ICS 35.040
L 80

GB/T 25058—2019
代替 GB/T 25058—2010

信息安全技术

护实施指南

规等要合管数

y technology—

ed protection of cybersecurity

Information securit

Implementation guide for classifi

2019-08-30发布

2020-03-01实

国家市场监督管理总局
中国国家标准化管理委员会

目　　次

前言 …… V
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　基本要求 …… 1
4.1　基本原则 …… 1
4.2　角色和职责 …… 2
4.3　实施的基本流程 …… 2
5　等级保护对象定级与备案 …… 4
5.1　定级与备案阶段的工作流程 …… 4
5.2　行业/领域定级工作 …… 4
5.3　等级保护对象定级 …… 5
5.3.1　对象重要性赋值 …… 5
5.3.2　定级对象确定 …… 6
5.4　安全保护等级确定 …… 7
5.4.1　定级、审核和批准 …… 7
5.4.2　形成定级报告 …… 8
5.5　定级结果备案 …… 8
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　总体安全需求分析报告 …… 10
6.3　总体安全设计 …… 10
6.4　总体安全规划 …… 11
6.5　形成安全建设项目规划 …… 11
7　安全设计与实施 …… 11
7.1　安全设计与实施阶段的工作流程 …… 11
7.2　安全方案详细设计 …… 12

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 设计输出的文档化 …… 17
7.3 技术措施的实现 …… 18
7.3.1 网络安全产品实施服务要求 …… 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 系统验收 …… 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
7.4.2 [illegible] …… 22
7.4.3 [illegible] …… 22
8 安全运行与维护 …… 23
8.1 安全运行与维护阶段的基本流程 …… 23
8.2 安全监理和控制 …… 23
8.2.1 运行管理过程控制 …… 23
8.2.2 运行管理过程检查 …… 24
8.3 变更管理和控制 …… 24
8.3.1 [illegible] …… 24
8.3.2 变更实施过程控制和检查 …… 25
8.4 安全状态监控 …… 25
8.4.1 监控对象确定 …… 25
8.4.2 监控对象状态信息收集 …… 26
8.4.3 监控状态分析和报告 …… 26
8.5 安全状态审查和持续改进 …… 26
8.5.1 安全状态审查 …… 26
8.5.2 改进方案制定 …… 27
8.5.3 安全改进实施 …… 27
8.6 [illegible] …… 28
8.6.1 [illegible] …… 28
8.6.2 服务监督 …… 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
8.9.2 [illegible] …… 31
8.9.3 [illegible] …… 32
9 定级对象终止 …… 32
9.1 定级对象终止所涉及的[illegible] …… 32
9.2 [illegible] …… 33

5.2 设备迁移或库存 22

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/T 22239—信息安全技术 网络安全等级保护基本要求

GB/T 25069—信息安全技术 术语

GB/T 28448—信息安全技术 网络安全等级保护测评要求

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。安全等级保护实施过程中应遵循以下基本原则：

a) 自主保护原则

等级保护对象运营、使用单位及其主管部门按照国家相关法规和标准，自主确定等级保护对象的安全保护等级，自行组织实施安全保护。

b) 重点保护原则

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，重新确定定级对象 [illegible]

4.2 角色和职责

等级保护对象实施网络安全等级保护过程中涉及的各类角色和职责如下：

a) 等级保护管理部门 [illegible]

b) 主管部门 [illegible]

c) 网络运营者 [illegible]

d) 网络安全服务机构 [illegible]

e) 网络安全等级测评机构 [illegible]

f) 网络安全产品供应商

负责按照国家网络安全等级保护的管理规范和技术标准，开发符合等级保护相关要求的网络安全产品，接受安全测评；按照等级保护相关要求销售网络安全产品并提供相关服务。

4.3 实施的基本流程

[illegible]

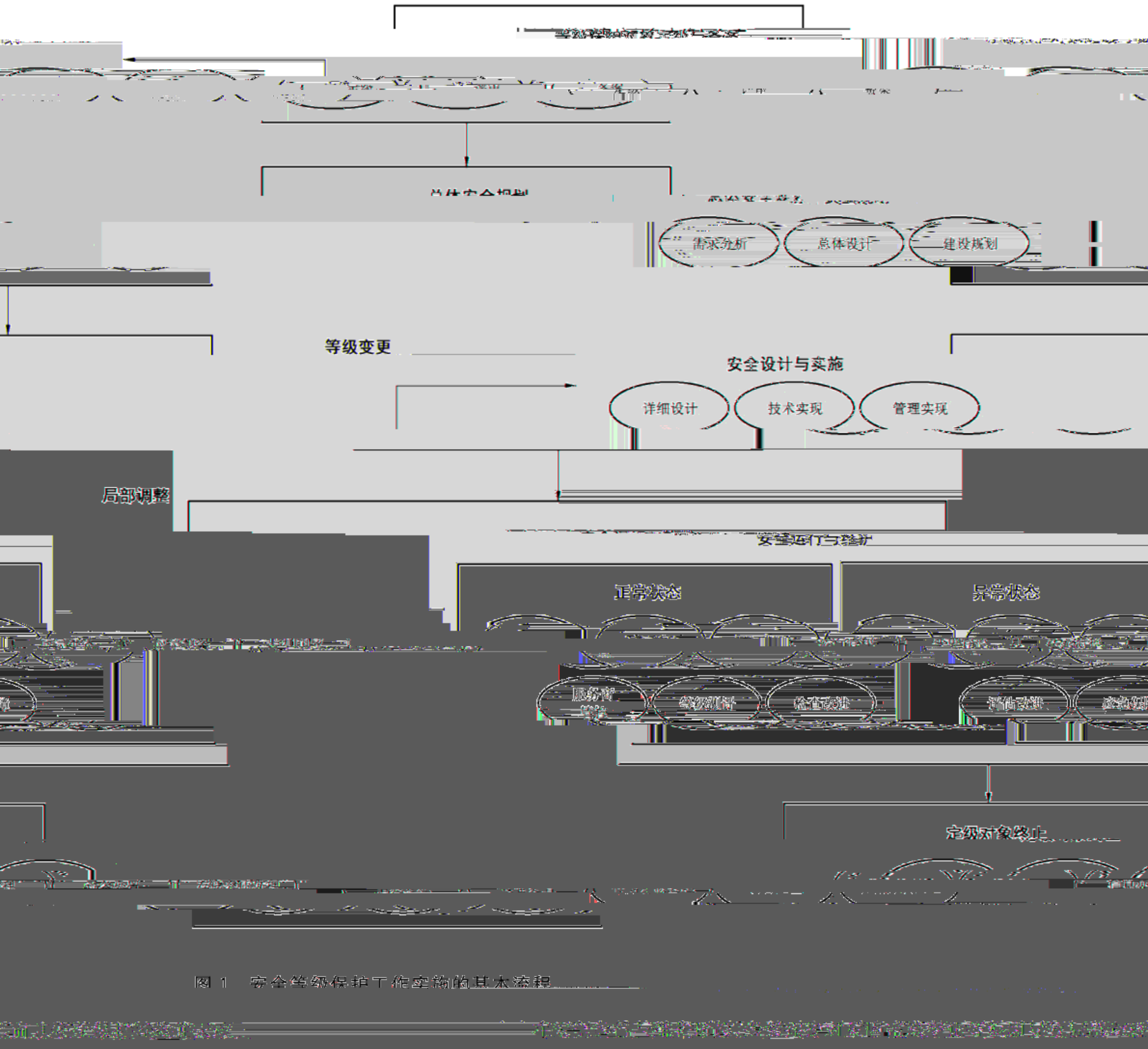


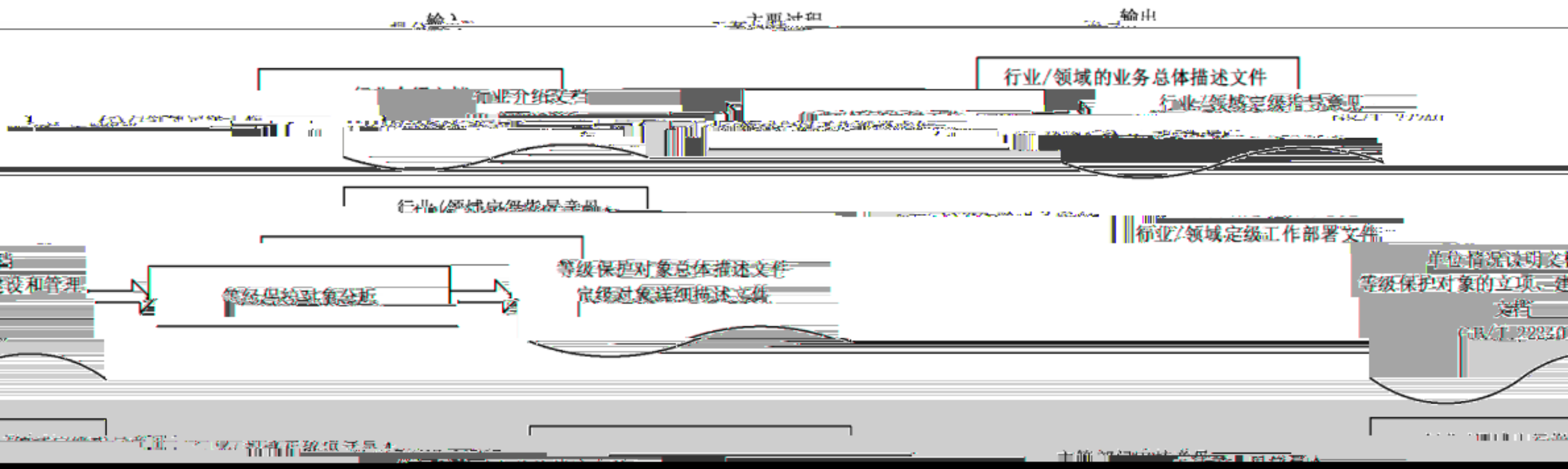
图 1　安全等级保护工作实施的基本流程

3

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

对信息进行综合分析和整理，分析单位的主要社会功
依赖的等级保护对象，整理等级保护对象处理的业务及
领域定级指导意见的还应依据行业/领域定级指导意

主管部门可调整本行业/领域重要级指导意见，并统一部署各行业/领域的定级

管部门应对下属单位的定级结果进行审核，指导

5.3 等级保护对象分析

5.3.1 对象重要性分析

活动目标：

通过收集了解有关等级保护对象的信息，并
能/职能及作用，确定履行主要社会功能/职能所
服务范围，最后依据分析和整理的内容，有行业

5

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总体描述文件应包含以下内容：

1) 等级保护对象概述；

2) [illegible]

3) 等级保护对象边界描述；

4) 网络拓扑；

5) 设备部署；

6) 支撑的业务应用的种类和特性；

7) 处理的信息资产；

8) 用户的范围和用户类型；

9) 等级保护对象的管理框架。

活动输出：等级保护对象总体描述文件。

5.3.2 定级对象确定

活动目标：

依据单位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/领域定级指导意见)，[illegible]

[illegible]

活动描述：

本活动主要包括以下子活动内容：

a) 划分方法的选择

[illegible]

b) 等级保护对象划分

[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。

工业控制系统主要包括现场采集/执行、现场控制、过程控制和生产管理等特征要素，其中现场采集/执行、现场控制和过程控制等要素应作为一个整体对象定级，各要素不单独定级；生产管理要素宜单独定级。对于大型工业控制系统，可以根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。

采用移动互联技术的等级保护对象主要包括移动终端、移动应用和无线网络等特征要素，可作为一个整体独立定级或与相关联业务系统一起定级，各要素不单独定级。

c) 定级对象详细描述：

在对等级保护对象进行划分并确定定级对象后，应在等级保护对象总体描述文件的基础上，进一步增加定级对象的描述，准确描述一个大型等级保护对象中包括的定级对象的个数。

进一步的定级对象详细描述文件应包含以下内容：

1) 相关的安全责任部门；
2) 每个定级对象的概述；
3) 每个定级对象的边界；
4) 每个定级对象的设备部署；
5) 每个定级对象支撑的业务应用及其处理的信息资产类型；
6) 每个定级对象的服务范围和用户类型；
7) 其他内容。

活动输出：定级对象详细描述文件。

5.4 安全保护等级确定

5.4.1 定级、审核和批准

活动目标：

按照国家有关管理规范和定级标准，确定定级对象的安全保护等级，并对定级结果进行评审、审核和批准，保证定级结果的准确性。

参与角色：主管部门，运营、使用单位。

活动输入：等级保护对象总体描述文件，定级对象详细描述文件。

活动描述：

运营、使用单位按照管理规范和定级标准，确定定级对象的安全保护等级，并对定级结果进行评审和审批。主要包括：

a) 定级对象安全保护等级初步确定

根据国家有关管理规范以及定级方法，确定定级对象的安全保护等级，编写定级报告。

b) 定级结果评审

运营、使用单位或主管部门（如果有）邀请信息安全专家或等级保护专家委员会对定级结果进行评审，并出具专家评审意见。

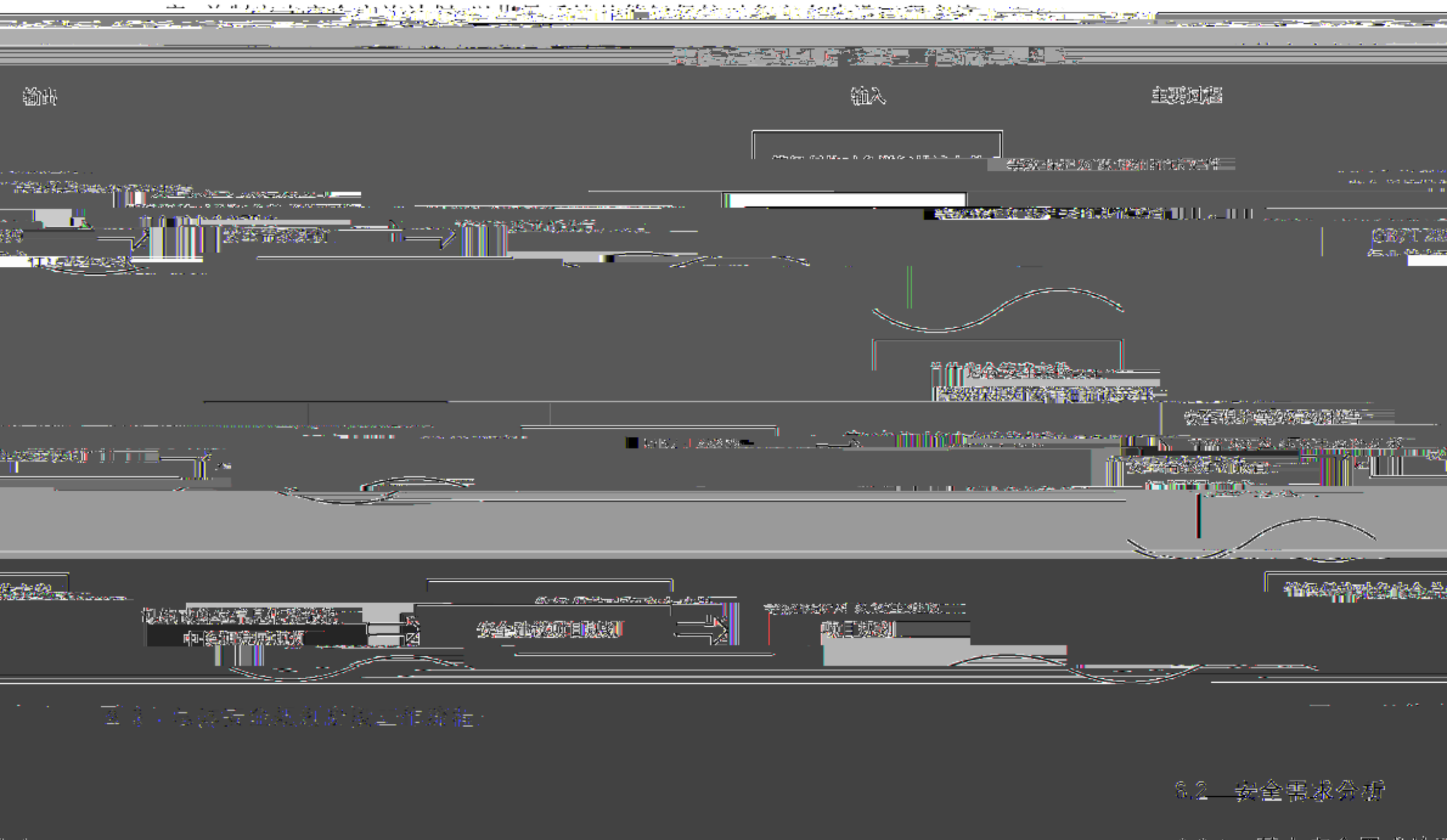
c) 定级结果审核批准

[illegible]

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：


输出
输入
主要过程
GB/T 25
5.3 等级保护安全建设工作流程
安全保护等级确定
安全规划设计
安全实施
安全运维
6.2 安全需求分析
6.2.1 基本安全需求的确定
为安全保护等级，提出等级保护对象的基本安全保护需求。
活动目标：
根据等级保护对象的
活动描述：
本活动主要包括以下子活动内容：

6.3 总体安全设计

6.3.1 总体安全策略设计

活动目标：

活动描述：

本活动主要包括以下子活动内容：

a) 确定安全方针

[illegible]

[illegible]

[illegible]

活动输出：总体安全策略文件。

系结构设计

6.3.2 安全技术体

活动目标：

[illegible]

[illegible]

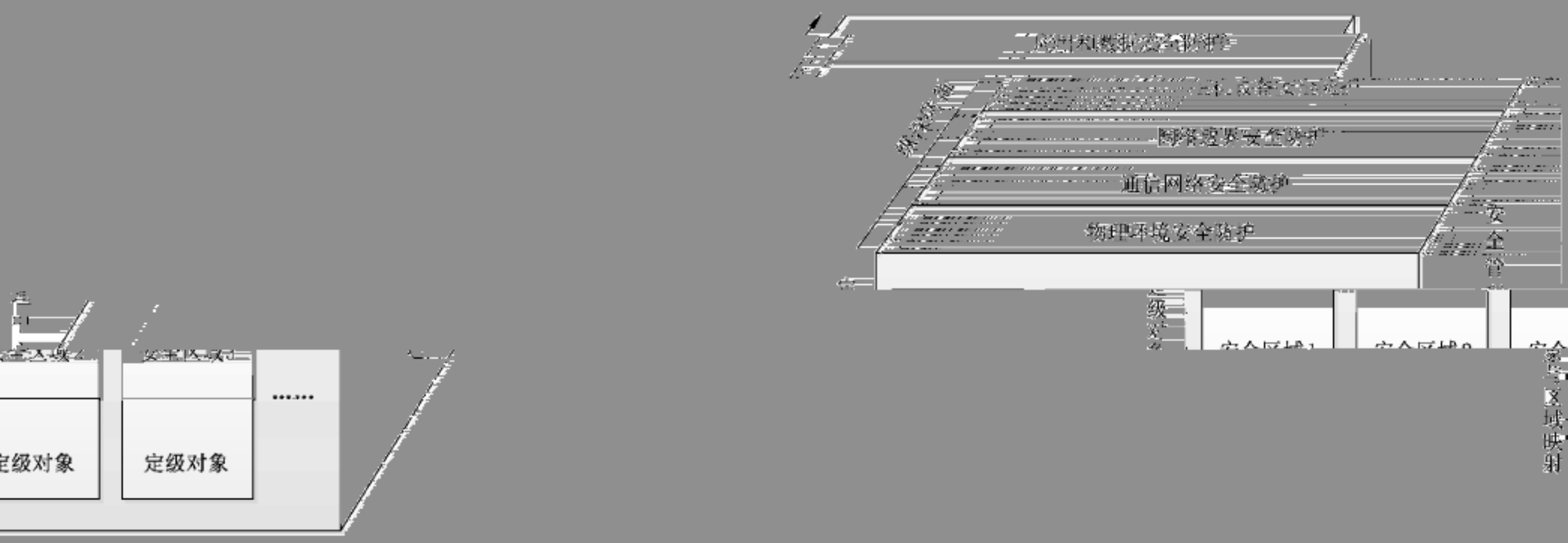
[illegible]

活动描述：

本活动主要包括以下子活动内容：

a) 设计安全技术体系架构

[illegible]



[illegible]

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：

a） 设计等级保护对象的安全管理体系框架

根据等级保护基本要求系列标准、行业基本要求、安全需求分析报告等，设计等级保护对象安全管

[redacted]

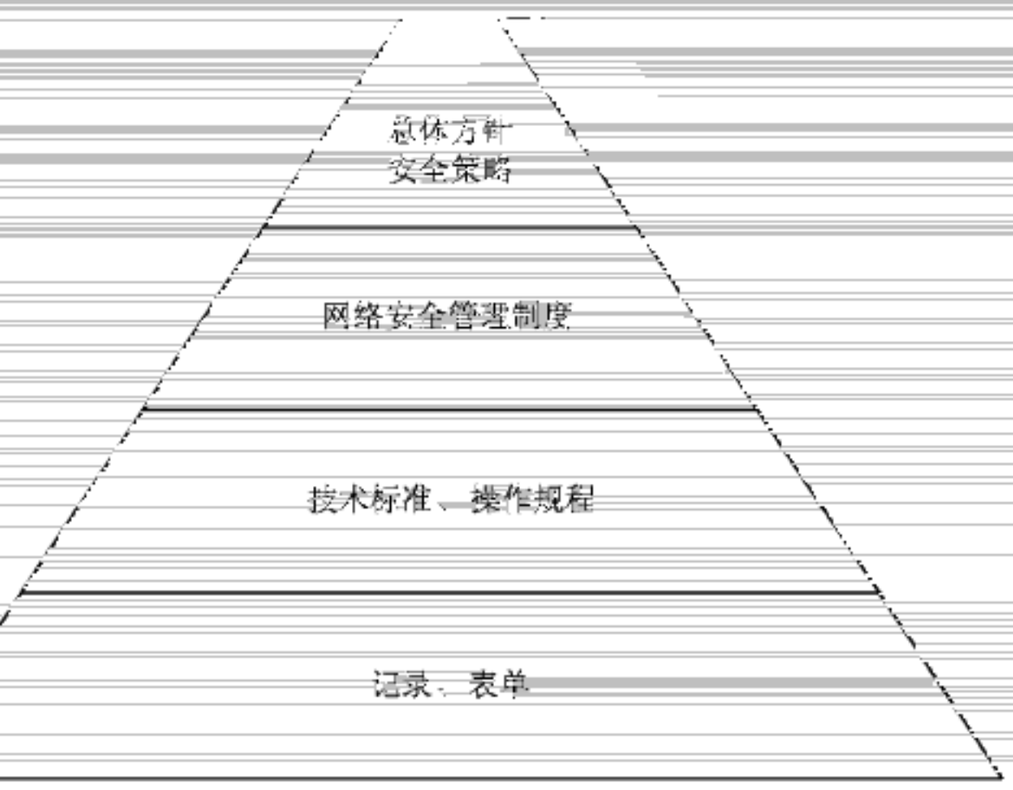


图 5 等级保护对象的安全管理体系框架

络安全的组织管理体系和对不同级别定级对象的安全管理职责

体安全策略文件、等级保护基本要求系列标准、行业基本要求和安全需求，提出机构的

[redacted]

b） 规定网

根据机构总

[redacted]

略等。

[redacted]

全管理策略等。

d） 规定不同级别定级对象机房及办公区等物理环境的安全管理策略

[redacted]

g) 规定不同级别定级对象安全事件处置和应急管理策略。

6.3.4 设计结果文档化

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：

总体安全目标；制定等级保护

，争取在短期内安全状况有大

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：

a) 确定主要安全建设内容

b)

c)

d)

e)

f)

g)

h)

6.4.3 形成安全建设项目规划

输入目标

活动描述

对等级保护对象分阶段安全建设目标、安全总体方案和安全建设内容等文档进行整理，形成等级保护对象安全建设项目规划。

输出信息：

a) 等级保护对象安全建设项目规划；

b)

c) 等级保护对象安全现状；

d) 信息化的中长期发展规划；

e) 等级保护对象安全建设的总体框架；

f) 安全技术体系建设规划；

g) 安全管理体系建设规划；



图6 安全设计与实施阶段的工作流程见图

7 安全详细设计

7.1 技术措施实现内容的设计

7.2

活动目标：

[illegible]

品共具体描述，并将安[illegible]构安全措施和要求落实到产品功能或物理形态上，理由能够实现的产品或组件

安全产品采购和安全控制的开发阶段具有依据。

品功能特征整理成文档，使得在网络安

参与角色：运营、使用单位、网络安全服务机构、网络安全产品供应商。

[illegible]

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

[illegible]

b） 安全功能要求的设计

7.2.3 设计结果的文档化

活动目标：

参与角色：运营、使用单位，网络安全服务机构。

a） 建设目标和建设内容；

b） 技术实现方案；

c） 网络安全产品或组件安全功能及性能要求；

d） 网络安全产品或组件部署；

e） 安全控制策略和配置；

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

[redacted]

本活动主要包括下列活动内容：

a） 制定产品或服务采购说明书

[redacted]

7.3.2 安全控制开发

活动目标：

[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：

[illegible]

本活动主要包括以下子活动内容：

a) 整体管理

整体管理需要在等级保护对象建[illegible]

[illegible]

b) 质量管理

在创建等级保护对象的过程中，要建立一个不断测试和改进质量的过程，在整个等级保护对象的[illegible]命周期中，通过测量、分析和修正活动，保证所完成目标和过程的质量。

c) 风险管理

为了识别、评估和减低风险，以保证工程活动和全部技术工作项目均得到成功实施。在整个等级保护对象建设过程中，风险管理要贯穿始终。

d) 变更管理

8 安全运行与维护

8.1 安全运行与维护阶段的工作流程

安全运行与维护是等级保护实施过程中确保等级保护对象正常运行的必要环节，涉及的内容较多，[illegible]

[illegible]



图 7　安全运行与维护阶段工作流程

8.2　运行管理和控制

8.2.1　运行管理职责确定

活动目标：

明确对运行管理活动或任务的角色划分，并授予相应的管理职责，至少划分为系统管理员、网络管理员、安全管理员和安全审计员。

参与角色：委托单位、使用单位、

活动描述：

本活动主要包括以下子活动内容：

b）授予管理权限：

活动目标：

活动描述：

本活动主要包括以下子活动内容：

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：

本活动主要包括以下子活动内容：

要性和可行性。

b) 变更影响分析

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

先决条件和后续活动等。

c) 明确变更的类别

8.3.2 变更过程控制

活动目标：

活动描述：

本活动主要包括以下子活动内容：

a) 变更内容审核和审批

对变更目的、内容、影响和

和地点以及人员权限进行审核，以确保变更合理、科学的流程，按照

案进行审批。

8.4 安全状态监控

8.4.1 监控对象确定

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) 安全关键点分析

对影响系统、业务安全性的关键要素进行分

b） 形成监控对象列表

监控对象列表。 根据确定的监控对象，分析监控的必要性和可行性、监控的开销和成本等因素，形成

集

8.4.2 监控对象状态信息收集

活动目标：

参与角色：运营、使用单位。

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。

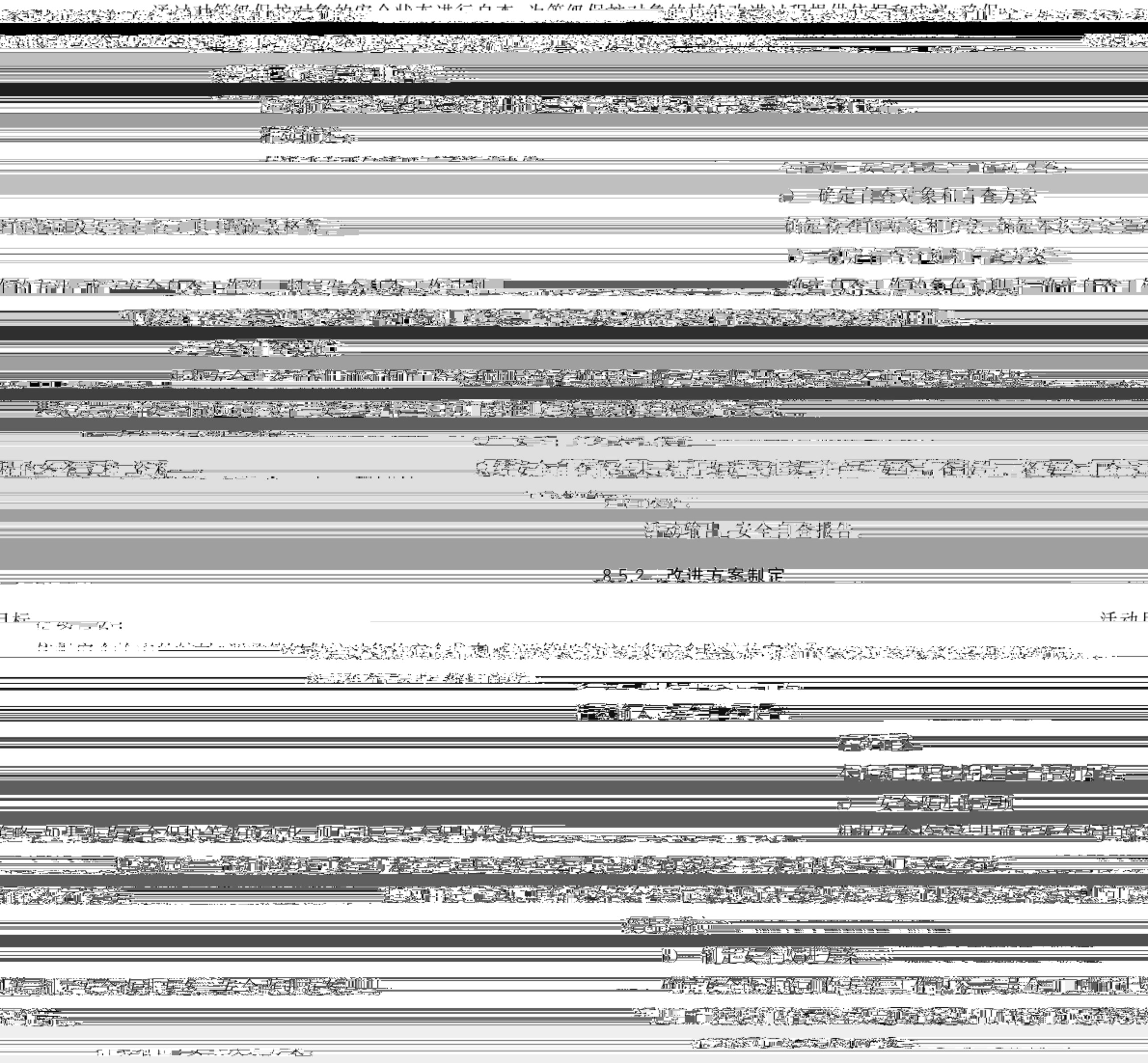
b） 影响分析

c） 形成安全状态分析报告

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：

保证按照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。

参与角色：运营、使用单位。

活动输入：安全改进方案。

活动描述：

本活动主要包括以下子活动内容：

a) 实施安全方案实施控制

见 7.4.3。

b) 安全措施测试与验收

见 7.3.4。

c) 把集成本文档管理范围的

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

按照安全设计方案实施和落实各

测试，验证各项安全

8.6 服务商管理和监控

8.6.1 服务商选择

活动目标：

设计、测评、建设资质的服务商，为后续的管理和监控奠定基础。

确定符合国家规定或行业规定的

参与角色：

活动输入：

活动指南：

a) 服务能力评

8.6.2 服务商管理

活动目标：

本活动主要包括以下子活动内容：

a） 人员管理

8.6.3 服务商监控

活动目标：

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。

活动输出:服务商分析评价报告 [illegible]

8.7 等级测评

[illegible]

活动目标:

[illegible]

[illegible]等级测评报告[illegible]确定整改需求。

[illegible]

8.8 监督检查

活动目标:

[illegible]

参与角色:主管部门、运营使用单位、等级保护管理部门。

活动输入:安全等级测评报告、备案材料、自查报告等。

活动描述:

[illegible]

活动输出:监督检查材料、监督检查结果报告。

8.9 应急响应与保障

8.9.1 应急准备

活动目标:

建立完善的应急组织体系,保证应急救援工作反应迅速、协调有序,通过分析安全事件的等级,在[illegible]

[illegible]

活动输入:[illegible]

活动描述:

[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]应急机构、应急专家组[illegible]应急管理的领导机构、办事机构、专项应急指挥机构、[illegible]责、职责和权限。

c) 安全事件分类分级

[illegible]

d) 确定[illegible]

[illegible]应急预案的对象。

e) 确定职责和运行机制方式

[illegible]

f) 制定应急预案的实施要求

[illegible]

8.9.2 应急监测与响应

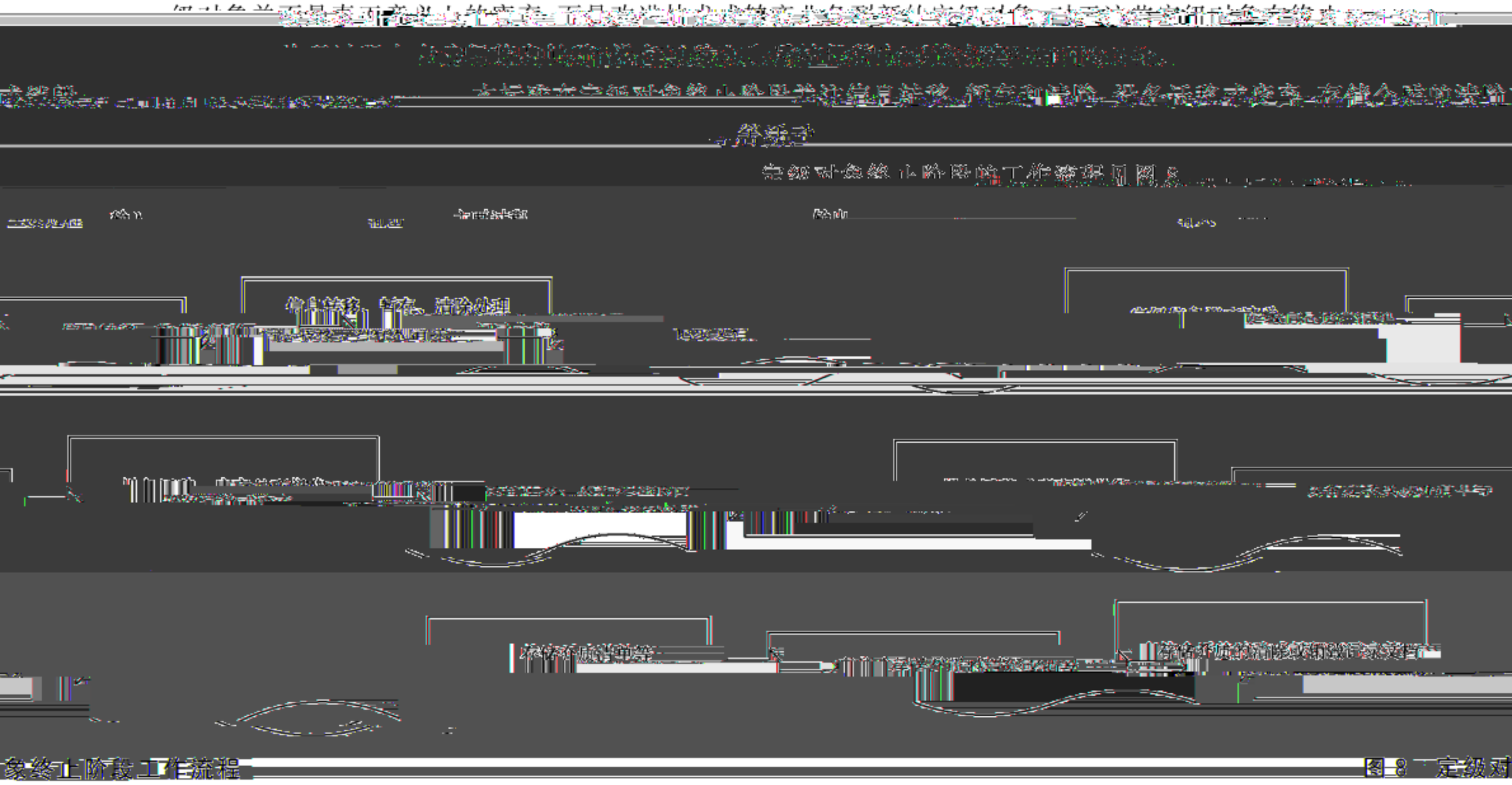
活动目标：

[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]



定级对象终止阶段工作流程

图 8

9.2 信息转移、暂存和清除

活动目标：

在定级对象终止处理过程中，对于可能会在

对象中的信息。

活动描述

根据要终止的定级对象的信息资产清单，识别重要信

活动目标：本活动的目标是确保信息系统终止后，迁移或废弃的设备内不包括敏感信息，对设备的处理方式应符合国家相关部门的要求。

参与角色：运营、使用单位。

活动输入：设备迁移或废弃清单等。

活动描述：

本活动主要包括以下子活动内容：

a) 软硬件设备识别

根据要终止的定级对象的设备清单，识别要被迁移或废弃的硬件设备、所处的位置以及当前的状态等，输出需要迁移或废弃的设备清单。

b) 制定硬件设备处理方案

[illegible]，包括重用设备、废弃设备、敏感信息清除方法等。

c) 处理方案审批

包括重用设备、废弃设备、敏感信息清除方法等的设备处理方案应经过主管领导审查和批准。

d) 设备处理和记录

[illegible]

活动输出：[illegible]

9.4 存储介质的清除或销毁

活动目标：本活动的目标是通过采用合理的方式对计算机介质（包括磁带、磁盘、打印结果和文档）进行信息清除或销毁处理，防止介质内的敏感信息泄露。

参与角色：运营、使用单位。

活动输入：存储介质清单等。

活动描述：

本活动主要包括以下子活动内容：

a) 识别要清除或销毁的介质

根据要终止的定级对象的存储介质清单，识别载有重要信息的存储介质、所处的位置以及当前状态等，输出需要进行清除或销毁的存储介质清单。

b) 确定存储介质处理方法和流程

根据存储介质所承载信息的敏感程度确定对存储介质的处理方式和处理流程，[illegible]。

c) 处理方案审批

[illegible]

d) 存储介质处理和记录

[illegible]

活动输出：[illegible]

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

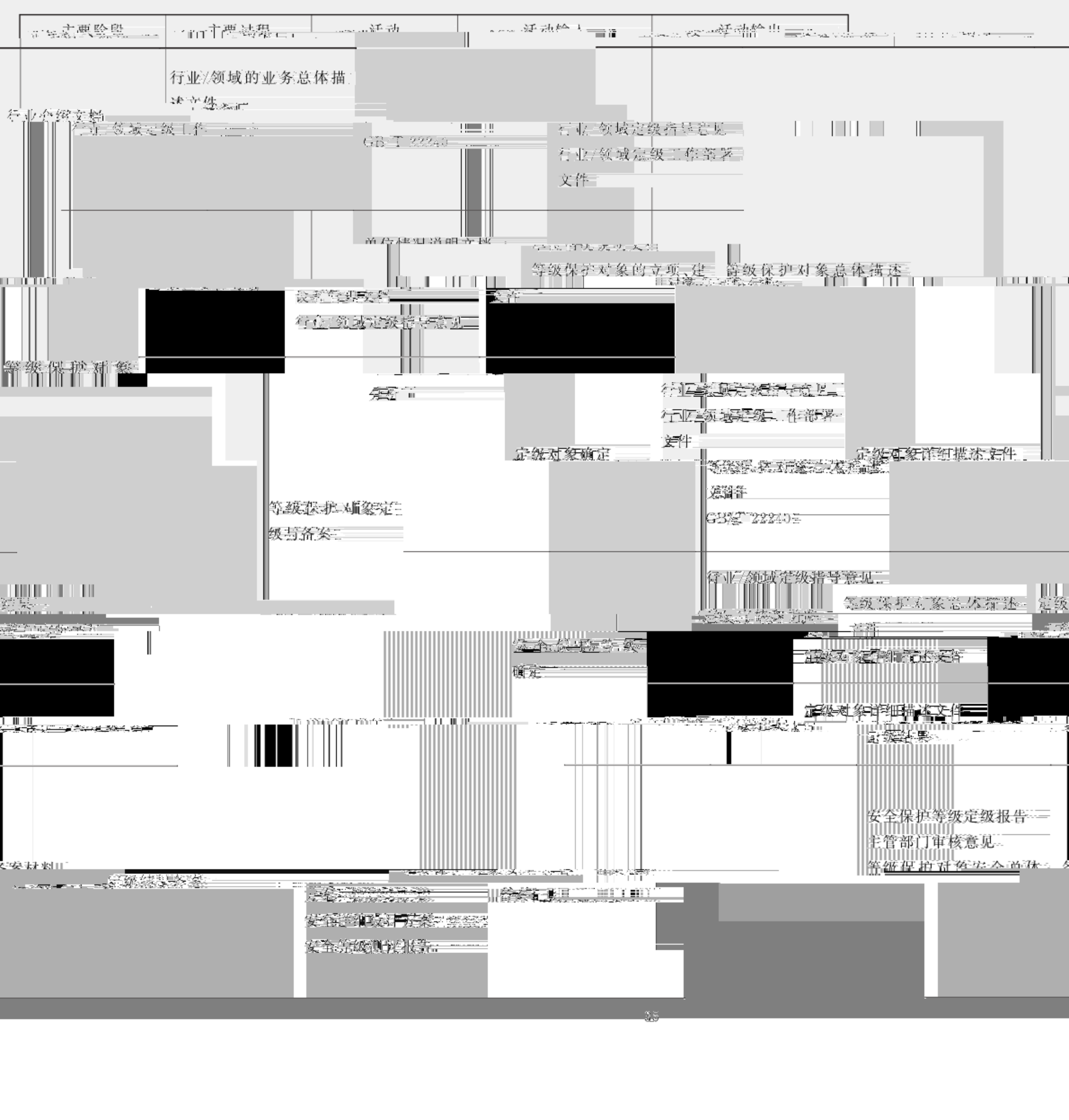


表 A.1（续）

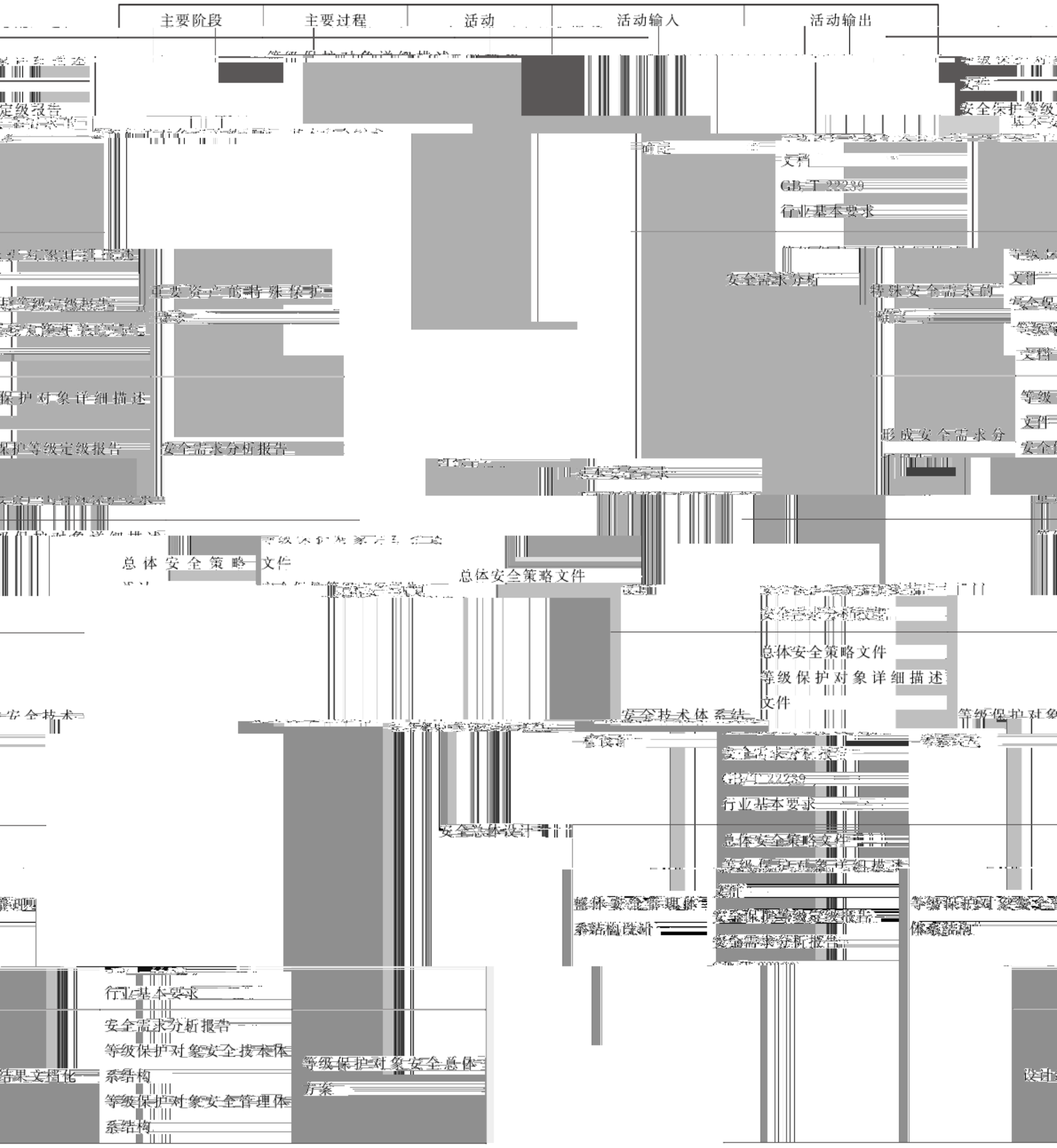

主要阶段
主要过程
活动
活动输入
活动输出
文件
安全保护等级
GB/T 22239
行业基本要求
安全需求分析
特殊安全需求
等级
文件
形成安全需求分
总体安全策略文件
等级保护对象详细描述
文件
安全技术体系结
安全总体设计
安全需求分析报告
GB/T 22239
行业基本要求
总体安全策略文件
等级保护对象详细描述
文件
安全保护等级定级报告
安全需求分析报告
总体安全策略文件
安全技术体系结
安全总体设计
GB/T 22239
行业基本要求
安全需求分析报告
等级保护对象安全技术体
系结构
等级保护对象安全管理体
系结构
等级保护对象安全总体
方案

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	等级保护对象安全总体方案 组织或单位信息化建设的安全建设目标	等级保护对象安全建设项目
建设项目总体安全规划	安全建设内容规划	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	安全建设项目列表（含安全建设内容）	总体安全规划 等级保护对象安全建设项目
		安全建设内容等	安全总体方案 安全建设项目列表	
	技术措施实现	网络安全产品和网络	技术措施实施方案	
		需采购的网络安全产品性能和关键技术要求		
		技术措施实现	技术措施实施方案	

表 A.1（续）

活动	活动输入	活动输出	主要阶段	主要过程
	监控对象确定	监控对象列表		
安全状态监控	监控对象状态信息收集	监控对象列表	安全状态信息	
	监控状态分析和报告	安全状态信息	安全状态分析报告	

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	
			总体应急预案	
定级对象终止		信息转移、暂存和清除	定级对象信息资产清单	信息转移、暂存、清除处理记录文档
		设备迁移或废弃	设备迁移或废弃清单等	设备迁移、废弃处理报告
				存储介质的清除或销毁

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
邮政编码：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

GB/T 25058-2019