



中华人民共和国国家标准

GB/T 37138—2018

电力信息系统安全等级保护实施指南

Implementation guide for cyber security classified protection of electric power
information system

2018-12-28 发布

2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 等级保护实施概述	2
4.1 基本原则	2
4.1.1 结构优先原则	2
4.1.2 联合防护原则	2
4.1.3 安全可控原则	2
4.1.4 立体防御原则	2
4.2 角色和职责	2
4.2.1 电力信息系统运行单位	2
4.2.2 电力调度机构	3
4.2.3 电力信息系统安全服务机构	3
4.2.4 电力信息系统安全等级测评机构	3
4.2.5 电力信息系统安全产品供应商	3
4.2.6 电力信息系统供应商	3
4.2.7 电力信息系统设计单位	4
4.2.8 主管部门	4
4.3 实施的基本活动	4
5 定级与备案	5
5.1 定级与备案阶段的流程	5
5.2 定级对象分析	5
5.2.1 电力信息系统分析	5
5.2.2 定级对象确定	6
5.3 安全保护等级确定	7
5.3.1 定级、审核和批准	7
5.3.2 形成定级报告	7
5.4 定级结果备案	7
6 测评与评估	7
6.1 测评与评估的流程	7
6.2 等级测评	9
6.2.1 测评机构选择	9
6.2.2 测评准备	9
6.2.3 方案编制	10

6.2.4	现场测评	10
6.2.5	分析与报告编制	11
6.3	电力监控系统安全防护评估	12
6.3.1	评估形式选择	12
6.3.2	评估准备	12
6.3.3	现场评估	13
6.3.4	分析与报告编制	13
7	安全整改	14
7.1	安全整改的流程	14
7.2	整改方案制定	14
7.3	安全整改实施	15
7.4	安全整改验收	16
8	退运	16
8.1	电力信息系统退运阶段的流程	16
8.2	信息转移、暂存和清除	16
8.3	设备迁移或退运	17
8.4	存储介质的清除或销毁	17
	参考文献	19

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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

本标准由国家能源局提出。

本标准由全国电力监管标准化技术委员会(SAC/TC 296)归口。

本标准起草单位：国家能源局信息中心、中国南方电网公司、国家电力投资集团公司、中国长江三峡集团公司、全球能源互联网研究院有限公司、北京卓识网安技术股份有限公司、中国电力科学研究院有限公司、国网电力科学研究院有限公司、国电南京自动化股份有限公司、南方电网科学研究院有限责任公司、中国软件评测中心。

本标准主要起草人：梁建勇、胡红升、王保喜、陈雪鸿、阴玉清、李焕、叶世超、陶文伟、王静、李旻照、张翎、毛澍、房磊、赵婷、焦安春、高艳坤、于学军、李凌、刘育辰、吴国华、秦学嘉、丁晓玉、刘寅、张敏、郁宝坤、张五一、许爱东、陈华军、蒙家晓、周锋、郝鑫。

引 言

为规范电力信息系统安全等级保护实施的流程、内容和方法,加强电力信息系统的安全管理,防范网络攻击对电力信息系统造成的侵害,保障电力系统的安全稳定运行,依据国家和行业有关政策,制定本标准。

在对电力信息系统实施网络安全等级保护的过程中,除使用本标准外,在不同的阶段,还应参照其他有关网络安全等级保护的标准开展工作。

电力信息系统安全等级保护实施指南

1 范围

本标准规定了电力信息系统安全等级保护实施的基本原则、角色和职责,以及定级与备案、测评与评估、安全整改、退运等基本活动。

本标准适用于指导电力信息系统安全等级保护的实施。

2 规范性引用文件

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

GB/T 20984 信息安全技术 信息安全风险评估规范
 GB/T 22239 信息安全技术 信息系统安全等级保护基本要求
 GB/T 25058 信息安全技术 信息系统安全等级保护实施指南
 GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069 和 GB/T 25058 界定的以及下列术语和定义适用于本文件。

3.1

电力信息系统 electric power information system

与电力企业的生产控制、管理运营相关的信息系统。

注:根据信息系统的责任单位、业务类型和业务重要性及物理位置差异等各种因素,可分为管理信息系统和电力监控系统。

3.2

管理信息系统 management information system

支持电力企业管理经营的信息系统。

注:包括门户网站系统、财务管理系统、人力资源管理系统等。

3.3

电力监控系统 electric power supervision and control system

用于监视和控制电力生产及供应过程的、基于计算机及网络技术的业务系统及智能设备,以及作为基础支撑的通信及数据网络等。

注:包括电力数据采集与监控系统、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、微机继电保护和自动装置、广域相量测量系统、负荷控制系统、水调自动化系统和水电梯级调度自动化系统、电能量计量系统、实时电力市场的辅助控制系统、电力调度数据网络等。

3.4

生产控制大区 production control zone

由具有数据采集与控制功能、纵向联接使用专用网络或专用通道的电力监控系统构成的安全区域。

注:一般包括控制区和非控制区。