ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25070—2019
代替 GB/T 25070—2010

信息安全技术
网络安全等级保护安全设计技术要求

Information security technology—
Technical requirements of security design for classified protection of cybersecurity

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 25070—2010《信息安全技术　信息系统等级保护安全设计技术要求》，与 GB/T 25070—2010 相比，主要变化如下：

——将标准名称变更为《信息安全技术　网络安全等级保护安全设计技术要求》；

——各个级别的安全计算环境设计技术要求调整为通用安全计算环境设计技术要求、云安全计算环境设计技术要求、移动互联安全计算环境设计技术要求、物联网系统安全计算环境设计技术要求和工业控制系统安全计算环境设计技术要求；

——各个级别的安全区域边界设计技术要求调整为通用安全区域边界设计技术要求、云安全区域边界设计技术要求、移动互联安全区域边界设计技术要求、物联网系统安全区域边界设计技术要求和工业控制系统安全区域边界设计技术要求；

——各个级别的安全通信网络设计技术要求调整为通用安全通信网络设计技术要求、云安全通信网络设计技术要求、移动互联安全通信网络设计技术要求、物联网系统安全通信网络设计技术要求和工业控制系统安全通信网络设计技术要求；

——删除了附录 B 中的 B.2“子系统间接口”和 B.3“重要数据结构”，增加了 B.4“第三级系统可信验证实现机制”。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：公安部第一研究所、北京工业大学、北京中软华泰信息技术有限责任公司、中国电子信息产业集团有限公司第六研究所、中国信息通信研究院、阿里云计算技术有限公司、中国银行股份有限公司软件中心、公安部第三研究所、国家能源局信息中心、中国电力科学研究院有限公司、中国科学院软件研究所、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、中国科学院信息工程研究所、启明星辰信息技术集团股份有限公司、浙江中烟工业有限责任公司、中央电视台、北京江南天安科技有限公司、华为技术有限公司、北京航空航天大学、北京理工大学、北京天融信网络安全技术有限公司、北京和利时系统工程有限公司、青岛海天炜业过程控制技术股份有限公司、北京力控华康科技有限公司、石化盈科信息技术有限责任公司、北京华大智宝电子系统有限公司、山东微分电子科技有限公司、北京中电瑞铠科技有限公司、北京广利核系统工程有限公司、北京神州绿盟科技有限公司。

本标准主要起草人：蒋勇、李超、李秋香、赵勇、袁静、徐晓军、宫月、吴薇、黄学臻、陈翠云、刘志宇、陈彦如、王昱镔、张森、卢浩、吕由、林莉、徐进、傅一帆、丰大军、龚炳铮、贡春燕、霍玉鲜、范文斌、魏亮、田慧蓉、李强、李艺、沈锡镛、陈雪秀、任卫红、孙利民、朱红松、阎兆腾、段伟恒、孟雅辉、章志华、李健俊、李威、顾军、陈卫平、琚宏伟、陈冠直、胡红升、陈雪鸿、高昆仑、张锎、张敏、李昊、王宝会、汤世平、雷晓锋、王弢、王晓鹏、刘美丽、陈聪、刘安正、刘利民、龚亮华、方亮、石宝臣、孙郁熙、巩金亮、周峰、郝鑫、梁猛、姜红勇、冯坚、黄敏、张旭武、石秦、孙洪涛。

本标准所代替标准的历次版本发布情况为：

——GB/T 25070—2010。

引　言

GB/T 25070—2010《信息安全技术　信息系统等级保护安全设计技术要求》在开展网络安全等级保护工作的过程中起到了非常重要的作用，被广泛应用于指导各个行业和领域开展网络安全等级保护建设整改等工作，但是随着信息技术的发展，GB/T 25070—2010 在适用性、时效性、易用性、可操作性上需要进一步完善。

为了配合《中华人民共和国网络安全法》的实施，同时适应云计算、移动互联、物联网、工业控制和大数据等新技术、新应用情况下网络安全等级保护工作的开展，需对 GB/T 25070—2010 进行修订，修订的思路和方法是调整原国家标准 GB/T 25070—2010 的内容，针对共性安全保护目标提出通用的安全设计技术要求，针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用领域的特殊安全保护目标提出特殊的安全设计技术要求。

本标准是网络安全等级保护相关系列标准之一。

与本标准相关的标准包括：

——GB/T 25058　信息安全技术　信息系统安全等级保护实施指南；

——GB/T 22240　信息安全技术　信息系统安全等级保护定级指南；

——GB/T 22239　信息安全技术　网络安全等级保护基本要求；

——GB/T 28448　信息安全技术　网络安全等级保护测评要求。

在本标准中，**黑体字部分**表示较低等级中没有出现或增强的要求。

信息安全技术
网络安全等级保护安全设计技术要求

1 范围

本标准规定了网络安全等级保护第一级到第四级等级保护对象的安全设计技术要求。

本标准适用于指导运营使用单位、网络安全企业、网络安全服务机构开展网络安全等级保护安全技术方案的设计和实施，也可作为网络安全职能部门进行监督、检查和指导的依据。

注：第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全设计技术要求，所以不在本标准中进行描述。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069—2010 信息安全技术 术语

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

3 术语和定义

GB 17859—1999、GB/T 22240—2008、GB/T 25069—2010、GB/T 31167—2014、GB/T 31168—2014 和 GB/T 32919—2016 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 31167—2014 中的一些术语和定义。

3.1

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/T 22239—2019，定义 3.1]

3.2

定级系统 classified system

已确定安全保护等级的系统。定级系统分为第一级、第二级、第三级、第四级和第五级系统。

3.3

定级系统安全保护环境 security environment of classified system

由安全计算环境、安全区域边界、安全通信网络和(或)安全管理中心构成的对定级系统进行安全保护的环境。

3.4

安全计算环境 security computing environment

对定级系统的信息进行存储、处理及实施安全策略的相关部件。

3.5

安全区域边界 security area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

3.6

安全通信网络 security communication network

对定级系统**安全计算环境**之间进行信息传输及实施**安全**策略的相关部件。

3.7

安全管理中心 **security management center**

对顶级系统的**安全**策略及**安全计算环境**、**安全区域边界**和**安全**通信网络上的**安全**机制实施统一管理的平台或**区域**。

3.8

跨定级系统**安全**管理中心 **security management center for cross classified system**

对相同或不同等级的定级系统之间**互联**的**安全**策略及**安全互联**部件上的**安全**机制实施统一管理的平台或**区域**。

3.9

定级系统互联 **classified system interconnection**

通过**安全互联**部件和跨定级系统**安全**管理中心实现的相同或不同等级的定级系统**安全**保护**环境**之间的**安全**连接。

3.10

云计算 cloud computing

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[**GB/T**32400—2015，定义 3.2.5]

3.11

云计算平台 **cloud computing platform**

云服务商提供的**云计算**基础设施及其上的服务层软件的集合。

[**GB/T** 31167—2014，定义 3.7]

3.12

云计算环境 cloud computing environment

云服务商提供的云计算平台及客户在云计算平台之上部署的软件及相关组件的集合。

[GB/T 31167—2014，定义 3.8]

3.13

移动互联系统 mobile interconnection system

采用了移动互联技术，以移动应用为主要发布形式，用户通过 mobile internet system 移动终端获取业务和服务的信息系统。

3.14

物联网 internet of things

将感知节点设备通过互联网等网络连接起来构成的系统。

[GB/T 22239—2019，定义 3.15]

3.15

感知层网关 sensor layer gateway

将感知节点所采集的数据进行汇总、适当处理或数据融合，并进行转发的装置。

3.16

感知节点设备 sensor node

对物或环境进行信息采集和/或执行操作，并能联网进行通信的装置。

3.17

数据新鲜性 data freshness

对所接收的历史数据或超出时限的数据进行识别的特性。

3.18

现场设备 field device

连接到ICS现场的设备，现场设备的类型包括ITU、PLC、传感器、执行器、人机界面以及相关的通讯设备等。

3.19

现场总线 fieldbus

一种处于工业现场底层设备(如传感器、执行器、控制器和控制室设备等)之间的数字串行多点双向数据总线或通信链路。利用现场总线技术不需要在控制器和每个现场设备之间点对点布线。总线协议是用来定义现场总线网络上的消息，每个消息标识了网络上特定的传感器。

4 缩略语

下列缩略语适用于本文件。

3G：第三代移动通信技术(3rd Generation Mobile Communication Technology)

4G：第四代移动通信技术(4th Generation Mobile Communication Technology)

API：应用程序编程接口(Application Programming Interface)

BIOS：基本输入输出系统(Basic Input Output System)

CPU：中央处理器(Central Processing Unit)

DMZ：隔离区(Demilitarized Zone)

GPS：全球定位系统(Global Positioning System)

ICS：工业控制系统(Industrial Control System)

IoT：物联网(Internet of Things)

NFC：近场通信/近距离无线通信技术(Near Field Communication)

OLE：对象连接与嵌入(Object Linking and Embedding)

OPC：用于过程控制的OLE(OLE for Process Control)

PLC：可编程逻辑控制器(Programmable Logic Controller)

RTU：远程终端单元(Remote Terminal Units)

VPDN：虚拟专用拨号网(Virtual Private Dial-up Networks)

SIM：用户身份识别模块(Subscriber Identification Module)

WiFi：无线保真(Wireless Fidelity)

5 网络安全等级保护安全技术设计概述

5.1 通用等级保护安全技术设计框架

网络安全等级保护安全技术设计包括各级系统安全保护环境的设计及其安全互联的设计，如图1所示。各级系统安全保护环境由相应级别的安全计算环境、安全区域边界、安全通信网络和(或)安全管理中心组成。定级系统互联由安全互联部件和跨定级系统安全管理中心组成。

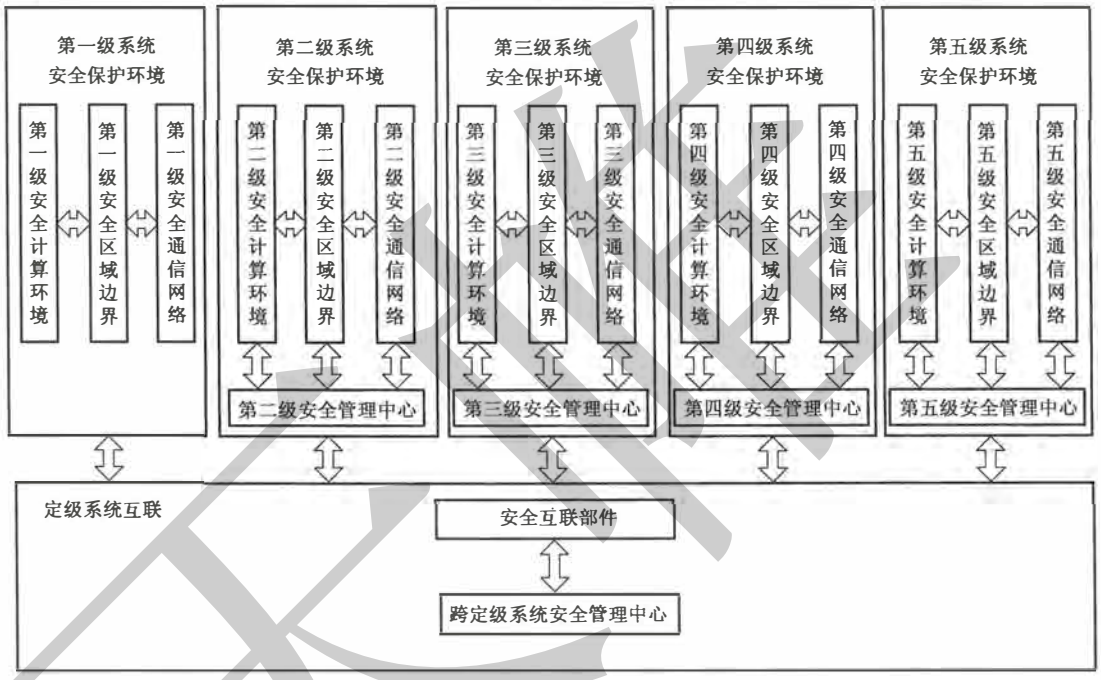


图1 网络安全等级保护安全技术设计框架

本标准第6章～第11章，对图1各个部分提出了相应的设计技术要求(第五级网络安全保护环境的设计要求除外)。附录A给出了访问控制机制设计，附录B给出了第三级系统安全保护环境设计示例。此外，附录C给出大数据设计技术要求。

在对定级系统进行等级保护安全保护环境设计时，可以结合系统自身业务需求，将定级系统进一步细化成不同的子系统，确定每个子系统的等级，对子系统进行安全保护环境的设计。

5.2 云计算等级保护安全技术设计框架

结合云计算功能分层框架和云计算安全特点，构建云计算安全设计防护技术框架，包括云用户层、访问层、服务层、资源层、硬件设施层和管理层(跨层功能)。其中一个中心指安全管理中心，三重防护包括安全计算环境、安全区域边界和安全通信网络，具体如图2所示。

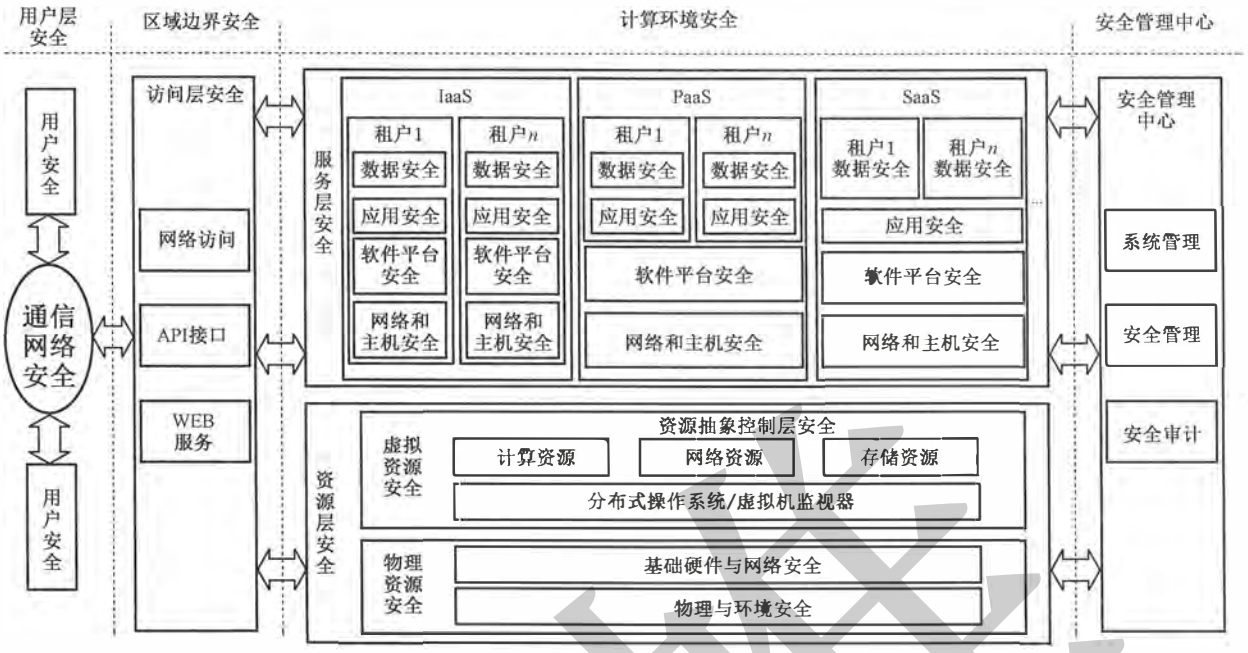


图 2　云计算等级保护安全技术设计框架

用户通过安全的通信网络以网络直接访问、API 接口访问和 WEB 服务访问等方式安全地访问云服务商提供的安全计算环境，其中用户终端自身的安全保障不在本部分范畴内。安全计算环境包括资源层安全和服务层安全。其中，资源层分为物理资源和虚拟资源，需要明确物理资源安全设计技术要求和虚拟资源安全设计要求，其中物理与环境安全不在本部分范畴内。服务层是对云服务商所提供服务的实现，包含实现服务所需的软件组件，根据服务模式不同，云服务商和云租户承担的安全责任不同。服务层安全设计需要明确云服务商控制的资源范围内的安全设计技术要求，并且云服务商可以通过提供安全接口和安全服务为云租户提供安全技术和安全防护能力。云计算环境的系统管理、安全管理和安全审计由安全管理中心统一管控。结合本框架对不同等级的云计算环境进行安全技术设计，同时通过服务层安全支持对不同等级云租户端（业务系统）的安全设计。

5.3　移动互联等级保护安全技术设计框架

移动互联系统安全防护参考架构如图 3，其中安全计算环境由核心业务域、DMZ 域和远程接入域三个安全域组成，安全区域边界由移动互联系统区域边界、移动终端区域边界、传统计算终端区域边界、核心服务器区域边界、DMZ 区域边界组成，安全通信网络由移动运营商或用户自己搭建的无线网络组成。

a）　核心业务域

核心业务域是移动互联系统的核心区域，该区域由移动终端、传统计算终端和服务器构成，完成对移动互联业务的处理、维护等。核心业务域应重点保障该域内服务器、计算终端和移动终端的操作系统安全、应用安全、网络通信安全、设备接入安全。

b）　DMZ 域

DMZ 域是移动互联系统的对外服务区域，部署对外服务的服务器及应用，如 Web 服务器、数据库服务器等，该区域和互联网相联，来自互联网的访问请求应经过该区域中转才能访问核心业务域。DMZ 域应重点保障服务器操作系统及应用安全。

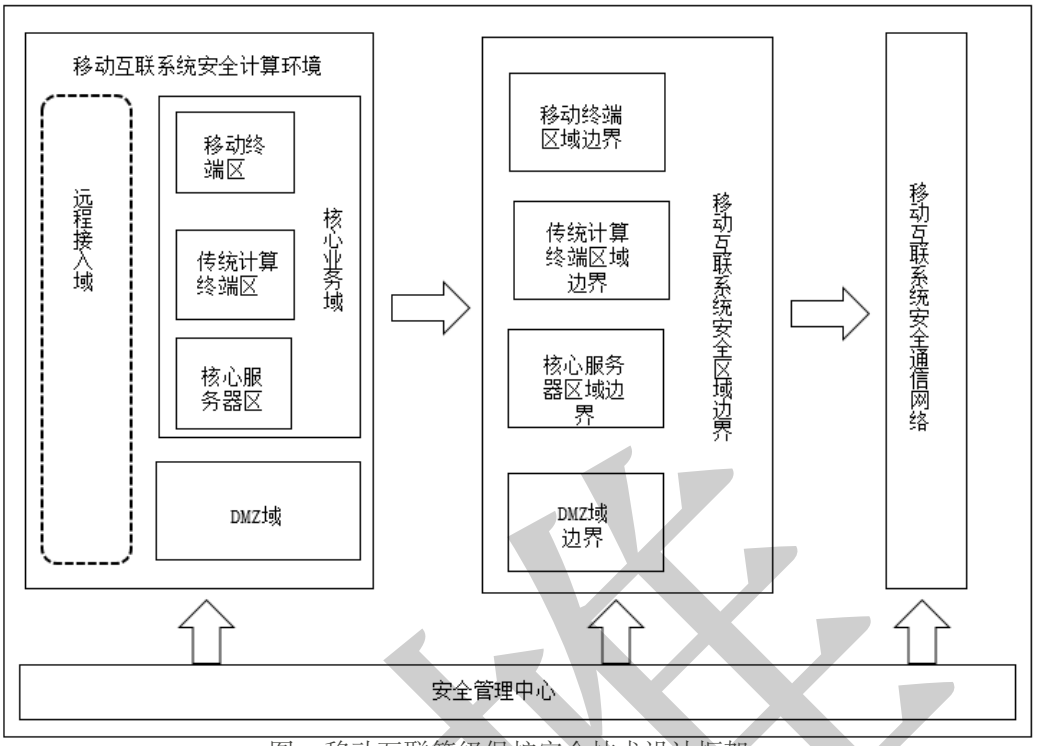


图3 移动互联等级保护安全技术设计框架

c) 远程接入域

远程接入域由移动互联系统运营使用单位可控的，通过VPN等技术手段远程接入移动互联系统运营使用单位网络的移动终端组成，完成远程办公、应用系统管控等业务。远程接入域应重点保障远程移动终端自身运行安全、接入移动互联应用系统安全和通信网络安全。

本标准将移动互联系统中的计算节点分为两类：移动计算节点和传统计算节点。移动计算节点主要包括远程接入域和核心业务域中的移动终端，传统计算节点主要包括核心业务域中的传统计算终端和服务器等。传统计算节点及其边界安全设计可参考通用安全设计要求，下文提到的移动互联计算环境、区域边界、通信网络的安全设计都是特制移动计算节点而言的。

5.4 物联网等级保护安全技术设计框架

结合物联网系统的特点，构建在安全管理中心支持下的安全计算环境、安全区域边界、安全通信网络三重防御体系。安全管理中心支持下的物联网系统安全保护设计框架如图4所示，物联网感知层和应用层都由完成计算任务的计算环境和连接网络通信域的区域边界组成。

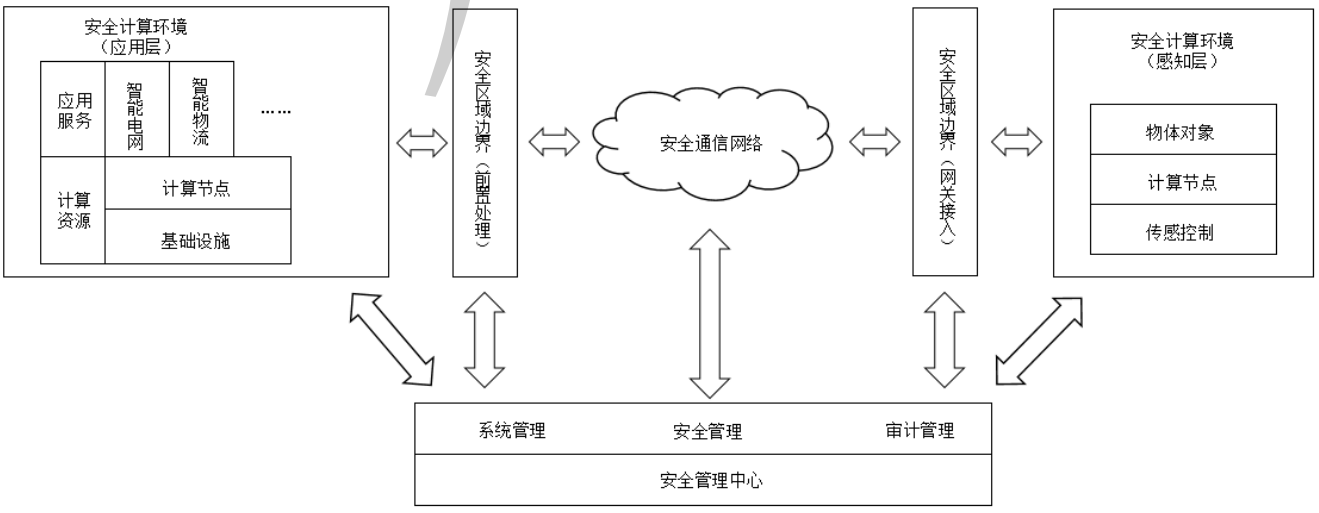


图 4 物联网系统等级保护安全技术设计框架

a) 安全计算环境

包括物联网系统感知层和应用层中对定级系统的信息进行存储、处理及实施安全策略的相关部件，如感知层中的物体对象、计算节点、传感控制设备，以及应用层中的计算资源及应用服务等。

b) 安全区域边界

包括物联网系统安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件，如感知层和网络层之间的边界、网络层和应用层之间的边界等。

c) 安全通信网络

包括物联网系统安全计算环境和安全区域之间进行信息传输及实施安全策略的相关部件，如网络层的通信网络以及感知层和应用层内部安全计算环境之间的通信网络等。

d) 安全管理中心

包括对物联网系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台，包括西ton管理、安全管理和审计管理三部分，只有第一级及第一级以上的安全保护环境设计有安全管理中心。

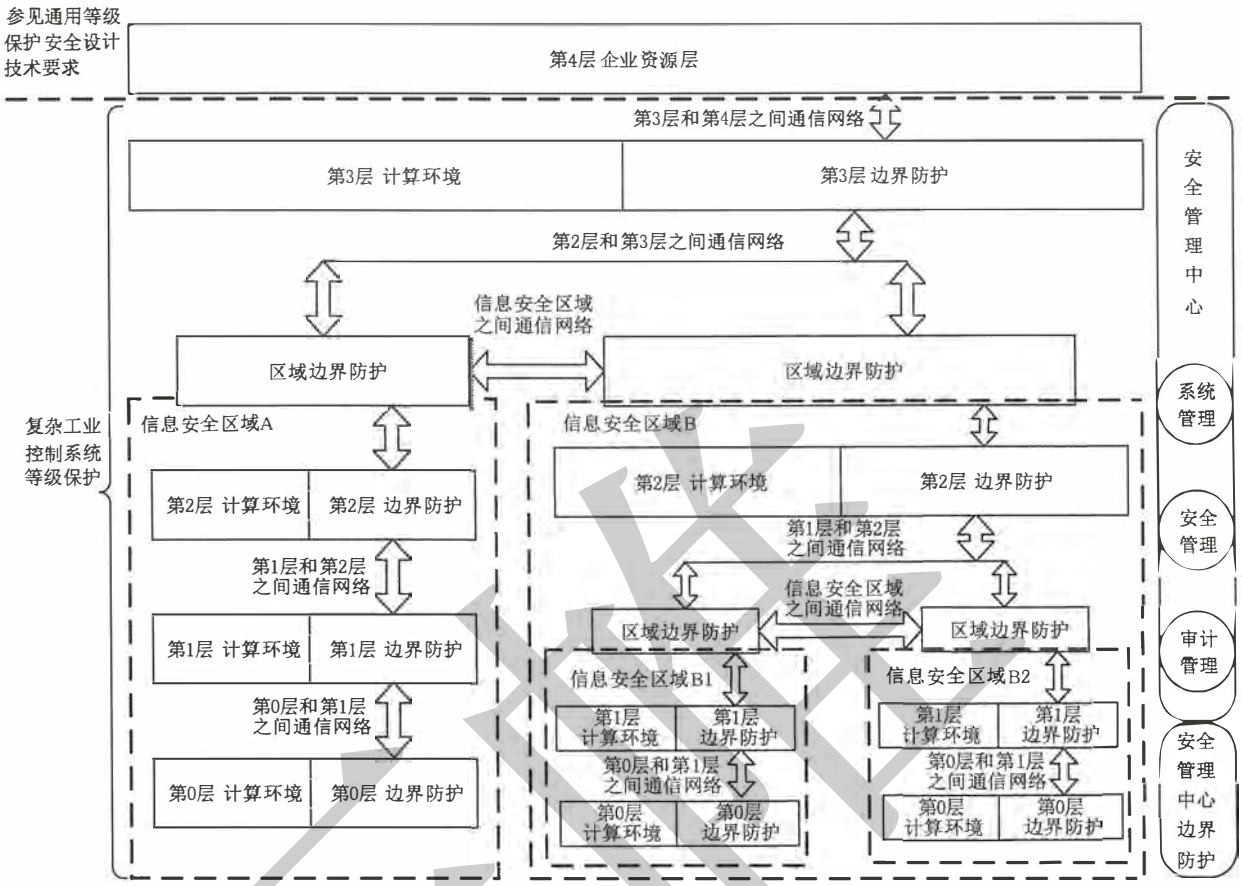
5.5 工业控制等级保护安全技术设计框架

对于工业控制系统根据被保护对象业务性质分区，针对功能层次技术特点实施的网络安全等级保护设计，工业控制系统等级保护安全技术设计框架如图5所示。工业控制系统等级保护安全技术设计合工业控制系统总线协议复杂多样、实时性要求强、节点计算资源有限、设备可靠性要求高、故障恢复时间短、安全机制不能影响实时性等特点进行设计，以实现可信、可控、可管的系统安全互联、区域边界安全防护和计算环境安全。

工业控制系统分为4层，即第0～3层为工业控制系统等级保护的范畴，为设计框架覆盖的区域；横向上对工业控制系统进行安全区域的划分，根据工业控制系统中业务的重要性、实时性、业务的关联性、对现场受控设备的影响程度以及功能范围、资产属性等，形成不同的安全防护区域，系统都应置于相应的安全区域内，具体分区以工业现场实际情况为准（分区方式包括但不限于：第0～2层组成一个安全区域、第0～1层组成一个安全区域、同层中有不同的安全区域等）。

分区原则根据业务系统或其功能模板的实时性、使用者、主要功能、设备使用场所、各业务系统间的相互关系、广域网通信方式以及对工业控制系统的影响程度等。对于额外的安全性和可靠性要求，在主要的安全区还可以根据操作功能进一步划分为子区，将设备划分为不同的区域可以有效地建立“纵深防御”策略。将具备相同功能和安全要求的各系统的控制功能划分为不同的安全区域，并按照方便管理和控制为原则为各安全功能区域分配网段地址。

设计框架逐级增强，但防护类别相同，只是安全保护设计的强度不同。防护类别包括：安全计算环境，包括工业控制系统0～3层中的信息进行存储、处理及实施安全策略的相关部件；安全区域边界，包括安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件；安全通信网络，包括安全计算环境和网络安全区域之间进行信息传输及实施安全策略的相关部件；安全管理中心，包括对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台，包括系统管理、安全管理和审计管理三部分。



注 1：参照 IEC/TS 62443-1-1 工业控制系统按照功能层次划分为第 0 层：现场设备层，第 1 层：现场控制层，第 2 层：过程监控层，第 3 层：生产管理层，第 4 层：企业资源层。

注 2：一个信息安全区域可以包括多个不同等级的子区域。

注 3：纵向上分区以工业现场实际情况为准（图中分区为示例性分区），分区方式包括但不限于：第 0～2 层组成一个安全区域、第 0～1 层组成一个安全区域等。

图 5　工业控制系统等级保护安全技术设计框架

6　第一级系统安全保护环境设计

6.1　设计目标

第一级系统安全保护环境的设计目标是：按照 GB 17859—1999 对第一级系统的安全保护要求，实现定级系统的自主访问控制，使系统用户对其所属客体具有自我保护的能力。

6.2　设计策略

第一级系统安全保护环境的设计策略是：遵循 GB 17859—1999 的 4.1 中相关要求，以身份鉴别为基础，提供用户和（或）用户组对文件及数据库表的自主访问控制，以实现用户与数据的隔离，使用户具备自主安全保护的能力；以包过滤手段提供区域边界保护；以数据校验和恶意代码防范等手段提供数据和系统的完整性保护。

第一级系统安全保护环境的设计通过第一级的安全计算环境、安全区域边界以及安全通信网络的设计加以实现。计算节点都应基于可信根实现开机到操作系统启动的可信验证。