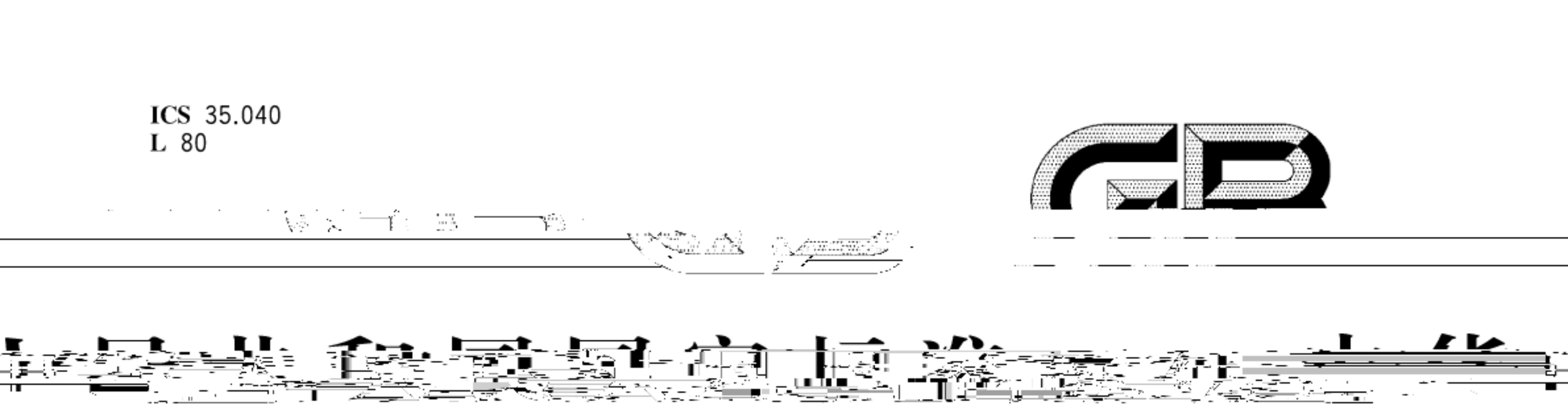
ICS 35.040
L 80



GB/T 25058—2019
代替 GB/T 25058—2010

# 信息安全技术

hnology—

otection of cybersecurity

Information security tech

Implementation guide for classified pro

2019-08-30 发布

2020-03-01 实施

# 目　　次

前言 …… V
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 2
4　信息安全等级保护概述 …… 3
5　等级保护实施与管理 …… 5
5.1　定级、备案和批准 …… 5
5.2　开展等级测评 …… 6
5.3　监督检查 …… 7
6　总体安全规划 …… 8
6.1　总体安全规划阶段的工作流程 …… 8
6.2　安全需求分析 …… 9
6.2.1　基本安全需求的确定 …… 9
6.2.2　特殊安全需求的确定 …… 9
6.2.3　形成安全需求分析报告 …… 10
6.3　总体安全设计 …… 10
6.3.1　总体安全策略设计 …… 10
6.3.2　安全技术框架设计 …… 11
6.4　安全建设规划 …… 14
6.4.1　安全建设目标确定 …… 14
6.4.2　安全建设内容规划 …… 14
6.4.3　形成安全建设项目规划 …… 15
7　安全设计与实施 …… 16
7.1　安全设计与实施阶段的工作流程 …… 16
7.2　安全方案详细设计 …… 16

7.2.1 技术措施实现内容的设计 …… 16
7.2.2 管理措施实现内容的设计 …… 17
7.2.3 设计结果的文档化 …… 17
7.3 技术措施的实现 …… 18
7.3.1 [illegible] …… 18
7.3.2 安全控制的开发 …… 18
7.3.3 安全控制集成 …… 19
7.3.4 [illegible] …… 20
7.4 管理措施的实现 …… 21
7.4.1 安全管理制度的建设和修订 …… 21
[illegible] …… 22
[illegible] …… 22
[illegible] …… 22
[illegible] …… 23
[illegible] …… 23
[illegible] …… 23
[illegible] …… 24
[illegible] …… 25
[illegible] …… 25
[illegible] …… 26
[illegible] …… 26
[illegible] …… 27
[illegible] …… 27
[illegible] …… 28
[illegible] …… 28
8.7 等级测评 …… 30
8.8 监督检查 …… 30
8.9 应急响应与保障 …… 30
8.9.1 应急准备 …… 30
[illegible] …… 31
[illegible] …… 32
9 定级对象终止 …… 32
[illegible] …… 33
[illegible] …… 35

5.2 设备迁移或库存 ……

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:公安部第三研究所(公安部信息安全等级保护评估中心)、中国电子科技集团公司

# 信息安全技术 网络安全等级保护实施指南

## 1 范围

本标准规定了等级保护对象实施网络安全等级保护工作的过程

## 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

## 3 术语和定义

GB 17859、GB/T 22239、GB/T 25069 和 GB/T 28448 界定的术语和定义适用于本文件。

## 4 等级保护实施概述

### 4.1 基本原则

安全等级保护的核心是将等级保护对象划分等级，按标准进行建设、管理和监督

其他原因，安全保护等级需要变更的，应根据等级保护的管理规范和技术标准的要求，重新确定定级对

角色和职责 4.2

4.3 实施的基本流程

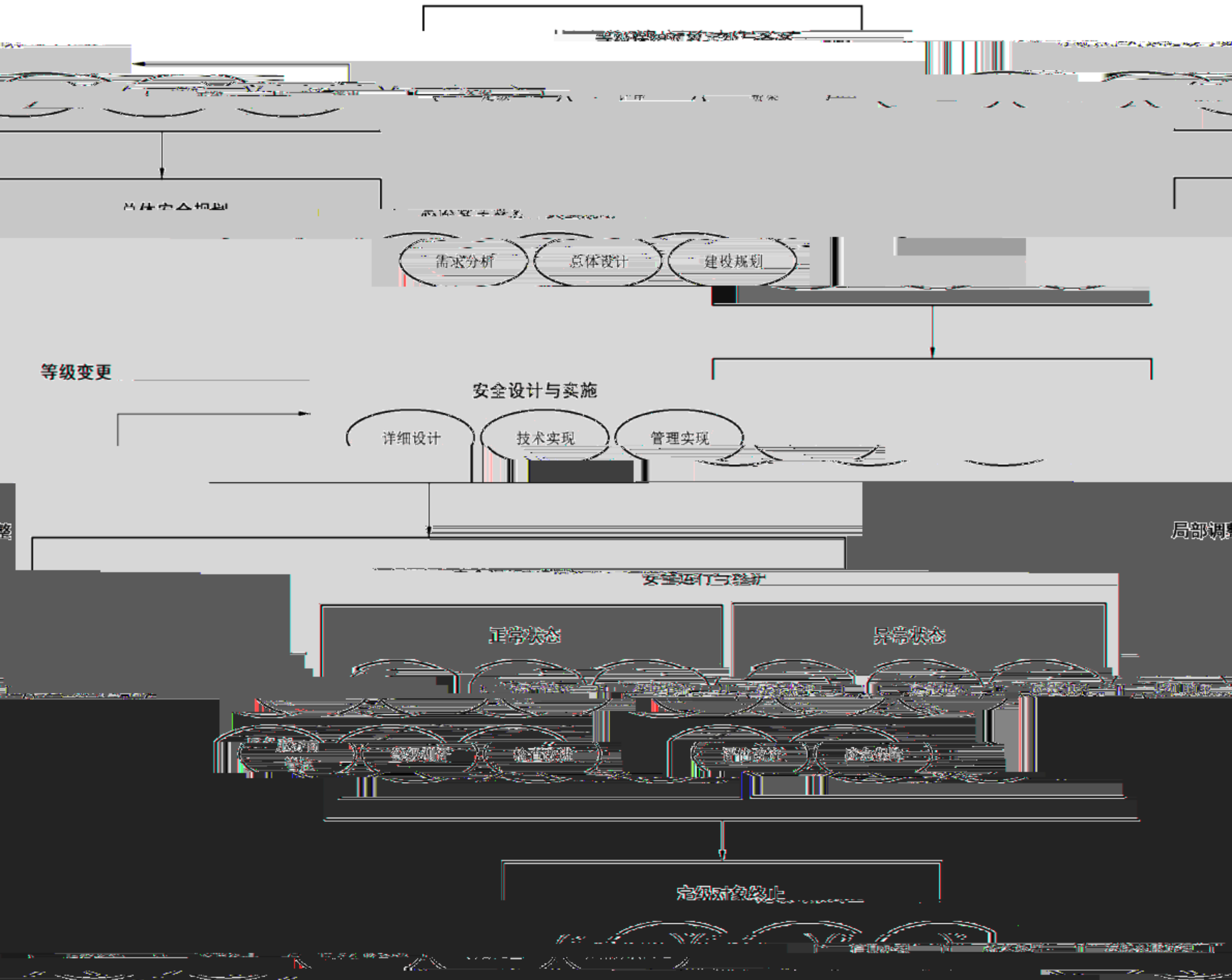



图 1 定级对象安全保护等级变更过程

安全性、动态性是统一的，应从安全运行与维护阶段进入安全设计与实施阶段，进行设计、调整和实施保护的要求，当等级保护对象发生重大变更导致安全保护等级变化时，应从安全运行与维护阶段进入等级变更过程。

安全事件时可能会发生应急响应与保障。

护过程中，发生

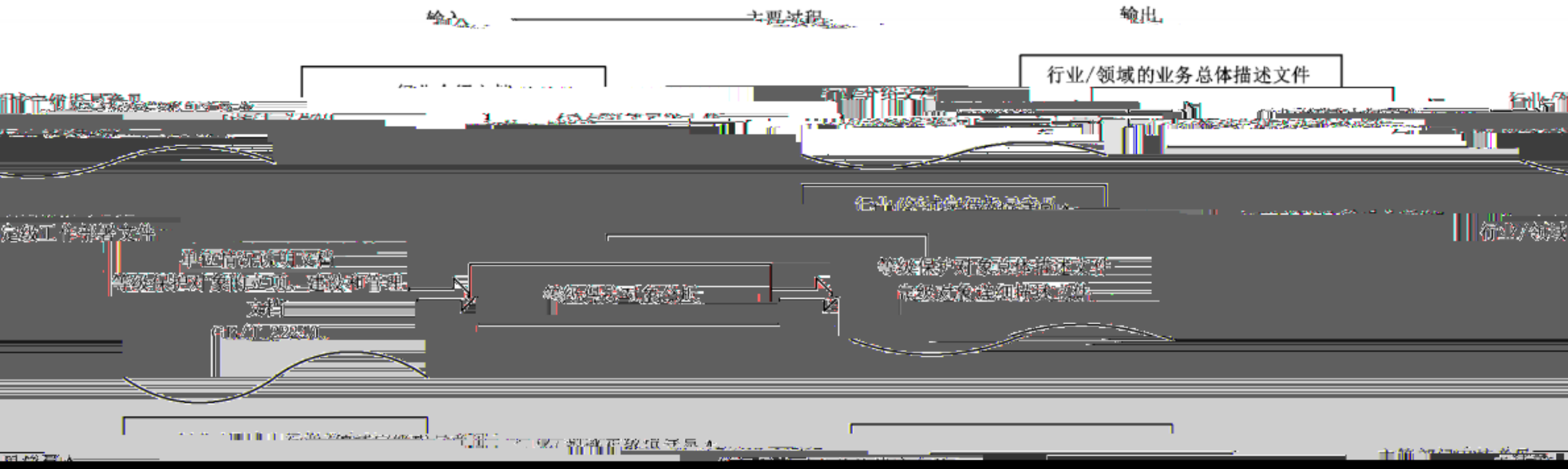
对象安全等级保护实施的基本流程中各个阶段的主要过程、活动、输入和输出见附录 A。

等级保护对

## 5 等级保护对象定级与备案

[redacted]

等级保护对象定级与备案阶段的工作流程见图 2。



主管部门可组织梳理本行业/领域内主要依靠信息化处理的业务情况，并按照业务承载的社会功

5.3 等级保护对象分析

活动目标：

通过收集了解有关等级保护对象的信息，并对信息进行综合分析和整理，分析单位的主要社会功能/职能及作用，确定履行主要社会功能/职能所依赖的等级保护对象，整理等级保护对象处理的业务及服务范围。最后按照分析和整理的内容，有行业/领域定级指导意见的还应依据行业/领域定级指导意

性程度。

g) 识别用户范围和用户类型

[illegible]

对收集的信息进行整理、分析，形成对等级保护对象的总体描述文件。一个典型的等级保护对象的

[illegible]

等级保护对象描述：

[illegible]

5 [illegible]

6 支撑的业务应用的种类和特性

7 处理的信息资产

8 [illegible]

9 等级保护实施的管理框架

[illegible]

对象确定

5.3.2 定级对

示：

活动目标

定的等级保护对象总体描述文件(有行业/领域定级指导意见的还应依据行业/领域定级指

依据单位

关工数

单位网络安全职务有效

参与单位年运营 集团

[illegible]

开始描述

本活动主要包括以下活动内容：

a) 划分方法的选择

[illegible]

b) 等级保护对象划分

依据等级保护对象划分原则参考行业/领域定

级指导意见(若有行业/领域定级指导意见)

[illegible]

物联网主要包括感知、网络传输和处理应用等特征要素，应将以上要素作为一个整体对象定级，各要素不单独定级。

[redacted]

[redacted]

[redacted]

活动输出：定级结果，主管部门审批意见。

#### 5.4.2 形成定级报告

活动目标：




图 1 信息安全等级保护工作流程

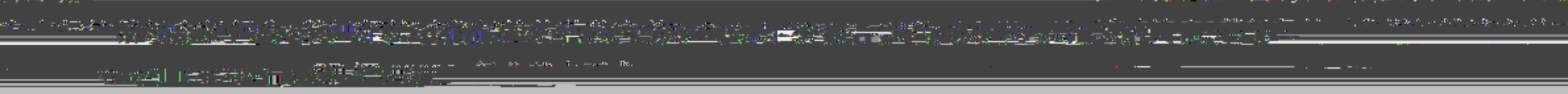
### 6.2 安全需求分析

#### 6.2.1 基本安全需求的确定

活动目标：

根据等级保护对象的安全保护等级，提出等级保护对象的基本安全

保护需求。



活动描述：

本活动主要包括以下子活动内容：

[redacted]

6.3 总体安全设计

6.3.1 总体安全策略设计

活动目标：

[redacted]

活动描述

本活动主要包括以下主要活动内容：

a) 确定安全方针

[illegible]

b) 制定安全策略

[illegible]

6.3.2 安全技术体系结构设计

活动目标：

根据GB/T 22239 行业技术要求、安全需求分析报告、机构总体安全管理文件等，提出等级保护对

[illegible]

[illegible]

[illegible]

活动输出：总体安

[illegible]

本活动主要包括以下主要活动内容：

a) 设计安全技术体系架构

根据相关安全管理文件、GB/T 22239 行业技术要求和安全需求分析报告，设计安全技术

[illegible]

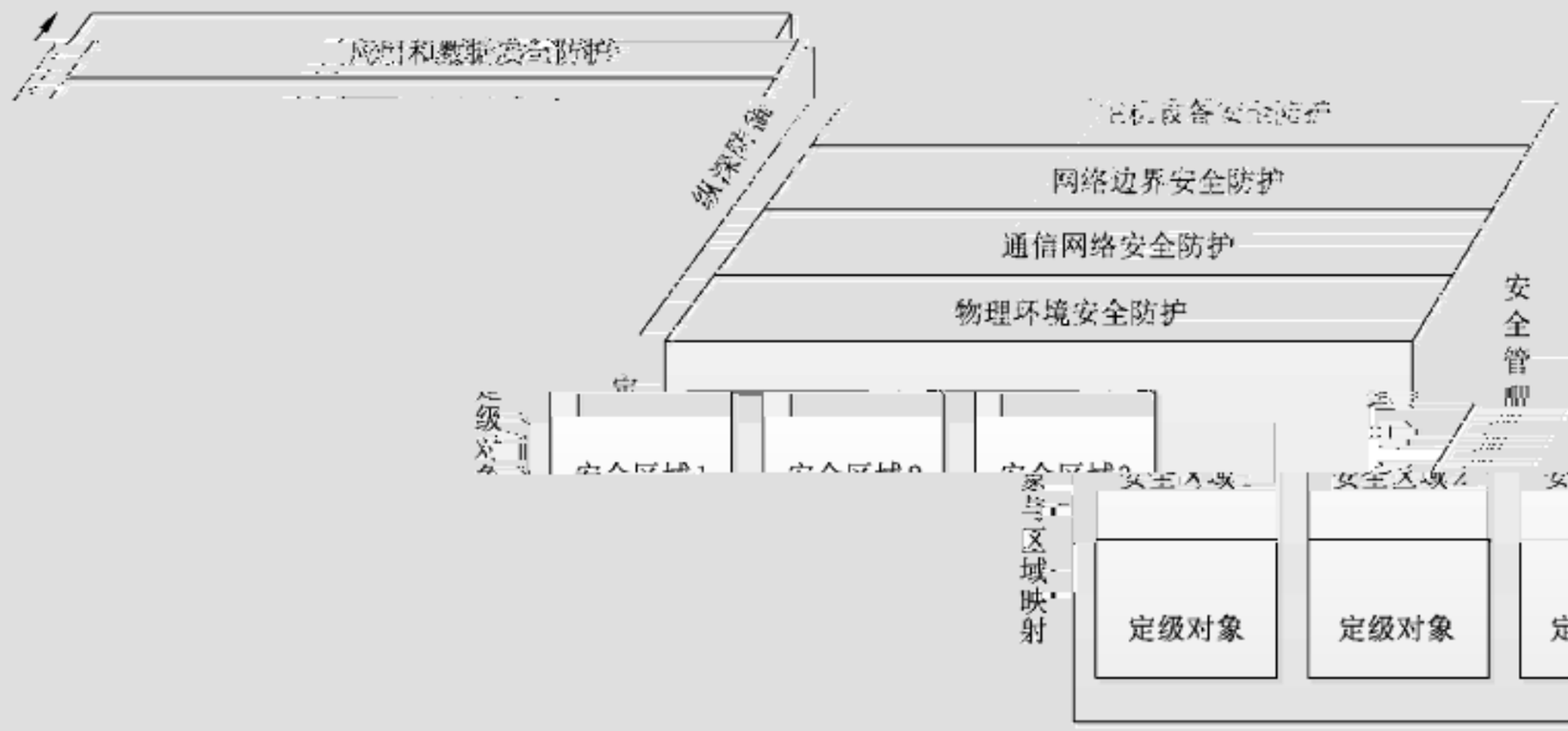



图 A 等级保护对象的安全技术体系架构

b） 规定不同级别定级对象物理环境的安全保护技术措施

活动描述：

本活动主要包括以下子活动内容：

[illegible]

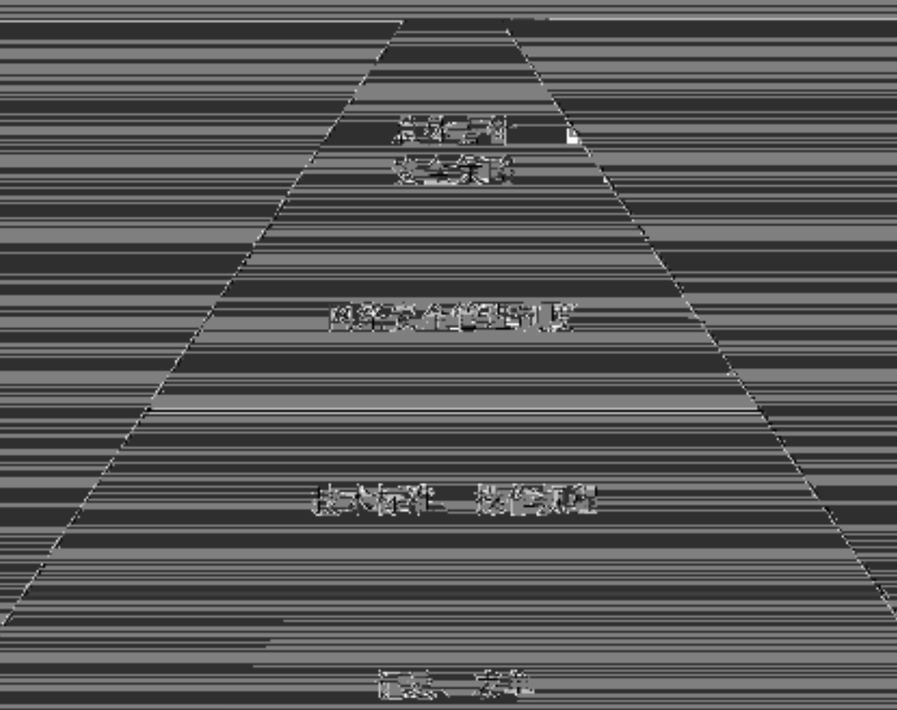


图5 等级保护对象的安全管理体系框架

[illegible]

[illegible]

[illegible]

[illegible]

g) 规定不同级别定级对象安全事件外置和应急管理策略

设计结果文档化 6.3.4

活动目标：

6.4 安全建设项目规划

6.4.1 安全建设目标确定

活动目标：

6.4.2 安全建设内容规划

活动目标：

根据安全建设目标和等级保护对象安全总体方案的要求，设计分期分批的主要建设内容，并将建设

参与角色：运营、使用单位，网络安全服务机构。

活动输入：等级保护对象安全总体方案；等级保护对象分阶段安全建设目标。

活动描述：

本活动主要包括以下子活动内容：

6.4.3 形成安全建设项目规划

活动目标：




图 6 安全设计与实施阶段的工作流程

## 7.2 安全方案详细设计

### 7.2.1 技术措施实现内容的设计

活动目标：

在网络安全产品采购和安全控制的开发阶段具有先进

品功能特征表现成文档，使得

者、网络安全服务机构、网络安全产品供应商。

参与角色：运营、使用单位

络安全服务机构评价材料。

活动描述：

本活动主要包括以下子活动内容：

a) 结构框架的设计

b） 安全功能要求的设计

[redacted]

7.2.3 设计结果的文档化

活动目标：

[redacted]

d) 网络安全产品或组件部署[illegible]

e) 安全整体策略和配置；

f) 配套的安全管理建设内容；

g) 工程实施计划；

h) 项目投资概算。

活动输出：安全详细设计方案。

## 7.3 技术措施的实现

### 7.3.1 网络安全产品或服务采购

活动目标：

按照安全详细设计方案中对于产品或服务的具体指标要求进行采购，根据产品、产品组合或服务实[illegible]

[illegible]

本活动主要包括以下子活动内容：

a) 制定产品或服务采购说明书；

[illegible]

[illegible]

[illegible]

地指导系统实施过程，该质量控制方案应确定系统实施各个阶段的质量控制目标，控制措施，工程质量

[redacted]

e) 集成实施：

[redacted]

[redacted]

[redacted]

## 7.4 管理措施的实现

### 7.4.1 安全管理制度的建设和修订

活动目标：

### 7.4.3 安全实施过程管理

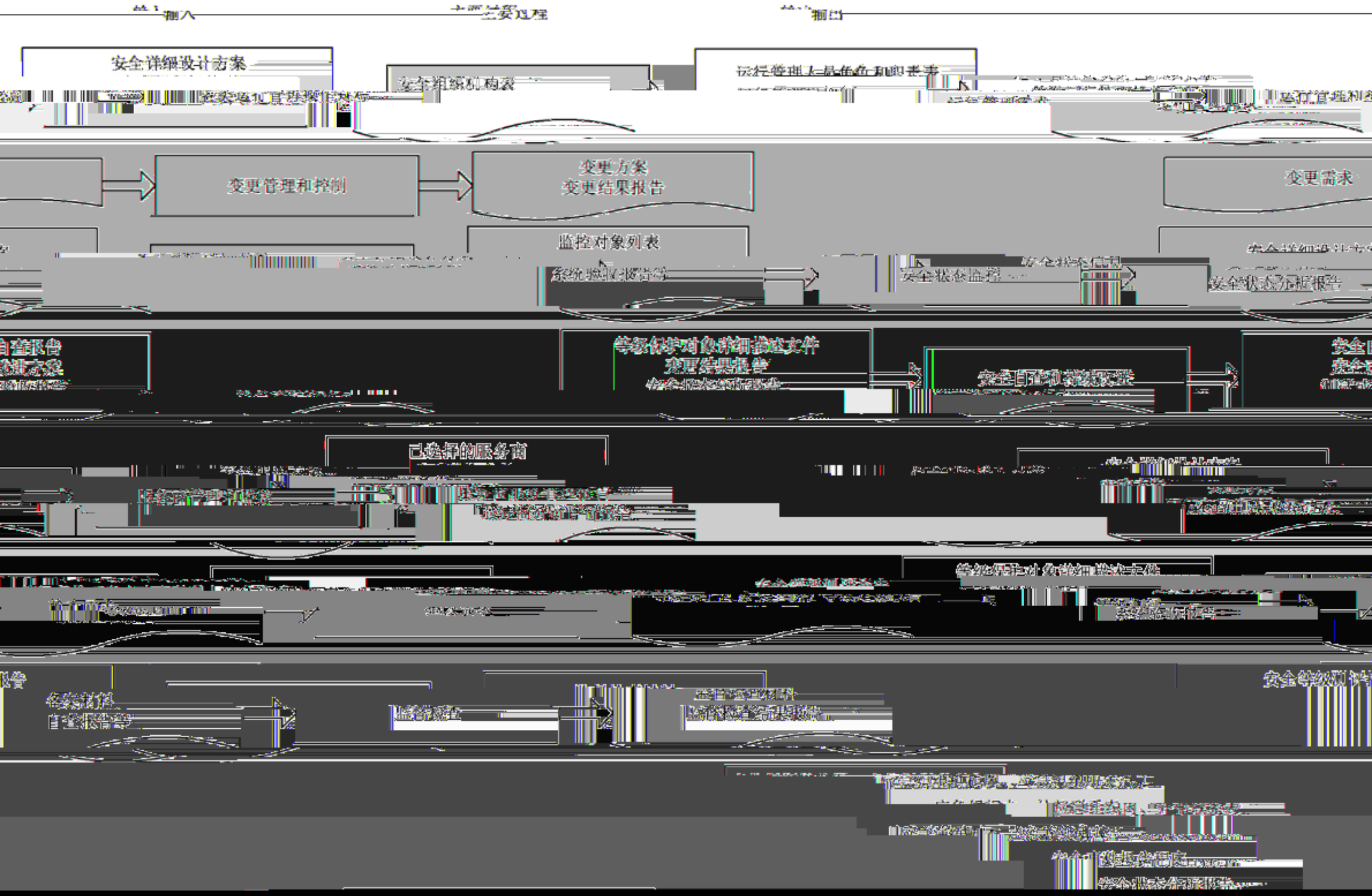
活动目标：

[redacted]

[redacted]

[redacted]

本标准关注安全运行与维护阶段的运行管理和控制、变更管理和控制、安全状态监控、安全自查和





8.3 变更管理和控制

8.3.1 变更需求和影响分析

活动目标：

活动描述：

参与角色：运营、使用单位；

活动输入：变更需求；

活动描述：

本活动主要包括以下子活动内容：

更的必要性和可行性。

b） 变更影响分析

对运行与维护过程中的变更可能引起的后果进行判断和分析、确定可能产生的影响大小、确定进行变更的先决条件和后续活动等。

c） 明确变更的类别

[illegible]

[illegible]

更方案

[illegible]

[illegible]

[illegible]

b) 形成监控对象列表

[illegible]根据确定的监控对象，分[illegible]

[illegible]

### 8.4.2 监控对象状态信息收集

活动目标：

[illegible]

参与角色：运营、使用单位。

活动输入：监控对象列表。

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

### 8.4.3 监控状态分析和报告

活动目标：

通过对安全状态信息进行分析，及时发现安全事件或安全变更需求，并对其影响程度和范围进行分析，形成安全状态结果分析报告。

参与角色：运营、使用单位。

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]对安全状态信息进行分析，及时发现验情、隐患或安全事件，并记录这些安全事件，分析其发展趋势；

b) 影响分析

根据对安全状况变化的分析，分析这些变化对安全的影响，通过判断他们的影响决定是否有必要作响应。

c) 形成安全状态分析报告

根据安全状态分析和影响分析的结果，形成安全状态分析报告，上报安全事件或提出变更需求。

[illegible]

## 8.5 安全自查和持续改进

### 8.5.1 安全状态自查

活动目标：

8.5.2 改进方案制定

8.5.3 安全改进实施

活动目标：

保证原型安全改进方案实现各项补充安全措施，并确保原有的技术措施和管理措施与各项补充的安全措施一致有效地工作。

本活动主要包括以下子活动内容：

a) 主安全方案实施控制

见 7.4.3。

b) 安全措施测试与验收

见 7.5.2。

c) 配套技术文件管理制度的修订

根据安全改进方案实施和落实各项补充的安全措施后，要编制和修订各类相关的技术文件和管理制度。

监控

8.8 服务商管理和

8.8.1 服务商选择

活动目标：

——服务商可能的恶意行为；

——服务商服务能力及行业经验；

——物理访问、信息资料丢失、系统

越权访问、误操作等。

c) 服务商管理总结

## 服务商管理

8.6.2

活动目标：

参与角色：

活动输入：

活动描述：

本活动主要包括以下子活动内容：

a） 人员管理

[illegible]

[illegible]

[illegible]

e) 服务过程中，服务商如因正当理由需要调整、变更人员的，应提前通知使用单位，做好工作交接，并获得使用单位同意后方可进行。

[illegible]

[illegible]

[illegible]

a） 建立应急组织

按照应急救援的需要，建立应急组织。应急组织一般分为五个核心应急功能机构，即指挥、行动、策划、后勤和财务。

b） 明确应急工作职责

[illegible]

员、职责和权限。

c） 安全事件分类分级

[illegible]

8.9.2 应急监测与响应

活动目标：

[illegible]

活动描述：

[illegible]

c) 安全事件上报和共享

根据安全状态分析和影响分析的结果，分析可能发生的安全事件，明确安全事件等级、影响程度以

[redacted]

[redacted]

[redacted]



# 附 录 A
（资料性附录）
主要过程及其活动和输入输出

等级保护对象实施网络安全等级保护工作的主要过程及其活动和输入输出见表 A.1。

表 A.1 等级保护对象实施网络安全等级保护工作的主要过程及其活动和输入输出

表 A.1（续）

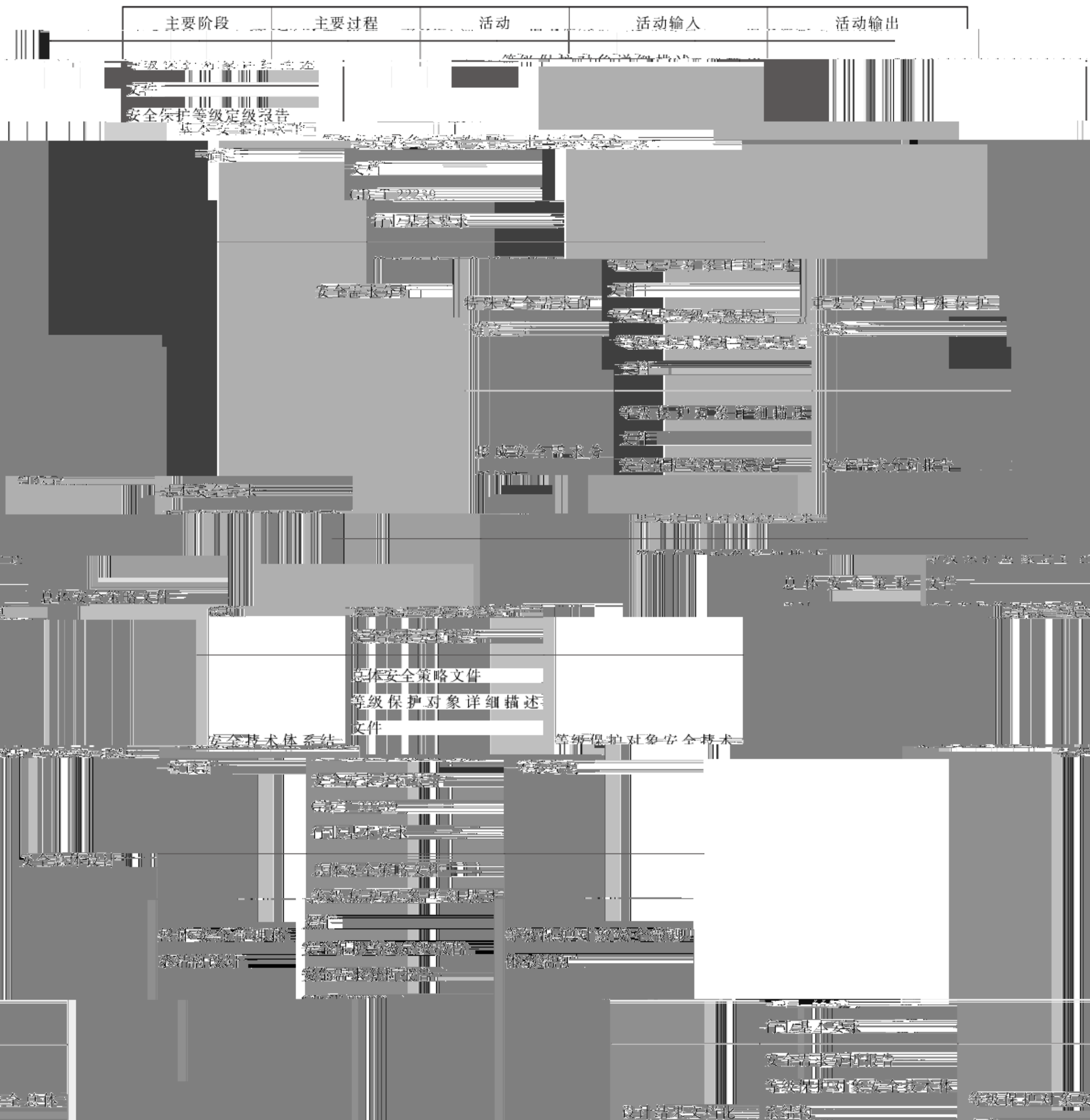

主要阶段
主要过程
活动
活动输入
活动输出
安全保护等级定级报告
GB/T 22239
行业基本要求
专家评审
安全需求分析
安全技术体系结
总体安全策略文件
等级保护对象详细描述文件
安全技术体系结
GB/T 22239
行业基本要求
总体安全策略文件
等级保护对象详细描述文件
安全技术体系结构设计
等级保护对象安全技术
设计
GB/T 22239
行业基本要求
安全技术设计报告
等级保护对象安全技术体系结构
等级保护对象安全管理体系结构

表 A.1（续）

| 主要阶段 | 主要过程 | 活动 | 活动输入 | 活动输出 |
| --- | --- | --- | --- | --- |
| | | 安全建设工程确定 | 等级保护对象安全建设项目列表（含安全建设内容） | 等级保护对象安全新建设备全清设目表 |
| | | 总体安全规划 | 规定 | 安全建设项目 |
| | | 形成安全建设项目规划 | 等级保护对象安全总体方案 | 等级保护对象分阶段安全建设规划 |
| | | 安全总体方案 | 安全建设项目规划 | 技术指施实现点 |
| | | 技术指施实现方案 | 各类信息技术产品和网络 | 设计 |
| | | 安全设计 | 技术指施实现方案 | 网络安全和安全机制等方 |
| | | 安全管理制度 | 安全管理机构 | 安全设计方案 |
| | | 安全设计方案评审 | 安全设计方案 | 评审意见 |

表 A.1（续）

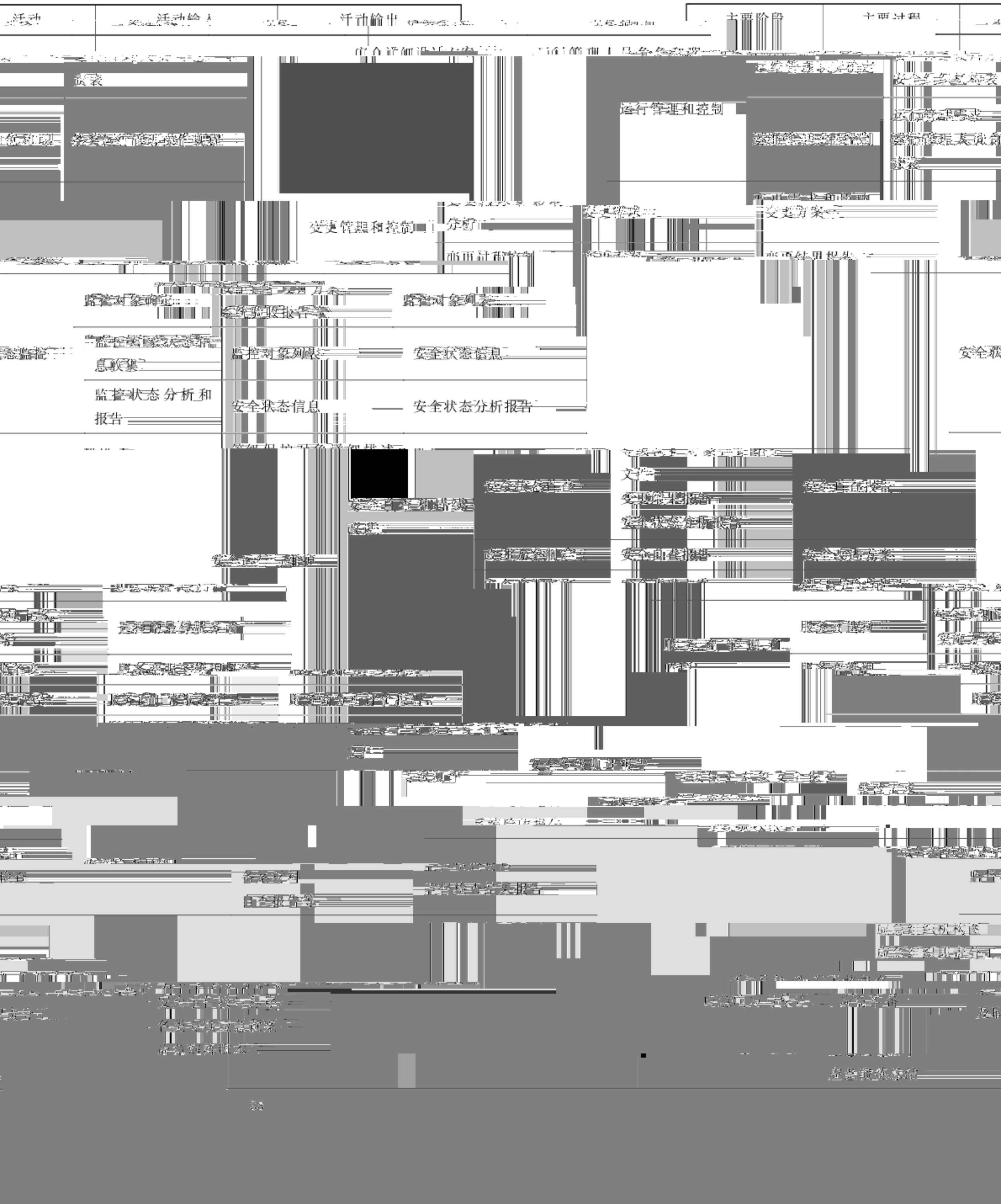


表 A.1（续）

| 主要阶段 | 主要过程 | 活动 | 活动输入 | 活动输出 |
| --- | --- | --- | --- | --- |
| | | 网络流量，日志信息，性能信息等 | | |
| | | | | |
| | | | | |
| | |

中华人民共和国
国家标准
信息安全技术
网络安全等级保护实施指南

GB/T 25058—2019

中国标准出版社出版发行
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019年7月第一版
*
书号:155066·1-63192

版权专有 侵权必究