

ICS 29.240
CCS K45

T/CEC

中国电力企业联合会标准

T/CECXXXXX—202X

继电保护智能运维检修
第3部分：网络安全要求

Intelligent operation and maintenance of relay protection
——Part 3: Network security requirements

（征求意见稿）

（在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上）

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中国电力企业联合会发布

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 总则..... 2

6 继电保护综合记录与智能运维装置要求..... 3

7 智能运检技术支持系统网络安全要求..... 4

8 运维行为要求..... 4

前 言

本文件依据 GB/T1.1—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》的规则起草。

本文件是 T/CEC XXXXX《继电保护智能运维检修》的第3部分。T/CEC XXXXX 已经发布了以下部分：

- 第1部分：管控系统检验；
- 第2部分：高级应用功能；
- 第3部分：网络安全要求；
- 第4部分：远方操作；
- 第5部分：在线监测站端信息描述；
- 第6部分：保护异常分析与处理；
- 第7部分：设备台账信息采集与应用；
- 第8部分：移动终端技术规范。

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。

本文件由中国电力企业联合会提出。

本文件由电力行业继电保护标准化技术委员会（DL/TC 15）归口。

本文件起草单位：

本文件主要起草人：

本文件为首次制定。

本文件在执行过程中的意见或建议反馈至中国电力企业联合会标准化中心（北京市白广路二条一号，100761）。

引 言

传统的以人工为主的继电保护运检模式，其技术和方法已无法适应智能变电站继电保护二次系统“数字化、网络化、信息化”发展的新特点。随着智能电网的建设和变电站自动化技术的发展，电网规模不断迅速扩大，继电保护运维业务的快速增长，电网运维人员数量并没有得到有效的增加。运维人员数量的严重不足，且电网保护类设备种类、数量众多，电网设备检修时间集中，传统检验模式工作量大、工作强度高的问题日益突出，导致设备安全运行压力在不断增大。因此，需要推进继电保护智能运维检修技术的应用，构建变电站继电保护智能运检架构和体系，推动继电保护运检模式的新变革，保障设备和电网安全稳定运行。

电力行业继电保护标准化技术委员会组织制定了“继电保护智能运维检修体系”。该体系由导则、运行管理及检修规程和支撑辅助标准三个层级的标准构成：

第一层：导则。《继电保护智能运维检修导则》，作为智能运检的纲领性文件，规定智能运检的一般性技术要求、功能要求和技术支持系统等。

第二层：运维管理、检修规程层。包括《继电保护和安全自动装置运行管理规程》、《继电保护和电网安全自动装置检验规程》、《继电保护装置状态检修导则》和《继电保护装置修理与退役要求》，承接导则的一般性要求，规定继电保护的运行管理要求、检修流程、检验项目等。

第三层：技术支持层。从装置研制、调试检测、定值管理、运维管控等方面，全面承接导则和运检规程所规定的实施条件、功能要求、实现方法和管控要求。

T/CEC XXXXX《继电保护智能运维检修》系列标准处于“继电保护智能运维检修体系”的第三层，该系列标准的制定，规范开展继电保护智能运维检修所需的设备要求和设计、检测、调试、验收、运行维护等全生命周期环节的要求，并能对变电站继电保护智能运检系统的设计、检测、调试、验收、运行维护等各个环节形成指导，提高变电站继电保护运维检修的标准化、规范化、智能化水平。系列文件由以下部分构成：

- 第 1 部分：管控系统检验；
- 第 2 部分：高级应用功能；
- 第 3 部分：网络安全要求；
- 第 4 部分：远方操作；
- 第 5 部分：在线监测站端信息描述；
- 第 6 部分：保护异常分析与处理；
- 第 7 部分：设备台账信息采集与应用；
- 第 8 部分：移动终端技术规范。

随着继电保护智能运维检修技术的不断发展，《继电保护智能运维检修》所包含的部分有可能进行相应的补充或扩展。

继电保护智能运维检修 第3部分：网络安全要求

1 范围

本文件规定继电保护智能运维检修（以下简称智能运检）网络安全方面的相关术语和定义，明确变电站继电保护智能运维检修设备、系统以及运维行为的网络安全要求。

本文适用于 35kV~1000kV 电压等级变电站继电保护智能运维检修系统在网络安全方面的规划、设计、验收与运维工作管理。

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 2900.1 电工术语基本术语

GB/T 2900.49 电工术语电力系统保护

GB/T 21052 信息安全技术 信息系统物理安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术术语

GB/T 36572 电力监控系统网络安全防护导则

NB/T 10680 继电保护和安全自动装置信息安全技术导则

NB/T 42015 智能变电站网络报文记录及分析装置技术条件

DL/T 2378 变电站继电保护综合记录与智能运维装置通用技术条件

DL/T 2192 并网发电厂变电站电力监控系统安全防护验收规范

3 术语和定义

GB/T 2900.1、GB/T 2900.49、GB/T 21052、GB/T 22239、GB/T 25069、NB/T 10680、DL/T 2378 界定的以及下列术语和定义适用于本文件。

3.1

身份鉴别 authentication

专用于鉴别传输、消息或发信方有效性的安全措施，或者对接收特定信息类别的个人授权进行验证的手段。

3.2

访问控制 access control

保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

4 缩略语

下列缩略语适用于本文件。

GOOSE：面向通用对象的变电站事件(Generic Object Oriented Substation Events)

MMS：制造报文规范（Manufacturing Message Specification）

5 总则

在变电站网络安全框架基础上，继电保护智能运维检修网络安全防护架构应满足运维对象网络安全等级保护相应级别要求，实现对运维设备、系统及行为进行网络安全管控，防范网络安全威胁。

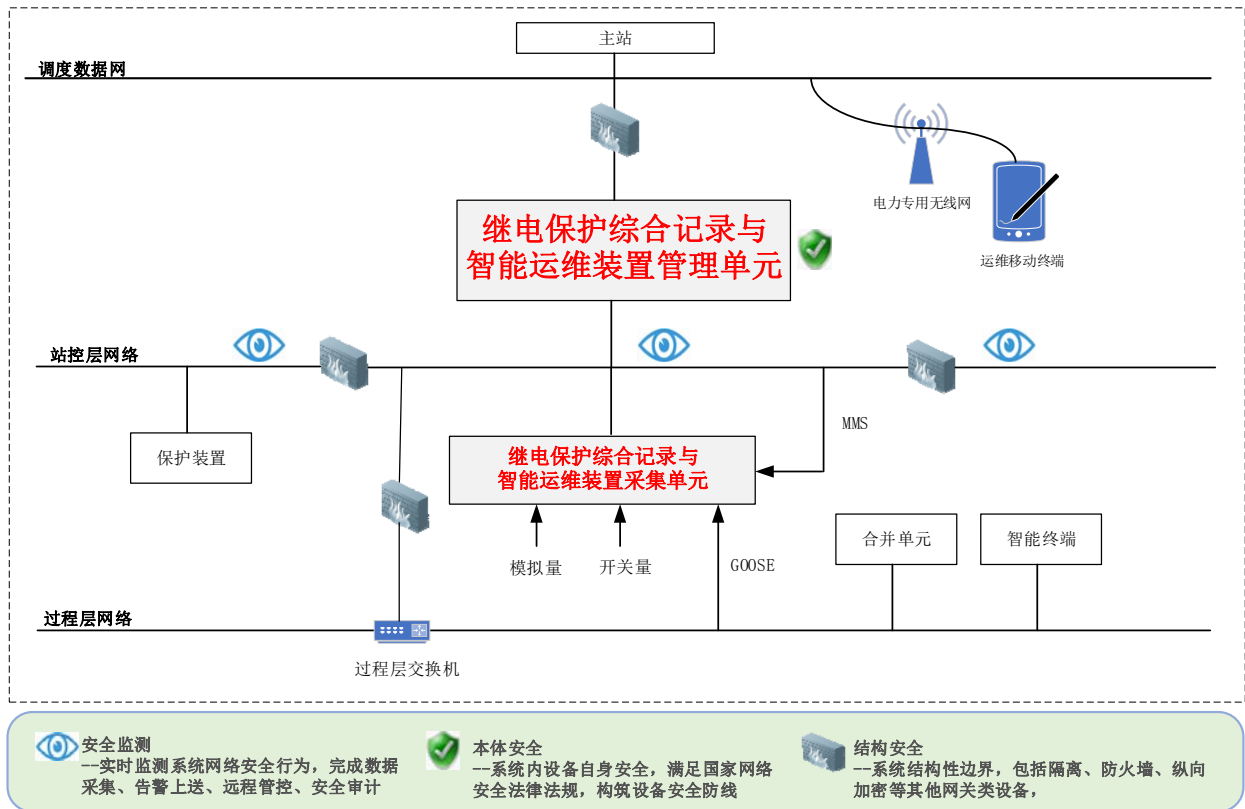


图 1 变电站继电保护智能运维检修网络安全防护架构

继电保护智能运维检修网络安全防护架构设计总体原则如下：

- 5.1 应满足国家法律法规和国家技术标准的相关要求，如国家网络安全法、数据安全法、GB/T 22239、GB/T 36572 等。
- 5.2 构建安全可靠的智能运检技术支持系统网络架构，严格遵循“安全分区、网络专用、横向隔离、纵向认证”的基本要求，提高智能运检技术支持系统网络的边界防护能力。
- 5.3 对智能运检技术支持系统内主机设备、网络交换设备、安全防护设备等实现全面的网络安全信息采集，并上送网络安全管理平台。
- 5.4 加强继电保护运维行为的网络安全管理，建立一套有效的运维操作流程，提升运维人员的网络安全意识与风险识别能力。

6 继电保护综合记录与智能运维装置要求

6.1 身份鉴别

本项要求包括：

- a) 继电保护综合记录与智能运维装置应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
- b) 继电保护综合记录与智能运维装置应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
- c) 继电保护综合记录与智能运维装置管理单元宜采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

6.2 访问控制

本项要求包括：

- a) 继电保护综合记录与智能运维装置应对登录的用户分配账户和权限；
- b) 继电保护综合记录与智能运维装置应重命名或删除默认账户，修改默认账户的默认口令；
- c) 继电保护综合记录与智能运维装置应及时删除或停用多余的、过期的账户，避免共享账户的存在；
- d) 继电保护综合记录与智能运维装置应授予管理用户所需的最小权限，实现管理用户的权限分离；
- e) 继电保护综合记录与智能运维装置应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

6.3 安全审计

本项要求包括：

- a) 继电保护综合记录与智能运维装置应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
- 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) 继电保护综合记录与智能运维装置应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
- d) 继电保护综合记录与智能运维装置应对审计进程进行保护，防止未经授权的中断。

6.4 控制设备安全

本项要求包括：

- a) 对于继电保护综合记录与智能运维装置的补丁更新、固件更新等工作不应影响系统安全稳定运行；
- b) 应使用专用设备和专用软件对继电保护综合记录与智能运维装置进行更新；
- c) 应保证继电保护综合记录与智能运维装置在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。

6.5 安全监测

本项要求包括：

- a) 继电保护综合记录与智能运维装置管理单元应上送网络安全信息到网络安全监测装置，上送信息种类包括但不限于登录操作、网络行为、USB 设备插拔、文件变更、设备运行状态（CPU 使用率、内存使用率等）、开放服务。

7 智能运检技术支持系统网络安全要求

7.1 网络架构

本项要求包括：

- a) 应保证智能运检技术支持系统网络各个部分的带宽满足运维检修业务高峰期需要；
- b) 智能运检技术支持系统内设备出现故障、死机或断电的情况下，不应网络产生影响；
- c) 运行通道与运维通道宜划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
- d) 重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
- e) 关键的通信线路和网络设备应提供硬件冗余，保证系统的可用性。

7.2 入侵防范

本项要求包括：

- a) 应在智能运检技术支持系统关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
- b) 应在智能运检技术支持系统关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
- c) 应采取技术措施对智能运检技术支持系统内行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

7.3 无线接入

本项要求包括：

- a) 运维移动终端应在具备纵向加密隔离的条件下通过电力专用无线网接入智能运检技术支持系统主站；
- b) 运维移动终端应采用带有加密认证功能的传输协议

8 运维行为要求

8.1 工程实施

本项要求包括：

- a) 继电保护运维检修工作开始前，应提前制定符合网络安全管理制度的实施方案，实施方案需执行审批流程；
- b) 继电保护运维检修工作开始前应制定应急机制，明确网络安全应急预案和现场处置方案；
- c) 需使用专门的继电保护设备调试工具与继电保护设备管理口通信，完成数据查阅、数据传输等信息交互，禁止使用未经授权的调试工具访问设备的任何功能；
- d) 调试工具宜通过运维网关类设备接入智能运检技术支持系统内运维对象；
- e) 运维结束后，需要进行常规安全检查，检查内容包括设备运行状态、软件版本和数据备份等情况。

8.2 测试验收

8.2.1 通信网络验收

本项要求包括：

- a) 智能运检技术支持系统网络部署应符合安全分区原则，不同分区之间应使用电力专用安全隔离装置实现物理隔离；
- b) 不同分区在调度数据网纵向边界需设置电力专用纵向加密认证装置，实现双向身份认证、数据加密和访问控制。

8.2.2 设备本体验收

本项要求包括：

- a) 继电保护综合记录与智能运维装置需出具国家指定机构的安全检测证明；
 - b) 继电保护综合记录与智能运维装置使用的操作系统、数据库、中间件等基础支撑软件 and 业务软件应安全可控，宜采用经国家有关部门检测认证的产品。
-