2017 中国互联网安全大会
China Internet Security Conference

用可信计算构筑区块链安全

沈昌祥

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

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

·科学的网络安全观

·中国可信计算革命性创新

·主动免疫的区块链安全

序

5月12日，一款名为“WannaCry”的勒索病毒网络攻击席卷全球。被攻击计算机的数据文件被加密，只有支付高额赎金才能解密恢复，从而导致大量信息系统无法正常工作，服务被中断、严重影响系统的可用性。

据统计，目前有近150个国家受害，仅当天我国就有数十万例感染报告，教育、交通、医疗、能源网络成为本轮攻击的重灾区，大量加油站无法提供服务。随着时间的推移，WannaCry病毒出现大量变种，如不进行有效扼制其造成的危害也会不断扩大

多家媒体报道：中国自主创新的可信计算3.0可以有效抵御“WannaCry”勒索病毒攻击。采用可信计算3.0技术的操作系统免疫平台能够在计算机信息系统上建立对未知病毒木马以及系统漏洞的防御能力，从根本阻止未知攻击事件

继“WannaCry”勒索病毒事件之后，最近又一起名为“Petrwrap”勒索病毒事件发生。通过对病毒样本的严格测试，在可信计算3.0安全机制的层层保护下，系统同样没有被干扰

《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

近期发布的《**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。”

ISC 2017 中国互联网安全大会

360互联网安全中心

科学的网络安全观

网络空间安全

是

- 计算科学问题
- 体系结构问题
- 计算模式问题

1、网络安全是永远主题

由于人们对IT的认知逻辑的局限性，不能穷尽所有组合，只能局限于完成计算任务去设计IT系统，必定存在逻辑不全的缺陷，从而难以应对人为利用缺陷进行攻击

因此，为了安全必须从**逻辑正确验证、计算体系结构**和**计算模式**等方面进行科学技术创新，以解决逻辑缺陷不被攻击者所利用的问题，形成攻防矛盾的统一体

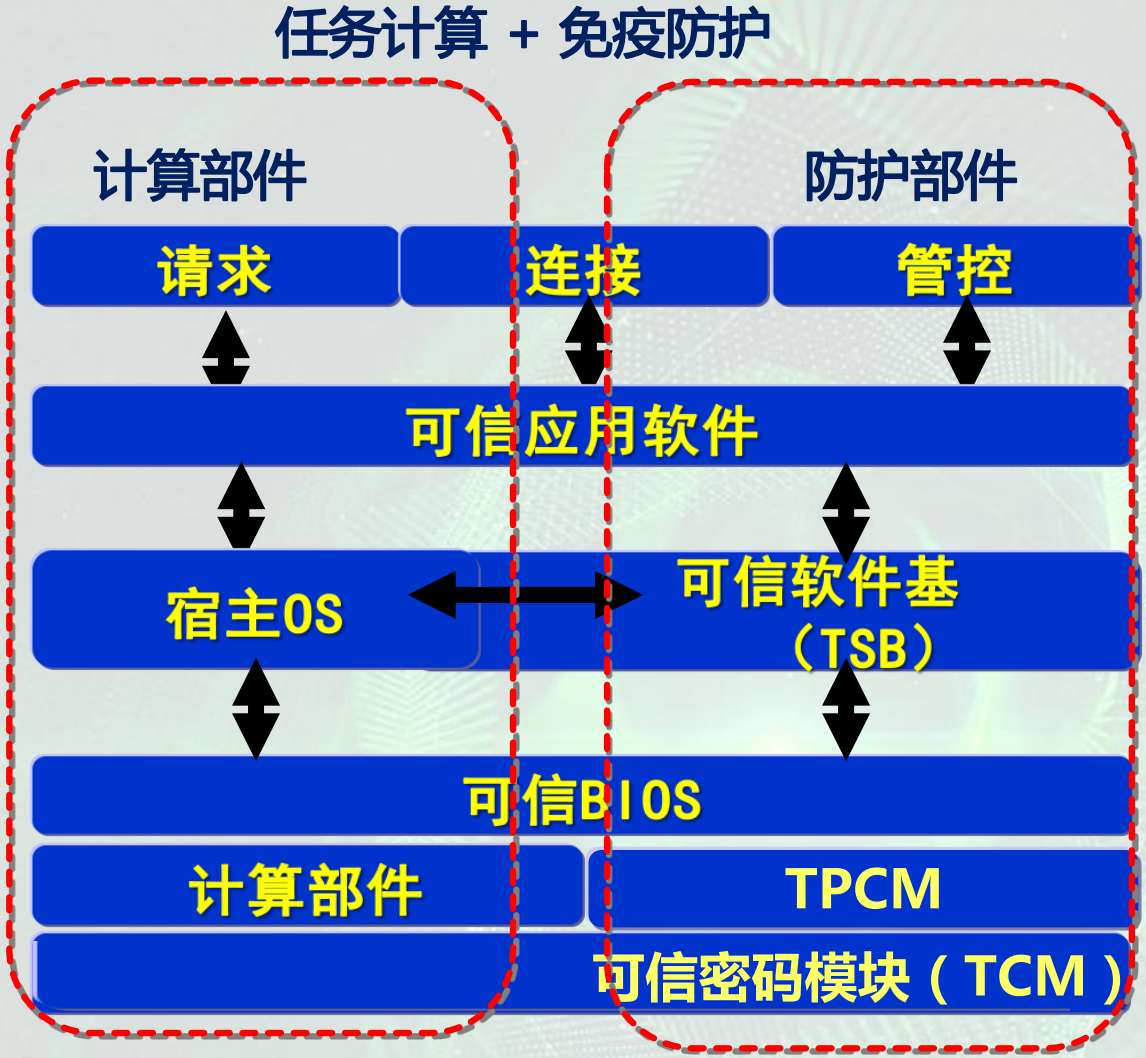
确保为完成计算任务的逻辑组合不被篡改和破坏，实现正确计算，这就是**主动免疫防御**，“老三样”封堵查杀被动防御已经过时

2、可信免疫的计算模式与结构

可信计算是指计算运算的同时进行安全防护，计算全程可测可控，不被干扰，使计算结果总是与预期一样。只有这样才能改变只讲求计算效率，而不讲安全防护的片面计算模式

是一种运算和防护并存的主动免疫的新计算模式，**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”成份，从而破坏与排斥进入机体的有害物质，相当于为计算机信息系统培育了免疫能力

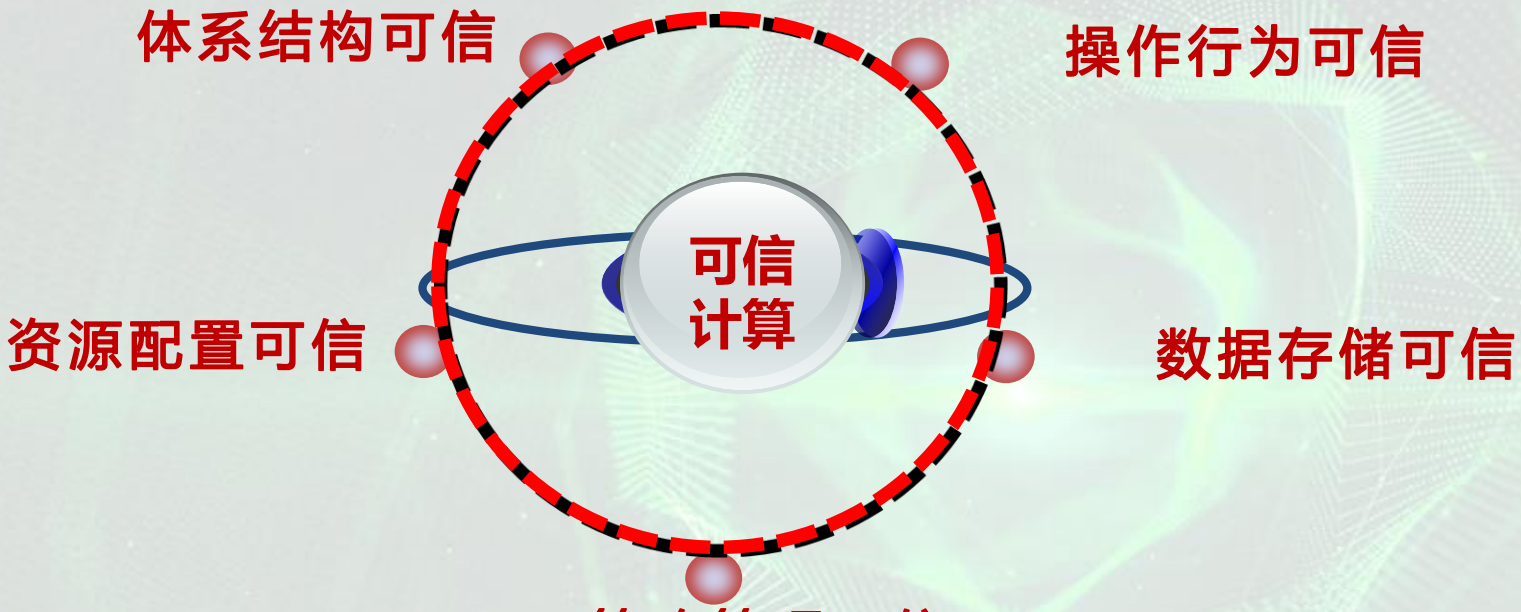
可信支持的双体系结构



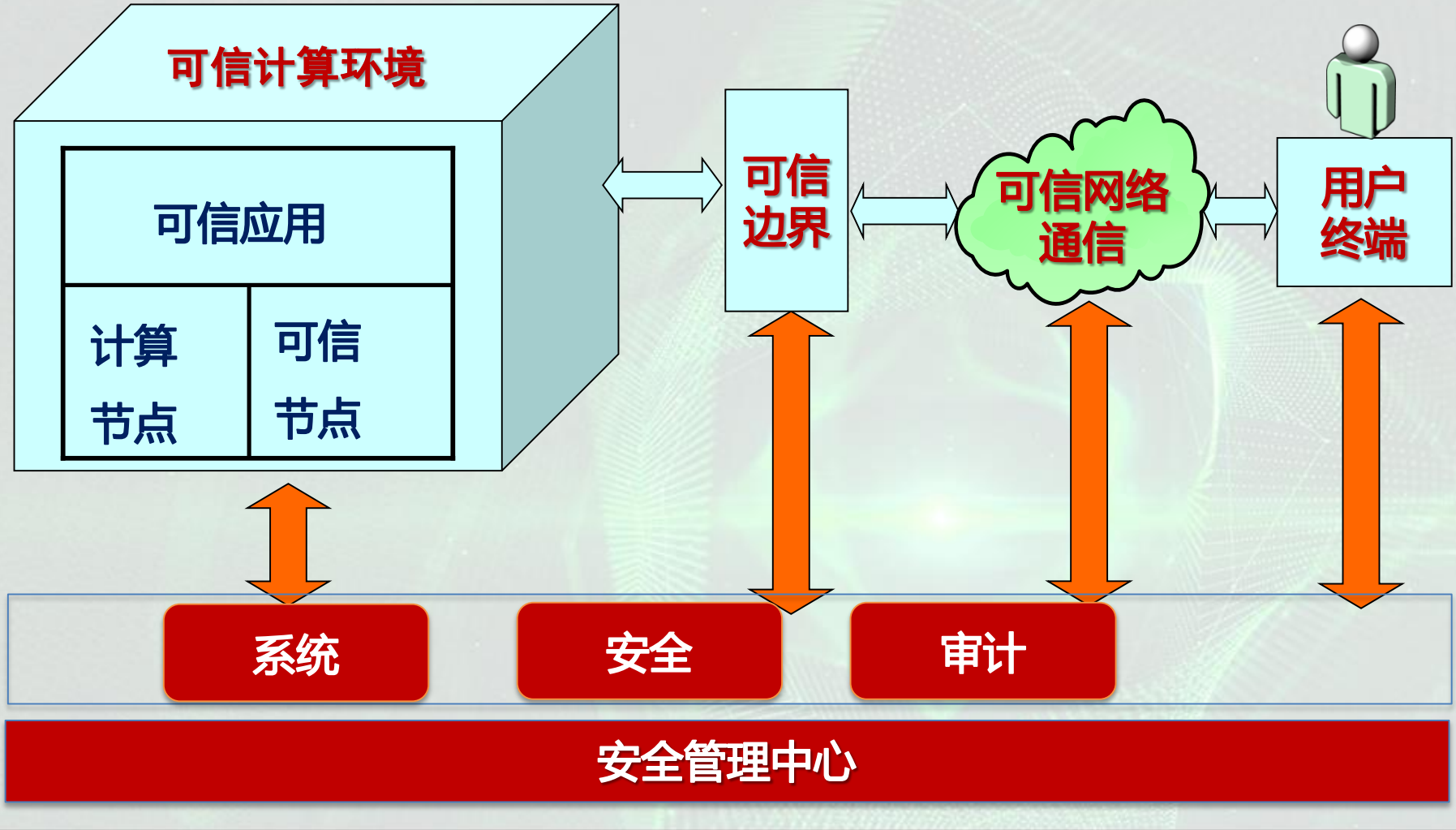
可信支持的双体系结构

3、安全可信系统架构

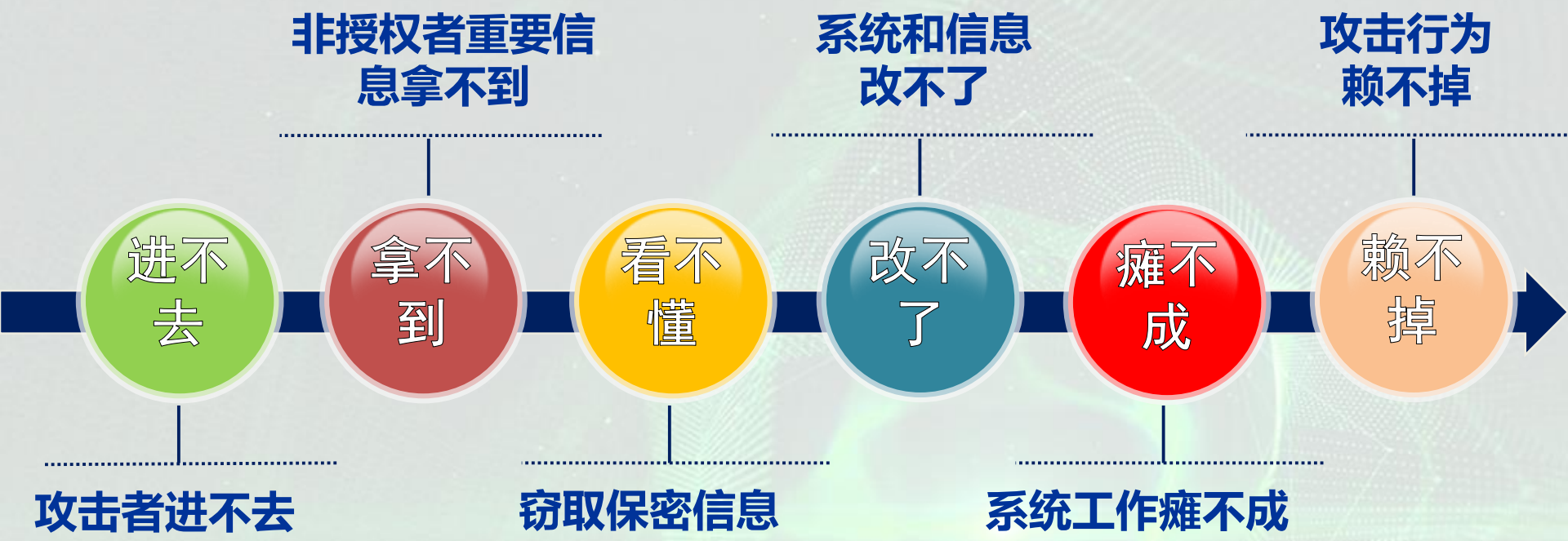
网络化基础设施、云计算、大数据、工业控制、物联网等新型计算环境必须进行可信度量、识别和控制，确保：



构建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 2017 中国互联网安全大会

360互联网安全中心

中国可信计算革命性创新发展

我国为确保核心机密安全，与1992年正式立项研究**主动免疫的综合防护系统**，经过长期攻关，军民融合，形成了自主创新的可信体系，（不少已被国际可信计算组织（TCG）采纳），已经成为夯实我国网络安全防线的基础

国内权威媒体进行高度评价

ISC 2017 中国互联网安全大会
360互联网安全中心

中国共产党中央委员会主办 2015·20
QIUSHI

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

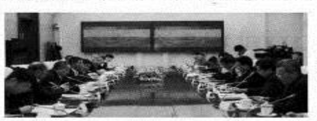
网络空间如今已成为大国博弈的又一个主战场。构筑网络安全堤坝离不开技术的支撑，可信计算作为一种主动免疫的新型计算模式，在确保数据安全等方面优势显著。在2016年1月8日召开的中国可信开放与网络安全高峰论坛上，与会专家纷纷表示，发展具有中国自主知识产权的可信高端计算系统产业链，对于维护我国的网络安全和网络空间主权意义深远。

中国可信开放与网络安全高峰论坛在京召开

加速推进可信计算产业化 构筑网络空间安全堤坝

网络安全挑战日益严峻

核心技术不能受制于人



可信计算安全优势凸显

CHINA TOP BRANDS 中国名牌

可信计算：网络安全的主动防御时代

可信计算技术及可信计算系统产业的出现，颠覆了人们以往对网络安全防护的认知，变"被动防御"为"主动防御"，让信息交互平台中最难能可贵的信任基础与信任保障，驶上高速信息安全的快车道。

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）讲述可信计算的研究与应用

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

2、创新可信密码体系

密码算法创新

全部采用国家自主设计的算法，
定义了可信计算密码模块（TCM）

密码机制创新

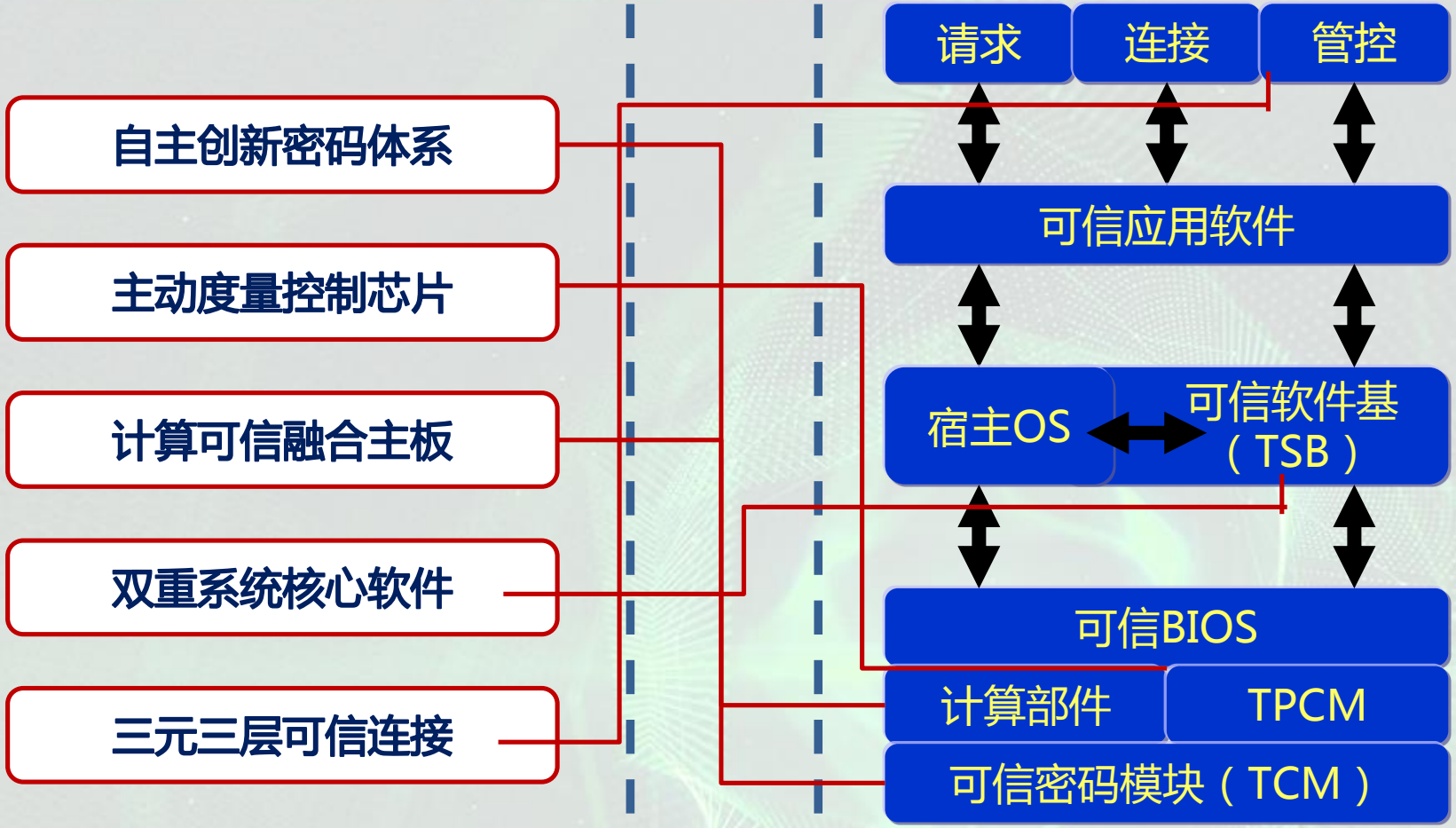
对称密码与公钥密码相结合，
提高了安全性和效率

证书结构创新

双证书结构，简化证书管理，
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

3、创新主动免疫体系结构

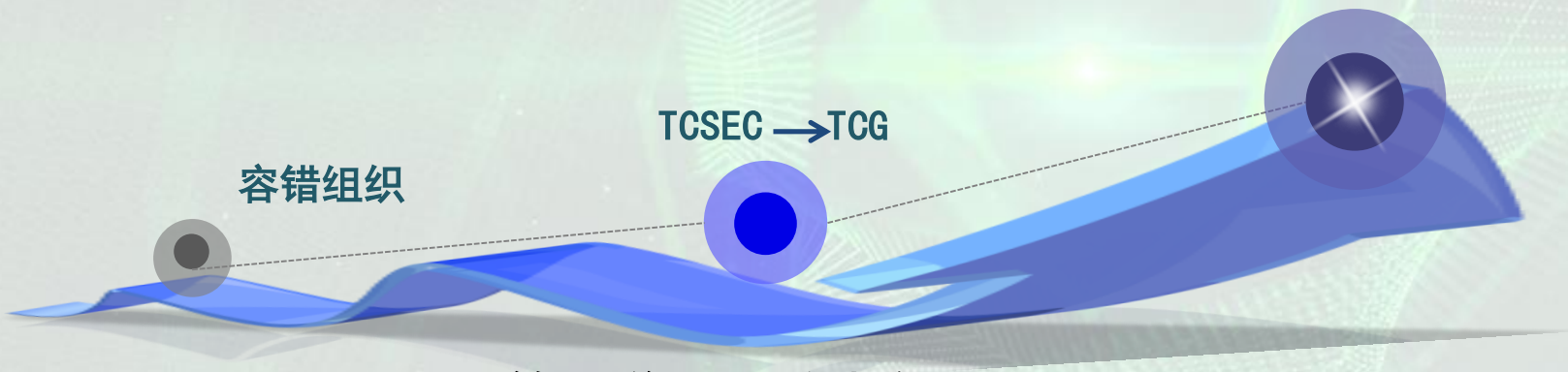


克服了TCG部件TPM被动挂接调用的局限性

4、开创可信计算3.0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	系统免疫性
对象	计算机部件	PC单机为主	节点虚拟动态链
结构	冗余备份	功能模块	宿主+可信双节点
机理	故障诊查	被动度量	主动免疫
形态	容错算法	TPM+TSS	可信免疫架构

世界容错组织为代表　　TCG为代表　　中国为代表



计算科学、体系结构的发展

5、构筑主动防御、安全可信的保障体系

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

可信计算构建主动免疫体系

控制

识别

制定可信主、客体间访问规则

报警

确定可信主、客体

审计主客体访问行为
监控主客体运行时状态

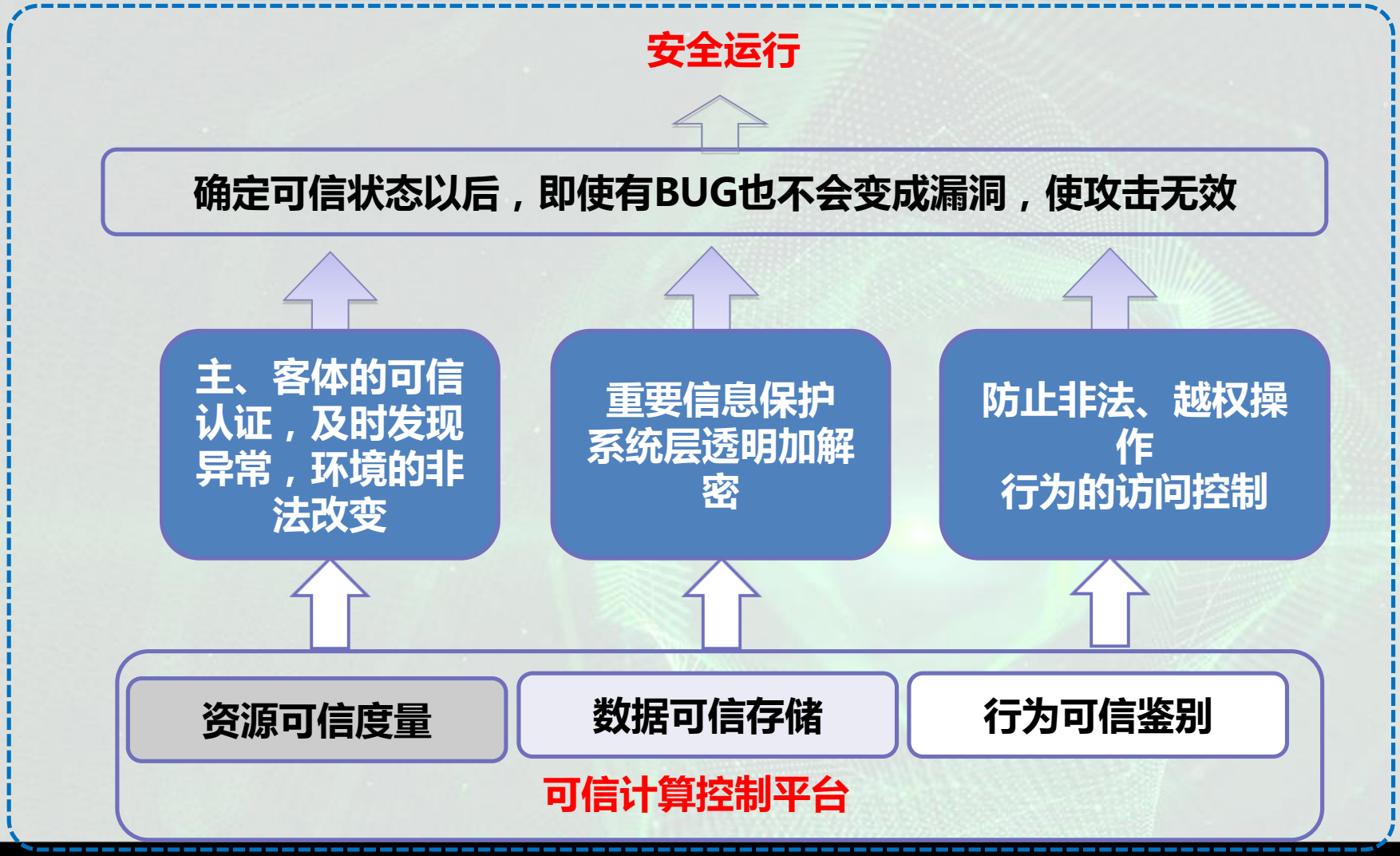
系统管理

安全管理

审计管理

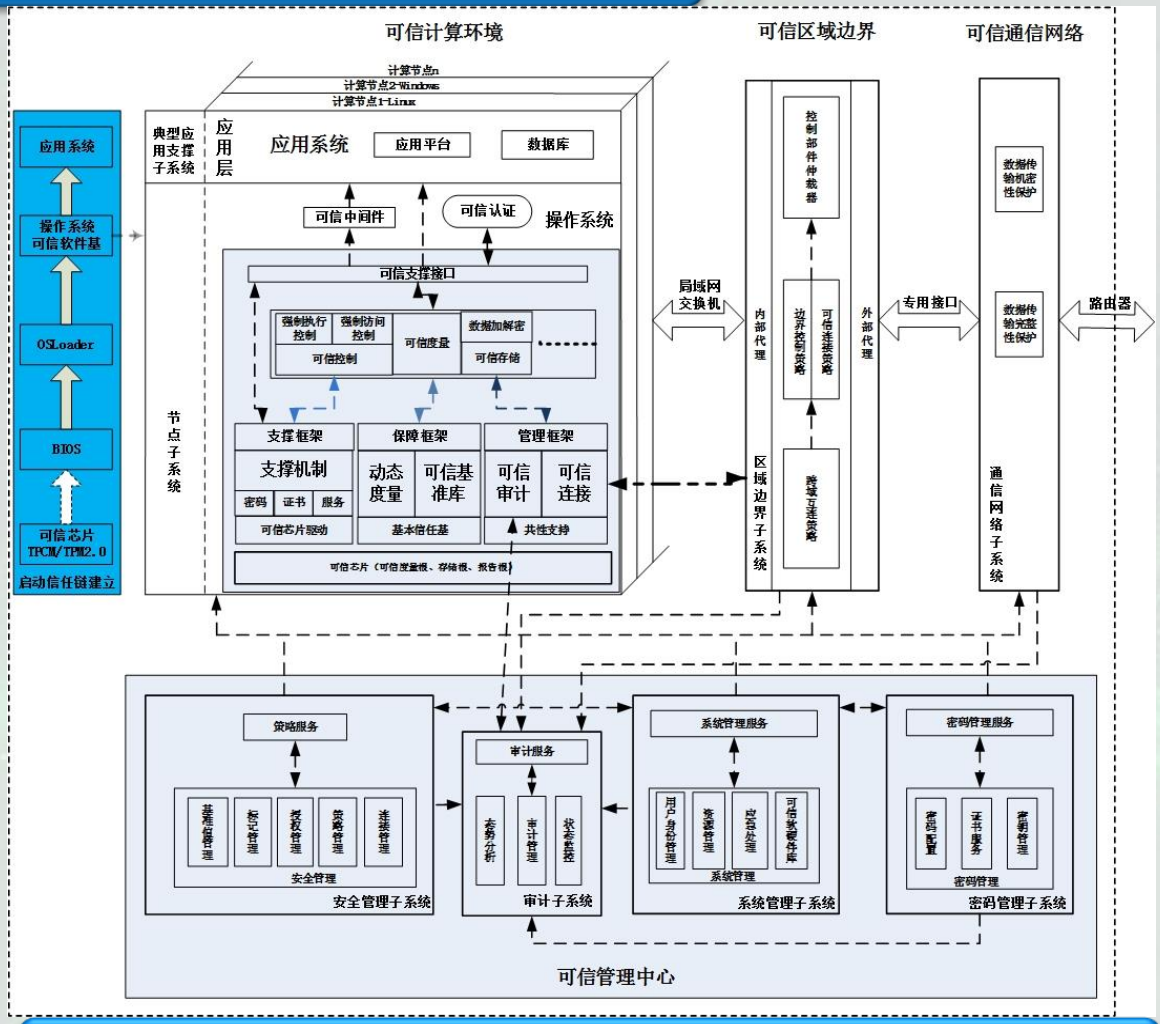
可信安全管理平台

可信计算构建主动免疫体系



高安全等级可信防护体系

部署可信计算平台后，在原有信息系统建立可信免疫的主动防御安全防护体系，实现高安全等级结构化保护，改变原被动防护局面



GB/T25070-2010

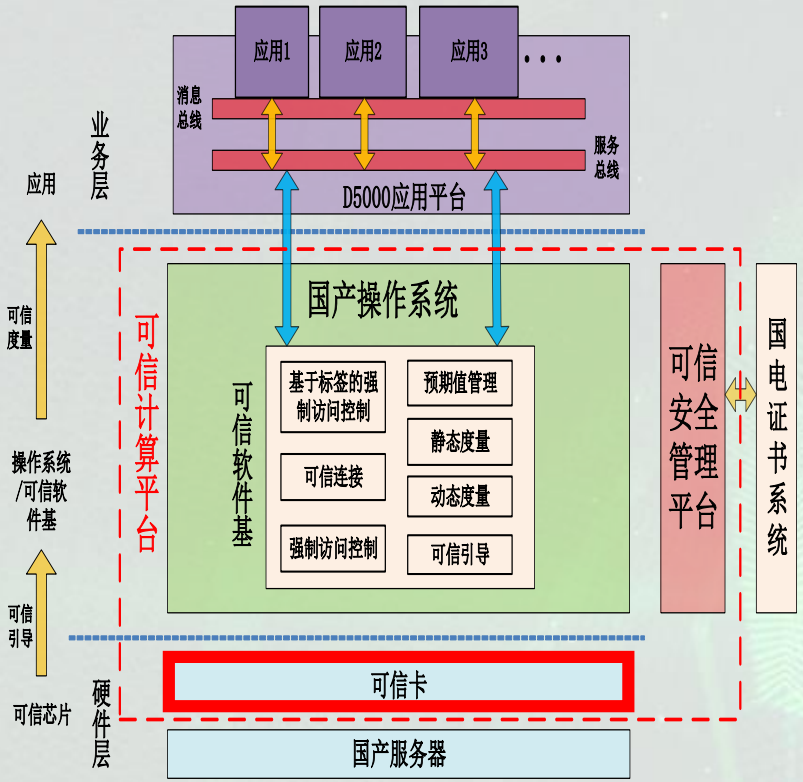
6、重要核心系统规模化建设应用

1）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34个省级以上调度控制中心和59个地级调度控制中心上线运行，覆盖了上万台服务器，确保了运行安全

国家电网电力调度系统



应用	CPU使用率			内存使用率			计算时间		
	加载前	加载后	影响度	加载前	加载后	影响度	加载前	加载后	影响度
应用1	2.92%	2.95%	1.03%	11%	11%	0%	69s	69.9s	1.3%
应用2	2.3%	2.33%	1.3%	6.9%	7%	1.45%	24.6s	25.1s	2.03%
应用3	2.8%	2.85%	1.79%	7.8%	7.9%	1.28%	18.9s	19.4s	2.65%

- 采用PCI可信卡的方式进行部署实施
- 实现了对已知、未知恶意代码的免疫
- 实现了可信保障机制，使得系统运行效率有限降低
- 基于D5000平台的安全标签，不许改动源代码

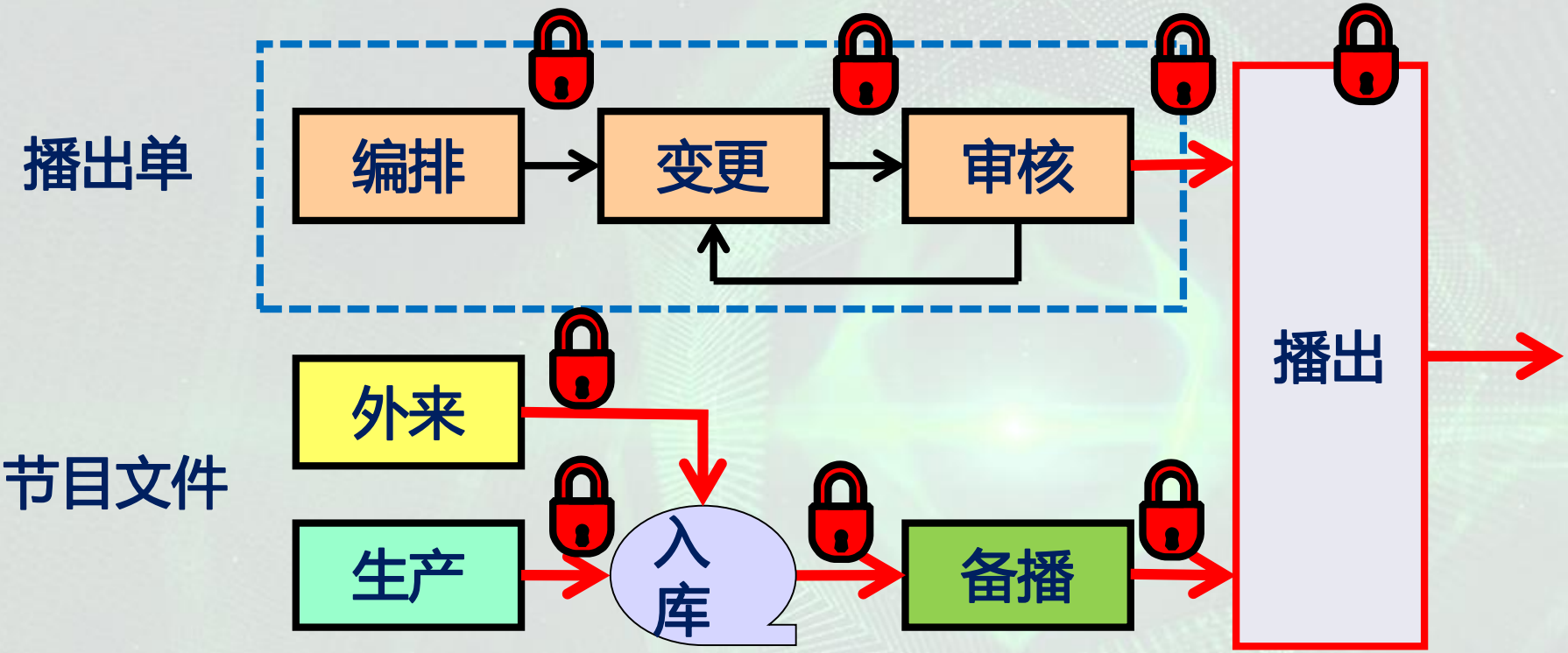
……

通过逐级认证实现系统的主动免疫，达到等级保护四级技术要求

2）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，在没有与互联网物理隔离的计算机网络环境下，构建了网络制播的可信计算安全技术体系，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

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



ISC 2017 中国互联网安全大会

360互联网安全中心

主动免疫的区块链安全

区块链的安全威胁

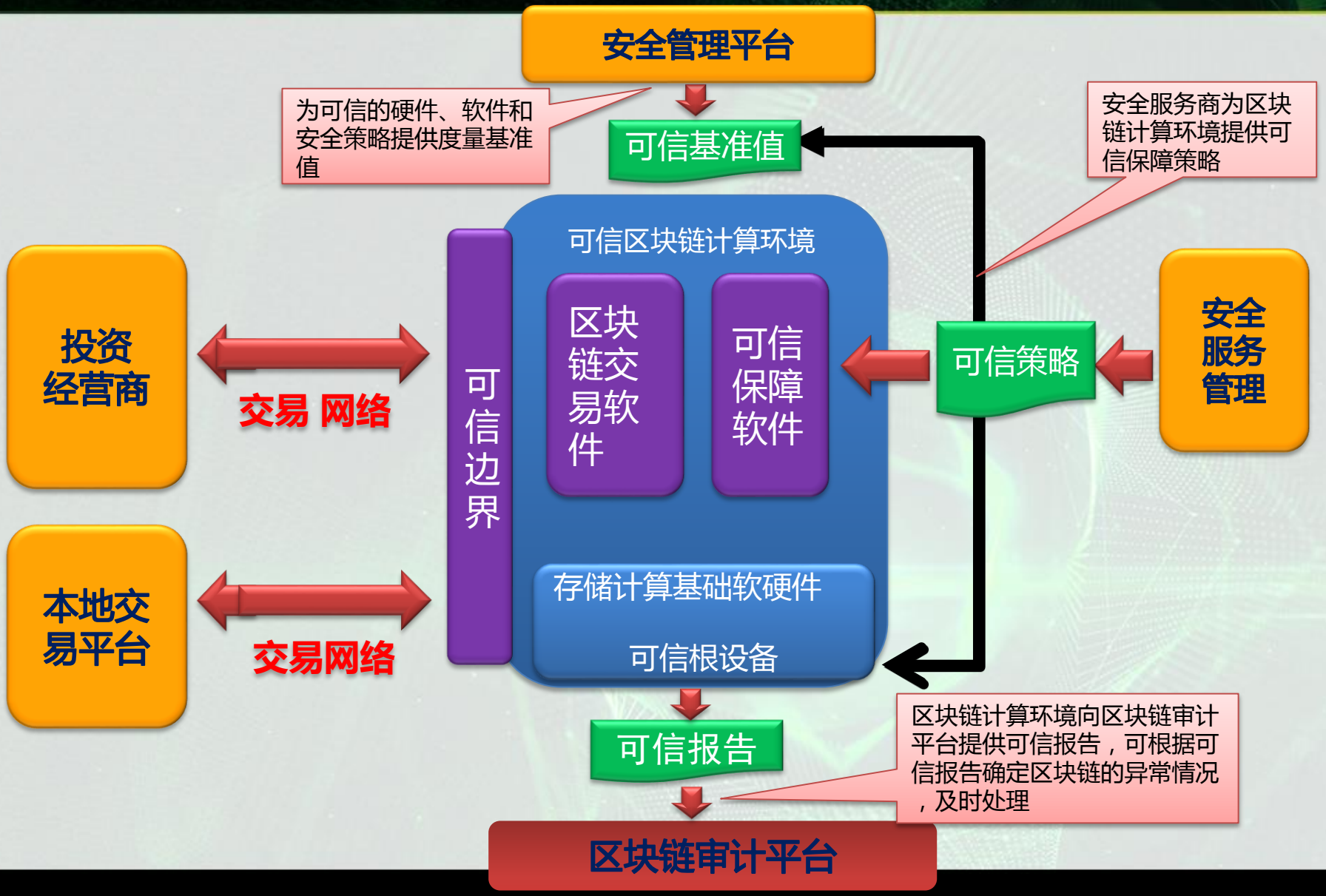
- 区块链是一种利用密码学技术，将系统内有效交易进行编码的可附加账本
  - 每次交易必须有效
  - 系统必须对数字资产的归属达成共识
  - 过往历史不能篡改
- 区块链的安全与其他重要信息系统等同
  - 业务应用信息安全：交易有效、达成共识
  - 系统服务资源安全：不能篡改、不能中断

- 2010年8月，曾发生利用整数溢出漏洞凭空造出了1840亿个比特币
- 2016年5月，数字自治组织DAO（风投基金、区块链创业者技术开发社区、去中心的基金）因发现有漏洞（9个）而失败
- 最近席卷全球的勒索病毒对区块链是极大的威胁

用主动免疫可信计算技术保护区块链

- 计算资源可信
  - 区块链计算过程不被恶意干扰，主动免疫防止恶意攻击
- 交易数据可控
  - 比特币等区块链数据能够安全可信存储与传输
- 交易过程可靠
  - 交易过程真实可信，不可伪造，可信共管

安全可信区块链组成


安全管理平台
为可信的硬件、软件和安全策略提供度量基准值
可信基准值
安全服务商为区块链计算环境提供可信保障策略
可信区块链计算环境
区块链交易软件
可信保障软件
可信边界
投资经营商
交易 网络
本地交易平台
交易网络
可信策略
安全服务管理
存储计算基础软硬件
可信根设备
可信报告
区块链计算环境向区块链审计平台提供可信报告，可根据可信报告确定区块链的异常情况，及时处理
区块链审计平台

结束语

面临日益严峻的国际网络空间形势，我们要立足国情，创新驱动，解决受制于人的问题。坚持纵深防御，用可信计算3.0构建网络空间安全主动免疫保障体系，筑牢网络安全防线，为把我国建设成为世界网络安全强国而努力奋斗！

谢　谢