

中华人民共和国电力行业标准

DL/T ××××—××××

电力行业信息系统安全等级保护基本要求

Baseline for classified protection of power industry information system

(征求意见稿)

201×-××-××发布

201×-××-××实施

电力行业网络与信息安全领导小组办公室

目 次

前 言	V
引 言	VI
第一部分 通用要求	1
1 适用范围	1
2 规范性参考文件	1
3 术语和定义	1
4 信息系统安全等级保护概述	1
4.1 信息系统安全保护等级	1
4.2 不同等级的安全保护能力	1
4.3 总体要求、基本技术要求和基本管理要求	2
4.4 基本技术要求的三种类型	2
第二部分：管理信息系统类要求	4
5 总体要求	4
5.1 总体技术要求	4
5.2 总体管理要求	4
6 第一级基本要求	5
6.1 技术要求	5
6.1.1 物理安全	5
6.1.2 网络安全	5
6.1.3 主机安全	6
6.1.4 应用安全	6
6.1.5 数据安全及备份恢复	7
6.2 管理要求	7
6.2.1 安全管理制度	7
6.2.2 安全管理机构	7
6.2.3 人员安全管理	7
6.2.4 系统建设管理	8
6.2.5 系统运维管理	9
7 第二级基本要求	10
7.1 技术要求	10
7.1.1 物理安全	10

7.1.2 网络安全	11
7.1.3 主机安全	13
7.1.4 应用安全	14
7.1.5 数据安全	15
7.2 管理要求	15
7.2.1 安全管理制度	15
7.2.2 安全管理机构	16
7.2.3 人员安全管理	16
7.2.4 系统建设管理	17
7.2.5 系统运维管理	19
8 第三级基本要求	21
8.1 技术要求	22
8.1.1 物理安全	22
8.1.2 网络安全	23
8.1.3 主机安全	25
8.1.4 应用安全	27
8.1.5 数据安全	29
8.2 管理要求	29
8.2.1 安全管理制度	29
8.2.2 安全管理机构	30
8.2.3 人员安全管理	31
8.2.4 系统建设管理	32
8.2.5 系统运维管理	35
第三部分：生产控制信息系统类要求	40
9 总体要求	40
9.1 总体技术要求	40
9.2 总体管理要求	40
10 第一级基本要求	41
10.1 技术要求	41
10.1.1 物理安全	41
10.1.2 网络安全	41
10.1.3 主机安全	42
10.1.4 应用安全	42
10.1.5 数据安全及备份恢复	42

10.2 管理要求	42
10.2.1 安全管理制度	42
10.2.2 安全管理机构	43
10.2.3 人员安全管理	43
10.2.4 系统建设管理	44
10.2.5 系统运维管理	45
11 第二级基本要求	46
11.1 技术要求	46
11.1.1 物理安全	46
11.1.2 网络安全	47
11.1.3 主机安全	48
11.1.4 应用安全	49
11.1.5 数据安全	50
11.2 管理要求	51
11.2.1 安全管理制度	51
11.2.2 安全管理机构	51
11.2.3 人员安全管理	52
11.2.4 系统建设管理	52
11.2.5 系统运维管理	54
12 第三级基本要求	56
12.1 技术要求	56
12.1.1 物理安全	56
12.1.2 网络安全	58
12.1.3 主机安全	60
12.1.4 应用安全	61
12.1.5 数据安全	63
12.2 管理要求	63
12.2.1 安全管理制度	63
12.2.2 安全管理机构	64
12.2.3 人员安全管理	65
12.2.4 系统建设管理	66
12.2.5 系统运维管理	68
13 第四级基本要求	71
13.1 技术要求	71
13.1.1 物理安全	72

13.1.2 网络安全	73
13.1.3 主机安全	75
13.1.4 应用安全	76
13.1.5 数据安全	78
13.2 管理要求	78
13.2.1 安全管理制度	78
13.2.2 安全管理机构	79
13.2.3 人员安全管理	80
13.2.4 系统建设管理	81
13.2.5 系统运维管理	84
附录 A 关于信息系统整体安全保护能力的要求	88
附录 B 基本安全要求的选择和使用	90
参考文献	92

前 言

本标准的附录 A 和附录 B 是规范性附录。

本标准由国家电力监管委员会提出。

引 言

依据国家信息安全等级保护管理规定和电力行业有关要求制定本标准。

本标准是电力行业信息安全等级保护相关系列规范性文件之一。

与本标准相关的系列标准包括：

——《电力行业信息系统安全等级保护定级工作指导意见》（电监信息[2007]44 号）。

本标准与 GB17859-1999、GB/T 22239—2008 等标准共同构成了电力行业信息系统安全等级保护的相关配套标准。其中 GB17859-1999 、GB/T 22239—2008 是基础性标准，本标准是在 GB17859-1999 和 GB/T 22239—2008 基础上，根据电力行业信息系统和信息安全防护特点及要求，对 GB/T 22239—2008 的进一步细化和扩展。

本标准在 GB17859-1999、GB/T 22239—2008 等技术类标准的基础上，根据电力行业现有技术的发展水平和安全防护要求，分管理信息系统类和生产控制信息系统类，分别提出和规定了不同安全保护等级信息系统的最低保护要求，即基本安全要求，基本安全要求包括总体要求、基本技术要求和基本管理要求，本标准适用于指导不同安全保护等级信息系统的安全建设和监督管理。

在本标准文本中，黑体字表示较低等级中没有出现或增强的要求。

为便于和 GB/T 22239—2008 比照，分别用“（新增）”、“（细化）”、“（增强）”和“（落实）”来标识本标准的该条目和 GB/T 22239—2008 中相关条目的差异，未标识则是等同采用。

电力行业信息系统安全等级保护基本要求

第一部分 通用要求

1 适用范围

本规范规定了电力行业管理类信息系统和生产控制类信息系统不同安全等级的信息系统等级保护要求,包括安全技术指标和安全管理指标,用于指导电力行业各单位信息系统的安全等级保护建设工作。其中,通用要求部分同时适用于管理类信息系统和生产控制类信息系统,管理信息系统类基本要求适用于管理类信息系统的安全等级保护建设工作,生产控制信息系统类基本要求适用于生产控制类信息系统的安全等级保护建设工作。

2 规范性参考文件

《信息安全等级保护管理办法》(公通字[2007]43号)

GB 17859-1999《计算机信息系统安全保护等级保护划分准则》

GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》

《电力二次系统安全防护规定》(电监会5号令)

《电力行业网络与信息安全监督管理暂行规定》(电监信息[2007]50号)

《电力行业信息系统安全等级保护定级工作指导意见》(电监信息[2007]44号)

3 术语和定义

GB/T 5271.8 和 GB 17859-1999 确立的以及下列术语和定义适用于本标准。

安全保护能力 security protection ability

系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。

4 信息系统安全等级保护概述

4.1 信息系统安全保护等级

信息系统根据其在国家安全、经济建设、社会生活中的重要程度,遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等,由低到高划分为五级。

4.2 不同等级的安全保护能力

不同等级的信息系统应具备的基本安全保护能力如下:

第一级安全保护能力:应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾害、以及其他相当危害程度的威胁所造成的关键资源损害,在系统遭到损害后,能够恢复部分功能。

第二级安全保护能力:应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶

意攻击、一般的自然灾害、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾害、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

第四级安全保护能力：应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾害、以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

第五级安全保护能力：（略）。

4.3 总体要求、基本技术要求和基本管理要求

信息系统安全等级保护应依据信息系统的安全保护等级情况保证它们具有相应等级的基本安全保护能力，不同安全保护等级的信息系统要求具有不同的安全保护能力。

基本安全要求是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的安全要求，根据实现方式的不同，基本安全要求分为总体要求、基本技术要求和基本管理要求三大类。总体要求与各个单位的总体安全策略相关，主要通过落实总体安全策略直接导出的、所有信息系统必须遵从的总体安全防护要求来体现；技术类安全要求与信息系统提供的技术安全机制有关，主要通过部署软硬件并正确的配置其安全功能来实现；管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

总体要求概括了电力行业信息安全防护策略的基本要求；基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出；基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出，总体要求、基本技术要求和基本管理要求是确保信息系统安全不可分割的三个部分。

基本安全要求从各个层面或方面提出了系统的每个组件应该满足的安全要求，信息系统具有的整体安全保护能力通过不同组件实现基本安全要求来保证。除了保证系统的每个组件满足基本安全要求外，还要考虑组件之间的相互关系，来保证信息系统的整体安全保护能力。关于信息系统整体安全保护能力的说明见附录 A。

对于涉及国家秘密的信息系统，应按照国家保密工作部门的相关规定和标准进行保护。对于涉及密码的使用和管理，应按照国家密码管理的相关规定和标准实施。

4.4 基本技术要求的三种类型

根据保护侧重点的不同，技术类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）；通用安全保护类要求（简记为 G）。

本规范中对基本安全要求使用了标记，其中的字母表示安全要求的类型，数字表示适用的安全保护等级。关于各类安全要求的选择和使用见附录 B。

第二部分：管理信息系统类要求

5 总体要求

5.1 总体技术要求

- a) 管理信息大区网络与生产控制大区网络应物理隔离；两网之间有信息通信交换时应部署符合电力系统要求的单向隔离装置；（新增）
- b) 管理信息大区网络可进一步划分为内部网络和外部网络，两网之间有信息通信交换时防护强度应强于逻辑隔离；（新增）
- c) 具有层次网络结构的单位可统一提供互联网出口；（新增）
- d) 二级系统统一成域，三级系统单独成域；（新增）
- e) 三级系统域由独立子网承载，每个域有唯一网络出口，可在网络出口处部署三级等级保护专用装置为系统提供整体安全防护。（新增）

5.2 总体管理要求

- a) 如果本单位管理信息大区仅有一级信息系统时，通用管理要求等同采用一级；（新增）
- b) 如果本单位管理信息大区含有二级及以下等级信息系统时，通用管理要求等同采用二级；（新增）
- c) 如果本单位管理信息大区含有三级及以下等级信息系统时，通用管理要求等同采用三级。（新增）

6 第一级基本要求

6.1 技术要求

6.1.1 物理安全

6.1.1.1 物理访问控制（G1）

机房出入应安排专人负责，控制、鉴别和记录进入的人员。

6.1.1.2 防盗窃和防破坏（G1）

本项要求包括：

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记。

6.1.1.3 防雷击（G1）

机房建筑应设置避雷装置。

6.1.1.4 防火（G1）

机房应设置灭火设备。

6.1.1.5 防水和防潮（G1）

本项要求包括：

- a) 应对穿过机房墙壁和楼板的水管增加必要的保护措施；
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

6.1.1.6 温湿度控制（G1）

机房应设置必要的温、湿度控制设施，使机房温、湿度的变化在设备运行所允许的范围之内。

6.1.1.7 电力供应（A1）

应在机房供电线路上配置稳压器和过电压防护设备。

6.1.2 网络安全

6.1.2.1 结构安全（G1）

本项要求包括：

- a) 应保证关键网络设备的业务处理能力满足基本业务需要；
- b) 应保证接入网络 and 核心网络的带宽满足基本业务需要；
- c) 应绘制与当前运行情况相符的网络拓扑结构图。

6.1.2.2 访问控制（G1）

本项要求包括：

- a) 应在网络边界部署访问控制设备，启用访问控制功能；
- b) 应根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包出入；
- c) 应通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度至少为用户组。

6.1.2.3 网络设备防护（G1）

本项要求包括：

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
- c) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

6.1.3 主机安全

6.1.3.1 身份鉴别（S1）

应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

6.1.3.2 访问控制（S1）

本项要求包括：

- a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 应限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
- c) 应及时删除多余的、过期的帐户，避免共享帐户的存在。

6.1.3.3 入侵防范（G1）

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更新。

6.1.3.4 恶意代码防范（G1）

应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

6.1.4 应用安全

6.1.4.1 身份鉴别（S1）

本项要求包括：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- c) 应启用身份鉴别和登录失败处理功能，并根据安全策略配置相关参数。

6.1.4.2 访问控制（S1）

本项要求包括：

- a) 应提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；
- b) 应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。

6.1.4.3 通信完整性（S1）

应采用约定通信会话方式的方法保证通信过程中数据的完整性。

6.1.4.4 软件容错（A1）

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

6.1.5 数据安全及备份恢复

6.1.5.1 数据完整性（S1）

应能够检测到重要用户数据在传输过程中完整性受到破坏。

6.1.5.2 备份和恢复（A1）

应能够对重要信息进行备份和恢复。

6.2 管理要求

6.2.1 安全管理制度

6.2.1.1 管理制度（G1）

应建立日常管理活动中常用的安全管理制度。

6.2.1.2 制定和发布（G1）

本项要求包括：

- a) 应指定或授权专门的人员负责安全管理制度的制定；
- b) 应将安全管理制度以某种方式发布到相关人员手中。

6.2.2 安全管理机构

6.2.2.1 资金保障

- a) 应保障落实信息系统安全建设、运维及等级保护测评资金等；（新增）
- b) 系统建设资金筹措方案和年度系统维护经费应包括信息安全保障资金项目。（新增）

6.2.2.2 岗位设置（G1）

应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。

6.2.2.3 人员配备（G1）

应配备一定数量的系统管理员、网络管理员、安全管理员等。

6.2.2.4 授权和审批（G1）

应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批。

6.2.2.5 沟通和合作（G1）

应加强与行业信息安全监管部门、公安机关、通信运营商、银行及相关单位和部门的合作与沟通。（增强）

6.2.3 人员安全管理

6.2.3.1 人员录用（G1）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责人员录用；
- b) 应对被录用人员的身份和专业资格等进行审查，并确保其具有基本的专业技术水平和安全管理知识。

6.2.3.2 人员离岗（G1）

本项要求包括：

- a) 应立即终止由于各种原因离岗员工的所有访问权限；
- b) 应收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。（落实）

6.2.3.3 安全意识教育和培训（G1）

本项要求包括：

- a) 应按照行业信息安全要求，制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行的培训应至少每年举办一次。（新增）
- b) 应对各类人员进行安全意识教育和岗位技能培训；
- c) 应告知人员相关的安全责任和惩戒措施。

6.2.3.4 外部人员访问管理（G1）

应确保在外部人员访问受控区域前得到授权或审批。

6.2.4 系统建设管理

6.2.4.1 系统定级（G1）

本项要求包括：

- a) 应明确信息系统的边界和安全保护等级；
- b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由；
- c) 应确保信息系统的定级结果经过行业信息安全主管部门等相关部门的批准。（细化）

6.2.4.2 安全方案设计（G1）

本项要求包括：

- a) 应根据系统的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
- b) 应以书面的形式描述对系统的安全保护要求和策略、安全措施等内容，形成系统的安全方案；
- c) 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。

6.2.4.3 产品采购和使用（G1）

- a) 应确保安全产品采购和使用符合国家的有关规定。
- b) 电力系统专用信息安全产品应经行业主管部门指定的安全机构测评方可采购使用。（新增）

6.2.4.4 自行软件开发（G1）

本项要求包括：

- a) 应确保开发环境与实际运行环境物理分开；
- b) 应确保软件设计相关文档由专人负责保管。

6.2.4.5 外包软件开发（G1）

本项要求包括：

- a) 应根据开发要求检测软件质量；
- b) 应在软件安装之前检测软件包中可能存在的恶意代码；
- c) 应确保提供软件设计的相关文档和使用指南。

6.2.4.6 工程实施 (G1)

应指定或授权专门的部门或人员负责工程实施过程的管理。

6.2.4.7 测试验收 (G1)

本项要求包括：

- a) 应对系统进行安全性测试验收；
- b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

6.2.4.8 系统交付 (G1)

本项要求包括：

- a) 应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 应对负责系统运行维护的技术人员进行相应的技能培训；
- c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

6.2.4.9 安全服务商选择 (G1)

本项要求包括：

- a) 应确保安全服务商的选择符合国家的有关规定；
- b) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。

6.2.5 系统运维管理

6.2.5.1 环境管理 (G1)

本项要求包括：

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
- b) 应对机房的出入、服务器的开机或关机等工作进行管理；
- c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。

6.2.5.2 资产管理 (G1)

应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

6.2.5.3 介质管理 (G1)

本项要求包括：

- a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护；
- b) 应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。

6.2.5.4 设备管理 (G1)

本项要求包括：

- a) 应对信息系统相关的各种设备、线路等指定专门的部门或人员定期进行维护管理；
- b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。

6.2.5.5 网络安全管理 (G1)

本项要求包括：

- a) 应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- b) 应定期进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。

6.2.5.6 系统安全管理（G1）

本项要求包括：

- a) 应根据业务需求和系统安全分析确定系统的访问控制策略；
- b) 应定期进行漏洞扫描，对发现的系统安全漏洞进行及时的修补；
- c) 应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。（增强）

6.2.5.7 恶意代码防范管理（G1）

应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。

6.2.5.8 备份与恢复管理（G1）

本项要求包括：

- a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等。

6.2.5.9 安全事件处置（G1）

本项要求包括：

- a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；
- b) 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

7 第二级基本要求

7.1 技术要求

7.1.1 物理安全

7.1.1.1 物理位置的选择（G2）

机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。

7.1.1.2 物理访问控制（G2）

本项要求包括：

- a) 机房各出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员；（增强）
- b) 进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

7.1.1.3 防盗窃和防破坏（G2）

本项要求包括：

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易去除的标记；
- c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 主机房应安装必要的防盗报警设施。

7.1.1.4 防雷击 (G2)

本项要求包括：

- a) 机房建筑应设置避雷装置；
- b) 机房应设置交流电源地线。

7.1.1.5 防火 (G2)

机房应设置灭火设备和火灾自动报警系统。

7.1.1.6 防水和防潮 (G2)

本项要求包括：

- a) 主机房尽量避开水源，与主机房无关的给排水管道不得穿过主机房，与主机房相关的给排水管道必须有可靠的防渗漏措施；（落实）
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

7.1.1.7 防静电 (G2)

关键设备应采用必要的接地防静电措施。

7.1.1.8 温湿度控制 (G2)

机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

7.1.1.9 电力供应 (A2)

本项要求包括：

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求。

7.1.1.10 电磁防护 (S2)

电源线和通信线缆应隔离铺设，避免互相干扰。

7.1.2 网络安全

7.1.2.1 结构安全 (G2)

本项要求包括：

- a) 管理信息大区网络与生产控制大区网络应物理隔离；两网之间有信息通信交换时应部署符合电力系统要求的单向隔离装置；（新增）
- b) 管理信息大区网络可进一步划分为内部网络和外部网络，两网之间有信息通信交换时防护强度应强于逻辑隔离；（新增）

- c) 具有层次网络结构的单位可统一提供互联网出口；（新增）
- d) 应保证关键网络设备的业务处理能力**具备冗余空间，满足业务高峰期需要**；
- e) 应保证接入网络 and 核心网络的带宽**满足业务高峰期需要**；
- a) 应绘制完整的网络拓扑结构图，有相应的网络配置表，包含设备IP地址等主要信息，与当前运行情况相符；（增强）
- f) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

7.1.2.2 访问控制 (G2)

本项要求包括：

- a) 应在网络边界部署访问控制设备，启用访问控制功能；
- b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；（增强）
- c) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为**单个用户**。以拨号或VPN等方式接入网络的，应采用强认证方式，并对用户访问权限进行严格限制。（增强）
- d) 应限制具有拨号、VPN等访问权限的用户数量。（增强）

7.1.2.3 安全审计 (G2)

本项要求包括：

- a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；
- b) 审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

7.1.2.4 边界完整性检查 (S2)

应能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。

7.1.2.5 入侵防范 (G2)

应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。

7.1.2.6 网络设备防护 (G2)

本项要求包括：

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应对网络设备的管理员登录地址进行限制；
- c) 网络设备标识应唯一；同一网络设备的用户标识应唯一；禁止多个人员共用一个账号；（增强）
- d) **身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换**。应修改默认用户和口令，不得使用缺省口令，口令长度不得小于8位，要求是字母和数字或特殊字符的混合并不得与用户名相同，口令应定期更换，并加密存储；（增强）

- e) 应具有登录失败处理功能,可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施;
- f) 当对网络设备进行远程管理时,采取必要措施防止鉴别信息在网络传输过程中被窃听;
- g) 应封闭不需要的网络端口,关闭不需要的网络服务。如需使用SNMP服务,应采用安全性增强版本;并应设定复杂的Community控制字段,不使用Public、Private等默认字段。(新增)

7.1.3 主机安全

7.1.3.1 身份鉴别 (S2)

本项要求包括:

- a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别;
- b) **操作系统和数据库系统管理用户身份鉴别信息应不易被冒用,口令复杂度应满足要求并定期更换。**口令长度不得小于8位,且为字母、数字或特殊字符的混合组合,用户名和口令禁止相同;(细化)
- c) 启用登录失败处理功能,可采取结束会话、限制非法登录次数和自动退出等措施。限制同一用户连续失败登录次数;(增强)
- d) 当对服务器进行远程管理时,应采取必要措施,防止鉴别信息在网络传输过程中被窃听;
- e) 应为操作系统和数据库系统的不同用户分配不同的用户名,确保用户名具有唯一性。

7.1.3.2 访问控制 (S2)

本项要求包括:

- a) 应启用访问控制功能,依据安全策略控制用户对资源的访问;
- b) 应实现操作系统和数据库系统特权用户的权限分离;
- c) 应限制默认帐户的访问权限,重命名系统默认帐户,修改这些帐户的默认口令;
- d) 应及时删除多余的、过期的帐户,避免共享帐户的存在。

7.1.3.3 安全审计 (G2)

本项要求包括:

- a) 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户;系统不支持该要求的,应以系统运行安全和效率为前提,采用第三方安全审计产品实现审计要求;(落实)
- b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。审计内容至少包括:用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作(如用户登录、退出)等;(细化)
- c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等;
- d) 应保护审计记录,避免受到未预期的删除、修改或覆盖等。

7.1.3.4 入侵防范 (G2)

操作系统应遵循最小安装的原则,仅安装必要的组件和应用程序,并通过设置升级服务器等方式保持系统补丁及时得到更新,补丁安装前应进行安全性和兼容性测试。(增强)

7.1.3.5 恶意代码防范 (G2)

本项要求包括：

- a) 应在本机安装防恶意代码软件或独立部署恶意代码防护设备，并及时更新防恶意代码软件版本和恶意代码库；（细化）
- b) 应支持防恶意代码的统一管理。

7.1.3.6 资源控制（A2）

本项要求包括：

- a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；
- b) 应根据安全策略设置登录终端的操作超时锁定；
- c) 应根据需要限制单个用户对系统资源的最大或最小使用限度。（细化）

7.1.4 应用安全

7.1.4.1 身份鉴别（S2）

本项要求包括：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) **应用系统用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。**应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用户在第一次登录系统时修改分发的初始口令，口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；应用软件不得明文存储口令数据；（增强）
- c) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- d) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

7.1.4.2 访问控制（S2）

本项要求包括：

- a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
- b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
- c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；
- d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

7.1.4.3 安全审计（G2）

本项要求包括：

- a) **应提供覆盖到每个用户的安全审计功能**，对应用系统的用户登录、用户退出、增加用户、修改用户权限等重要安全事件进行审计；（细化）
- b) **应保证审计活动的完整性，保证无法删除、修改或覆盖审计记录；**（增强）
- c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

7.1.4.4 通信完整性（S2）

应采用校验码技术保证通信过程中数据的完整性。

7.1.4.5 通信保密性 (S2)

本项要求包括：

- a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始验证；
- b) 应对通信过程中用户口令、会话密钥等敏感信息字段进行加密。（细化）

7.1.4.6 软件容错 (A2)

本项要求包括：

- a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- b) 在故障发生时，应用系统应能够继续提供部分功能，确保系统能够实施恢复措施。（细化）

7.1.4.7 资源控制 (A2)

本项要求包括：

- a) 当应用系统的通信双方中的一方在一段时间内未作响应，另一方应能够自动结束会话；
- b) 应能够对应用系统的最大并发会话连接数进行限制；
- c) 应能够对单个帐户的多重并发会话进行限制。

7.1.5 数据安全

7.1.5.1 数据完整性 (S2)

应能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。

7.1.5.2 数据保密性 (S2)

应采用加密或其他保护措施实现鉴别信息的存储保密性。

7.1.5.3 备份和恢复 (A2)

本项要求包括：

- a) 应对重要信息进行备份，并对备份介质定期进行可用性测试；（增强）
- b) 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

7.2 管理要求

7.2.1 安全管理制度

7.2.1.1 管理制度 (G2)

本项要求包括：

- a) 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- b) 应对安全管理活动中重要的管理内容建立安全管理制度；
- c) 应对安全管理人员或操作人员执行的重要管理操作建立操作规程。

7.2.1.2 制定和发布 (G2)

本项要求包括：

- a) 应指定或授权专门的部门或人员负责安全管理制度的制定；

- b) 应组织相关人员对制定的安全管理制度进行论证和审定；
- c) 应将安全管理制度以某种方式发布到相关人员手中。

7.2.1.3 评审和修订 (G2)

定期或在发生重大变更时对安全管理制度进行检查和审定,对存在不足或需要改进的安全管理制度进行修订。(增强)

7.2.2 安全管理机构

7.2.2.1 岗位设置 (G2)

本项要求包括:

- a) 应设立安全主管、安全管理各个方面的负责人岗位,并定义各负责人的职责;
- b) 应设立系统管理员、网络管理员、安全管理员等岗位,并定义各个工作岗位的职责。

7.2.2.2 人员配备 (G2)

本项要求包括:

- a) 应配备一定数量的系统管理员、网络管理员、安全管理员等;
- b) 安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。

7.2.2.3 资金保障 (G2)

- a) 应保障落实信息系统安全建设、运维及等级保护测评资金等; (新增)
- b) 系统建设资金筹措方案和年度系统维护经费应包括信息安全保障资金项目。(新增)

7.2.2.4 授权和审批 (G2)

本项要求包括:

- a) 应根据各个部门和岗位的职责明确授权审批部门及批准人,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批;
- b) 应针对关键活动建立审批流程,并由批准人签字确认,并存档备查。(增强)

7.2.2.5 沟通和合作 (G2)

本项要求包括:

- a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通;
- b) 应加强与行业信息安全监管部门、公安机关、通信运营商、银行及相关单位和部门的合作与沟通。(细化)

7.2.2.6 审核和检查 (G2)

安全管理员应负责定期进行安全检查,检查内容包括系统日常运行、系统漏洞和数据备份等情况。

7.2.3 人员安全管理

7.2.3.1 人员录用 (G2)

本项要求包括:

- a) 应指定或授权专门的部门或人员负责人员录用;

- b) 应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核；
- c) 应与安全管理员、系统管理员、网络管理员等关键岗位的人员签署保密协议。（细化）

7.2.3.2 人员离岗（G2）

本项要求包括：

- a) 应规范人员离岗过程，及时收回离岗员工的所有访问权限；（增强）
- b) 应收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
- c) 只有在收回访问权限和各种证件、设备之后方可办理调离手续。（细化）

7.2.3.3 人员考核（G2）

应定期对各个岗位的人员进行安全技能及安全认知的培训级考核。

7.2.3.4 安全意识教育和培训（G2）

本项要求包括：

- a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- b) 应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒；
- c) 应按照行业信息安全要求，制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行的培训应至少每年举办一次。（增强）

7.2.3.5 外部人员访问管理（G2）

应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。

7.2.4 系统建设管理

7.2.4.1 系统定级（G2）

本项要求包括：

- a) 应明确信息系统的边界和安全保护等级；
- b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由；
- c) 对于跨电力公司联网运行的信息系统，由电力行业网络与信息安全领导小组办公室统一确定安全保护等级。对于属同一电力公司，但跨省联网运行的信息系统，由公司责任部门统一确定安全保护等级。对于通用信息系统，由领导小组办公室提出安全保护等级建议，运营使用单位自主确定安全保护等级。对于运营使用单位所特有的信息系统，各运营使用单位自行确定安全保护等级。对拟确定为第四级以上信息系统的，由领导小组办公室邀请国家信息安全保护等级专家评审委员会评审。（细化）
- d) 应确保信息系统的定级结果经过行业信息安全主管部门批准，方可到公安机关备案。（细化）

7.2.4.2 安全方案设计（G2）

本项要求包括：

- a) 应根据系统的安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
- b) 应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案；
- c) 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案；

- d) 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定, **重大项目应报行业信息安全主管部门进行信息安全专项审查批准。(落实)**

7.2.4.3 产品采购和使用 (G2)

本项要求包括:

- a) 应确保安全产品采购和使用符合国家的有关规定;
- b) **应确保密码产品采购和使用符合国家密码主管部门的要求;**
- c) **应指定或授权专门的部门负责产品的采购。**
- d) **电力系统专用信息安全产品应经行业主管部门指定的安全机构测评方可采购使用。(新增)**

7.2.4.4 自行软件开发 (G2)

本项要求包括:

- a) 应确保开发环境与实际运行环境物理分开;
- b) **应制定软件开发管理制度, 明确说明开发过程的控制方法和人员行为准则;**
- c) 应确保提供软件设计的相关文档**和使用指南**, 并由专人负责保管。

7.2.4.5 外包软件开发 (G2)

本项要求包括:

- a) 应根据开发要求检测软件质量;
- b) 应确保提供软件设计的相关文档和使用指南;
- c) 应在软件安装之前检测软件包中可能存在的恶意代码;
- d) **外包开发的软件应在本单位存有源代码备份, 并已通过软件后门等安全性检测。(增强)**

7.2.4.6 工程实施 (G2)

本项要求包括:

- a) 应指定或授权专门的部门或人员负责工程实施过程的管理;
- b) **应制定详细的工程实施方案, 控制工程实施过程。**

7.2.4.7 测试验收 (G2)

本项要求包括:

- a) 应委托国家及电力行业认可的测评单位对系统进行安全性测试, 并出具安全性测试报告; (细化)
- b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案, 在测试验收过程中应详细记录测试验收结果, 并形成测试验收报告;
- c) **应组织相关部门和相关人员对系统测试验收报告进行审定, 并签字确认。**

7.2.4.8 系统交付 (G2)

本项要求包括:

- a) 应制定系统交付清单, 并根据交付清单对所交接的设备、软件和文档等进行清点;

- b) 应应对负责系统运行维护的技术人员每年进行相应的技能培训,对安全教育和培训的情况和结果进行记录并归档保存; (细化)
- c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

7.2.4.9 系统备案 (G2)

应将系统等级及相关材料报系统主管部门备案;电力企业汇总系统等级及相关信息报电力行业网络与信息安全领导小组办公室备案。(新增)

7.2.4.10 等级测评 (G2)

应选择具有国家相关技术资质和安全资质,经电力行业网络与信息安全领导小组办公室批准的测评单位进行等级测评。(新增)

7.2.4.11 安全服务商选择 (G2)

本项要求包括:

- a) 应选择符合国家及行业有关规定的服务商开展安全服务; (细化)
- b) 应与选定的安全服务商签订安全协议,明确安全责任; (细化)
- c) 应与服务商签订安全服务合同,明确技术支持和服务承诺。(增强)

7.2.5 系统运维管理

7.2.5.1 环境管理 (G2)

本项要求包括:

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理;
- b) 应配备机房安全管理人员,对机房的出入、服务器的开机或关机等工作进行管理;
- c) 应建立机房安全管理制度,对有关机房物理访问,物品带进、带出机房和机房环境安全等方面的管理作出规定;
- d) **应加强对办公环境的保密性管理,包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。**

7.2.5.2 资产管理 (G2)

本项要求包括:

- a) 应编制与信息系统相关的资产清单,包括资产责任部门、重要程度和所处位置等内容;
- b) **应建立资产安全管理制度,规定信息系统资产管理的责任人员或责任部门,并规范资产管理和使用的行为。**

7.2.5.3 介质管理 (G2)

本项要求包括:

- a) 应确保介质存放在安全的环境中,对各类介质进行控制和保护, **并实行存储环境专人管理;**
- b) 应建立移动存储介质安全管理制度,对移动存储介质的使用进行管控; (新增)
- c) 应对介质归档和查询等过程进行记录,并根据存档介质的目录清单定期盘点;
- d) **应对需要送出维修或销毁的介质,首先清除其中的敏感数据,防止信息的非法泄露;**

- e) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理。

7.2.5.4 设备管理 (G2)

本项要求包括:

- a) 应对信息系统相关的各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理;
- b) 应建立基于申报、审批和专人负责的设备安全管理制度,对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理;
- c) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理,按操作规程实现关键设备(包括备份和冗余设备)的启动/停止、加电/断电等操作;
- d) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

7.2.5.5 网络安全管理 (G2)

本项要求包括:

- a) 应指定人员对网络进行管理,负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作;
- b) 应建立网络安全管理制度,对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定;
- c) 应根据厂家提供的软件升级版本对网络设备进行更新,并在更新前对现有的重要文件进行备份;
- d) 应定期对网络系统进行漏洞扫描,对发现的网络系统安全漏洞进行及时的修补;
- e) 应对网络设备的配置文件进行定期备份;
- f) 应保证所有与外部系统的连接均得到授权和批准。

7.2.5.6 系统安全管理 (G2)

本项要求包括:

- a) 应根据业务需求和系统安全分析确定系统的访问控制策略;
- b) 应定期进行漏洞扫描,对发现的系统安全漏洞及时进行修补;
- c) 应安装系统的最新补丁程序,在安装系统补丁前,应首先在测试环境中测试通过,并对重要文件进行备份后,方可实施系统补丁程序的安装;
- d) 应建立系统安全管理制度,对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定;
- e) 应依据操作手册对系统进行维护,详细记录操作日志,包括重要的日常操作、运行维护记录、参数的设置和修改等内容,严禁进行未经授权的操作;
- f) 应定期对运行日志和审计数据进行分析,以便及时发现异常行为。

7.2.5.7 恶意代码防范管理 (G2)

本项要求包括:

- a) 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
- b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

7.2.5.8 密码管理（G2）

应使用符合国家密码管理规定的密码技术和产品。

7.2.5.9 变更管理（G2）

本项要求包括：

- a) 应确认系统中要发生的重要变更，并制定相应的变更方案；
- b) 系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。

7.2.5.10 备份与恢复管理（G2）

本项要求包括：

- a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；
- c) 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。

7.2.5.11 安全事件处置（G2）

本项要求包括：

- a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；
- b) 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；
- d) 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。

7.2.5.12 应急预案管理（G2）

本项要求包括：

- a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
- b) 应对安全管理员、系统管理员、网络管理员等相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。（细化）

8 第三级基本要求

8.1 技术要求

8.1.1 物理安全

8.1.1.1 物理位置的选择（G3）

本项要求包括：

- a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
- b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁，如果不可避免，应采取有效防水措施。（落实）

8.1.1.2 物理访问控制（G3）

本项要求包括：

- a) 机房各出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员；（增强）
- b) 进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；
- c) 应对机房划分区域进行管理，区域和区域之间应用物理方式隔断，在重要区域前设置交付或安装等过渡区域；（增强）
- d) 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

8.1.1.3 防盗窃和防破坏（G3）

本项要求包括：

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
- c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 应利用光、电等技术设置机房防盗报警系统；
- f) 应对机房设置监控报警系统。

8.1.1.4 防雷击（G3）

本项要求包括：

- a) 机房建筑应设置避雷装置；
- b) 应设置防雷保安器，防止感应雷；
- c) 机房应设置交流电源地线。

8.1.1.5 防火（G3）

本项要求包括：

- a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警、自动灭火；
- b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- c) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

8.1.1.6 防水和防潮（G3）

本项要求包括：

- a) 主机房尽量避开水源，与主机房无关的给排水管道不得穿过主机房，与主机房相关的给排水管道必须有可靠的防渗漏措施；（落实）
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
- d) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

8.1.1.7 防静电（G3）

本项要求包括：

- a) 主要设备采用必要的接地防静电措施；
- b) 机房应采用防静电地板。

8.1.1.8 温湿度控制（G3）

机房应设置**温、湿度自动调节设施**，使机房温、湿度的变化在设备运行所允许的范围之内。

8.1.1.9 电力供应（A3）

本项要求包括：

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期的备用电力供应，至少满足**主要设备**在断电情况下的正常运行要求；
- c) 设置冗余或并行的电力电缆线路为计算机系统供电，输入电源应采用双路自动切换供电方式；（增强）
- d) 应建立备用供电系统。

8.1.1.10 电磁防护（S3）

本项要求包括：

- a) 电源线和通信线缆应隔离铺设，避免互相干扰；
- b) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；
- c) 应对关键设备和磁介质实施电磁屏蔽。

8.1.2 网络安全

8.1.2.1 结构安全（G3）

本项要求包括：

- a) 管理信息大区网络与生产控制大区网络应物理隔离；两网之间有信息通信交换时应部署符合电力系统要求的单向隔离装置；（新增）
- b) 管理信息大区网络可进一步划分为内部网络和外部网络，两网之间有信息通信交换时防护强度应强于逻辑隔离；（新增）
- c) 具有层次网络结构的单位可统一提供互联网出口；（新增）
- d) 单个系统应单独划分安全域，系统由独立子网承载，每个域的网络出口应唯一；（新增）
- e) 应保证**主要网络设备**的业务处理能力具备冗余空间，满足业务高峰期需要；
- f) 应保证网络各个部分的带宽满足业务高峰期需要；
- g) 应在**业务终端与业务服务器**之间进行路由控制建立安全的访问路径；

- h) 应绘制完整的网络拓扑结构图,有相应的网络配置表,包含设备IP地址等主要信息,与当前运行情况相符; (增强)
- i) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素,划分不同的子网或网段,并按照方便管理和控制的原则为各子网、网段分配地址段;
- j) 在业务高峰时段,现有宽带不能满足要求时,应按照对业务服务的重要次序来制定带宽分配优先级,保证在网络发生拥堵的时候优先保障重要业务服务的带宽; (落实)
- k) 采用冗余技术设计网络拓扑结构,提供主要网络设备、通信线路的硬件冗余,避免关键节点存在单点故障。 (增强)
- l) 在进行内外网隔离的情况下,应将应用系统部署在内网,如有外网交互功能的应用系统,可将前端部署在外网,数据库部分部署在内网。 (新增)

8.1.2.2 访问控制 (G3)

本项要求包括:

- a) 应在网络边界部署访问控制设备,启用访问控制功能;
- b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力, **控制粒度为端口级**;
- c) 应按用户和系统之间的允许访问规则,决定允许或拒绝用户对受控系统进行资源访问,控制粒度为**单个用户**。以拨号或VPN等方式接入网络的,应采用强认证方式,并对用户访问权限进行严格限制; (增强)
- d) 应限制具有拨号、VPN等访问权限的用户数量; (增强)
- e) **应对进出网络的信息内容进行过滤,实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制**;
- f) 应在会话处于非活跃一定时间或会话结束后终止网络连接;
- g) 在互联网出口和核心网络接口处应限制网络最大流量数及网络连接数; (细化)
- h) 重要网段应采取技术手段防止地址欺骗。

8.1.2.3 安全审计 (G3)

本项要求包括:

- a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录;
- b) 审计记录应包括:事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;
- c) 应能够根据记录数据进行分析,并生成审计报表,网络设备不支持的应采用第三方工具生成审计报表; (落实)
- d) **应对审计记录进行保护,避免受到未预期的删除、修改或覆盖等。**

8.1.2.4 边界完整性检查 (S3)

本项要求包括:

- a) 应能够对非授权设备私自联到内部网络的行为进行检查,准确定出位置,并对其进行有效阻断;

- b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定位，并对其进行有效阻断。

8.1.2.5 入侵防范（G3）

本项要求包括：

- a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等；
- b) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

8.1.2.6 恶意代码防范（G3）

本项要求包括：

- a) 应在网络边界处对恶意代码进行检测和清除；
- b) 应维护恶意代码库的升级和检测系统的更新。

8.1.2.7 网络设备防护（G3）

本项要求包括：

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应对网络设备的管理员登录地址进行限制；
- c) 网络设备标识应唯一；同一网络设备的用户标识应唯一；禁止多个人共用一个账号；（增强）
- d) **身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。**应修改默认用户和口令，不得使用缺省口令，口令长度不得小于8位，要求是字母和数字或特殊字符的混合并不得与用户名相同，口令应定期更换，并加密存储；（增强）
- e) **主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；**
- f) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
- g) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
- h) 应实现设备特权用户的权限分离，系统不支持的应部署日志服务器保证管理员的操作能够被审计，并且网络特权用户管理员无权对审计记录进行操作；（细化）
- i) 应封闭不需要的网络端口，关闭不需要的网络服务。如需使用SNMP服务，应采用安全性增强版本；并应设定复杂的Community控制字段，不使用Public、Private等默认字段。（新增）

8.1.3 主机安全

8.1.3.1 身份鉴别（S3）

本项要求包括：

- a) 对登录操作系统的用户进行身份标识和鉴别；
- b) **操作系统和数据库系统管理用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。**口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；（细化）

- c) 启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。限制同一用户连续失败登录次数；（增强）
- d) 当对服务器进行远程管理时，采取必要措施，防止鉴别信息在网络传输过程中被窃听；
- e) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；
- f) **应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。**

8.1.3.2 访问控制（S3）

本项要求包括：

- a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
- c) 应实现操作系统和数据库系统特权用户的权限分离；
- d) 应限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
- e) 应及时删除多余的、过期的帐户，避免共享帐户的存在；
- f) 应对重要信息资源设置敏感标记，系统不支持设置敏感标记的，应采用专用安全设备生成敏感标记，用以支持强制访问控制机制；（落实）
- g) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

8.1.3.3 安全审计（G3）

本项要求包括：

- a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；系统不支持该要求的，应以系统运行安全和效率为前提，采用第三方安全审计产品实现审计要求；（落实）
- b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等；（细化）
- c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等；
- e) 应能够通过操作系统自身功能或第三方工具根据记录数据进行分析，并生成审计报表；（细化）
- f) 应保护审计进程，避免受到未预期的中断。

8.1.3.4 剩余信息保护（S3）

本项要求包括：

- a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

8.1.3.5 入侵防范（G3）

本项要求包括：

- a) 操作系统应遵循最小安装的原则，仅安装必要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新，补丁安装前应进行安全性和兼容性测试；（增强）
- b) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
- c) 应能够对重要程序的完整性进行检测，并具有完整性恢复的能力。（增强）

8.1.3.6 恶意代码防范（G3）

本项要求包括：

- a) 应在本机安装防恶意代码软件或独立部署恶意代码防护设备，并及时更新防恶意代码软件版本和恶意代码库；（细化）
- b) 应支持防恶意代码的统一管理；
- c) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

8.1.3.7 资源控制（A3）

本项要求包括：

- a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；
- b) 应根据安全策略设置登录终端的操作超时锁定；
- c) 应根据需要限制单个用户对系统资源的最大或最小使用限度；（细化）
- d) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；
- e) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

8.1.4 应用安全

8.1.4.1 身份鉴别（S3）

本项要求包括：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) 应用系统用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用户在第一次登录系统时修改分发的初始口令，口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；应用软件不得明文存储口令数据；（增强）
- c) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
- d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

8.1.4.2 访问控制（S3）

本项要求包括：

- a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
- b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
- c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；

- d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
- e) 应对重要信息资源设置敏感标记，系统不支持设置敏感标记的，应采用专用安全设备生成敏感标记，用以支持强制访问控制机制；（落实）
- f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

8.1.4.3 安全审计（G3）

本项要求包括：

- a) **应提供覆盖到每个用户的安全审计功能**，对应用系统的用户登录、用户退出、增加用户、修改用户权限等重要安全事件进行审计；（细化）
- b) **应保证审计活动的完整性和连续性，保证无法删除、修改或覆盖审计记录；（落实）**
- c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；
- d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

8.1.4.4 剩余信息保护（S3）

本项要求包括：

- a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- b) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

8.1.4.5 通信完整性（S3）

应采用**密码技术**保证通信过程中数据的完整性；

8.1.4.6 通信保密性（S3）

本项要求包括：

- a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；
- b) 应对通信过程中的**整个报文或会话过程**进行加密。

8.1.4.7 抗抵赖（G3）

本项要求包括：

- a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
- b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能；

8.1.4.8 软件容错（A3）

本项要求包括：

- a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- b) 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

8.1.4.9 资源控制（A3）

本项要求包括：

- a) 当应用系统的通信双方中的一方在一段时间内未作响应，另一方应能够自动结束会话；
- b) 应能够对系统的最大并发会话连接数进行限制；
- c) 应能够对单个帐户的多重并发会话进行限制；
- d) 应能够对一个时间段内可能的并发会话连接数进行限制；
- e) 应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；
- f) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警；
- g) 应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

8.1.5 数据安全

8.1.5.1 数据完整性（S3）

本项要求包括：

- a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
- b) 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

8.1.5.2 数据保密性（S3）

本项要求包括：

- a) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；
- b) 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

8.1.5.3 备份和恢复（A3）

本项要求包括：

- a) 应提供数据本地备份与恢复功能，对重要信息进行备份，数据备份至少每天一次，已有数据备份可完全恢复至备份执行时状态，并对备份可恢复性进行定期演练，备份介质场外存放；（增强）
- b) 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；
- c) 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

8.2 管理要求

8.2.1 安全管理制度

8.2.1.1 管理制度（G3）

本项要求包括：

- a) 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- b) 应对安全管理活动中的各类管理内容建立安全管理制度；
- c) 应对要求管理人员或操作人员执行的日常管理操作建立操作规程；

d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

8.2.1.2 制定和发布 (G3)

本项要求包括：

- a) 应指定或授权专门的部门或人员负责安全管理制度的制定；
- b) 安全管理制度应具有统一的格式，并进行版本控制；
- c) 应组织相关人员对制定的安全管理制度进行论证和审定；
- d) 安全管理制度应通过正式、有效的方式发布；
- e) 安全管理制度应注明发布范围，并对收发文进行登记。

8.2.1.3 评审和修订 (G3)

本项要求包括：

- a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
- b) 定期或在发生重大变更时对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。（细化）

8.2.2 安全管理机构

8.2.2.1 岗位设置 (G3)

本项要求包括：

- a) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
- b) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；
- c) 应成立指导和管理信息安全工作的委员会或领导小组，电力企业主要负责人是本单位信息安全的**第一责任人**，对本单位的网络与信息安全负全面责任；（增强）
- d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

8.2.2.2 人员配备 (G3)

本项要求包括：

- a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
- b) 每个电力企业应配备专职安全管理员，不可兼任；（落实）
- c) 关键事务岗位应配备多人共同管理。

8.2.2.3 资金保障 (G3)

- c) 应保障落实信息系统安全建设、运维及等级保护测评资金等；（新增）
- d) 系统建设资金筹措方案和年度系统维护经费应包括信息安全保障资金项目。（新增）

8.2.2.4 授权和审批 (G3)

本项要求包括：

- a) 应根据各个部门和岗位的职责明确**授权审批事项**、审批部门和批准人等；

- b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- d) 应针对关键活动建立审批流程，并由批准人签字确认，并存档备查。（落实）

8.2.2.5 沟通和合作（G3）

本项要求包括：

- a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；
- b) 应加强与行业信息安全监管部门、公安机关、通信运营商、银行及相关单位和部门的合作与沟通；（细化）
- c) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通；
- d) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- e) 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

8.2.2.6 审核和检查（G3）

本项要求包括：

- a) 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- b) 应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
- d) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

8.2.3 人员安全管理

8.2.3.1 人员录用（G3）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责人员录用；
- b) 应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
- c) 应与安全管理员、系统管理员、网络管理员等关键岗位的人员签署保密协议；（细化）
- d) 应与安全管理员、系统管理员、网络管理员等关键岗位的人员签署岗位安全协议。（细化）

8.2.3.2 人员离岗（G3）

本项要求包括：

- a) 应严格规范人员离岗过程，及时收回离岗员工的所有访问权限；（细化）
- b) 应收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

- c) 只有在收回访问权限和各种证件、设备之后方可办理调离手续，**关键岗位人员离岗须承诺调离后的保密义务后方可离开。（细化）**

8.2.3.3 人员考核（G3）

本项要求包括：

- a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；
- b) **应对安全管理员、系统管理员、网络管理员、信息安全主管或专责等关键岗位的人员进行全面、严格的安全审查和技能考核；（细化）**
- c) **应对考核结果进行记录并保存。**

8.2.3.4 安全意识教育和培训（G3）

本项要求包括：

- a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- b) **应对安全责任和惩戒措施进行书面规定**并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
- c) 应按照行业信息安全要求，**对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划**，对信息安全基础知识、岗位操作规程等进行的培训应至少每年举办一次；（增强）
- d) 应对安全教育和培训的情况和结果进行记录并归档保存。

8.2.3.5 外部人员访问管理（G3）

本项要求包括：

- a) 应确保在外部人员访问受控区域**前先提出书面申请**，批准后由专人全程陪同或监督，并登记备案；
- b) **对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。**

8.2.4 系统建设管理

8.2.4.1 系统定级（G3）

本项要求包括：

- a) 应明确信息系统的边界和安全保护等级；
- b) 应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；
- c) **对于跨电力公司联网运行的信息系统，由电力行业网络与信息安全领导小组办公室统一确定安全保护等级。对于属同一电力公司，但跨省联网运行的信息系统，由公司责任部门统一确定安全保护等级。对于通用信息系统，由领导小组办公室提出安全保护等级建议，运营使用单位自主确定安全保护等级。对于运营使用单位所特有的信息系统，各运营使用单位自行确定安全保护等级。对拟确定为第四级以上信息系统的，由领导小组办公室邀请国家信息安全保护等级专家评审委员会评审。（细化）**
- d) 应确保信息系统的定级结果经过行业信息安全主管部门批准，方可到公安机关备案。（细化）

8.2.4.2 安全方案设计（G3）

本项要求包括：

- a) 应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；
- b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；
- c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；
- d) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；
- e) 应根据等级测评、安全评估的结果每年定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

8.2.4.3 产品采购和使用（G3）

本项要求包括：

- a) 应确保安全产品采购和使用符合国家的有关规定；
- b) 应确保密码产品采购和使用符合国家密码主管部门的要求；
- c) 应指定或授权专门的部门负责产品的采购；
- d) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；
- e) 电力系统专用信息安全产品应经行业主管部门指定的安全机构测评方可采购使用。（新增）

8.2.4.4 自行软件开发（G3）

本项要求包括：

- a) 应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；
- b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
- c) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
- d) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；
- e) 应确保对程序资源库的修改、更新、发布进行授权和批准。

8.2.4.5 外包软件开发（G3）

本项要求包括：

- a) 应根据开发要求检测软件质量；
- b) 应在软件安装之前检测软件包中可能存在的恶意代码；
- c) 应要求开发单位提供软件设计的相关文档和使用指南；
- d) 外包开发的软件应在本单位存有源代码备份，并已通过软件后门等安全性检测。（增强）

8.2.4.6 工程实施（G3）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责工程实施过程的管理；

- b) 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；
- c) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

8.2.4.7 测试验收（G3）

本项要求包括：

- a) 应委托国家或电力行业认可的测评单位对系统进行安全性测试，并出具安全性测试报告；（细化）
- b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
- c) 应对系统测试验收的控制方法和人员行为准则进行书面规定；
- d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
- e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

8.2.4.8 系统交付（G3）

本项要求包括：

- a) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 应对负责系统运行维护的技术人员每年进行相应的技能培训，对安全教育和培训的情况和结果进行记录并归档保存；（细化）
- c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；
- d) 应对系统交付的控制方法和人员行为准则进行书面规定；
- e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

8.2.4.9 系统备案（G3）

本项要求包括：

- a) 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；
- b) 应将系统等级及相关材料报系统主管部门备案；电力企业汇总系统等级及相关信息报电力行业网络与信息安全领导小组办公室备案；（细化）
- c) 跨电力公司联网运行，且由电力行业网络与信息安全领导小组办公室统一确定安全等级的信息系统，领导小组办公室负责统一向公安部办理备案手续。电力公司内部跨省联网运行，且由公司责任部门统一确定安全等级的信息系统，由公司责任部门负责统一向公安部办理备案手续。其它信息系统的由运营使用单位直接向当地设区的市级以上公安机关备案。跨省联网运行的信息系统，在各地运行、应用的分支系统，向当地设区的市级以上公安机关备案。（细化）

8.2.4.10 等级测评（G3）

本项要求包括：

- a) 在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
- b) 应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
- c) 应选择具有国家相关技术资质和安全资质，经电力行业信息安全测评中心批准的测评单位进行等级测评；（增强）
- d) 应指定或授权专门的部门或人员负责等级测评的管理。

8.2.4.11 安全服务商选择（G3）

本项要求包括：

- a) 应选择符合国家及行业有关规定的服务商开展安全服务；（细化）
- b) 应与选定的安全服务商签订安全协议，明确安全责任；（细化）
- c) 应与服务商签订安全服务合同，明确技术支持和服务承诺。（增强）

8.2.5 系统运维管理

8.2.5.1 环境管理（G3）

本项要求包括：

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
- b) **应指定部门负责机房安全**，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
- c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
- d) 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、**工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。**

8.2.5.2 资产管理（G3）

本项要求包括：

- a) 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
- c) **应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；**
- d) **应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。**

8.2.5.3 介质管理（G3）

本项要求包括：

- a) **应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；**
- b) 应建立移动存储介质安全管理制度，对移动存储介质的使用进行管控；（新增）
- c) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；

- d) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；
- e) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；
- f) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；
- g) 对重要数据或软件采用加密介质存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。（增强）

8.2.5.4 设备管理（G3）

本项要求包括：

- a) 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理，每年至少维护一次；
- b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- c) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；
- d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- e) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

8.2.5.5 监控管理和安全管理中心（G3）

本项要求包括：

- a) 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
- b) 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；
- c) 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

8.2.5.6 网络安全管理（G3）

本项要求包括：

- a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- b) 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；

- c) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；
- d) 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
- e) **应实现设备的最小服务配置**，并对配置文件进行定期**离线**备份；
- f) 应保证所有与外部系统的连接均得到授权和批准；
- g) **应依据安全策略允许或者拒绝便携式和移动式设备的网络接入**；
- h) **应定期检查违反规定拨号上网或其他违反网络安全策略的行为**。

8.2.5.7 系统安全管理（G3）

本项要求包括：

- a) 应根据业务需求和系统安全分析确定系统的访问控制策略；
- b) 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；
- c) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；
- d) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；
- e) **应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则**；
- f) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
- g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

8.2.5.8 恶意代码防范管理（G3）

本项要求包括：

- a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
- b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；
- d) **应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报**。

8.2.5.9 密码管理（G3）

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

8.2.5.10 变更管理（G3）

本项要求包括：

- a) 应确认系统中要发生的变更，并制定变更方案；

- b) **应建立变更管理制度**，系统发生变更前，向主管领导申请，变更和变更方案经过**评审、审批**后方可实施变更，并在实施后将变更情况向相关人员通告；
- c) **应建立变更控制的申报和审批文件化程序**，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；
- d) **应建立中止变更并从失败变更中恢复的文件化程序**，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

8.2.5.11 备份与恢复管理（G3）

本项要求包括：

- a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) **应建立备份与恢复管理相关的安全管理制度**，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；
- c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；
- d) **应建立控制数据备份和恢复过程的程序**，对备份过程进行记录，所有文件和记录应妥善保存；
- e) **应定期执行恢复程序**，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

8.2.5.12 安全事件处置（G3）

本项要求包括：

- a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；
- b) 应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；
- d) **应制定安全事件报告和响应处理程序**，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；
- e) **应在安全事件报告和响应处理过程中**，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；
- f) **对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。**

8.2.5.13 应急预案管理（G3）

本项要求包括：

- a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
- b) **应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；**

- c) 应对安全管理员、系统管理员、网络管理员等相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；（细化）
- d) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
- e) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

第三部分：生产控制信息系统类要求

9 总体要求

9.1 总体技术要求

- a) 电力生产企业、电网企业、供电企业内部基于计算机和网络技术的业务系统，原则上划分为生产控制大区和管理信息大区，生产控制大区可以分为控制区（又称安全区I）和非控制区（又称安全区II）；（新增）
- b) 生产控制大区网络与管理信息大区网络应物理隔离；两网之间有信息通信交换时应部署符合电力系统要求的单向隔离装置，确保单向隔离装置策略配置安全有效，禁止任何穿越边界的E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务；（新增）
- c) 在生产控制大区与广域网的纵向交接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施，确保纵向加密认证装置策略配置安全有效，实现双向身份认证、数据加密和访问控制；（新增）
- d) 电力调度数据网应当在专用通道上使用独立的网络设备组网，在物理层面上实现与其它数据网及外部公共信息网的安全隔离；（新增）
- e) 控制区的信息系统数据通信应使用电力调度数据网的实时子网或专用通道进行传输，非控制区的信息系统数据通信应使用电力调度数据网的非实时子网；（新增）
- f) 控制区与非控制区之间应采用国产防火墙，或采用具有访问控制功能的设备进行隔离；（新增）
- g) 二级系统统一成域，三级及以上系统单独成域；（新增）
- h) 三级及以上系统域由独立子网承载，每个域有唯一网络出口，可在网络出口处部署满足相应等级要求的等级保护专用装置为系统提供整体安全防护；（注1：等级保护装置）（新增）
- i) 省级以上及有实际业务需要的地区调度中心的电力监控系统、电力调度数据网上的关键应用、关键用户和关键设备应使用电力调度数字证书系统实现身份认证、安全数据传输及鉴权；（新增）
- j) 生产控制大区所部署的安全审计系统，可对网络运行日志、操作系统运行日志、数据库访问日志、业务应用系统运行日志、安全设施运行日志等进行集中收集、自动分析。（新增）

9.2 总体管理要求

- a) 如果本单位生产控制大区仅有一级信息系统时，通用管理要求等同采用一级；（新增）
- b) 如果本单位生产控制大区含有二级及以下等级信息系统时，通用管理要求等同采用二级；（新增）
- c) 如果本单位生产控制大区含有三级及以下等级信息系统时，通用管理要求等同采用三级；（新增）
- d) 如果本单位生产控制大区含有四级及以下等级信息系统时，通用管理要求等同采用四级。（新增）

10 第一级基本要求

10.1 技术要求

10.1.1 物理安全

10.1.1.1 物理访问控制（G1）

机房出入应安排专人负责，控制、鉴别和记录进入的人员。

10.1.1.2 防盗窃和防破坏（G1）

本项要求包括：

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记。

10.1.1.3 防雷击（G1）

机房建筑应设置避雷装置。

10.1.1.4 防火（G1）

机房应设置灭火设备。

10.1.1.5 防水和防潮（G1）

本项要求包括：

- a) 应对穿过机房墙壁和楼板的水管增加必要的保护措施；
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

10.1.1.6 温湿度控制（G1）

机房应设置必要的温、湿度控制设施，使机房温、湿度的变化在设备运行所允许的范围之内。

10.1.1.7 电力供应（A1）

应在机房供电线路上配置稳压器和过电压防护设备。

10.1.2 网络安全

10.1.2.1 结构安全（G1）

本项要求包括：

- a) 应保证关键网络设备的业务处理能力满足基本业务需要；
- b) 应保证接入网络 and 核心网络的带宽满足基本业务需要；
- c) 应绘制与当前运行情况相符的网络拓扑结构图。

10.1.2.2 访问控制（G1）

本项要求包括：

- a) 应在网络边界部署访问控制设备，启用访问控制功能；
- b) 应根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包出入；
- c) 应通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度至少为用户组。

10.1.2.3 网络设备防护（G1）

本项要求包括：

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

c) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

10.1.3 主机安全

10.1.3.1 身份鉴别（S1）

应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

10.1.3.2 访问控制（S1）

本项要求包括：

- a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 应限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
- c) 应及时删除多余的、过期的帐户，避免共享帐户的存在。

10.1.3.3 入侵防范（G1）

操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更新。

10.1.3.4 恶意代码防范（G1）

应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。

10.1.4 应用安全

10.1.4.1 身份鉴别（S1）

本项要求包括：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- c) 应启用身份鉴别和登录失败处理功能，并根据安全策略配置相关参数。

10.1.4.2 访问控制（S1）

本项要求包括：

- a) 应提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；
- b) 应由授权主体配置访问控制策略，并严格限制默认用户的访问权限。

10.1.4.3 通信完整性（S1）

应采用约定通信会话方式的方法保证通信过程中数据的完整性。

10.1.4.4 软件容错（A1）

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

10.1.5 数据安全及备份恢复

10.1.5.1 数据完整性（S1）

应能够检测到重要用户数据在传输过程中完整性受到破坏。

10.1.5.2 备份和恢复（A1）

应能够对重要信息进行备份和恢复。

10.2 管理要求

10.2.1 安全管理制度

10.2.1.1 管理制度（G1）

本项要求包括：

- a) 应按照“谁主管谁负责，谁运营谁负责”的原则，建立电力二次系统安全管理制度，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将电力二次系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理；（新增）
- b) 应对安全管理活动中重要的管理内容建立安全管理制度，主要包括：门禁管理、人员管理、权限管理、访问控制管理、安全防护系统的维护管理、常规设备及各系统的维护管理、恶意代码的防护管理、审计管理、数据及系统的备份管理、用户口令密钥及数字证书的管理、培训管理等。（增强）

10.2.1.2 制定和发布（G1）

本项要求包括：

- a) 应指定或授权专门的人员负责安全管理制度的制定；
- b) 应将安全管理制度以某种方式发布到相关人员手中。

10.2.2 安全管理机构

10.2.2.1 岗位设置（G1）

本项要求包括：

- a) 应明确由主管安全生产的领导作为电力二次系统安全防护的主要责任人；（新增）
- b) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。

10.2.2.2 资金保障（G1）

本项要求包括：

- a) 应保障落实电力二次系统安全建设、运维及等级保护测评资金等；（新增）
- b) 系统建设资金筹措方案和年度系统维护经费应包括信息安全保障资金项目。（新增）

10.2.2.3

10.2.2.4 人员配备（G1）

应配备一定数量的系统管理员、网络管理员、安全管理员等。

10.2.2.5 授权和审批（G1）

本项要求包括：

- a) 应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批。
- b) 接入电力调度数据网络的节点、设备和应用系统，其接入技术方案和安全防护措施须经负责本级电力调度数据网络的调度机构核准。（新增）

10.2.2.6 沟通和合作（G1）

应加强与行业信息监管部门、公安机关、通信运营商、银行及相关单位和部门的合作与沟通。（细化）

10.2.3 人员安全管理

10.2.3.1 人员录用（G1）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责人员录用；
- b) 应对被录用人员的身份和专业资格等进行审查，并确保其具有基本的专业技术水平和安全管理知识。

10.2.3.2 人员离岗（G1）

本项要求包括：

- a) 应立即终止由于各种原因离岗员工的所有访问权限；
- b) 应收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。（落实）

10.2.3.3 安全意识教育和培训（G1）

本项要求包括：

- a) 应对各类人员进行安全意识教育和岗位技能培训；
- b) 应告知人员相关的安全责任和惩戒措施。
- c) 应按照行业信息安全要求，制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行的培训至少每年举办一次。（新增）

10.2.3.4 外部人员访问管理（G1）

应确保在外部人员访问受控区域前得到授权或审批。

10.2.4 系统建设管理

10.2.4.1 系统定级（G1）

本项要求包括：

- a) 应明确信息系统的边界和安全保护等级；
- b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由；
- c) 应确保信息系统的定级结果经过行业信息安全主管部门等相关部门的批准。（细化）

10.2.4.2 安全方案设计（G1）

本项要求包括：

- a) 应根据系统的安全保护等级选择基本安全措施，并依据电力二次系统安全防护要求和风险分析的结果补充和调整安全措施；（增强）
- b) 应以书面的形式描述对系统的安全保护要求和策略、安全措施等内容，形成系统的安全方案；
- c) 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。

10.2.4.3 产品采购和使用（G1）

本项要求包括：

- a) 应确保安全产品采购和使用符合国家的有关规定。
- b) 接入电力二次系统生产控制大区中的安全产品，其功能、性能应获得国家或行业指定机构安全检测证明，其电磁兼容性还需有电力系统电磁兼容检测证明。（新增）

10.2.4.4 自行软件开发（G1）

本项要求包括：

- a) 应确保开发环境与实际运行环境物理分开；
- b) 应确保软件设计相关文档由专人负责保管。

10.2.4.5 外包软件开发（G1）

本项要求包括：

- a) 应根据开发要求检测软件质量；
- b) 应在软件安装之前检测软件包中可能存在的恶意代码；
- c) 应确保提供软件设计的相关文档和使用指南；

- d) 应在外包开发合同中明确开发单位、供应商所提供的电力二次设备及系统应包含保密、生命周期、禁止关键技术和设备扩散等方面的条款。（新增）

10.2.4.6 工程实施（G1）

应指定或授权专门的部门或人员负责工程实施过程的管理。

10.2.4.7 测试验收（G1）

本项要求包括：

- a) 应对系统进行安全性测试验收；
- b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

10.2.4.8 系统交付（G1）

本项要求包括：

- a) 应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 应对负责系统运行维护的技术人员进行相应的技能培训；
- c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

10.2.4.9 安全服务商选择（G1）

本项要求包括：

- a) 应选择符合国家及行业有关规定的服务商开展安全服务；（增强）
- b) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。

10.2.5 系统运维管理

10.2.5.1 环境管理（G1）

本项要求包括：

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
- b) 应对机房的出入、服务器的开机或关机等工作进行管理；
- c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。

10.2.5.2 资产管理（G1）

应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

10.2.5.3 介质管理（G1）

本项要求包括：

- a) 应建立生产控制大区移动存储介质安全管理制度，对移动存储介质的使用进行限制；（新增）
- b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护；
- c) 应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点。

10.2.5.4 设备管理（G1）

本项要求包括：

- a) 应对信息系统相关的各种设备、线路等指定专门的部门或人员定期进行维护管理；
- b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。

10.2.5.5 网络安全管理（G1）

本项要求包括：

- a) 应指定人员对网络进行管理,负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作;
- b) 应定期进行网络系统漏洞扫描,对发现的网络系统安全漏洞进行及时的修补。

10.2.5.6 系统安全管理 (G1)

本项要求包括:

- a) 应根据业务需求和系统安全分析确定系统的访问控制策略;
- b) 应定期进行漏洞扫描,对发现的系统安全漏洞进行及时的修补;
- c) 应安装系统的最新补丁程序,在安装系统补丁前,应首先在测试环境中测试通过,并对重要文件进行备份后,方可实施系统补丁程序的安装; (增强)
- d) 电力调度机构应指定专人负责管理本级调度数字证书系统。(新增)

10.2.5.7 恶意代码防范管理 (G1)

本项要求包括:

- a) 应提高所有用户的防病毒意识,告知及时升级防病毒软件,在读取移动存储设备上的数据以及网络上接收文件或邮件之前,先进行病毒检查,对外来计算机或存储设备接入网络系统之前也应进行病毒检查;
- b) 在更新恶意代码库、木马库以及IDS规则库前,应首先在测试环境中测试通过,更新操作应离线进行,生产控制大区恶意代码更新应由专人负责,并保存更新记录。(新增)

10.2.5.8 备份与恢复管理 (G1)

本项要求包括:

- a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等;
- b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等。

10.2.5.9 安全事件处置 (G1)

本项要求包括:

- a) 应建立电力二次系统联合防护和应急机制,负责处置跨部门电力二次系统安全事件; (新增)
- b) 应报告所发现的安全弱点和可疑事件,但任何情况下用户均不应尝试验证弱点;
- c) 应制定安全事件报告和处置管理制度,规定安全事件的现场处理、事件报告和后期恢复的管理职责。

11 第二级基本要求

11.1 技术要求

11.1.1 物理安全

11.1.1.1 物理位置的选择 (G2)

机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。

11.1.1.2 物理访问控制 (G2)

本项要求包括:

- a) 机房各出入口应安排专人值守或配置电子门禁系统,控制、鉴别和记录进入的人员; (增强)
- b) 进入机房的来访人员应经过申请和审批流程,并限制和监控其活动范围。

11.1.1.3 防盗窃和防破坏 (G2)

本项要求包括:

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
- c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 主机房应安装必要的防盗报警设施。

11.1.1.4 防雷击（G2）

本项要求包括：

- a) 机房建筑应设置避雷装置；
- b) 机房应设置交流电源地线。

11.1.1.5 防火（G2）

机房应设置灭火设备和火灾自动报警系统。

11.1.1.6 防水和防潮（G2）

本项要求包括：

- a) 主机房尽量避开水源，与主机房无关的给排水管道不得穿过主机房，与主机房相关的给排水管道必须有可靠的防渗漏措施；（增强）
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

11.1.1.7 防静电（G2）

主要设备采用必要的接地防静电措施。（增强）

11.1.1.8 温湿度控制（G2）

机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

11.1.1.9 电力供应（A2）

本项要求包括：

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期的备用电力供应，至少满足关键设备在断电情况下的正常运行要求。

11.1.1.10 电磁防护（S2）

电源线和通信线缆应隔离铺设，避免互相干扰。

11.1.2 网络安全

11.1.2.1 结构安全（G2）

本项要求包括：

- a) 应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
- b) 应保证网络各个部分的带宽满足业务高峰期需要；（增强）
- c) 应绘制完整的网络拓扑结构图，有相应的网络配置表，包含设备IP地址等主要信息，与当前运行情况相符；（增强）
- d) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

11.1.2.2 访问控制（G2）

本项要求包括：

- a) 应在网络边界部署访问控制设备，启用访问控制功能；

- b) 访问控制设备应根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；（增强）
- c) 应按用户和系统之间的允许访问规则，边界的网络控制设备决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。以拨号或VPN等方式接入网络的，应采用强认证方式，并对用户访问权限进行严格限制；（增强）
- d) 生产控制大区的拨号访问服务，服务器和客户端均应使用经安全加固的达到国家二级等级保护要求的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施；（新增）
- e) 应该采用严格的接入控制措施，保证业务系统接入的可信性。经过授权的节点允许接入电力调度数据网，进行广域网通信；（新增）
- f) 应限制具有拨号、VPN等访问权限的用户数量。（增强）

11.1.2.3 安全审计（G2）

本项要求包括：

- a) 应在生产控制大区应部署专用审计系统，或启用设备或系统审计功能，应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；（增强）
- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

11.1.2.4 边界完整性检查（S2）

应能够对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。

11.1.2.5 入侵防范（G2）

应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。

11.1.2.6 网络设备防护（G2）

本项要求包括：

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应对网络设备的管理员登录地址进行限制；
- c) 网络设备标识应唯一；同一网络设备的用户标识应唯一；禁止多个人员共用一个账号；（增强）
- d) 身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应修改默认用户和口令，不得使用缺省口令，口令长度不得小于8位，要求是字母和数字或特殊字符的混合并不得与用户名相同，口令应定期更换，并加密存储；（增强）
- e) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
- f) 当对网络设备进行远程管理时，采取必要措施防止鉴别信息在网络传输过程中被窃听；
- g) 应封闭不需要的网络端口，关闭不需要的网络服务。如需使用SNMP服务，应采用安全性增强版本；并应设定复杂的Community控制字段，不使用Public、Private等默认字段。（新增）

11.1.3 主机安全

11.1.3.1 身份鉴别（S2）

本项要求包括：

- a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
- b) 操作系统和数据库系统管理用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；（增强）

- c) 启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。限制同一用户连续失败登录次数；（增强）
- d) 当对服务器进行远程管理时，采取必要措施，防止鉴别信息在网络传输过程中被窃听；
- e) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

11.1.3.2 访问控制（S2）

本项要求包括：

- a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 应实现操作系统和数据库系统特权用户的权限分离；
- c) 应限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
- d) 应及时删除多余的、过期的帐户，避免共享帐户的存在。

11.1.3.3 安全审计（G2）

本项要求包括：

- a) 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户；系统不支持该要求的，应以系统运行安全和效率为前提，采用第三方安全审计产品实现审计要求；（增强）
- b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等；（细化）
- c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

11.1.3.4 入侵防范（G2）

操作系统应遵循最小安装的原则，仅安装必要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新，补丁安装前应进行安全性和兼容性测试。（增强）

11.1.3.5 恶意代码防范（G2）

本项要求包括：

- a) 应在本机安装防恶意代码软件或独立部署恶意代码防护设备，并及时更新防恶意代码软件版本和恶意代码库；（增强）
- b) 应支持防恶意代码的统一管理。

11.1.3.6 资源控制（A2）

本项要求包括：

- a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；
- b) 应根据安全策略设置登录终端的操作超时锁定；
- c) 应根据需要限制单个用户对系统资源的最大或最小使用限度。
- d) 应关闭或拆除主机的软盘驱动、光盘驱动、USB接口、串行口等，确需保留的必须通过安全管理平台实施严格管理。（新增）

11.1.4 应用安全

11.1.4.1 身份鉴别（S2）

本项要求包括：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) 应用系统用户身份鉴别信息应不易被冒用，口令复杂度应满足要求，并定期更换口令。应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用

户在第一次登录系统时修改分发的初始口令，口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；应用软件不得明文存储口令数据；（增强）

- c) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- a) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

11.1.4.2 访问控制（S2）

本项要求包括：

- a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
- b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
- c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；
- a) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

11.1.4.3 安全审计（G2）

本项要求包括：

- a) 应提供覆盖到每个用户的安全审计功能，对应用系统的用户登录、用户退出、增加用户、修改用户权限等重要安全事件进行审计；（增强）
- b) 应保证审计活动的完整性，保证无法删除、修改或覆盖审计记录；（增强）
- c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

11.1.4.4 通信完整性（S2）

应采用校验码技术保证通信过程中数据的完整性。

11.1.4.5 通信保密性（S2）

本项要求包括：

- a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；
- b) 应对通信过程中的用户口令、会话密钥等敏感信息字段进行加密。（细化）

11.1.4.6 软件容错（A2）

本项要求包括：

- a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- b) 在故障发生时，应用系统应能够继续提供部分功能，确保系统能够实施恢复措施。

11.1.4.7 资源控制（A2）

本项要求包括：

- a) 当应用系统的通信双方中的一方在一段时间内未作响应，另一方应能够自动结束会话；
- b) 应能够对应用系统的最大并发会话连接数进行限制；
- c) 应能够对单个帐户的多重并发会话进行限制。

11.1.5 数据安全

11.1.5.1 数据完整性（S2）

应能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。

11.1.5.2 数据保密性（S2）

应采用加密或其他保护措施实现鉴别信息的存储保密性。

11.1.5.3 备份和恢复（A2）

本项要求包括：

- a) 应对重要信息进行备份和恢复；
- b) 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

11.2 管理要求

11.2.1 安全管理制度

11.2.1.1 管理制度（G2）

本项要求包括：

- a) 应按照“谁主管谁负责，谁运营谁负责”的原则，建立电力二次系统安全管理制度，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将电力二次系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理；（细化）
- b) 应对安全管理活动中重要的管理内容建立安全管理制度，主要包括：门禁管理、人员管理、权限管理、访问控制管理、安全防护系统的维护管理、常规设备及各系统的维护管理、恶意代码的防护管理、审计管理、数据及系统的备份管理、用户口令密钥及数字证书的管理、培训管理等；（增强）
- c) 应对安全管理人员或操作人员执行的重要管理操作建立操作规程。

11.2.1.2 制定和发布（G2）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责安全管理制度的制定；
- b) 应组织相关人员对制定的安全管理制度进行论证和审定；
- c) 应将安全管理制度以某种方式发布到相关人员手中。

11.2.1.3 评审和修订（G2）

定期或在发生重大变更时对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。（增强）

11.2.2 安全管理机构

11.2.2.1 岗位设置（G2）

本项要求包括：

- a) 应明确由主管安全生产的领导作为电力二次系统安全防护的主要责任人；
- b) 应设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
- c) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。

11.2.2.2 人员配备（G2）

本项要求包括：

- a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
- b) 安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。

11.2.2.3 资金保障（G2）

本项要求包括：

- a) 应保障落实电力二次系统安全建设、运维及等级保护测评资金等；（新增）
- b) 系统建设资金筹措方案和年度系统维护经费应包括信息安全保障资金项目。（新增）

11.2.2.4 授权和审批（G2）

本项要求包括：

- a) 应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批；
- b) 应针对关键活动建立审批流程，并由批准人签字确认；
- c) 接入电力调度数据网络的节点、设备、和应用系统，其接入技术方案和安全防护措施须经负责本级电力调度数据网络的调度机构核准。（增强）

11.2.2.5 沟通和合作（G2）

本项要求包括：

- a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通；（细化）
- b) 应加强与行业信息安全监管部门、公安机关、通信运营商、银行及相关单位和部门的合作与沟通。（细化）

11.2.2.6 审核和检查（G2）

安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

11.2.3 人员安全管理

11.2.3.1 人员录用（G2）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责人员录用；
- b) 应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核；
- c) 应与安全管理员、系统管理员、网络管理员等关键岗位的人员签署保密协议。（细化）

11.2.3.2 人员离岗（G2）

本项要求包括：

- a) 应规范人员离岗过程，及时终止离岗员工的所有访问权限；
- b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
- c) 只有在收回访问权限和各种证件、设备之后方可办理调离手续。（细化）

11.2.3.3 人员考核（G2）

应定期对各个岗位的人员进行安全技能及安全认知的考核。

11.2.3.4 安全意识教育和培训（G2）

本项要求包括：

- a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- b) 应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒；
- c) 应按照行业信息安全要求，制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行的培训应至少每年举办一次。（增强）

11.2.3.5 外部人员访问管理（G2）

应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。

11.2.4 系统建设管理

11.2.4.1 系统定级（G2）

本项要求包括：

- a) 应明确信息系统的边界和安全保护等级；
- b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由；
- c) **应确保信息系统的定级结果经过行业信息安全主管部门批准，方可到公安机关备案。（增强）**

11.2.4.2 安全方案设计（G2）

本项要求包括：

- a) 应根据系统的安全保护等级选择基本安全措施，并依据电力二次系统安全防护要求和风险分析的结果补充和调整安全措施；
- b) 应以书面形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案；
- c) 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案；
- d) **应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并经过上级信息安全主管部门和相应电力调度机构的审核，方案实施完成后应当由相关机构共同组织验收。（增强）**

11.2.4.3 产品采购和使用（G2）

本项要求包括：

- a) 应确保安全产品采购和使用符合国家的有关规定；
- b) **应确保密码产品采购和使用符合国家密码主管部门的要求；**
- c) **应指定或授权专门的部门负责产品的采购；**
- d) **接入电力二次系统生产控制大区中的安全产品，其功能、性能应获得国家或行业指定机构安全检测证明，其电磁兼容性还需有电力系统电磁兼容检测证明。（新增）**

11.2.4.4 自行软件开发（G2）

本项要求包括：

- a) 应确保开发环境与实际运行环境物理分开；
- b) **应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；**
- c) 应确保提供软件设计的相关文档**和使用指南**，并由专人负责保管。

11.2.4.5 外包软件开发（G2）

本项要求包括：

- a) 应根据开发要求检测软件质量；
- b) 应确保提供软件设计的相关文档和使用指南；
- c) 应在软件安装之前检测软件包中可能存在的恶意代码；
- d) **应在外包开发合同中明确开发单位、供应商所提供的电力二次设备及系统应包含保密、生命周期、禁止关键技术和设备扩散等方面的条款；（增强）**
- e) **外包开发的软件应在本单位存有源代码备份，并已通过软件后门等安全性检测。（细化）**

11.2.4.6 工程实施（G2）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) **应制定详细的工程实施方案，控制工程实施过程。**

11.2.4.7 测试验收（G2）

本项要求包括：

- a) 应对系统进行安全性测试验收；

- b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案,在测试验收过程中应详细记录测试验收结果,并形成测试验收报告;
- c) **应组织相关部门和相关人员对系统测试验收报告进行审定,并签字确认。**

11.2.4.8 系统交付 (G2)

本项要求包括:

- a) 应制定系统交付清单,并根据交付清单对所交接的设备、软件和文档等进行清点;
- b) 应对负责系统运行维护的技术人员进行相应的技能培训;
- c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

11.2.4.9 安全服务商选择 (G2)

本项要求包括:

- a) 应选择符合国家及行业有关规定的服务商开展安全服务; (增强)
- b) 应与选定的安全服务商签订安全协议,明确安全责任; (增强)
- c) 应与服务商签订安全服务合同,确保提供技术培训,并明确服务承诺。 (增强)

11.2.5 系统运维管理

11.2.5.1 环境管理 (G2)

本项要求包括:

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理;
- b) 应配备机房安全管理人员,对机房的出入、服务器的开机或关机等工作进行管理;
- c) 应建立机房安全管理制度,对有关机房物理访问,物品带进、带出机房和机房环境安全等方面的管理作出规定;
- d) **应加强对办公环境的保密性管理,包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。**

11.2.5.2 资产管理 (G2)

本项要求包括:

- a) 应编制与信息系统相关的资产清单,包括资产责任部门、重要程度和所处位置等内容;
- b) **应建立资产安全管理制度,规定信息系统资产管理的责任人员或责任部门,并规范资产管理和使用的行为。**

11.2.5.3 介质管理 (G2)

本项要求包括:

- a) 应建立生产控制大区移动存储介质安全管理制度,对移动存储介质的使用进行严格限制; (增强)
- b) 应确保介质存放在安全的环境中,对各类介质进行控制和保护, **并实行存储环境专人管理;**
- c) 应对介质归档和查询等过程进行记录,并根据存档介质的目录清单定期盘点;
- d) **应对需要送出维修或销毁的介质,首先清除其中的敏感数据,防止信息的非法泄漏;**
- e) **应根据所承载数据和软件的重要程度对介质进行分类和标识管理。**

11.2.5.4 设备管理 (G2)

本项要求包括:

- a) 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- c) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- d) 应确保信息处理设备必须经过审批才能带离机房或办公地点；
- e) 应确保信息处理设备必须经过审批才能带入机房或办公地点。（新增）

11.2.5.5 网络安全管理（G2）

本项要求包括：

- a) 应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- b) 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；
- c) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；
- d) 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
- e) 应对网络设备的配置文件进行定期备份；
- f) 应保证所有与外部系统的连接均得到授权和批准。

11.2.5.6 系统安全管理（G2）

本项要求包括：

- a) 应根据业务需求和系统安全分析确定系统的访问控制策略；
- b) 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；
- c) 应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；
- d) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定；
- e) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
- f) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为；
- g) 电力调度机构应指定专人负责管理本级调度数字证书系统。（增强）

11.2.5.7 恶意代码防范管理（G2）

本项要求包括：

- a) 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
- b) 在更新恶意代码库、木马库以及IDS规则库前，应首先在测试环境中测试通过，更新操作应离线进行，生产控制大区恶意代码更新应由专人负责，并保存更新记录；（新增）
- c) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；

d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

11.2.5.8 密码管理（G2）

应使用符合国家密码管理规定的密码技术和产品。

11.2.5.9 变更管理（G2）

本项要求包括：

- a) 应确认系统中要发生的重要变更，并制定相应的变更方案；
- b) 系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告。

11.2.5.10 备份与恢复管理（G2）

本项要求包括：

- a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；
- c) 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法。

11.2.5.11 安全事件处置（G2）

本项要求包括：

- a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；
- b) 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；
- d) 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生；
- e) 应建立电力二次系统联合防护和应急机制，负责处置跨部门电力二次系统安全事件。（新增）

11.2.5.12 应急预案管理（G2）

本项要求包括：

- a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
- b) 应制定电力二次系统联合防护和应急处置预案，并经过演练；（新增）
- c) 应对安全管理员、系统管理员、网络管理员等相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。（增强）

12 第三级基本要求

12.1 技术要求

12.1.1 物理安全

12.1.1.1 物理位置的选择（G3）

本项要求包括：

- a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

- b) 机房场地应避免设在建筑物的高层或地下室, 以及用水设备的下层或隔壁, 如果不可避免, 应采取有效防水措施。 (落实)

12.1.1.2 物理访问控制 (G3)

本项要求包括:

- a) 机房各出入口应安排专人值守或配置电子门禁系统, 控制、鉴别和记录进入的人员; (增强)
- b) 进入机房的来访人员应经过申请和审批流程, 并限制和监控其活动范围;
- c) 应对机房划分区域进行管理, 区域和区域之间应用物理方式隔断, 在重要区域前设置交付或安装等过渡区域; (增强)
- d) 重要区域应配置电子门禁系统, 控制、鉴别和记录进入的人员。

12.1.1.3 防盗窃和防破坏 (G3)

本项要求包括:

- a) 应将主要设备放置在机房内;
- b) 应将设备或主要部件进行固定, 并设置明显的不易除去的标记;
- c) 应将通信线缆铺设在隐蔽处, 可铺设在地下或管道中;
- d) 应对介质分类标识, 存储在介质库或档案室中;
- e) 应利用光、电等技术设置机房防盗报警系统;
- f) 应对机房设置监控报警系统。

12.1.1.4 防雷击 (G3)

本项要求包括:

- a) 机房建筑应设置避雷装置;
- b) 应设置防雷保安器, 防止感应雷;
- c) 机房应设置交流电源地线。

12.1.1.5 防火 (G3)

本项要求包括:

- a) 机房应设置火灾自动消防系统, 能够自动检测火情、自动报警, 自动灭火;
- b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料;
- c) 机房应采取区域隔离防火措施, 将重要设备与其他设备隔离开。

12.1.1.6 防水和防潮 (G3)

本项要求包括:

- a) 主机房尽量避开水源, 与主机房无关的给排水管道不得穿过主机房, 与主机房相关的给排水管道必须有可靠的防渗漏措施; (增强)
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透;
- c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透;
- d) 应安装对水敏感的检测仪表或元件, 对机房进行防水检测和报警。

12.1.1.7 防静电 (G3)

本项要求包括:

- a) 主要设备采用必要的接地防静电措施;
- b) 机房应采用防静电地板。

12.1.1.8 温湿度控制 (G3)

机房应设置温、湿度自动调节设施, 使机房温、湿度的变化在设备运行所允许的范围之内。

12.1.1.9 电力供应 (A3)

本项要求包括：

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求；
- c) 设置冗余或并行的电力电缆线路为计算机系统供电，输入电源应采用双路自动切换供电方式；
(增强)
- d) 应建立备用供电系统。

12.1.1.10 电磁防护 (S3)

本项要求包括：

- a) 电源线和通信线缆应隔离铺设，避免互相干扰；
- b) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；
- c) 应对关键设备和磁介质实施电磁屏蔽。

12.1.2 网络安全

12.1.2.1 结构安全 (G3)

本项要求包括：

- a) 应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
- b) 应保证网络各个部分的带宽满足业务高峰期需要；
- c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；
- d) 应绘制完整的网络拓扑结构图，有相应的网络配置表，包含设备IP地址等主要信息，与当前运行情况相符； (增强)
- e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；
- f) 单个系统应单独划分安全域，系统由独立子网承载，每个域的网络出口应唯一； (新增)
- g) 采用冗余技术设计网络拓扑结构，提供主要网络设备、通信线路的硬件冗余，避免关键节点存在单点故障； (增强)
- h) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保障重要业务服务的带宽。 (增强)

12.1.2.2 访问控制 (G3)

本项要求包括：

- a) 应在网络边界部署访问控制设备，启用访问控制功能；
- b) 访问控制设备应根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； (增强)
- c) 应按用户和系统之间的允许访问规则，边界的网络控制设备决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。以拨号或VPN等方式接入网络的，应采用强认证方式，并对用户访问权限进行严格限制； (增强)
- d) 生产控制大区的拨号访问服务，服务器均应使用经安全加固的达到国家三级等级保护要求的操作系统，客户端应使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施； (新增)
- e) 应限制具有拨号、VPN等访问权限的用户数量； (增强)

- f) 应该采用严格的接入控制措施，保证业务系统接入的可信性。经过授权的节点允许接入电力调度数据网，进行广域网通信；（新增）
- g) 应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；
- h) 应在会话处于非活跃一定时间或会话结束后终止网络连接；
- i) 在网络出口和核心网络接口处应限制网络最大流量数及网络连接数；（落实）
- j) 重要网段应采取技术手段防止地址欺骗。

12.1.2.3 安全审计（G3）

本项要求包括：

- a) 应在生产控制大区应部署专用审计系统，或启用设备或系统审计功能，应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；（增强）
- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- c) 应能够根据记录数据进行分析，并生成审计报表，网络设备不支持的应采用第三方工具生成审计报表；（增强）
- d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

12.1.2.4 边界完整性检查（S3）

本项要求包括：

- c) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；
- d) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

12.1.2.5 入侵防范（G3）

本项要求包括：

- a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等；
- b) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

12.1.2.6 恶意代码防范（G3）

本项要求包括：

- a) 应在网络边界处对恶意代码进行检测和清除；
- b) 应维护恶意代码库的升级和检测系统的更新。

12.1.2.7 网络设备防护（G3）

本项要求包括：

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应对网络设备的管理员登录地址进行限制；
- c) 网络设备标识应唯一；同一网络设备的用户标识应唯一；禁止多个人员共用一个账号；（增强）
- d) 身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应修改默认用户和口令，不得使用缺省口令，口令长度不得小于8位，要求是字母和数字或特殊字符的混合并不得与用户名相同，口令应定期更换，并加密存储；（增强）
- e) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

- f) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
- g) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
- h) 应实现设备特权用户的权限分离，系统不支持的应部署日志服务器保证管理员的操作能够被审计，并且网络特权用户管理员无权对审计记录进行操作；（增强）
- i) 应封闭不需要的网络端口，关闭不需要的网络服务。如需使用SNMP服务，应采用安全性增强版本；并应设定复杂的Community控制字段，不使用Public、Private等默认字段。（新增）

12.1.3 主机安全

12.1.3.1 身份鉴别（S3）

本项要求包括：

- a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
- b) 操作系统和数据库系统管理用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；（增强）
- c) 启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。限制同一用户连续失败登录次数；（增强）
- d) 当对服务器进行远程管理时，采取必要措施，防止鉴别信息在网络传输过程中被窃听；
- e) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；
- f) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

12.1.3.2 访问控制（S3）

本项要求包括：

- a) 应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
- c) 应实现操作系统和数据库系统特权用户的权限分离；
- d) 应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
- e) 应及时删除多余的、过期的帐户，避免共享帐户的存在；
- f) 应对重要信息资源设置敏感标记，系统不支持设置敏感标记的，应采用专用安全设备生成敏感标记，用以支持强制访问控制机制；（落实）
- g) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

12.1.3.3 安全审计（G3）

本项要求包括：

- a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；系统不支持该要求的，应以系统运行安全和效率为前提，采用第三方安全审计产品实现审计要求；（增强）
- b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等；（细化）
- c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等；
- e) 应能够通过操作系统自身功能或第三方工具根据记录数据进行分析，并生成审计报表；（增强）
- f) 应保护审计进程，避免受到未预期的中断。

12.1.3.4 剩余信息保护（S3）

本项要求包括：

- a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

12.1.3.5 入侵防范（G3）

- a) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
- b) 应能够对重要程序的完整性进行检测，并具有完整性恢复的能力；（落实）
- c) 操作系统应遵循最小安装的原则，仅安装必要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新，补丁安装前应进行安全性和兼容性测试。（增强）

12.1.3.6 恶意代码防范（G3）

本项要求包括：

- a) 应在本机安装防恶意代码软件或独立部署恶意代码防护设备，并及时更新防恶意代码软件版本和恶意代码库；（增强）
- b) 应支持防恶意代码的统一管理；
- c) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

12.1.3.7 资源控制（A3）

本项要求包括：

- a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；
- b) 应根据安全策略设置登录终端的操作超时锁定；
- c) 应根据需要限制单个用户对系统资源的最大或最小使用限度；
- d) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；
- e) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警；
- f) 应关闭或拆除主机的软盘驱动、光盘驱动、USB接口、串行口等，确需保留的必须通过安全管理平台实施严格管理。（新增）

12.1.4 应用安全

12.1.4.1 身份鉴别（S3）

本项要求包括：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) 应用系统用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用户在第一次登录系统时修改分发的初始口令，口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；应用软件不得明文存储口令数据；（增强）
- c) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；
- d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

12.1.4.2 访问控制（S3）

本项要求包括：

- a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
- b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
- c) 应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；
- d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
- e) 应对重要信息资源设置敏感标记，系统不支持设置敏感标记的，应采用专用安全设备生成敏感标记，用以支持强制访问控制机制；
- f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

12.1.4.3 安全审计（G3）

本项要求包括：

- a) 应提供覆盖到每个用户的安全审计功能，对应用系统的用户登录、用户退出、增加用户、修改用户权限等重要安全事件进行审计；（增强）
- b) 应保证审计活动的完整性和连续性，保证无法删除、修改或覆盖审计记录；（落实）
- c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；
- d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

12.1.4.4 剩余信息保护（S3）

本项要求包括：

- a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- b) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

12.1.4.5 通信完整性（S3）

应采用密码技术保证通信过程中数据的完整性。

12.1.4.6 通信保密性（S3）

本项要求包括：

- a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；
- b) 应对通信过程中的整个报文或会话过程进行加密。

12.1.4.7 抗抵赖（G3）

本项要求包括：

- a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
- b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

12.1.4.8 软件容错（A3）

本项要求包括：

- a) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- b) 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

12.1.4.9 资源控制（A3）

本项要求包括：

- a) 当应用系统的通信双方中的一方在一段时间内未作响应，另一方应能够自动结束会话；
- b) 应能够对系统的最大并发会话连接数进行限制；
- c) 应能够对单个帐户的多重并发会话进行限制；

- d) 应能够对一个时间段内可能的并发会话连接数进行限制;
- e) 应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额;
- f) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警;
- g) 应提供服务优先级设定功能,并在安装后根据安全策略设定访问帐户或请求进程的优先级,根据优先级分配系统资源。

12.1.5 数据安全

12.1.5.1 数据完整性 (S3)

- a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏,并在检测到完整性错误时采取必要的恢复措施;
- b) 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏,并在检测到完整性错误时采取必要的恢复措施。

12.1.5.2 数据保密性 (S3)

- a) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性;
- b) 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

12.1.5.3 备份和恢复 (A3)

本项要求包括:

- a) 应提供数据本地备份与恢复功能,完全数据备份至少每天一次,备份介质场外存放;
- b) 应提供异地数据备份功能,利用通信网络将关键数据定时批量传送至备用场地;
- c) 应提供主要网络设备、通信线路和数据处理系统的硬件冗余,保证系统的高可用性。

12.2 管理要求

12.2.1 安全管理制度

12.2.1.1 管理制度 (G3)

本项要求包括:

- a) 应按照“谁主管谁负责,谁运营谁负责”的原则,建立电力二次系统安全管理制度,制定信息安全工作的总体方针和安全策略,说明机构安全工作的总体目标、范围、原则和安全框架等,并将电力二次系统安全防护及其信息报送纳入日常安全生产管理体系,负责所辖范围内计算机及数据网络的安全管理;(细化)
- b) **应对安全管理活动中各类管理内容**建立安全管理制度,主要包括:门禁管理、人员管理、权限管理、访问控制管理、防尾随管理、安全防护系统的维护管理、常规设备及各系统的维护管理、恶意代码的防护管理、审计管理、数据及系统的备份管理、用户口令密钥及数字证书的管理、培训管理等;(增强)
- c) 应对安全管理人员或操作人员执行的重要管理操作建立操作规程;
- d) **应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。**

12.2.1.2 制定和发布 (G3)

本项要求包括:

- a) 应指定或授权专门的部门或人员负责安全管理制度的制定;
- b) **安全管理制度应具有统一的格式,并进行版本控制;**
- c) 应组织相关人员对制定的安全管理制度进行论证和审定;

- d) 安全管理制度应通过正式、有效的方式发布；
- e) 安全管理制度应注明发布范围，并对收发文进行登记。

12.2.1.3 评审和修订（G3）

- a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
- b) 应定期或不定期或在发生重大变更时对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。（增强）

12.2.2 安全管理机构

12.2.2.1 岗位设置（G3）

本项要求包括：

- a) 应明确由主管安全生产的领导作为电力二次系统安全防护的主要责任人，成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；（增强）
- b) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
- c) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；
- d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

12.2.2.2 人员配备（G3）

本项要求包括：

- a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
- b) 应配备专职安全管理员，不可兼任；
- c) 关键事务岗位应配备多人共同管理。

12.2.2.3 资金保障（G3）

本项要求包括：

- a) 应保障落实电力二次系统安全建设、运维及等级保护测评资金等；（新增）
- b) 系统建设资金筹措方案和年度系统维护经费应包括信息安全保障资金项目。（新增）

12.2.2.4 授权和审批（G3）

本项要求包括：

- a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批；（细化）
- b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- d) 应记录审批过程并保存审批文档；
- e) 接入电力调度数据网络的节点、设备 and 应用系统，其接入技术方案和安全防护措施须经负责本级电力调度数据网络的调度机构核准。（新增）

12.2.2.5 沟通和合作（G3）

本项要求包括：

- a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；

- b) 应加强与行业信息安全监管部门、公安机关、通信运营商、银行及相关单位和部门的合作与沟通；（细化）
- c) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通；
- d) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- e) 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

12.2.2.6 审核和检查（G3）

- a) 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- b) 应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
- d) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

12.2.3 人员安全管理

12.2.3.1 人员录用（G3）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责人员录用；
- b) 应**严格**规范人员录用过程，对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
- c) 应与安全管理员、系统管理员、网络管理员等关键岗位的人员**签署保密协议**；（细化）
- d) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

12.2.3.2 人员离岗（G3）

本项要求包括：

- a) 应**严格**规范人员离岗过程，及时终止离岗员工的所有访问权限；
- b) 应收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；（落实）
- c) 应严格调离手续的办理程序，只有在收回访问权限和各种证件、设备后，**关键岗位人员承诺履行调离后的保密义务后，方可办理调离手续**。（细化）

12.2.3.3 人员考核（G3）

- a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；
- b) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；
- c) 应对考核结果进行记录并保存。

12.2.3.4 安全意识教育和培训（G3）

本项要求包括：

- a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- b) 应对**安全责任和惩戒措施进行书面规定**并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
- c) 应按照行业信息安全要求，**对定期安全教育和培训进行书面规定**，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行的培训应至少每年举办一次；（新增）

d) 应对安全教育和培训的情况和结果进行记录并归档保存。

12.2.3.5 外部人员访问管理（G3）

a) 应确保在外部人员访问受控区域**前先提出书面申请**，批准后由专人全程陪同或监督，并登记备案；

b) **对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。**

12.2.4 系统建设管理

12.2.4.1 系统定级（G3）

本项要求包括：

a) 应明确信息系统的边界和安全保护等级；

b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由；

c) **应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；**

d) 应确保信息系统的定级结果经过行业信息安全主管部门批准，方可到公安机关备案。（增强）

12.2.4.2 安全方案设计（G3）

本项要求包括：

a) 应根据系统的安全保护等级选择基本安全措施，并依据电力二次系统安全防护要求和风险分析的结果补充和调整安全措施；（增强）

b) **应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；**

c) **应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；**

d) 应组织相关部门和有关安全技术专家对**总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件**的合理性和正确性进行论证和审定，并经过上级信息安全主管部门和相应电力调度机构的审核，方案实施完成后应当由相关机构共同组织验收；（增强）

e) **应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。**

12.2.4.3 产品采购和使用（G3）

本项要求包括：

a) 应确保安全产品采购和使用符合国家的有关规定；

b) 应确保密码产品采购和使用符合国家密码主管部门的要求；

c) 应指定或授权专门的部门负责产品的采购；

d) **应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；**

e) 接入电力二次系统生产控制大区中的安全产品，其功能、性能应获得国家或行业指定机构安全检测证明，其电磁兼容性还需有电力系统电磁兼容检测证明。（新增）

12.2.4.4 自行软件开发（G3）

本项要求包括：

a) 应确保开发环境与实际运行环境物理分开，**开发人员和测试人员分离，测试数据和测试结果受到控制；**

b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

- c) 应制定代码编写安全规范，要求开发人员参照规范编写代码；
- d) 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；
- e) 应确保对程序资源库的修改、更新、发布进行授权和批准。

12.2.4.5 外包软件开发（G3）

本项要求包括：

- a) 应根据开发要求检测软件质量；
- b) 应确保提供软件设计的相关文档和使用指南；
- c) 应在软件安装之前检测软件包中可能存在的恶意代码；
- d) 应在外包开发合同中明确开发单位、供应商所提供的电力二次设备及系统应包含保密、生命周期、禁止关键技术和设备扩散等方面的条款；（增强）
- e) 外包开发的软件应在本单位存有源代码备份，并已通过软件后门等安全性检测。（细化）

12.2.4.6 工程实施（G3）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；
- c) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

12.2.4.7 测试验收（G3）

本项要求包括：

- a) 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；
- b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
- c) 应对系统测试验收的控制方法和人员行为准则进行书面规定；
- d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
- e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

12.2.4.8 系统交付（G3）

本项要求包括：

- a) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 应对负责系统运行维护的技术人员进行相应的技能培训；
- c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；
- d) 应对系统交付的控制方法和人员行为准则进行书面规定；
- e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

12.2.4.9 系统备案（G3）

本项要求包括：

- a) 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；
- b) 应将系统等级及相关材料报系统主管部门备案；
- c) 应将系统等级及其他要求的备案材料报相应公安机关备案。

12.2.4.10 等级测评（G3）

本项要求包括：

- a) 在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
- b) 应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
- c) 应选择具有国家相关技术资质和安全资质的并由行业信息安全主管部门指定的测评单位进行等级测评；（落实）
- d) 应指定或授权专门的部门或人员负责等级测评的管理。

12.2.4.11 安全服务商选择（G3）

本项要求包括：

- a) 应选择符合国家及行业有关规定的服务商开展安全服务；（增强）
- b) 应与选定的安全服务商签订安全协议，明确安全责任；（增强）
- c) 应与服务商签订安全服务合同，确保提供技术培训，并明确服务承诺。（增强）

12.2.5 系统运维管理

12.2.5.1 环境管理（G3）

本项要求包括：

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
- b) 应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
- c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
- d) 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。

12.2.5.2 资产管理（G3）

本项要求包括：

- a) 应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。
- c) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
- d) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

12.2.5.3 介质管理（G3）

本项要求包括：

- a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；
- b) 应建立生产控制大区移动存储介质安全管理制度，对移动存储介质的使用进行严格限制；（增强）
- c) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；
- d) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；

- e) 应对存储介质的**使用过程**、送出维修以及销毁等进行严格的管理，**对带出工作环境的存储介质进行内容加密和监控管理**，对送出维修或销毁的介质应首先清除介质中的敏感数据，**对保密性较高的存储介质未经批准不得自行销毁**；
- f) **应根据数据备份的需要对某些介质实行异地存储**，存储地的环境要求和管理方法应与本地相同；
- g) **应对重要介质中的数据和软件采取加密存储**，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

12.2.5.4 设备管理（G3）

本项要求包括：

- a) 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- c) **应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等**；
- d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- e) 应确保信息处理设备必须经过审批才能带离机房或办公地点；
- f) 应确保信息处理设备必须经过审批才能带入机房或办公地点。（新增）

12.2.5.5 监控管理和安全管理中心（G3）

本项要求包括：

- a) **应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存**；
- b) **应定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；（落实）**
- c) **应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。**

12.2.5.6 网络安全管理（G3）

本项要求包括：

- a) 应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- b) 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；
- c) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行测试和备份；（增强）
- d) 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
- e) **应实现设备的最小服务配置，并对配置文件进行定期离线备份**；
- f) 应保证所有与外部系统的连接均得到授权和批准；
- g) **应依据安全策略对允许或者拒绝便携式和移动式设备的网络接入**；

- h) 应依据安全策略对接入网络的便携式和移动式设备的网络使用行为进行管控；（新增）
- i) 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

12.2.5.7 系统安全管理（G3）

本项要求包括：

- a) 应根据业务需求和系统安全分析确定系统的访问控制策略；
- b) 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；
- c) 应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中对补丁的兼容性和安全性进行测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；（细化）
- d) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定；
- e) 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；
- f) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
- g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为；
- h) 电力调度机构应指定专人负责管理本级调度数字证书系统。（增强）

12.2.5.8 恶意代码防范管理（G3）

本项要求包括：

- a) 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
- b) 在更新恶意代码库、木马库以及IDS规则库前，应首先在测试环境中对恶意代码库、木马库以及IDS规则库的安全性和兼容性进行测试通过，更新操作应离线进行，生产控制大区恶意代码更新应由专人负责，并保存更新记录；（新增）
- c) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；
- e) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

12.2.5.9 密码管理（G3）

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

12.2.5.10 变更管理（G3）

本项要求包括：

- a) 应确认系统中要发生的重要变更，并制定相应的变更方案；
- b) 应建立变更管理制度，明确变更执行及变更校核程序，系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告；（增强）
- c) 应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；

- d) 应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

12.2.5.11 备份与恢复管理（G3）

本项要求包括：

- a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；
- b) 应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；
- c) 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法；
- d) 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；
- e) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

12.2.5.12 安全事件处置（G3）

本项要求包括：

- a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；
- b) 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；
- d) 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；
- e) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；
- f) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；
- g) 应建立电力二次系统联合防护和应急机制，负责处置跨部门电力二次系统安全事件。（新增）

12.2.5.13 应急预案管理（G3）

本项要求包括：

- a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
- b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
- c) 应对安全管理员、系统管理员、网络管理员等相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。（增强）
- d) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
- e) 应制定电力二次系统联合防护和应急处置预案，并经过演练；（新增）
- f) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

13 第四级基本要求

13.1 技术要求

13.1.1 物理安全

13.1.1.1 物理位置的选择（G4）

本项要求包括：

- a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
- b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁，如果不可避免，应采取有效防水措施。（落实）

13.1.1.2 物理访问控制（G4）

本项要求包括：

- a) 机房各出入口应安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员；
- b) 进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；
- c) 应对机房划分区域进行管理，区域和区域之间应用物理方式隔断，在重要区域前设置交付或安装等过渡区域；（增强）
- d) 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。

13.1.1.3 防盗窃和防破坏（G4）

本项要求包括：

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
- c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 应利用光、电等技术设置机房防盗报警系统；
- f) 应对机房设置监控报警系统。

13.1.1.4 防雷击（G4）

本项要求包括：

- a) 机房建筑应设置避雷装置；
- b) 应设置防雷保安器，防止感应雷；
- c) 机房应设置交流电源地线。

13.1.1.5 防火（G4）

本项要求包括：

- a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，自动灭火；
- b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
- c) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

13.1.1.6 防水和防潮（G4）

本项要求包括：

- a) 主机房尽量避开水源，与主机房无关的给排水管道不得穿过主机房，与主机房相关的给排水管道必须有可靠的防渗漏措施；（增强）
- b) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
- c) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
- d) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

13.1.1.7 防静电（G4）

本项要求包括：

- a) 主要设备采用必要的接地防静电措施；
- b) 机房应采用防静电地板；
- c) 应采用静电消除器等装置，减少静电的产生。

13.1.1.8 温湿度控制（G4）

机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

13.1.1.9 电力供应（A4）

本项要求包括：

- a) 应在机房供电线路上配置稳压器和过电压防护设备；
- b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
- c) 设置冗余或并行的电力电缆线路为计算机系统供电，输入电源应采用双路自动切换供电方式；
（增强）
- d) 应建立备用供电系统。

13.1.1.10 电磁防护（S4）

本项要求包括：

- a) 电源线和通信线缆应隔离铺设，避免互相干扰；
- b) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；
- c) 应对关键区域实施电磁屏蔽。

13.1.2 网络安全

13.1.2.1 结构安全（G4）

本项要求包括：

- a) 应保证网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
- b) 应保证网络各个部分的带宽满足业务高峰期需要；
- c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；
- d) 应绘制完整的网络拓扑结构图，有相应的网络配置表，包含设备IP地址等主要信息，与当前运行情况相符；**（增强）**
- e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；
- f) 单个系统应单独划分安全域，系统由独立子网承载，每个域的网络出口应唯一；**（新增）**
- g) 采用冗余技术设计网络拓扑结构，提供主要网络设备、通信线路的硬件冗余，避免关键节点存在单点故障；**（增强）**
- h) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保障重要业务服务的带宽。**（增强）**

13.1.2.2 访问控制（G4）

本项要求包括：

- a) 应在网络边界部署访问控制设备，启用访问控制功能；
- b) 应不允许数据带通用协议通过；
- c) 应根据数据的敏感标记允许或拒绝数据通过；
- d) 应不开放远程拨号访问功能。

13.1.2.3 安全审计（G4）

本项要求包括：

- a) 应在生产控制大区应部署专用审计系统，或启用设备或系统审计功能，应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；（增强）
- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
- c) 应能够根据记录数据进行分析，并生成审计报表，网络设备不支持的应采用第三方工具生成审计报表；（增强）
- d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等；
- e) 应定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生；
- f) 应根据信息系统的统一安全策略，实现集中审计，时钟保持与时钟服务器同步。

13.1.2.4 边界完整性检查（S4）

本项要求包括：

- a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；
- b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

13.1.2.5 入侵防范（G4）

本项要求包括：

- a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等；
- b) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警，必要时可配置为自动采取相应动作。（落实）

13.1.2.6 恶意代码防范（G4）

本项要求包括：

- a) 应在网络边界处对恶意代码进行检测和清除；
- b) 应维护恶意代码库的升级和检测系统的更新。

13.1.2.7 网络设备防护（G4）

本项要求包括：

- a) 应对登录网络设备的用户进行身份鉴别；
- b) 应对网络设备的管理员登录地址进行限制；
- c) 网络设备标识应唯一；同一网络设备的用户标识应唯一；禁止多个人共用一个账号；（增强）
- d) 身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应修改默认用户和口令，不得使用缺省口令，口令长度不得小于8位，要求是字母和数字或特殊字符的混合并不得与用户名相同，口令应定期更换，并加密存储；（增强）
- e) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；
- f) 网络设备用户的身份鉴别信息至少应有一种是不可伪造的；
- g) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
- h) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
- i) 应实现设备特权用户的权限分离，系统不支持的应部署日志服务器保证管理员的操作能够被审计，并且网络特权用户管理员无权对审计记录进行操作；（增强）

- j) 应封闭不需要的网络端口，关闭不需要的网络服务。如需使用SNMP服务，应采用安全性增强版本；并应设定复杂的Community控制字段，不使用Public、Private等默认字段。（新增）

13.1.3 主机安全

13.1.3.1 身份鉴别（S4）

本项要求包括：

- a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
- b) 操作系统和数据库系统管理用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；（增强）
- c) 启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。限制同一用户连续失败登录次数；（增强）
- d) 应设置鉴别警示信息，描述未授权访问可能导致的后果；
- e) 当对服务器进行远程管理时，采取必要措施，防止鉴别信息在网络传输过程中被窃听；
- f) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性；
- g) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，并且身份鉴别信息至少有一种是不可伪造的。

13.1.3.2 安全标记（S4）

应对所有主体和客体设置敏感标记。

13.1.3.3 访问控制（S4）

本项要求包括：

- a) 应依据安全策略和所有主体和客体设置的敏感标记控制主体对客体的访问；
- b) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表、记录和字段级。
- c) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
- d) 应实现操作系统和数据库系统特权用户的权限分离；
- e) 应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；
- f) 应及时删除多余的、过期的帐户，避免共享帐户的存在；

13.1.3.4 可信路径（S4）

本项要求包括：

- a) 在系统对用户进行身份鉴别时，系统与用户之间应能够建立一条安全的信息传输路径；
- b) 在用户对系统进行访问时，系统与用户之间应能够建立一条安全的信息传输路径。

13.1.3.5 安全审计（G4）

本项要求包括：

- a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；系统不支持该要求的，应以系统运行安全和效率为前提，采用第三方安全审计产品实现审计要求；（增强）
- b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等；（细化）
- c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等；
- e) 应能够通过操作系统自身功能或第三方工具根据记录数据进行分析，并生成审计报表；（落实）

- f) 应保护审计进程，避免受到未预期的中断；
- g) 应能够根据信息系统的统一安全策略，实现集中审计。

13.1.3.6 剩余信息保护（S4）

本项要求包括：

- a) 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- b) 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

13.1.3.7 入侵防范（G4）

- a) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
- b) 应能够对重要程序的完整性进行检测，并具有完整性恢复的能力；（落实）
- c) 操作系统应遵循最小安装的原则，仅安装必要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新，补丁安装前应进行安全性和兼容性测试。（增强）

13.1.3.8 恶意代码防范（G4）

本项要求包括：

- a) 应在本机安装防恶意代码软件或独立部署恶意代码防护设备，并及时更新防恶意代码软件版本和恶意代码库；（增强）
- b) 应支持防恶意代码的统一管理；
- c) 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

13.1.3.9 资源控制（A4）

本项要求包括：

- a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；
- b) 应根据安全策略设置登录终端的操作超时锁定；
- c) 应根据需要限制单个用户对系统资源的最大或最小使用限度；
- d) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；
- e) 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警；
- f) 应关闭或拆除主机的软盘驱动、光盘驱动、USB接口、串行口等，确需保留的必须通过安全管理平台实施严格管理。（新增）

13.1.4 应用安全

13.1.4.1 身份鉴别（S4）

本项要求包括：

- a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；
- b) 应用系统用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用户在第一次登录系统时修改分发的初始口令，口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；应用软件不得明文存储口令数据；（增强）
- c) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，其中一种是不可伪造的；
- d) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

- e) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

13.1.4.2 安全标记 (S4)

应提供为主体和客体设置安全标记的功能并在安装后启用；

13.1.4.3 访问控制 (S4)

本项要求包括：

- a) 应提供自主访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
- b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；
- c) 应由授权主体配置访问控制策略，并禁止默认帐户的访问；
- d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
- e) 应通过比较安全标记来确定是授予还是拒绝主体对客体的访问。

13.1.4.4 可信路径 (S4)

本项要求包括：

- a) 在应用系统对用户进行身份鉴别时，应能够建立一条安全的信息传输路径；
- b) 在用户通过应用系统对资源进行访问时，应用系统应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。

13.1.4.5 安全审计 (G4)

本项要求包括：

- a) 应提供覆盖到每个用户的安全审计功能，对应用系统的用户登录、用户退出、增加用户、修改用户权限等重要安全事件进行审计；（增强）
- b) 应保证审计活动的完整性和连续性，保证无法删除、修改或覆盖审计记录；（落实）
- c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；
- d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；
- e) 应根据系统统一安全策略，提供集中审计接口。

13.1.4.6 剩余信息保护 (S4)

本项要求包括：

- a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- b) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

13.1.4.7 通信完整性 (S4)

应采用密码技术保证通信过程中数据的完整性。

13.1.4.8 通信保密性 (S4)

本项要求包括：

- a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；
- b) 应对通信过程中的整个报文或会话过程进行加密；
- c) 应基于硬件化的设备对重要通信过程进行加解密运算和密钥管理。

13.1.4.9 抗抵赖 (G4)

本项要求包括：

- a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；

b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

13.1.4.10 软件容错 (A4)

本项要求包括:

- a) 应提供数据有效性检验功能, 保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求;
- b) 应提供自动保护功能, 当故障发生时自动保护当前所有状态;
- c) 应提供自动恢复功能, 当故障发生时立即自动启动新的进程, 恢复原来的工作状态。

13.1.4.11 资源控制 (A4)

本项要求包括:

- a) 当应用系统的通信双方中的一方在一段时间内未作响应, 另一方应能够自动结束会话;
- b) 应能够对系统的最大并发会话连接数进行限制;
- c) 应能够对单个帐户的多重并发会话进行限制;
- d) 应能够对一个时间段内可能的并发会话连接数进行限制;
- e) 应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额;
- f) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警;
- g) 应提供服务优先级设定功能, 并在安装后根据安全策略设定访问帐户或请求进程的优先级, 根据优先级分配系统资源。

13.1.5 数据安全

13.1.5.1 数据完整性 (S4)

- a) 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏, 并在检测到完整性错误时采取必要的恢复措施;
- b) 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏, 并在检测到完整性错误时采取必要的恢复措施;
- c) 应对重要通信提供专用通信协议或安全通信协议服务, 避免来自基于通用通信协议的攻击破坏数据完整性。

13.1.5.2 数据保密性 (S4)

- a) 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性;
- b) 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性;
- c) 应对重要通信提供专用通信协议或安全通信协议服务, 避免来自基于通用通信协议的攻击破坏数据保密性。

13.1.5.3 备份和恢复 (A4)

本项要求包括:

- a) 应提供数据本地备份与恢复功能, 完全数据备份至少每天一次, 备份介质场外存放;
- b) 应建立异地灾难备份中心, 配备灾难恢复所需的通信线路、网络设备和数据处理设备, 提供业务应用的实时无缝切换;
- c) 应提供异地实时备份功能, 利用通信网络将数据实时备份至灾难备份中心;
- d) 应提供主要网络设备、通信线路和数据处理系统的硬件冗余, 保证系统的高可用性。

13.2 管理要求

13.2.1 安全管理制度

13.2.1.1 管理制度（G4）

本项要求包括：

- a) 应按照“谁主管谁负责，谁运营谁负责”的原则，建立电力二次系统安全管理制度，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将电力二次系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的~~安全管理~~；（细化）
- b) 应对安全管理活动中各类管理内容建立安全管理制度，主要包括：门禁管理、人员管理、权限管理、访问控制管理、防尾随管理、安全防护系统的维护管理、常规设备及各系统的维护管理、恶意代码的防护管理、审计管理、数据及系统的备份管理、用户口令密钥及数字证书的管理、培训管理等；（增强）
- c) 应对安全管理人员或操作人员执行的重要管理操作建立操作规程；
- d) 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

13.2.1.2 制定和发布（G4）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责安全管理制度的制定；
- b) 安全管理制度应具有统一的格式，并进行版本控制；
- c) 应组织相关人员对制定的安全管理制度进行论证和审定；
- d) 安全管理制度应通过正式、有效的方式发布；
- e) 安全管理制度应注明发布范围，并对收发文进行登记；
- f) **有密级的安全管理制度，应注明安全管理制度密级，并进行密级管理。**

13.2.1.3 评审和修订（G4）

- a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
- b) 应定期或不定期或在发生重大变更时对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订；（增强）
- c) **应明确需要定期修订的安全管理制度，并指定负责人或负责部门负责制度的日常维护；**
- d) **应根据安全管理制度的相应密级确定评审和修订的操作范围。**

13.2.2 安全管理机构

13.2.2.1 岗位设置（G4）

本项要求包括：

- a) 应明确由主管安全生产的领导作为电力二次系统安全防护的主要责任人，成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；（增强）
- b) 应设立信息安全管理工作职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
- c) 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；
- d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

13.2.2.2 人员配备（G4）

本项要求包括：

- a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；

- b) 应配备专职安全管理员，不可兼任；
- c) 关键事务岗位应配备多人共同管理。

13.2.2.3 资金保障（G4）

本项要求包括：

- a) 应保障落实电力二次系统安全建设、运维及等级保护测评资金等；（新增）
- b) 系统建设资金筹措方案和年度系统维护经费应包括信息安全保障资金项目。（新增）

13.2.2.4 授权和审批（G4）

本项要求包括：

- a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批；（细化）
- b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- d) 应记录审批过程并保存审批文档；
- e) 接入电力调度数据网络的节点、设备和应用系统，其接入技术方案和安全防护措施须经负责本级电力调度数据网络的调度机构核准。（新增）

13.2.2.5 沟通和合作（G4）

本项要求包括：

- a) 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；
- b) 应加强与行业信息安全监管部门、公安机关、通信运营商、银行及相关单位和部门的合作与沟通。（细化）
- c) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通；
- d) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- e) 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

13.2.2.6 审核和检查（G4）

- a) 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- b) 应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；
- d) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

13.2.3 人员安全管理

13.2.3.1 人员录用（G4）

本项要求包括：

- a) 应指定或授权专门的部门或人员负责人员录用；

- b) 应严格规范人员录用过程，对被录用人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；
- c) 应与安全管理员、系统管理员、网络管理员等关键岗位的人员签署保密协议；（细化）
- d) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

13.2.3.2 人员离岗（G4）

本项要求包括：

- a) 应制定有关管理规范，严格规范人员离岗过程，及时终止离岗员工的所有访问权限；
- b) 应收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；（落实）
- c) 应严格调离手续的办理程序，只有在收回访问权限和各种证件、设备后，关键岗位人员承诺履行调离后的保密义务后，方可办理调离手续。（细化）

13.2.3.3 人员考核（G4）

- a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；
- b) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；
- c) 应建立保密制度，并定期或不定期对保密制度执行情况进行检查或考核；
- d) 应对考核结果进行记录并保存。

13.2.3.4 安全意识教育和培训（G4）

本项要求包括：

- a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- b) 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；
- c) 应按照行业信息安全要求，对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行的培训应至少每年举办一次；（新增）
- d) 应对安全教育和培训的情况和结果进行记录并归档保存。

13.2.3.5 外部人员访问管理（G4）

- a) 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；
- b) 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行；
- c) 对关键区域不允许外部人员访问。

13.2.4 系统建设管理

13.2.4.1 系统定级（G4）

本项要求包括：

- a) 应明确信息系统的边界和安全保护等级；
- b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由；
- c) 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；
- d) 应确保信息系统的定级结果经过行业信息安全主管部门批准，方可到公安机关备案。（增强）

13.2.4.2 安全方案设计（G4）

本项要求包括：

- a) 应根据系统的安全保护等级选择基本安全措施，并依据电力二次系统安全防护要求和风险分析的结果补充和调整安全措施；（增强）

- b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划,制定近期和远期的安全建设工作计划;
- c) 应根据信息系统的等级划分情况,统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案,并形成配套文件;
- d) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定,并经过上级信息安全主管部门和相应电力调度机构的审核,方案实施完成后应当由相关机构共同组织验收;(增强)
- e) 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

13.2.4.3 产品采购和使用 (G4)

本项要求包括:

- a) 应确保安全产品采购和使用符合国家的有关规定;
- b) 应确保密码产品采购和使用符合国家密码主管部门的要求;
- c) 应指定或授权专门的部门负责产品的采购;
- d) 应预先对产品进行选型测试,确定产品的候选范围,并定期审定和更新候选产品名单;
- e) **应对重要部位的产品委托专业测评单位进行专项测试,根据测试结果选用产品;**
- f) 接入电力二次系统生产控制大区中的安全产品,其功能、性能应获得国家或行业指定机构安全检测证明,其电磁兼容性还需有电力系统电磁兼容检测证明。(新增)

13.2.4.4 自行软件开发 (G4)

本项要求包括:

- a) 应确保开发环境与实际运行环境物理分开,开发人员和测试人员分离,测试数据和测试结果受到控制;
- b) 应制定软件开发管理制度,明确说明开发过程的控制方法和人员行为准则;
- c) 应制定代码编写安全规范,要求开发人员参照规范编写代码;
- d) 应确保提供软件设计的相关文档和使用指南,并由专人负责保管;
- e) 应确保对程序资源库的修改、更新、发布进行授权和批准;
- f) **应确保开发人员为专职人员,开发人员的开发活动受到控制、监视和审查。**

13.2.4.5 外包软件开发 (G4)

本项要求包括:

- a) 应根据开发要求检测软件质量;
- b) 应确保提供软件设计的相关文档和使用指南;
- c) 应在软件安装之前检测软件包中可能存在的恶意代码;
- d) 应在外包开发合同中明确开发单位、供应商所提供的电力二次设备及系统应包含保密、生命周期、禁止关键技术和设备扩散等方面的条款;(增强)
- e) 外包开发的软件应在本单位存有源代码备份,并已通过软件后门和隐蔽信道等安全性检测。
(细化)

13.2.4.6 工程实施 (G4)

本项要求包括:

- a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；
- c) 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则；
- d) **应通过第三方工程监理控制项目的实施过程。**

13.2.4.7 测试验收（G4）

本项要求包括：

- a) 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；
- b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；
- c) 应对系统测试验收的控制方法和人员行为准则进行书面规定；
- d) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；
- e) 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

13.2.4.8 系统交付（G4）

本项要求包括：

- a) 应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
- b) 应对负责系统运行维护的技术人员进行相应的技能培训；
- c) 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；
- d) 应对系统交付的控制方法和人员行为准则进行书面规定；
- e) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

13.2.4.9 系统备案（G4）

本项要求包括：

- a) 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；
- b) 应将系统等级及相关材料报系统主管部门备案；
- c) 应将系统等级及其他要求的备案材料报相应公安机关备案。

13.2.4.10 等级测评（G4）

本项要求包括：

- a) 在系统运行过程中，应至少每半年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
- b) 应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
- c) 应选择具有国家相关技术资质和安全资质的并由行业信息安全主管部门指定的测评单位进行等级测评；（落实）
- d) 应指定或授权专门的部门或人员负责等级测评的管理。

13.2.4.11 安全服务商选择（G4）

本项要求包括：

- a) 应选择符合国家及行业有关规定的服务商开展安全服务；（增强）
- b) 应与选定的安全服务商签订安全协议，明确安全责任；（增强）

- c) 应与服务商签订安全服务合同，确保提供技术培训，并明确服务承诺。（增强）

13.2.5 系统运维管理

13.2.5.1 环境管理（G4）

本项要求包括：

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；
- b) 应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
- c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
- d) 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等；
- e) **应对机房和办公环境实行统一策略的安全管理，对出入人员进行相应级别的授权，对进入重要安全区域的活动行为实时监视和记录。**

13.2.5.2 资产管理（G4）

本项要求包括：

- a) 应编制与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- b) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
- c) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
- d) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

13.2.5.3 介质管理（G4）

本项要求包括：

- a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；
- b) 应建立生产控制大区移动存储介质安全管理制度，对移动存储介质的使用进行严格限制；（增强）
- c) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；
- d) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；
- e) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，重要数据的存储介质带出工作环境必须进行内容加密并进行监控管理，对于需要送出维修或销毁的介质应采用**多次读写覆盖、清除敏感或秘密数据、对无法执行删除操作的受损介质必须销毁，保密性较高的信息存储介质应获得批准并在双人监控下才能销毁，销毁记录应妥善保存；**
- f) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；
- g) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

13.2.5.4 设备管理（G4）

本项要求包括：

- a) 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- c) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；
- d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- e) 应确保信息处理设备必须经过审批才能带离机房或办公地点；
- f) 应确保信息处理设备必须经过审批才能带入机房或办公地点。（新增）

13.2.5.5 监控管理和安全管理中心（G4）

本项要求包括：

- a) 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；
- b) 应定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；（落实）
- c) 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

13.2.5.6 网络安全管理（G4）

本项要求包括：

- a) 应指定人员对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；
- b) 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；
- c) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行测试和备份；（增强）
- d) 应定期对网络系统进行漏洞扫描，对发现的网络安全漏洞进行及时的修补；
- e) 应实现设备的最小服务配置，并对配置文件进行定期离线备份；
- f) 应保证所有与外部系统的连接均得到授权和批准；
- g) **应禁止便携式和移动式设备接入网络；**
- h) 应定期检查违反规定拨号上网或其他违反网络安全策略的行为；
- i) **应严格控制网络管理用户的授权，授权程序中要求必须有两人在场，并经双重认可后方可操作，操作过程应保留不可更改的审计日志。**

13.2.5.7 系统安全管理（G4）

本项要求包括：

- a) 应根据业务需求和系统安全分析确定系统的访问控制策略；
- b) 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；
- c) 应安装系统的最新补丁程序，在安装系统补丁前，应首先在测试环境中对补丁的兼容性和安全性进行测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；（细化）

- d) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定；
- e) 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；
- f) 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；
- g) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为；
- h) **应对系统资源的使用进行预测，以确保充足的处理速度和存储容量，管理人员应随时注意系统资源的使用情况，包括处理器、存储设备和输出设备；**
- i) 电力调度机构应指定专人负责管理本级调度数字证书系统。（增强）

13.2.5.8 恶意代码防范管理（G4）

本项要求包括：

- a) 应提高所有用户的防病毒意识，告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；
- b) 在更新恶意代码库、木马库以及IDS规则库前，应首先在测试环境中对恶意代码库、木马库以及IDS规则库的安全性和兼容性进行测试通过，更新操作应离线进行，生产控制大区恶意代码更新应由专人负责，并保存更新记录；（新增）
- c) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；
- d) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；
- e) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

13.2.5.9 密码管理（G4）

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

13.2.5.10 变更管理（G4）

本项要求包括：

- a) 应确认系统中要发生的重要变更，并制定相应的变更方案；
- b) 应建立变更管理制度，明确变更执行及变更校核程序，系统发生重要变更前，应向主管领导申请，审批后方可实施变更，并在实施后向相关人员通告；（增强）
- c) 应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；
- d) 应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；
- e) **应定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性。**

13.2.5.11 备份与恢复管理（G4）

本项要求包括：

- a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

- b) 应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；
- c) 应根据数据的重要性及其对系统运行的影响，制定数据的备份策略和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输方法；
- d) 应建立控制数据备份和恢复过程的程序，记录备份过程，**对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场**，所有文件和记录应妥善保存；
- e) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复；
- f) **应根据信息系统的备份技术要求，制定相应的灾难恢复计划，并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新。**

13.2.5.12 安全事件处置（G4）

本项要求包括：

- a) 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；
- b) 应制定安全事件报告和处置管理制度，明确安全事件类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；
- c) 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；
- d) 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；
- e) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；
- f) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；
- g) **发生可能涉及国家秘密的重大失、泄密事件，应按照有关规定向公安、安全、保密等部门汇报；**
- h) **应严格控制参与涉及国家秘密事件处理和恢复的人员，重要操作要求至少两名工作人员在场并登记备案；**
- i) 应建立电力二次系统联合防护和应急机制，负责处置跨部门电力二次系统安全事件。（新增）

13.2.5.13 应急预案管理（G4）

本项要求包括：

- a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；
- b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
- c) 应对安全管理员、系统管理员、网络管理员等相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次。（增强）
- d) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
- e) 应制定电力二次系统联合防护和应急处置预案，并经过演练；（新增）
- f) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行；
- g) **应随着信息系统的变更定期对原有的应急预案重新评估，修订完善。**

附录 A

（规范性附录）

关于信息系统整体安全保护能力的要求

信息系统安全等级保护的核心是保证不同安全保护等级的信息系统具有相适应的安全保护能力。本标准第一部分提出了不同安全保护等级信息系统的安全保护能力要求，第二部分就管理类信息系统分别针对不同安全保护等级信息系统应该具有的安全保护能力提出了相应的基本安全要求，第三部分就生产控制类信息系统分别针对不同安全保护等级信息系统应该具有的安全保护能力提出了相应的基本安全要求，满足基本安全要求是保证信息系统具有相应等级的安全保护能力的前提。

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，保证信息系统的整体安全保护能力。

1、构建纵深的防御体系

本标准从技术和管理两个方面提出基本安全要求，在采取由点到面的各种安全措施时，在系统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，保证信息系统整体的安全保护能力。应从通信网络、局域网络边界、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。

2、采取互补的安全措施

本标准以安全控制组件的形式提出基本安全要求，在将各种安全控制组件集成到特定信息系统中时，应考虑各个安全控制组件的互补性，关注各个安全控制组件在层面内、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，保证各个安全控制组件共同综合作用于信息系统的安全功能上，使得信息系统的整体安全保护能力得以保证。

3、保证一致的安全强度

本标准将基本安全功能要求，如身份鉴别、访问控制、安全审计、入侵防范、安全标记等内容，分解到信息系统中的各个层面，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系统整体安全保护能力在这个安全功能上削弱。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；要实现强制访问控制，则应保证在各个层面均基于低层操作系统实现强制访问控制，并保证标记数据在整个信息系统内部流动时标记的唯一性等。

4、建立统一的支撑平台

本标准在较高级别信息系统的安全功能要求上，提到了使用密码技术，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、抗抵赖等）为了获得更高的强度，均要基于密码技术，为了保证信息系统整体安全防护能力，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、抗抵赖等安全功能的实现。

5、进行集中的安全管理

本标准在较高级别信息系统的安全功能管理要求上，提到了统一安全策略、统一安全管理等要求，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，各个安全控制组件在可控情况下发挥各自的作用，应建立安全管理中心，集中管理信息系统中的各个安全控制组件，支持统一安全管理。

附录 B
（规范性附录）
基本安全要求的选择和使用

信息系统由于承载的业务不同，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。

不同安全保护等级的信息系统，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；即使相同安全保护等级的信息系统，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。信息系统的安全保护等级由业务信息安全性等级和系统服务保证性等级较高者决定，因此对某一个定级后的信息系统的安全保护的侧重点可以有多种组合。

信息系统定级后，不同安全保护等级的信息系统可能形成的定级结果组合见表。

表 各等级信息系统定级结果组合

安全保护等级	信息系统定级结果的组合
第一级	S1A1G1
第二级	S1A2G2, S2A2G2, S2A1G2
第三级	S1A3G3, S2A3G3, S3A3G3, S3A2G3, S3A1G3
第四级	S1A4G4, S2A4G4, S3A4G4, S4A4G4, S4A3G4, S4A2G4, S4A1G4
第五级	

本规范中的每一个安全保护等级的基本安全要求按照业务信息安全性等级和系统服务保证性等级相同的情况组织，也就是每一级的基本安全要求针对 S1A1G1、S2A2G2、S3A3G3 和 S4A4G4 情况给出。

对于确定了安全保护等级的信息系统，选择和使用基本安全要求时，可以按照以下过程进行：

1、明确信息系统应该具有的安全保护能力，根据信息系统的安全保护等级选择基本安全要求，包括总体要求、技术要求和管管理要求。简单的方法是根据本标准，一级系统选择总体要求和第一级基本安全要求，二级系统选择总体要求和第二级基本安全要求，三级系统选择总体要求和第三级基本安全要求，四级系统选择总体要求和第四级基本安全要求，以此作为出发点。

2、根据信息系统的定级结果对基本安全要求进行调整。根据系统服务保证性等级选择相应等级的系统服务保证类（A 类）基本安全要求；根据业务信息安全性等级选择相应等级的业务信息安全类（S 类）基本安全要求。

3、针对不同系统的特点，分析可能在某些方面的特殊安全保护能力要求，选择较高级别的基本安全要求或补充基本安全要求。对于本标准中提出的基本安全要求无法实现或有更加有效的安全措施可以替代的，可以对基本安全要求进行调整，调整的原则是保证不降低整体安全保护能力。

总体来讲，保证不同安全保护等级的信息系统具有相应级别的安全保护能力，满足相应级别的基本

安全要求，是信息系统等级保护的核心。选用本规范中提供的基本安全要求是保证信息系统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它相关标准和安全方面的其它相关标准，调整和补充基本安全要求，从而实现信息系统在满足等级保护基本要求基础上，又具有自身特点的保护。

参考文献

- [1] GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
- [2] GB/T 20269-2006 信息安全技术 信息系统安全管理要求
- [3] GB/T 20270-2006 信息安全技术 网络基础安全技术要求
- [4] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
- [5] GB/T 20272-2006 信息安全技术 操作系统安全技术要求
- [6] GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
- [7] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求
- [8] GB/T 18336-2000 信息技术 信息技术安全性评估准则
- [9] GB/T 19716-2005 信息技术 信息安全管理实用规则
- [10] NIST Special Publication 800-53 联邦信息系统推荐性安全控制措施
- [11] DoD Directive & Instruction 8500-1, 2 信息保障 & 信息保障实施