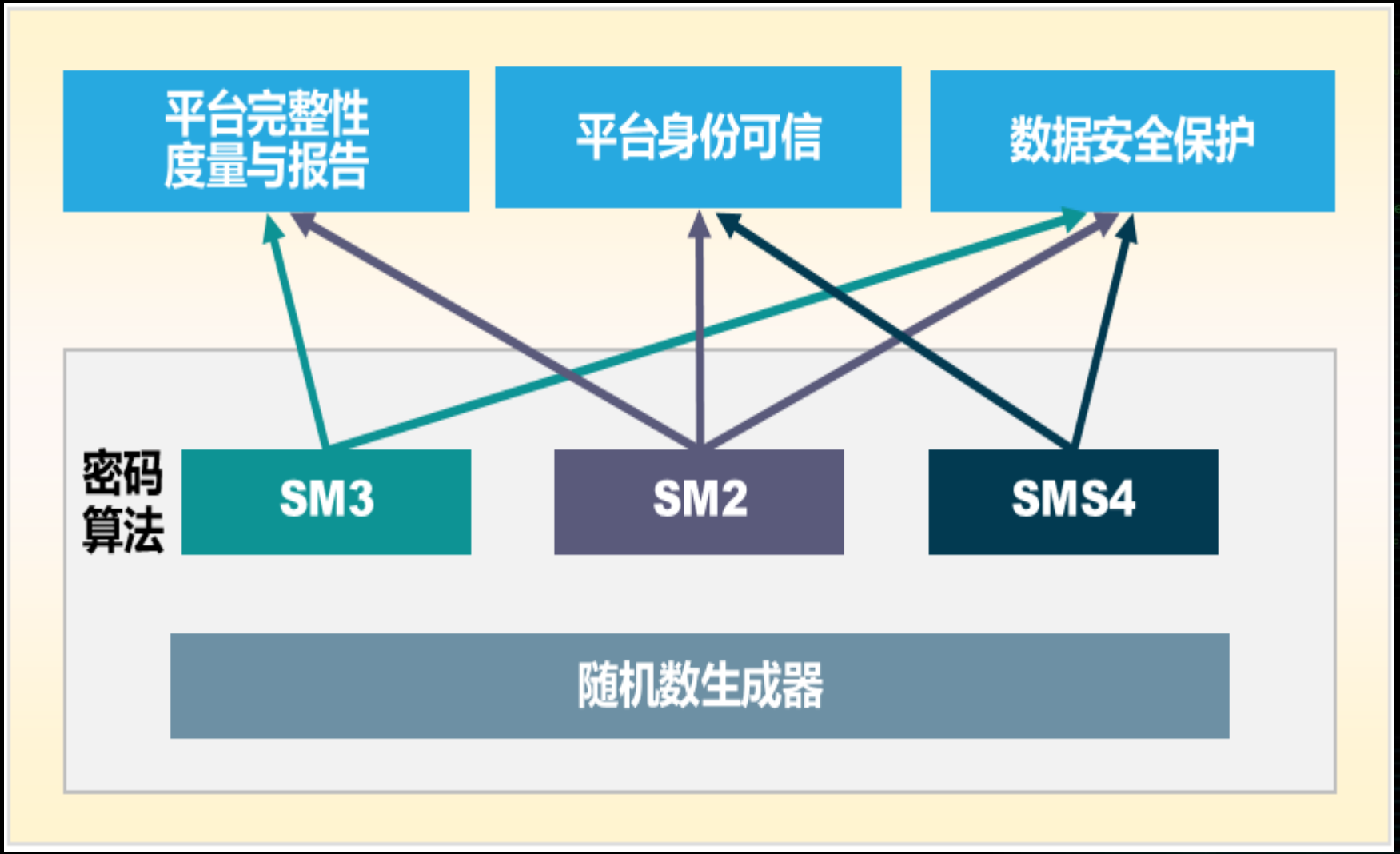
全部采用国有自主设计的算法，定义了可信计算密码模块（TCM）

证书结构创新

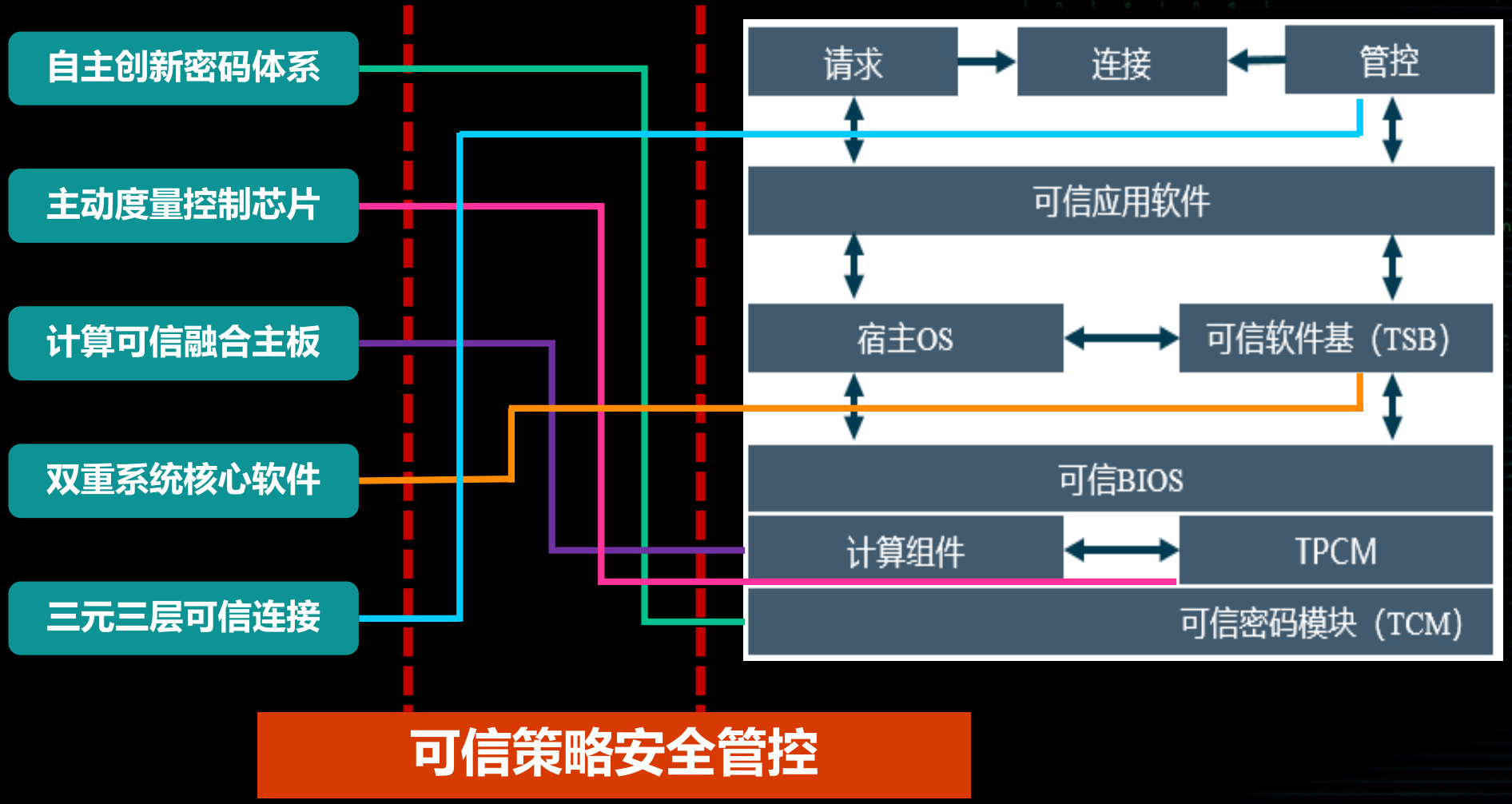
采用双证书结构，简化了证书管理，提高了可用性和可管性

纠正了TCG密码体制的缺失，已成为ISO国际标准

密码算法与可信功能的关系

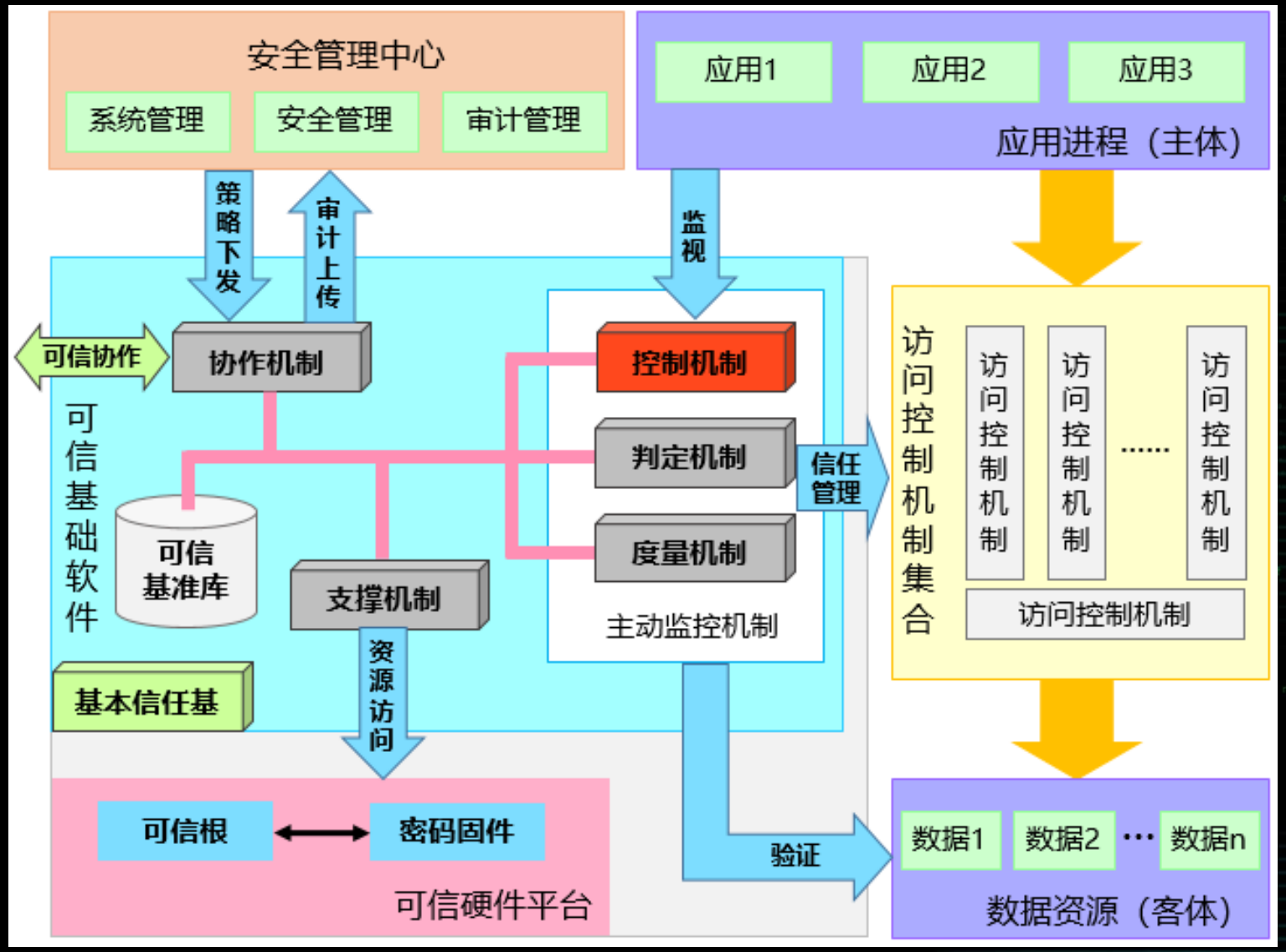


3、创新主动免疫体系结构



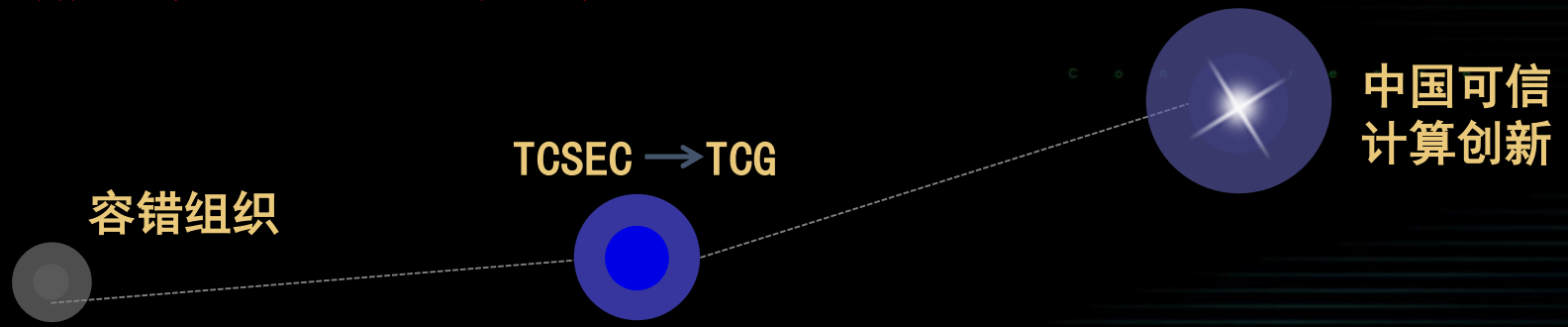
克服了TCG部件TPM被动挂接调用的局限性

计算节点可信架构


安全管理中心
系统管理
安全管理
审计管理
应用1
应用2
应用3
应用进程（主体）
策略下发
审计上传
监视
可信协作
协作机制
控制机制
判定机制
度量机制
主动监控机制
可信基础软件
可信基准库
支撑机制
基本信任基
资源访问
信任管理
访问控制机制集合
访问控制机制
访问控制机制
.....
访问控制机制
访问控制机制
可信根
密码固件
可信硬件平台
验证
数据1
数据2
数据n
数据资源（客体）

4、开创可信计算3.0新时代

	可信1.0（主机）	可信2.0（PC）	可信3.0（网络）
特性	主机可靠性	节点安全性	公钥、对称双密码主动系统免疫
对象	计算机部件	PC单机为主	终端、服务器、存储系统体系可信
结构	冗余备份	功能模块	宿主+可信双节点平行架构
机理	故障诊查	被动度量	基于网络可信服务验证
形态	容错算法	TPM+TSS	动态度量实时感知
	世界容错组织为代表	TCG为代表	中国为代表



可信计算3.0主动防御免疫特性

分项	特性
理论基础	计算复杂性，可信验证
应用适应面	适用服务器、存储系统、终端、嵌入式系统
安全强度	强\可抵御未知病毒、未知漏洞的攻击、智能感知
保护目标	统一管理平台策略支撑下的数据信息处理可信和系统服务资源可信
技术手段	密码为基因，主动识别、主动度量、主动保密存储
防范位置	行为的源头，网络平台自动管理
成本	低，可在多核处理器内部实现可信节点
实施难度	易实施，既可适用于新系统建设也可进行旧系统改造
对业务的影响	不需要修改原应用程序代码，通过制定策略进行主动实时防护/业务性能影响3%以下

ISC 2019 7th
第七届互联网安全大会

3 PART

用可信计算3.0筑牢网络安全防线

1、坚持自主可控安全可信，加快产品推广应用

《国家中长期科学技术发展（2006-2020年）》明确提出“以发展高可信网络为重点，开发网络安全技术及相关产品，建立网络安全技术保障体系”。

可信计算广泛应用于国家重要信息系统，如：增值税防伪、彩票防伪、二代居民身份证安全系统、中央电视台制播系统、电网调度系统等关键信息基础设施安全保障，已成为国家法律、战略、等级保护制度要求，推广应用。

重要核心系统规模化推广应用

自主可信计算平台产品设备有三种形态：

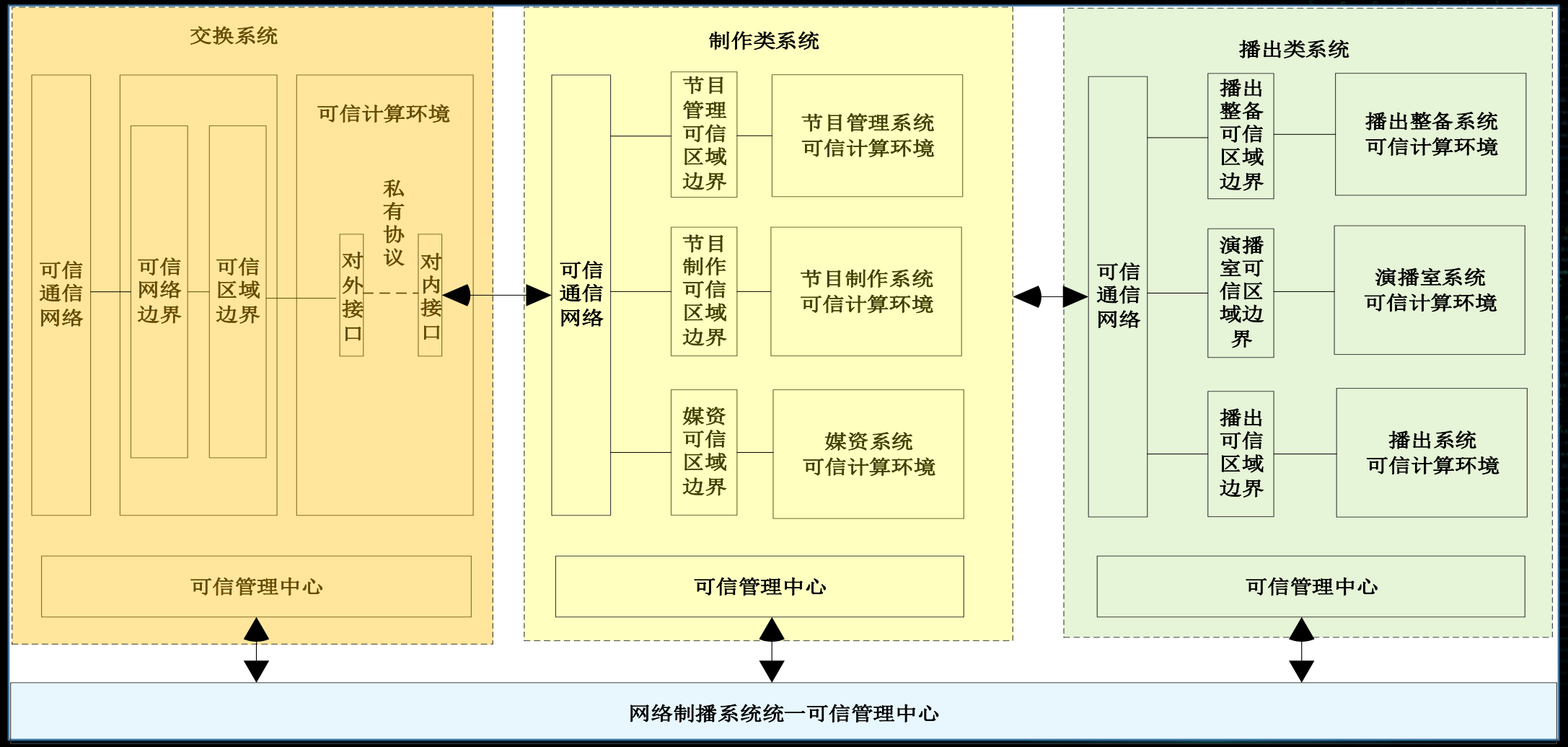
- 系统重构可信主机
- 主板配插PCI可信控制卡
- 配接USB可信控制模块

可以方便地通过可信网络支撑平台把现有设备升级为可信计算机系统，而应用系统不用改动，便于新老设备融为一体，构成全系统安全可信。

1）中央电视台可信制播环境建设

中央电视台播出42个频道节目，面向全球提供中、英、西、法、俄、阿等语言电视节目，在不能与互联网物理隔离的环境下，建立了可信、可控、可管的网络制播环境，达到四级安全要求，确保节目安全播出。**经受住了永恒之蓝勒索病毒攻击的考验，胜利完成了一带一路世界峰会的保障任务。**

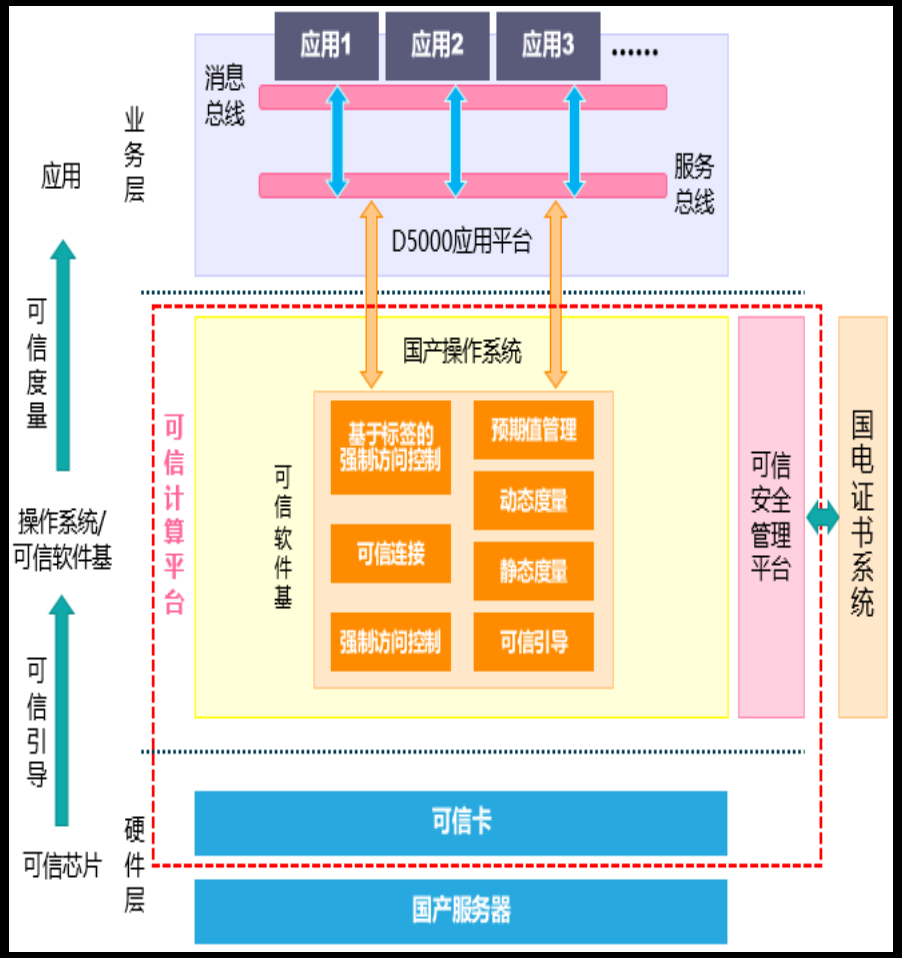
中央电视台电视节目生产、存储、编排和播出流程可信环境建设示意图



2）国家电网电力调度系统安全防护建设

发改委14号令决定以可信计算架构实现等级保护四级。

电力可信计算密码平台已在三十四个省级以上调度控制中心使用，覆盖上千套地级以上电网调度控制系统，涉及十几万个节点，约四万座变电站和一万座发电厂，有效抵御各种网络恶意攻击，确保电力调度系统安全运行。



国家电网电力调度系统安全架构

- 高效处理：实时调度
- 不打补丁：免疫抗毒
- 不改代码：方便实施
- 精练消肿：降低成本

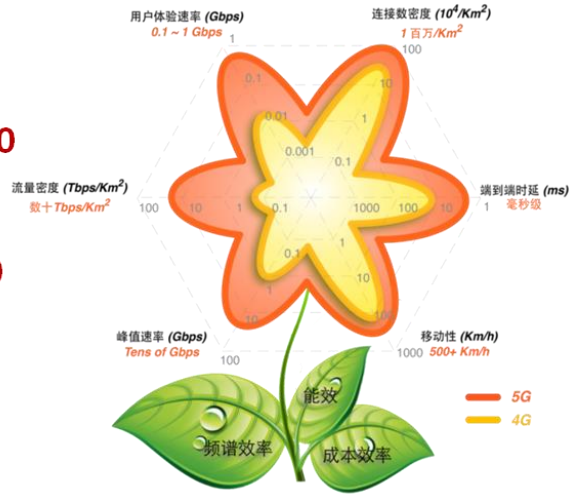
2、5G移动网络安全可信保障

5G愿景：面向**万物互联**的愿景设计

网络指标：**5G之花**

峰值速率**更高**
4G x **10~100**

体验速率**更快**
4G x **10~100**



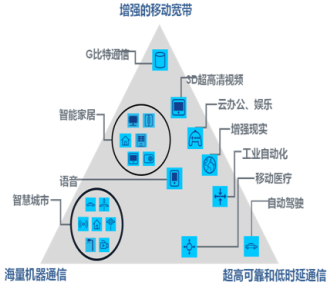
空口时延**更低**
4G x **1/5**

频谱效率**更高**
4G x **3~5**

能效**更高**
4G x **100**

不仅考虑人与人，也考虑人与物、物与物：
增强移动宽带、海量物联网、低时延高可靠物联网

增强移动宽带（
100Mbps~1Gbps）

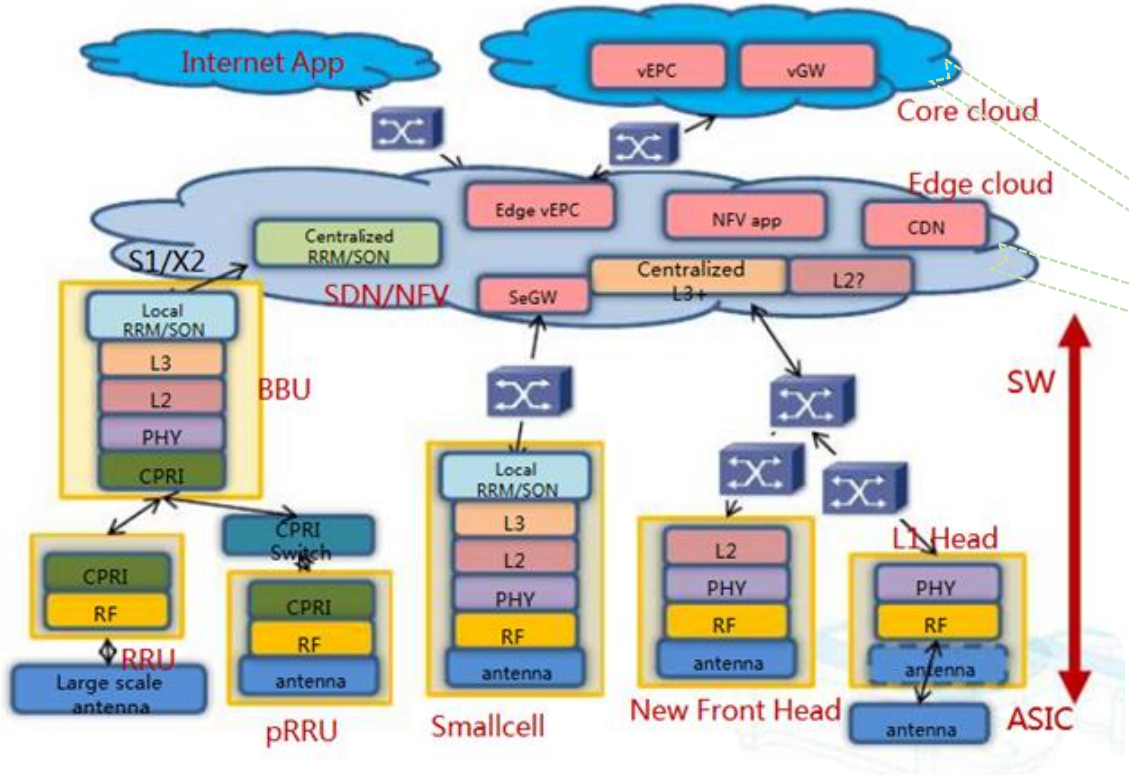


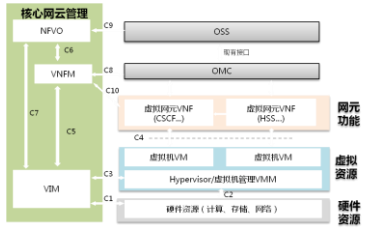
海量机器连接
（百万/平方公里）

超高可靠、低时延
（99.999%）

5G移动网络的演进

5G网络在传统电信云的基础上引入**NFV/SDN**等技术进行ICT融合，将移动通信网络**云化**、**虚拟化**和**软件化**，使网络变得更灵活、敏捷和开放。





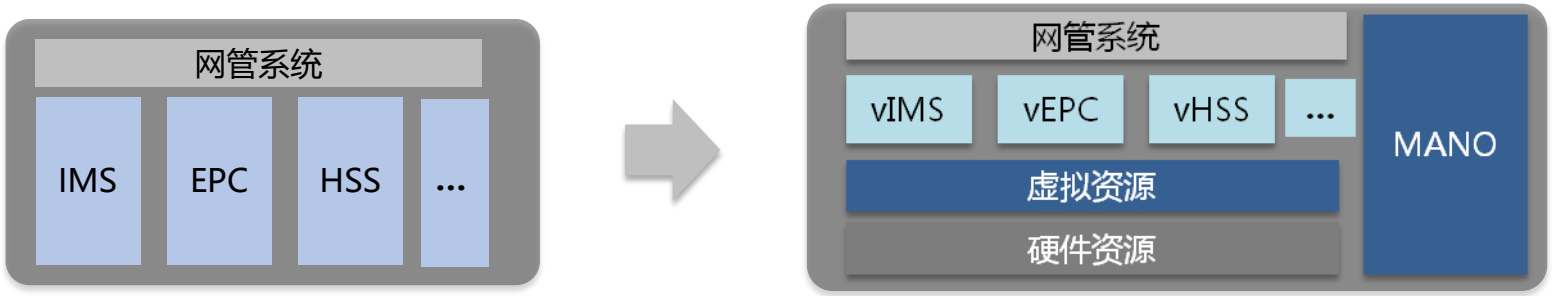
虚拟化软件及网元

通用服务器

在5G网络的核心云和边缘云中传统的网络设备将被**通用服务器**及**虚拟化网元**软件所代替

5G网络虚拟化-NFV技术

NFV（Network Function Virtualization）于13年在ETSI由13家运营商发起，是采用虚拟化技术、基于通用硬件实现电信功能节点的软件化，专注于快速部署、应用规模扩展和升级



四大基本特征

虚拟化
采用开放和工业标准的Hypervisor和管理软件将电信业务的软硬件分离

通用基础设施
标准化计算、存储、网络

云化管理
应用和业务的生命周期管理，虚拟资源配置

网络自动化
可与SDN结合，使用SDN技术自动化配置网络

NFV打破传统电信设备的竖井式体系，其核心是设备虚拟化、网元的分层解耦和引入新的MANO集中管理体系实现全生命周期管理

5G核心网络可信计算架构

★ 网络基础设施可信防护

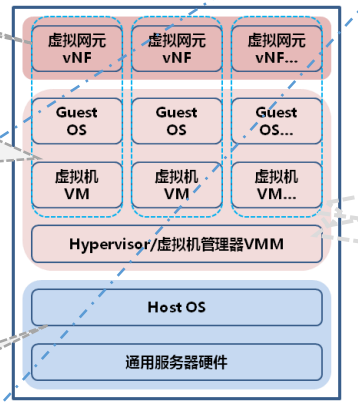
★ 网络管理连接可信防护

可信安全管理平台

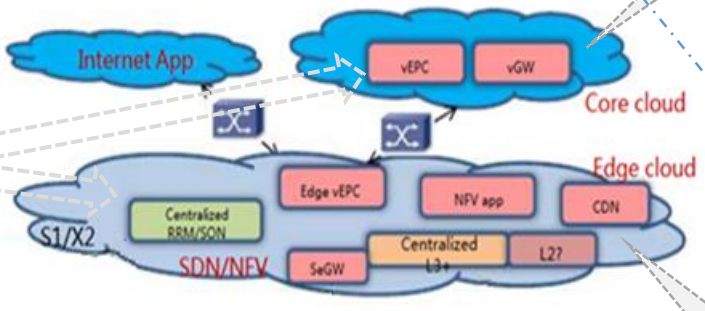
虚拟网元安全：
- 虚拟网元度量及运行监控
- 虚拟网元配置度量

虚拟系统安全：
- 虚拟可信根
- VMM度量及运行监控
- VM镜像度量及启停监控
- VM可信迁移
- GuestOS+可信软件基
- 虚拟机可信隔离

通用服务器安全：
- 物理可信根
- 启动度量及可信链扩展
- HostOS+可信软件基



通用服务器及虚拟系统



核心云安全：
- 网络编排管理可信
- 切片管理可信
- 外部管理终端可信

边缘云安全：
- MEC管理可信
- 移动专网管理可信
- 网络接入可信

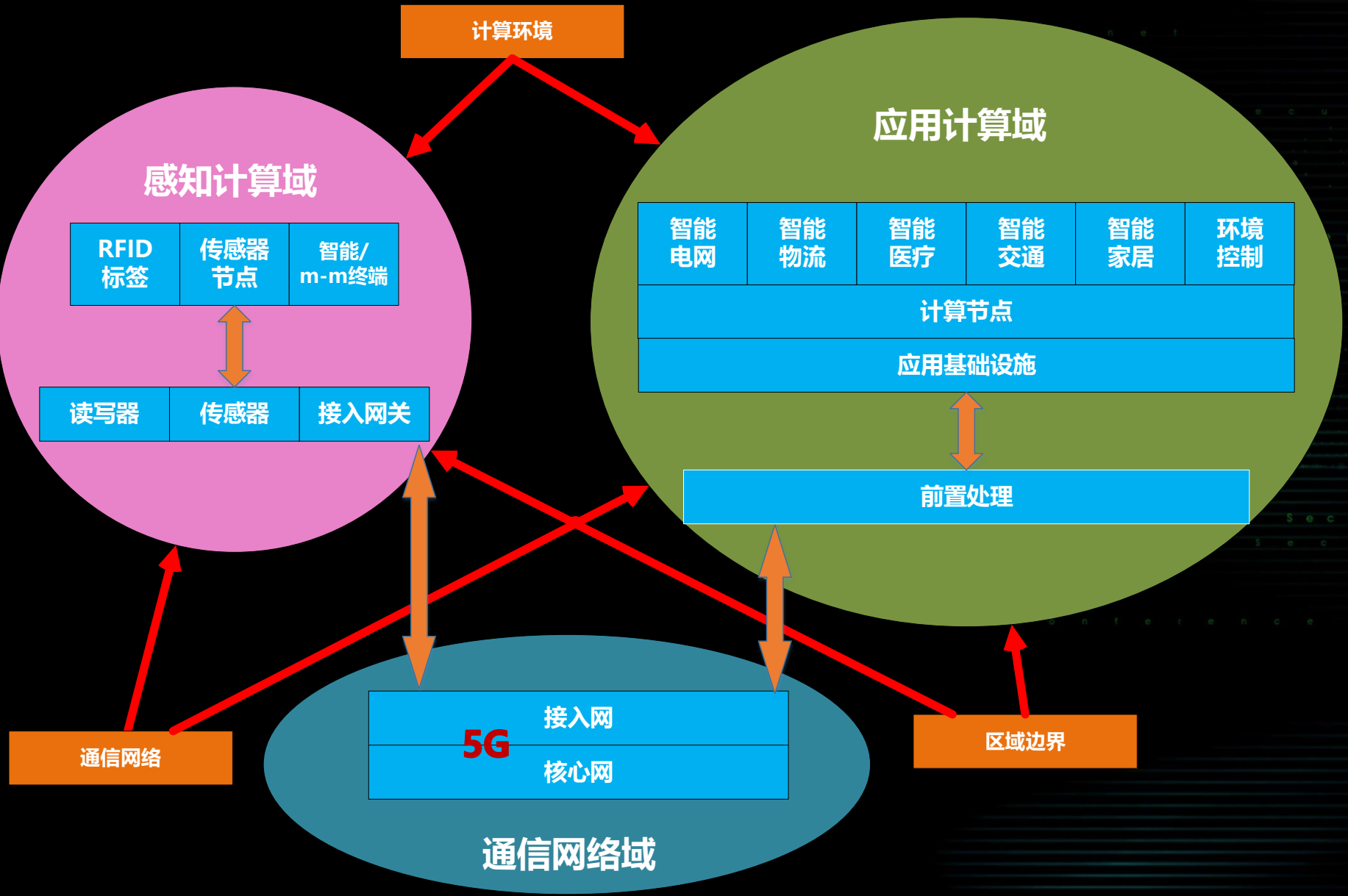
3、执行等级保护2.0标准筑牢网络安全防线

网络安全等级保护新标准特点

1. 基本要求、测评要求和技术要求框架统一，安全管理中心支持下的三重防护结构框架
2. 通用安全要求+新型应用安全扩展要求，将云计算、移动互联、物联网、工业控制等列入标准规范
3. 把基于可信根的可信验证列入各级别和各环节的主要功能要求

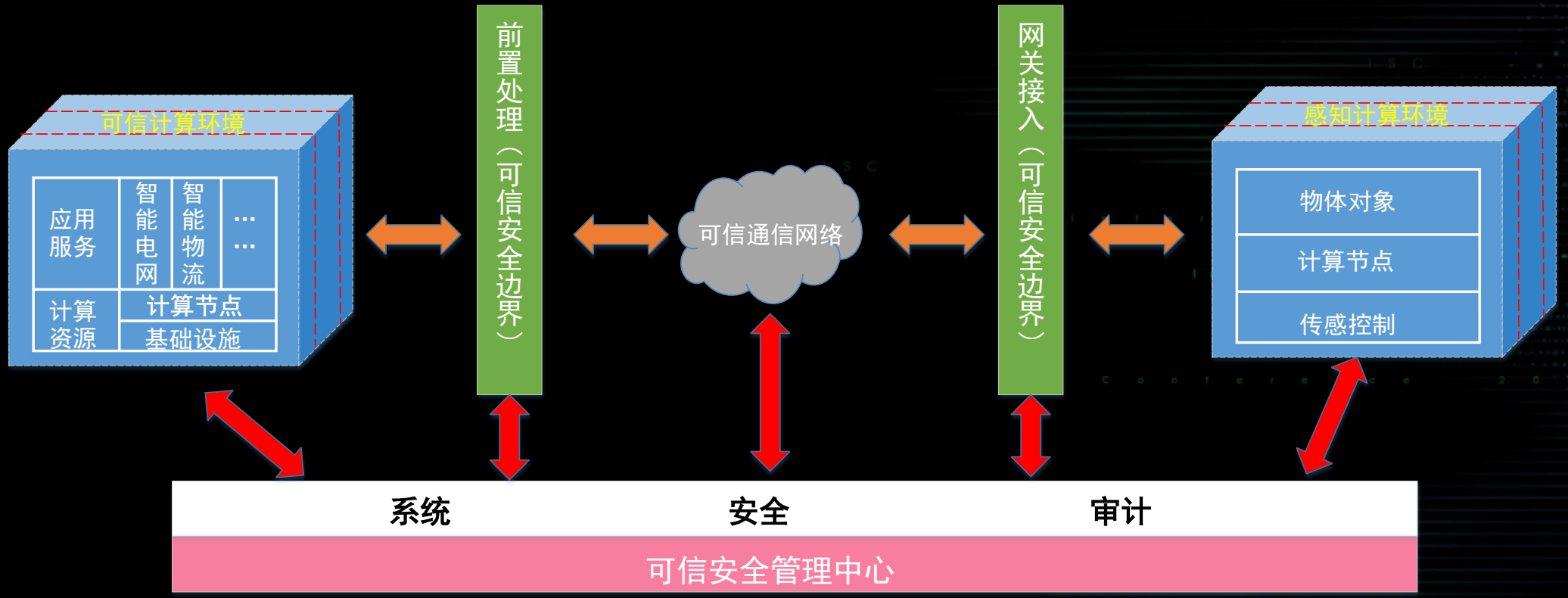
可信宿主	TCM	TPCM	检验软件	可信软件基（TSB）		
	静态可信验证基础软件可信			建链检验 应用程序可信	动态度量 执行环境	实时感知 关联态势
	BIOS	引导OS，装载系统		应用加载	应用执行	所有执行
	一级			二级	三级	四级

建设安全可信的物联网系统



物联网环境安全架构

（安全管理中心支持下的三重防御）



ISC 2019 第七届互联网安全大会

谢　谢