第三章 网络安全基础
第三节 网络安全工程与管理

主讲人：李建华 张全海
网络空间安全技术研究院

2024 年 12 月

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

法律规范

安全等级保护：《网络安全法》第二十一条规定，国家实行网络安全等级保护制度，该制度的核心是对网络实施等级保护和分等级监督。根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，网络分为五个安全保护等级。

网络安全等级保护相关政策

- 信息安全等级保护是党中央国务院决定在信息系统安全领域实施的基本国策
- 信息安全等级保护是国家信息安全保障工作的基本制度
- 信息安全等级保护是国家信息安全保障工作的基本方法

安全等级划分

第一级

- 用户自主保护级
  - ◆一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益的一般网络

第二级

- 系统审计保护级
  - ◆一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络

第三级

- 安全标记保护级
  - ◆一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络

第四级

- 结构化保护级
  - ◆一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络

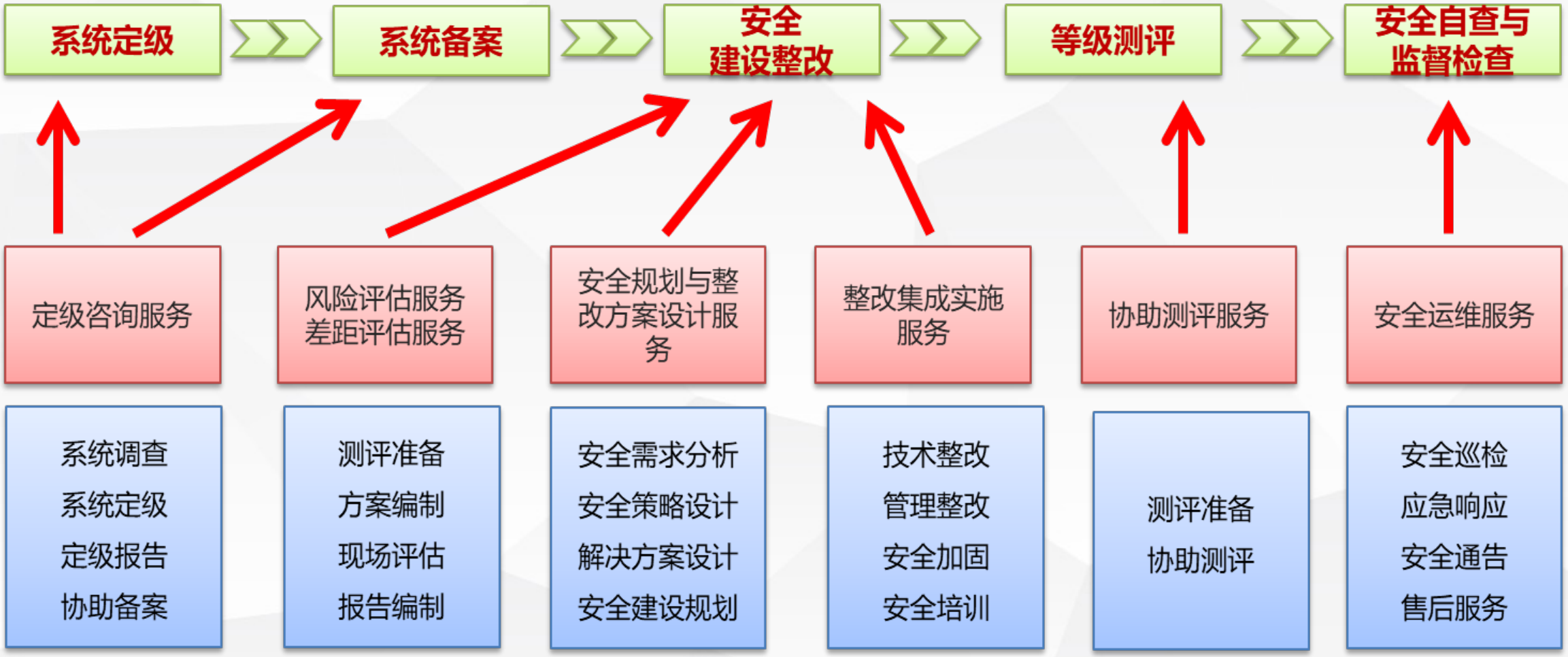
第五级

- 访问验证保护级
  - ◆一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络

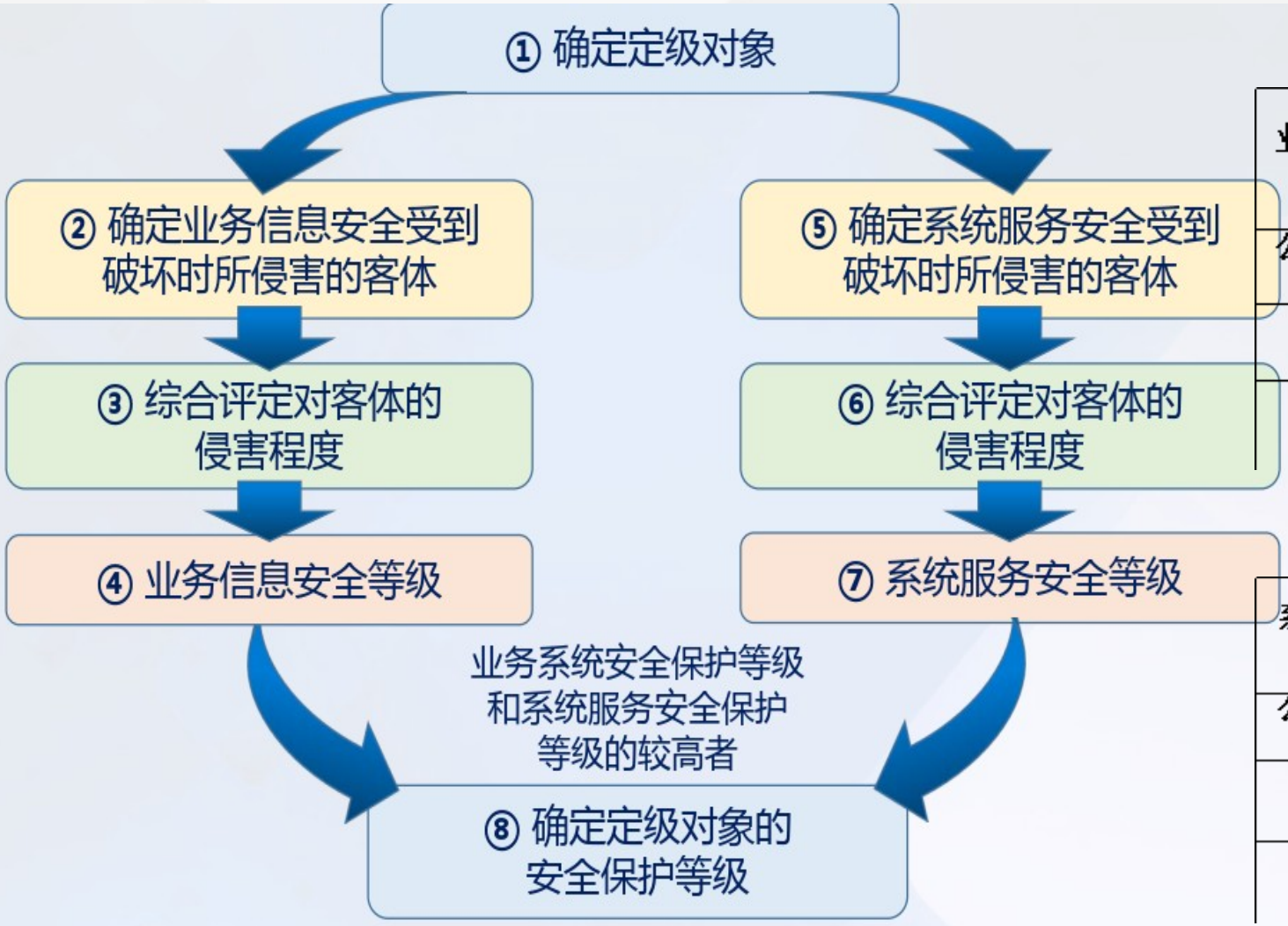
安全等级设计要素

访问验证保护级	可信恢复		
结构化保护级	隐蔽信道分析	可信路径	
安全标记保护级	强制访问控制	标记	
系统审计保护级	审计	客体重用	
用户自主保护级	自主访问控制	身份鉴别	数据完整性

等级保护工作流程


系统定级
系统备案
安全建设整改
等级测评
安全自查与监督检查
定级咨询服务
风险评估服务
差距评估服务
安全规划与整改方案设计服务
整改集成实施服务
协助测评服务
安全运维服务
系统调查
系统定级
定级报告
协助备案
测评准备
方案编制
现场评估
报告编制
安全需求分析
安全策略设计
解决方案设计
安全建设规划
技术整改
管理整改
安全加固
安全培训
测评准备
协助测评
安全巡检
应急响应
安全通告
售后服务

安全定级流程



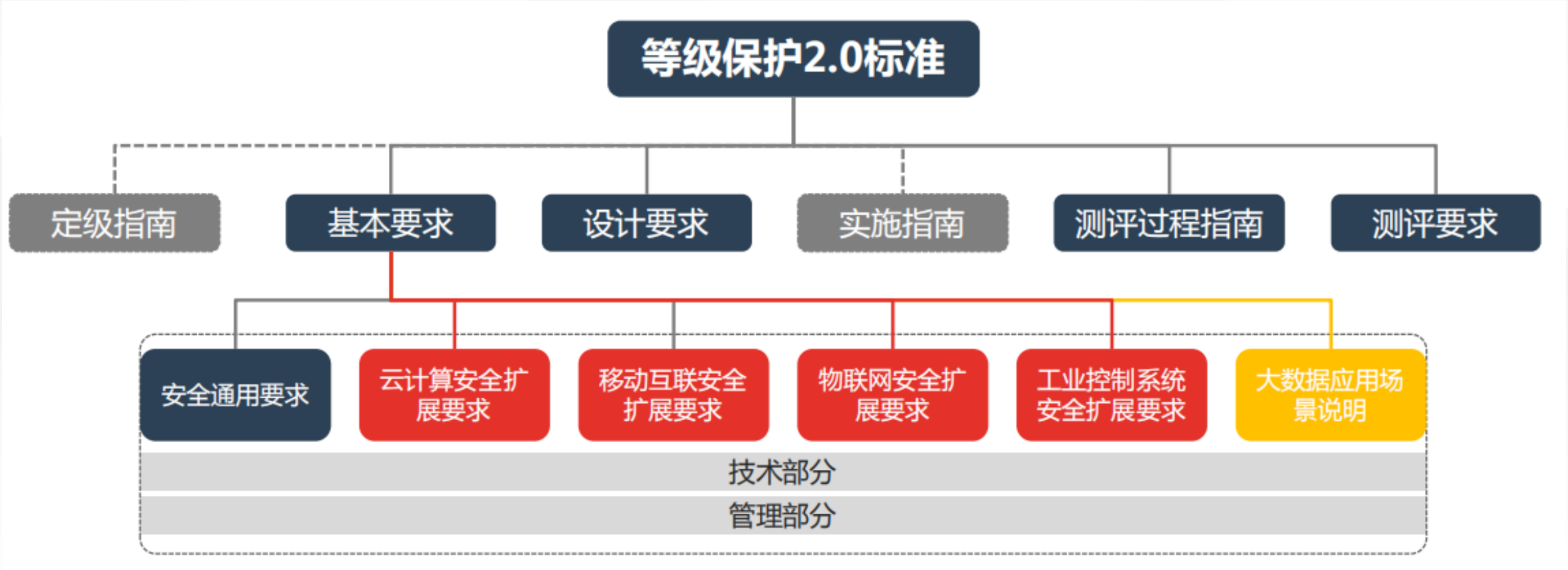
业务信息安全保护等级

业务信息坏时所侵害的客体安全被破	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

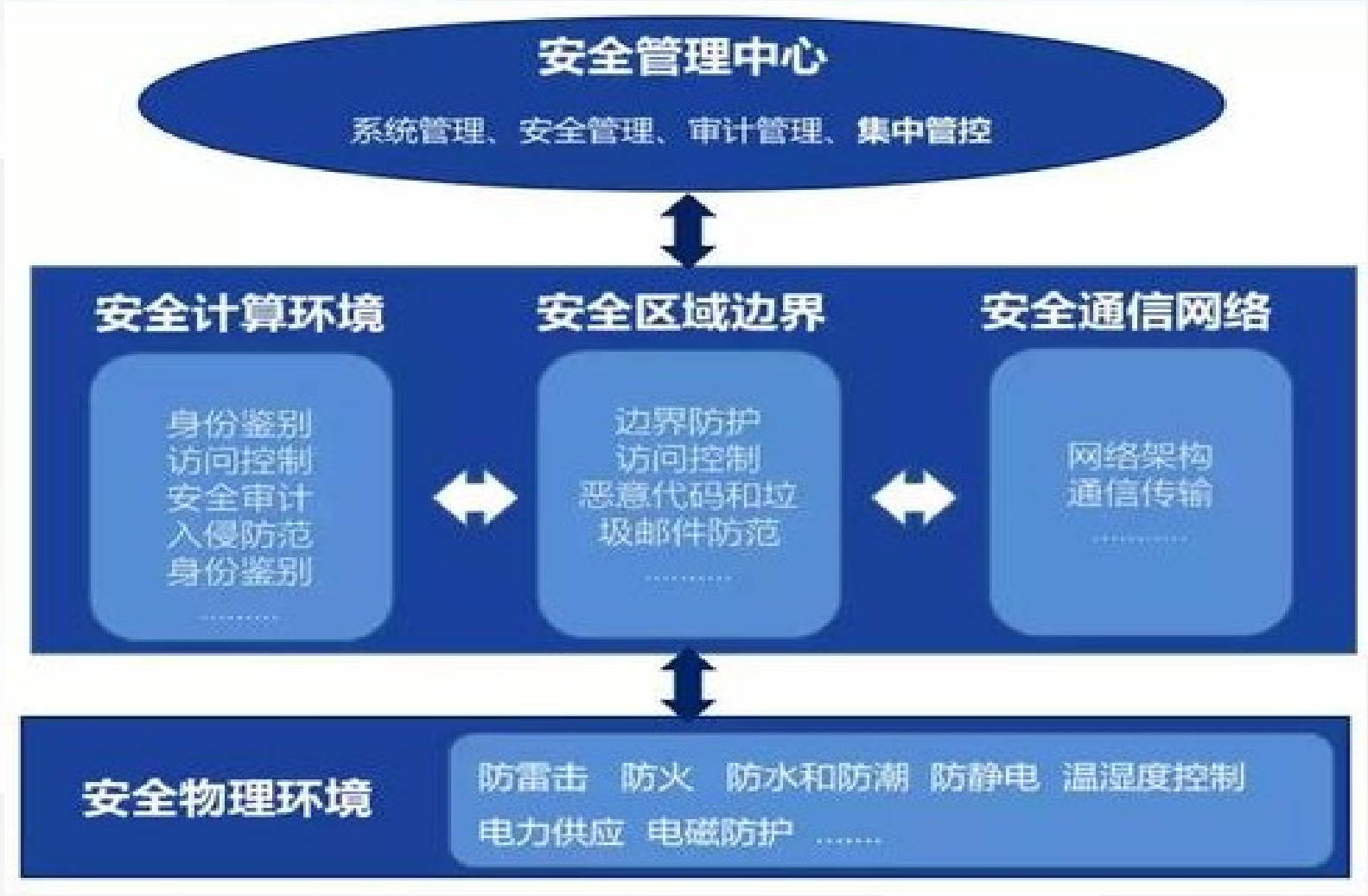
系统服务安全保护等级

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

等级保护 2.0 标准体系


等级保护2.0标准
定级指南
基本要求
设计要求
实施指南
测评过程指南
测评要求
安全通用要求
云计算安全扩展要求
移动互联安全扩展要求
物联网安全扩展要求
工业控制系统安全扩展要求
大数据应用场景说明
技术部分
管理部分

等级保护安全设计技术框架



上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

网络安全管理

网络安全管理是网络安全工作中的重要概念，网络安全管理控制措施与网络安全技术控制措施一起构成了网络安全防护措施的全部。

美国国家标准与技术研究院（NIST）将网络技术控制措施定义为完全机器由及其来完成的活动；网络安全管理措施定义为完全由人来完成的活动，并将由机器和人共同完成的活动定义为网络安全运行控制措施。简言之，网络安全管理是指把**分散的网络安全技术因素和人的因素，通过策略、规则协调整合为一体，服务于网络安全的目标。**

网络安全管理体系（ ISMS ）

国外网络安全管理相关标准

目前，ISO/IEC2700X 标准系列是国际主流，国家标准化组织（ ISO ）专门为 ISMS 预留了一批标准序号。该系列的两个核心、基础标准 ISO/IEC 27001 和 ISO/IEC 27002 已于 2005 年 10 月正式发布第一版，2013 年 10 月正式发布第二版。

我国网络安全管理相关标准

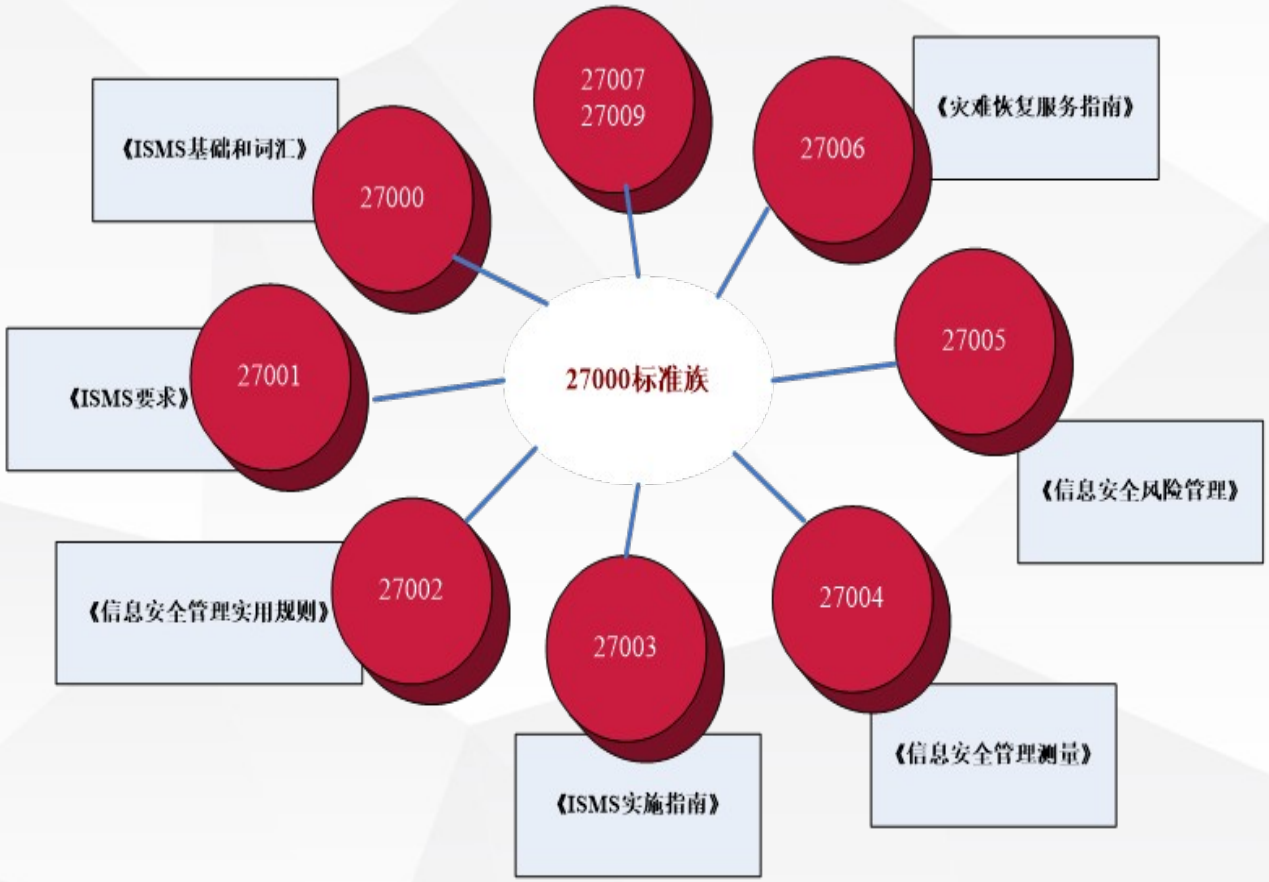
我国早期主要采用与国际标准靠拢的方式，近年来加强网络安全管理标准的自主制定，已经开始向国际标准化组织提交国际标准提案。在全国信息安全标准化技术委员会内，第 7 工作组 (WG7) 的努力下，我国已经正式发布一系列网络安全管理标准。

网络安全管理控制措施

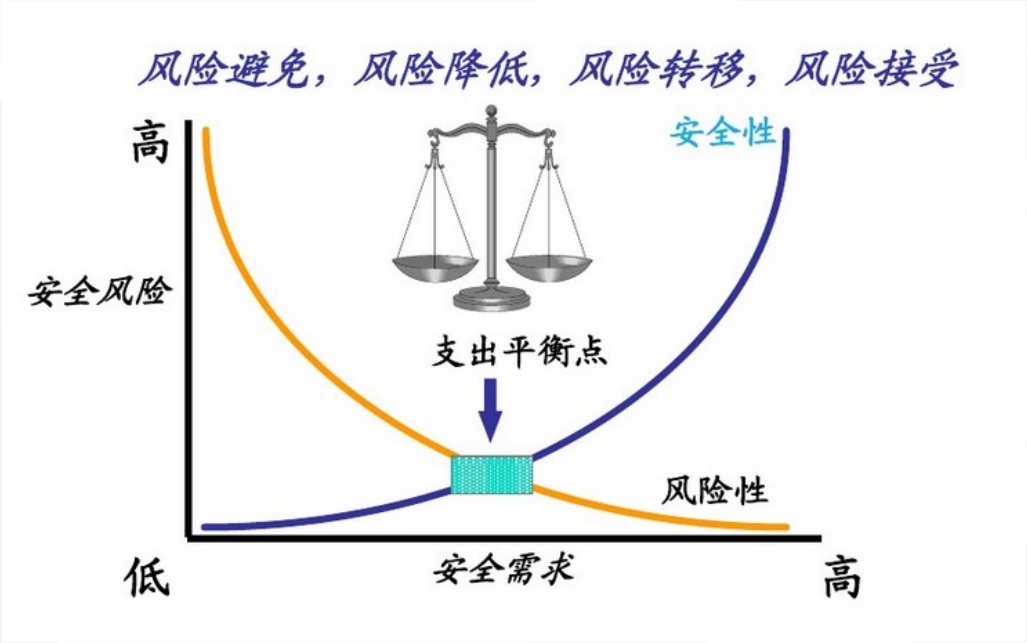
为了对组织所面临的的安全风险实施有效的控制，应针对具体地安全威胁和脆弱性，采取适当的控制措施。 ISO/IEC 27002 标准提出了 14 个方面的管理控制措施，包括网络安全策略、网络安全组织、人力资源安全、资产管理、访问控制、密码、物理和环境安全、运行安全、通信安全、系统获取、开发和维护、供应商关系、网络安全事件管理、业务连续性管理和网络安全方面、符合性

ISO27000 系列

- 信息安全管理体系（ Information Security Management Systems，简称 ISMS ）是组织整体管理体系的一个部分，是基于风险评估建立、实施、运行、监视、评审、保持和持续改进信息安全等一系列的管理活动。
  - 基于风险管理思想，建立一个系统化、程序化和文件化的管理体系。
  - 强调全过程和动态控制。
  - 控制费用与风险平衡的原则，保护关键信息资产，使得网络安全风险的发生概率和结果降低到可接受的水平。

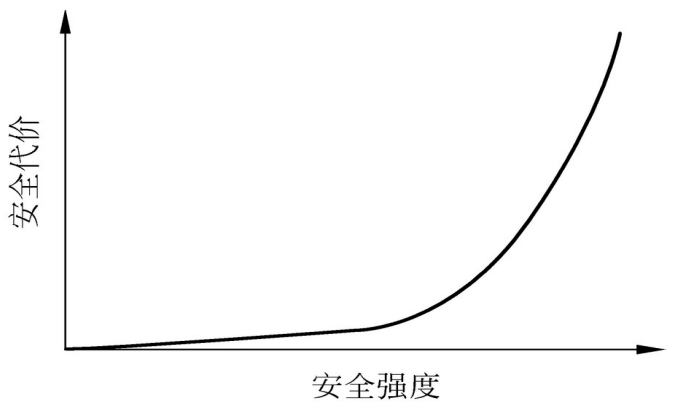


网络安全风险管理

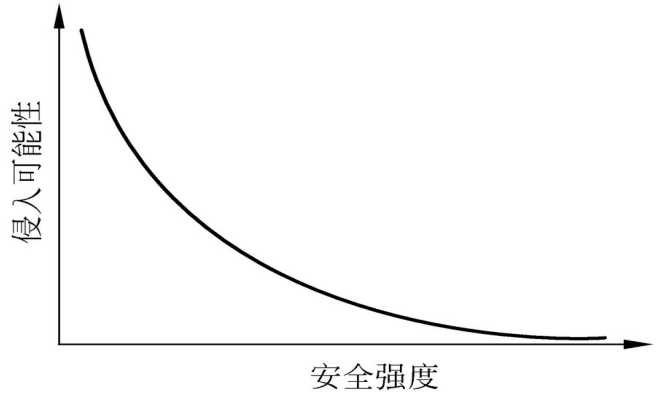


- 风险管理：**一种在风险评估的基础上对风险进行处理的工程。**网络安全风险管理实质是**基于风险的网络安全管理。**
  - 风险评估：对信息资产面临的威胁、存在的弱点、造成的影响，以及三者综合作用而带来的风险的可能性的评估。
  - 信息系统安全评估，或简称为**系统评估**，是在具体的操作环境与任务下对一个系统的**安全保护能力**进行的评估 。具体是指依据**国家风险评估有关管理要求和技术标准**，对信息系统及由其存储、处理和传输的信息的机密性、完整性和可用性等安全属性进行**科学、公正的综合评价**的过程。
  - **信息安全风险评估是建立信息安全保障机制中的一种科学方法。**
- 信息安全风险评估涉及**资产、威胁、脆弱性和风险** 4 个主要因素，基本过程主要分为：
  - 风险评估准备过程
  - 资产识别过程、威胁识别过程、脆弱性识别过程
  - 风险分析过程

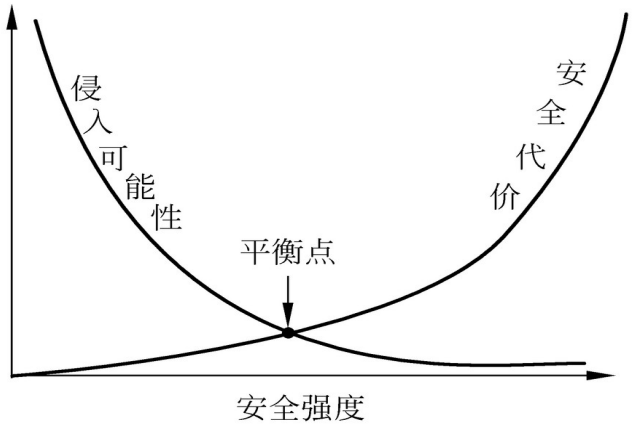
资产的有效保护



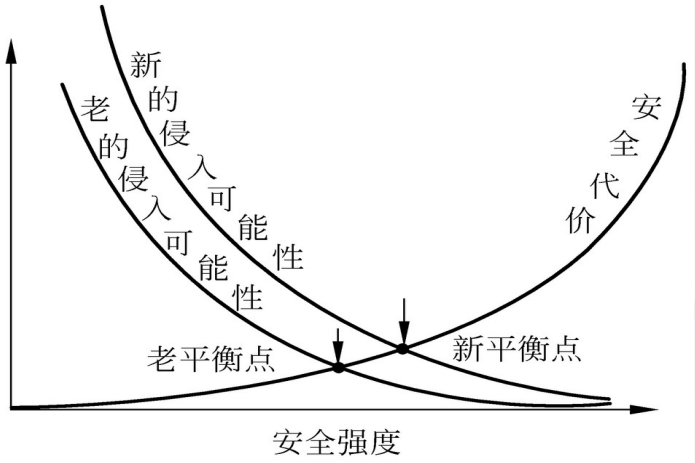
(a) 安全强度和安全代价的关系



(b) 安全强度和侵入可能性的关系



(c) 安全代价和侵入可能性的折中

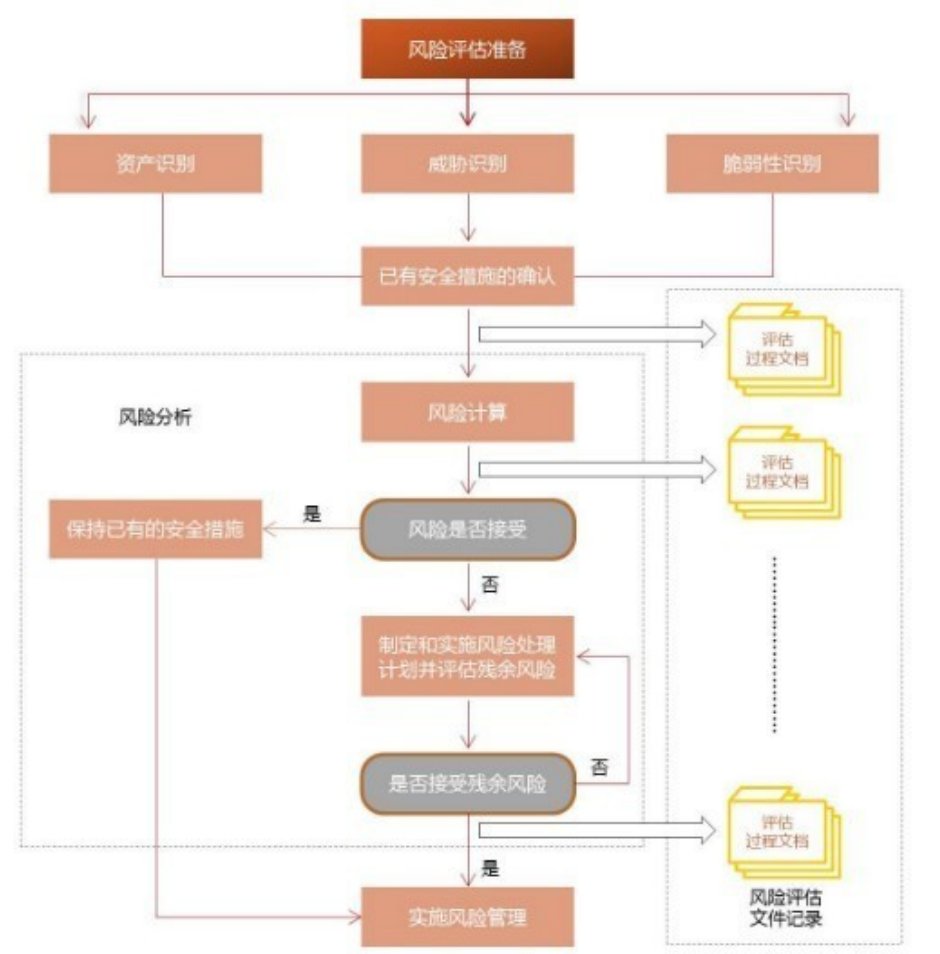


(d) 平衡点的变化

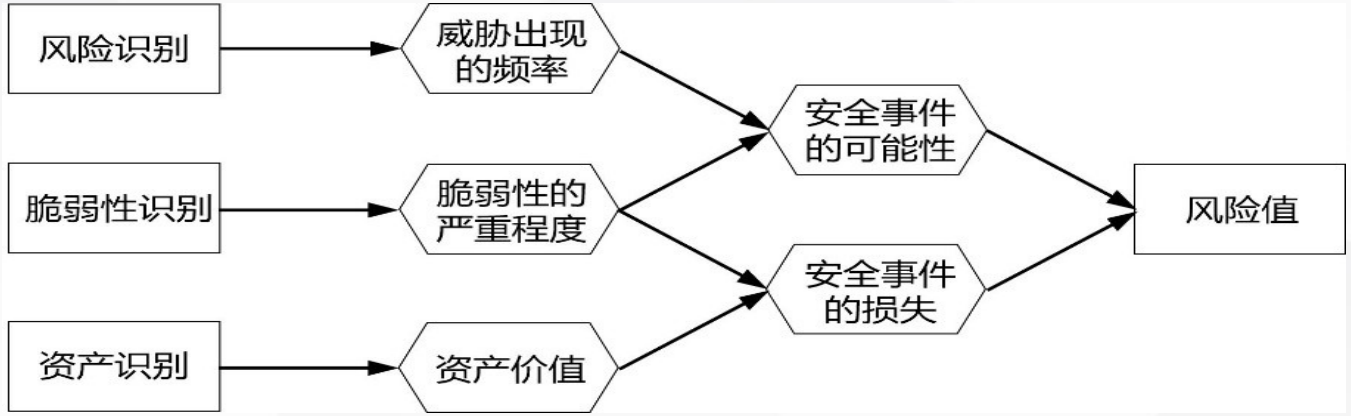
- 资产一旦受到威胁和破坏，就会带来两类损失
  - **即时的损失**，如由于系统被破坏，员工无法使用，因而降低了劳动生产率。
  - **长期的恢复所需花费**，也就是从攻击或失效到恢复正常需要的花费。
- 为了有效保护资产，应尽可能**降低资产受危害的潜在代价**。由于采取一些安全措施，也要付出安全的操作代价。**网络安全最终是一个折中的方案，需要对危害和降低危害的代价进行权衡。**

风险管理实施流程

风险管理实施流程

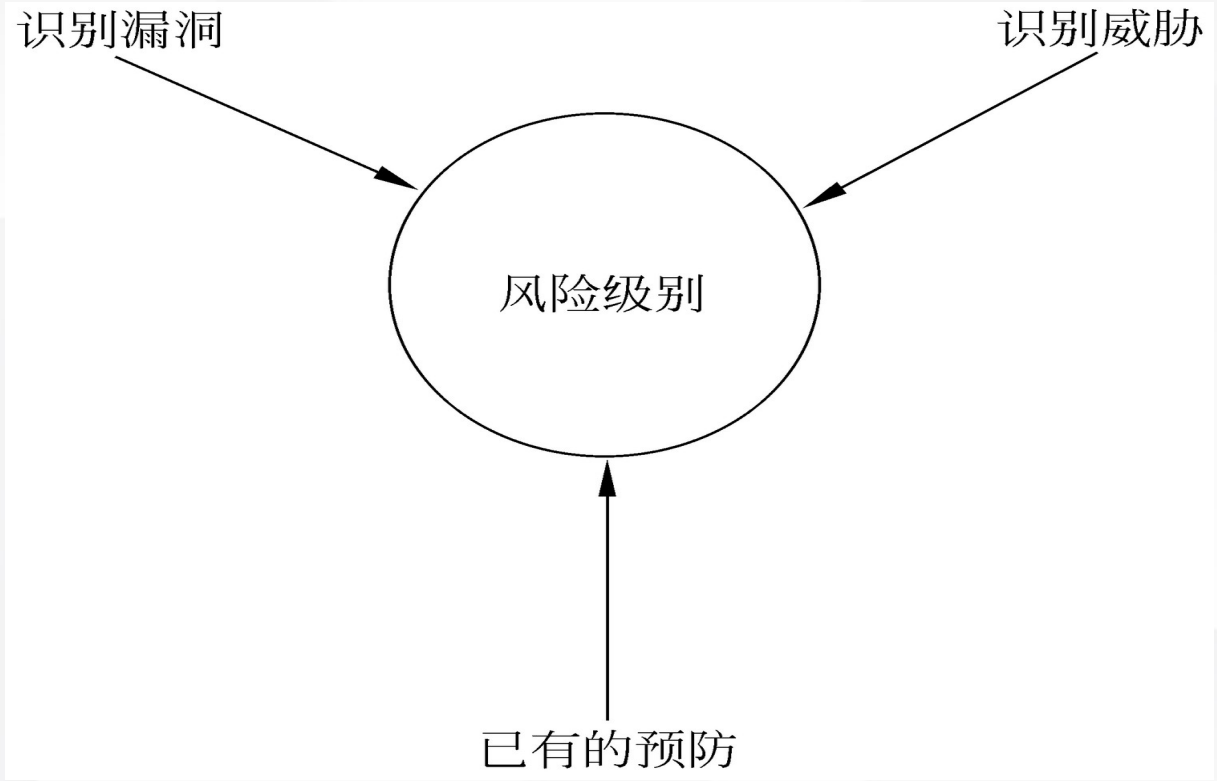


风险分析原理

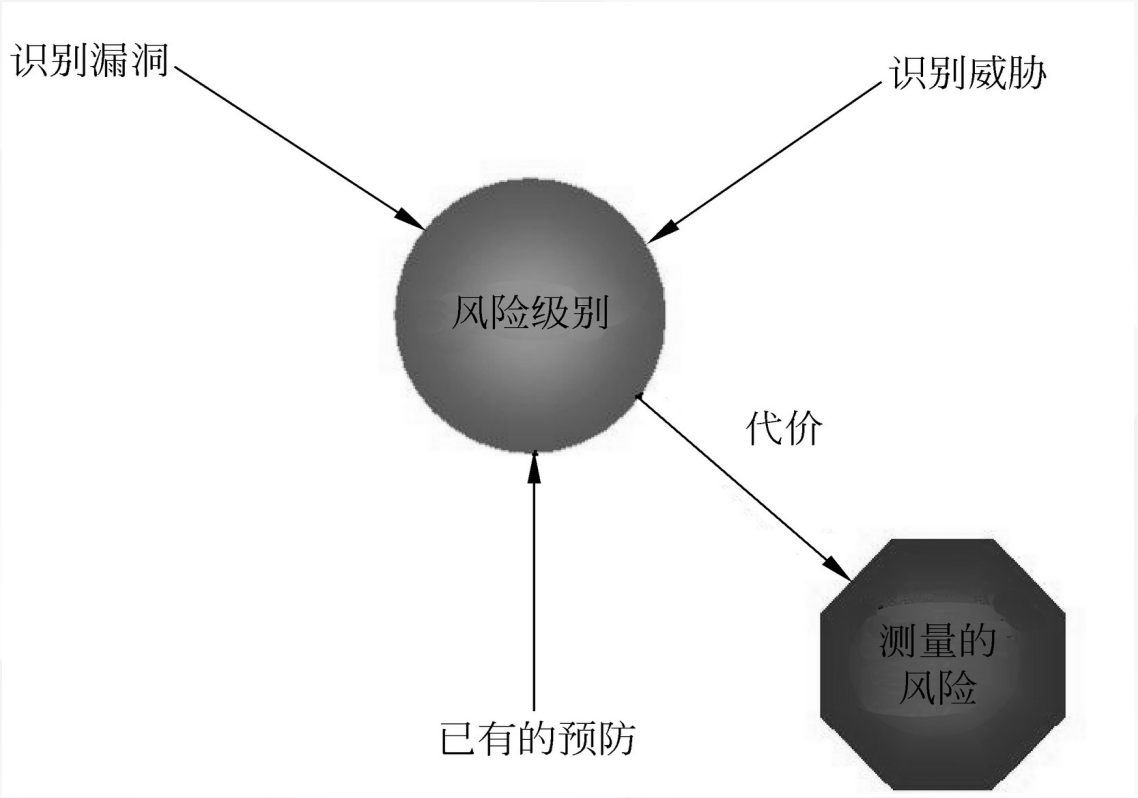


- 风险管理的核心部分：**风险分析**
  - 资产属性：资产价值
  - 威胁属性：威胁主体、影响对象、出现频率、动机
  - 脆弱性属性：资产弱点的严重程度

风险管理实施流程



风险识别

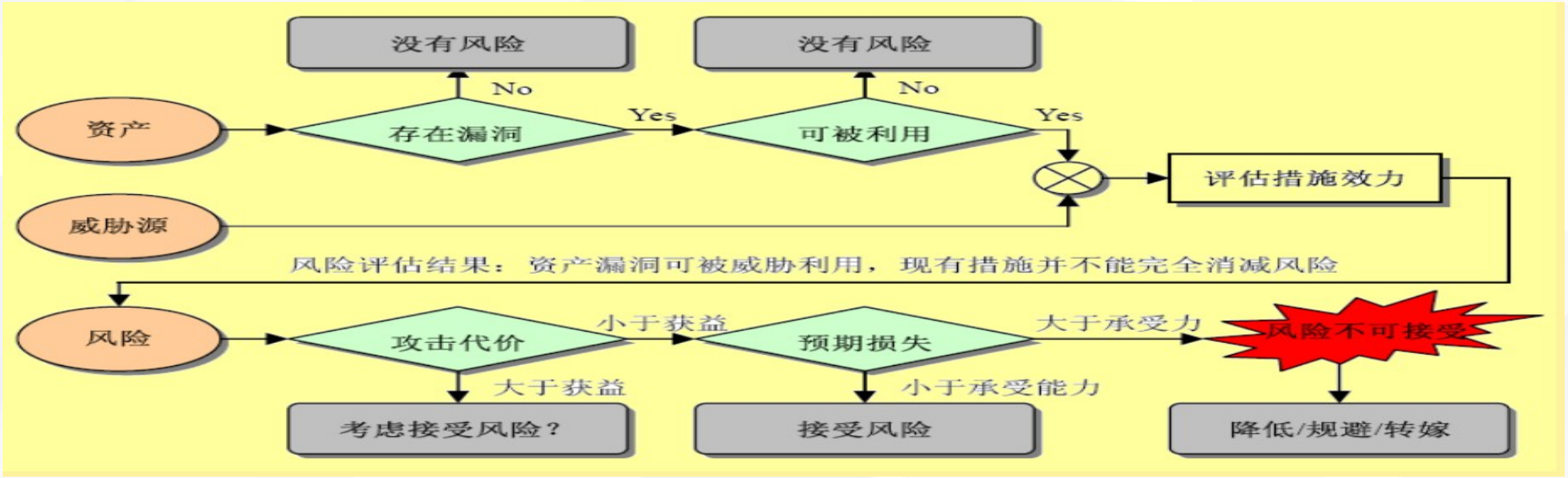


风险测量

风险分析

- 定性分析法：定性分析法主要是根据操作者的经验知识、业界的一些标准和惯例等非量化方式对风险状况作出判断的过程
  - 定性分析法**操作起来相对简单**，为风险管理诸要素（资产价值、 威胁出现的概率、弱点被利用的容易度、现有控制措施的效力等）的**大小或高低程度定性分级**
  - 该方法具有**很强的主观性**，同时也会因为操作者的经验和直觉偏差导致分析结果发生偏差，从而出现多次评估结果不一致的情况。
- 定量分析：是对构成风险的各个要素和潜在损失的水平赋予数值，当度量风险的所有要素（**资产价值、威胁频率、弱点利用程度、安全措施的效率和成本**等）都被赋值，风险评估的整个过程和结果就都可以被量化了。
  - 定量分析就是试图**从数字上**对安全风险进行分析评估的一种方法。
  - 定量分析的优点是评估结果用**直观的数据来表示**，看起来一目了然。但是也存在为了量化而把复杂事物简单化的问题，甚至有些风险要素因量化而被曲解

风险控制



风险控制措施

- **风险降低**：实施安全措施，把风险降低到一个可接受的级别
- **风险承受**：接受潜在的风险并继续运行网络和信息系统
- **风险规避**：通过消除风险的原因或后果，来规避风险，即不介入风险
- **风险转移**：通过使用其他措施来补偿损失，从而转移风险，如买保险

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

网络安全事件分类与分级

网络安全事件分类

国家标准 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》将网络安全事件分为 7 个基本分类：

- 有害程序事件
- 网络攻击事件
- 信息破坏事件
- 信息内容安全事件
- 设备设施故障
- 灾难性事件
- 其他网络安全事件

网络安全事件分级

《国家网络安全事件应急预案》（2017 年 6 月 中央网信办）将网络安全事件分为 4 个级别：

- ✓特别重大事件（Ⅰ级）
- ✓重大事件（Ⅱ级）
- ✓较大事件（Ⅲ级）
- ✓一般事件（Ⅳ级）

网络安全事件分类与分级

安全事件分级：其中主要考虑三个要素：信息系统的重要程度、系统损失和社会影响

- **信息系统的重要程度**主要考虑信息系统所承载的业务对国家安全、经济建设、社会生活的重要性以及业务对信息系统的依赖程度划分为特别重要信息系统、重要信息系统和一般信息系统。
- **系统损失**是指由于信息安全事件对信息系统的软硬件、功能以及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失

网络安全应急处理过程

01	准备阶段	主要工作包括建立合理的防御 / 控制措施、建立适当的策略和程序、获得必要的资源和组建相应队伍等。
02	检测阶段	目标是对网络安全事件做出初步的动作与响应，根据获得的初步材料和分析结果，预估事件的范围和影响程度，制定进一步的影响策略，并保留相关证据
03	抑制阶段	目标是限制攻击的范围，抑制潜在的或进一步的攻击和破坏。主要工作包括阻止入侵者访问被攻陷系统；限制入侵的程度；防止入侵者进一步破坏等。
04	根除阶段	目标是在事件被抑制之后，通过分析有关恶意代码或行为找出事件发生的根源，并予以彻底根除。
05	恢复阶段	目标是将网络安全事件所涉及的系统还原到正常状态。
06	总结阶段	目标是回顾网络安全事件处理的全过程，整理相关信息，尽可能把所有情况记录到文档中。

网络安全应急响应相关概念

- **网络安全事件：**引起网络系统的安全受到威胁和破坏的任何事件，这些威胁包括：丢失数据机密性，破坏数据和系统的完整性，破坏系统的可用性使之不能提供服务等等
- **网络安全应急响应能力：**网络系统的整体的应急事件的处理能力，包括针对于安全事件的技术响应手段，流程管理，人员组织等多个方面
- **计算机安全应急响应团队（ CSIRT ）：**负责日常情况下安全保障和紧急情况下应急响应任务的组织
- **CERT®/CC 的目的建立一个单一的 Internet 社区组织，协调 Internet 上的安全事件响应。** 1988 年 11 月底， CERT® Coordination Center 在卡耐基梅隆大学软件工程协会（ SEI ）正式成立。
- **事件响应和安全团队论坛**（ the Forum of Incident Response and Security Teams 缩写为 **FIRST** ）把政府，商业机构，和学术组织的安全应急响应团队联合起来，组成一个有机的整体。

国内安全应急响应组织

国内的应急响应服务组织的建设

- CCERT（ 1999 年 5 月），中国教育科研网紧急响应组
- NJCERT（ 1999 年 10 月），中国教育网华东（北）地区网络安全事件响应组
- 2000 年 8 月，国家计算机病毒应急处理中心
- 中国电信 ChinaNet 安全小组
- 解放军，公安部
- 商业网络安全服务公司
- 中国计算机应急响应处理协调中心 CNCERT/CC

信息系统灾难恢复

灾难恢复服务是指将信息系统从灾难造成的**故障或瘫痪状态**恢复到**可正常运行**的状态，并将其支持的业务功能从灾难造成的**不正常状态**恢复到**可接受状态**的活动和流程。包括灾难恢复规划和灾难备份中心的日常运行、关键业务功能在灾难备份中心的恢复和重续运行，以及主系统的灾后重建和回退工作，还涉及突发事件发生后的应急响应。灾难恢复可分为 4 个关键过程。

信息系统灾难恢复

灾难恢复能力划分为 6 个级别：

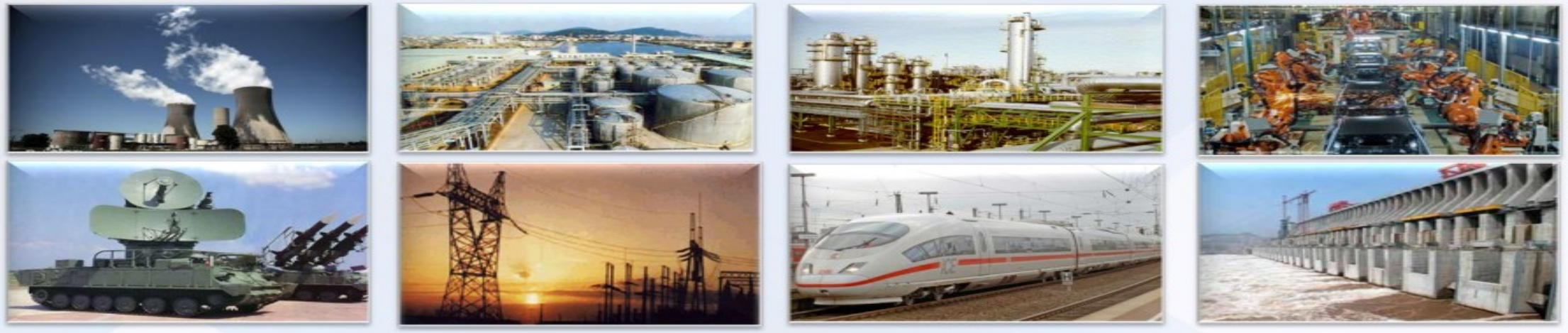
- 第 1 级 基本支持
- 第 2 级 备用场地支持
- 第 2 级 电子传输和部分设备支持
- 第 4 级 电子传输及完整设备支持
- 第 5 级 实时数据传输及完整设备支持
- 第 6 级 数据零丢失和远程集群支持

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

工业互联网

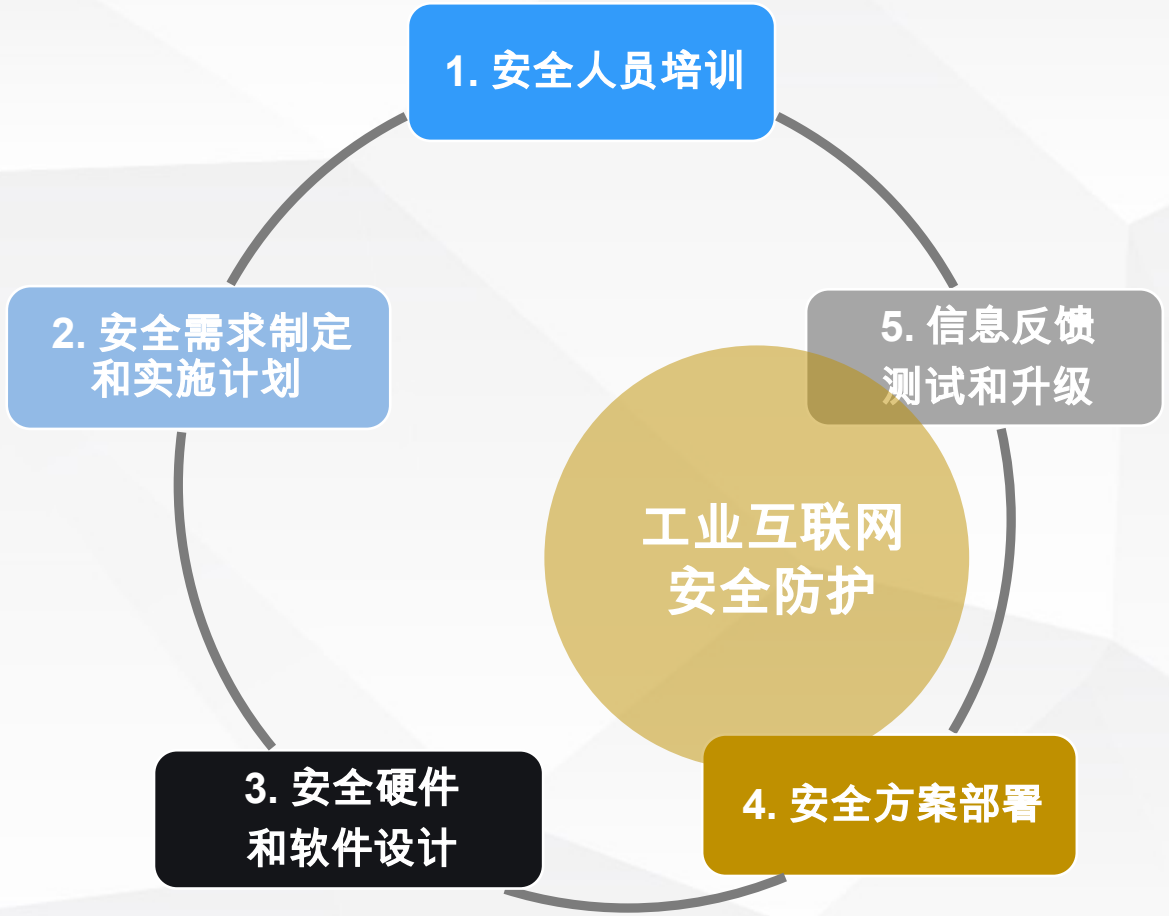
工业互联网概念：工业互联网的本质是通过开放式的全球化工业级网络平台，紧密融合物理设备、生产线、工厂、运营商、产品和客户，通过自动化和智能化的生产方式降低成本、提高效率。**工业互联网广泛应用**于核设施、钢铁、电力、水利、城市轨道交通、铁路、石油石化等，其中**超过 80%** 的涉及**国计民生**的**关键基础设施**可以通过工业互联网实现自动化和智能化作业。



工业互联网安全挑战

工业互联网安全挑战：工业互联网含有大量 CPS（ Cyber-Physical Systems 信息物理系统）设备，**安全防护措施相对滞后**，改进后的蠕虫、病毒和木马等传统攻击方式会严重威胁工业互联网安全，而且由于工业互联网集成多类不同系统，所以存在多种攻击发起点，攻击者可以从**物理层、网络层和控制层**分别发起攻击。例如 Stuxnet 蠕虫 利用“零日漏洞”导致伊朗核设施中的离心机故障。因此，工业互联网遭受攻击会**严重影响国家安全**。

工业互联网主要安全防护技术



移动互联网安全防护

移动互联网概念：移动互联网是指利用互联网的技术、平台、应用以及商业模式与移动通信技术相结合并实践的活动统称。移动互联网的组成主要包括 4 大部分：**移动互联网终端设备、移动互联网通信网络、移动互联网应用和移动互联网相关技术**。

移动互联网安全架构

移动互联网安全架构：根据移动互联网的特征和组成架构，移动互联网的安全问题可以分为 3 大部分：**移动互联网终端安全、移动互联网网络安全和移动互联网应用安全**。

移动互联网安全挑战

- 移动互联网却十分严格地强调对**用户隐私和用户行为**的保护；因此，移动互联网比传统互联网具有更高的安全性要求。
- 移动互联网涉及大量的用户个人信息（如位置信息、通信信息、日志信息、账户信息、支付信息、设备信息、文件信息等），给移动互联网安全监管和用户隐私保护带来极大的挑战
- 当前，移动通信终端智能化程度日益提高，处理的信息更加多样化。因此，终端成为攻击者的重要目标之一，恶意攻击行为逐步向强制推广、风险传播、越权收集等行为转变。终端被攻击，容易造成用户经济损失、信息泄漏、业务滥用等问题。

物联网概念

物联网是未来互联网的集成部分，被定义为动态的全球网络框架，具有自配置能力标准和互操作的通信协议。在物联网中，“物体”被期望参与商业、信息和社会过
它们相互之间能够通信和交互，感知环境并与之交互
同时，在
响应“真实
影响事件
现智能化
信息与通

IBM：智慧地球

2009

物联网是指通过信息传感设备，按照约定的
换和通讯
化识别、定位、跟踪
和扩展的网络

中国工信部：物联网白皮书

2011

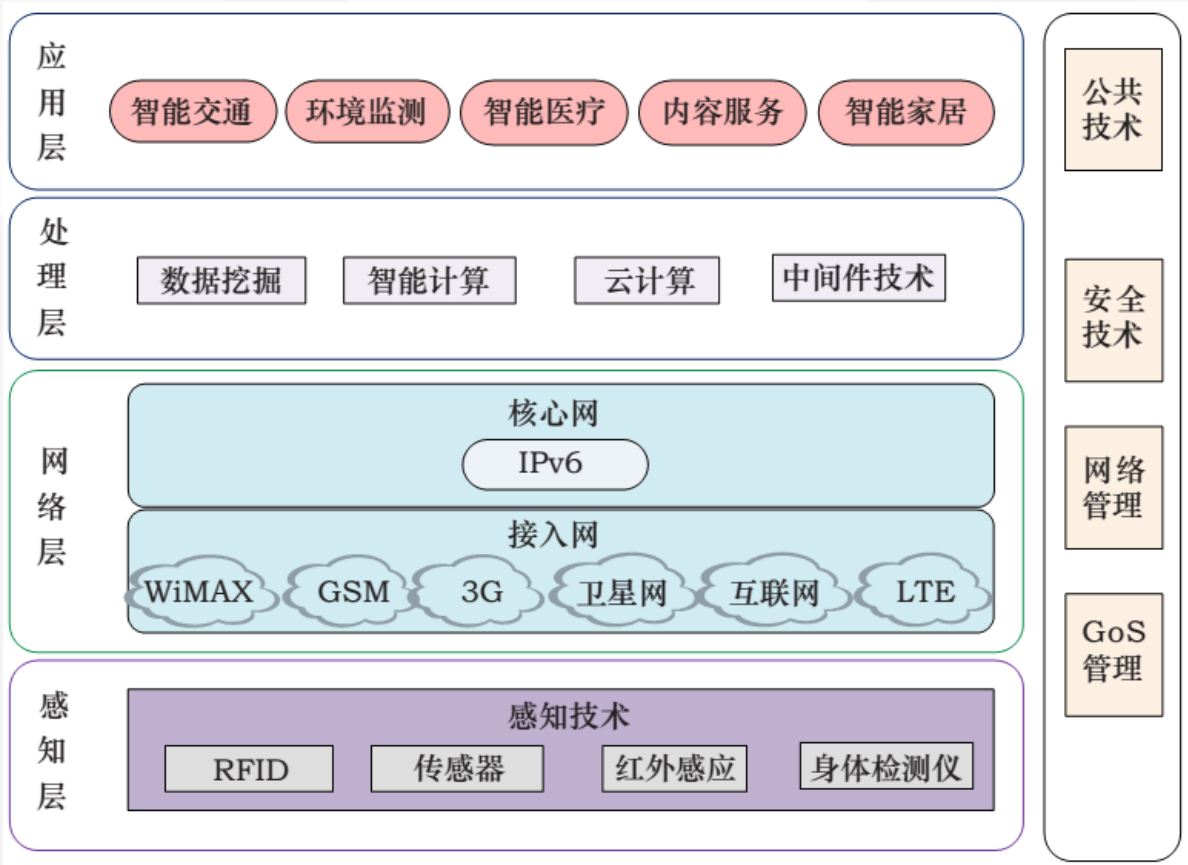
将感应器嵌入和装备到电网、铁路、建筑、大坝、油气管道等各种物体中，形成物物相联，通过超级计算机和云计算将其整合，实现社会与物理世界融合。

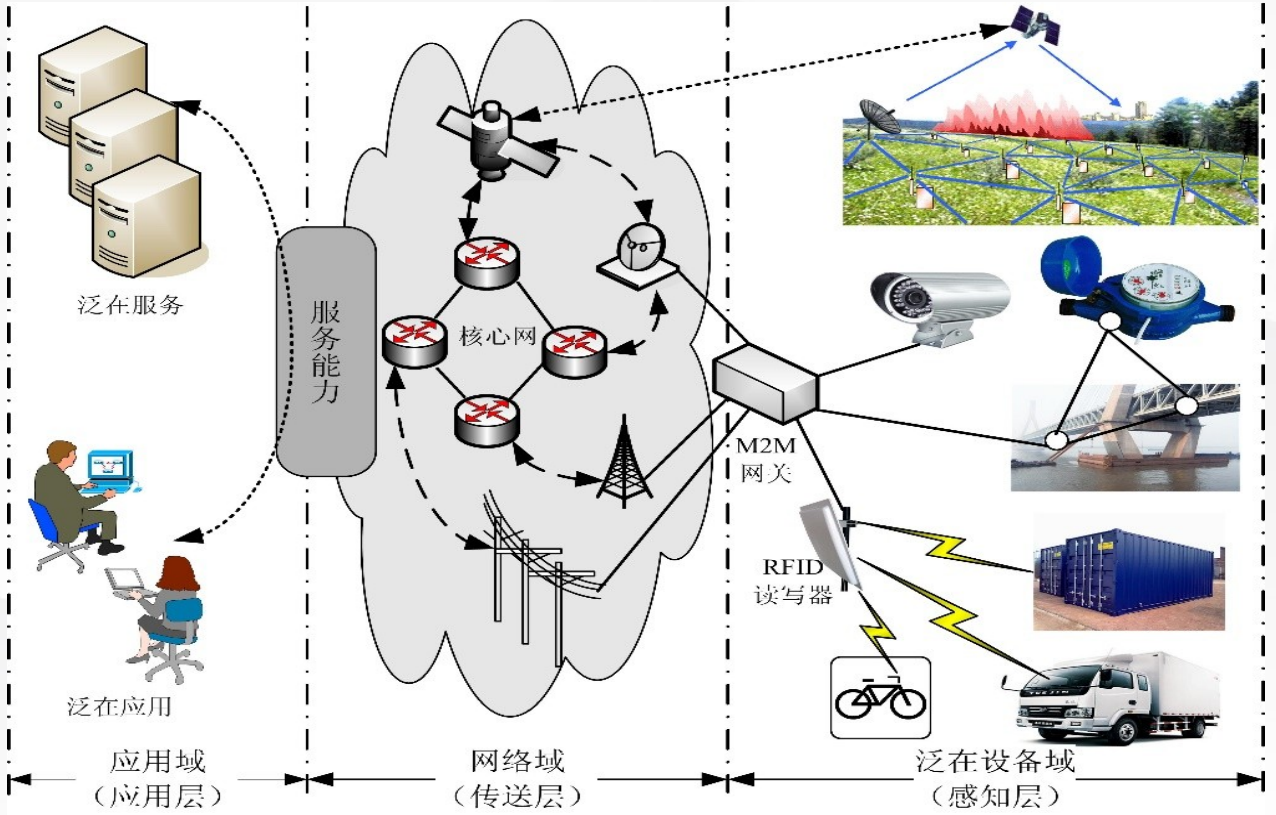
中国政府工作

2010

2010

物联网组成架构


应用层
智能交通
环境监测
智能医疗
内容服务
智能家居
处理层
数据挖掘
智能计算
云计算
中间件技术
网络层
核心网
IPv6
接入网
WiMAX
GSM
3G
卫星网
互联网
LTE
感知层
感知技术
RFID
传感器
红外感应
身体检测仪
公共技术
安全技术
网络管理
GoS管理


泛在服务
服务能力
核心网
M2M
网关
RFID
读写器
泛在应用
应用域
（应用层）
网络域
（传送层）
泛在设备域
（感知层）

物联网安全问题

全球物联网平台缺少统一的语言，很容易造成多个物联网设备彼此之间通信受阻并产生多个竞争性的标准和平台。

Mirai创造的物联网僵尸Botnets of Things，可发动DDos攻击，致使Dyn、Twitter、PayPal 等诸多人气网站暂时瘫痪。

中央服务器管理者在未经授权的情况下可能使用其存储和转发隐私数据。成都的266个监控摄像头被网络“直播”。

很多物联网都是运营商、企业内部网络。当涉及到跨多个运营商、多个对等主体之间协作时，建立信用的成本很高。

目前，物联网数据流都汇总到单一的中心控制系统，随着设备几何级数增长，中心化服务成本难以负担。

物联网安全挑战

感知层

感知层节点：网关节点、普通法节点等容易被恶意控制、捕获，容易受到外部 DOS 攻击；接入物联网的超大量传感节点的标识、认证易被劫持。

网络层

异构的物联网应用协议无法被安全设备识别，被篡改和入侵后无法及时发现

DOS 攻击、假冒攻击、中间人攻击、跨异构网络攻击等

管理服务层

存在高智能自动化处理系统带来不确定性，人为的干预导致服务不可用，设备丢失

来自于超大量终端的海量数据的识别和处理

应用层

许多应用层平台本身存在漏洞易导致未授权的访问、数据破坏和泄露、用户隐私保护；取证和销毁数据、保护知识产权

物联网安全防护技术

物联网安全防护技术：安全和隐私保护方面，物联网应用的仍然是互联网或通信网中常规的安全防护技术。

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

谢谢！

饮水思源 爱国荣校