ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

工业电气自动化控制程序安全管控规范

Specification for Safety Management and Control of Industrial Electrical Automatic Control Programs

（工作组讨论稿）

（本草案完成时间：2026 - 5 - 6 ）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　　发 布

目　　次

前　言

本文件依据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。

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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

工业电气自动化控制程序安全管控规范

1 引言

在国家新型工业化推进、工业互联网深度融合及数字化转型战略落地的大背景下，PLC、DCS、SCADA 等电气自动化控制程序已成为能源、交通、石化等关键基础设施的核心支撑，是保障国家工业体系稳定运行、维护国计民生与公共利益的重要基石。为深入贯彻《关键信息基础设施安全保护条例》《工业控制系统网络安全防护指南》等国家法规政策要求，填补控制程序全生命周期安全管理短板，规范程序编写、测试、下载、变更、备份及退役全流程行为，防范程序失控引发的国家安全风险、人员伤亡、环境污染及重大经济损失，筑牢工业安全防线，特制定本文件。本文件的制定旨在推动工业控制程序安全管理与国家工控安全战略同频共振，助力制造业高端化、智能化、绿色化发展，为国家关键信息基础设施安全提供坚实保障。

2 范围

严格依据国家工业控制系统安全防护相关标准，明确了电气自动化控制程序在开发、测试、发布、部署、变更、备份、退役及应急恢复全生命周期内的安全管控要求，全面覆盖权限管理、版本控制、防篡改机制、审计溯源及供应链安全等核心环节，构建全方位、多层次、闭环式的安全管理体系。适用于电力、石化、冶金、市政、轨道交通及制造业等国家重点行业领域，涉及控制系统（PLC、DCS、SCADA、CNC）的业主单位、运维服务商、系统集成商及设备供应商，是各相关单位落实工控安全主体责任、规范控制程序管理、防范安全风险的重要依据，同步衔接国家网络安全等级保护、工控安全分级规范等相关要求，确保执行落地与国家战略要求高度一致。

3 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，确保本规范与国家、国际最新标准同步，保障管理要求的科学性和权威性。

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

GB/T 36324-2018 信息安全技术工业控制系统信息安全分级规范

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB 46038-2025 工业机械电气设备及系统安全要求

GB/T 42457-2023 工业自动化和控制系统信息安全产品安全开发生命周期要求

IEC 62443-3-3:2022 工业通信网络网络和系统安全系统安全要求和安全等级

工信部网安〔2024〕14 号 工业控制系统网络安全防护指南

《关键信息基础设施安全保护条例》（国务院令第 745 号）

4 术语和定义

下列术语和定义适用于本文件，统一规范关键概念表述，确保各相关单位执行过程中的认知一致，契合国家工控安全领域标准术语规范。

4.1 控制程序

指运行于可编程逻辑控制器（PLC）、分散控制系统（DCS）、监控与数据采集系统（SCADA）、计算机数控系统（CNC）等自动化设备中的梯形图、结构化文本、功能块图、顺序功能图及组态配置文件，是保障关键基础设施自动化运行的核心软件载体。

4.2 基线版本

指经过完整测试、严格审批并正式部署于生产环境中，作为后续程序变更比对、追溯校验基准的控制程序实体，是保障程序变更安全性、一致性的基础。

4.3 程序下载

将经过编译或解析的控制程序从工程师站、便携式维护终端传输至目标控制器（PLC、DCS 控制器等）非易失性存储区并使其生效的行为，是程序落地运行的关键环节，直接关系到生产系统的稳定安全。

4.4 逻辑互锁

指程序中为防止设备误动作、规避安全风险而设置的基于安全状态的强制制约条件，是保障设备运行安全、防范生产安全事故的核心逻辑设计。

5 总体要求

本章节基于国家关键信息基础设施安全保护要求，确立控制程序全生命周期安全管理的核心原则，确保管理工作的方向性和整体性，全面衔接国家工控安全战略部署。

5.1 全生命周期闭环原则

应建立覆盖“编写—验证—审批—下载—运行—变更—退役”的全过程闭环管控机制，贯穿程序从产生到废止的全流程，确保任一环节可追溯、可审计、可管控，落实国家工控安全全流程防护要求，防范流程断点引发的安全风险。

5.2 权限最小化与职责分离原则

严格遵循国家网络安全权限管理相关规范，实现程序修改权、下载权与运行操作权的分离管控，构建“权责清晰、相互制衡、全程监督”的管理体系。严禁同一人同时持有程序源码编辑权限与生产环境下载执行权限，从源头防范人为操作风险，落实最小授权原则。

5.3 安全优先原则

坚持“安全第一、预防为主、综合治理”的方针，当程序修改为提高生产效率与保障安全发生冲突时，必须优先保障安全联锁与保护功能的正确性，坚决守住安全底线。任何临时性的强制（Force）或跳转（Jump）操作必须具有 48 小时内的自动失效机制，防范临时操作失控引发的安全事故，契合国家工控安全应急管控要求。

6 组织机构与人员权限管控

围绕国家工控安全主体责任落实要求，明确各相关岗位职能与身份鉴别标准，强化人员管理，防范人为因素引发的安全风险，构建专业化、规范化的管理团队。

6.1 岗位职能划分

6.1.1 编程工程师：负责控制程序的编写、静态测试与单元测试，持有开发环境编辑权，严格遵循国家编码安全规范，确保程序编写质量，承担程序开发阶段的安全责任。

6.1.2 审核专家（或委员会）：由行业专家、安全技术人员组成，负责审查程序逻辑是否符合国家安全规范、行业标准及本文件要求，审查周期不超过 40 个工作时，确保程序安全合规后进入下一环节。

6.1.3 发布管理员：负责将审批通过的程序写入“只读”发布区，管理软件版本库，严格管控程序发布流程，防范未授权程序流入生产环境，落实版本管控主体责任。

6.1.4 现场操作/维护工程师：仅具备监视权限、参数（P、I、D 等）设定权限，严禁修改核心联锁梯形图，严格按照操作规范开展运维工作，做好操作记录，确保生产环境程序稳定运行。

6.2 身份鉴别要求

6.2.1 访问控制器或工程师站必须采用“口令+硬件 Key”的双因素认证，契合国家工控安全身份鉴别相关要求。口令长度不小于 8 位，包含大小写字母、数字及特殊符号，有效期不超过 90 天，定期更换，严禁使用默认口令、弱口令，强化身份认证安全性。

6.2.2 所有第三方运维人员接入控制系统网络必须申请临时访客账号，明确授权范围与有效期，该账号权限应在授权期满后自动冻结，全程记录运维操作，落实第三方运维安全管控要求，防范外部人员非法访问。

7 程序开发与测试验证

严格按照国家工业自动化和控制系统信息安全相关标准，规范程序开发与测试验证流程，确保程序质量安全，从源头防范程序漏洞引发的安全风险，助力国家工业软件安全自主可控发展。

7.1 编码安全规范

7.1.1 死循环规避：在 PLC 程序中，任何功能块或子程序扫描周期严禁超过系统设定的看门狗（Watchdog）时间（一般为 200ms~500ms），防范程序卡死导致设备失控，保障系统稳定运行。

7.1.2 安全数据范围：模拟量输入（如 4-20mA）必须在程序中进行断线监测，结合国家工控数据安全保护要求，当数值超出传感器量程-5%至 105%范围时，程序应导向预设的安全状态（如输出置 0 或保持上一可靠值），防范数据异常引发的安全事故。

7.1.3 冗余切换：涉及 CPU 冗余切换的逻辑，必须进行主备程序一致性校验，切换时间应不大于 50ms，保障关键设备连续稳定运行，契合国家关键基础设施高可用性要求。

7.2 实验室仿真测试

程序在进入现场下载前，必须在硬件在环（HIL）仿真平台或同等测试环境中完成至少 72 小时的连续运行测试，落实国家工控安全测试验证相关要求。测试用例的覆盖率需覆盖全部联锁逻辑的真值表，通过率必须达到 100%，未通过测试的程序严禁进入生产环境，确保程序安全可靠。

8 变更管理与发布流程

规范程序变更与发布流程，实行分级管控、严格审批，防范程序变更引发的安全风险，确保变更过程合规、可控，契合国家工控安全配置管理要求。

8.1 变更分级

8.1.1 重大变更：涉及安全联锁逻辑、核心算法、控制策略架构或跨 CPU 通讯协议的修改，此类变更可能影响系统安全运行，需严格履行最高级别审批流程，落实重大变更安全评估要求。

8.1.2 一般变更：非关键参数的设定值修改、报警上下限调整、非安全相关的界面优化，此类变更不影响系统核心安全功能，按标准流程审批后实施。

8.1.3 紧急变更：为应对即将发生的人员伤亡或重大设备损坏事故，需立即下装的修改，此类变更可启动紧急流程，同时强化事后追溯，确保变更合规。

8.2 审批流程

8.2.1 标准流程：申请（填写 ECN 表格）→ 技术论证（风险评估）→ 安全审核 → 批准签发。该流程超过 5 个工作日未批复的，视为驳回，确保审批效率与合规性，落实变更风险管控要求。

8.2.2 紧急流程：必须获得副总工程师及以上级别管理人员授权，同步报行业主管部门备案，在变更实施后的 24 小时内补全所有书面手续，确保紧急变更可追溯、可审计。

8.3 版本号规则

必须采用三段式命名规则：V<主版本>.<次版本>.<修订号>，统一版本管理标准，便于追溯、比对与管控，契合国家工控软件版本管理规范。主版本：架构重构或不兼容变更；次版本：新增功能性逻辑；修订号：Bug 修复或参数微调。

9 下载与现场实施管控

严格规范程序下载与现场实施操作，强化过程管控，防范现场操作失误引发的安全事故，落实国家工控安全现场运维管理要求，保障生产系统稳定运行。

9.1 操作票制度

必须执行“电气自动化控制系统程序变更操作票”制度，操作票需经多方审核确认，明确操作责任。操作票应包含：设备编号、当前运行版本、目标版本、预计下载时长、可能导致的结果（如设备停机、阀门瞬间失电）及应急处置措施，确保操作全过程可控。

9.2 下载操作硬性规定

9.2.1 环境确认：进行程序下载前，必须确认控制器处于“停止”模式或“远程”模式。涉及热停工（Hot

Cutover）的操作，必须确认设备处于安全静态或已切除联锁总开关，做好安全防护措施，防范操作过程中引发的设备误动作。

9.2.2 双人操作：必须遵循“一人操作、一人复核”原则，落实国家工控安全双人管控要求。操作员手持键盘鼠标执行下载点击，复核员手持操作票逐一核对通讯端口与文件名，确认无误后签字确认，防范单人操作失误风险。

9.2.3 比对机制：下载软件必须开启“在线/离线程序比对”功能，确认差异仅为本次变更项，无误码后方可执行写入，防范程序误下载、错下载引发的安全风险，保障程序完整性。

9.3 禁止性行为

严禁在工艺装置正常运行（即连续生产投料状态）且未停机的情况下，对涉及紧急停车（ESD）功能的控制器进行逻辑组态下装，除非该控制器支持无扰切换且已通过风险评估，并报行业主管部门备案，坚决守住生产安全底线。

10 备份、恢复与审计

建立健全程序备份、恢复与审计机制，落实国家工控数据备份与审计溯源要求，防范程序丢失、损坏或非法操作引发的安全风险，保障系统可恢复、操作可追溯。

10.1 强制备份频率

10.1.1 离线备份：每次成功下载新程序后，必须在 4 小时内将最终版源码、编译文件及配置参数导出至 U 盘或网络存储，一式两份异地存放，落实国家数据异地备份要求，防范单点故障导致程序丢失。

10.1.2 定期备份：即使无程序变更，每月的 1 日必须对所有控制系统进行一次全量备份。备份保留周期不少于 3 年，契合国家工控数据留存相关规范，确保程序可追溯、可恢复。

10.2 恢复演练

涉及重大危险源的重点装置（如大型机组、反应釜），每年至少组织一次基于“裸机”环境的控制程序全量恢复演练，落实国家工控安全应急演练要求。从硬件安装到程序成功运行的时间（恢复时间目标，RTO）应不大于 4 小时，提升应急处置能力，保障关键设备快速恢复运行。

10.3 审计日志

10.3.1 控制系统必须启用审计日志功能，全面记录所有登录、退出、程序修改、模式切换、强制（Force）操作等行为，落实国家工控安全审计溯源要求，确保操作可追溯、可追责。

10.3.2 审计日志的存储空间应满足至少 6 个月的容量需求，并具备防溢出、防删除（即使是管理员也无法删除）的保护机制，契合国家网络安全等级保护相关要求，确保日志完整性和安全性。

11 网络安全与防篡改

紧扣国家网络安全等级保护与工控网络安全防护要求，强化程序传输、访问及终端安全管控，防范网络攻击、恶意代码入侵及程序篡改风险，筑牢工控网络安全防线。

11.1 传输加密与完整性

程序从工程师站到控制器的传输通道应使用私有协议或加密隧道，优先采用商用密码，契合国家密码安全相关要求。下载完成后，控制器应自动计算程序的哈希值（如 SHA-256）并与工程师站源文件哈希值进行比对，防止传输过程中的数据位翻转或中间人攻击，保障程序传输安全与完整性。

11.2 访问控制列表（ACL）

在工业交换机或控制器本体上配置访问控制列表，仅允许指定的工程师站（基于 MAC 地址和 IP 双重绑定）具有下载权限，落实国家工控网络访问控制要求。严禁将编程软件默认的“Anyone”或“Full Control”权限应用于生产环境，防范非法访问与程序篡改。

11.3 恶意代码防范

用于编程和调试的便携式计算机（便携式维护终端）在接入控制网络前，必须经过专用查杀介质扫描，部署防病毒软件并定期升级病毒库。严禁在连接控制器的电脑上使用来源不明的 U 盘或连接互联网，防范勒索软件等恶意代码入侵，落实国家工控终端安全防护要求。

12 应急响应与废止

建立健全程序失控应急处置与废止管理机制，落实国家工控安全应急响应与数据留存要求，提升应急处置能力，规范程序生命周期末端管理，防范废旧程序误用风险。

12.1 程序失控处置

一旦发现由于程序原因导致设备异常动作，现场处置应遵循“急停优先于查原因”的原则，立即启动应急处置预案，及时上报行业主管部门。安全回路（Safety PLC）发出的停机指令优先级必须高于普通 PLC 的逻辑指令，最大限度减少人员伤亡和财产损失，落实国家工控安全应急处置要求。

12.2 废止程序管理

废止的旧版本程序应移交档案室进行“冷存储”，保存期限为设备全生命周期加 1 年，契合国家工控数据留存相关规范，确保程序可追溯。废止程序应在所有运维人员的本地硬盘及共享服务器中彻底清除，建立清除记录并留存备查，防止误用，规范程序生命周期末端管理。