国家电网公司 STATE GRID CORPORATION OF CHINA

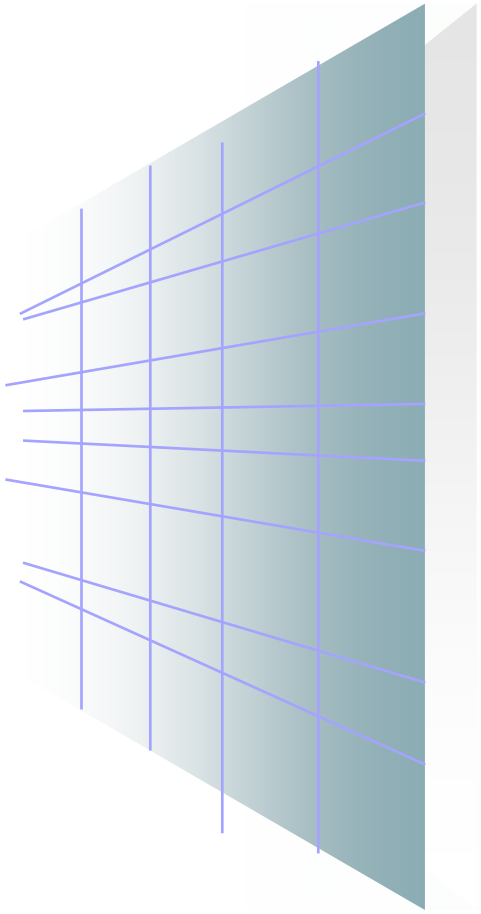
浙江省电力公司
电力科学研究院

《发电厂监控系统信息安全评估导则》编写大纲征求意见

国网浙江省电力公司电力科学研究院 尹峰

2017年9月14日

主要内容



1 立项背景与基本情况

2 编制依据与总体结构

3 基本思路与工作安排

1 立项背景与基本情况

网络事件频繁发生，攻击性增强

2016年10月，美国主要域名服务器DNS供应商Dyn遭遇DDoS攻击，互联网服务几乎全面宕机。旧金山市政运输部门售票系统被入侵勒索7万美金。

2017年5月，勒索病毒WannaCry爆发，席卷全球，电脑文件被加密锁定，勒索赎金。

2017年6月，新一轮Petya病毒蔓延欧洲多国，多个组织、多家企业的系统出现瘫痪。

国内网络安全重视度持续提升

面对复杂的网络和信息安全态势，网络安全已上升到国家战略高度。

随着各类针对公共设施的网络攻击事件不断出现，关系国计民生的关键信息基础设施与工业生产系统的网络安全已迅速引起重视。

《中华人民共和国网络安全法》已于2016年11月7日通过，规定对能源、交通、水利、金融、公共服务等重要行业和领域的关键信息基础设施，以及其他一旦遭到破坏可能严重危害国计民生的关键设施，实行重点保护。

1 立项背景与基本情况

国家电网公司 STATE GRID CORPORATION OF CHINA

浙江省电力公司
电力科学研究院

发电系统是工业领域关键基础设施

作为国民经济最重要的基础性支撑，全国投产单机1000MW超超临界发电机组已近70台，运行参数最高已达623℃/33.5MPa，全网电气设备互联，控制信息互联，非法入侵造成的安全风险极大。

发电设施极易成为攻击目标

发电厂监控信息系统脆弱性增加

随着计算机和网络技术的发展，以及两化深度融合与智能电厂建设，发电控制系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式实现网络互连互通。

信息化需求增加了控制系统与外界隔离的难度，各类摆渡攻击考验监控系统内部防线，国内发电机组已有发生因病毒原因导致设备异常事件。

还缺少针对性的信息安全相关标准，需要边积累经验边健全体系。

1 立项背景与基本情况

电力行业信息安全指导性文件

2014年，国家发改委第14号令：《电力监控系统安全防护规定》

2014年，国家能源局317号文：《电力行业网络与信息安全管理办法》国能安全【2014】317号

2015年，国家能源局36号文：《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》国能安全【2015】36号

电力行业信息安全工作开展情况

2015年6月，国家能源局启动《电力工控系统安全防护专项监管》，提出六项具体意见，包括：加强体系建设、强化防护措施、推进评估及等保工作、抓好应急管理、加强教育培训、规范产品选型。

2016年，国家能源局印发了《关于开展电力监控系统安全防护 专项检查工作的通知》国能综安全【2016】92号，组织开展电力监控系统安全防护专项检查。

2017年，发布了《电力监控系统安全防护专项监管报告（2016）》，并组织开展电力监控系统安全防护专项检查工作的“回头看”督查。

工控信息安全相关体系标准

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 30976.1-2014 工业控制系统信息安全 第1部分：评估规范

GB/T 32919-2016 信息安全技术 工业控制系统安全控制应用指南

GA/T 1390.5-2017 信息安全技术 网络安全等级保护基本要求 第5部分：工业控制系统安全扩展要求

信息安全技术 工业控制系统安全管理基本要求（国标报批）

信息安全技术 工业控制系统安全防护技术要求和测试评价方法（国标报批）

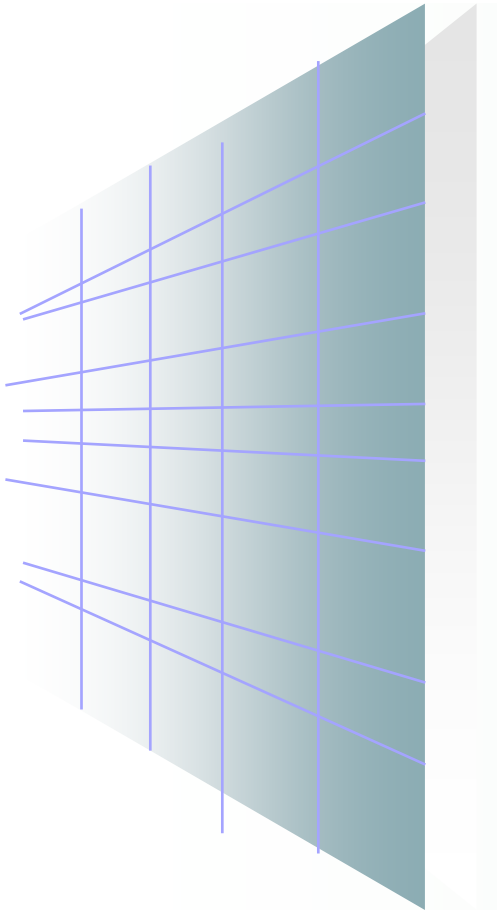
发电厂监控系统信息安全标准

电力监控系统网络安全防护导则（国标报批）

发电控制与信息系统网络安全防护技术要求（国标申报）

发电厂监控系统信息安全评估导则（团标编制）

主要内容



1 立项背景与基本情况

2 编制依据与总体结构

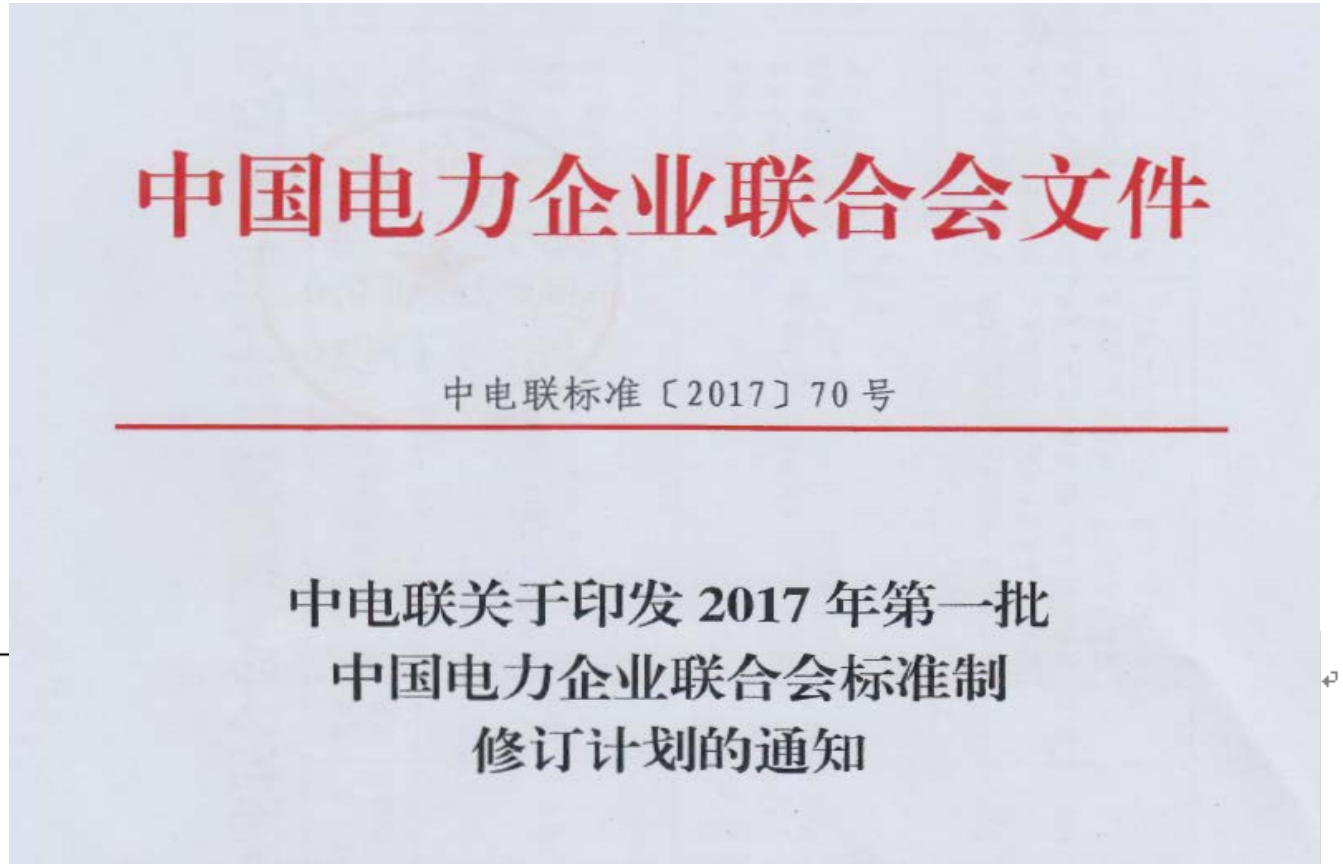
3 基本思路与工作安排

2 编制依据与总体结构

本标准编制计划

中国电力企业联合会 团体标准

T/CEC 20170173



中国电力企业联合会文件

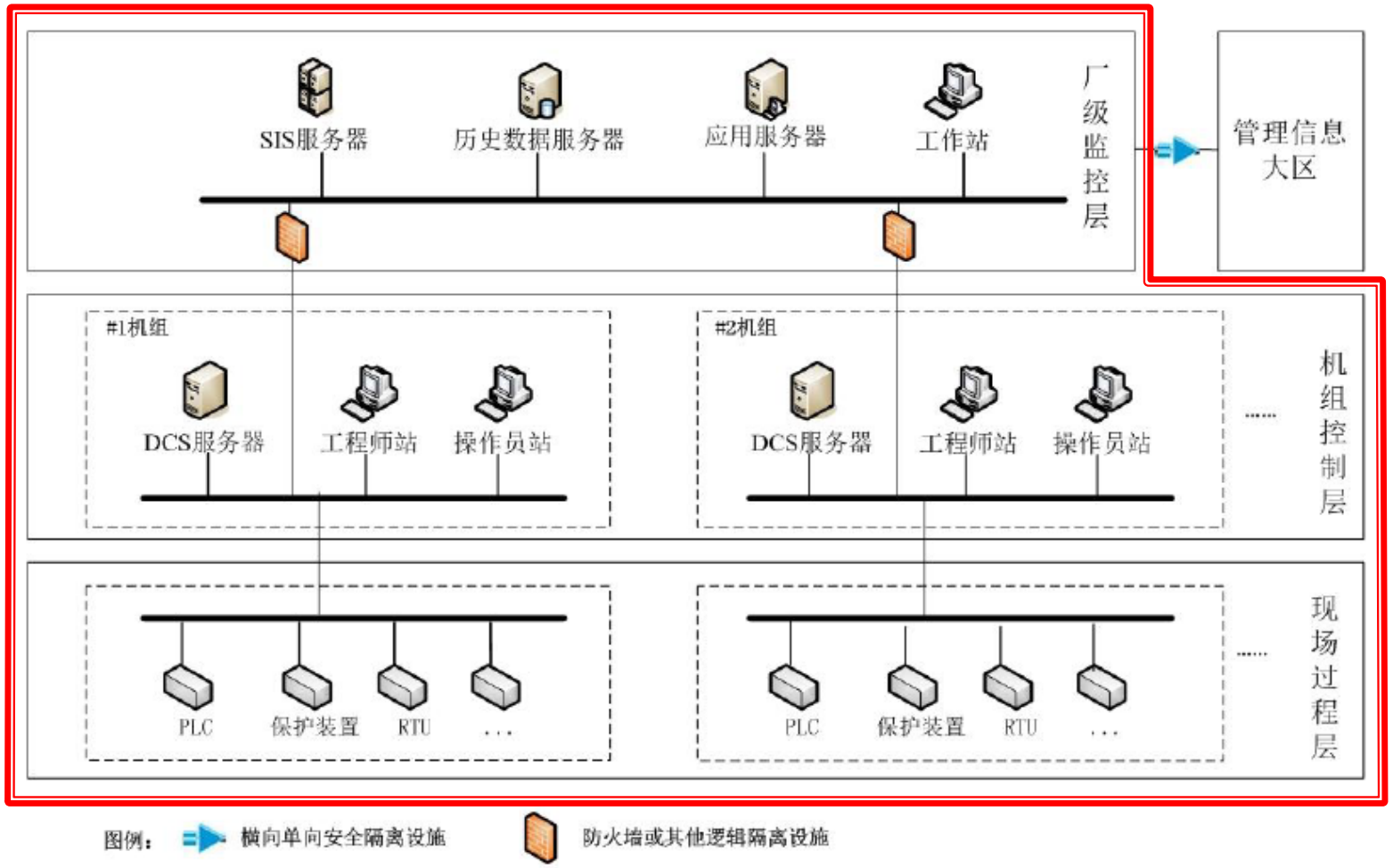
中电联标准〔2017〕70号

中电联关于印发2017年第一批
中国电力企业联合会标准制
修订计划的通知

73	T/CEC 20170173	发电厂工控系统信息安全评估导则	方法	制定	2018	估、网络监测与安全防护技术规定，作为发电厂工控系统测试评价、管理与检修、试验和日常运行维护的技术要求。	中国电力企业联合会	价咨询院、国网浙江电力公司电力科学研究院、浙江能源集团有限公司、华能国际电力股份有限公司等

2 编制依据与总体结构

1 范围



本标准描述了发电厂监控系统信息安全基本要求，提出了发电厂监控系统信息安全评估的方法、内容和要求。

本标准适用于燃煤、燃气、水力、风力、光伏发电厂生产控制大区的监控系统信息安全评估工作指导，核能发电厂可参照实施。

2 编制依据与总体结构

2 规范性引用文件

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
GB/T 22240-2008 信息安全技术 信息系统安全保护等级定级指南
GB/T 20984-2007 信息安全技术 信息系统安全风险评估规范
GB/T 25069-2010 信息安全技术_术语
GB/T 26863-2011 火电站监控系统术语
GB/T 30976.1-2014 工业控制系统信息安全 第1部分:评估规范
GB/T 30976.2-2014 工业控制系统信息安全 第2部分:验收规范
GB/T 32919-2016 信息安全技术 工业控制系统安全控制应用指南
GB/T XXXXX-XXXX 信息安全技术 工业控制系统安全管理基本要求
GB/T XXXXX-XXXX 信息安全技术 工业控制系统安全防护技术要求和测试评价方法

2 规范性引用文件

GB/T XXXXX-XXXX电力监控系统网络安全防护导则
GB/T 33008.1-2016 工业自动化和控制系统网络安全 可编程序控制器(PLC)
第1部分:系统要求
GB/T 33009.1-2016 工业自动化和控制系统网络安全 集散控制系统(DCS)
第1部分:防护要求
GB/T 33009.2-2016 工业自动化和控制系统网络安全 集散控制系统(DCS)
第2部分:管理要求
GB/T 33009.3-2016 工业自动化和控制系统网络安全 集散控制系统(DCS)
第3部分:评估指南
GB/T 33009.4-2016 工业自动化和控制系统网络安全 集散控制系统(DCS)
第4部分:风险与脆弱性检测要求

2 编制依据与总体结构

国家电网公司 STATE GRID CORPORATION OF CHINA

浙江省电力公司
电力科学研究院

3 术语和定义

4 缩略语

5 发电厂监控系统信息安全总体要求

5.1 发电厂监控系统概述

发电厂监控系统包括：分散控制系统（DCS、DEH、TCS）、继保与自动化系统（NCS、PMU、保护装置）、独立配置控制系统（PLC、OCS）、厂级监控信息系统（SIS）等。

5.2 发电厂信息安全防护基本原则

安全分区、网络专用、横向隔离、纵向认证、等级保护。

5.3 信息安全基本技术要求和管理要求

5.4 发电厂监控系统全生命周期安全评估要求

6 监控系统信息安全防护技术评估要求

6.1 物理安全评估 电源、消防、防水防潮、选址、控制站、环境控制、电磁防护、物理访问、防盗窃破坏

6.2 控制网网络安全评估 网络架构、边界防护、安全审计、冗余容差、无线接入、远程访问

6.3 网络设备安全评估要求 版本更新、设备标识、口令管理、访问与特权、配置管理、协议安全、端口安全、日志管理

6.4 主机安全评估 身份标识、访问、口令、审计、恶意代码防护、入侵防范

6.5 应用软件安全评估 版本更新、身份标识、访问控制、口令管理、安全审计

6.6 数据与通信安全评估 完整性、保密性、资源控制、备份恢复

6.7 控制设备安全评估 固件版本更新、设备标识、访问与特权、远程访问

7 监控系统信息安全管理评估要求

7.1 信息安全规划管理评估 信息安全规划、信息安全方案设计

7.2 信息安全制度管理评估 管理制度范围、制定发布信息、评审修订记录

7.3 信息安全组织建设评估 岗位设置、人员配备、授权审批、沟通合作、审核检查

7.4 人员安全管理评估 录用、离职、变动、教育培训、考核、第三方人员管理、处罚

7.5 信息安全开发运维管理评估 信息资产、介质、设备、维护、系统监控、补丁、采购、第三方评估、离线测试、验收交付

7.6 信息安全应急管理评估 应急预案、应急演练、应急保障、业务连续性规划

8 发电厂监控系统安全评估内容

8.1 **安全评估评分要素** 资产分类、资产赋值

8.2 **主控系统安全评估** 系统类型、系统设备识别与赋值

分类	信息资产	资产等级	威胁频率	安全价值

8.3 **辅控系统安全评估** 系统类型、系统设备识别与赋值

8.4 **电气二次系统安全评估** 系统类型、系统设备识别与赋值

8.5 **非控制实时系统安全评估** 系统类型、系统设备识别与赋值

8.6 **安全评估评分算法** 设备系统分值分配、定量计算公式

信息设备	安全配置要求	安全价值	符合性	得分

9 监控系统信息安全评估流程及实施方法

9.1 **安全评估准备** 组建团队、系统调研、制定方案

9.2 **安全评估启动** 启动会议

9.3 **现场评估** 技术评估、管理评估、已有安全措施评估

9.4 **报告编制** 数据汇总、风险分析、整改建议

9.5 **安全评估收尾** 企业整改、复评估、会议反馈

9.6 **监控系统信息安全评估实施方法** 文档查阅、现场访谈、现场核查、工具检测

2 编制依据与总体结构

附录A 信息安全评估评估表

附录A.1 燃煤发电厂信息安全评估表

附录A.2 燃气发电厂信息安全评估表

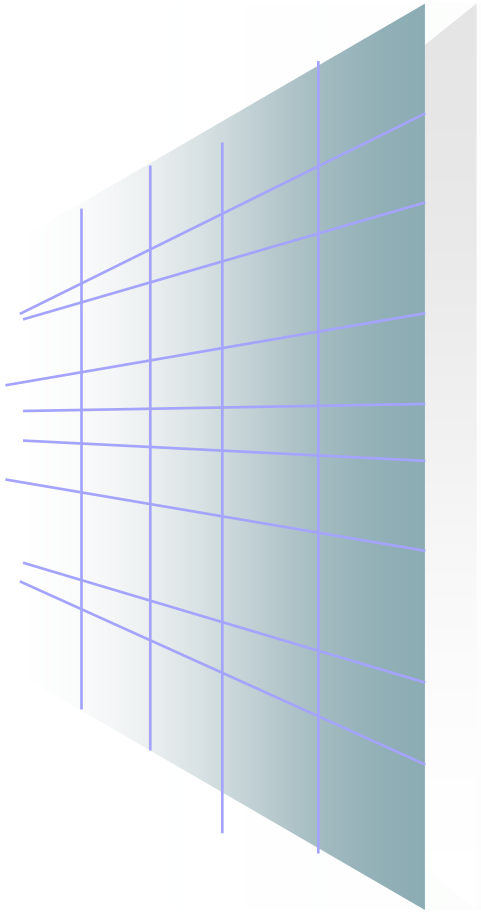
附录A.3 水力发电厂信息安全评估表

附录A.4 风力发电厂信息安全评估表

附录A.5 光伏发电厂信息安全评估表

附录B 监控系统信息安全评估工具要求

主要内容



1 立项背景与基本情况

2 编制依据与总体结构

3 基本思路与工作安排

3 基本思路与工作安排

基本编制思路

1）融合兼顾信息安全等级保护、电力监控信息安全防护、信息安全风险评估理念与要求，使信息安全评估结果同时满足政府、行业与专业要求，简化操作程序，避免重复工作。

2）使国家、部委、行业与专业各管理与技术要求具体化，根据不同类型发电厂实际细化落地，直接指导操作，具备较强的针对性。

3）对过于复杂的理论做适当简化变形，降低维度，提高实际可操作性：

借鉴发电机组安全性评价的做法，将风评中的脆弱性指标简化为合规判断，资产等级与威胁性指标变形为安全价值权重，最后得出安全性分值结果。

3 基本思路与工作安排

工作开展情况

2017年4月20日，标准计划下达。

2017年5月至8月，中电联及中国自动化学会发电专委会组织浙江电科院、杭州安恒公司、浙江能源集团、华能国际公司等单位收资、调研、讨论并完成大纲起草工作。

2017年8月30日，中电联标准化中心在浙江杭州召开了大纲审查会，组织专家对所完成的编写大纲进行审查。

根据审查会意见进行修改后，于2017年9月7日在浙江三门组织了大纲完善暨项目启动会，成立编制组。

后续工作安排

9月15日前，各组员分别提交燃煤、燃机、水电、风电、光伏电厂设备分类清册。

9月30日前，提交各分章节编写初稿。

10月15日，征求意见稿初稿讨论；10月22日完成征求意见稿。

10月23日，向行标委部份委员和专家发出征求意见稿。

11月23日征求意见结束。

11月30日，完成反馈意见处理，提交送审稿。

12月份，完成送审稿审查。

谢 谢！