附 录 A
（规范性附录）
关于安全通用要求和安全扩展要求的选择和使用

由于等级保护对象承载的业务不同，对其的安全关注点会有所不同，有的更关注信息的安全性，即更关注对搭线窃听、假冒用户等可能导致信息泄密、非法篡改等；有的更关注业务的连续性，即更关注保证系统连续正常的运行，免受对系统未授权的修改、破坏而导致系统不可用引起业务中断。

不同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求是有差异的，即使相同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求也有差异。

等级保护对象定级后，可能形成的定级结果组合见表 A.1。

表 A.1 等级保护对象定级结果组合

安全保护等级	定级结果的组合
第一级	S1A1
第二级	S1A2，S2A2，S2A1
第三级	S1A3，S2A3，S3A3，S3A2，S3A1
第四级	S1A4，S2A4，S3A4，S4A4，S4A3，S4A2，S4A1
第五级	S1A5，S2A5，S3A5，S4A5，S5A4，S5A3，S5A2，S5A1

安全保护措施的选择应依据上述定级结果，本标准中的技术安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为 S）；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 A）；其他安全保护类要求（简记为 G）。本标准中所有安全管理要求和安全扩展要求均标注为 G，安全要求及属性标识见表 A.2。

表 A.2 安全要求及属性标识

技术/管理	分类	安全控制点	属性标识
安全技术要求	安全物理环境	物理位置选择	G
		物理访问控制	G
		防盗窃和防破坏	G
		防雷击	G
		防火	G
		防水和防潮	G
		防静电	G
		温湿度控制	G
		电力供应	A
		电磁防护	S

表 A.2（续）

技术/管理	分类	安全控制点	属性标识
安全技术要求	安全通信网络	网络架构	G
		通信传输	G
		可信验证	S
	安全区域边界	边界防护	G
		访问控制	G
		入侵防范	G
		可信验证	S
		恶意代码防范	G
		安全审计	G
	安全计算环境	身份鉴别	S
		访问控制	S
		安全审计	G
		可信验证	S
		入侵防范	G
		恶意代码防范	G
		数据完整性	S
		数据保密性	S
		数据备份恢复	A
		剩余信息保护	S
		个人信息保护	S
	安全管理中心	系统管理	G
		审计管理	G
		安全管理	G
		集中管控	G
安全管理要求	安全管理制度	安全策略	G
		管理制度	G
		制定和发布	G
		评审和修订	G
	安全管理机构	岗位设置	G
		人员配备	G
		授权和审批	G
		沟通和合作	G
		审核和检查	G

表 A.2（续）

技术/管理	分类	安全控制点	属性标识
安全管理要求	安全管理人员	人员录用	G
		人员离岗	G
		安全意识教育和培训	G
		外部人员访问管理	G
	安全建设管理	定级和备案	G
		安全方案设计	G
		产品采购和使用	G
		自行软件开发	G
		外包软件开发	G
		工程实施	G
		测试验收	G
		系统交付	G
		等级测评	G
		服务供应商管理	G
	安全运维管理	环境管理	G
		资产管理	G
		介质管理	G
		设备维护管理	G
		漏洞和风险管理	G
		网络与系统安全管理	G
		恶意代码防范管理	G
		配置管理	G
		密码管理	G
		变更管理	G
		备份与恢复管理	G
		安全事件处置	G
		应急预案管理	G
		外包运维管理	G

对于确定了级别的等级保护对象，应依据表 A.1 的定级结果，结合表 A.2 使用安全要求，应按照以下过程进行安全要求的选择：

a) 根据等级保护对象的级别选择安全要求。方法是根据本标准，第一级选择第一级安全要求，第二级选择第二级安全要求，第三级选择第三级安全要求，第四级选择第四级安全要求，以此作为出发点。

b) 根据定级结果，基于表 A.1 和表 A.2 对安全要求进行调整。根据系统服务保证性等级选择相

应级别的系统服务保证类(A 类)安全要求;根据业务信息安全性等级选择相应级别的业务信息安全类(S 类)安全要求;根据系统安全等级选择相应级别的安全通用要求(G 类)和安全扩展要求(G 类)。

c) 根据等级保护对象采用新技术和新应用的情况,选用相应级别的安全扩展要求作为补充。采用云计算技术的选用云计算安全扩展要求,采用移动互联技术的选用移动互联安全扩展要求,物联网选用物联网安全扩展要求,工业控制系统选用工业控制系统安全扩展要求。

d) 针对不同行业或不同对象的特点,分析可能在某些方面的特殊安全保护能力要求,选择较高级别的安全要求或其他标准的补充安全要求。对于本标准中提出的安全要求无法实现或有更加有效的安全措施可以替代的,可以对安全要求进行调整,调整的原则是保证不降低整体安全保护能力。

总之,保证不同安全保护等级的对象具有相应级别的安全保护能力,是安全等级保护的核心。选用本标准中提供的安全通用要求和安全扩展要求是保证等级保护对象具备一定安全保护能力的一种途径和出发点,在此出发点的基础上,可以参考等级保护的其他相关标准和安全方面的其他相关标准,调整和补充安全要求,从而实现等级保护对象在满足等级保护安全要求基础上,又具有自身特点的保护。

附 录 B
（规范性附录）
关于等级保护对象整体安全保护能力的要求

网络安全等级保护的核心是保证不同安全保护等级的对象具有相适应的安全保护能力。本标准第5章提出了不同级别的等级保护对象的安全保护能力要求，第6章～第10章分别针对不同安全保护等级的对象应该具有的安全保护能力提出了相应的安全通用要求和安全扩展要求。

依据本标准分层面采取各种安全措施时，还应考虑以下总体性要求，保证等级保护对象的整体安全保护能力。

a） 构建纵深的防御体系

本标准从技术和管理两个方面提出安全要求，在采取由点到面的各种安全措施时，在整体上还应保证各种安全措施的组合从外到内构成一个纵深的安全防御体系，保证等级保护对象整体的安全保护能力。应从通信网络、网络边界、局域网络内部、各种业务应用平台等各个层次落实本标准中提到的各种安全措施，形成纵深防御体系。

b） 采取互补的安全措施

本标准以安全控制的形式提出安全要求，在将各种安全控制落实到特定等级保护对象中时，应考虑各个安全控制之间的互补性，关注各个安全控制在层面内、层面间和功能间产生的连接、交互、依赖、协调、协同等相互关联关系，保证各个安全控制共同综合作用于等级保护对象上，使得等级保护对象的整体安全保护能力得以保证。

c） 保证一致的安全强度

本标准将安全功能要求，如身份鉴别、访问控制、安全审计、入侵防范等内容，分解到等级保护对象的各个层面，在实现各个层面安全功能时，应保证各个层面安全功能实现强度的一致性。应防止某个层面安全功能的减弱导致整体安全保护能力在这个安全功能上削弱。例如，要实现双因子身份鉴别，则应在各个层面的身份鉴别上均实现双因子身份鉴别；要实现基于标记的访问控制，则应保证在各个层面均实现基于标记的访问控制，并保证标记数据在整个等级保护对象内部流动时标记的唯一性等。

d） 建立统一的支撑平台

本标准针对较高级别的等级保护对象，提到了使用密码技术、可信技术等，多数安全功能（如身份鉴别、访问控制、数据完整性、数据保密性等）为了获得更高的强度，均要基于密码技术或可信技术，为了保证等级保护对象的整体安全防护能力，应建立基于密码技术的统一支撑平台，支持高强度身份鉴别、访问控制、数据完整性、数据保密性等安全功能的实现。

e） 进行集中的安全管理

本标准针对较高级别的等级保护对象，提到了实现集中的安全管理、安全监控和安全审计等要求，为了保证分散于各个层面的安全功能在统一策略的指导下实现，各个安全控制在可控情况下发挥各自的作用，应建立集中的管理中心，集中管理等级保护对象中的各个安全控制组件，支持统一安全管理。

附　录　C
（规范性附录）
等级保护安全框架和关键技术使用要求

在开展网络安全等级保护工作中应首先明确等级保护对象，等级保护对象包括通信网络设施、信息系统（包含采用移动互联等技术的系统）、云计算平台/系统、大数据平台/系统、物联网、工业控制系统等；确定了等级保护对象的安全保护等级后，应根据不同对象的安全保护等级完成安全建设或安全整改工作；应针对等级保护对象特点建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系。应依据国家网络安全等级保护政策和标准，开展组织管理、机制建设、安全规划、安全监测、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、安全可控、队伍建设、教育培训和经费保障等工作。等级保护安全框架见图 C.1。

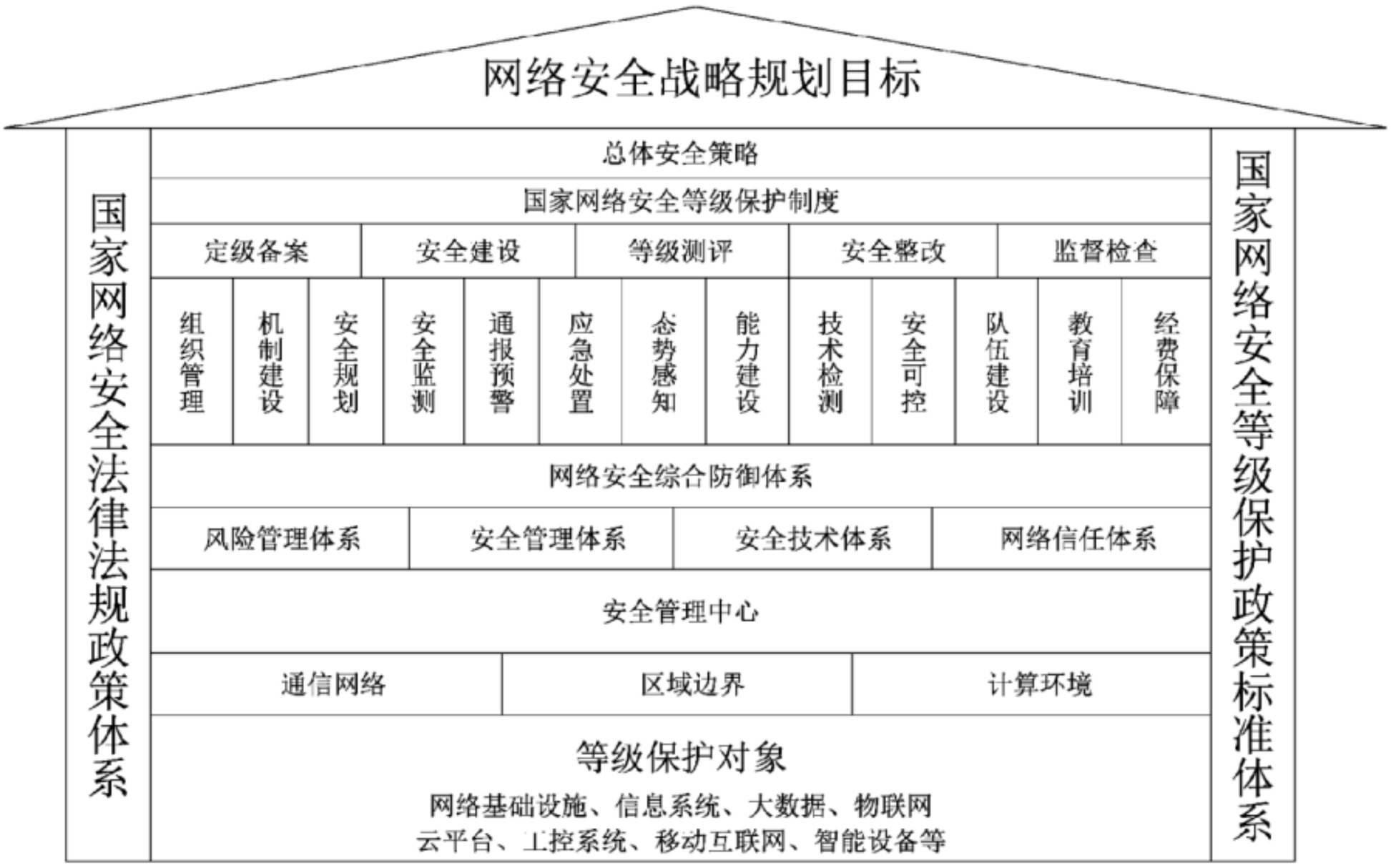


图 C.1　等级保护安全框架

应在较高级别等级保护对象的安全建设和安全整改中注重使用一些关键技术：

a）　可信计算技术

应针对计算资源构建保护环境，以可信计算基（TCB）为基础，实现软硬件计算资源可信；针对信息资源构建业务流程控制链，基于可信计算技术实现访问控制和安全认证，密码操作调用和资源的管理等，构建以可信计算技术为基础的等级保护核心技术体系。

b）　强制访问控制

应在高等级保护对象中使用强制访问控制机制，强制访问控制机制需要总体设计、全局考虑，在通信网络、操作系统、应用系统各个方面实现访问控制标记和策略，进行统一的主客体安全标记，安全标记随数据全程流动，并在不同访问控制点之间实现访问控制策略的关联，构建各

个层面强度一致的访问控制体系。

c) 审计追查技术

应立足于现有的大量事件采集、数据挖掘、智能事件关联和基于业务的运维监控技术，解决海量数据处理瓶颈，通过对审计数据快速提取，满足信息处理中对于检索速度和准确性的需求；同时，还应建立事件分析模型，发现高级安全威胁，并追查威胁路径和定位威胁源头，实现对攻击行为的有效防范和追查。

d) 结构化保护技术

应通过良好的模块结构与层次设计等方法来保证具有相当的抗渗透能力，为安全功能的正常执行提供保障。高等级保护对象的安全功能可以形式表述、不可被篡改、不可被绕转，隐蔽信道不可被利用，通过保障安全功能的正常执行，使系统具备源于自身结构的、主动性的防御能力，利用可信技术实现结构化保护。

e) 多级互联技术

应在保证各等级保护对象自治和安全的前提下，有效控制异构等级保护对象间的安全互操作，从而实现分布式资源的共享和交互。随着对结构网络化和业务应用分布化动态性要求越来越高，多级互联技术应在不破坏原有等级保护对象正常运行和安全的前提下，实现不同级别之间的多级安全互联、互通和数据交换。

附 录 D
（资料性附录）
云计算应用场景说明

本标准中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。如图 D.1 所示，在不同的服务模式中，云服务商和云服务客户对计算资源拥有不同的控制范围，控制范围则决定了安全责任的边界。在基础设施即服务模式下，云计算平台/系统由设施、硬件、资源抽象控制层组成；在平台即服务模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；在软件即服务模式下，云计算平台/系统包括设施、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。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。

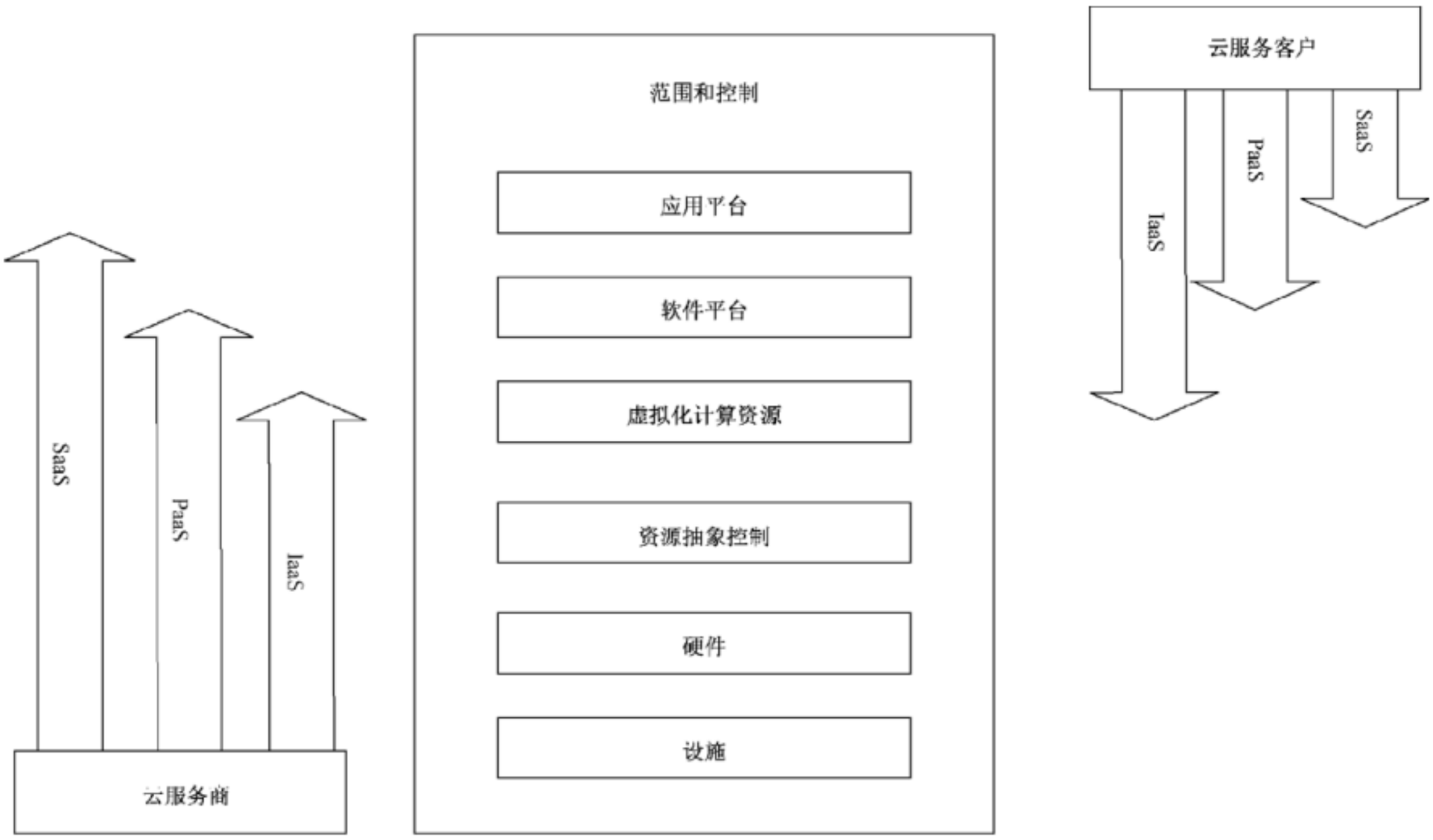


图 D.1 云计算服务模式与控制范围的关系

附 录 E
（资料性附录）
移动互联应用场景说明

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，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，如图 E.1 所示，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。本标准的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。

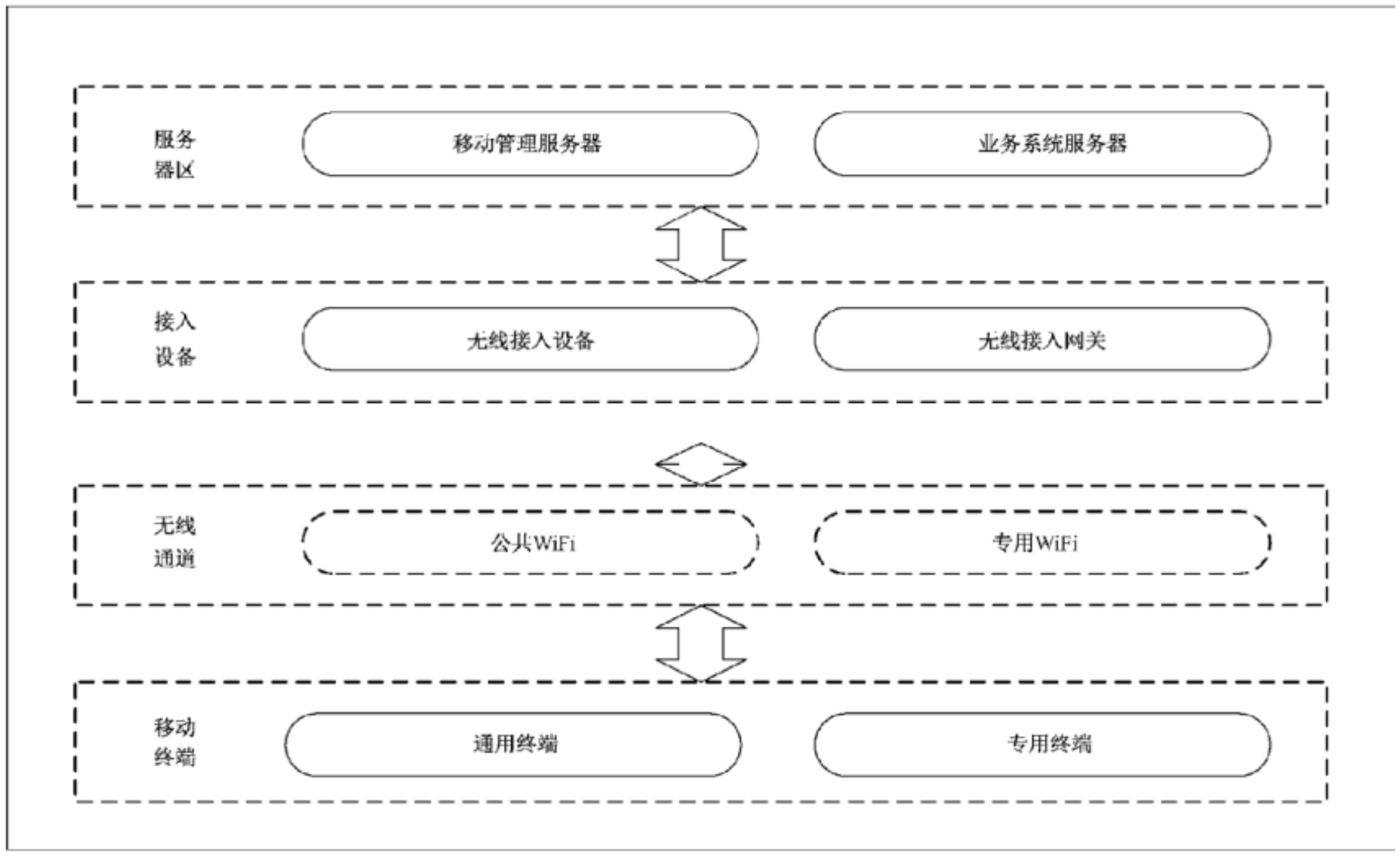


图 E.1 移动互联应用架构

附 录 F
（资料性附录）
物联网应用场景说明

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。其中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。对大型物联网来说，处理应用层一般是云计算平台和业务应用终端设备。物联网构成示意图如图 F.1 所示。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，本标准的物联网安全扩展要求针对感知层提出特殊安全要求，与安全通用要求一起构成对物联网的完整安全要求。

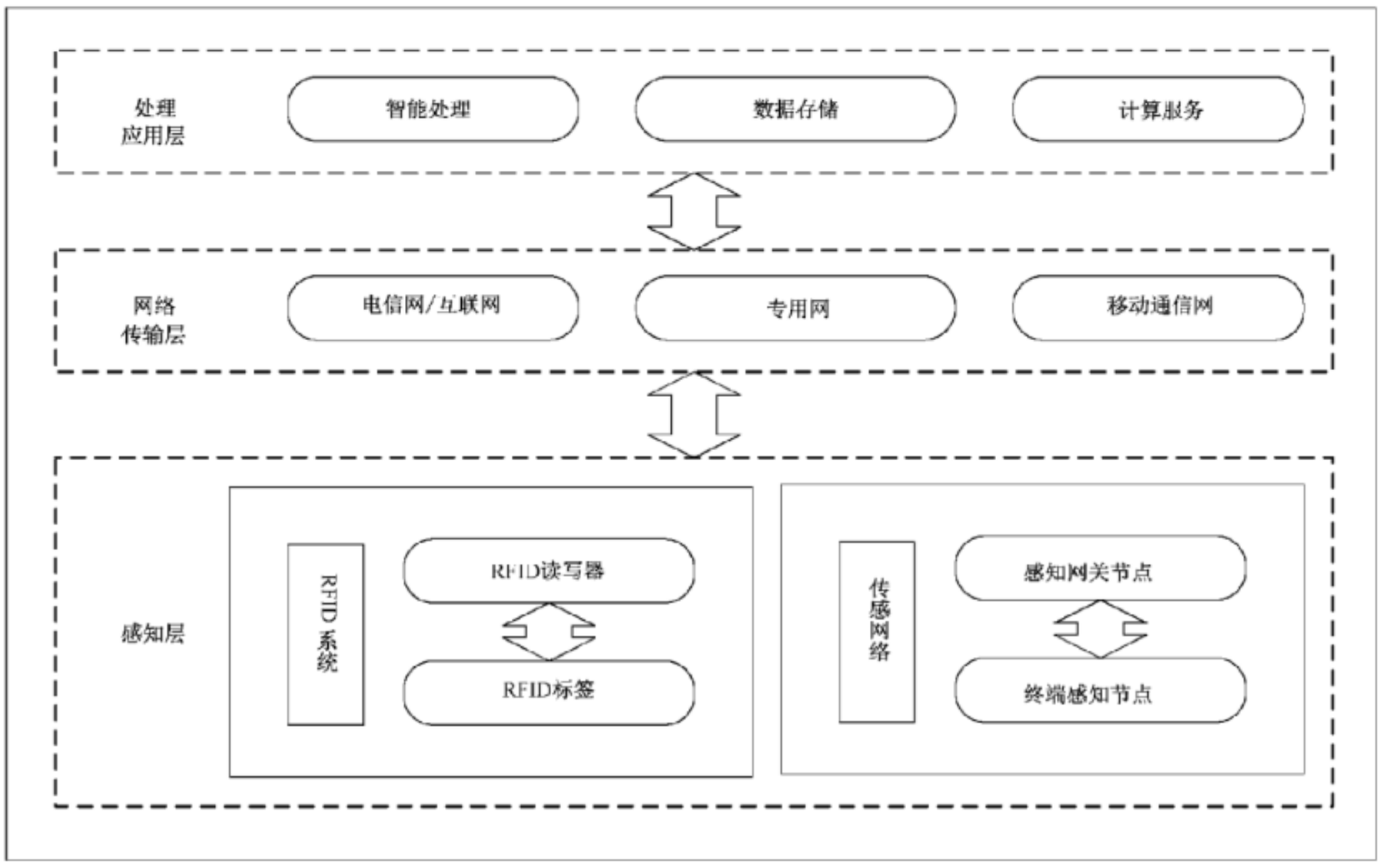


图 F.1 物联网构成

附 录 G
（资料性附录）
工业控制系统应用场景说明

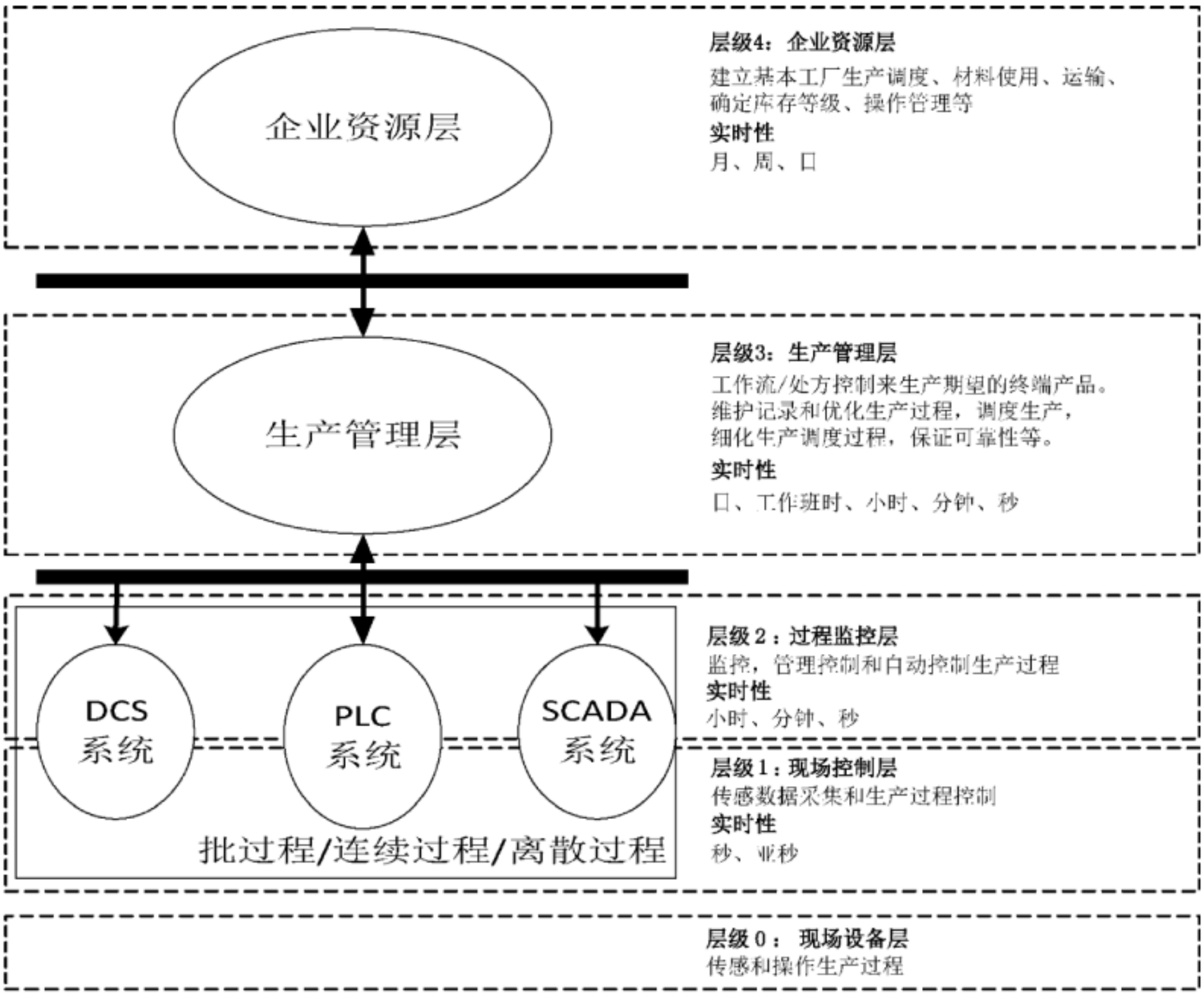
G.1 工业控制系统概述

工业控制系统(ICS)是几种类型控制系统的总称，包括数据采集与监视控制系统(SCADA)、集散控制系统(DCS)和其他控制系统，如在工业部门和关键基础设施中经常使用的可编程逻辑控制器(PLC)。工业控制系统通常用于诸如电力、水和污水处理、石油和天然气、化工、交通运输、制药、纸浆和造纸、食品和饮料以及离散制造(如汽车、航空航天和耐用品)等行业。工业控制系统主要由过程级、操作级以及各级之间和内部的通信网络构成，对于大规模的控制系统，也包括管理级。过程级包括被控对象、现场控制设备和测量仪表等，操作级包括工程师和操作员站、人机界面和组态软件、控制服务器等，管理级包括生产管理系统和企业资源系统等，通信网络包括商用以太网、工业以太网、现场总线等。

G.2 工业控制系统层次模型

本标准参考 IEC 62264-1 的层次结构模型划分，同时将 SCADA 系统、DCS 系统和 PLC 系统等模型的共性进行抽象，对工业控制系统采用层次模型进行说明。

图 G.1 给出了功能层次模型。层次模型从上到下共分为 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。



注：该图为工业控制系统经典层次模型参考 IEC 62264-1，但随着工业 4.0、信息物理系统的发展，已不能完全适用，因此对于不同的行业企业实际发展情况，允许部分层级合并。

图 G.1　功能层次模型

G.3　各个层次实现等级保护基本要求的差异

工业控制系统构成的复杂性，组网的多样性，以及等级保护对象划分的灵活性，给网络安全等级保护基本要求的使用带来了选择的需求。表 G.1 按照上述描述的功能层次模型和各层次功能单元映射模型给出了各个层次使用本标准相关内容的映射关系。

表 G.1　各层次与等级保护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)

表 G.1（续）

功能层次	技术要求
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)
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)

G.4 实现等级保护要求的一些约束条件

工业控制系统通常是对可用性要求较高的等级保护对象，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。例如用于基本功能的账户不应被锁定，甚至短暂的也不行；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等。

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。

附 录 H
（资料性附录）
大数据应用场景说明

H.1 大数据概述

本标准中将采用了大数据技术的信息系统，称为大数据系统。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，图 H.1 给出了大数据系统的模型。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，大数据安全涉及大数据平台的安全和大数据应用的安全。

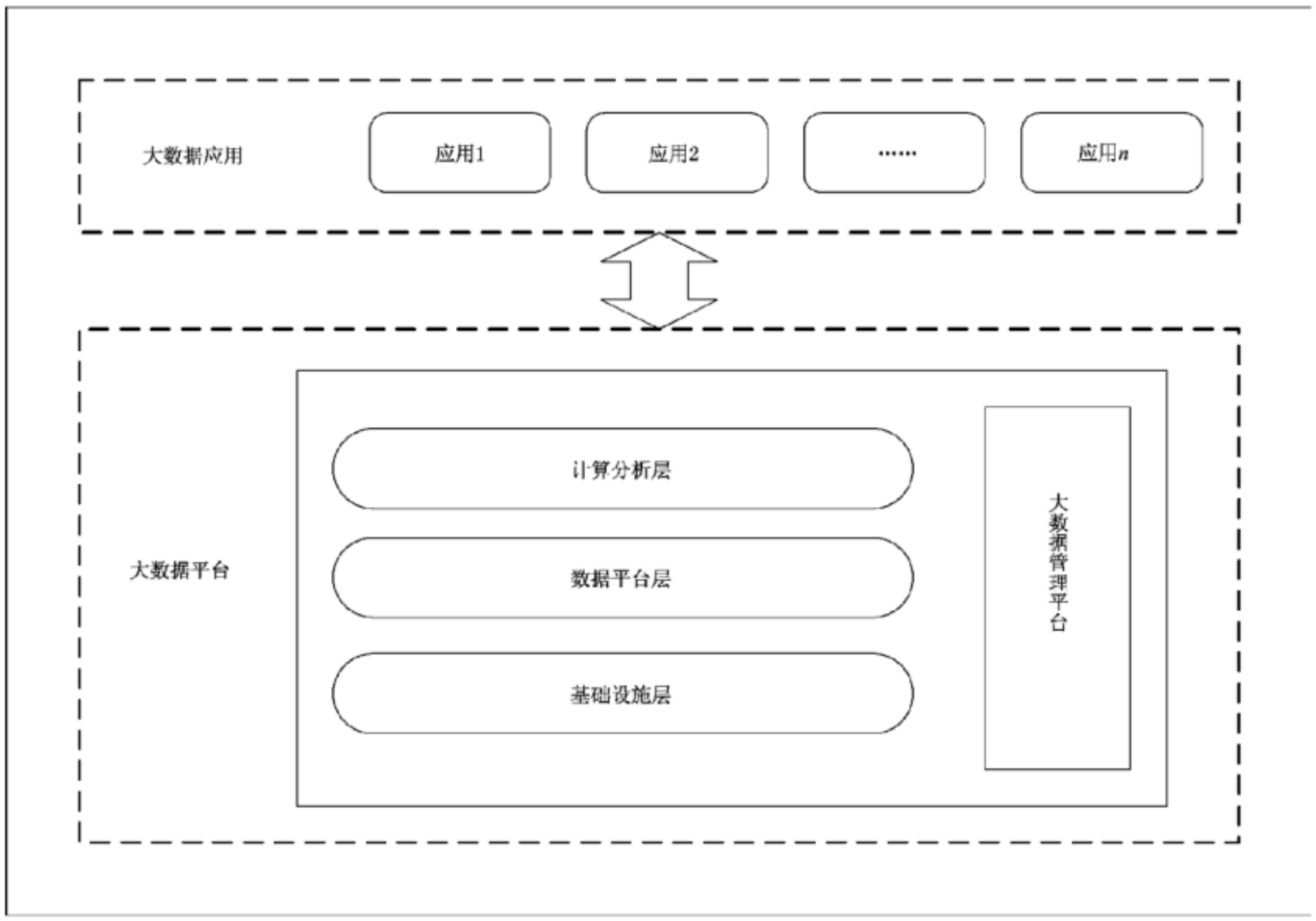


图 H.1 大数据系统构成

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。大数据系统除按照本标准的要求进行保护外，还需要考虑其特点，参照本附录补充和完善安全控制措施。

以下给出大数据系统可补充的安全控制措施供参考。

H.2 第一级可参考安全控制措施

H.2.1 安全通信网络

应保证大数据平台不承载高于其安全保护等级的大数据应用。

H.2.2 安全计算环境

大数据平台应对数据采集终端、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。

H.2.3 安全建设管理

应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。

H.3 第二级可参考安全控制措施

H.3.1 安全物理环境

应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。

H.3.2 安全通信网络

应保证大数据平台不承载高于其安全保护等级的大数据应用。

H.3.3 安全计算环境

本方面控制措施包括：

a) 大数据平台应对数据采集终端、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；
b) 大数据平台应能对不同客户的大数据应用实施标识和鉴别；
c) 大数据平台应为大数据应用提供管控其计算和存储资源使用状况的能力；
d) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理；
e) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；
f) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
g) 对外提供服务的大数据平台，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。

H.3.4 安全建设管理

本方面控制措施包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。