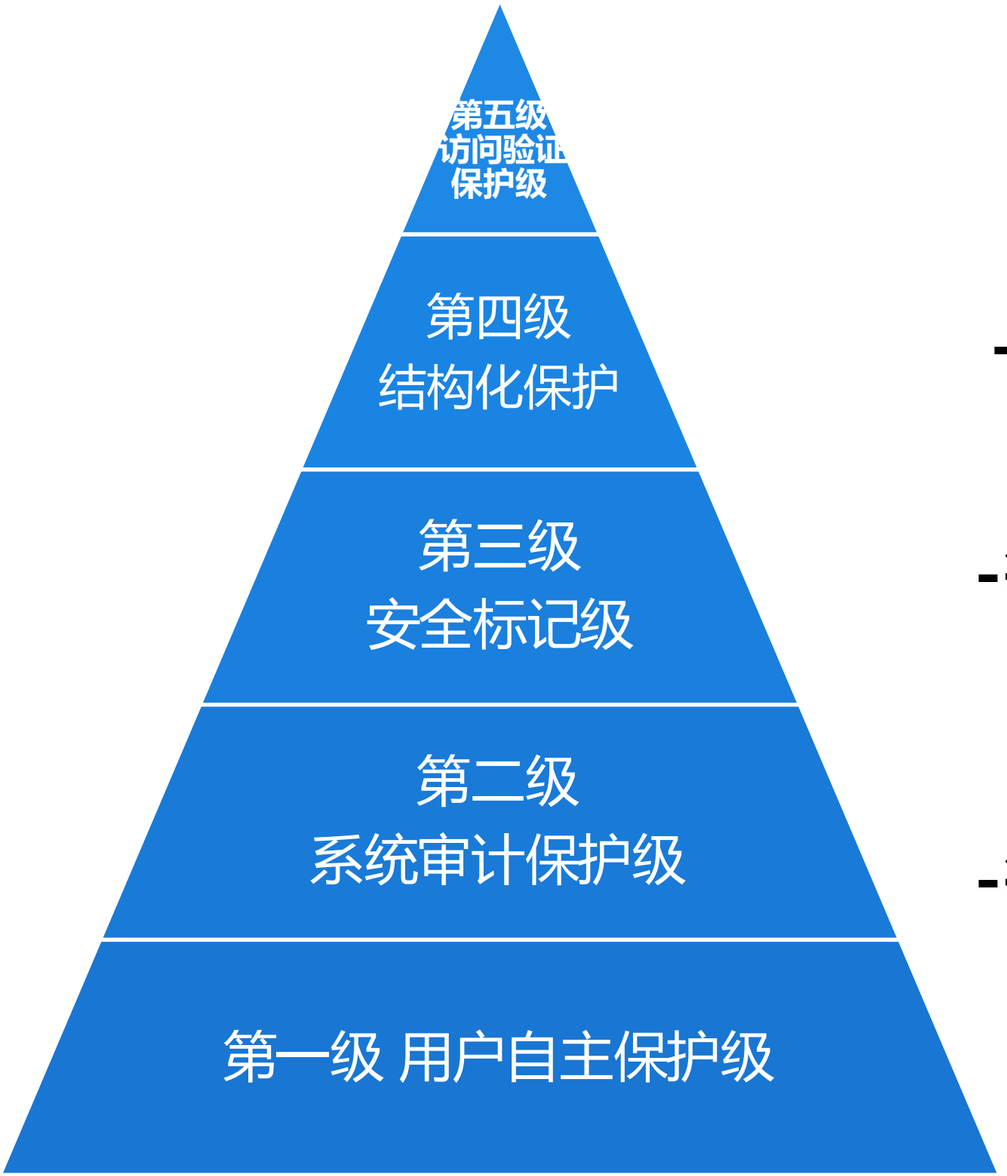
等级保护2.0《基本要求》解读

2019年5月

目录

01 等保2.0制度结构性变化解读

等级保护基本概念



-定义

- 等级保护全称为“信息系统安全等级保护”，现改为“**网络安全等级保护**”，是指对网络和信息系统按照**重要性等级分级别保护**的一种工作；根据网络与信息系统在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的**危害程度**等，由低到高被划分为**五个安全保护等级**

-概括说明

- 系统重要程度有多高，安全保护就应当有多强，既**不能保护不足，也不能过度保护。**

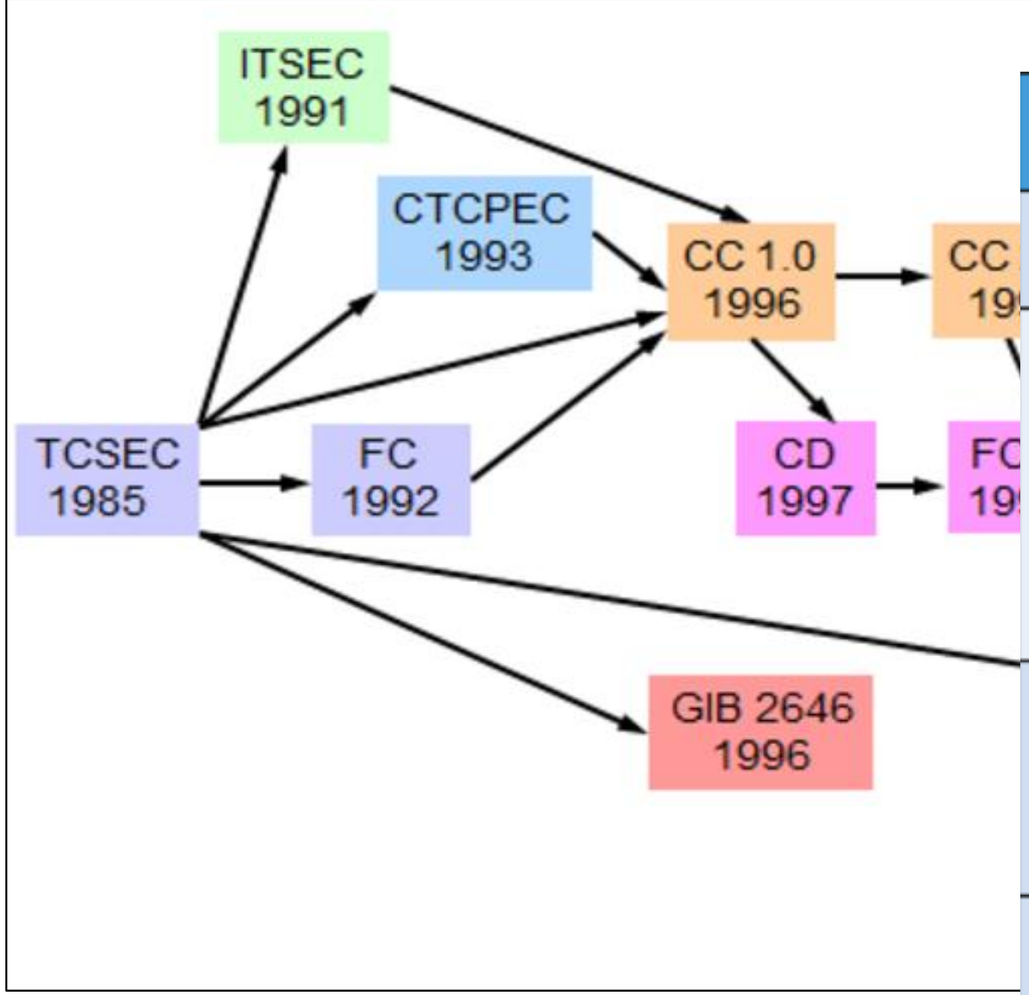
-等级保护对客户意义

- 遵循客观规律，网络安全的**等级是客观存在的**
- 有利于突出重点，**加强安全建设和管理**
- 有利于控制信息安全建设的成本，**平衡安全建设与成本**

-等级保护对国家意义

- **制度：**是为了构建国家信息安全保障体系。
- **抓手：**提高信息系统安全防护能力。
- **带有很强技术性的国家风险管控行为**

等级保护技术标准渊源

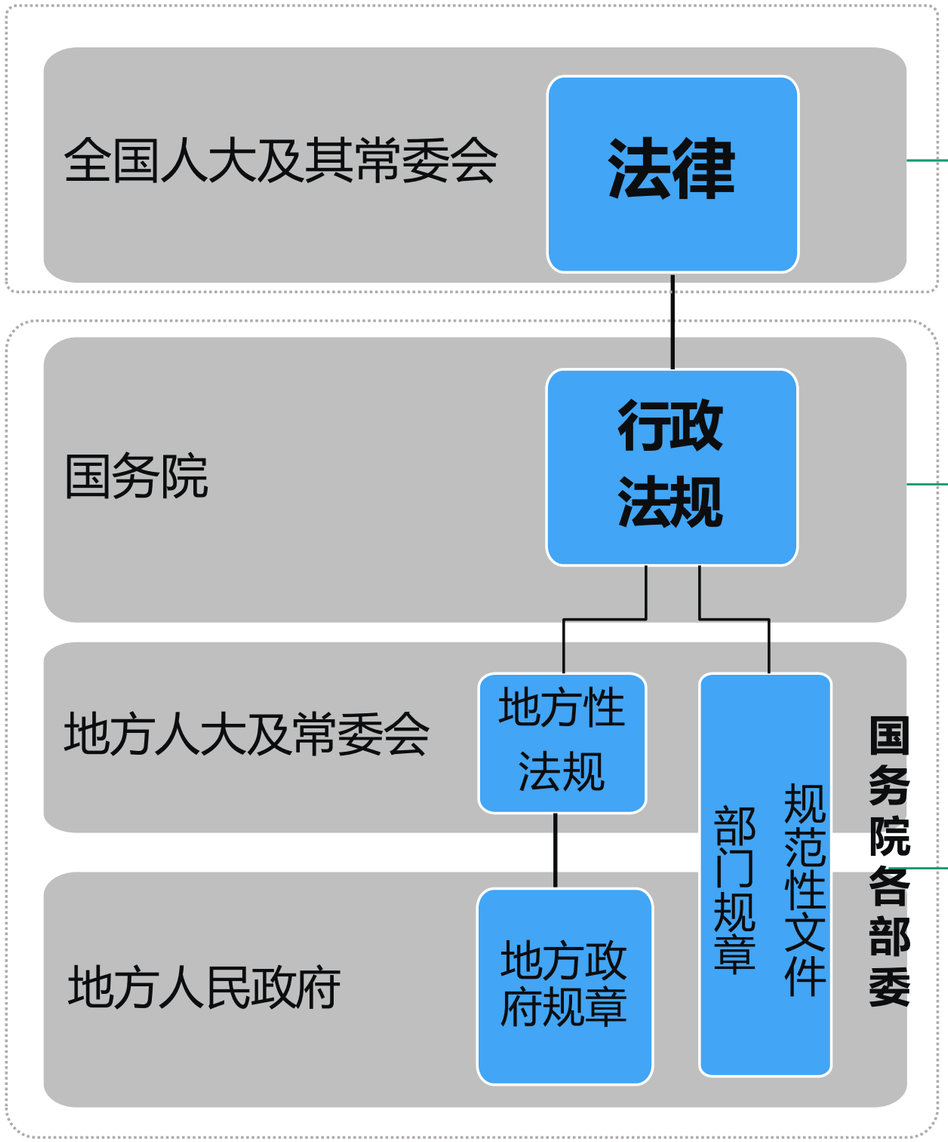


TCSEC		CC	GB 17859
A 验证保护级	A1 验证设计级	EAL7	——
B 强制保护级	B3 安全区域保护级	EAL6	第五级 访问验证保护级
	B2 结构化保护级	EAL5	第四级 结构化保护级
	B1 标记安全保护级	EAL4	第三级 安全标记保护级
C 自主保护级	C2 控制访问保护级	EAL3	第二级 系统审计保护级
	C1 自主安全保护级	EAL2	第一级 用户自主保护级
——	——	EAL1	——
D 无保护级别	D1	——	——

等级保护制度演进

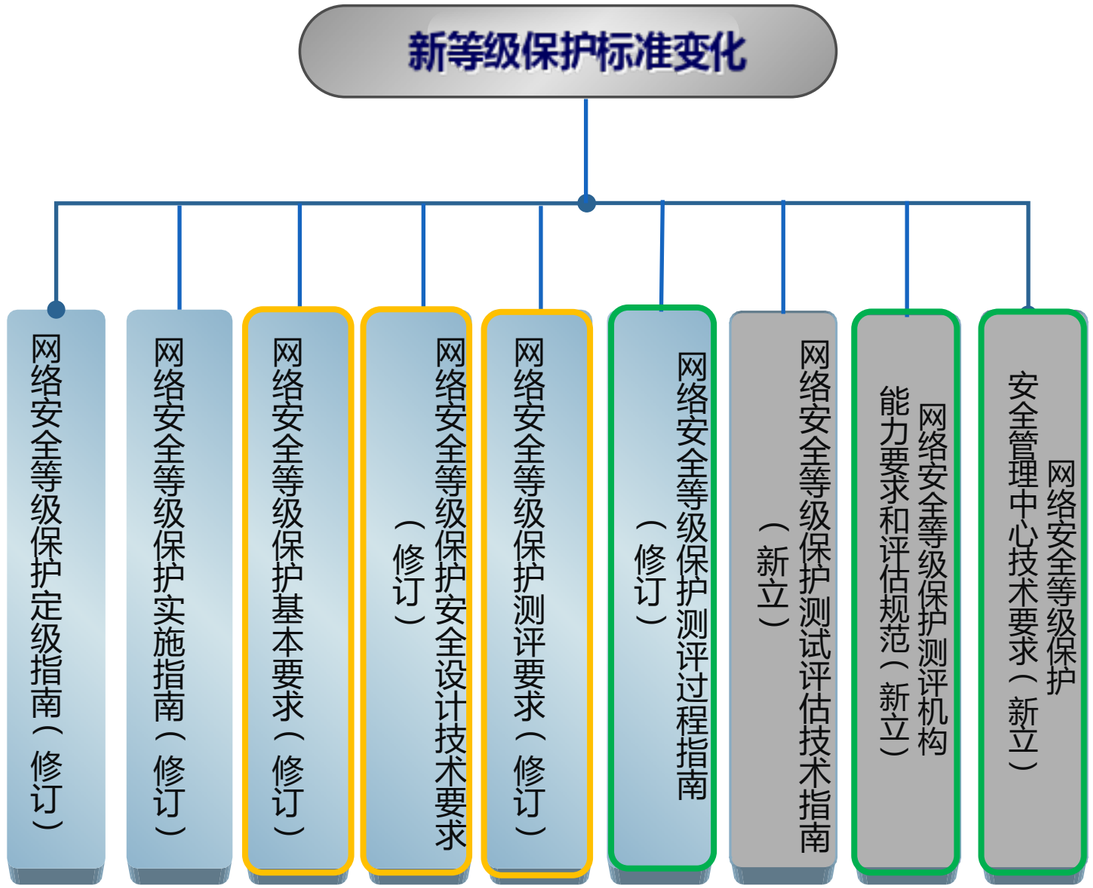

新时代
发展
启动
《网络安全等级保护条例》（征求意见稿）-公安部2018年6月
《中华人民共和国网络安全法》（全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行）
《关于加强国家级重要信息系统安全保障工作有关事项的通知》（工信安【2014】2182号）
《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发【2012】23号）
落实等保
定级
备案
安全建设整改
等级测评
检查
《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字【2007】861号）
《信息安全等级保护备案实施细则》（公信安【2007】1360号）
《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安【2009】1429号）
《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技【2008】2071号）
《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安【2010】303号）
关于印发《信息系统安全等级测评报告模板（试行）》的通知（公信安【2009】1487号）
《关于开展信息安全等级保护专项监督检查工作》的通知（公信安【2010】1175号）
《公安机关信息安全等级保护检查工作规范（试行）》（公信安【2008】736号）
发展等保
《信息安全等级保护管理办法》（公通字【2007】43号）
《关于信息安全等级保护工作的实施意见》（公通字【2004】66号）
《中华人民共和国计算机信息系
（国务院147号令）
首提等保
《国家信息化领导小组关于加强信息安全保障工作的
（中办发【2003】27号）
实行等保

等保政策法律地位的提升



	等级保护1.0	等级保护2.0
法律	宪法、刑法（部分条款） 国家安全法（部分条款） 保守国家秘密法 电子签名法 …	宪法、刑法（部分条款） 国家安全法（部分条款） 保守国家秘密法 电子签名法 网络安全法 …
行政法规	计算机信息系统安全保护条例 （国务院令 第147号） 商用密码管理条例 （国务院令 第273号）	计算机信息系统安全保护条例 （国务院令 第147号） 商用密码管理条例 （国务院令 第273号） 网络安全等级保护条例 关键信息基础设施安全保护条例
国务院各部委规范性文件、部门规章	信息安全等级保护管理办法 （公通字[2007]43号） 电子政务等级保护相关制度 （发改委） …	关键信息基础设施相关制度 （国家互联网信息办公室） 电子政务等级保护相关制度 （发改委） …

新等级保护标准体系


新等级保护标准变化
网络安全等级保护定级指南（修订）
网络安全等级保护实施指南（修订）
网络安全等级保护基本要求（修订）
网络安全等级保护安全设计技术要求（修订）
网络安全等级保护测评要求（修订）
网络安全等级保护测评过程指南（修订）
网络安全等级保护测试评估技术指南（新立）
网络安全等级保护测评机构能力要求和评估规范（新立）
网络安全等级保护安全管理中心技术要求（新立）


网络安全等级保护定级指南（GB/T 22240-20XX）
网络安全等级保护行业定级细则
网络安全等级保护测评机构能力要求和评估规范（GB/T 36959-2018）
网络安全等级保护测试评估技术指南（新立）
网络安全等级保护测评过程指南（GB/T 28449-2018）
网络安全等级保护测评要求（GB/T 28448-2019）
等级测评
安全定级
网络安全等级保护建设整改工作
基线要求
方法指导
网络安全等级保护实施指南（GB/T 25058-20XX）
网络安全等级保护安全设计技术要求（GB/T 25070-2019）
网络安全等级保护基本要求行业细则
网络安全等级保护基本要求（GB/T 22239-2019）
技术类
物理安全技术要求
网络基础安全技术要求
云计算服务安全指南
云计算服务安全能力要求
其他技术类标准
管理类
信息系统安全管理要求
安全工程管理要求
信息安全事件管理指南
信息安全风险评估规范
其他管理类标准
产品类
操作系统安全技术要求
数据库管理系统安全技术要求
网络和终端设备隔离部件技术要求
网络安全等级保护管理中心技术要求（GB/T 36958-2018）
其他产品类标准
计算机信息系统安全保护等级划分准则（GB 17859-1999）

新旧等级保护标准核心内涵对比

发展阶段	等级保护1.0时代	等级保护2.0时代
名称	信息（系统）安全等级保护	网络安全等级保护
顶层规范性文件	计算机信息系统安全保护条例 （行政法规）	网络安全法 （法律）
核心体系文件	信息安全等级保护管理办法 （部门规范性文件）	网络安全等级保护条例（征求意见） （行政法规）
配套标准	以GB/T 22239-2008、GB/T 28448-2012等为核心的信息系统安全等级保护标准及其他配套标准	以修订GB/T 22239、28448等为核心的网络安全等级保护标准（俗称等保2.0标准）及其它配套标准
流程	五个规定动作：定级、备案、建设整改、等级测评和监督检查	除五个规定动作外 风险评估、安全监测、通报预警、事件调查、应急演练、灾难备份、自主可控、供应链安全、效果评价、综治考核等重点措施纳入

等保1.0到2.0不仅仅是标准修订、技术升级，其核心更是法律效力的极大提升

定级备案中的变化

	等保1.0	等保2.0
定级依据	信息安全等级保护管理办法 第十条规定，《信息系统安全等级保护定级指南》配套使用	网络安全等级保护条例（征求意见稿）第二条中定义 修订GB/T 22240作为进一步细化
定级对象	信息安全等级保护工作直接作用的具体的信息和信息系统	网络安全等级保护工作的作用对象，主要包括基础信息网络、工业控制系统、云计算平台、物联网、使用移动互联技术的网络、其他网络以及大数据等。
定级对象基本特征	1）具有唯一确定的安全责任单位 2）具有信息系统的基本要求 3）承载单一或相对独立的业务应用	1）具有确定的主要安全责任主体； 2）承载相对独立的业务应用； 3）包含相互关联的多个资源。
定级特征之外要求	无	详细规定了：基础信息网络、 工业控制系统、 云计算平台、物联网、 采用移动互联技术的网络和大数据必须遵循的其他要求

	等保1.0	等保2.0
特定定级对象说明	无	对于基础信息网络、云计算平台、大数据平台等支撑类网络，原则上应不低于其承载的等级保护对象的安全保护等级 大数据安全保护等级不低于第三级。
关基要求	无	原则上不低于第三级
定级原则	自主定级、自主保护、监督指导	明确等级、增强保护、常态监督
备案对象与时限要求	二级以上系统，在安全保护等级确定后或新建系统投入使用30日内	第二级以上网络运营者应当在网络的安全保护等级确定后10个工作日内
定级流程	直接根据定级要素与安全等级关系定级	确定定级对象→初步确定等级→专家评审→主管部门审核→公安机关备案审查

安全要求变化

旧版标准

安全通用要求

新版标准

安全通用要求+安全扩展要求

■ 安全通用要求

不管等级保护对象的形态如何必须满足的要求。

■ 安全扩展要求

针对云计算、移动互联、物联网和工业控制系统提出了 特殊安全要求。

例

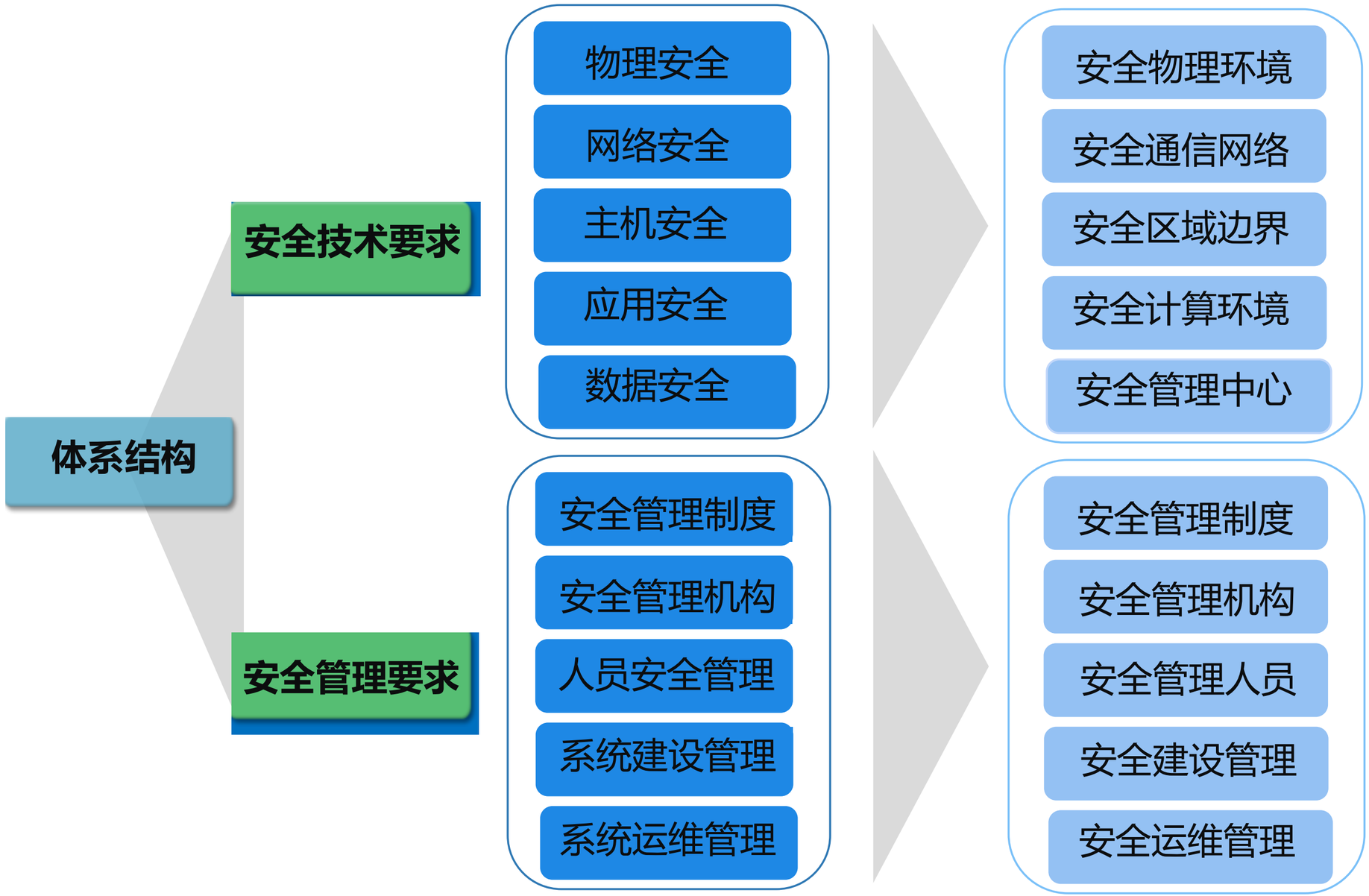
新标准某级安全要求

- 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

涉及标准：

■信息安全技术 网络安全等级保护基本要求
■信息安全技术 网络安全等级保护安全设计技术要求
■信息安全技术 网络安全等级保护测评要求

三个核心标准结构的统一

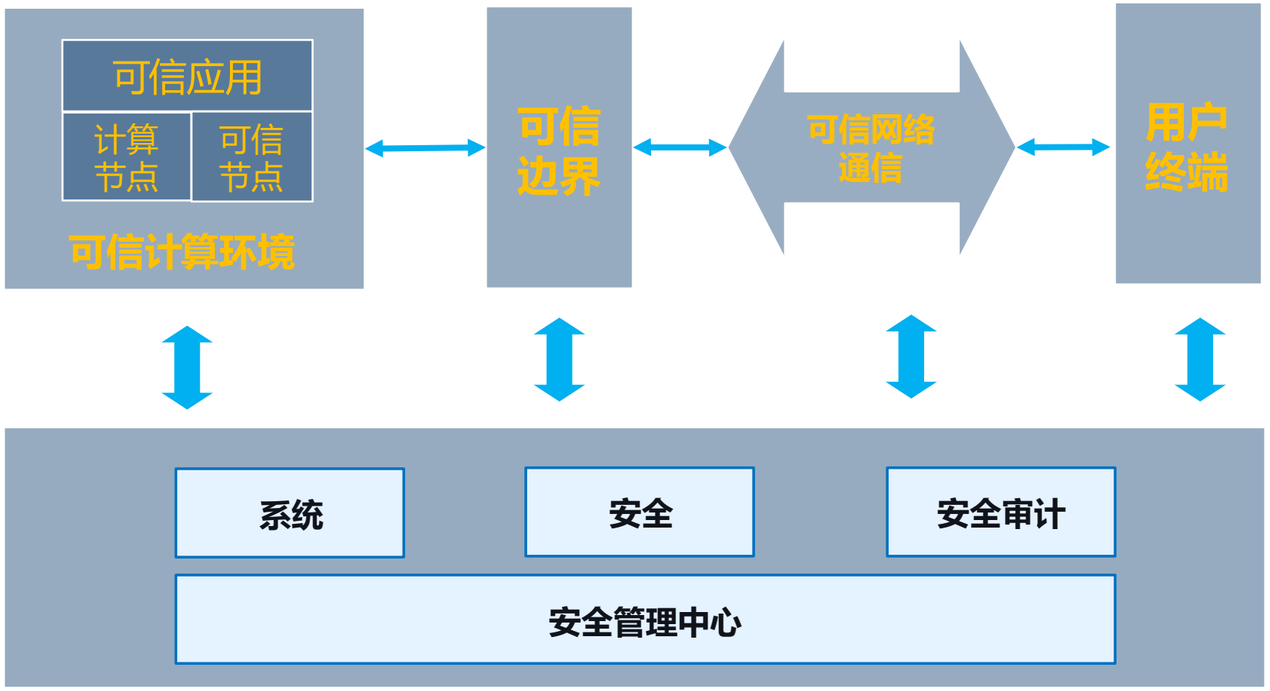


与GB/T 25070《网络安全等级保护安全设计技术要求》的体系结构保持一致.

等保2.0重要新增-可信计算

等保2.0加强可信体系作为重要思想，解决了GB 17859-1999在等级划分准则提出的“可信计算基” 要求

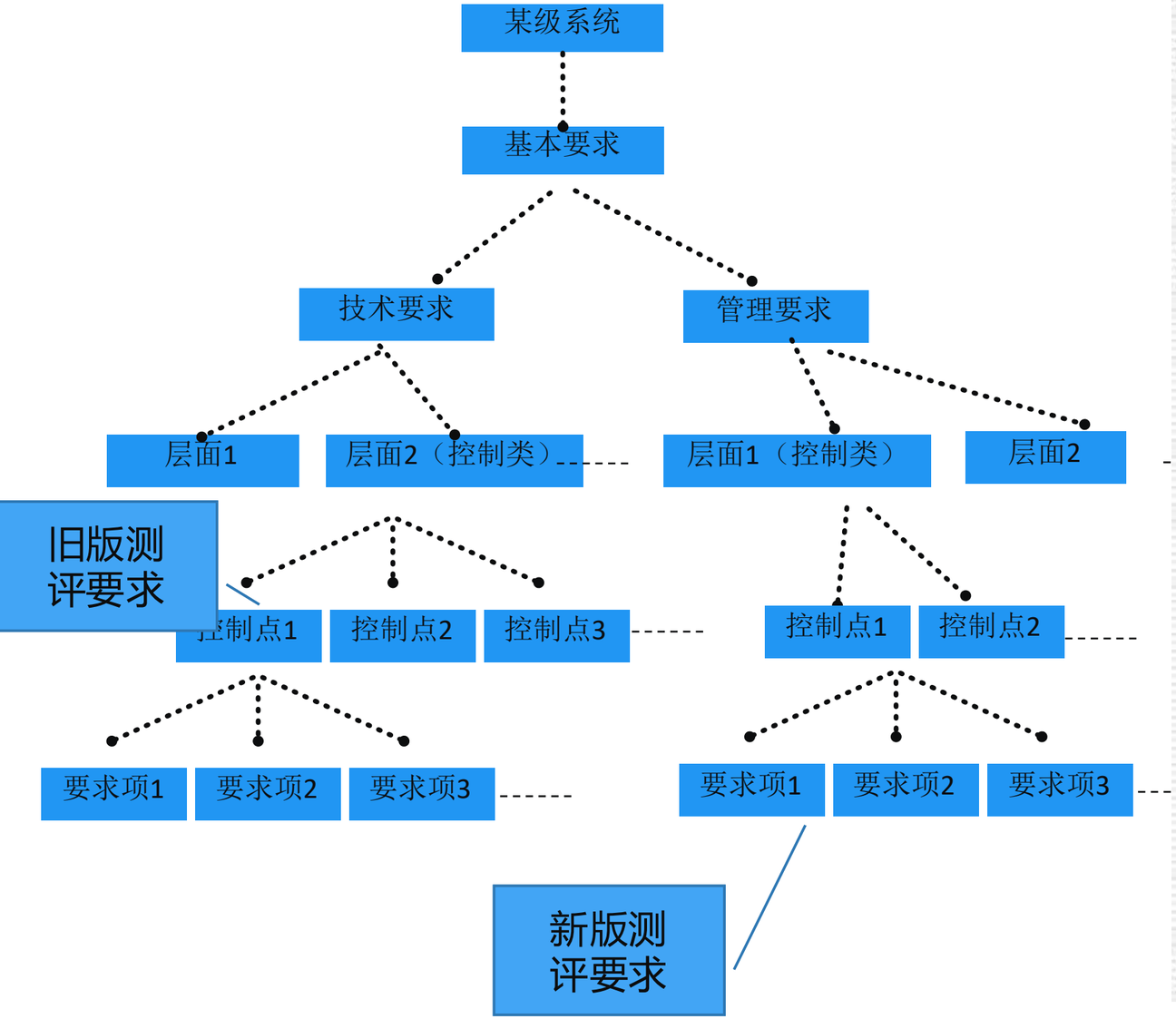
- 安全通信网络可信验证：可基于可信根对**通信设备**的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证
- 安全区域边界可信验证：可基于可信根对**边界设备**的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证
- 安全计算环境可信验证：可基于可信根对**计算设备**的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证



保护要求精简

《基本要求》1.0（三级通用要求）				《基本要求》2.0（三级通用要求）			
序号	安全控制类	安全控制点	安全要求项	序号	安全控制类	安全控制点	安全要求项
1	物理安全	10	32	1	安全物理环境	10	22
2	网络安全	7	33	2	安全通信网络	3	8
3	主机安全	8	32	3	安全区域边界	6	20
4	应用安全	8	31	4	安全计算环境	11	34
5	数据安全	3	8	5	安全管理中心	4	12
6	安全管理制度	3	11	6	安全管理制度	4	7
7	安全管理机构	5	20	7	安全管理机构	5	14
8	人员安全管理	5	16	8	安全管理人员	4	12
9	系统建设管理	11	45	9	安全建设管理	10	34
10	系统运维管理	13	62	10	安全运维管理	14	48
合计		73	290	合计		71	211

测评要求细化



8 第三级测评要求

8.1 安全测评通用要求

8.1.1安全物理环境

8.1.1.1 物理位置选择

8.1.1.1.1 测评单元（L3-PES1-01）

该测评单元包括以下要求：

a) 测评指标：机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 测评对象：机房。

c) 测评实施包括以下内容：

1) 应检查所在建筑物是否具有建筑物抗震设防审批文档；

2) 应检查是否存在雨水渗漏；

3) 应检查门窗是否因风导致的尘土严重；

4) 应检查屋顶、墙体、门窗和地面等是否破损开裂。

d) 单项判定：如果1）-4）均为肯定，则等级保护对象符合本单项测评指标要求，否则，等级保护对象不符合或部分符合本单项测评指标要求。

由原来的控制点变为要求项

此处为新增项

针对要求项的测评实施

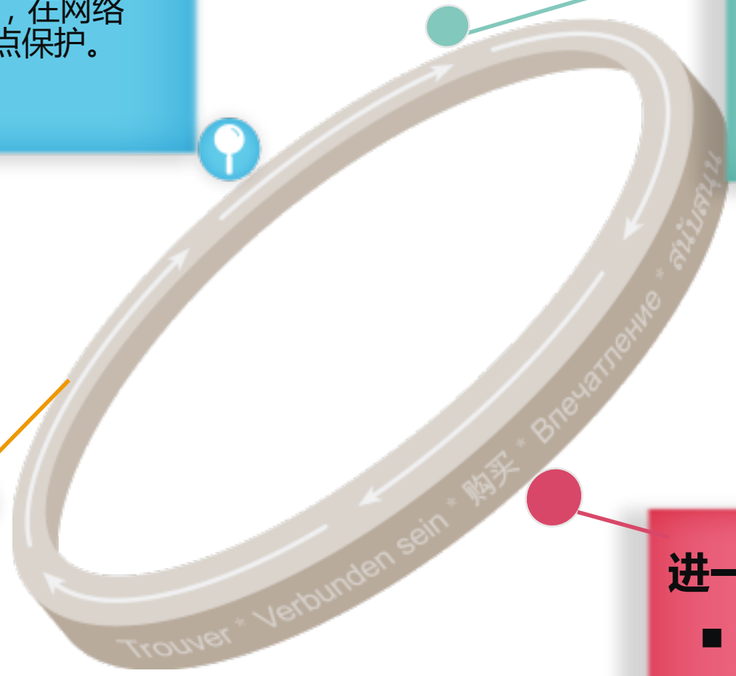
新形势下的等级保护

网络安全法确立等级保护制度地位

- 21条规定：国家实行等级保护制度；
- 31条规定：国家对关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

等级保护外延进一步丰富和完善

- 等级保护对象不断扩充（云计算、工业控制、物联网、移动安全）；
- 工作内容更加完善（供应链安全、通报预警等）
- 保护要求更加适应新威胁形势（针对高级威胁、增加可信计算）。



等级保护政策体系进一步细化完善

- 等级保护管理条例/关键信息基础设施保护条例发布征求意见稿；
- 配套管理规范、实施细则正在陆续出台。

进一步提升适用性和可操作性

- 核心标准全部修订，内容精简、结构统一、测评要求细化、充分考虑可操作性；
- 适应新技术发展变化，增加扩展要求。

02 《基本要求》的变化及主要条款解读

《基本要求》的修订过程


2013.12
成立标准编制组
2015.3
形成新标草案第一稿
形成通用要求、云计算、物联网、移动互联、工业控制5个分册
2016.9
历经7次草案修改，形成征求意见稿。
2017.8
根据网信、公安意见将五分册合一，形成送审稿。
2017.10
参加安标委WG5工作组会议，征求127家单位意见，修订后形成报批稿。
2018.7
根据沈昌祥院士的意见再次调整分类结构，强化可信计算，形成修订后报批稿。

《基本要求》的主要变化

安全要求的变化

- 增加了安全扩展要求
- 文档章节结构随着变化，如：

8 第三级安全要求

8.1 安全通用要求

8.2 云计算安全扩展要求

8.3 移动互联安全扩展要求

8.4 物联网安全扩展要求

8.5 工业控制系统安全扩展要求

增加了安全框架和应用场景说明

- 附录B 关于等级保护对象整体安全保护能力的要求
- 附录C 等级保护安全框架和关键技术使用要求
- 附录D 云计算应用场景说明
- 附录E 移动互联应用场景说明
- 附录F 物联网应用场景说明
- 附录G 工业控制系统应用场景说明
- 附录H 大数据应用场景说明

取消了控制点的标注

取消了对控制点“S” “A” “G”的标记，在附录A“关于安全通用要求和安全扩展要求的选择和使用” 中增加了安全控制措施选择时，控制点的标注及使用说明。

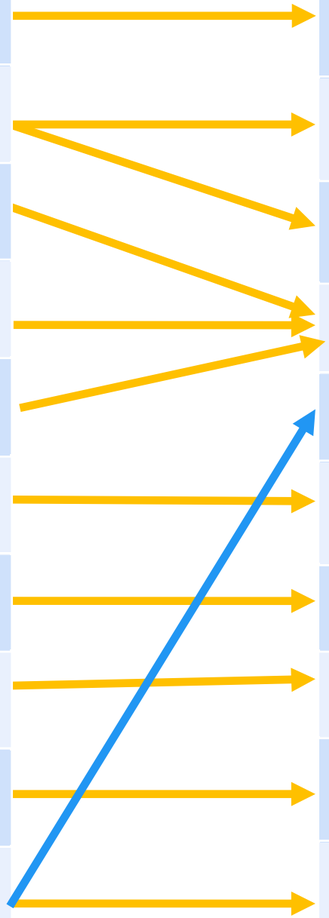
控制措施结构变化

技术部分：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心

管理部分：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理

《基本要求》控制点的对应关系

等保1.0		等保2.0最新版	
技术要求	物理安全	安全物理环境	技术要求
	网络安全	安全通信网络	
	主机安全	安全区域边界	
	应用安全	安全计算环境	
	数据安全及备份恢复	安全管理中心	
管理要求	安全管理制度	安全管理制度	管理要求
	安全管理机构	安全管理机构	
	人员安全管理	安全管理人员	
	系统建设管理	安全建设管理	
	系统运维管理	安全运维管理	



《基本要求》扩展要求的增加

安全要求项	第一级	第二级	第三级	第四级	增加内容说明
云计算安全扩展要求	11	29	46	49	主要增加的内容包括 “基础设施的位置”、“虚拟化安全保护”、“镜像和快照保护”、“云服务商选择” 和 “云计算环境管理” 等方面。
移动互联安全扩展要求	5	14	19	21	主要增加的内容包括 “无线接入点的物理位置”、“移动终端管控”、“移动应用管控”、“移动应用软件采购” 和 “移动应用软件开发” 等方面。
物联网安全扩展要求	4	7	20	21	主要增加的内容包括 “感知节点的物理防护”、“感知节点设备安全”、“感知网关节点设备安全”、“感知节点的管理” 和 “数据融合处理” 等方面。
工业控制系统安全扩展要求	9	15	21	11	主要增加的内容包括 “室外控制设备防护”、“工业控制系统网络架构安全”、“拨号使用控制”、“无线使用控制” 和 “控制设备安全” 等方面，针对工业控制系统实时性要求高的特点调整了 “漏洞和风险管理” 和 “恶意代码防范管理” 方面的要求。

《基本要求》——通用要求
主要变化内容解读

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	层面名称	旧版控制点	层面名称	新版控制点
1	物理安全	物理位置的选择	安全物理环境	物理位置选择
2		物理访问控制		物理访问控制
3		防盗窃和防破坏		防盗窃和防破坏
4		防雷击		防雷击
5		防火		防火
6		防水和防潮		防水和防潮
7		防静电		防静电
8		温湿度控制		温湿度控制
9		电力供应		电力供应
10		电磁防护		电磁防护

安全物理环境

1. 物理位置选择：防震、防风、防雨，避免顶层或地下室
2. 物理访问控制：机房专人值守或电子门禁；**机房电子门禁；重要区域第二道电子门禁**
3. 防盗防破坏：主要设备有标记；设备有标记，电缆要隐蔽(底下或管道)；**机房防盗报警系统或专人值守的视频监控**
4. 防雷击：接地，**防雷保安器或过压保护**
5. 防火：机房有灭火设备；自动消防系统，耐火建筑材料，**机房区域隔离**
6. 防水防潮：机房防水渗透；机房防水蒸气结露，地下积水转移渗透；**防水检测仪表**
7. 防静电：防静电地板，**静电消除器，防静电手环**
8. 温湿度控制：温湿度可调节；温湿度自动调节设施
9. 电力供应：电路稳压过压保护，短期备用电力供应，**冗余供电或并行电缆；提供应急供电设施**
10. 电磁防护：电源线与通信线缆隔离铺设，**关键设备电磁屏蔽；关键区域电磁防护**

等保2.0对部分条款进行了精简，体现可操作性，整体变化不大。
关注点：
- 机房不要在顶层(承重)或地下(漏水)
- 电子门禁、视频监控
- 冗余供电

- **符合GB 50174-2017《数据中心设计规范》**（*替换GB 50174-2008《电子信息系统机房设计规范》*）**的要求.**

*注：黑色字体为二级要求；**黑色加粗字体**为三级要求；红色字体为四级要求。*

主要差异

控制点	旧版标准	新版标准	差异	
物理位置选择	机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。	机房场地应选择在具有防震、防风和防雨等能力的建筑内。	符合实际	改
	机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。	机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。	符合实际	改
物理访问控制	机房出入口应安排专人值守，控制、鉴别和记录进入的人员。 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。（二级） 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。（三级）	符合实际	删、改
防盗窃和防破坏	应将主要设备放置在机房内	——	符合实际	删
	应利用光、电等技术设置机房防盗报警系统。 应对机房设置监控报警系统。	应设置机房防盗报警系统或设置有专人值守的视频监控系统。	符合实际	改
防火和防潮	水管安装，不得穿过机房屋顶和活动地板下。	——	符合实际	删
电力供应	应建立备用供电系统	——	符合实际	删
电磁防护	应对关键设备和磁介质实施电磁屏蔽	应对关键设备实施电磁屏蔽	符合实际	删、改

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	旧版层面名称	旧版控制点	序号	新版层面名称	新版控制点
1	网络安全	结构安全	1	安全通信网络	网络架构
2		访问控制	2		通信传输
3		安全审计	3		可信验证
4		边界完整性检查	4		
5		入侵防范	5		
6		恶意代码防范	6		
7		网络设备防护	7		

安全通信网络

1. 网络架构：划分不同网络区域，避免将重要区域部署在网络边界处；**设备业务处理能力和带宽满足业务高峰需要**；**关键设备与链路冗余；可根据业务重要程度分配带宽，优先保障重要业务。**
2. 通信传输：采用校验技术保证数据完整性；采用校验技术**或密码技术**保证数据完整性，**采用密码技术保证数据保密性；双向身份验证；重要通信采用基于密码模块的加解密和密钥管理。**
3. 可信验证：可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，**并在应用程序的所有执行环节进行动态可信验证**，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，**并进行动态关联感知。**

等保2.0变化点：
1、改结构安全为网络架构，强调设备处理能力与带宽供给。
2、在原应用通信完整性和保密性基础上增加网络通信传输安全要求。
3、新增可信验证，对通信设备提出基于可信根的可信验证要求，本项为可选项。
4、将等保1.0“网络安全”中的访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范的主要内容放在等保2.0“安全区域边界”部分中。
5、将等保1.0“网络安全”中的网络设备防护的主要内容放在“安全管理中心”部分中。

主要差异

旧版标准		新版标准		差异	
结构安全	应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。	网络架构	应保证网络设备的业务处理能力满足业务高峰期需要。	网络设备性能	增
	应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。		——（放在第四级）		删
——	应采用密码技术保证通信过程中数据的完整性（应用安全-通信完整性）	通信传输	应采用校验技术或密码技术保证通信过程中数据的完整性。	SSL VPN、IPSEC VPN	增
	在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证； 应对通信过程中的整个报文或会话过程进行加密（应用安全-通信保密性）		应采用密码技术保证通信过程中数据的保密性。		增
——		可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证， 并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	通信设备可信模块	增

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	旧版层面名称	旧版控制点	序号	新版层面名称	新版控制点
1	网络安全	结构安全	1	安全区域边界	边界防护
2		访问控制	2		访问控制
3		安全审计	3		入侵防范
4		边界完整性检查	4		恶意代码和垃圾邮件防范
5		入侵防范	5		安全审计
6		恶意代码防范	6		可信验证
7		网络设备防护	7		

安全区域边界

1. 边界防护：访问与数据流通过受控接口；**非授权用户接入检查或限制（发现时阻断）；内部用户外检查或限制（发现时阻断）；无线接入网关边界；采用可信验证机制对接入设备进行可信验证。**
2. 访问控制：网络边界部署访问控制策略，优化ACL表，协议检查；访问控制策略部署扩展到域边界，根据会话状态信息控制访问，粒度到端口；**基于应用协议和应用内容的访问控制；通信协议转化或隔离方式交换数据。**
3. 入侵防范：关键网络节点监控攻击，**限制从外向内的攻击，限制从内向外的攻击，通过对行为分析检测新型网络攻击；记录检测到的攻击并报警。**
4. 恶意代码和垃圾邮件防范：关键节点处检测和清除恶意代码，维护更新；**关键节点检测和防护垃圾邮件，维护更新。**
5. 安全审计：网络边界与重要网络节点，审计覆盖每个用户，审计重要用户行为和重要安全事件；审计记录包含必要信息；审计记录防篡改防删除，定期备份；**对远程访问行为和互联网访问行为单独审计分析。**
6. 可信验证：基于可行根对边界设备进行可信验证，**并在应用程序的关键执行环节进行动态可信验证，**在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，**并进行动态关联感知。**

等保2.0变化点：
1、新增“边界防护”，明确跨越边界数据通过受控接口，控制内联、外联、**无线接入**等非授权网络出入口。
2、访问控制能基于应用协议和应用内容。
3、入侵检测要求提高，能检测、防止或限制从内向外和从外向内的攻击，能检测新型网络攻击。
4、增加对垃圾邮件检测、防护要求。
5、安全审计强调远程访问与互联网行为的审计。
6、增加对边界设备的可信验证要求（可选）。

主要差异

旧版标准		新版标准		差异	
——	——	边界防护	应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络	无线接入安全网关	增
访问控制	应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；	访问控制	应对进出网络的数据流实现基于应用协议和应用内容的访问控制。	第二代防火墙	改
	——		应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	策略管理	增
入侵防范	应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。	入侵防范	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；	入侵防护、天眼、抗DDOS系统，威胁情报	增
	——		应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；		增
安全审计	——	安全审计	应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	上网行为管理	
恶意代码防范	——	恶意代码和垃圾邮件防范	应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	防垃圾邮件网关	增

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	旧版层面名称	旧版控制点	序号	新版类名称	新版控制点
1	主机安全	身份鉴别	1	安全计算环境	身份鉴别
2		安全标记	2		访问控制
3		访问控制	3		安全审计
4		可信路径	4		可信验证
5		安全审计	5		入侵防范
6		剩余信息保护	6		恶意代码防范
7		入侵防范	7		数据完整性
8		恶意代码防范	8		数据保密性
9		系统资源控制	9		数据备份恢复
1	应用安全	身份鉴别	10		剩余信息保护
2		安全标记	11		个人信息保护
3		访问控制			
4		可信路径			
5		安全审计			
6		剩余信息保护			
7		通信完整性			
8		通信保密性			
9		软件容错			
10		资源控制			
1	数据安全及备份恢复	数据完整性			
2		数据保密性			
3		备份和恢复			

安全计算环境

1. 身份鉴别：身份标识唯一，登录失败处理；远程管理防鉴别窃听；**双因子身份鉴别；至少一种是密码技术**；
2. 访问控制：重命名默认账户与口令，清理无用账户与共享账户；管理用户最小授权，管理权限分离；**授权管理，主体粒度为用户或进程，客体到文件或数据库表，重要主体和客体设置安全标记，控制访问；对所有主客体安全标记，主客体设置安全标记，实现强制性访问控制。**
3. 安全审计：审计覆盖每个用户，审计重要用户行为和安全事件；审计记录包含必要信息（**主客体标识**），审计记录定期备份，防篡改防删除；**审计进程进行保护，防止中断；**
4. 入侵防范：最小安装，关闭不需要服务、默认共享和高危端口；限制管理终端接入方式与地址，数据有效性校验；发现漏洞并修补；**能检测到对重要节点的入侵并报警。**
5. 恶意代码防范：采用免受恶意代码攻击的技术措施**或主动免疫可信验证机制（采用主动免疫可信验证机制）**及时识别入侵和病毒行为，并将其有效阻断；
6. 可信验证：基于可行根对计算设备进行可信验证，**并在应用程序的关键执行环节进行动态可信验证，**在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，**并进行动态关联感知。**

等保2.0变化点

1、将等保1.0中“主机安全”、“应用安全”和“数据安全及备份恢复”的内容融合合并。

2、身份鉴别、访问控制、安全审计要求针对的对象相应扩大，包括设备、操作系统、应用、数据库等。涵盖虚拟化系统、感知节点设备、控制设备、移动终端等。

3、将原等保1.0中主机安全中“资源控制”控制点的部分内容移到“安全计算环境”中；将应用安全中“资源控制”控制点的内容删除。

4、在主机恶意代码防范中增加主动免疫可信验证机制方式，三级可选，四级应实现。

5、增加对计算设备的可信验证要求（可选）。

安全计算环境

7. 数据完整性：重要数据传输校验完整性；**采用校验码技术或密码技术保护数据传输与存储时的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；采用密码技术提供数据原发证据与数据接收证据，实现抗抵赖。**
8. 数据保密性：**采用密码技术保护数据传输与存储时的保密性，包括鉴别数据、重要业务数据和重要个人信息等。**
9. 数据备份恢复：重要数据本地备份与恢复；异地备份，定时批量数据同步；**异地实时备份，重要系统热冗余；建设异地灾备中心，业务应用实时切换。**
10. 剩余信息保护：鉴别信息使用后的空间清除；**敏感数据使用后空间完全清除。**
11. 个人信息保护：只采集存储必需的；禁止未授权访问和非法使用。

等保2.0变化点：
6、将等保1.0应用安全中“抗抵赖”、数据安全中“数据完整性”和“数据保密性”的内容合并为等保2.0中安全计算环境中的“数据完整性”和“数据保密性”，并细化和扩充对象范围。
7、增加对个人信息保护的要求，二级系统及以上均要求。

主要差异

旧版标准		新版标准		差异	
身份鉴别	应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	身份鉴别	应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	身份鉴别采用密码技术	改、增
恶意代码防范	应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库； 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库； 应支持防恶意代码的统一管理。	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	终端范围包括宿主机、虚拟机、移动终端、控制设备	改、增
——	——	个人信息保护	应仅采集和保存业务必需的用户个人信息； 应禁止未授权访问和非法使用用户个人信息。	主要针对应用系统	增
备份和恢复	应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。	数据备份恢复	应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； 应提供重要数据处理系统的热冗余，保证系统的高可用性。	包括边界路由器、边界防火墙、核心交换机、应用服务器、数据库服务器等。	增

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

新版类名称	新版控制点
安全管理中心	系统管理
	审计管理
	安全管理
	集中管控

安全管理中心

1. 系统管理：对系统管理员身份鉴别，只允许通过特定命令或界面操作，并对操作进行审计；通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
2. 审计管理：对审计管理员身份鉴别，只允许通过特定命令或界面操作，并对操作进行审计；通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
3. **安全管理：对安全管理员身份鉴别，只允许通过特定命令或界面操作，并对操作进行审计；通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。**
4. **集中管控：划分出特定的管理区域，并建立安全的信息传输路径，对分布在网络中的安全设备或安全组件进行管控；对设备、链路运行状况进行集中监测；对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；对网络中发生的各类安全事件进行识别、报警和分析；保证系统范围内的时间由唯一确定的时钟产生。**

突出了“一个中心”的核心地位

等保2.0变化点：
1、本**控制类**为新增，等保1.0中将安全管理中心的相关要求在网络安全、主机安全部分中分散描述。
2、明确了系统三员（系统管理员、审计管理员和安全管理员）及相关工作职责。
3、本控制类是对整个安全管理区的要求，具体要求可参见GB/T 36958-2018《网络安全等级保护安全管理中心技术要求》。

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	旧版层面名称	旧版控制点	序号	新版层面名称	新版控制点
1	安全管理制度	管理制度	1	安全管理制度	安全策略
2		制定和发布	2		管理制度
3		评审和修订	3		制定和发布
			4		评审和修订

安全管理制度

1. 安全策略：制定总体方针与安全策略，包括总体目标、范围、原则与框架等。
2. 管理制度：日常工作有安全管理制度；为主要（**各类**）管理内容建立安全制度，日常管理有操作规程；**形成安全管理体系(四级体系：安全策略、管理制度、操作规程、记录表单等)。**
3. 制定和发布：专门发布部门或人员，正式发布，版本控制。
4. 评审和修订：定期评审和修订。

等保2.0变化点
1、增加“安全策略” 控制点，将等保1.0中“管理制度”控制点中的部分内容移至“安全策略” 中，强调安全策略要求 。
2、借鉴ISO 27001的四级安全管理体系。

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	旧版层面名称	旧版控制点	序号	新版层面名称	新版控制点
1	安全管理机构	岗位设置	1	安全管理机构	岗位设置
2		人员配备	2		人员配备
3		授权和审批	3		授权和审批
4		沟通和合作	4		沟通和合作
5		审核和检查	5		审核和检查

安全管理机构

1. 岗位设置：**成立安全管理委员会或领导小组，最高领导由单位主管领导担任或授权**；定义安全部门与安全主管等的职责；设立三员，定义部门及岗位职责。
2. 人员配备：一定数量的三员配置；**专职安全管理员，不可兼任；关键岗位多人共同管理。**
3. 授权和审批：明确审批事项与流程；重要事项包括系统变更、重要操作、物理访问、系统接入等，**重要活动建立逐级审批制度；定期审查审批事项，更新审批相关信息。**
4. 沟通和合作：内部沟通会，外部沟通通信录(网络安全职能部门、供应商、专家、组织等)。
5. 审核和检查：定期常规检查(日常运行、系统漏洞、数据备份等)**；定期全面检查，如策略与配置的一致，安全措施的有效性等，制定检查表格，形成检查报告，结果进行通报。**

等保2.0变化点
1、明确安全管理一把手为单位主管领导或其授权。
2、将部分内容进行了归并精简，措辞调整，如公安机关改为“网络安全职能部门”。

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	旧版层面名称	原有控制点	序号	新版层面名称	新的控制点
1	人员安全管理	人员录用	1	安全管理人员	人员录用
2		人员离岗	2		人员离岗
3		人员考核	3		安全意识教育和培训
4		安全意识教育和培训	4		外部人员访问管理
5		外部人员访问管理			

安全管理人员

1. 人员录用：专人负责录用；人员背景审查；**技能考核，人员签保密协议，关键岗位签岗位责任协议；关键岗位人员内部选拔。**
2. 人员离岗：及时终止权限，收回设备；**承诺调离保密义务。**
3. 安全意识教育和培训：对各类人员进行安全意识教育和岗位技能培训，告知安全责任与惩戒措施；**不同岗位制定不同培训计划；定期对不同岗位人员进行技能考核。**
4. 外部人员访问管理：访问受控区域书面申请，需授权或审批，专人全程陪同，登记备案；访问受控网络书面申请，专人开设账户，分配权限，登记备案；离场后及时清除来访者权限；**与外部授权人员签保密协议，不得复制和泄露敏感信息；关键区域与关键应用不允许外部人员访问。**

等保2.0变化点
1、将等保1.0中的“人员考核”和“安全意识教育和培训”合并到等保2.0的“安全意识教育和培训”，描述适当精简。
2、细化和明确了外部人员访问的受控网络的权限管理要求。

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	旧版层面名称	旧版控制点	序号	新版层面名称	新版控制点
1	系统建设管理	系统定级	1	安全建设管理	系统定级和备案
2		安全方案设计	2		安全方案设计
3		产品采购和使用	3		产品采购和使用
4		自行软件开发	4		自行软件开发
5		外包软件开发	5		外包软件开发
6		工程实施	6		工程实施
7		测试验收	7		测试验收
8		系统交付	8		系统交付
9		系统备案	9		等级测评
10		等级测评	10		服务供应商选择
11		安全服务商选择			

安全建设管理

1. 定级备案：书面说明安全等级及确定方法和理由；组织专家论证，相关部门批准；主管部门及公安备案。
2. 安全方案设计：依据等级选择措施，依据风险补充调整措施；**考虑与其他等级保护对象的关系，进行安全整体规划和方案设计，包括密码技术内容，形成配套文件；对安全整体规划及配套文件进行评审，批准后实施。**
3. 产品采购和使用；网络安全产品符合国家规定；密码产品符合密码主管部门有关规定；**预先产品选型，定期更新候选名单；重要部位产品委托专项测试后选择。**
4. 自行软件开发：开发与实际环境分离，测试数据受控；开发中安全性测试；上线前恶意代码检测；**开发管理制度，代码编写安全规范，开发过程文档管理，程序资源库的修改、更新、发布进行授权和批准，严格版本控制；专职开发人员，开发活动受控。**
5. 外包软件开发：恶意代码检测；提供设计文档与使用指南；**提供源代码，审查后门或隐秘通道。**
6. 工程实施：专人管理实施过程；制定工程实施方案；**第三方监理。**
7. 测试验收：测试验收方案，验收报告；上线前安全测试报告；**包含密码应用的安全性测试。**
8. 系统交付：交付清单，根据清单清点；对运维人员培训；提供建设过程文档，运维文档。
9. 等级测评：定期测评，及时整改；重大变更或级别变化需要测评；选择合规的测评机构。
10. 服务商选择：选择合规服务商，签订协议；明确服务供应链各方的安全义务；**定期监督评审服务，控制服务内容变更。**

等保2.0变化点

1、根据新的等级保护实施流程，将等保1.0中的“系统定级”和“系统备案”合并为等保2.0的“定级备案”。

2、三级系统方案设计强调保护对象的关联性和整体安全规划，包含密码技术。

3、明确了自行开发的安全性测试和上线前检测的要求。

4、三级系统要求第三方工程监理，（等保1.0仅对四级系统要求）。

5、等保1.0中在“等级测评”中要求三级系统每年测评一次，四级系统每半年测评一次，等保2.0中调整为“定期等级测评”，在定级指南中明确三级以上均为每年测评一次。

6、将等保1.0中“安全服务商选择”改为“服务供应商选择”，要求明确服务供应链各方安全义务。

《基本要求》控制点的变化

技术要求					管理要求				
安全物理环境	安全通信网络	安全区域边界	安全计算环境	安全管理中心	安全管理制度	安全管理机构	安全管理人员	安全建设管理	安全运维管理

序号	旧版层面名称	旧版控制点	序号	新版层面名称	新版控制点
1	系统运维管理	环境管理	1	安全运维管理	环境管理
2		资产管理	2		资产管理
3		介质管理	3		介质管理
4		设备管理	4		设备维护管理
5		监控管理和安全管理中心	5		漏洞和风险管理
6		网络安全管理	6		网络和系统安全管理
7		系统安全管理	7		恶意代码防范管理
8		恶意代码防范管理	8		配置管理
9		密码管理	9		密码管理
10		变更管理	10		变更管理
11		备份与恢复管理	11		备份与恢复管理
12		安全事件处置	12		安全事件处置
13		应急预案管理	13		应急预案管理
			14		外包运维管理

安全运维管理

1. 环境管理：专人或专门部门负责机房安全管理，机房进出与运维管理；制定**机房安全管理制度**；含敏感信息介质和文档不随意放置；**对出入人员按级别授权，重要区域实时监控。**
2. 资产管理：资产清单(责任部门、重要程度、位置等)；**资产标识管理；规定信息分类并标识方法，对信息的使用、传输和存储进行规范化管理。**
3. 介质管理：安全存放，环境专人管理，定期盘点；介质流转控制并记录。
4. 设备维护管理：专人维护；包括配套设施与软硬件的维护，建立维护制度，明确责任，审批监督；**设备外出要审批，有存储介质的设备带出时重要数据加密；有存储介质的设备报废或重用前先彻底清除信息。**
5. 漏洞与风险管理：识别，及时修补或评估后修补；**定期测评，形成报告，采取措施应对。**
6. 网络和系统安全管理：区分网络与系统运维，专人账户管理；建立网络和系统安全管理制度(策略、账户、口令、配置、日志、操作、补丁等)；制定重要设备配置与操作手册，进行安全配置；记录运维日志；**专人或部门分析日志与监控数据；严控变更性运维，操作中保留日志，同步更新配置库；严格运维工具使用，保留日志，及时删除敏感信息；严控远程运维通道开通，审批后开通，保留日志，及时关闭；外部连接均要授权和审批，定期检查违规无线上网。**
7. 恶意代码防范管理：外来接入要先查杀病毒；规定恶意代码防范要求；检查病毒库升级，并分析捕获样本；**定期验证防病毒技术措施的有效性。**
8. 配置管理：记录基本信息(拓扑、组件、版本、补丁、配置参数)；**基本配置信息的变更管理。**
9. 密码管理：合规的算法与产品；**采用密码模块加解密与密钥管理。**
10. 变更管理：明确变更需求，制定变更方案，评审后实施；**建立变更审批流程，记录变更实施过程；制定变更失败回退流程，必要时进行演练。**
11. 备份与恢复管理：识别需备份的重要业务信息、系统数据与软件；规定备份方式、介质、频率等；制定备份策略和恢复策略和程序。
12. 安全事件处置：及时报告安全事件；制定安全事件报告与处置管理制度；分析原因，总结教训；**对重大服务中断与信息泄露事件有不同的处理流程与报告程序；建立联合防护和应急机制，处置跨单位安全事件。**
13. 应急预案管理：**制定统一的应急预案框架**；重要事件制定应急预案(处理与恢复流程)；定期人员培训与演练；**定期对应急预案重新评估，修订完善；建立重大安全事件的跨单位联合应急预案，并进行演练。**
14. 外包运维管理：选择合规外包服务商，签订协议，明确范围；**协议中明确要求服务商符合等保运维能力，明确安全能力(如基础设施故障的应急保障，敏感信息保护等)。**

等保2.0变化点

1、将等保1.0中“监控管理和安全管理中心”控制点删除，部分内容合并至等保2.0的“网络和系统安全管理”控制点中。

2、在等保2.0中增加“漏洞和风险管理”控制点，将等保1.0中“网络安全管理”和“系统安全管理”中的相关内容纳入其中。

3、将等保1.0中的“网络安全管理”和“系统安全管理”的内容整合合并。

4、增加“配置管理”控制点，说明对系统基本信息的管理要求。

4、对于4级系统要求采用密码模块进行加密解密。

5、删除对涉密事件处置的相关描述。

6、对应急预案要求为定期培训和演练，四级系统要求建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练。

7、等保2.0增加“外部运维管理”控制点，对外部方运维管理能力和工作责任的要求。

《基本要求》——扩展要求
主要内容解读

云计算安全扩展要求—云计算平台组成

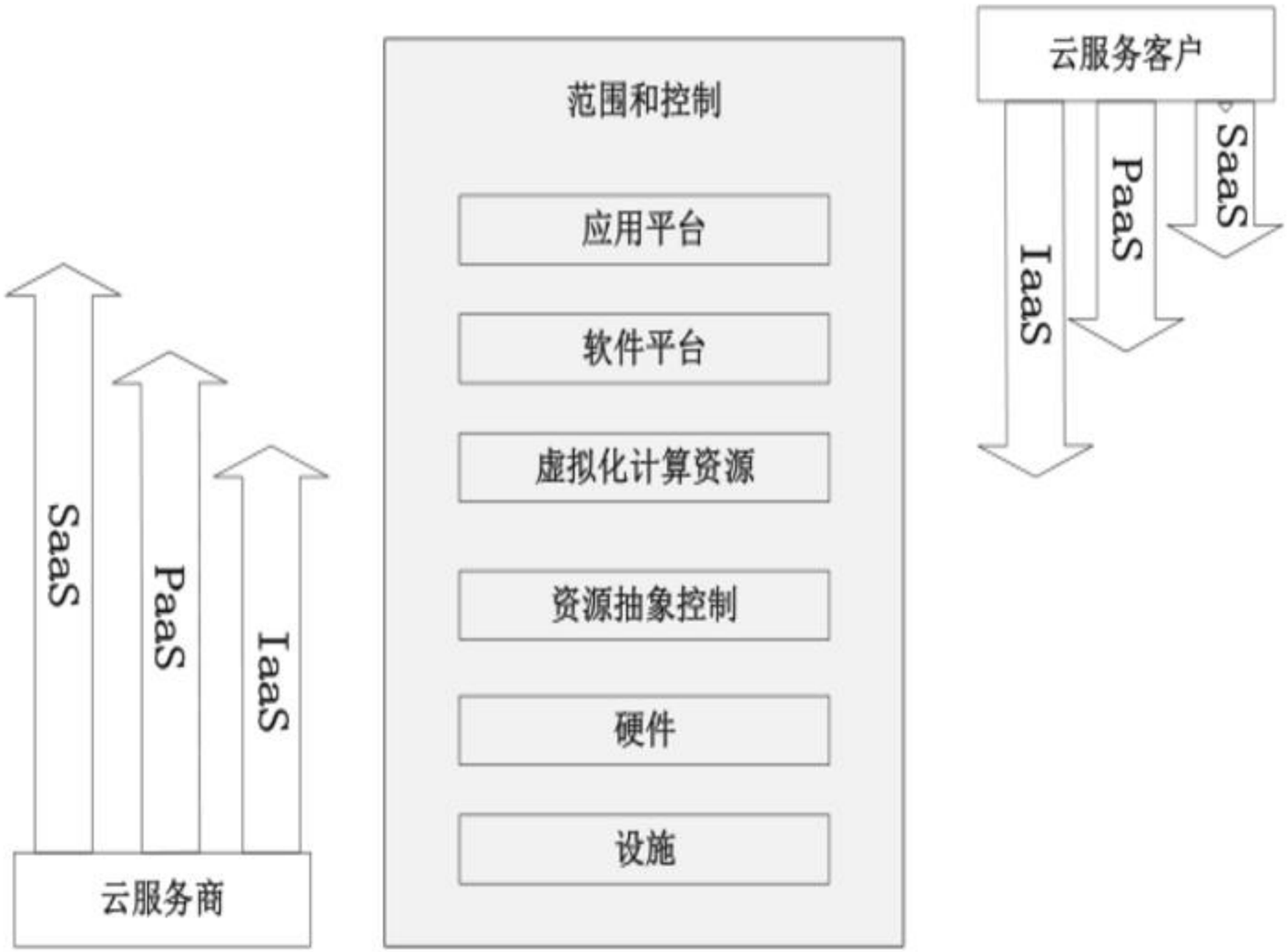


图 云计算服务模式与控制范围的关系

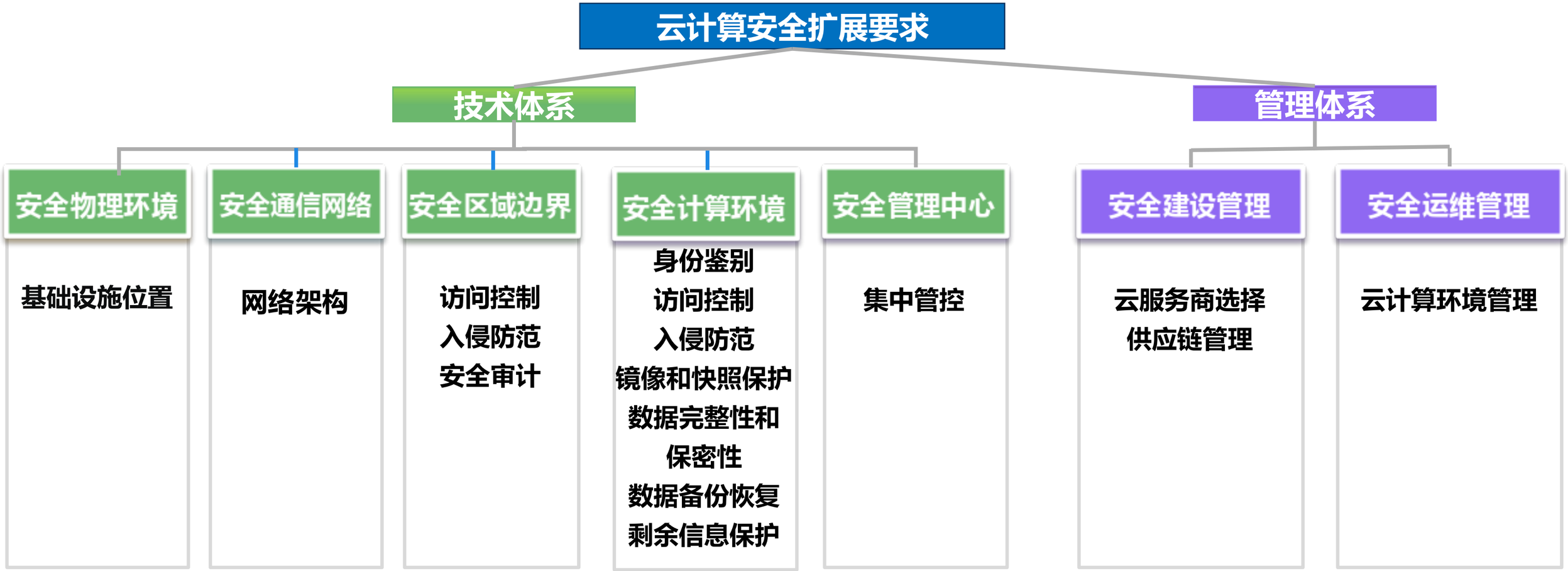
- 将采用了云计算技术的信息系统，称为云计算平台/系统。
- 云计算平台/系统由设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成。
- 软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）是三种基本的云计算服务模式。
- 不同服务模式下云服务商和云服务客户的安全管理责任有所不同。

云计算安全扩展要求—IaaS模式下的责任划分

表 IaaS模式下云服务商与租户的责任划分

层面	安全要求	安全组件	责任主体
安全物理环境	物理位置选择	数据中心、机房及物理设施、办公场地、云计算平台及管理平台等软硬件设施	云服务商
安全通信网络	网络架构	综合网管系统、云管理平台、云平台边界安全设备、开放性安全接口和安全服务、网络资源隔离措施	云服务商
		云服务客户网络安全策略	云服务客户
安全区域边界	访问控制、入侵防范、安全审计	物理网络及附属设备、虚拟网络管理平台	云服务商
		云服务客户虚拟网络设备、虚拟安全设备、虚拟机等	云服务客户
安全计算环境	身份鉴别、访问控制、入侵防范、镜像和快照保护、数据完整性和保密性、数据备份恢复、剩余信息保护	云管理平台（含运维和运营）、镜像、快照等	云服务商
		云服务客户虚拟网络设备、虚拟安全设备、虚拟机等、云服务客户应用系统及相关软件组件、云服务客户应用系统配置、云服务客户业务相关数据等	云服务客户
安全管理中心	集中管控	资源调度平台、云管理平台、综合审计系统或相关组件（云服务商集中审计）	云服务商
		综合审计系统（云服务客户集中审计）	云服务客户
安全建设管理	云服务商选择、供应链管理	供应链管理流程、安全事件和重要变更信息	云服务商
		云服务商选择及管理流程	云服务客户
安全运维管理	云计算环境管理	运维设备、运维地点、运维记录	云服务商

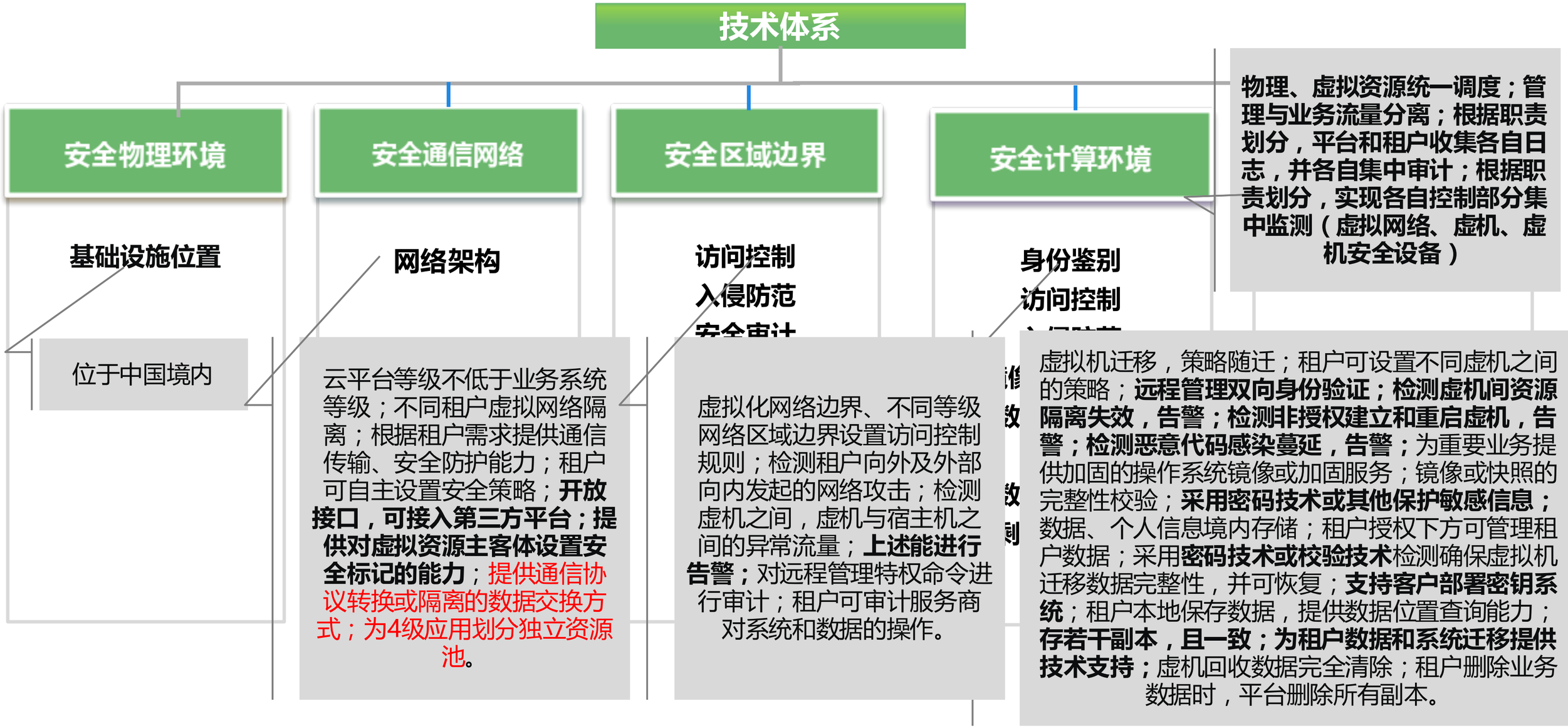
云计算安全扩展要求—控制点及测评要点



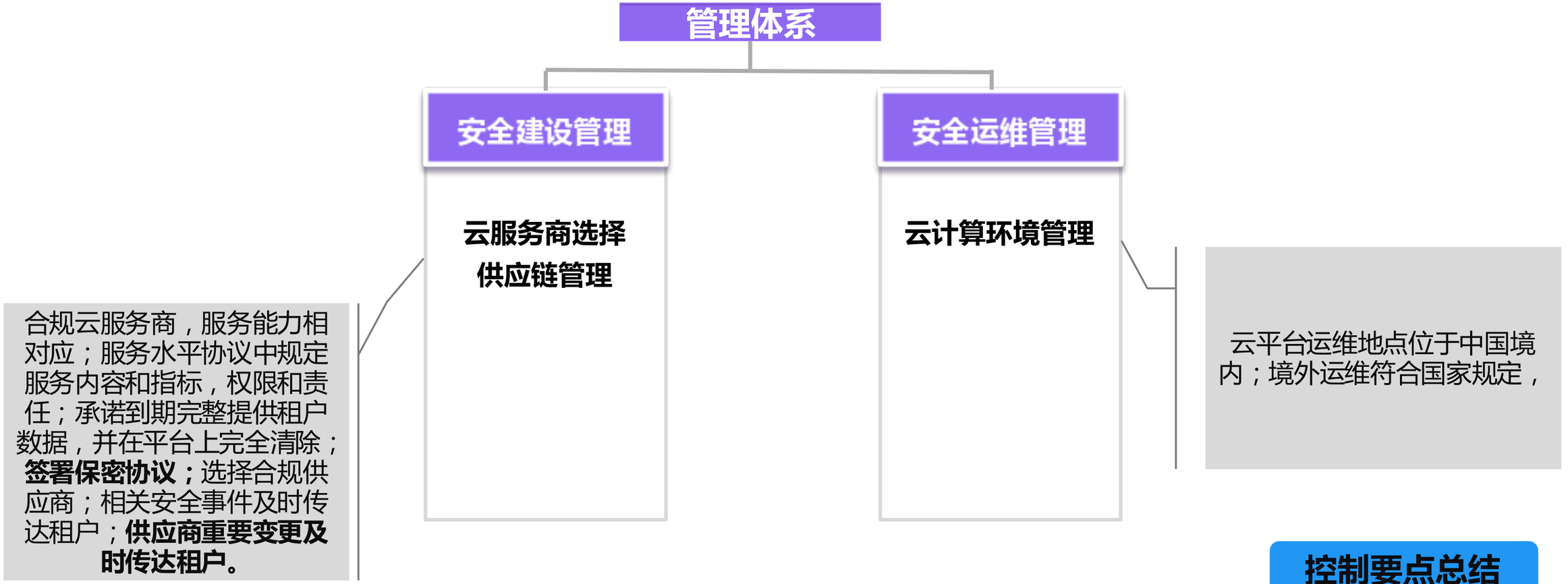
云计算测评要求

- 责任主体一分为二：云服务商、云服务客户均需独立定级备案、过等保测评；
- 国家关键信息基础设施（重要云计算平台）的安全保护等级应不低于第三级；
- 云平台其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级；
- 对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象

云计算安全扩展要求—技术要求



云计算安全扩展要求—管理要求



控制要点总结

- 强调平台与租户的责任界面
- 强调云平台的安全能力，SLA
- 强调平台与租户间，租户与租户间安全隔离
- 强调租户数据和信息的安全

移动互联安全扩展要求—移动互联系统组成

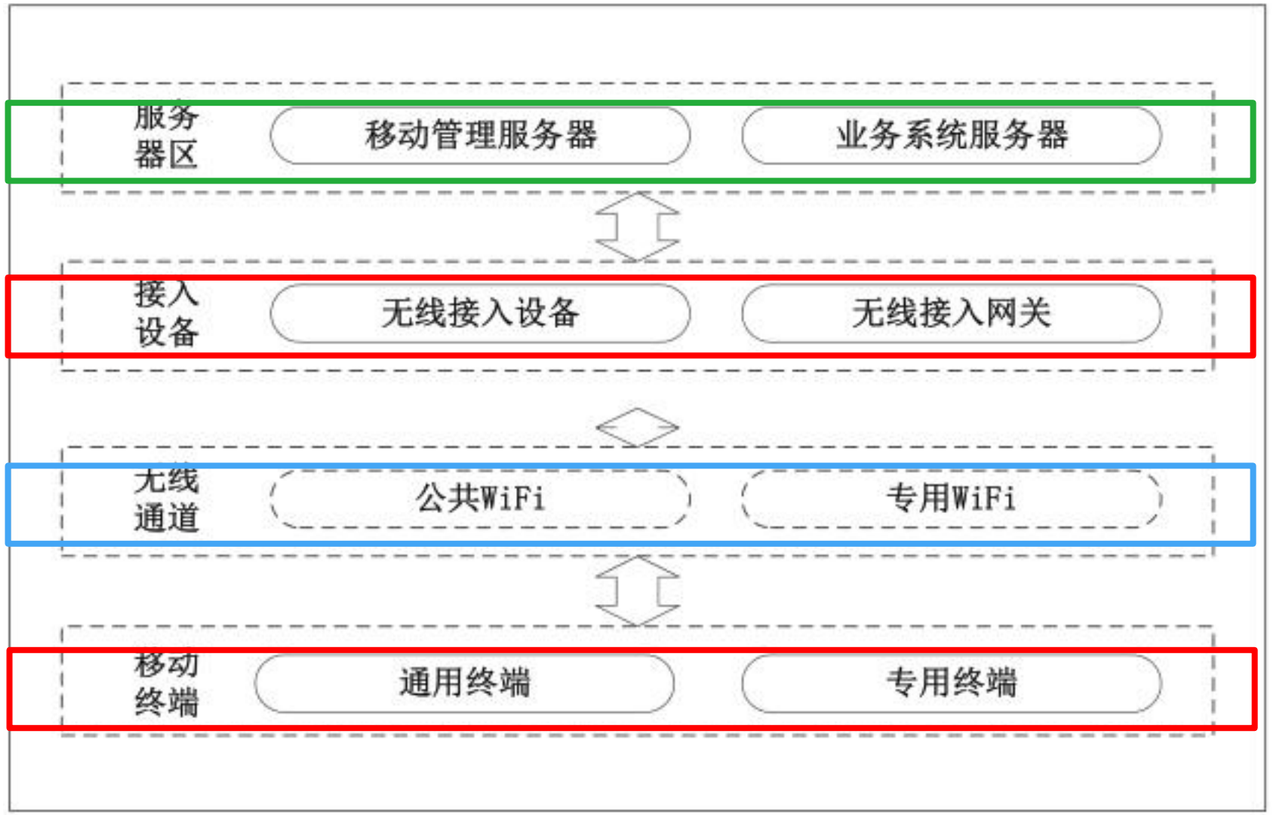


图　移动互联应用架构

使用通用测评要求

使用通用测评要求+扩展要求

运营商网络

使用通用测评要求+扩展要求

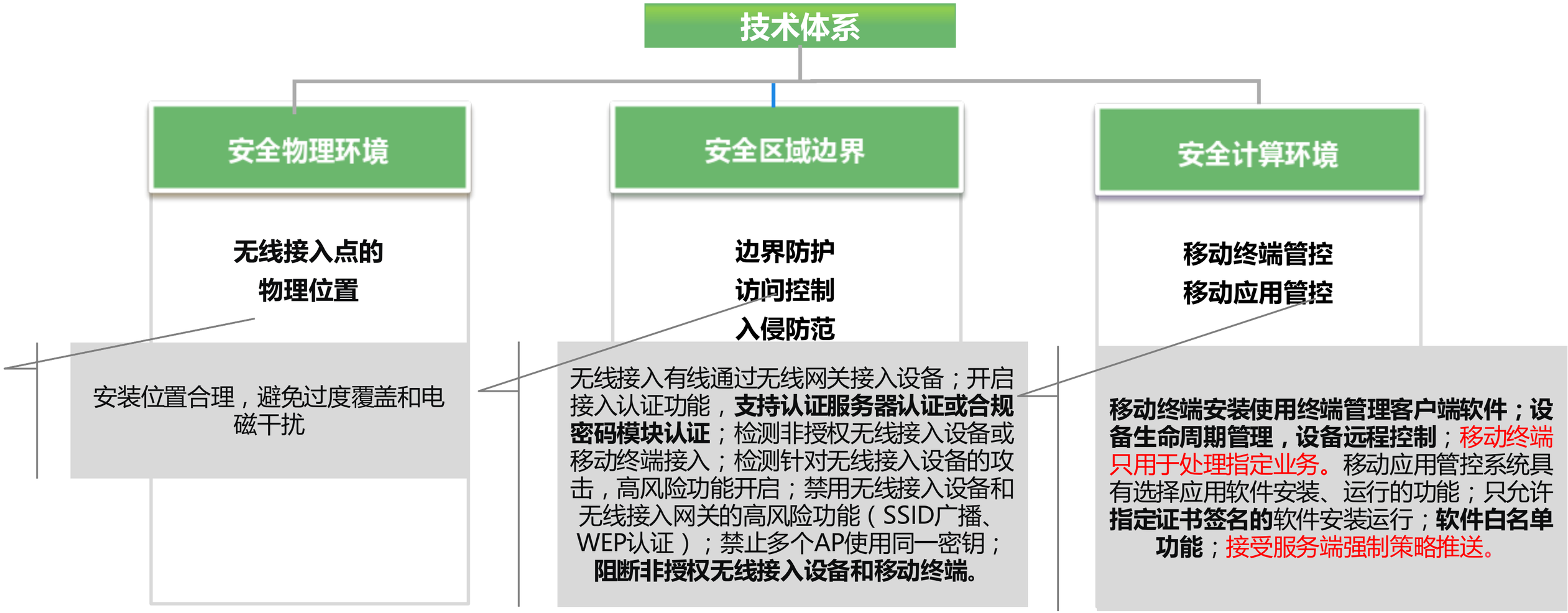
- 移动互联技术的等级保护对象其移动互联部分由移动终端、移动应用和无线网络三部分组成。
- 移动终端通过无线通道连接无线接入设备接入，无线接入网关通过访问控制策略限制移动终端的访问行为，后台的移动终端管理系统负责对移动终端的管理，包括向客户端软件发送移动设备管理、移动应用管理和移动内容管理策略等。

移动互联安全扩展要求—控制点及测评要点

移动互联安全测评要求

- 采用移动互联技术的等级保护对象其移动互联部分由移动终端、移动应用和无线网络三部分组成；采用移动互联技术的等级保护对象应作为一个整体对象定级，移动终端、移动应用和无线网络等要素不单独定级。
- 移动互联安全扩展要求主要针对移动终端、移动应用和无线网络部分提出特殊安全要求，与安全通用要求一起构成对采用移动互联技术的等级保护对象的完整安全要求，测评时需要和移动平台应用系统结合完成等级测评。

移动互联安全扩展要求—技术要求



移动互联安全扩展要求—管理要求

控制要点总结

- 强调对无线接入网关和无线接入设备的安全控制
- 移动终端管控（MDM）
- 移动应用APP管控（分发渠道、白名单、策略）
- 无线通信认证、加密

工控系统安全扩展要求—工控系统组成

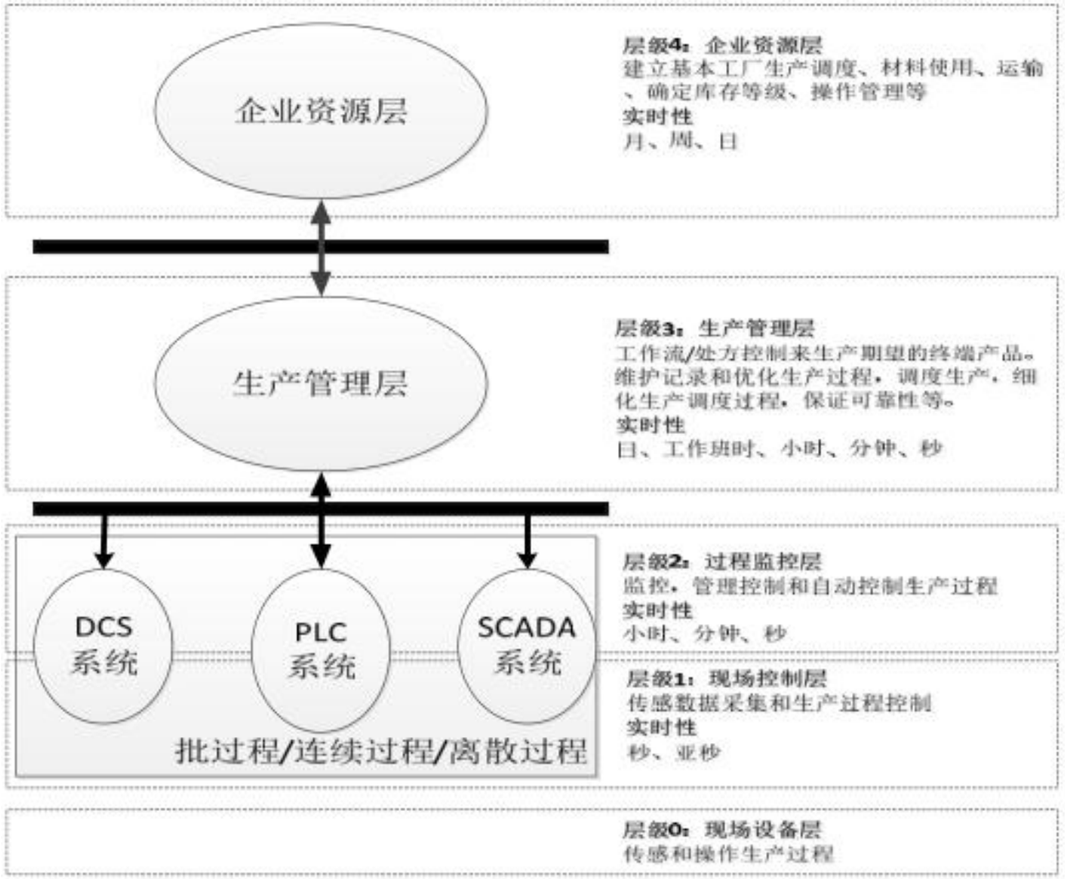


图 典型工控系统功能层次模型（IEC 62264-1）

工业控制系统从上到下共分为5个层级，依次为企业资源层、生产管理层、过程监控层、现场控制层和现场设备层，不同层级的实时性要求不同。

- ✓ 企业资源层主要包括ERP系统功能单元，用于为企业决策层员工提供决策运行手段；
- ✓ 生产管理层主要包括MES系统功能单元，用于对生产过程进行管理，如制造数据管理、生产调度管理等；
- ✓ 过程监控层主要包括监控服务器与HMI系统功能单元，用于对生产过程数据进行采集与监控，并利用HMI系统实现人机交互；
- ✓ 现场控制层主要包括各类控制器单元，如PLC、DCS控制单元等，用于对各执行设备进行控制；
- ✓ 现场设备层主要包括各类过程传感设备与执行设备单元，用于对生产过程进行感知与操作。

工控系统安全扩展要求—工控系统层次与基本要求的映射关系

功能层次	技术要求
企业资源层	安全通用要求（安全物理环境）
	安全通用要求（安全通信网络）
	安全通用要求（安全区域边界）
	安全通用要求（安全计算环境）
	安全通用要求（安全管理中心）
生产管理层	安全通用要求（安全物理环境）
	安全通用要求（安全通信网络）+安全扩展要求（安全通信网络）
	安全通用要求（安全区域边界）+安全扩展要求（安全区域边界）
	安全通用要求（安全计算环境）
	安全通用要求（安全管理中心）

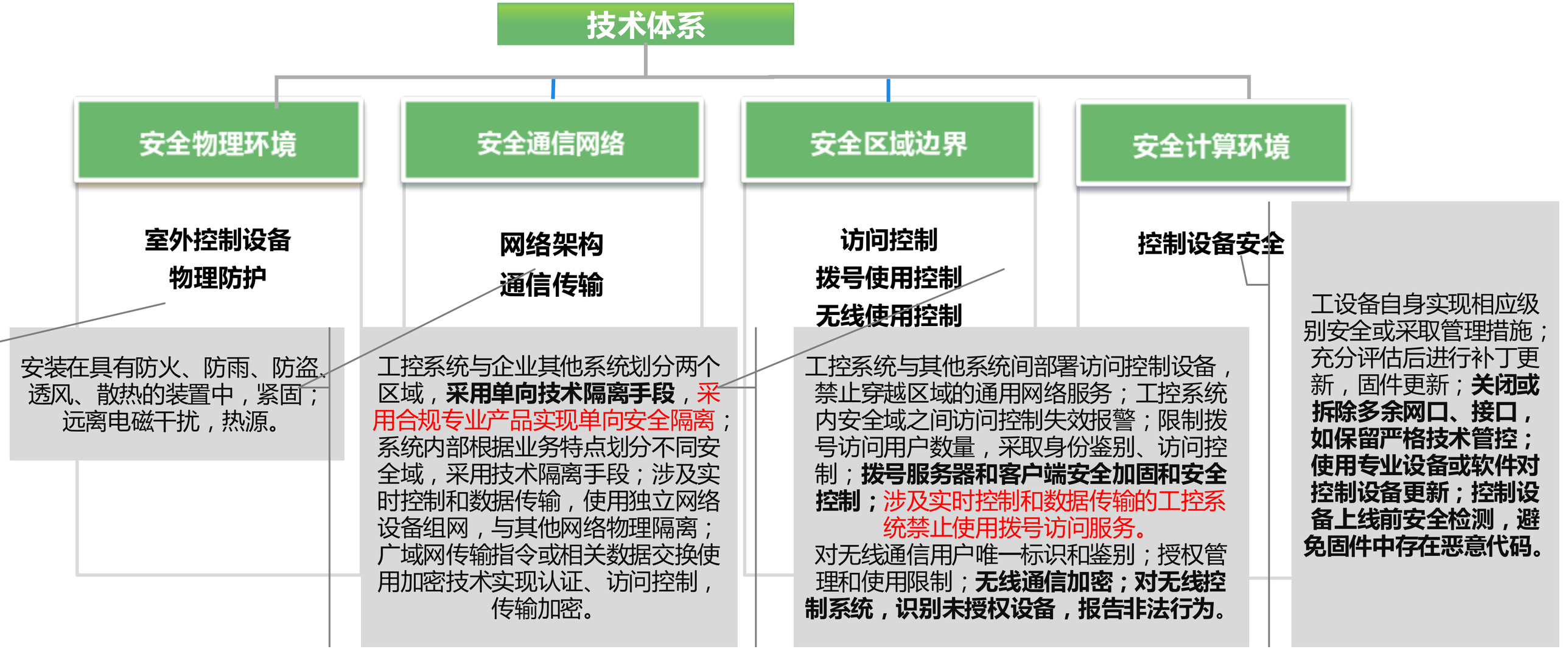
功能层次	技术要求
过程监控层	安全通用要求（安全物理环境）
	安全通用要求（安全通信网络）+安全扩展要求（安全通信网络）
	安全通用要求（安全区域边界）+安全扩展要求（安全区域边界）
	安全通用要求（安全计算环境）
	安全通用要求（安全管理中心）
现场控制层	安全通用要求（安全物理环境）+安全扩展要求（安全物理环境）
	安全通用要求（安全通信网络）+安全扩展要求（安全通信网络）
	安全通用要求（安全区域边界）+安全扩展要求（安全区域边界）
	安全通用要求（安全计算环境）+安全扩展要求（安全计算环境）
现场设备	安全通用要求（安全物理环境）+安全扩展要求（安全物理环境）
	安全通用要求（安全通信网络）+安全扩展要求（安全通信网络）
	安全通用要求（安全区域边界）+安全扩展要求（安全区域边界）

工控系统安全扩展要求—控制点和测评要点

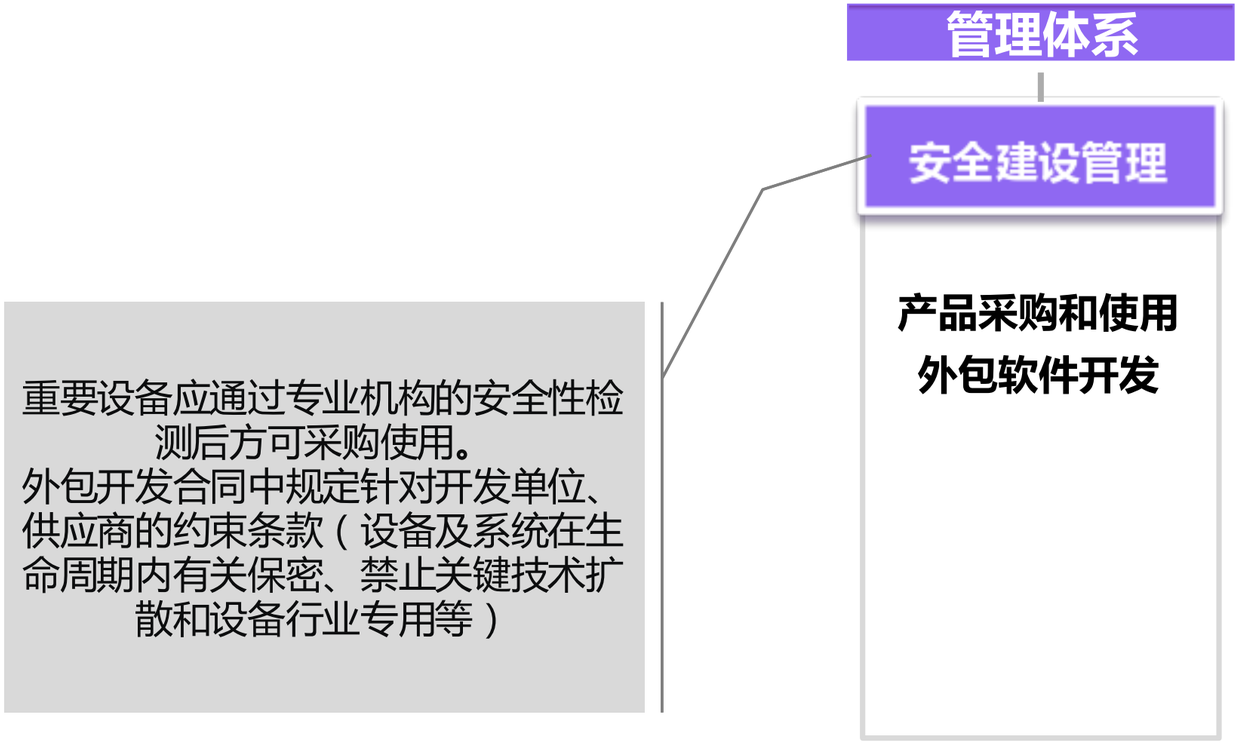
工业控制系统测评要求

- 高度关注可用性，工业控制系统中的一些装置如果实现特定类型的安全措施可能会终止其连续运行，原则上安全措施不应对高可用性的工业控制系统基本功能产生不利影响。
- 安全措施的部署不应显著增加延迟而影响系统响应时间；对于高可用性的控制系统，安全措施失效不应中断基本功能。
- 经评估对可用性有较大影响而无法实施和落实安全等级保护要求的相关条款时，应进行安全声明，分析和说明此条款实施可能产生的影响和后果，以及使用的补偿措施。

工控系统安全扩展要求—技术要求



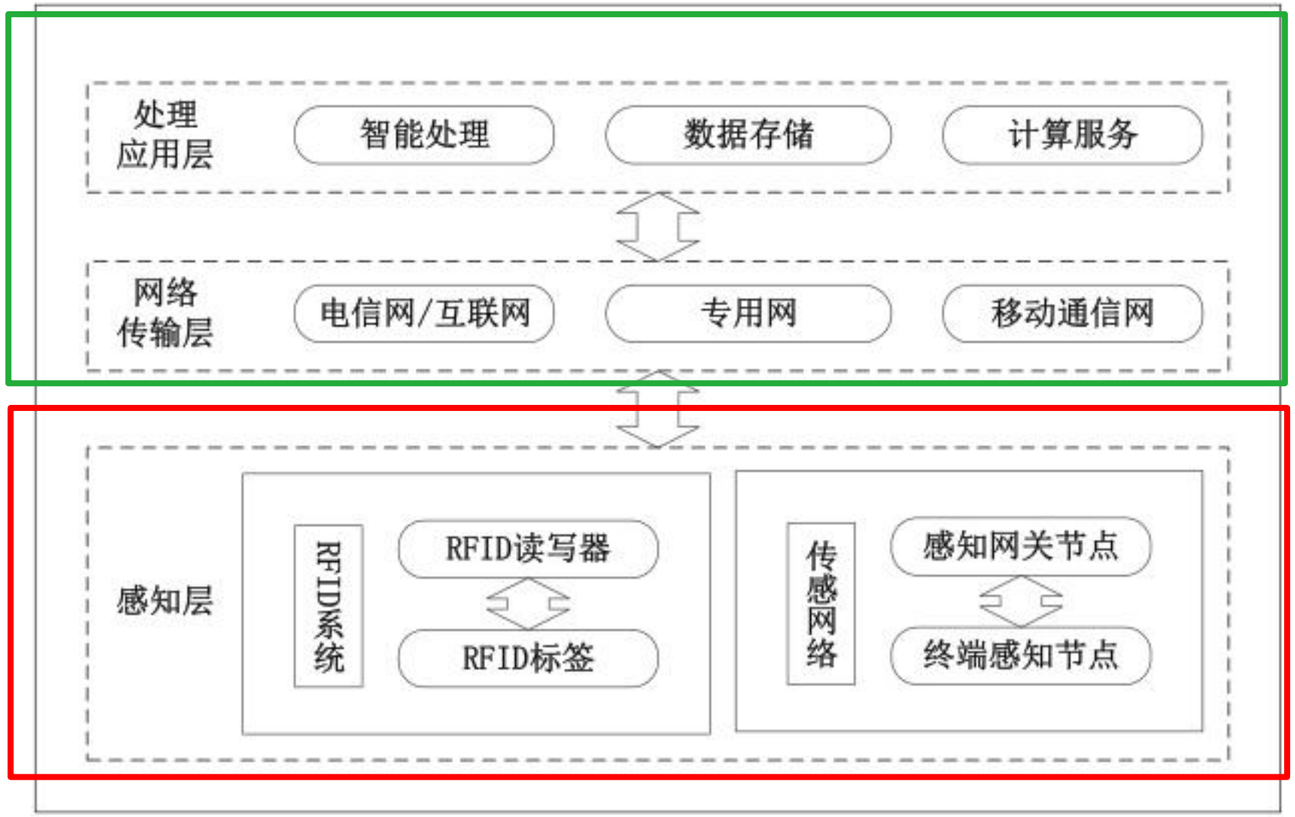
工控系统安全扩展要求—管理要求



控制要点总结

- 强调安全域划分，对边界安全防护能力要求高；
- 对不同功能层级安全控制侧重点不同
- 关注控制设备的高可用性，高可靠性

物联网安全扩展要求—物联网构成



使用通用测评要求

使用通用测评要求+扩展要求

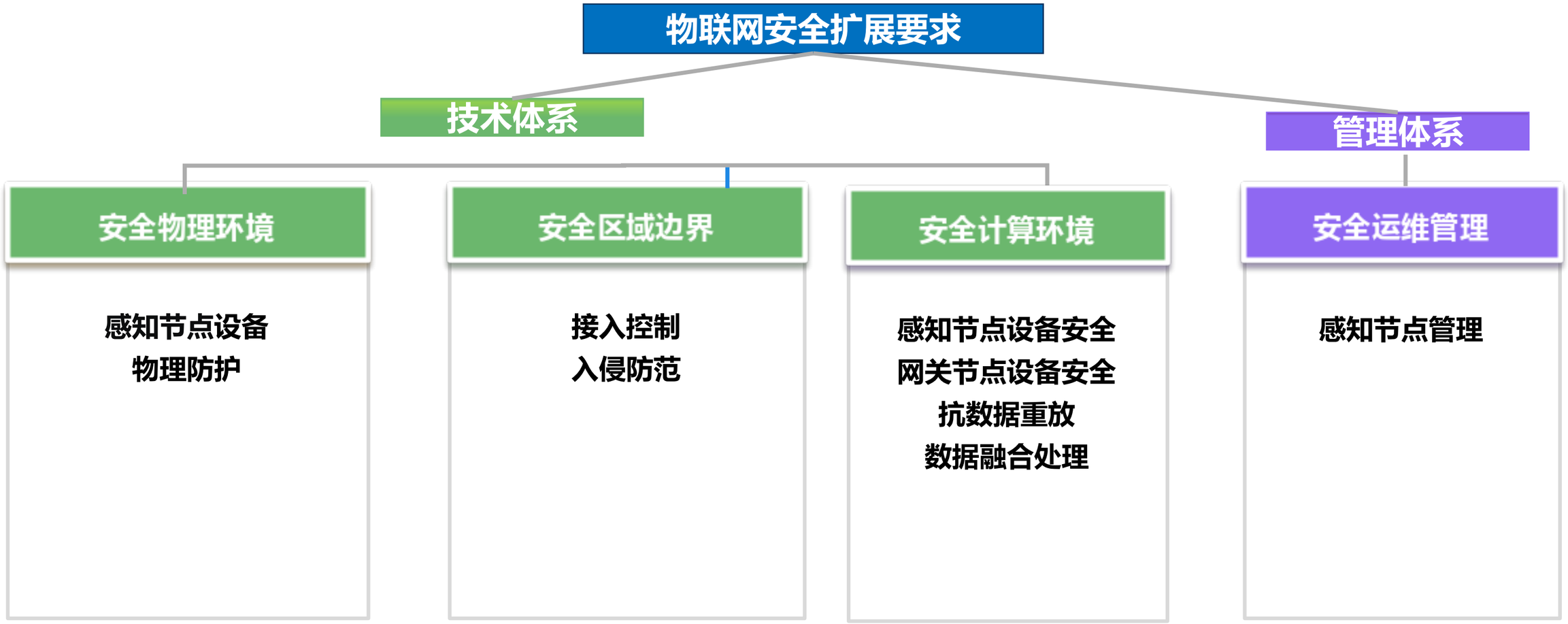
图 物联网构成

物联网通常从架构上可分为三个逻辑层，即感知层、网络传输层和处理应用层。

- ✓ 感知层包括传感器节点和传感网网关节点，或RFID标签和RFID读写器，也包括这些感知设备及传感网网关、RFID标签与阅读器之间的短距离通信（通常为无线）部分；
- ✓ 网络传输层包括将这些感知数据远距离传输到处理中心的网络，包括互联网、移动网等，以及几种不同网络的融合；
- ✓ 处理应用层包括对感知数据进行存储与智能处理的平台，并对业务应用终端提供服务。

对物联网的安全防护应包括感知层、网络传输层和处理应用层，由于网络传输层和处理应用层通常是由计算机设备构成，因此这两部分按照安全通用要求提出的要求进行保护。

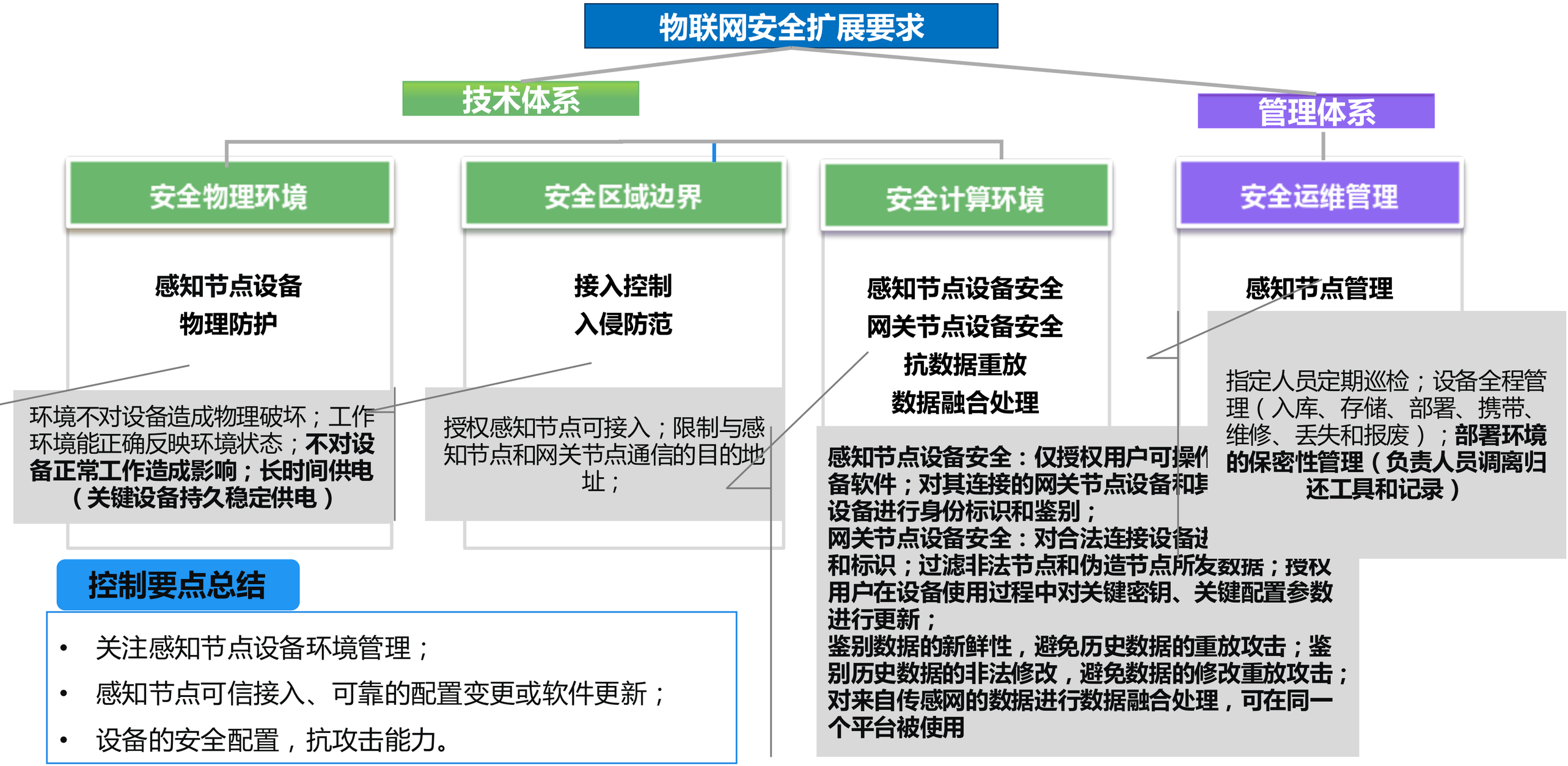
物联网安全扩展要求—控制点和测评要点



物联网测评要求

- 测评以感知节点设备、网关节点设备（包括读卡器）、传感网、入网访问控制设备等为主。
- 重点在于对物联网系统安全技术方面的测评，尤其需要加强测试验证的技术测评手段。
- 测试工具除了传统系统测评的工具外，还需采用感知层产品安全评估的专用工具。

物联网安全扩展要求—技术要求和管理要求



控制要点总结

- 关注感知节点设备环境管理；
- 感知节点可信接入、可靠的配置变更或软件更新；
- 设备的安全配置，抗攻击能力。

大数据安全扩展要求—大数据系统构成

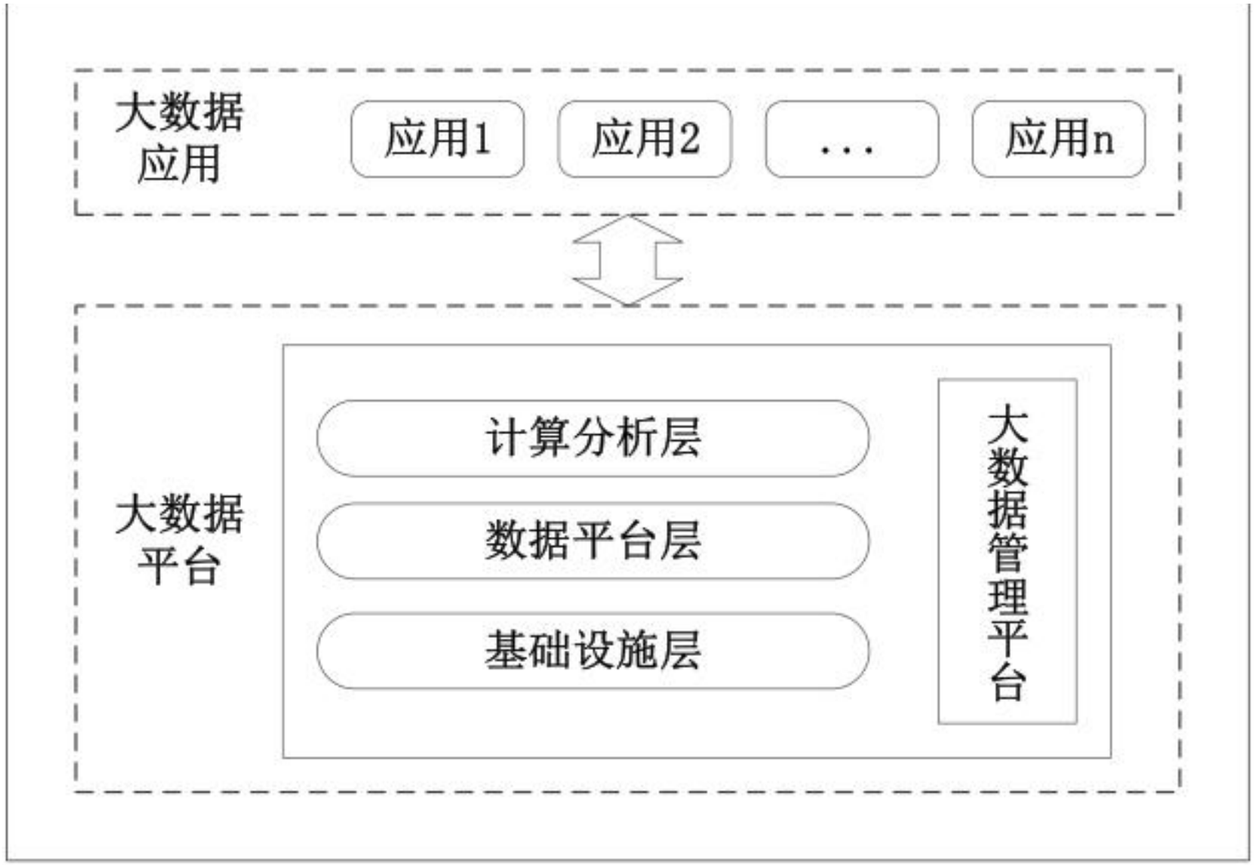


图　大数据系统构成

- 大数据系统的特征是数据体量大、种类多、聚合快、价值高，受到破坏、泄露或篡改会对国家安全、社会秩序或公共利益造成影响。
- 大数据系统通常由大数据平台、大数据应用以及处理的数据集合构成。大数据安全涉及大数据平台的安全和大数据应用的安全。
- 大数据平台是为大数据应用提供资源和服务的支撑集成环境，包括基础设施层、数据平台层和计算分析层。
- 大数据应用是基于大数据平台对数据的处理过程，通常包括数据采集、数据存储、数据应用、数据交换和数据销毁等环节，上述各个环节均需要对数据进行保护，通常需考虑的安全控制措施包括数据采集授权、数据真实可信、数据分类标识存储、数据交换完整性、敏感数据保密性、数据备份和恢复、数据输出脱敏处理、敏感数据输出控制以及数据的分级分类销毁机制等。

大数据安全扩展要求—技术要求

技术体系

安全物理环境

保证承载大数据存储、处理和分析的设备机房位于中国境内

安全通信网络

大数据平台不承载高于其安全保护等级的大数据应用；
大数据平台的管理流量与系统业务流量分离。

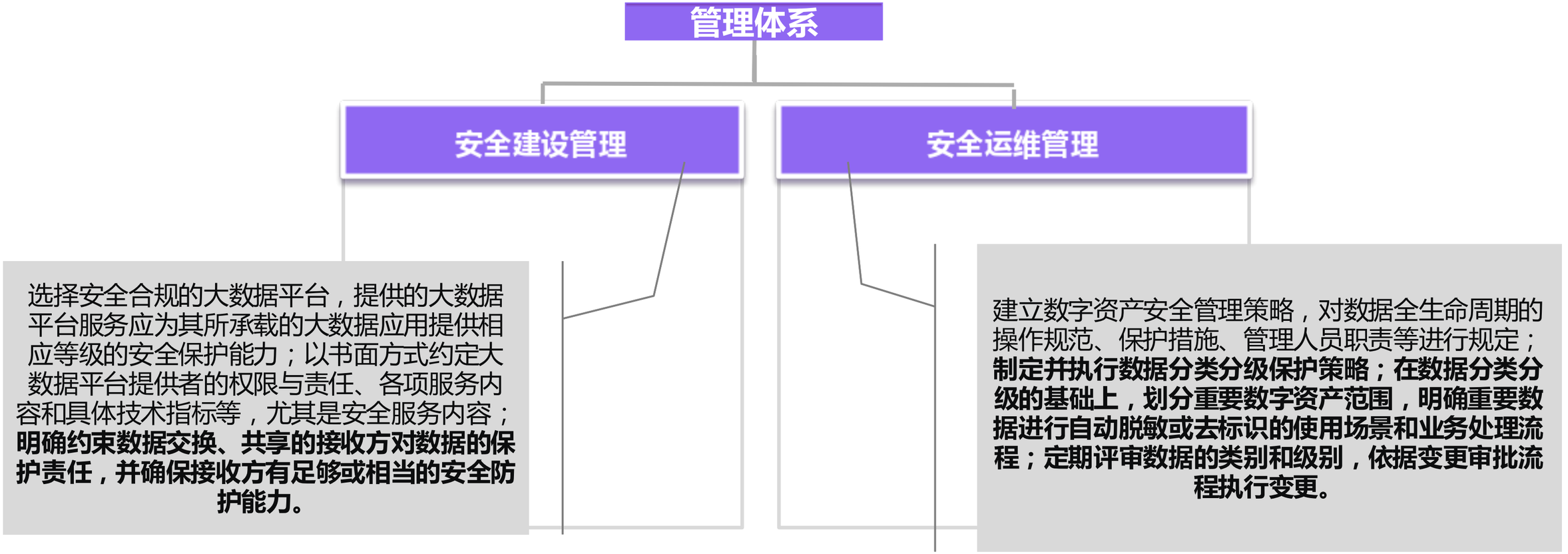
安全计算环境

能对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；能对不同客户的大数据应用实施标识和鉴别；为大数据应用提供集中管控其计算和存储资源使用状况的能力；对其提供的辅助工具或服务组件，实施有效管理；屏蔽计算、内存、存储资源故障，保障业务正常运行；提供静态脱敏和去标识化的工具或服务组件技术；平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；**提供数据分类分级安全管理功能；提供设置数据安全标记功能，基于安全标记的授权和访问控制措施；在数据采集、存储、处理、分析等各个环节，支持对数据进行分类分级处置，并保证安全保护策略保持一致；涉及重要数据接口、重要服务接口的调用，应实施访问控制；在数据清洗和转换过程中对重要数据进行保护,以保证重要数据清洗和转换后的一致性，并在产生问题时能有效还原和恢复；跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程，溯源数据满足合规审计要求；保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；大数据平台应具备对不同类别、不同级别数据全生命周期区分处置的能力。**

控制要点总结

- 能够支撑数据全生命周期安全
- 大数据平台要求提供相应管理能力
- 三级要求数据分类分级、安全标记功能
- 关注重要数据的完整性、保密性保护
- 数据处理过程可溯源、可审计

大数据安全扩展要求—管理要求



大数据测评要求

- 组件（大数据、大数据应用、大数据平台、基础设施）单独或组合可以构成定级对象，当涉及不同责任主体时，应当分别定级 ；当安全责任主体相同，大数据、大数据平台和应用可作为一个整体对象定级。
- 如果大数据基础设施、大数据平台、大数据应用为不同的定级对象，下层定级对象的安全保护等级应不低于其承载的上层定级对象的等级。
- 测评关注业务数据生命周期流程及相关控制措施，关注个人敏感信息、出境数据、溯源数据。

新等保、新体系

■ **应对新威胁**

新等保更加强调增强未知威胁检测能力，强调安全检测能力和安全响应能力的建设。

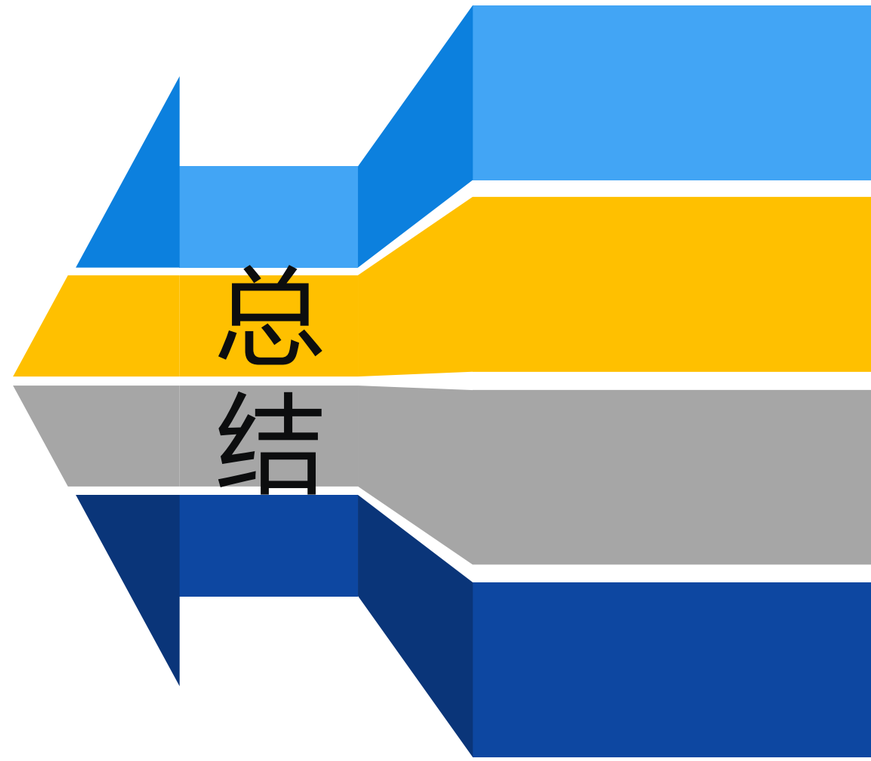
■ **应对新风险**

新等保体系更体现了动态的、积极防御的安全理念；安全规划、能力建设、态势感知、集中监控管理成为新等保体系的重要思想。

■ **应对新技术**

针对云计算、大数据、物联网等新技术，不断扩大等级保护外延，新的信息技术同样催生新的安全技术。

等保2.0的核心变化



Thank you!