ICS 29.240.30
K 07
备案号：50775-2015

DL

中华人民共和国电力行业标准

DL / T 1455 — 2015

电力系统控制类软件安全性及其测评技术要求

Technical requirements of safety and security for electric power system control software and software testing

2015-07-01发布　　2015-12-01实施

国家能源局　发布

目　　次

前　言

电力系统控制类软件为电网安全稳定运行提供了重要技术保障。为确保电力系统控制类软件的安全性和可靠性，规范和指导电力系统控制类软件的安全性测评、设计、开发、建设、运行和维护，制定本标准。

本标准按照GB/T 1.1—2009《标准化工作导则　第1部分：标准的结构和编写》给出的规则起草。

本标准由中国电力企业联合会提出。

本标准由全国电网运行与控制标准化委员会（SAC/TC 446）归口。

本标准起草单位：国家电力调度控制中心、中国电力科学研究院、南方电网公司电力调度控制中心、南京南瑞集团公司、国家电网公司华北分部、国网福建省电力有限公司、广东电网有限责任公司电力科学研究院、积成电子股份有限公司、东方电子股份有限公司。

本标准主要起草人：陶洪铸、李立新、严亚勤、花静、孙炜、韩秀文、郑志千、李宇佳、张东院、高昆仑、慈国兴、杨清波、刘楠、狄方春、单松玲、陈郑平、张勇、江泽鑫、陈鹏、陈宁、韩丽芳、李凌、林静怀、梁智强、米为民、梅峥。

本标准首次发布。

本标准在执行过程中的意见或建议请反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

电力系统控制类软件安全性及其测评技术要求

1 范围

本标准规定了电力系统控制类软件的功能安全性、网络安全性的技术要求和测评要求。

本标准适用于电力系统控制类软件的安全性测评、设计、开发、建设、运行和维护。

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 11457 信息技术 软件工程术语

GB/T 20272 信息安全技术 操作系统安全技术要求

GB/T 20273 信息安全技术 数据库管理系统安全技术要求

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 22240 信息安全技术 信息系统安全等级保护定级指南

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 30149 电网通用模型描述规范

DL/T 476 电力系统实时数据通信应用层协议

DL/T 634.5101 远动设备及系统 第5-101部分：传输规约 基本远动任务配套标准

DL/T 634.5104 远动设备及系统 第5-104部分：传输规约 采用标准传输协议集的IEC 60870-5-101网络访问

DL/T 667 远动设备及系统 第5部分：传输规约 第103篇：继电保护设备信息接口配套标准

DL/T 860（所有部分） 变电站通信网络和系统

DL/T 890（所有部分） 能量管理系统应用程序接口

DL/T 1169 电力调度消息邮件传输规范

DL/T 1170 电力调度工作流程描述规范

DL/T 1230 电力系统图形描述规范

DL/T 1232 电力系统动态消息编码规范

DL/T 1233 电力系统简单服务接口规范

国家发展和改革委员会2014年第14号令 电力监控系统安全防护规定

3 术语和定义

GB/T 11457界定的以及下列术语和定义适用于本文件。

3.1

电力系统控制类软件 power system control software

对电力系统一、二次设备进行操作控制的调控主站和厂站软件，一般可分为调控主站控制类软件和厂站控制类软件两类，支持人工操作控制或自动控制。

3.2

功能安全性 functional safety

在电力系统控制类软件运行过程中防止误控，保障电网安全、设备安全和人身安全的能力。

3.3

网络安全性　cyber security

为电力系统控制类软件采取的安全保护措施，防止计算机硬件、软件、网络、数据因偶然或恶意的原因而遭到存取、使用、修改、毁坏或泄露。

3.4

圈复杂度　cyclomatic complexity

用来衡量一个模块判定结构的复杂程度，数量上表现为独立现行路径条数。

3.5

修订条件/判定覆盖率　modified condition/decision coverage

用于机载系统和设备中软件开发、软件合格审定的白盒测试方法，修订条件/判定覆盖率用于度量代码测试的有效性和充分性。

3.6

代码覆盖率　code coverage fraction

代码测试有效性和充分性的度量，包括语句覆盖率、分支覆盖率、条件覆盖率、修订条件/判定覆盖率。

3.7

完整性　integrity

软件的完整性既包含了数据的完整性，即保证数据不被非法地改动和销毁，也包含了系统的完整性，即保证系统不被有意或无意的非法操作所破坏。

3.8

安全审计　security audit

为评估电力系统控制类软件工作产品或工作产品集是否符合保护资产、维护数据完整、最经济使用资源等要求而进行的一种独立的检查，检查内容包括识别、记录、存储和分析那些与网络安全性相关的信息。

4　符号、代号和缩略语

下列缩略语适用于本文件。

AGC：自动发电控制（automatic generation control）

AVC：自动电压控制（automatic voltage control）

CCS：协调控制系统（coordinated control system）

DCS：分布式控制系统（distributed control system）

IP：网络互连协议（internet protocal）

LCU：逻辑控制单元（logical control unit）

MAC：介质访问控制（media access control）

MC/DC：修订条件/判定覆盖（modified condition/decision coverage）

SCADA：数据采集与监视控制（supervisory control and data acquisition）

SM2：商密椭圆曲线算法

UKey：通用串行总线接口型密码验证存储设备（usb key）

5　安全性技术要求

5.1　控制类软件分类

电力系统控制类软件包括调控主站控制类软件和厂站控制类软件，总体范围如图 1 所示。主站控制

类软件包括前置通信、SCADA、AGC、AVC 和配电 SCADA，厂站控制类软件包括变电站监控系统（含升压站、换流站）、发电厂监控系统（火电厂 DCS、水电厂 CCS 等）和配电自动化子站。主站控制类软件与厂站控制类软件通过电力调度数据网的实时子网或专用通道进行数据传输，经电力调度数据网传输的通道应部署纵向加密装置（卡）。

电力系统控制类软件安全性测评应包含功能安全性及网络安全性测评，测评工作对象应包含主站控制类软件和厂站控制类软件。

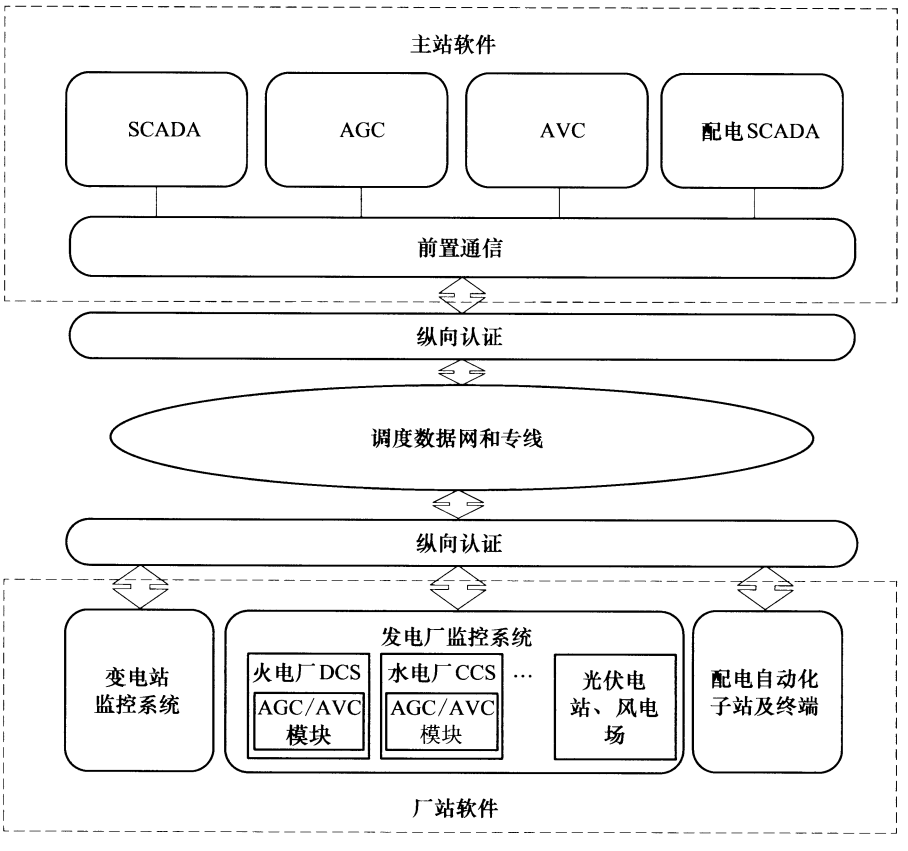

图 1　电力系统控制类软件分类

5.2　通用技术要求

电力系统控制类软件应满足以下通用要求：

a）　应满足国家发展和改革委员会 2014 年第 14 号令所规定的要求。

b）　应具备控制命令的校核、闭锁功能，厂站和主站之间的数据传输应满足实时性、可靠性、准确性、规范性及保密性要求，软件中不应存在恶意代码及内存泄露等重要代码缺陷。

c）　应具备控制命令传输的全过程安全认证及安全审计机制，控制命令在传输过程中的安全认证应涵盖控制命令执行的全过程，包括人机界面、监控应用、数据采集模块以及传输通道等环节；人机与监控应用通信过程中，应采用带安全认证的模式进行安全防护，监控应用与数据采集模块通信过程中，应采用在原有事件结构中增加安全验证信息的模式进行安全防护。

d）　应具备独立的开发、运行、维护及离线测试环境；应采用安全可控的服务器、操作系统、数据库等；宜具备安全可信计算功能，实现系统主动安全免疫。

e）　应具备冗余热备容错机制，软件的功能、性能等质量属性应满足安全运行要求，在系统开发过程及投运前，对控制环节所涉及的控制操作功能，应综合采用黑盒、白盒、灰盒测试方法验证其功能安全。

5.3 主站控制类软件技术要求

主站控制类软件应满足以下技术要求：

a） 应支持单设备控制、序列控制、顺控、群控等控制模式；
b） 应支持限定的“选择-返校-执行”步骤进行遥控操作；
c） 应支持直接控制操作；
d） 应具备遥控操作监护功能，支持双人双机遥控操作；
e） 应具备控制拓扑防误校核功能；
f） 应具备一、二次设备异常信号闭锁控制操作功能；
g） 应支持设备挂牌注释等功能，闭锁不满足控制条件的设备；
h） 应支持对多源数据进行一致性校验；
i） 应支持对控制下发通道的手动和自动选择；
j） 应支持前置缓存控制指令的时效性校验；
k） 应具备基于调度数字证书及标签的安全认证功能；
l） 应具备口令、权限等安全配置校验功能；
m） 应具备遥控、遥调表的摘要、签名和验证功能；
n） 应具备控制操作记录保存及定期审计功能；
o） 应具备遥控过程中异常中断处理功能。

5.4 厂站控制类软件技术要求

厂站控制类软件应满足以下技术要求：

a） 应支持单设备控制、序列控制、顺控、群控等控制模式；
b） 应具备接收、处理和执行调控主站远方控制指令的功能；
c） 应具备向调控主站提供设备运行数据、设备运行状态等信息的功能；
d） 应支持厂站内设备就地和远方的操作控制；
e） 应具备告警直传功能；
f） 应具备基于逻辑和电气的控制闭锁功能；
g） 应具备控制配置校验功能；
h） 应具备通信网关双机配置一致性校验功能；
i） 同期条件不具备时，控制操作不应成功；
j） 应具备监控信息的一致性校验功能；
k） 应具备控制操作记录保存和定期审计功能；
l） 宜具备对控制操作指令安全校核功能；
m） 应拒绝执行不合理的控制命令。

5.5 主站与厂站接口技术要求

主站和厂站之间的通信和数据交换应遵循标准化原则，满足数据交换实时性、可靠性、准确性的要求；主站与厂站接口开展标准符合性测试时的测试内容及依据见表 1，应根据软件的具体情况选择相关测试项进行测试。

表 1 电力系统控制类软件主要接口标准符合性基本要求

测 试 内 容	标 准 依 据
电网通用模型描述规范	GB/T 30149

表 1（续）

测 试 内 容	标 准 依 据
电力调度消息邮件传输	DL/T 1169
电力调度工作流程描述	DL/T 1170
电力系统图形描述	DL/T 1230
电力系统动态消息编码规范	DL/T 1232
电力系统简单服务接口	DL/T 1233
电力系统实时数据通信协议	DL/T 476、DL/T 634.5101、DL/T 634.5104 等
继电保护设备信息接口配套标准	DL/T 667
能量管理系统应用程序接口	DL/T 890
变电站通信网络与系统	DL/T 860

5.6 数据传输技术要求

数据传输应满足以下技术要求：

a） 应具备纵向传输的数据加密功能；

b） 应支持数据传输的机密性和完整性保护；

c） 应具备双向身份认证功能；

d） 应支持监控信息的唯一性控制与可追溯机制；

e） 应在监控信息规定的数据范围内采集数据；

f） 应具备数据传输通道状态校验功能；

g） 应具备数据传输通道被非法入侵或专线通道串线造成误控的判定功能。

6 功能安全性测评要求

6.1 主站控制类软件测评要求

主站控制类软件功能安全性测试内容主要包括控制基本功能、控制安全要求、控制策略、控制操作统计及判据、拓扑防误校核、用户权限管理等，应满足以下要求：

a） SCADA 软件应满足附录 A 的表 A.1 中 SCADA 软件项所规定的功能安全性要求；

b） AGC 软件应满足附录 A 的表 A.1 中 AGC 软件项所规定的功能安全性要求；

c） AVC 软件应满足附录 A 的表 A.1 中 AVC 软件项所规定的功能安全性要求；

d） 前置通信软件应满足附录 A 的表 A.1 中前置通信软件项所规定的功能安全性要求；

e） 配电 SCADA 软件应满足附录 A 的表 A.1 中配电 SCADA 软件项所规定的功能安全性要求。

6.2 厂站控制类软件测评要求

厂站控制类软件功能安全性测试内容主要包括设备控制、序列控制、操作闭锁、控制权限、控制策略等，应满足以下要求：

a） 变电站监控软件应满足附录 B 的表 B.1 中变电站监控系统软件项所规定的功能安全性要求；

b） 发电厂监控软件应满足附录 B 的表 B.1 中发电厂监控系统软件项所规定的功能安全性要求；

c） 发电厂监控软件的 AGC 模块软件应满足附录 B 的表 B.1 中 AGC 模块项所规定的功能安全性要求；

d） 变电站及发电厂监控软件的 AVC 模块软件应满足附录 B 的表 B.1 中 AVC 模块项所规定的功能安全性要求；

e） 配电自动化子站及终端软件应满足附录 B 的表 B.1 中配电自动化子站及终端软件项所规定的功能安全性要求。

6.3 数据传输测评要求

电力系统控制类软件数据传输应满足以下要求：

a） 主站软件和厂站软件都应具备数据加密认证功能，对端有装置的应启用密通功能；

b） 应支持配置 IP 地址和限定端口的安全策略；

c） 应支持基于 SM2 算法的调度数字证书双向身份认证和访问控制；

d） 应基于数字签名和版本号管理实现监控信息版本发布与管理；

e） 主站软件应具备遥控信息表文件和遥控相关配置审计功能；

f） 主站软件及厂站通信网关机应具备厂站设备地址校验机制，对控制报文的厂站设备地址进行校核。

6.4 代码质量测评要求

6.4.1 恶意代码识别

电力系统控制类软件中不应包含具有病毒、蠕虫、木马特征的代码，并应支持以下恶意代码注入防范功能：

a） 应具备软件进程、服务和服务端口白名单功能；

b） 应具备系统调试接口关闭功能；

c） 宜不包含使用管理员权限的资源访问代码；

d） 宜支持软件执行程序校验机制。

6.4.2 代码实现正确性

检查代码缺陷验证编程实现的正确性，应对代码进行控制流、数据流、接口和表达式等分析，检查代码缺陷所引起的问题，包括但不限于附录 C 中静态结构分析项目规定的内容，应满足以下要求：

a） 不包含以下缺陷类型：

1） 内存泄露缺陷；

2） 数组越界缺陷；

3） 空指针引用缺陷；

4） 代码不可达缺陷；

5） 内存释放后引用缺陷；

6） 并发机制缺陷；

7） 资源利用缺陷。

b） 千行代码缺陷率≤0.5%。

6.4.3 质量度量

应对软件的文件类型、代码量、模块数、模块圈复杂度等信息进行度量、分析、统计，包括但不限于附录 C 中质量度量项目所规定的内容。代码质量度量宜满足以下要求：

a） 模块圈复杂度平均值≤10；

b） 圈复杂度过大（＞10）的模块比例数≤0.8%；

c） 模块平均代码行数≤100；
d） 源代码行数过大（＞200 行）的模块比例≤0.5%；
e） 源代码注释率≥20%。

6.4.4 编程规则符合性

应对源代码进行编程规则的检查与分析，并统计千行代码规则违背率。源代码编程应采用统一的变量命名规范，且千行代码规则违背率≤5%。

6.4.5 测试充分性

电力系统控制软件白盒测试充分性应满足以下覆盖率要求：
a） 语句覆盖率为 100%；
b） 分支覆盖率为 100%；
c） 条件覆盖率≥80%；
d） MC/DC 覆盖率≥80%。

7 网络安全性测评要求

7.1 一般要求

电力系统控制类软件进行网络安全性检查和测试时应按 7.2～7.11 的要求开展，并根据 GB/T 20272、GB/T 20273、GB/T 22239、GB/T 22240、GB/T 25058 规定的安全级别确定检查和测试的项目。

7.2 身份鉴别

身份鉴别应满足以下要求：
a） 应对登录用户进行身份标识和鉴别，确保用户身份标识的唯一性；
b） 应提供基于口令、调度数字证书、指纹卡等鉴别技术的两种或两种以上组合的方式对用户身份进行鉴别；
c） 应对使用者在被授予敏感操作权限（如遥控操作）之前进行鉴别；
d） 应限制用户口令的有效期，并限制用户在更改口令时使用重复口令；
e） 应具备用户登录失败检测功能；
f） 应具备远方操作权限控制功能，并与交接班管理模块关联，应支持当班监控员、当前登录调度数字证书、监控员工作站等信息的一致性校验；
g） 应具备用户弱口令周期自动检测告警功能，对于弱口令或重复口令用户，限制其登录系统，强制口令修改时间间隔，用户口令应在系统中加密存储；
h） 应依据 IP 地址、MAC 地址等属性对连接服务器的客户端工作站进行限制。

7.3 访问控制

访问控制应满足以下要求：
a） 应支持基于调度员、监控员、运维人员、审计管理员、系统管理员等角色的访问控制功能；
b） 应支持角色与权限的绑定，不同角色人员应按照工作范围、职责分工分配相应的访问控制权限；
c） 应支持角色互斥功能，禁止配置同时具有控制和维护修改权限的角色，系统中不得存在超级管理员角色；
d） 应依据安全策略控制用户对监控信息等文件或数据库表等客体的访问；

e） 应支持对重要信息资源设置安全标记功能，并提供基于安全标记的访问控制。

7.4 安全审计

安全审计应满足以下要求：

a） 应具备覆盖每个用户的安全审计功能；
b） 审计功能中应对遥控等业务事件和新建用户、授权等系统事件进行记录；
c） 应具备对审计数据进行搜索、查询、分类、排序等功能；
d） 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
e） 应具备审计数据的管理功能，并能够对审计事件的项目进行选择和设置；
f） 应支持定义分级的系统异常事件类型，并且根据异常的严重程度分别采用日志记录、警告提示、声光报警等方式进行通知。

7.5 数据完整性

数据完整性应满足以下要求：

a） 应具备对监控信息等关键数据的存储完整性保护功能；
b） 应具备对监控信息、信息点、控制命令等关键数据的传输完整性保护功能；
c） 应在检测到关键数据完整性错误时，提供必要的恢复手段。

7.6 数据保密性

数据保密性应满足以下要求：

a） 应对通信过程中的关键报文进行加密；
b） 应支持用户口令等关键数据的加密存储和传输；
c） 应支持基于 UKey 等硬件设备对重要通信过程进行加解密运算和密钥管理。

7.7 抗抵赖

电力系统控制类软件应具备对遥控等关键操作的原发抗抵赖功能。

7.8 软件容错

软件容错应满足以下要求：

a） 应对人工输入数据有效性进行检验；
b） 应具备自动保护功能；
c） 应具备系统恢复功能。

7.9 资源控制

资源控制应满足以下要求：

a） 应对登录用户的会话超时时间进行限制；
b） 应对请求进程占用的系统资源分配最大限额、最小限额和资源水平降低到预先规定的最小值进行检测和报警；
c） 应具备服务优先级设置功能。

7.10 信息探测

软件运行时应关闭存在风险的无关服务和端口。

7.11 剩余信息保护

软件应保证系统内的文件、目录和数据库记录等敏感信息所在的存储空间被释放或再分配给其他用户前被完全清除。

附 录 A
（规范性附录）
主站控制类软件功能安全性测评要求

主站控制类软件功能安全性测评要求见表 A.1。

表 A.1 主站控制类软件功能安全性测评要求

功 能 项	技 术 要 求
a）SCADA 软件	
责任区设置	1）遥控、置数、挂牌等人工操作应只对本责任区范围内的对象有效，禁止操作无关对象； 2）限值修改等数据维护应只对本责任区范围内的对象有效； 3）人员、机器均配置责任区，本责任区的人员、机器应只能操作本责任区范围内的对象； 4）人员可配置角色，不同的角色配置拥有不同的权限； 5）机器可配置角色，不同的角色配置拥有不同的权限； 6）责任区的操作权限范围可灵活控制到全网、控制区、厂站、间隔、设备级别； 7）不同责任区的操作和浏览权限可灵活设置电网范围，可互斥隔离，也可有交叉重叠； 8）模型参数修改等数据维护操作应对人员、机器的权限进行验证，禁止不具备权限的人员和机器进行操作
人工置数	人工输入数据应进行有效性检查
标识牌操作	1）禁止对具有禁止操作类标识牌的设备进行操作； 2）禁止对具有保持分闸/保持合闸标识牌的设备进行合闸/分闸操作； 3）对于不具备接地开关的点挂临时接地线时，应支持设置接地标识牌并禁止操作
闭锁和解锁操作	1）闭锁功能用于禁止对所选对象进行特定的处理，包括数据更新、告警处理和远方操作等； 2）闭锁功能和解锁功能应成对提供； 3）所有的闭锁和解锁操作应进行存档记录
操作和控制	1）控制操作应有防误校核机制，校核不通过不能进行控制； 2）应支持通过双机认证之后的强制控制功能； 3）变压器挡位调节应逐级调节，禁止跳挡操作； 4）遥控进行选择操作后在设定时间内没有响应的应自动撤销遥控操作； 5）遥控执行前应返校成功才能执行遥控； 6）应支持置入状态下遥控操作许可性配置； 7）应禁止两个及以上控制台在同一时刻对同一设备进行遥控操作； 8）应保存所有操作记录，提供详细的存档信息，包括操作人员姓名、操作对象、操作内容、操作时间、操作结果等，可供调阅和打印
操作权限	1）应对所有操作进行权限控制，操作应限定在有权限的工作站上进行； 2）操作人员应有相应的权限
b）AGC 软件	

表 A.1（续）

功 能 项	技 术 要 求
控制校核	1）应进行控制目标有功值上下限校验，检查控制目标值是否超过机组调节上下限； 2）应对控制目标值调节步长进行限制； 3）应对关键量测（频率、联络线交换功率、机组出力、机组上下限）的量测状态和实时值变化合理性进行校核； 4）应对全厂/单机控制指令是否处于机组全厂/单机禁止运行区进行校验； 5）应对模式无扰切换进行验证
控制闭锁	在进行控制时对于不符合控制条件的厂站、LCU 或发电机应可闭锁、封锁厂站或机组的控制命令
c）AVC 软件	
闭锁和解锁操作	1）应能禁止 AVC 对所选对象进行控制，但是不影响其他模块的处理等； 2）闭锁功能和解锁功能应成对提供； 3）所有的 AVC 闭锁和解锁操作应进行存档记录； 4）软件在检测到控制设备故障信息、异常信号或其他预设条件时，应可靠闭锁
控制校核	1）控制下发设备应在许可的厂站范围内，防止对未许可的厂站下发控制命令； 2）控制设备应满足一定的编码或者命名规则，防止控制到错误的设备； 3）应校验控制目标电压值上下限； 4）应限制控制目标电压调节步长； 5）应校验关键量测（电压、机组无功）的量测状态和实时值变化合理性； 6）机组可调无功上下限应根据 *P-Q* 曲线加以限制，并考虑厂站上送的无功调节能力； 7）离散设备投切应满足动作次数、动作时间间隔、动作顺序的要求
d）前置通信软件	
数据校核	1）前置通信应对通信接收的数据进行严格校验，禁止将不合法的数据传递给上一层应用； 2）前置通信应对发送数据进行严格校验，禁止将不合法的数据转发出去
控制校核	1）前置通信应判断控制命令的正确性，禁止将非法值下发给厂站； 2）前置通信应从规约通信层面判断控制返回命令，将校核命令返回结果传递给上层应用
通信加密	重要厂站不应通过公网通信链路进行通信，如需要通信，应采用经过认证的加密方式进行通信
e）配电 SCADA 软件	
操作闭锁	禁止对具有禁止操作类标识牌的设备进行操作
控制与调节	调度操作与控制应有校核机制，校核不通过，不能进行调节
双席监督	双席操作校验时，监护员应对控制操作进行确认
控制权限	1）操作应从有控制权限的工作站上进行； 2）操作人员应有相应的权限

表 A.1（续）

功 能 项	技 术 要 求
遥控操作	1）操作应对人员、机器的权限进行验证，禁止无权限的人员、机器进行遥控操作； 2）应具备设备遥控操作许可属性的配置功能； 3）应具备置入状态下遥控操作许可属性的配置功能； 4）应具备单席操作/双席操作模式的配置功能； 5）应具备普通操作/快捷操作方式的配置功能； 6）操作时每一步应有提示，每一步的结果应有相应的响应； 7）双席操作校验时，监护员应对控制操作进行确认； 8）遥控进行选点操作后在设定时间内没有响应自动撤销遥控操作； 9）遥控执行前应返校成功才能执行遥控； 10）同一时刻禁止两个及以上控制台对同一设备进行遥控操作； 11）禁止对挂接地牌的设备进行遥控操作； 12）应保存所有操作记录，提供详细的存档信息，包括操作人员姓名、操作对象、操作内容、操作时间、操作结果等，可供调阅和打印
序列控制	1）应验证人员、机器的操作权限，禁止无权限的人员、机器进行序列控制操作； 2）控制过程中对每一个控制点都应进行遥信返校； 3）禁止控制条件不满足的序列被自动执行或手动执行； 4）可中断控制过程中的控制操作； 5）控制过程中出现操作失败的，应自动停止后续控制
防误闭锁	1）常规防误闭锁，应按预定义的操作闭锁条件进行闭锁； 2）拓扑防误闭锁，应不依赖于人工定义，通过网络拓扑分析设备运行状态，约束调度员安全操作
信号确认	1）操作应对人员、机器的权限进行验证，无权限的人员、机器禁止信号确认操作； 2）信号确认只对本责任区内信号有效； 3）应支持信号、间隔、全站、全系统四级确认功能，各级别提供权限验证
标识牌操作	1）应验证人员、机器的权限，禁止无权限的人员、机器进行挂牌操作； 2）禁止对具有锁住标识牌的设备进行操作； 3）禁止对具有保持分闸/保持合闸标识牌的设备进行合闸/分闸操作； 4）对具有警告标识牌的设备执行操作时应进行提示； 5）对于不具备接地开关的点挂接地线时，应设置接地标识牌，并在操作时检查接地标识牌； 6）应能通过人机界面设置标识牌或撤销标识牌，在执行远方控制操作前应先检查对象的标识牌； 7）挂检修牌之前应先挂接地牌； 8）挂有人牌之前应先挂检修牌； 9）设备处于运行状态时禁止挂除保持合闸之外的标识牌； 10）设备处于冷备状态时禁止挂保持合闸标识牌
馈线自动化	1）可自动生成非故障区段的恢复供电方案，避免恢复过程导致其他线路、主变压器等设备过负荷； 2）可设置故障处理闭锁条件，避免保护调试、设备检修等人为操作的影响； 3）故障处理过中应具备必要的安全闭锁措施（如通信故障闭锁、设备状态异常闭锁等），保证故障处理过程不受其他操作干扰； 4）主站馈线自动化功能应支持人工预设、调整、优化处理方案等辅助功能； 5）应保存故障处理的全部过程信息，以备故障分析时使用

附 录 B
（规范性附录）
厂站控制类软件功能安全性测评要求

厂站控制类软件功能安全性测评要求见表 B.1。

表 B.1 厂站控制类软件功能安全性测评要求

功 能 项	技 术 要 求
a）变电站监控系统软件	
远程浏览	应具备安全措施，禁止无控制权限的人员远程浏览时进行控制操作
分级控制	1）操作按照优先级可分为设备就地操作、间隔层操作、站控层操作和远方控制，其中本地操作优先级最高，远方控制优先级最低，应具备远方/就地控制方式的切换功能； 2）站内同一个时间只执行一个控制操作命令，禁止同时响应多个操作命令
单设备控制	1）控制操作前应有校核的步骤，校核不通过禁止执行； 2）控制对象设置禁止操作标识牌时禁止执行； 3）操作员应有相应的权限，双席操作校验时，监护员应确认； 4）操作有记录，且记录不可篡改和删除
同期操作	同期操作应检测断路器两侧的母线、线路电压幅值、相角及频率，实现自动同期捕捉合闸
定值修改	1）应对定值修改进行权限控制； 2）应支持定值修改校核机制； 3）应支持远方切换定值区
软压板投退	应支持远方投退软压板校核机制
主变压器分接头调节	主变压器分接头调节应逐级上调或下调，禁止跳挡
调度操作与控制	应支持调度操作与控制校核机制，校核不通过时，禁止调节操作
防误闭锁	1）防误闭锁可分为站控层闭锁、间隔层联闭锁和机构电气闭锁三个层次； 2）站控层闭锁宜由监控主机实现，操作应经过防误逻辑检查后方能将控制命令发至间隔层，如发现错误应闭锁该操作； 3）站控层闭锁、间隔层联闭锁和机构电气闭锁属于串联关系，站控层闭锁失效时应不影响间隔层联闭锁，站控层和间隔层联闭锁均失效时应不影响机构电气闭锁
b）发电厂监控系统软件	
遥调接口测试	DCS 系统经过转换的指令值应与远动装置一致，误差应不超过 0.5%
机组量测异常保护	出现机组量测异常时，DCS 应能退出 AGC 远方控制，机组出力无异常变化
内部异常退出 AGC 远方控制	电厂内部故障信号，机组应主动退出 AGC 远方控制
远动装置掉电/复位	应识别远动装置掉电进而闭锁控制，机组出力无异常变化
控制方式及切换安全	1）机组控制方式可支持就地命令方式、调度远方命令方式、曲线方式、手动方式等控制方式切换，在切换中人为设置命令和曲线异常，各种模式切换时，控制系统和机组出力应运行平稳；

表 B.1（续）

功 能 项	技 术 要 求
控制方式及切换安全	2）命令或曲线异常时，DCS 应有保护闭锁功能
通信中断 AGC 保护	网络中断后在一定时间内恢复的，全厂 AGC 状态应保持不变；否则，全厂 AGC 功能应退出运行，各机组出力应无异常变化
c）AGC 模块	
信号一致性和精度	1）各个通道均应能正确接收调度下发的指令； 2）经过转换的指令值应和远动装置一致，遥测和遥调误差应不超过 0.5%
机组 AGC 不合理调节命令保护	1）应拒绝执行调度下发的不合理控制命令，用实发出力覆盖遥调命令值； 2）连续三次收到不合理控制命令后，AGC 功能应自动退出运行
控制校核	1）应对机组有功功率、断路器位置、并网状态等关键量的数据质量进行监测，对数据一致性和合理性进行校核； 2）对发生拒动、调节超时等异常情况的机组应能及时闭锁控制，并向主站发送信号； 3）水电厂机组可调有功上下限应根据水头实时计算加以限制，且应避开不可运行区； 4）应对控制权和模式无扰切换进行验证
d）AVC 模块	
信号一致性和精度	1）各个通道均应能接收调度下发指令； 2）经过转换的指令值应和远动装置一致，无功遥测和遥调误差应不超过 0.5%，电压遥测和遥调误差应不超过 0.2%
AVC 不合理调节命令保护	1）应拒绝执行调度下发的不合理控制命令，并自动保持当前的电厂母线电压值； 2）连续三次收到不合理控制命令后 AVC 功能应自动退出主站闭环控制，转化就地自动控制运行
控制校核	1）应对机组有功功率、无功功率、断路器位置、并网状态等关键量的数据质量进行监测，对数据一致性和合理性进行校核； 2）对发生拒动、调节超时等异常情况的机组应及时闭锁控制，并向主站发送信号； 3）应对控制权和模式无扰切换进行验证
e）配电自动化子站及终端软件	
操作闭锁	禁止对具有该标识牌的设备进行操作
控制与调节	调度操作与控制应有校核机制，校核不通过，不能进行调节
控制权限	1）操作应从有控制权限的工作站上进行； 2）操作人员应有相应的权限
遥控操作	1）操作应对人员、机器的权限进行验证，无权限的人员、机器禁止进行遥控操作； 2）应具备设备遥控操作许可属性的配置功能； 3）应具备置入状态下遥控操作许可属性的配置功能； 4）操作时每一步应有提示，每一步的结果应有相应的响应；

表 B.1（续）

功 能 项	技 术 要 求
遥控操作	5）遥控进行选点操作后在设定时间内没有响应自动撤销遥控操作； 6）遥控执行前应返校成功才能执行遥控； 7）同一时刻禁止两个及以上控制台对同一设备进行遥控操作； 8）禁止对挂接地牌的设备进行遥控操作； 9）应保存所有操作记录，提供详细的存档信息，包括操作人员姓名、操作对象、操作内容、操作时间、操作结果等，可供调阅和打印
防误闭锁	1）常规防误闭锁，应按预定义的操作闭锁条件进行闭锁； 2）拓扑防误闭锁，不应依赖于人工定义，通过网络拓扑分析设备运行状态，约束调度员安全操作
信号确认	1）操作应对人员、机器的权限进行验证，无权限的人员、机器禁止信号确认操作； 2）信号确认应只对本责任区内信号有效
标识牌操作	1）操作应对人员、机器的权限进行验证，无权限的人员、机器禁止进行挂牌操作； 2）禁止对具有锁住标识牌的设备进行操作； 3）禁止对具有保持分闸/保持合闸标识牌的设备进行合闸/分闸操作； 4）对具有警告标识牌的设备执行操作时应进行提示； 5）对于不具备接地开关的点挂接地线时，应设置接地标识牌，并在操作时检查接地标识牌； 6）应能通过人机界面设置标识牌或撤销标识牌，在执行远方控制操作前应先检查对象的标识牌； 7）挂检修牌之前应先挂接地牌； 8）挂有人牌之前应先挂检修牌； 9）设备处于运行状态时禁止挂除保持合闸之外的标识牌； 10）设备处于冷备状态时禁止挂保持合闸标识牌
馈线自动化	1）可自动生成非故障区段的恢复供电方案，避免恢复过程导致其他线路、主变压器等设备过负荷； 2）可设置故障处理闭锁条件，避免保护调试、设备检修等人为操作的影响； 3）故障处理过程中应具备必要的安全闭锁措施（如通信故障闭锁、设备状态异常闭锁等），保证故障处理过程不受其他操作干扰； 4）子站馈线自动化功能应能与主站馈线自动化功能相配合，及时将故障处理信息上送给主站； 5）应保存故障处理的全部过程信息，以备故障分析时使用

附 录 C
（规范性附录）
电力系统控制类软件代码质量测评项目

电力系统控制类软件代码质量测评项目见表 C.1。

表 C.1 电力系统控制类软件代码质量测评项目

序号	测 评 项 目	
1	静态结构分析	数组越界
2		空指针引用
3		代码不可达
4		变量使用前未初始化
5		打印函数格式
6		编译器警告
7		迭代器使用不当
8		内存释放后引用
9		资源处理问题
10		函数返回类型不匹配
11		并发机制问题
12		非法的用户输入
13		函数参数格式校验
14		内存分配问题
15		可疑代码操作
16	质量度量	源文件数
17		头文件数
18		源代码总行数（包括空行）
19		总注释行数
20		总注释率（总注释行/总行数）
21		文件注释率小于 20%的比例
22		模块数
23		模块圈复杂度
24		圈复杂度过大（＞10）的模块数
25		模块行数
26		模块规模（＞200 行）过大模块数

中 华 人 民 共 和 国
电 力 行 业 标 准
电力系统控制类软件安全性及其测评技术要求
DL / T 1455 — 2015
*
中国电力出版社出版、发行
（北京市东城区北京站西街 19 号　100005　http://www.cepp.sgcc.com.cn）
北京九天众诚印刷有限公司印刷
*
2016 年 4 月第一版　　2016 年 4 月北京第一次印刷
880 毫米×1230 毫米　16 开本　1.25 印张　33 千字
印数 001—300 册
*
统一书号 155123・2842　定价 **11.00** 元

中国电力出版社官方微信　　掌上电力书屋

刮开涂层
查询真伪

155123.2842