ICS 35.040
L 80

GB/T 25058—2019
代替 GB/T 25058—2010

信息安全技术 网络安全等级保护实施指南

Information security technology—
Implementation guide for classified protection of cybersecurity

2020-03-01 实施　　2019-08-30 发布

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 …… V

1　范围 …… 1

2　规范性引用文件 …… 1

3　术语和定义 …… 1

4　等级保护实施概述 …… 1

4.1　基本原则 …… 2

4.2　角色和职责 …… 2

4.3　实施的基本流程 …… 4

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 …… 5

5.3　等级保护对象定级 …… 5

5.3.1　对象重要性描述 …… 6

5.3.2　定级对象确定 …… 7

5.4　安全保护等级确定 …… 7

5.4.1　定级、审核和批准 …… 8

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　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　安全保障体系框架设计 …… 11

6.3.3　基本安全措施和特殊安全措施 …… 12

6.3.4　设计结果文档化 …… 14

6.4　安全建设项目规划 …… 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 设计输出的文档化 …… 17
7.3 技术措施的实现 …… 18
7.3.1 为等保工程实施服务交底 …… 18
7.3.2 安全控制的开发 …… 18
7.3.3 安全控制集成 …… 19
7.4 系统验收 …… 20
7.4.1 管理措施的实现 …… 21
7.4.2 安全管理制度的建设和修订 …… 21
8 安全运行与维护
8.1 运行与维护阶段的工作流程 …… 22
8.2 变更和控制 …… 22
8.2.1 变更管理组织和职责 …… 23
8.2.2 变更管理过程控制 …… 24
8.3 变更前评估 …… 24
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 安全状态评估 …… 26
8.5.1 安全状态自查 …… 26
8.5.2 改进方案制定 …… 27
8.5.3 安全改进实施 …… 27
8.6 符合性检查 …… 28
8.6.1 检查准备 …… 28
8.6.2 检查实施 …… 29
8.6.3 检查结果 …… 30
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 应急监测与响应 …… 31
8.9.3 应急演练与改进 …… 32
9 定级对象终止 …… 32

8.2 设备迁移或库存 …… 33
9 …… 34
10 …… 34
附录A(规范性附录) 主要过程及其活动和输入输出 …… 35

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

GB/T 28448—信息安全技

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。

一）重点保护原则

根据等级对象的重要程度，业务特点，

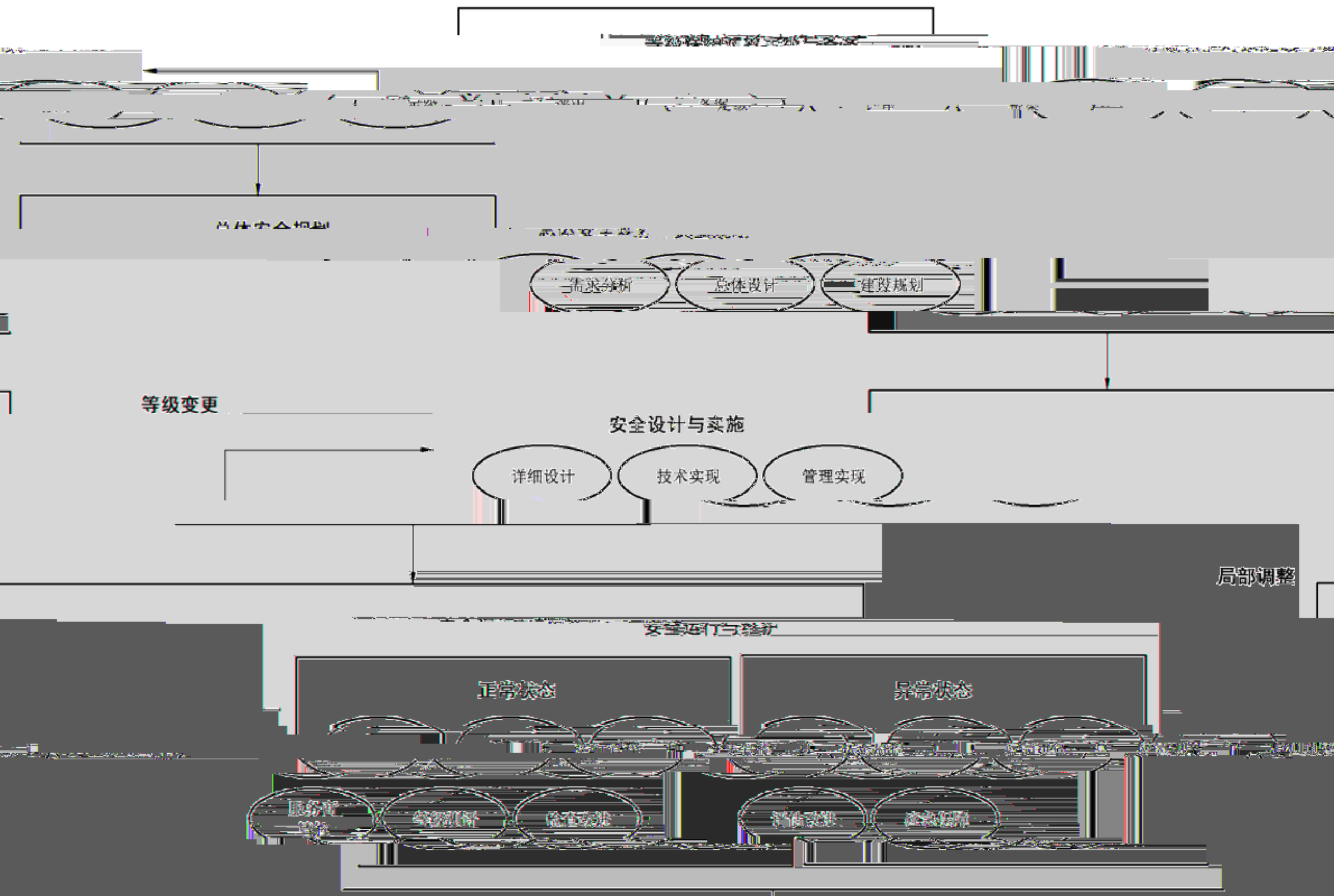
二）动态发展原则

三）整体保

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

4.2 角色和职责

4.3 实施的基本流程



保护工作实施的基本流程

图 1　安全等级

应从安全运行与维护阶段进入安全设计与实施环节，重新设计、开发和实施安全措施，直到满足等级保护的要求。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，确定变更后等级保护对象的安全保护等级，并与原有安全保护等级进行比较，针对变化部分进行调整，直至符合新的等级保护要求。

应与保障。

护过程中，发生安全事件时可能会发生应急响

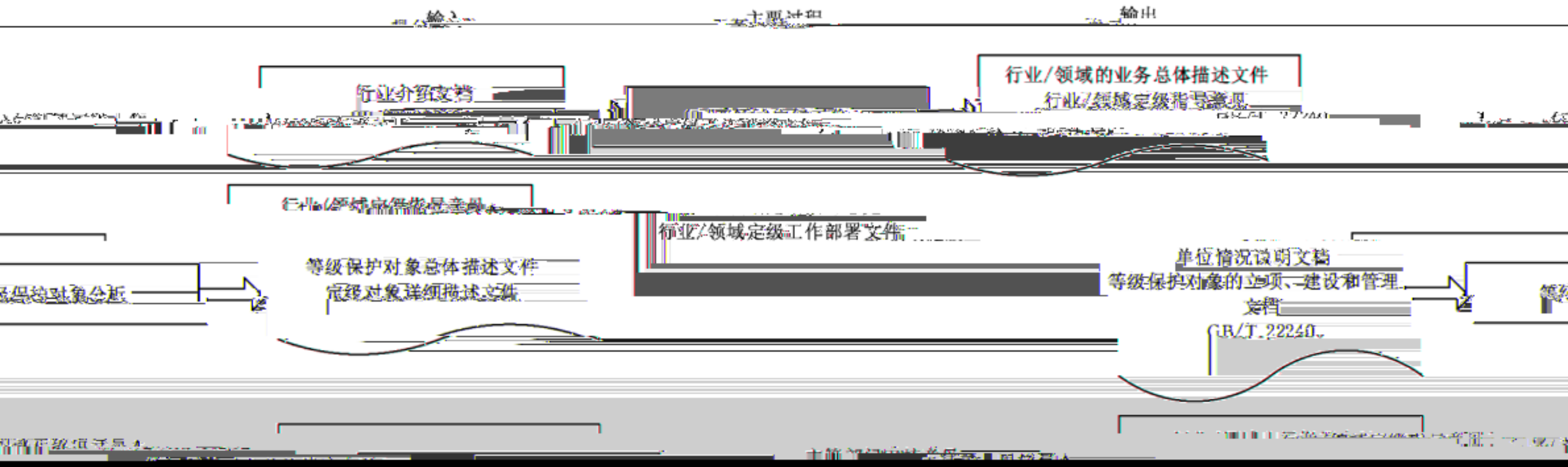
程中各个阶段的主要过程、活动、输入和输出见附录 A。

等级保护对象安全等级保护实施的基本

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

理，分析单位的主要社会功

等级保护对象处理的业务及

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，并对信息进行综合分析和整理

性程度。

g) 识别用户范围和用户类型。

[illegible]

b) 等级保护对象描述

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[illegible]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（在行业/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]

活动输入：

[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) 等级保护对象确定

[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。

[illegible]

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[illegible]

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：

[illegible]

活动输入：[illegible]

活动描述：

本活动主要包括以下子活动内容：

a) 定级对象安全保护等级初步确定

[illegible]

b) 定级结果审核

[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：

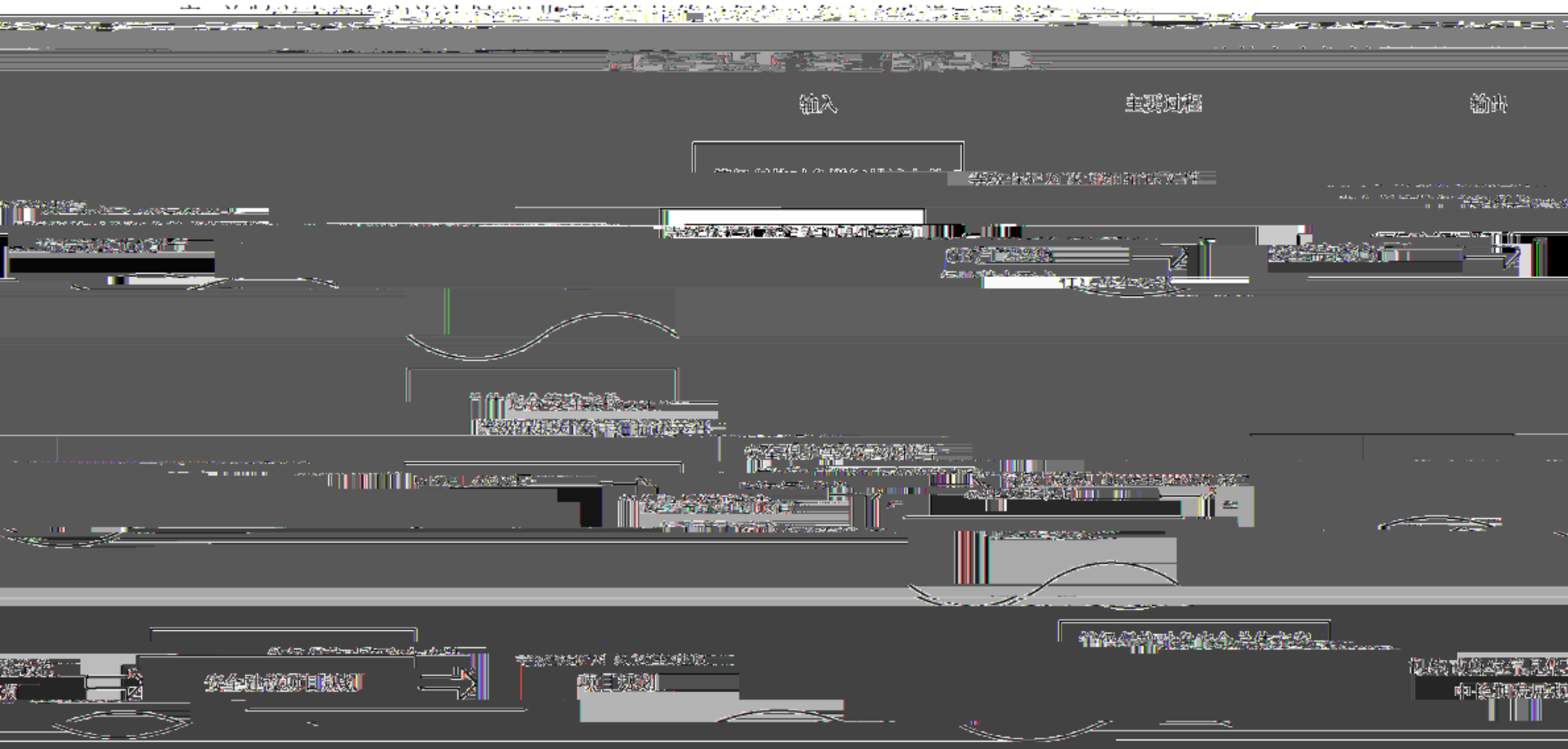


图 A.1 安全工程监理工作流程

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：

6.3 总体安全设计

6.3.1 总体安全策略设计

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

……

6.3.2 安全技术体系结构设计

活动目标：

……

活动描述：

本活动主要包括以下子活动内容：

a) 设计安全技术体系架构

……

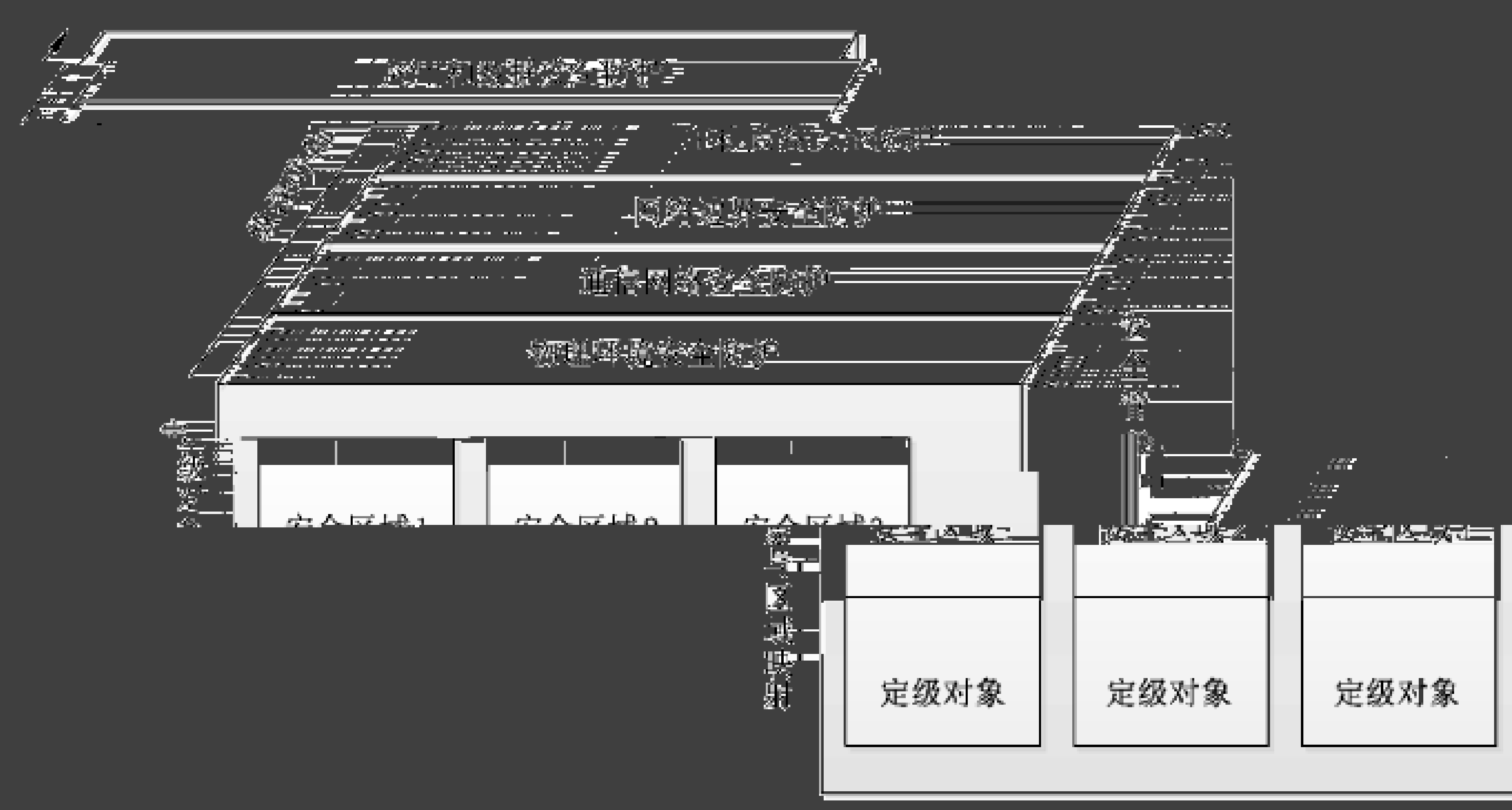


图4 等级保护对象安全技术……

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

[illegible]



图 5 等级保护对象的安全管理体系框架

b） 规定网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

根据机构总体安全策略文件、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

[illegible]

略等。

[illegible]

[illegible]

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

g) 规定不同级别定级对象安全事件外置和应急管理策略。

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：

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



设计与实施阶段的工作流程见图。

7.2 安全方案详细设计

7.2.1 技术措施实现内容的

活动目标：

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。

活动描述：

主要包括以下子活动内容：

a) 结构

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：

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]

在依据产品或服务采购说明书对候选产品或服务进行选择时，应综合考虑产品或服务的使用环境

[redacted]

7.3.2 安全控制的开发

活动目标：

[redacted]

活动描述：

本活动主要包括下列活动内容：

a） 安全措施需求分析

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[illegible]

[illegible]

c) [illegible]

[illegible]

[illegible]会影响到的系统能否安全运行。

e) 形成安全控制集成报告

应将安全控制集成过程相关内容文档化，并形成安全控制集成报告，其包含集成实施方案、质量控制[illegible]

[illegible]

活动输出：安全控制集成报告。

7.2.4 系统验收

活动目标：

[illegible]

[illegible]

活动输入：[illegible]

活动要求：

a) [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]文档。

d) 系统交付

在等级保护对象验收通过以后，要进行等级保护对象的交付，需要安全服务机构提交系统建设过程[illegible]

活动输出：[illegible]

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：

在等级保护对象定级、规划设计、实施过程中，对工程的质量、进度、文档和变更等方面的工作进行监督控制和科学管理[illegible]

[illegible]

[illegible]

a) 整体管理

[illegible]

b) 质量管理

在创建等级保护对象的[illegible]在整个等级保护对象的生[illegible]命周期[illegible]测量、分析和[illegible]务正常运行，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

[illegible]

e) 进度管理

[illegible]

f) 文档管理

[illegible]

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，包括安全运行与维护机构和安全运行与维护机制的建立，环境、资产、设备、介质的管理，网络、系统的管理[illegible]

[illegible]

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

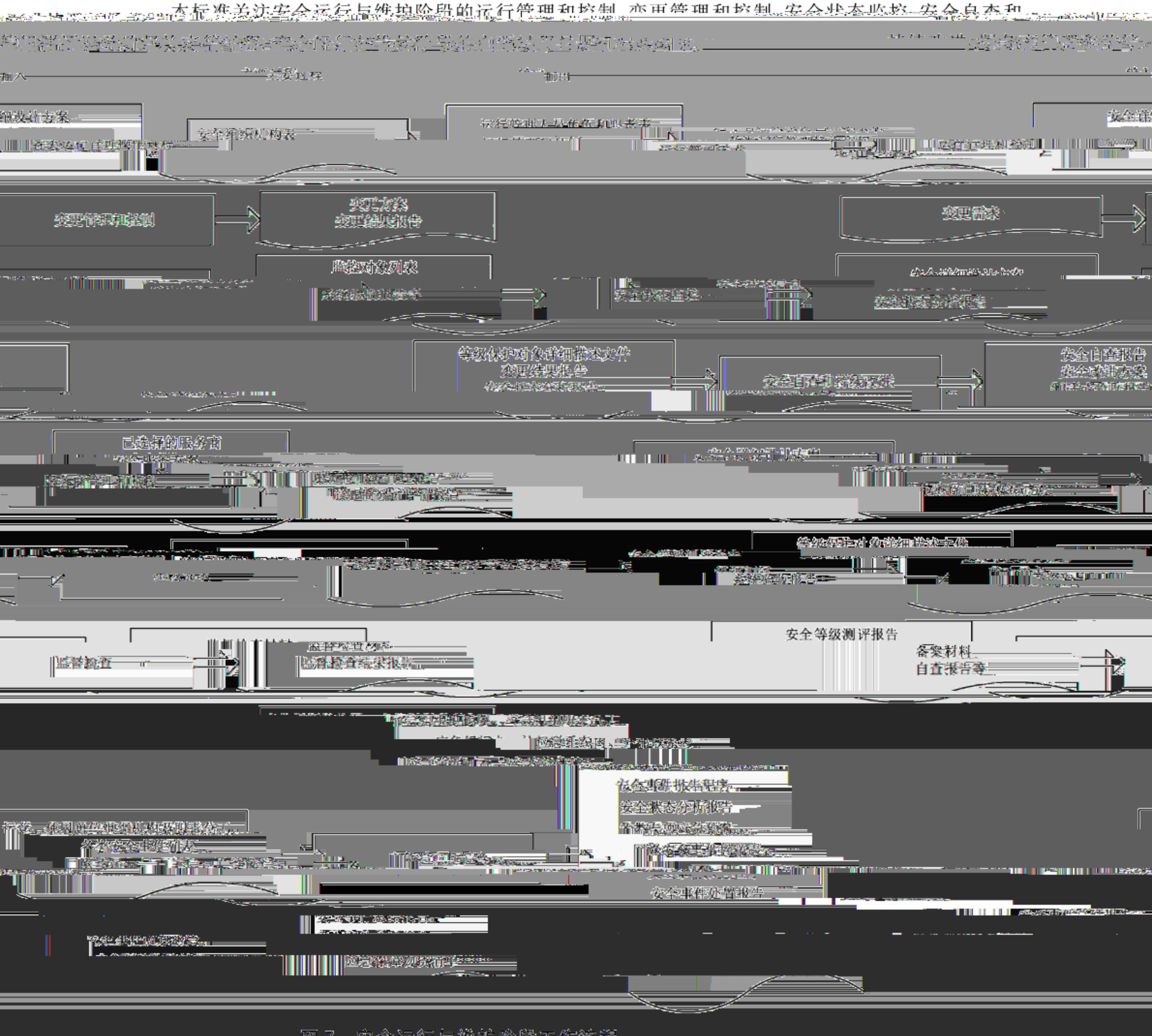


图 7 安全运行与维护阶段工作流程

6.6 运行管理和控制

6.6.1 运行管理职责确定

活动目标：

通过对运行管理活动或任务的角色划分，并授予相应的管理权限，确定实施运行管理的具体人员和职责，应至少划分为系统管理员、安全管理员和安全审计员。

参与角色：运营、使用单位。

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：

通过对运行与维护过程中的变更需求和影响的分析，来确定变更的类别，计划后续的活动。

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

[redacted]

8.3.2 变更过程控制

[redacted]

8.4 安全状态监控

8.4.1 监控对象确定

[redacted]

活动目标：

确定可能造成等级保护对象安全造成影响的因素以确定安全状态监控的对象；

参与角色：运营/使用单位；

活动输入：安全详细设计方案、系统验收报告等；

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析，确定安全状态监控的对象，这些对象可能包括防火

[redacted]

b) 形成监控对象列表

[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。

[illegible]

活动输入：监控对象列表。

[illegible]

活动描述：

本活动主要包括以下三个活动内容：

a) 状态信息采集

收集来自监控对象的各类状态信息，可能包括网络流量、日志信息、安全报警和性能状况等，或者是[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]

活动输入：安全状态信息。

活动描述：

本活动主要包括以下三个活动内容：

a) 趋势分析

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

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[illegible]

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：

保原有的技术措施和管理措施与各项补充的

参与角色：运营、使用单位。

活动输入：安全改进方案。

活动描述：

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
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) 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) 配合变更及相关管理

按照安全设计方案实施和落

8.6 服务商管理和监控

8.6.1 服务商选择

活动目标：

确定符合国家规定或行业规

参与角色：

活动输入：

活动描述：

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

——如因服务商人员原因，给使用单位或第三方造成人员人身伤害或财产损失的，服务商应承担赔偿责任。

——使用单位应督促服务商对服务人员开展培训及安全教育工作。

活动输出：服务商服务管理报告。

8.6.3 服务商监控

活动目标：

活动输入：服务商日常服务记录、安全服务方案。

活动描述：

本活动主要包括以下子活动内容：

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。

8.7 等级测评

活动目标：

[illegible]

活动描述：

[illegible]

8.8 监督检查

活动目标：

[illegible]

参与角色：主管部门、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：

等级保护管理部门按照国家网络安全等级保护、行业监管要求等对等级保护对象进行检查 [illegible]

[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、实 [illegible]

[illegible]

参与角色：主管部门、运营、使用单位。

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

[redacted]

c） 安全事件分类分级

[redacted]

8.9.2 应急监测与响应

活动目标：

[redacted]

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、影响程度以及传播途径等，形成安全状态分析报告和网络安全事件报送表，按照安全事件等级以及安全事件报告程序……

d) 安全事件处置

对于应启动应急预案的安全事件按照应急预案响应机制进行安全事件处置；对于未知安全事件的处置，应根据安全事件的等级，制定安全事件处置方案，包括安全事件处置方法以及应采取的措施等，并按照安全事件处置流程和方案对安全事件进行处置。

e) 安全事件总结和报告

对于已解决的安全事件……使安全事件得到解决……

活动输出：网络安全事件报送表、安全状态分析报告、安全事件处置报告。

8.9.3 后期评估与改进

活动目标：

对安全事件原因、处置过程进行调查分析，并根据分析结果进行责任认定及制定改进预防措施。

参与角色：运营、使用单位。

活动输入：安全事件报告程序、各类专项应急预案、安全事件处置报告。

活动描述：

本活动主要包括以下子活动：

b) 改进预防

根据网络安全事件调查评估报告，制定改进预防措施，修改相应应急预案，结合实际情况进行落实。

活动输出：安全事件调查评估报告、安全改进报告、应急预案。

8.9.4 应急保障

活动目标：

建立健全应急保障体系，实现应急预案保障工作科学化。

参与角色：运营、使用单位。

活动输入：总体应急预案、各类专项应急预案。

活动描述：

针对各类专项应急预案进行分析，制定应急预案执行所需要的人员、设备、数据、环境、交通运输、经费和……保障措施等。

活动输出：应急保障物资清单。

9 定级对象终止

9.1 定级对象终止阶段的工作流程

定级对象终止阶段是等级保护实施过程中的最后环节。当定级对象被转移、终止或废弃时，……

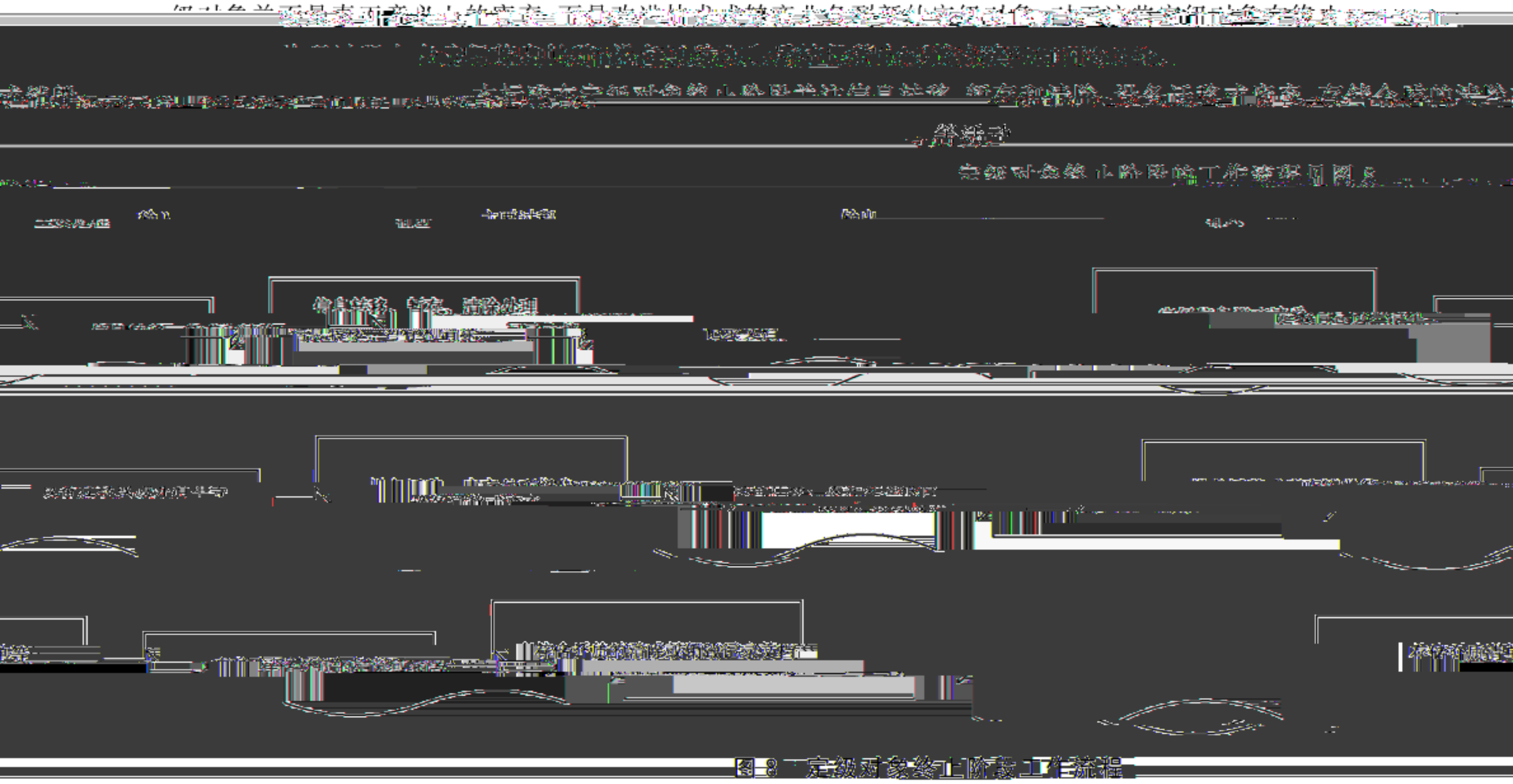


图 8 定级对象终止阶段工作流程

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，对于可能会在另外的定级对象中使用的信息采取适当的方法将其安

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，识别重要信息资产所处的

附 录 A
（规范性附录）
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

主要阶段	主要过程	活动	活动输入	活动输出
定级准备	行业/领域的业务总体描述	描述业务	行业/领域定级指导意见 行业/领域定级工作等级文件	行业/领域的业务总体描述文件
	等级保护对象的立项、建设或改造文件	描述等级保护对象	等级保护对象总体描述文件	等级保护对象总体描述文件
	行业/领域定级指导意见	确定定级对象	等级保护对象总体描述文件	等级保护对象确定文件
	等级保护对象总体描述文件	细化定级对象	等级保护对象确定文件	等级保护对象详细描述文件
	等级保护对象详细描述文件	初步确定等级	等级保护对象详细描述文件	等级保护对象安全保护等级定级报告
	等级保护对象安全保护等级定级报告	组织专家评审	等级保护对象安全保护等级定级报告	专家评审意见
	专家评审意见	主管部门审核	等级保护对象安全保护等级定级报告 专家评审意见	主管部门审核意见
	主管部门审核意见	备案	等级保护对象安全保护等级定级报告 主管部门审核意见 备案所需其他证明材料	备案证明
安全设计	安全保护等级定级报告 备案证明	总体安全规划	安全保护等级定级报告 备案证明	安全建设总体规划方案
	安全建设总体规划方案	设计安全方案	安全建设总体规划方案	安全设计方案
	安全设计方案	调整安全方案	安全设计方案 安全测评报告	安全设计方案
安全实施	安全设计方案	实施安全工程	安全设计方案	安全工程实施报告
	安全工程实施报告	工程监理	安全工程实施报告	工程监理报告
	安全工程实施报告 工程监理报告	工程测试验收	安全工程实施报告 工程监理报告	工程测试验收报告
安全测评	安全保护等级定级报告 安全设计方案 安全工程实施报告 工程测试验收报告	测评准备活动	安全保护等级定级报告 安全设计方案 安全工程实施报告 工程测试验收报告	测评方案
	测评方案	方案编制活动	测评方案	测评方案
	测评方案	现场测评活动	测评方案 安全设计方案	现场测评结果记录 安全问题清单
	现场测评结果记录 安全问题清单	报告编制活动	现场测评结果记录 安全问题清单	安全等级测评报告
安全运维	安全等级测评报告 安全整改建议	运维管理	安全等级测评报告 安全整改建议	运维记录

表 A.1（续）

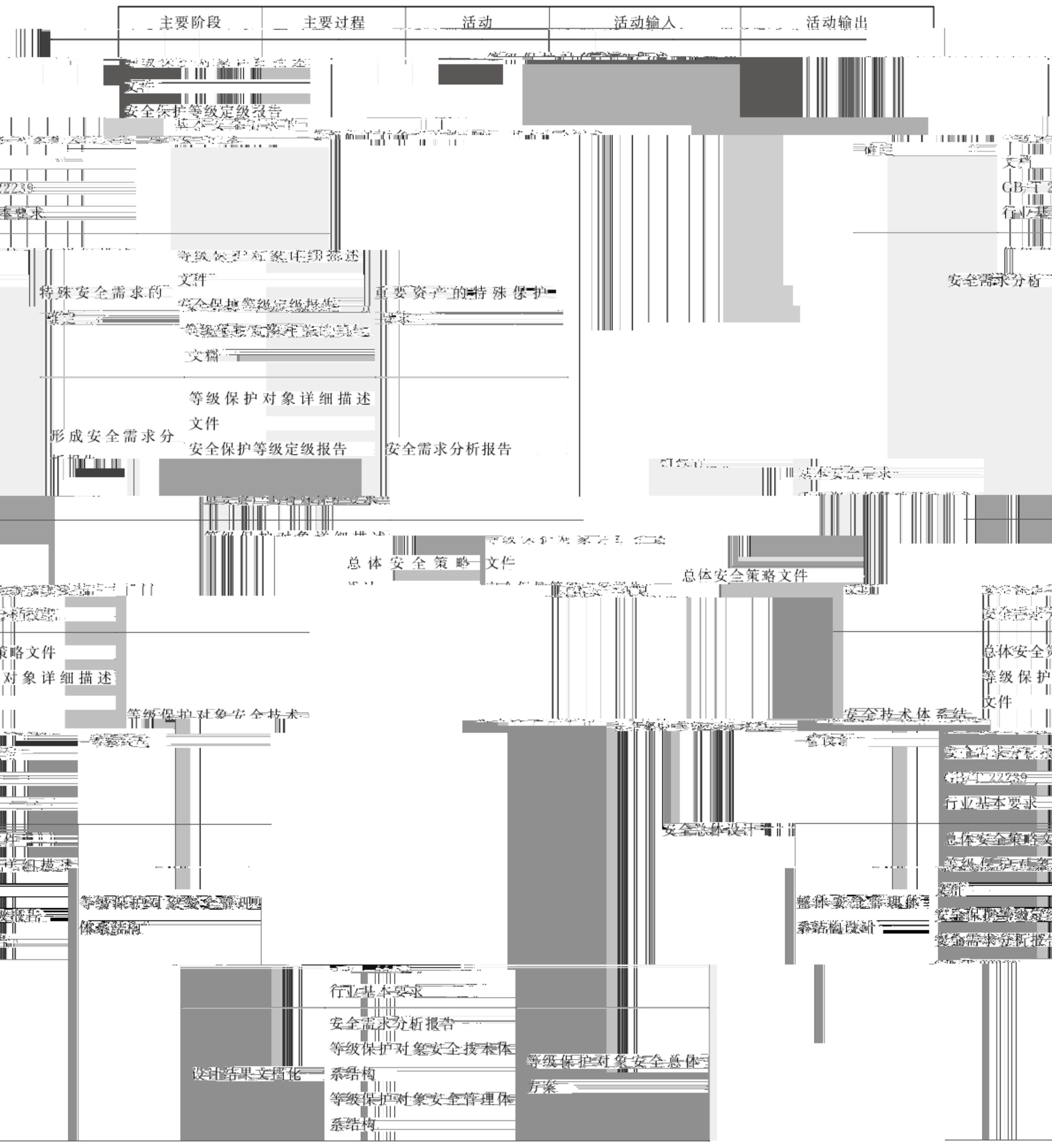

主要阶段
主要过程
活动
活动输入
活动输出
安全保护等级定级报告
特殊安全需求的确定
等级保护对象详细描述文件
安全保护等级定级报告
等级保护对象详细描述文件
形成安全需求分析报告
安全保护等级定级报告
安全需求分析报告
总体安全策略文件
总体安全策略文件
等级保护对象详细描述文件
等级保护对象安全技术体系结构
等级保护对象安全管理体系结构
行业基本要求
安全需求分析报告
等级保护对象安全技术体系结构
等级保护对象安全管理体系结构
设计结果文档化
等级保护对象安全总体方案

表 A.1（续）

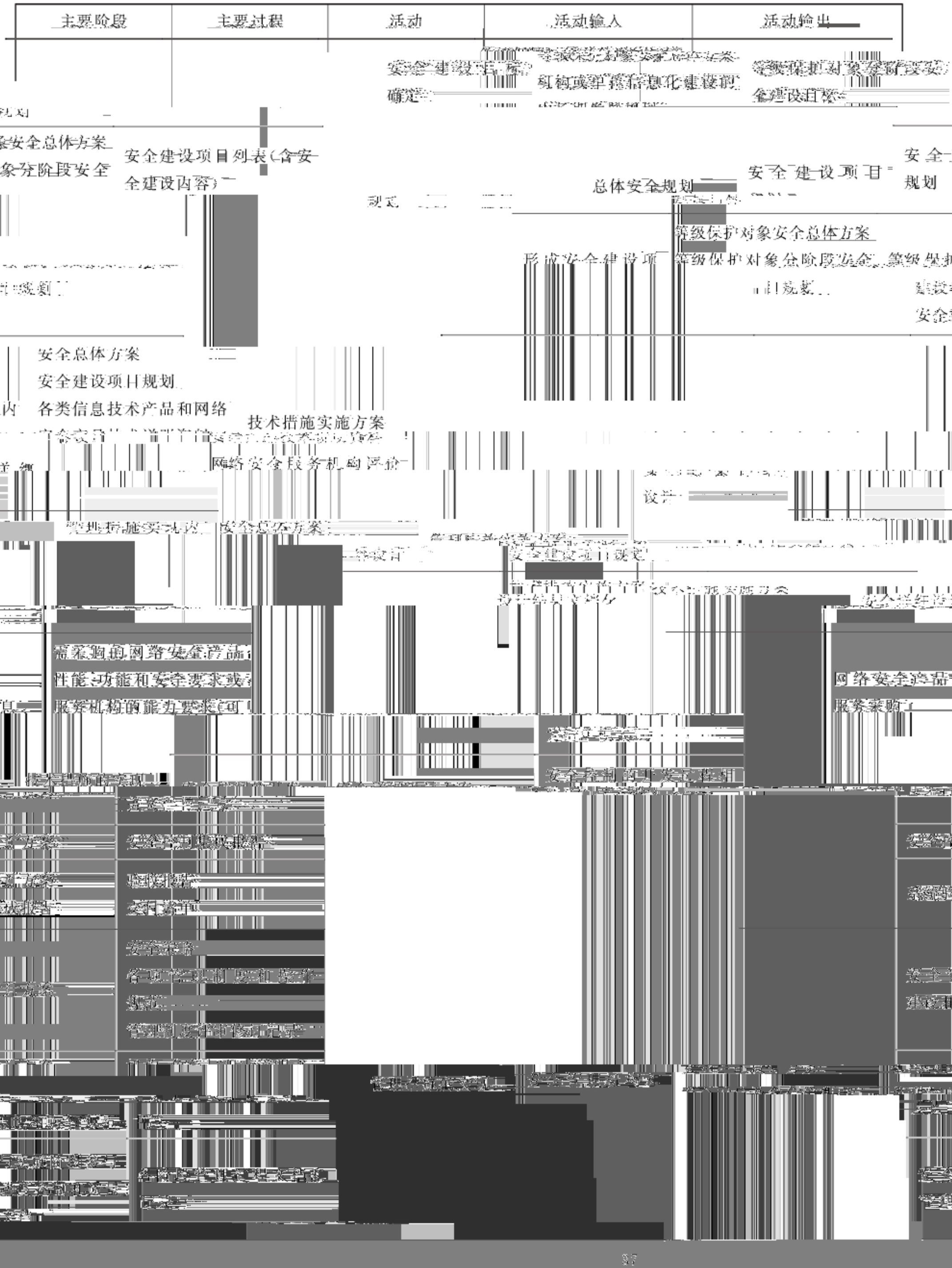

主要阶段
主要过程
活动
活动输入
活动输出
等级保护对象安全总体方案
等级保护对象分阶段安全建设规划
安全建设项目列表（含安全建设内容）
安全总体方案
安全建设项目规划
各类信息技术产品和网络
技术措施实施方案
网络安全服务机构评价
需采购的网络安全产品的性能、功能和安全要求或服务机构的能力要求
安全建设项目规定

表 A.1（续）

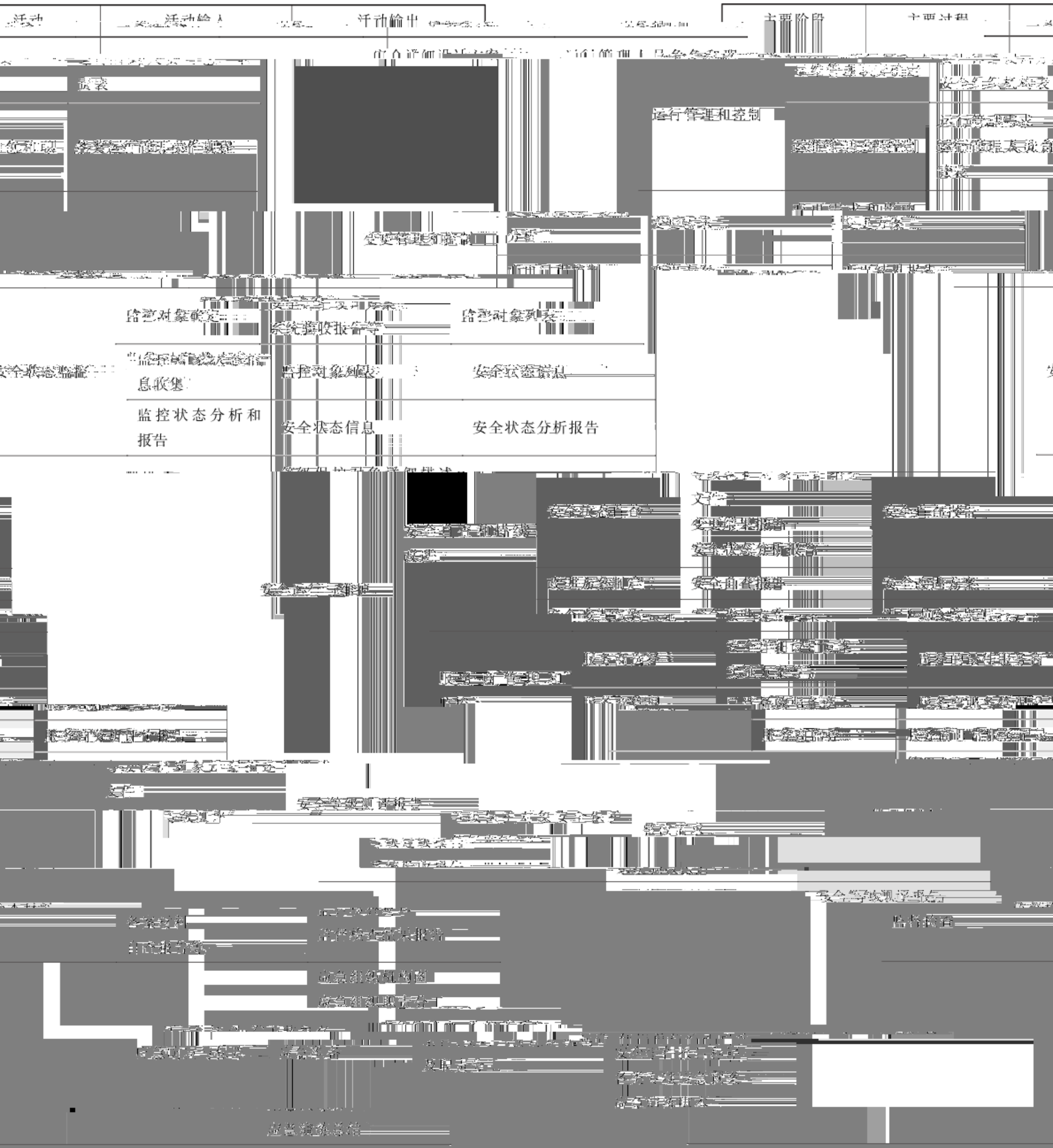


表 A.1（续）

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	
			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、暂存和清除处理记录文档	
	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

GB/T 25058—2019