网络空间安全导论

主讲人： 杜瑞颖



目录

信息系统安全

一 信息系统安全的概念

二 信息系统的硬件系统安全

三 信息系统的操作系统安全

四 信息系统的数据库系统安全

五 可信计算

六 工业控制系统安全

五. 可信计算

可信计算的发展历程

① 可信计算的出现

□彩虹系列的不足

- 提出了安全要求，却没有给出如何达到的技术路线
- 强调了秘密性，忽视了完整性和可用性

□ 彩虹系列的出现形成了可信计算的第一次高潮。

□ 彩虹系列成为评价计算机系统安全的主要准则。

□ 至今对计算机系统安全有指导意义。

五. 可信计算

可信计算的发展历程

② 可信计算的高潮

- 1999年底美国IBM、HP、Intel、微软和日本Sony等著名企业参加，成立了可信计算联盟TCPA，标志着可信计算高潮的形成。
- 2003年TCPA改组为可信计算组织TCG（Trusted Computing Group）。TCG的成立标志着可信计算技术和应用领域的扩大。
- 在中国，瑞达公司和武汉大学合作，2000年开始研究可信计算
- 在欧洲，2006年OpenTC成立，推进欧洲可信计算

五. 可信计算

十年来可信计算的发展成果

① 在世界范围形成了可信计算的高潮

- TCG
  - **美国**：几乎所有著名IT公司都参加了TCG
  - **中国**：武汉大学、清华大学、北京工业大学、台湾高雄师范大学、联想、华为、国民技术、中标软件、瑞达等
- 欧洲OpenTC
- 中国可信计算联盟（CTCU）
- 产业化
- 广泛性

五. 可信计算

十年来可信计算的发展成果

② 制定出一系列的规范

- TCG的规范
  - 可信PC规范
  - 可信服务器规范
  - 可信平台模块（TPM）规范
  - 可信软件栈（TSS）规范
  - 可信网络连接（TNC）规范
  - 可信手机模块规范
  - 可信存储规范

五. 可信计算

十年来可信计算的发展成果

② 制定出一系列的规范

- 中国的规范
  - 可信计算平台密码技术方案（TCM）
  - 可信计算密码支撑平台功能与接口规范
  - 可信PC平台主板技术规范
  - 可信网络连接技术规范

  （已公示）
  - 可信平台模块芯片、服务器、软件、测评等规范还在制定中

五. 可信计算

十年来可信计算的发展成果

③ 推出一系列的可信计算产品

- 国外可信计算产品:
  - 推出多种TPM芯片，已销售5亿多片
  - 几乎所有的品牌笔记本电脑都配备了TPM芯片
  - 品牌台式机都配备了TPM芯片
  - IBM、HP、Intel提出可信服务器
  - 日本研制了可信PDA
  - MOTOROLA研制了可信手机
  - 多种可信网络连接产品

五. 可信计算

十年来可信计算的发展成果

③ 推出一系列的可信计算产品

- 国内可信计算产品
  - 瑞达和国民技术推出可信计算密码模块（TCM）安全芯片
  - 国民技术推出世界第一款TPM 2.0芯片
  - 多家公司推出了“可信计算密码支撑平台”
  - 瑞达、联想等公司推出几款可信PC机
  - 瑞达、华为等公司推出可信服务器
  - 武汉大学研制出可信PDA
  - 武汉大学研制出可信计算平台测评原形系统
  - 武汉大学、清华大学，研制出可信网络连接原形系统

五. 可信计算

可信计算的目标

- 提高计算机系统的可信性
- **现阶段做到**：确保平台资源完整性，数据安全存储，平台可信性远程证明

  注意：能够确保系统资源完整性，即可确保平台在一定条件下无恶意软件！
- **TCG的观点**：如果一个实体是可信的，则它的行为总是以预期的方式达到预期的目标。
- **我们的观点**：可信计算系统是能够提供系统的可靠性、可用性、安全性的计算机系统。通俗地说：可信≈可靠+安全（Trust≈Dependability + Security）。

五. 可信计算

可信计算的主要技术路线

- 首先在系统中建立一个信任根：
  - 硬件芯片　TPM
  - 软件　CRTM
- 然后再建立一条信任度量链，从信任根开始，一级度量一级，一级信任一级，从而把信任关系扩大到整个计算机系统，确保计算机系统的可信。
- 类似地，可将此技术路线用于网络连接和存储器，可得到可信网络连接和可信存储
- 可信计算的思想源于社会，把社会的成功管理经验用于计算机系统中

五. 可信计算

可信计算主要理论与技术

- 信任根技术

- **信任根的概念**

  - *信任根是系统可信的基础。*
  - *信任根的可信性由物理安全和管理安全确保。*
  - *TCG认为一个可信计算平台必须包含三个信任根：*
    - *可信测量根RTM（root of trust for measurement）*
    - *可信存储根RTS（root of trust for storage）*
    - *可信报告根RTR（root of trust for reporting）*

五. 可信计算

- **可信平台模块 TPM**
  - *可信存储根和可信报告根*
  - TPM本身就是一种SOC芯片（System on Chip）。
  - 它由CPU、存储器、I/O、密码运算器、随机数产生器和嵌入式操作系统等部件组成。

五. 可信计算

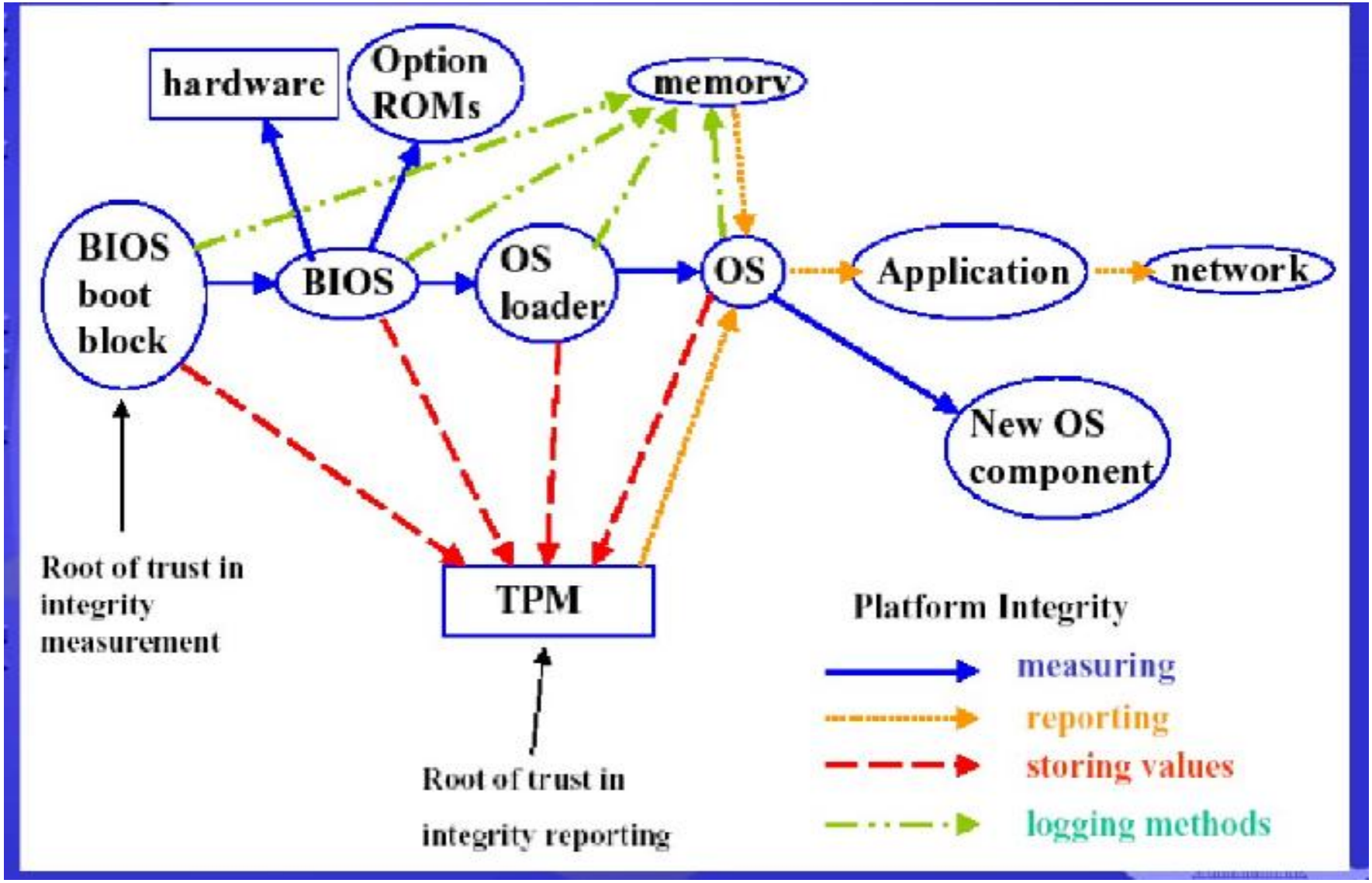

TPM的结构
I/O
密码协处理器
密钥产生
HMAC引擎
随机数产生器
SHA-1引擎
电源检测
Opt-Ln
执行引擎
非易失存储器
易失存储器

五. 可信计算

信任链技术

- 从信任根开始到硬件平台、到操作系统、再到应用，一级测量认证一级，一级信任一级。
- 信任链中的测量即是完整性测量，因此可确保系统资源的完整性。
- 完整性用被校验数据的HASH值来表征。

五. 可信计算


hardware
Option ROMs
memory
BIOS boot block
BIOS
OS loader
OS
Application
network
New OS component
Root of trust in integrity measurement
TPM
Root of trust in integrity reporting
Platform Integrity
measuring
reporting
storing values
logging methods

五. 可信计算

Wuhan University

可信计算主要理论与技术

- 可信计算平台技术

●主要特征是在主板上嵌有可信构建模块TBB。

● TBB就是可信PC平台的信任根。

♣可信测量根：软件的可信测量根核CRTM(Core Root of Trust for Measurement)

♣可信存储根和可信报告根：硬件的可信平台模块TPM(Trused Platform Module)。

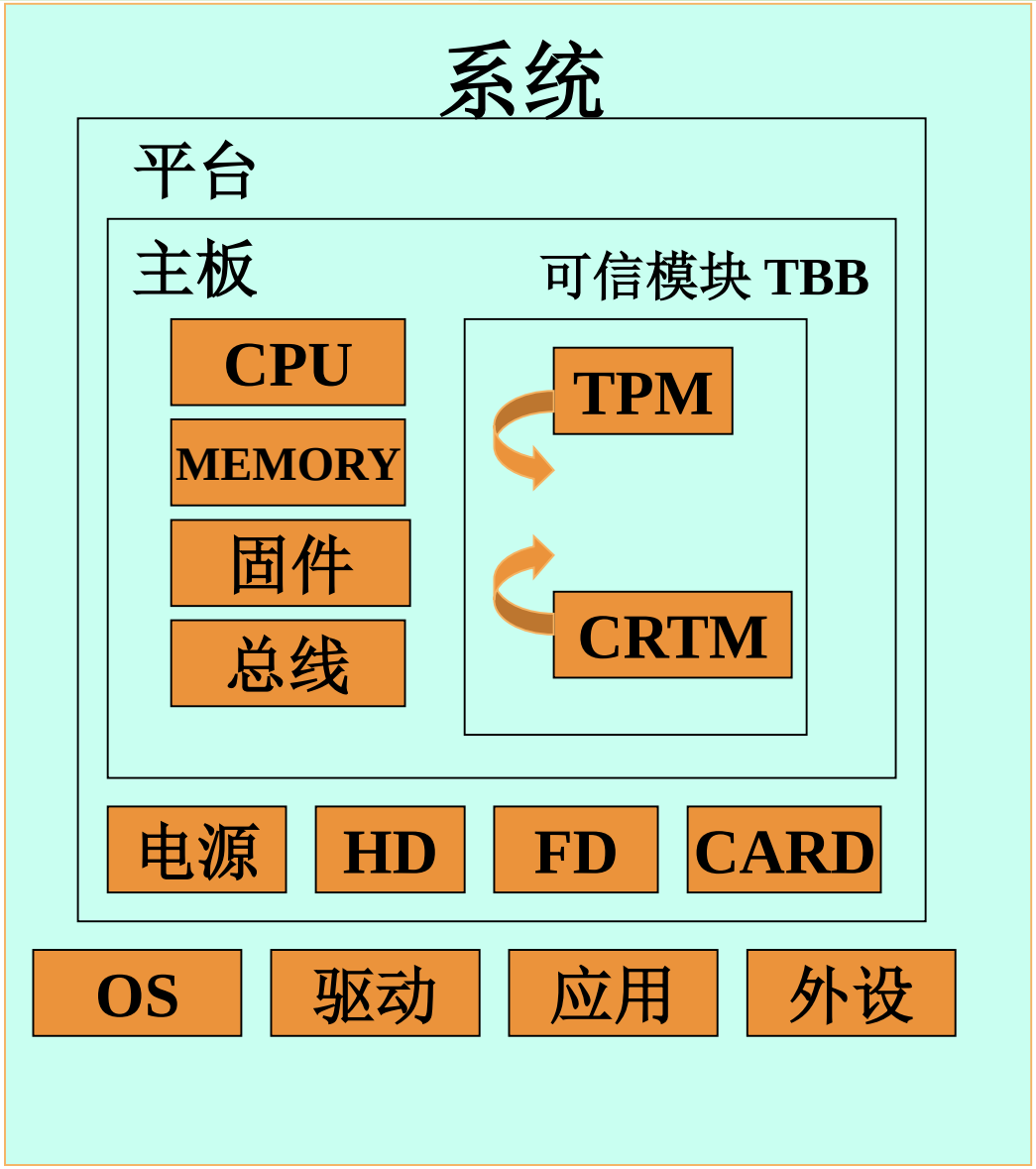
五. 可信计算

可信计算的主要技术路线

- **举例：可信PC硬件平台**
  - 主板
  - CPU、存储器和一些主要的外围设备
  - 嵌入式固件BIOS
  - 信任根：主板上的可信构建模块TBB（TPM和CRTM）（Trusted Building Block）

五. 可信计算

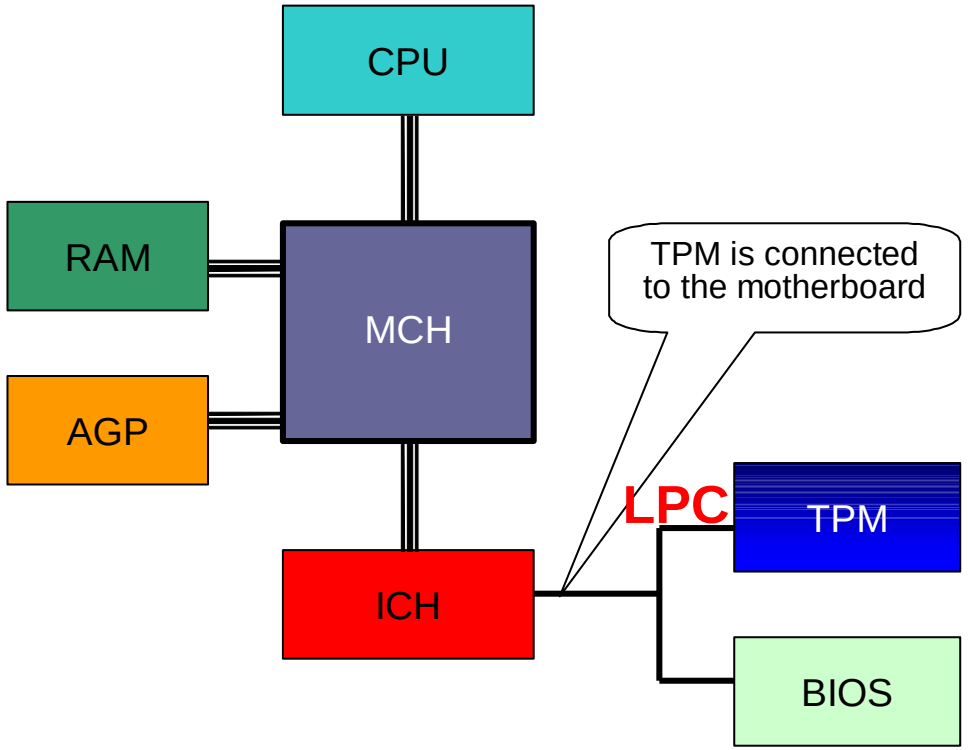
- 可信PC机


系统
平台
主板
可信模块 TBB
CPU
MEMORY
固件
总线
TPM
CRTM
电源
HD
FD
CARD
OS
驱动
应用
外设

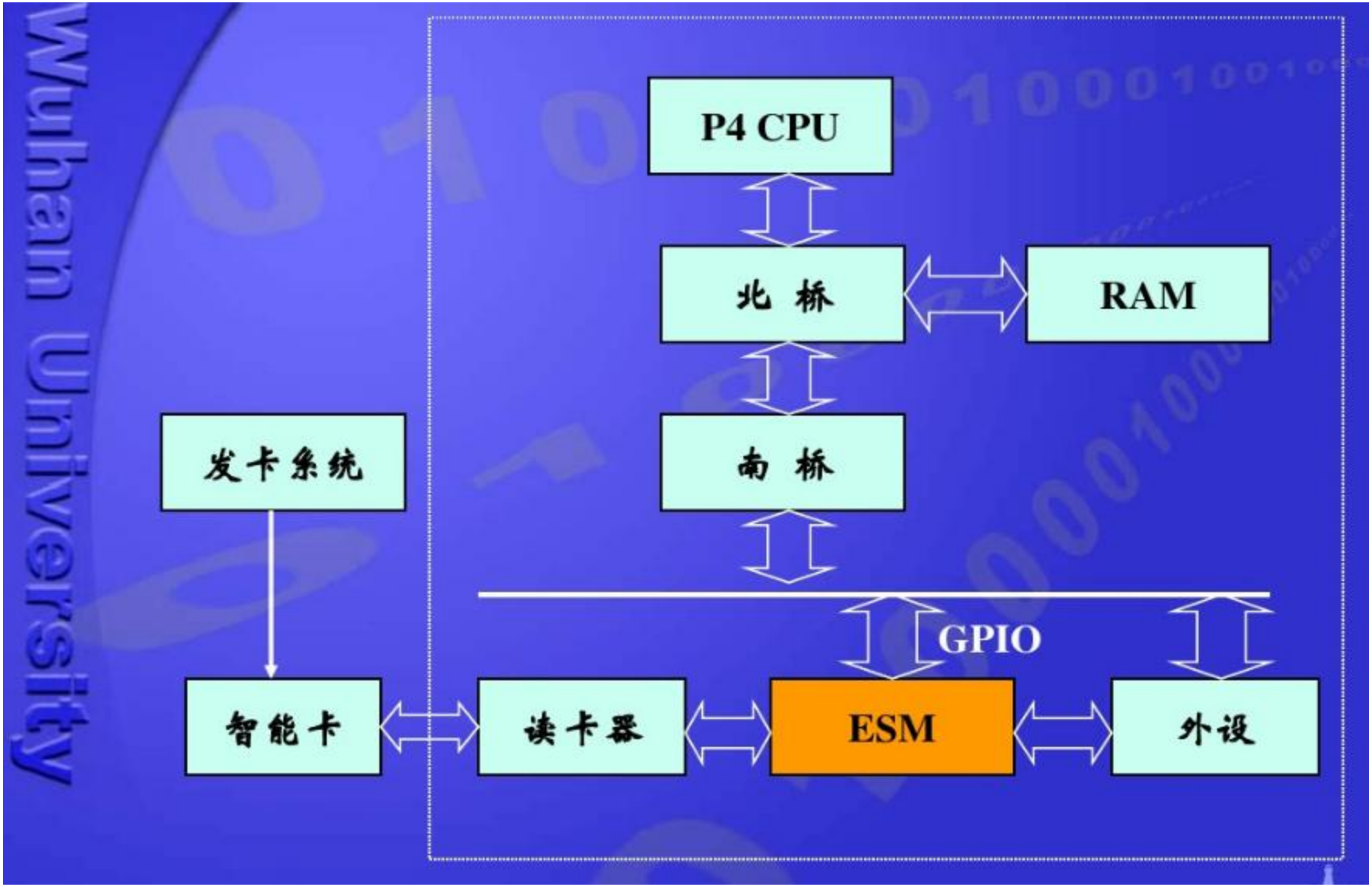
五. 可信计算

举例：可信PC硬件平台

- **TPM与主板通过LPC总线与南桥芯片连接**
  - **北桥是管理高速设备的芯片：管理内存和显卡**
  - **南桥是管理低速设备的芯片：管理硬盘、键盘等**
  - **LPC是一种低速总线**
- **CRTM是存储在ROM中的BIOS的启动模块**



五. 可信计算



五. 可信计算

1. **BIOS的中文名称就是基本输入输出系统**，是一组固化到计算机内主板上一个ROM芯片上的程序，其主要功能是为计算机提供最底层的、最直接的硬件设置和控制;
2. **BIOS的功能分为三个部分**：
   - **第一部分是自检及初始化**，即主要负责启动电脑，包括用于电脑刚接通电源时对硬件部分的检测、初始化、引导程序；
   - **第二部分是程序服务处理**，即主要是为应用程序和操作系统服务，这些服务主要与输入输出设备有关，例如读磁盘、文件输出到打印机等；
   - **第三部分是硬件中断处理**，主要是分别处理PC机硬件的需求，BIOS的服务功能是通过调用中断服务程序来实现的，这些服务分为很多组，每组有一个专门的中断。

五. 可信计算

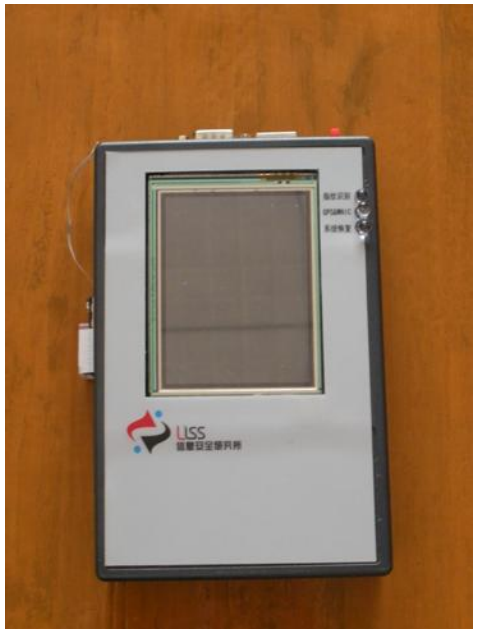
J2810芯片

J3210芯片

五. 可信计算

中国瑞达的可信计算机

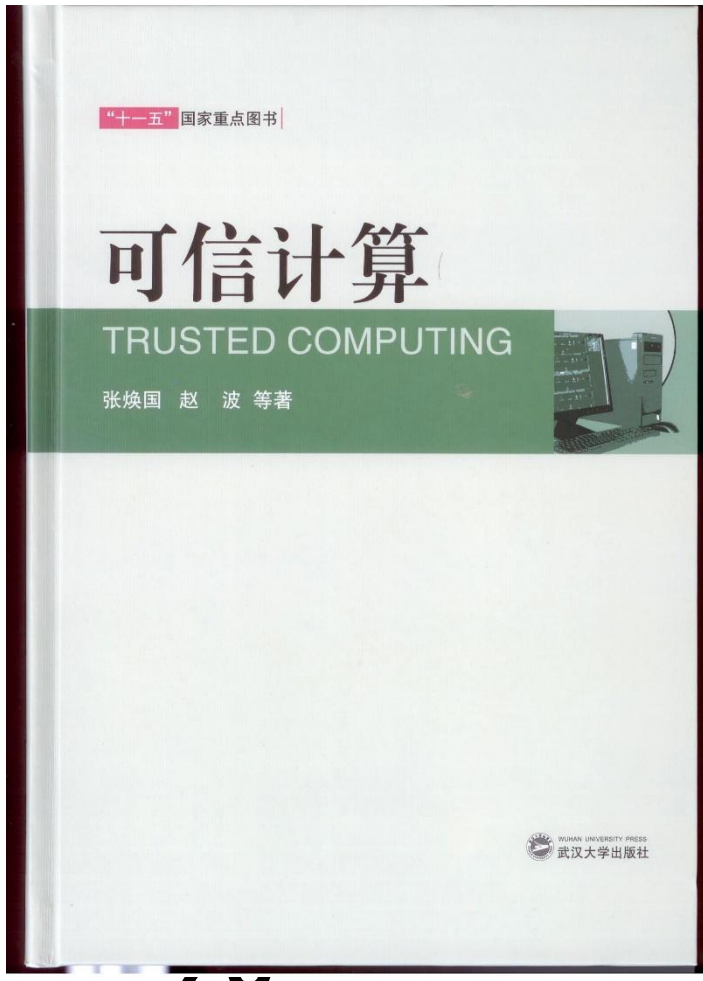
武汉大学的可信PDA



五. 可信计算

武汉大学的可信计算平台测评系统

专著



五. 可信计算

可信计算的新发展

- 中国公布了3个可信计算技术标准
- 2012年10月TCG公布了TPM2.0新规范，并将陆续发布其余规范。
  - TPM2.0新规范支持中国商用密码
- 2012年10月微软发布了WIN8，WIN8 全面支持可信计算。 WIN8.1进一步增强了安全性
- 我们认为：从2013年开始的一段时期内将形成可信计算的一个小高潮。这一小高潮阶段，以扩展可信计算的应用为主要特征！

五. 可信计算

可信计算小结

- 我国在可信计算领域起步不晚，水平不低，成果可喜。
- 我国已经站在国际可信计算领域的前列
- 可信计算在发展中也存在一些问题
  - 技术超前，理论滞后
  - 硬件平台超前，缺少可信软件配套
  - 目前应用较少

信息系统安全

一 信息系统安全的概念

二 信息系统的硬件系统安全

三 信息系统的操作系统安全

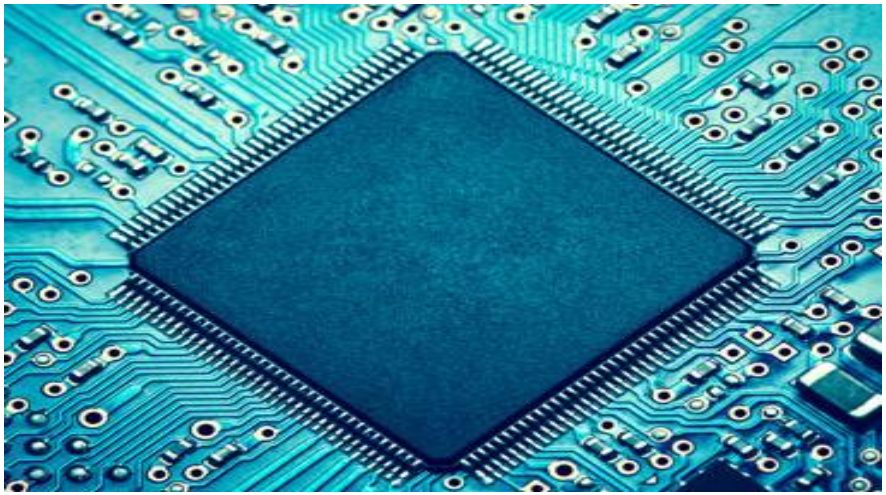
四 信息系统的数据库系统安全

五 可信计算

六 工业控制系统安全

六、工业控制系统安全——核心技术

- 我国基础信息技术与产品受控于国外,主要的集成电路芯片依赖从欧美进口。



- 专家指出，国外芯片制造厂商有可能通过在芯片面板某一程序上植入木马来窃取商业数据或机密，也可以通过病毒、恶意软件来操控控制系统，引发安全事故。

- “芯片”的集成电路目前广泛应用于电脑、手机以及水利、电力等公共设施和军事设备上，已经成为经济发展和国家安全的命脉。
- 每年我国进口芯片的金额已经超过了石油，在通信领域，华为、中兴通讯等光通信设备中绝大多数的核心芯片，如DSP、激光器、调制器、MCU、存储器等，大部分来自于美国供应商。而手机端的高端处理器芯片，也大多来自美国高通公司。且绝大多数高端芯片国产实难替代。

六、工业控制系统安全——核心技术

- 在集成电路中植入病毒、后门、窃听器是容易的。
- 只要存在国家和利益斗争，给CPU或操作系统留后门的行为就永远存在。

- 熟悉IC设计（Integrated Circuit Design）的开发者应该都知道，一个IP（intellectual property core）设计公司在对第三方提供其设计好的IP时，即便是较开放的软核授权，也不会做到所有代码可读可修改，而是包装了好多模块，其中有些可以配置、有些可以修改，而在大部分模块内部都不可能进行随意修改。
- 对研发单位来说，员工在自己写的代码里设置后门，可能会在code review的过程中被发现，但第三方在没有设计文档和验证环境等技术支持下，要想发现设计单位埋设的后门却非常困难。而且设计单位可以对源码进行变量置乱，所有变量全部用随机字母和数字代替，在这种情况下，第三方想要破解源码中埋设的后门近乎是一件不可能完成的任务。
- 最让人恐慌的是，极微小的硬件后门基本无法通过任何现代硬件安全分析手段检测出来，而且只要芯片工厂中的一位员工就能进完成植入。

六、工业控制系统安全——核心技术

- 2016年3月8日，美国商务部对中兴通讯施行“出口限制”的制裁。禁止美国供应商向中兴通讯出口任何货物。

- 对中兴而言，由于重要元器件自美进口，美国供应商被美国政府禁止供货后，中兴将面临严重的元器件短缺，并且欧盟、日本等国与美国的出口管制步调往往保持一致，一旦制裁扩大，中兴将面临更大损失。鉴于该事件存在重大的不确定性，中兴自3月7日停牌。

- 虽然目前华为已有麒麟芯片，中兴已有迅龙。但是，这些国产芯片的成功应用大多在消费类领域，在对稳定性和可靠性要求很高的通信、工业、医疗以及军事的大批量应用中，国产芯片距离国际一般水平差距较大。尤其是一些技术含量很高的关键器件如高速光通信接口、大规模FPGA、高速高精度ADC/DAC等领域，还完全依赖美国供应商。

六、工业控制系统安全——核心技术

- 另据有关机构统计，国内银行、证券、民航、电力、铁路、邮政等重要经济部门，75以上信息设备来自国外，特别是核心软件和部件严重依赖进口。
- Cryponym公司发现，自win95到win2000都给美国国家安全局提供一个后门，美国国家安全局无需经过认证可以调用所有windowns系统提供的安全服务，随时可以完全控制我们的重要系统，威胁到我国国家安全。

- 软件作为高新技术产业的基础和灵魂已经成为影响国家安全的关键因素。
- 成为我国走新型工业化道路的核心要素，成为重要领域和关键基础设施可靠、安全运行的关键因素。
- 自主可控是基于安全的战略需求。

六、工业控制系统安全——核心技术


TOP 500 CERTIFICATE
The List.

Sunway TaihuLight, a NRCPC System at the
National Supercomputing Center in Wuxi, BinHu, China

is ranked

No. 1

among the World's TOP500 Supercomputers
with 93 PFlop/s Linpack Performance
on the TOP500 List published at ISC High Performance, June 20, 2016

Congratulations from the TOP500 Editors

Erich Strohmaier, NERSC/Berkeley Lab
Jack Dongarra, University of Tennessee
Horst Simon, NERSC/Berkeley Lab
Martin Meuer, ISC Group

- 2015年，美国禁止英特尔向我国销售芯片，如今，“神威•太湖之光”的出现可谓是绝地之后的反击。**从CPU到操作系统再到互联网络等核心部件的全自主化**，证明我国完全有能力实现自主可控。
- 我们需要在自主可控的基础上构建安全可信的生态链，某一个地方的安全加固是不解决问题的，如果基于国外的产品，可能只是用打补丁的方式进行开发，能解决我们一时的需求，但从长远来看，并不能解决我们的需求，这需要构建完整的安全可信生态链。

六、工业控制系统安全——关键基础设施

□ “震网”病毒摧毁伊朗核设施

◆ 在该病毒攻击的一年中，核科学家最初认为是设备故障，所以不断的更换设备，但是每次又再次被感染。于是他们查是否购买的设备有问题，但每次检查都是完美的。病毒就是这么狡猾的利用人们对计算机的信任来隐瞒攻击，甚至一度伊朗的工程师都没有怀疑是网络攻击。

◆ 该病毒至少利用了四个新的“零日”漏洞，能够在Windows所有版本中运行；针对西门子WinCC/PCS7 SCADA控制系统软件；只允许每台被感染的计算机扩散到小于3台计算机上；它有自我保护的自毁机制，2012年删除自己；专门针对级联在一起的一系列离心机上。

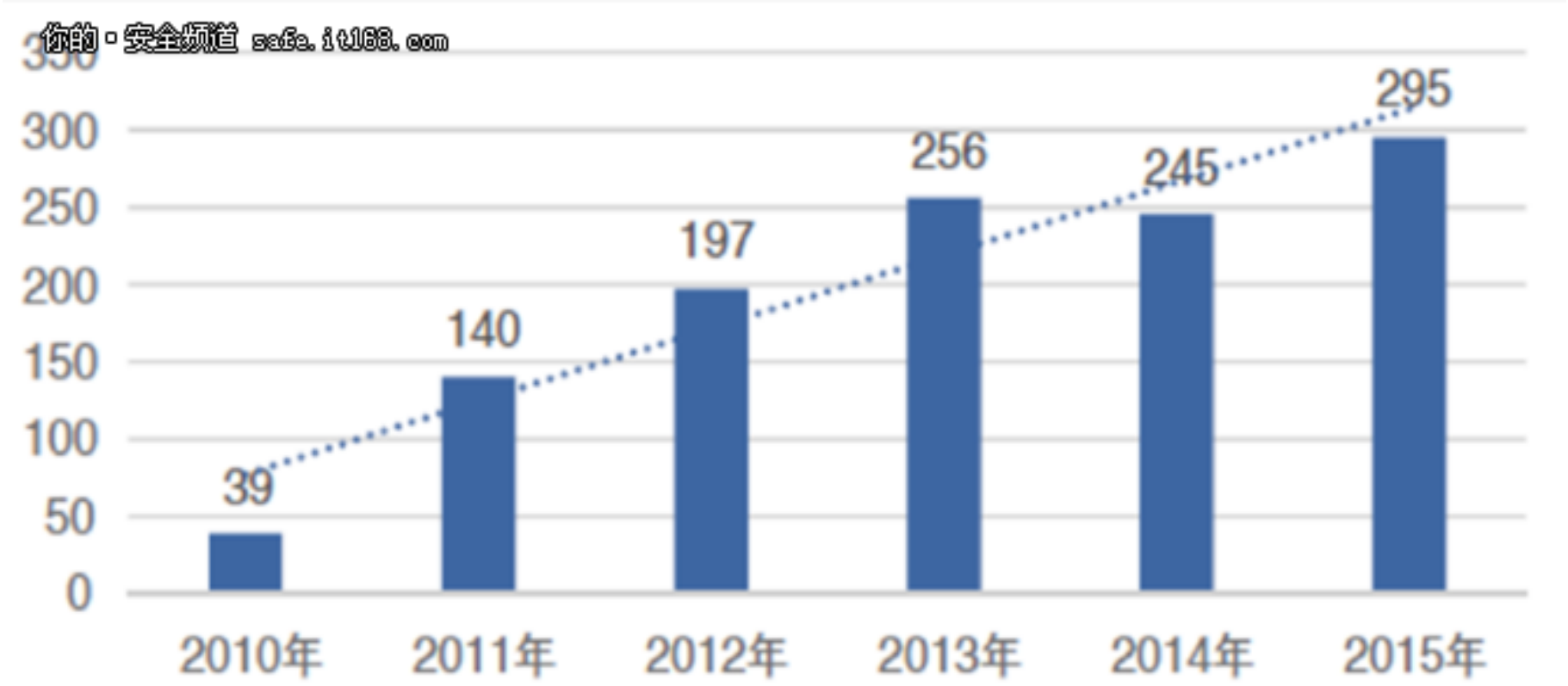
六、工业控制系统安全——关键基础设施

2011年4月，韩国四大银行之一的农协银行信息系统500台服务器中，约有一半以上遭到黑客攻击，大量数据被恶意删除和篡改，包括数十万客户信息，导致该行所有分行网点全部停业。

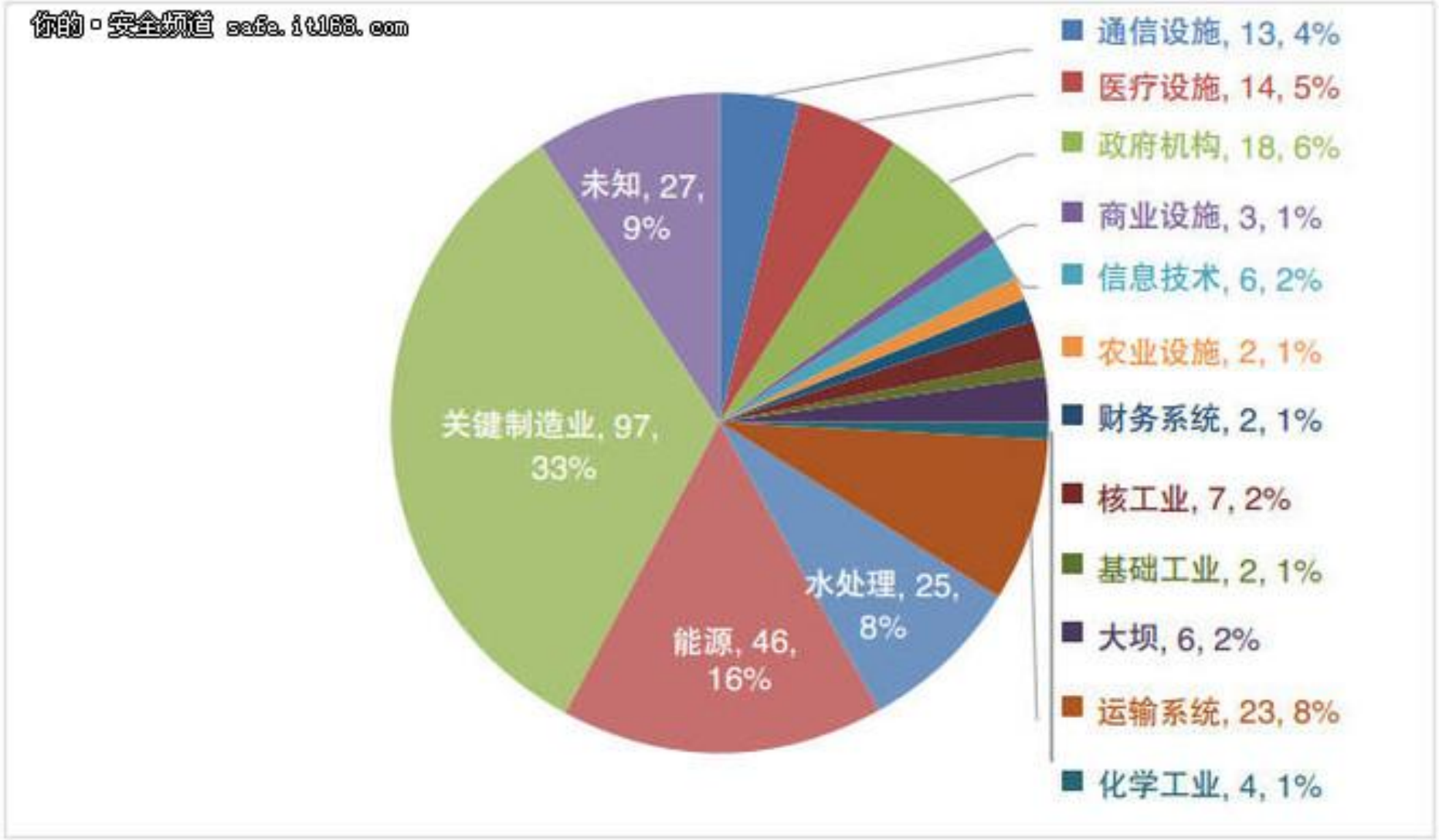
六、工业控制系统安全——关键基础设施

该事件发生后不久，韩国检察机关发布了该事件是“网络恐怖袭击”所致的调查结论。调查结果表示，负责维护服务器外包的韩国IBM职员韩某在接受一家咖啡屋提供的免费下载礼券，并在用于业务管理服务笔记本上下载电影的时候被感染了这种攻击病毒。

工控行业每年安全事件数量统计



2015年各行业攻击事件统计



六、工业控制系统安全——关键基础设施

- 2015年12月，网络攻击使乌克兰境内近三分之一的地区发生断电事故。据分析，此次网络攻击利用了一款名为“黑暗力量”的恶意程序，获得了对发电系统的远程控制能力，导致电力系统长时间停电。

- 2015年，国家信息安全漏洞共享平台共收录工控漏洞125个，发现多个国内外工控厂商的多款产品普遍存在缓冲区溢出、缺乏访问控制机制、弱口令、目录遍历等漏洞风险，可被攻击者利用实现远程访问。
- 据监测，2015年境外有千余个IP地址对我国大量使用的某款工控系统进行渗透扫描，有数百个IP地址对我国互联网上暴露的工控设备进行过访问。

六、工业控制系统安全——关键基础设施

- 不幸的是，目前绝大多数的工控网基本处于不设防的状态，而由于在**大多数企业中，工控网的管理往往不在IT部门的范围之内**，有些工控系统甚至是由企业外的第三方来通过远程进行管理和维护的因此，在工控网安全方面，存在着很多漏洞和误区。
- 给工控网打补丁是个很困难的事。工控网常常担负着企业最重要的生产流程。而停掉这些流程往往会产生巨大的成本以及运营风险。因此，集中式的自动化的补丁管理系统是不存在的。

结论

目前我国金融、能源、交通、通信、军工、钢铁、有色、化工、装备制造等重点领域基础网络与重要信息系统及工业控制系统，**长期缺乏全面的信息安全防护技术手段与产品配备**，关键产品和高端服务仍严重信赖进口。这意味着国外几大工控系统中存在的安全隐患，在我国同样存在，甚至更为严重。

六、工业控制系统安全——关键基础设施

攻击持续性威胁（Advanced Persistent Threat，APT）

- APTs与其他网络威胁的区别是，它有一定规划，是团队合作，结合了组织化、智能化、复杂性和耐心。
- APTs的目标，从军用喷气式飞机的设计到石油公司的商业秘密，都在范围内。
- 它甚至可以利用楼道内的一个自动调温器或一台打印机向外传送文件。
- APT对任何组织都是噩梦，多数人不知道自己已经成为目标，往往是知道的时候为时已晚。

口 据行业报告显示，2015年对我国发起APT攻击的黑客组织近30个，主要针对我国境内科研教育、政府机构等。

六、工业控制系统安全——关键基础设施

嵌入式系统（ Embedded system ）

- 是一种完全嵌入受控器件内部，为特定应用而设计的专用计算机系统。
- 以应用为中心，以计算机技术为基础，软硬件可裁剪，适应应用系统对功能、可靠性、成本、体积、功耗等严格要求的专用计算机系统。
- 由于嵌入式系统只针对一项特殊的任务，设计人员能够对它进行优化，减小尺寸降低成本。
- 通常，嵌入式系统是一个控制程序存储在ROM中的嵌入式处理器控制板。 有些嵌入式系统还包含操作系统，但大多数嵌入式系统都是由单个程序实现整个控制逻辑。

六、工业控制系统安全——关键基础设施

嵌入式系统应用

- 所有带有数字接口的设备，如手表、微波炉、冰箱、洗衣机、录像机、汽车、心脏起搏器等，都使用嵌入式系统。
- 另外，工业过程控制、数字机床、电力系统、电网安全、电网设备监测、石油化工系统都使用了嵌入式系统。

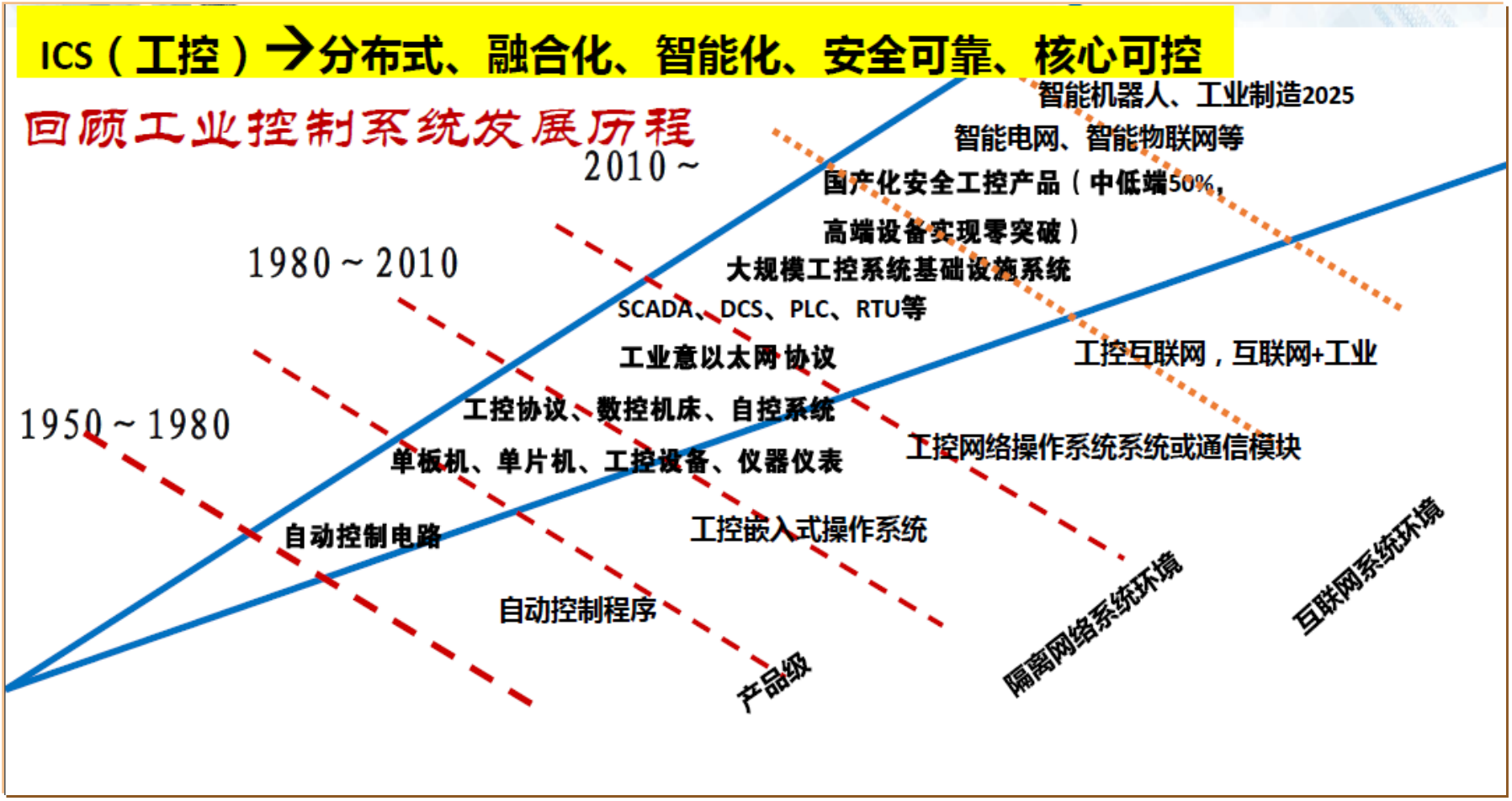
因此，工控系统的安全包括了嵌入式系统的安全问题！

六、工业控制系统安全——关键基础设施

建　议

- 加快工控网络安全技术与产品研发，解决工控设备本体安全，实现自主可控;
- 加快工控网络安全体系建设，解决工控网络结构安全，实现真实可靠;
- 加快基于行业应用的工业过程研究，解决工控系统行为安全，在持续对抗中保持领先优势;
- 安全与工控深度融合，以自主安全工控芯片为基础，在工控系统从设计到生产到部署到运营的全过程都有安全因素介入，为工控注入安全基因，实现本质安全。

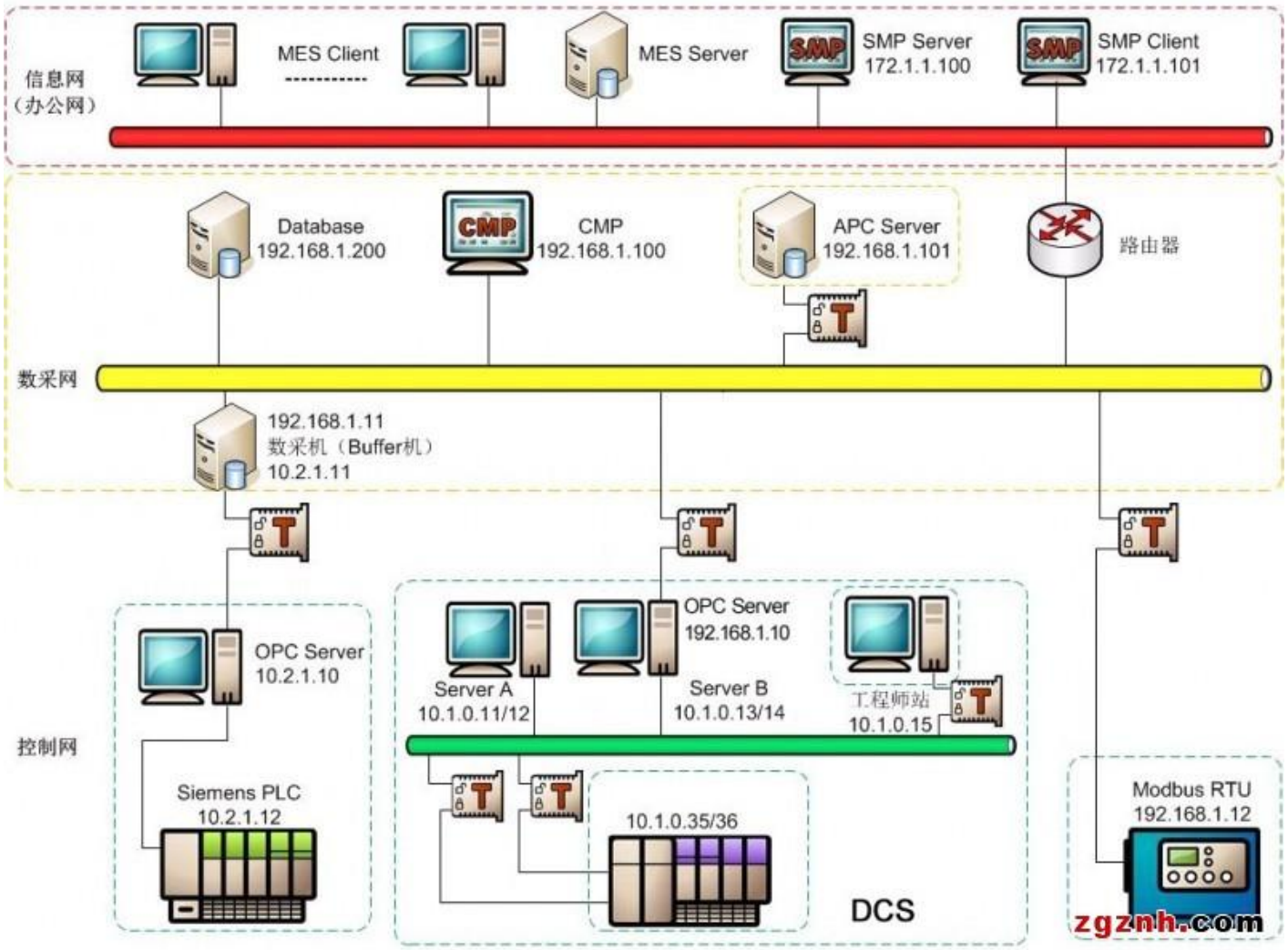
六、工业控制系统安全——关键基础设施



六、工业控制系统安全——关键基础设施

- 关键基础设施”，包括：农业、食品、银行、医疗、交通、水利、电力、净水、燃气、金融，这些系统通过“数据采集与监控系统”接入网络空间。
- 前美国总统乔治布什曾经说过“网络空间正演变为神经系统，控制着我们的经济。”
- 《连线》杂志编辑Ben Hammersley描述说“网络空间成为21世纪占据主导地位的平台”。
- **无论人们承认与否，互联网就是生活。**

六、工业控制系统安全——关键基础设施



六、工业控制系统安全——关键基础设施

- 2016年1月19日，农业部农业信息化领导小组召开会议，贯彻落实中央农村工作会议和全国农业工作会议有关推进农业信息化的决策部署。会议原则通过了《全球农业数据调查分析系统实施办法》《“互联网+”现代农业三年行动实施方案》。会议强调，要把创新、协调、绿色、开放、共享的发展理念贯彻落实到推进农业信息化的各行业各领域全过程，2016年要重点做好以下几项工作：一是强化顶层设计，加快编制“十三五”农业农村信息化发展规划；二是继续推进农业物联网试验示范、农业电子商务、信息进村入户等重点工作，要把信息进村入户作为农业部门推进农业电子商务的重要抓手；三是加强农村主体信息化能力建设，组织开展政府工作人员、农业干部、农民应用信息化能力培训；四是筹备开好全国“互联网+”现代农业暨新农民创业创新大会。

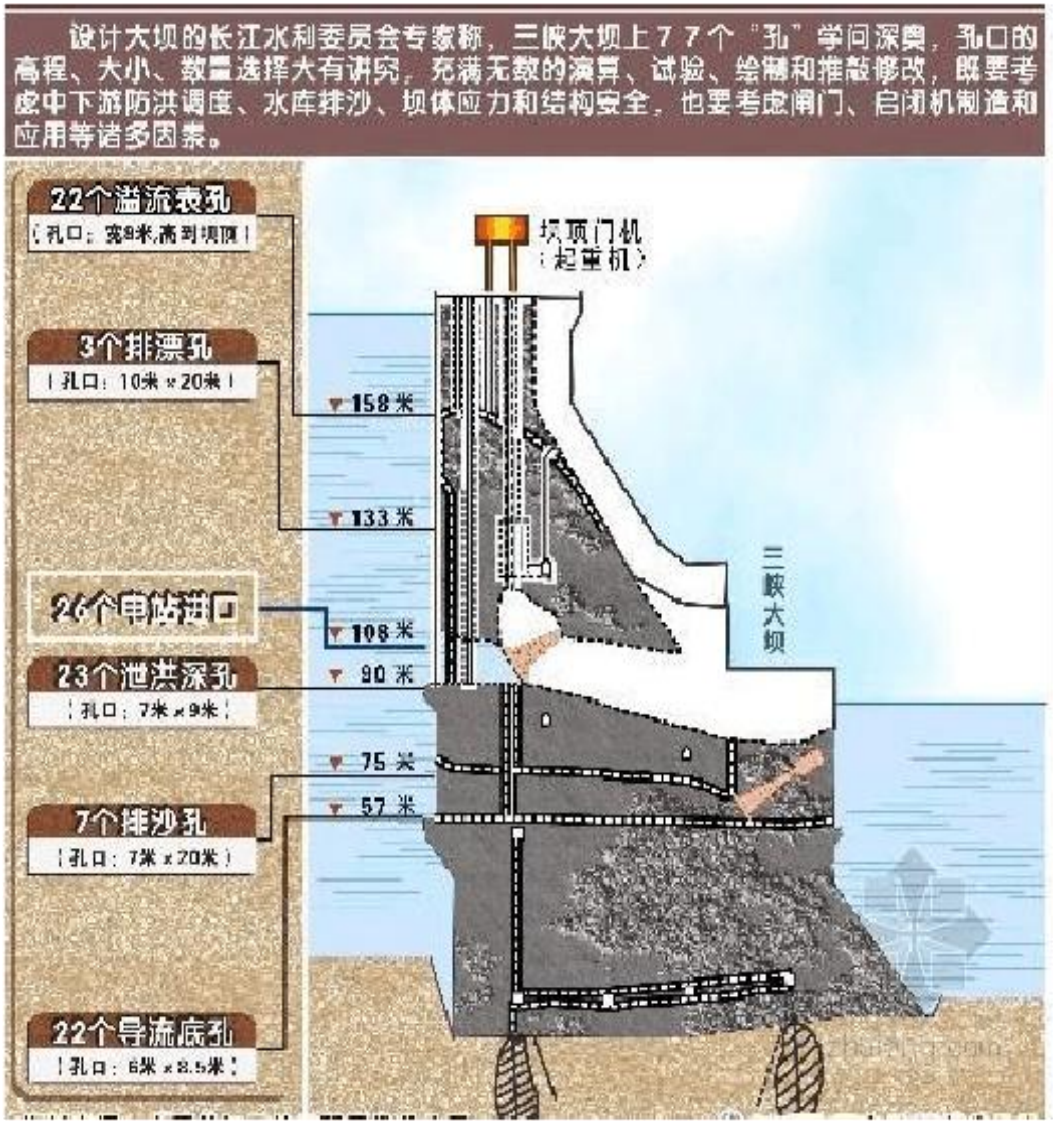
六、工业控制系统安全——关键基础设施

六、工业控制系统安全——关键基础设施

一、互联网的发展——关键基础设施（水利）

口 据介绍，包括埋设在坝内的16252台/只仪器和检测传感器，三峡工程在坝区红线内外，总共埋设了监测仪器近10万台/支，监测系统和规模居世界第一，时刻监护着三峡大坝是否稳定，有无沉降。

口使用了水位计（传感器）后，系统可以通过计算相关闸室的水位，自动发出动水关阀指令，实现在一定水位差时动水关阀，从而实现了自动动水关阀，防止了超灌、超泄。



六、工业控制系统安全——关键基础设施

思考题

1. 上网搜集资料，计算机技术的发展。
2. 了解操作系统和数据库系统的安全问题。
3. 了解我国在操作系统和数据库方面的发展。
4. 了解BIOS的功能。

谢谢！