ICS 29.240.10
CCS F 20

中华人民共和国国家标准

GB/T 45906.4—2025

变电站二次系统
第4部分：网络安全防护

Substation secondary system—Part 4：Cyber security protection

2025-08-01 发布　　2026-02-01 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 45906《变电站二次系统》的第4部分。GB/T 45906已经发布了以下部分：

——第1部分：通用要求；

——第2部分：数据与模型；

——第3部分：通信报文规范；

——第4部分：网络安全防护；

——第5部分：保护控制及相关设备；

——第6部分：站内监控系统；

——第7部分：集中监控系统；

——第8部分：电气操作防误；

——第9部分：建设规范；

——第10部分：试验与检测。

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专利的责任。

本文件由中国电力企业联合会提出。

本文件由全国电网运行与控制标准化技术委员会(SAC/TC 446)、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。

本文件起草单位：国家电力调度控制中心、国网上海市电力公司、南京南瑞信息通信科技有限公司、中国电力科学研究院有限公司、国网湖北省电力有限公司、国网北京市电力公司、国网江西省电力有限公司、国网宁夏电力有限公司、国家电网有限公司西北分部、国网河北省电力有限公司、国网江苏省电力有限公司、国网河南省电力公司、国网青海省电力公司、中国南方电网有限责任公司、南京南瑞继保电气有限公司、北京科东电力控制系统有限公司、国电南瑞科技股份有限公司、北京四方继保工程技术有限公司、许继电气股份有限公司、国电南京自动化股份有限公司、国网经济技术研究院有限公司、北京同创安全可信科技有限公司。

本文件主要起草人：周劼英、王治华、张晓(国家电力调度控制中心)、李明节、周泽昕、舒治淮、詹雄、朱江、邵立嵩、吕鹏飞、刘宇、金龙、杨维永、汤震宇、刘苇、张晓(湖北)、张宏杰、高鑫、韩盟、栗维勋、陈明亮、余璟、王丹、李延和、林青、宁志言、沈艳、贾玲、马斌、吴金宇、仇伟杰、张龙、王旭宁、汤成俊、沈志浩、余越、李仲青、朱朝阳、李劲松、孟江雯、卢曦、高明慧、王鹏、常家乐、孙瑜、刘长卿。

引　言

为满足变电站二次系统转型发展需求，实现变电站二次系统整体架构、功能、数据、设备的顶层设计，助推新型电力系统设备制造产业优化升级，提升变电站二次系统整体性能和可靠性水平，制定本系列标准。

GB/T 45906《变电站二次系统》从通用需求、设备系统功能需求和工程实施与检测等方面全面涵盖了变电站二次系统各环节，拟由10个部分构成。

——第1部分：通用要求。目的在于规范变电站二次系统总体要求和可靠性、功能集成、信息交互、网络安全等技术要求。

——第2部分：数据与模型。目的在于规范变电站二次系统数据和模型框架，明确数据分类、采集处理要求、建模方法和模型配置流程。

——第3部分：通信报文规范。目的在于规范变电站二次系统的通信协议集，明确数据对象和通信服务的实现方法。

——第4部分：网络安全防护。目的在于规范变电站二次系统安全防护的技术要求。

——第5部分：保护控制及相关设备。目的在于规范变电站继电保护及安全自动装置、自动化设备、电能计量及电能质量设备、采集执行设备、通信设备及辅助监控设备等的技术要求。

——第6部分：站内监控系统。目的在于规范站内监控系统的功能、性能、信息交互等技术要求。

——第7部分：集中监控系统。目的在于规范变电站集中监控系统的系统架构、功能、性能、信息交互等技术要求。

——第8部分：电气操作防误。目的在于规范变电站二次系统电气操作防误的总体要求、架构、功能、性能及应用要求。

——第9部分：建设规范。目的在于规范变电站二次系统工程建设的总体要求、设计原则、过程控制和技术要求。

——第10部分：试验与检测。目的在于规范变电站二次系统设备和系统的检测总体原则、检测要求等。

变电站二次系统
第4部分:网络安全防护

1 范围

本文件规定了变电站二次系统网络安全防护的总则、安全防御、安全监测和安全评估。

本文件适用于变电站二次系统网络安全设施的设计、研发、采购、部署、维护、评估等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 36572—2018 电力监控系统网络安全防护导则

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全 cyber security

通过采取必要措施,防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故,使网络处于稳定可靠运行的状态,以及保障网络数据的完整性、保密性、可用性的能力。

注:网络是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

[来源:GB/T 22239—2019,3.1,有修改]

3.2

本体安全 self security

变电站二次系统各模块自身的安全、可控,包括业务系统软件的安全、操作系统和基础软件的安全、计算机和变电站二次设备的安全等。

[来源:GB/T 36572—2018,3.9,有修改]

3.3

可信安全免疫 trust security immunology

基于可信计算技术实现变电站二次系统的安全免疫,保障操作系统和业务系统软件安全可信,防范已知和未知的病毒、木马及恶意代码的侵害。

[来源:GB/T 36572—2018,3.10,有修改]

3.4

可信根实体 entity of root of trust

用于支撑可信计算平台信任链建立和传递的可对外提供完整性度量、安全存储、密码计算等服务的功能模块。