

T/CASME

中国中小商业企业协会团体标准

T/CASME XXXX—2023

无线同步测录系统建设技术规范

Technical specification for construction of wireless synchronous recording system

（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。

2023 – XX – XX 发布

2023 – XX – XX 实施

中国中小商业企业协会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 建设原则 1

5 系统结构 2

6 系统要求 2

7 系统交付 4

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。

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××××提出。

本文件由××××归口。

本文件起草单位：××××

本文件主要起草人：××××

无线同步测录系统建设技术规范

1 范围

本文件规定了无线同步测录系统的建设原则、系统结构、系统要求、系统交付等内容。
本文件适用于无线同步测录系统建设。

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 20271 信息安全技术 信息系统通用安全技术要求
- 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 网络安全等级保护基本要求
- GB/T 31168 信息安全技术 云计算服务安全能力要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

无线同步技术 wireless synchronization technology

是利用相互通信的两个或多个无线模块，达到时间同步的目标，从而实现无线同步的技术。

3.2

节点 node

表示一个连接点或通信端点（一些终端设备），用于连接两个或更多的电子线路和电气元件，作为它们之间传递信息的通道。

3.3

录波 recording wave

是电力系统的一种检测方法。它主要用于检测电力系统特定设备的运行状况，通过录波图分析诊断特定设备是否正常运行，包括设备的开机联网、通电的电流、电压等稳定性等。

4 建设原则

4.1 兼容性

测录系统应采用模块化设计，具有良好的互联互通及迭代能力，任何一个模块的升级短期内都不应影响到其他模块的正常运行。

4.2 安全性

测录系统应有抵抗恶性攻击、抵抗入侵系统和企图从系统中获取敏感数据和信息的能力，应具有一定的防暴力破坏和防窃取信息的能力，保证数据的安全性、保密性、完整性、一致性和相容性。

4.3 可扩展性

测录系统应考虑预留接口和容量，可根据要求加装其他测量单元，满足测录系统扩展、升级、改进的需要。

4.4 易维护性

测录系统应易于维护，应符合以下要求：

- 应符合业内通用规范，易于维护；
- 系统界面应友好，易安装、使用、维护；
- 业务流程应清晰，符合常规业务处理习惯；
- 数据维护应方便，数据备份及恢复应快速简单；
- 系统配置应简便，应避免复杂的系统配置程序。

5 系统结构

无线同步测录系统总体技术框架宜采用数据层、支撑层、应用层三层体系结构：

- a) 第一层应为数据层，即运行系统的数据库，对数据资源进行收集、共享、储存，为应用层系统功能提供数据支持，数据资源主要包括：用户信息、工程及节点信息、波形数据等；
- b) 第二层应为支撑层，即应用支撑环境，包括应用中间件、基础构件等；
- c) 第三层应为应用层，为用户提供应用服务，包括信息查询、设备控制、工程管理、录波操作等。

6 系统要求

6.1 信息展示

6.1.1 信息展示要求

信息展示应满足以下要求：

- 应具备普通用户、直属用户、系统管理员多级权限管理功能，实现功能管理和信息展示区分；
- 应可设置预警临界值，对系统工作异常和监测要素异常进行报警；
- 应具备接入新增测录工程的功能。

6.1.2 信息展示类型

6.1.2.1 硬件信息

硬件信息应直接由客户维护到对应的数据库表中，包括但不限于以下参数：

- 设备 IP；
- 分组；
- 采集节点 IP；
- 通道挡为；
- 开关动作；
- 触发方式及出发条件；
- 设备电池量比。

6.1.2.2 设备工作信息

设备工作与状态相关信息应包括但不限于以下参数：

- 连网状态；
- 对应的工程、任务名称；
- 当前活跃状态。

6.1.2.3 设备操作信息

设备操作信息展示，主要展示对设备的操作功能，应包括但不限于以下功能：

- 设备开关机状态；
- 设备工程设置；
- 执行工程计划及任务；
- 强制触发；
- 查看设备采集节点；
- 查看实时波形。

6.2 设备控制

设备控制功能应同6.1.3中所展示的功能：

- 设备开关机控制；
- 设备工程设置；
- 执行工程计划及任务；
- 强制触发（工程计划不满足触发录波条件时，可采取强制触发和录波）；
- 设备采集节点查询；
- 实时波形监控。

6.3 工程管理

6.3.1 新建工程

工程管理模块应提供新建工程功能，宜包括以下操作步骤：

- a) 工程名称输入；
- b) 采集节点选择；
- c) 节点信息核对；
- d) 提交创建。

6.3.2 工程与计划配置

工程管理模块应提供工程与计划配置功能，宜包括以下操作步骤：

- a) 节点通道选择；
- b) 计划信息核对：
 - 计划名，
 - 设备名，
 - 节点IP，
 - 开关动作，
 - 档位，
 - 触发方式；
- c) 提交保存。

6.4 录波操作

录波操作应按照以下步骤进行：

- a) 选择设备，点击设备开机按钮；
- b) 选择工程及录波工程任务；
- c) 点击开始录波按钮；
- d) 按需调节波形速度及偏移位置，设置档位则至少应设置4个档位（1个通道为4000个点，档位单位为ms）：
 - 1) 20档——160个点，
 - 2) 50档——400个点，
 - 3) 100档——800个点，
 - 4) 500档——2000个点；
- e) 结束录波；
- f) 按需上传、下载、删除波形数据。

6.4.1 录波数据应形成文件，存于缓存中。系统应提供手动上传、下载、删除波形数据的功能。

6.5 信息安全

系统建设与运行应遵守以下安全要求：

- 应符合 GB/T 20271、GB/T 20273 的安全技术要求；
- 信息安全级别应达到 GB/T 22239 第二级或以上的要求；
- 采用云计算系统架构时，系统安全服务能力应符合 GB/T 31168 的相关要求；

- 应建立系统身份认证机制，提供用户权限控制、系统应采取用户权限分级管理，角色职责与权限应清晰，各类用户必要时可采用实名认证；
- 应建立系统数据安全处理机制，数据的传输，处理和存储应建立全过程安全控制；制定针对如数据泄露等突发安全事件的应急预案；
- 应建立系统安全响应和反馈机制，及时受理安全性相关的提示、咨询和建议等；
- 应提供系统级安全控制，如登录时效性、连接数等控制；对程序资源的访问进行安全控制，如页面功能权限等；
- 应建立相应的信息安全运行体系，包括数据安全策略，如数据库安全、数据备份与恢复机制等，数据交换安全机制、应用安全策略保障、系统安全策略及网络安全策略等。

6.6 权限管理

6.6.1 应具备独立的权限管理，包括但不限于菜单管理、员工账号管理、角色权限三部分功能：

- 菜单管理：管理菜单的增删改查；
- 员工账号：增加删除账号、查询员工账号信息（账号角色、账号、账号名称、所属公司等）；
- 角色权限：可根据权限进行增加、编辑、修改、删除等维护和操作。可分别设置菜单、页面及模块权限权限。

6.6.2 宜设置至少一名系统管理员。

6.6.3 普通员工权限宜根据项目成员角色进行授予，角色分类及权限授予可参照以下内容。

- 项目管理员：
 - 查看设备状态；
 - 波形展示。
- 设备测试操作者：
 - 增加新设备、设备节点；
 - 录波、波形数据下载、上传。

7 系统交付

7.1 系统测试

7.1.1 测试要求

应根据系统架构、客户需要进行系统测试，系统测试的内容由单元测试、集成测试和验收测试三部分组成。其中单元测试和集成测试在项目组内部完成，验收测试则以用户为主，由系统开发人员和系统测试人员参加，共同完成。

7.1.2 测试类型

7.1.2.1 单元测试

应针对系统设计的最小单位（程序模块）进行正确性检验的测试，发现并排除各模块内部可能存在的各种差错。

7.1.2.2 集成测试

应查找发现系统中不符合总体设计的错误。在单元测试的基础上，将所有模块按照总体设计的要求组装成为系统，发现并排除模块组合中出现的问题。

7.1.2.3 验收测试

7.1.2.3.1 应测试系统的功能和性能是否满足需求分析报告、总体设计的要求。

7.1.2.3.2 应有用户参加设计测试用例，由用户输入测试数据，分析测试的结果。除功能和性能测试外，还应进行系统的可移植性、兼容性、可维护性、容错性等方面的测试。验收测试包括但不限于以下方面的测试：

- 功能测试：根据项目建设要求，参考本规范，对平台各应用系统的实际功能进行验证，测试通过后验收方应签署功能测试报告（通过）；

- 性能测试：采用行业内稳定、主流的测试软件，根据项目立项方案、需求变更说明书、技术方案等材料要求，参照本规范，对平台性能进行测试，测试通过后验收方应签署性能测试报告（通过）；
- 安全测试：由符合资质要求的测评机构，对系统进行二级信息安全等级保护测评。

7.1.3 测试方法步骤

测试方法步骤包括设计选择测试用例、运行被测程序、检测输出结果。为了测试不同的功能，选择测试用例应满足多方面的要求，并有一定的错误数据。在设计测试用例时，应考虑以下内容：

- 功能测试：应保证每个功能至少测试一次；
- 性能测试：记录每次测试的系统响应时间和结果输出时间；系统数据处理容量测试时，记录系统能否处理最大容量的数据，系统的处理时间、稳定性、系统资源消耗情况等；
- 稳定性测试：模拟系统可能运行的最长时间，不退出系统能否正常连续运行规定时间；
- 安全测试：模拟系统用户，测试可否执行超过用户权限的功能；
- 多用户共享测试：测试多个用户同时操作时，他们的操作是否产生冲突、矛盾。

7.1.4 测试结果分析

测试结束后，测试小组应对测试的各项指标进行分析，编制测试分析报告，作为系统评审和验收的依据。测试结果存在问题的，应根据测试结果进行改进、优化。

7.2 系统部署

7.2.1 应提供系统安装服务，安装后进行配置和调试。部署后应进行系统培训并提供操作手册。部署应考虑软件、硬件环境，以及系统的兼容性和稳定性。系统部署宜遵循以下步骤：

- a) 确定部署目标和环境；
- b) 确定部署策略和流程；
- c) 准备系统部署所需资源和工具；
- d) 系统部署和配置；
- e) 系统测试和验证；
- f) 系统优化和调整；
- g) 编写系统部署文档和操作手册；
- h) 进行系统备份和恢复测试；
- i) 进行系统培训和交付；
- j) 系统维护和更新。

7.3 运行维护

7.3.1 应建立系统运维方案，维护服务应包括以下内容（可与客户协商增加或修改）。

- 系统日常运行维护：
 - 系统操作指导；
 - 定期对软、硬件系统检查、维护和升级，保证系统持续、安全、可靠运行；
 - 保障数据的实时监测、质量控制和有效录波，并填写平台运行状况记录表，记录平台运行状况。
- 系统突发事件的诊断、排除：
 - 系统出现故障或漏洞而不能正常服务时，系统运维人员应对故障进行及时处理，使系统尽快恢复正常运行；
 - 服务器软硬件损坏、黑客攻击、病毒感染等原因导致系统服务系统出现故障致使停止服务时，应在2个工作日内恢复系统运作；
 - 系统出现的故障不能短时间恢复的，运维人员应及时上报，并按规定启动紧急预案，直至原系统恢复正常。
- 因客户发展需要或需求变动引发对系统的新增、完善部件功能且工作量小于（含）1人/天的开发工作，年累计不能超过30个工作日。
- 系统咨询服务。解答客户提出的系统相关的业务和技术问题，包括但不限于：

- 技术咨询;
 - 技术指导;
 - 信息提供。
- 数据库数据清理。应对系统文件定期整理、备份、存档，并根据情况对文件设置权限和保密等级，定期清理运维过程中所产生的无用数据。客户有保密需求的，则按照需求进行数据库清理。
- 运维总结。运维人员应定期撰写本期运维总结报告，总结本期运维工作开展情况，重点分析出现的技术问题，并给出整改方案。
- 7.3.2 维护形式分为被动式和主动式两种。
- 被动式服务。包括现场技术服务方式、远程维护方式：
- 现场技术服务方式：指因应用软件系统出现重大故障导致业务中止时，应及时派技术人员远程协助客户技术、业务人员一起对故障进行分析，提出解决方案，在征得客户同意后对故障进行处理和排除；
 - 远程维护方式：通过电话、电子邮件、传真或远程访问等方式进行系统故障的处理、技术支持、咨询服务等工作。
- 主动式服务。包括定期巡检、主动服务：
- 定期巡检：应安排人员按约定周期定期到系统部署现场对系统进行全面检查。优化系统，同时做好各类系统运行情况的记录。对可能出现的故障提出解决预案及系统功能改进等方面的技术咨询工作，并提供必要的现场指导。另外，可根据用户需求，在现场对其技术、业务人员进行系统运行管理、日常维护、使用操作及开发技术等方面的培训；
 - 主动服务：可定期将行业内一些先进的理念以书面形式发与用户。
-