



# 中华人民共和国国家标准

GB/T 38318—2019

---

## 电力监控系统网络安全评估指南

Cyber security assessment guide for  
electric power system supervision and control

2019-12-10 发布

2020-07-01 实施

---

国家市场监督管理总局  
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 缩略语 .....	2
5 评估内容 .....	2
6 系统生命周期各阶段的安全评估 .....	3
6.1 评估概述 .....	3
6.2 规划阶段 .....	3
6.3 设计阶段 .....	3
6.4 实施阶段 .....	3
6.5 运行维护阶段 .....	3
6.6 废弃阶段 .....	3
7 评估流程及方法 .....	3
7.1 总体要求 .....	3
7.2 评估流程 .....	5
7.3 评估方法 .....	5
7.4 评估注意事项 .....	6
8 安全防护技术评估 .....	6
8.1 基本要求 .....	6
8.2 基础设施安全 .....	6
8.3 体系结构安全 .....	7
8.4 本体安全 .....	10
8.5 可信安全免疫 .....	12
9 应急备用措施评估 .....	13
9.1 冗余备用 .....	13
9.2 应急响应 .....	13
9.3 多道防线 .....	14
10 安全管理评估 .....	14
10.1 安全管理体系 .....	14
10.2 全体人员安全管理 .....	14
10.3 全部设备及系统安全管理 .....	15
10.4 全生命周期安全管理 .....	16

## 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。

本标准由中国电力企业联合会提出。

本标准由全国电力系统管理及其信息交换标准化技术委员会(SAC/TC 82)归口。

本标准起草单位：中国电力科学研究院有限公司、全球能源互联网研究院有限公司、国家能源局、国家电网有限公司、中国南方电网有限责任公司、国家电力投资集团公司、中国华电集团有限公司、中国华能集团公司、中国长江三峡集团公司、国家电网公司华东分部、国网宁夏电力公司、国网吉林省电力有限公司、国网山东省电力公司、国网重庆市电力公司、国网江苏省电力有限公司、南瑞集团信息通信技术分公司、北京科东电力控制系统有限责任公司、广东电网公司电力科学研究院。

本标准主要起草人：张涛、李凌、马媛媛、郑义、郭旭、费稼轩、黄秀丽、高可、陈雪鸿、王景欣、陶洪铸、朱朝阳、林为民、刘楠、单松玲、杨维永、张亮、张宏杰、胡可为、刘勇、欧睿、裴培、马骁、陶文伟、梁智强、余勇、詹雄、刘森、刘莹、郑晓崑、梁潇、王静、张珂、李旻照、陈刚、刘行、刘寅、张骞、石聪聪、张小建。

## 引 言

本标准与 GB/T 36572—2018 配套使用。

# 电力监控系统网络安全评估指南

## 1 范围

本标准规定了电力监控系统网络安全评估工作的评估内容、系统生命周期各阶段的安全评估、评估流程及方法、安全防护技术评估、应急备用措施评估、安全管理评估。

本标准适用于各电力企业电力监控系统规划阶段、设计阶段、实施阶段、运行维护阶段和废弃阶段的网络安全防护评估工作。

## 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 9361 计算机场地安全要求
- GB 17859—1999 计算机信息系统 安全保护等级划分准则
- GB/T 18336.2—2015 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能组件
- GB/T 20272—2006 信息安全技术 操作系统安全技术要求
- GB/T 20984—2007 信息安全技术 信息安全风险评估规范
- GB/T 21028—2007 信息安全技术 服务器安全技术要求
- GB/T 21050—2007 信息安全技术 网络交换机安全技术要求(评估保证级3)
- GB/T 22186—2016 信息安全技术 具有中央处理器的IC卡芯片安全技术要求
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南
- GB/T 25058—2010 信息安全技术 信息系统安全等级保护实施指南
- GB/T 25068.3—2010 信息技术 安全技术 IT 网络安全 第3部分:使用安全网关的网间通信安全保护
- GB/Z 25320(所有部分) 电力系统管理及其信息交换 数据和通信安全
- GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南
- GB/T 36572—2018 电力监控系统网络安全防护导则

## 3 术语和定义

GB/T 36572—2018 和 GB/T 20984—2007 界定的以及下列术语和定义适用于本文件。

### 3.1

#### 自评 **self-assessment**

运行单位对本单位电力监控系统组织实施的安全评估,以及调度机构在调度管辖范围内(以下简称“调管范围内”)各运行单位自评结果基础上,对调管范围内电力监控系统组织实施的安全评估。