

中华人民共和国电力行业标准

DL/T 578—95

水电厂计算机监控系统 基本技术条件

Specification of supervisory computer control system
for hydroelectric power plants

1995—07—13 发布

1995—12—01 实施

中华人民共和国电力工业部 发布

目 次

1 主题内容与适用范围	(3)
2 引用标准	(3)
3 术语	(3)
4 基本结构	(5)
5 系统功能和操作要求	(5)
6 硬件基本技术要求	(11)
7 软件基本技术要求	(18)
8 环境条件	(20)
9 系统特性	(22)
10 试验和检验	(24)
11 标志、包装、运输和储存	(25)
12 文件	(26)
附录 A	(28)

1 主题内容与适用范围

本标准规定了水电厂计算机监控系统的有关术语、基本结构、技术要求、试验和检验、包装和运输以及文件等内容。

本标准适用于大型水电厂计算机监控系统的设计、制造和运行管理，梯级水电厂和中型水电厂计算机监控系统亦应参照使用。

2 引用标准

GB2887	计算机场地技术要求
DL5003	电力系统调度自动化设计技术规程
DL5002	地区电网调度自动化设计技术规程
GB6162	静态继电器及保护装置的电器干扰试验
GB7450	电子设备雷击保护导则
GB3453	数据通信基本型控制规程
GB3454	数据终端（DTE）和数据电路终端设备（DCE）之间的接口定义
GB7260	不间断电源设备
DL476	电力系统实时数据通信应用层协议
JB/T5234	工业控制计算机系统验收大纲

3 术 语

- 3.0.1 电站级（或主控级）（Power Plant Level）：**指水电厂中央控制一级。
- 3.0.2 现地控制单元级（Local Control Unit）：**指水电厂被控设备按单元划分后在现地建立的控制级。
- 3.0.3 人机接口（Man—Machine Interface）：**指操作人员与计算机监控系统设备的联系。等同人机通信（MMI）或人机联系。
- 3.0.4 通信接口（Communication Interface）：**计算机与标准通信系统之间的接口。
- 3.0.5 局部网（Local Area Network）：**局部区域计算机网络的简称。
- 3.0.6 点设备（Point）：**输入输出接口设备。点的分类含义如下：
- （1）报警点（Alarm Point）：它用于输入能产生报警功能的信息。
 - （2）累加点（Accumulator Point）：它接收脉冲数字输入信号，累加到脉冲计数的总数中去。
 - （3）模拟点（Analog Point）：它输入模拟量完成模数转换。
 - （4）控制点（Control Point）：它输出实现控制功能的信息。
 - （5）指示（状态）点（Indication（Status） Point）：它接收作为指示功能的数字信号输入。
 - （6）事件顺序点（Sequence of Event Point）：它接收实现寄存事件顺序功能的数字信号输入。
 - （7）备用点（Spare Point）：指没有被使用但已经配好线和有设备的点。
 - （8）布线点（Wired Point）：这些点的公用设备、布线和空间位置均已提供，要使用这些点只需要加入硬插件。

(9) 空位点 (Space on Point)：机柜中留下的点设备空间位置，可供将来添加插件、设备、机箱和布线。

3.0.7 数字量 (Digital Quantity)：用编码脉冲或状态所代表的变量。

3.0.8 模拟量 (Analog Quantity)：连续变化量，它被数字化并用标量表示。

3.0.9 数据 (Data)：数字量或模拟量含义的数值表示。

3.0.10 比特率 (Bit Rate)：传送二进制位的速度。单位为每秒传送的位数。

3.0.11 波特 (Baud)：信号传输速度的一种单位。它等于每秒内离散状态或信号事件的个数。在每个信号事件表示一个二进制位的情况下，波特和每秒比特数一样；在异步传输中，波特是调制率的单位，它是单位间隔的倒数。若单位间隔的宽度是 20ms，则调制率是 50 波特。

3.0.12 信息 (Information)：根据数据表示形式中所用的约定赋予数据的意义。

3.0.13 报文 (Message)：用于传递信息的字符有序序列。

3.0.14 事件 (Event)：系统或设备状态的离散变化。

3.0.15 分辨率 (Resolution)：被测量可能被识别的最小值。

3.0.16 事件分辨率 (Event Resolution)：事件发生时间的可识别的最小值。

3.0.17 状态 (State)：指元件或部件所处的状态。例如，逻辑“0”或“1”。

3.0.18 状况 (Status)：描述一个点或一台设备或一个软件工作状况的信息。例如，点报警状态，点禁扫状态。

3.0.19 禁止 (Disable)：阻止某个特定事件处理的命令或条件。

3.0.20 允许 (Enable)：允许某个特定事件处理的命令或条件。

3.0.21 人工操作 (Manual Operation)：通过人机接口对被控设备进行操作。

3.0.22 响应时间 (Response Time)：从启动某一操作到得到结果之间的时间。

3.0.23 平均故障间隔时间 (Mean—Time—Between Failures)：工作设备的故障之间所能期望的间隔时间 (小时)。

3.0.24 平均维修时间 (Mean Time to Repair)：使故障设备恢复正常工作所能期望的时间 (小时)。

3.0.25 电磁相容性 (Electromagnetically Compatibility (EMC))：设备对外界电磁场容忍能力的一种量度。

3.0.26 电磁干扰 (Electromagnetic Interference (EMI))：从设备中辐射出的电磁场的一种量度。

3.0.27 有功功率联合控制 (Joint Control of Active Power)：在电厂内调整有功功率以如此方式进行，即让被控制的多台发电机组的行为同单台机组的行为一样。其发电机联合组成和执行控制规律是按照电厂控制任务特性来确定的。

3.0.28 无功功率联合控制 (Joint Control of Reactive Power)：在电厂内调整无功功率以如此方式进行，即让被控制的多台发电机组的行为同单台机组的行为一样。其发电机联合组成和执行控制规律是按照电厂控制任务特性来确定的。

3.0.29 厂内自动发电控制 (Automatic Generation Control)：水电站自动发电控制是电力系统自动发电控制一个子系统。它的任务是：在满足各项限制条件的前提下，以迅速、经济的方式控制整个电站的有功功率来满足系统的需要。

3.0.30 厂内自动电压控制 (Automatic Voltage Control)：水电站自动电压控制是电力系统自动电压控制一个子系统。它的任务是按厂内高压母线电压及全厂的无功功率进行优化实时控制，以满足电力系统的需要。

4 基本结构

4.1 开放、分布式计算机监控系统结构

按水电厂控制对象或系统功能分布设置多台计算机装置，它们连接到资源共享的网络上实现分布处理。

4.2 开放、分层分布式计算机监控系统结构

按水电厂控制层次和对象设置电站级和现地控制单元级：

- a. 电站级根据要求可以配置成单机、双机或多机系统；
- b. 现地单元控制级按被控对象（如水轮发电机组、开关站、公用设备、闸门等）由多台现地控制单元（LCU）装置组成；
- c. 电站级和现地控制单元级间一般采用星形网络或总线网络结构。

4.3 现地控制单元级结构

4.3.1 现地控制单元级可以选用下列设备装置：

- a. 工业控制微机；
- b. 高性能的可编程控制器；
- c. 工业控制微机加可编程控制器。

4.3.2 现地控制单元是实现水电厂计算机监控的关键设备，根据计算机监控系统实用要求，其结构配置可为：

- a. 双重化冗余结构；
- b. 局部双重化冗余结构；
- c. 多处理器非冗余与简化常规设备相结合的结构。

4.3.3 现地控制单元应能独立运行，具有现地监控手段。

5 系统功能和操作要求

5.1 数据采集

5.1.1 数据类型：

- a. 模拟量；
- b. 数字输入状态量；
- c. 数字输入脉冲量；
- d. 数字输入 BCD 码；
- e. 数字输入事件顺序量；
- f. 外部链路数据。

5.1.2 现地控制单地（级）数据采集：

- a. 应能自动（定时和随机）采集以上各类实时数据；

b. 事故及故障情况下，应能自动采集事故、故障发生时刻的各类数据。

5.1.3 电站控制单元（级）数据采集：

- a. 自动（定时和随机）采集各现地控制单元的各类实时数据。
- b. 自动接收各调度级的命令信息（任选项）。
- c. 自动接收电厂监控系统以外的数据信息（任选项）。

5.2 数据处理

数据处理应定义对每一设备和每种数据类型的数据处理能力和方式，以用于支持系统完成监测、控制和记录功能。

5.2.1 模拟量数据处理：

应包括模拟数据的滤波、数据合理性检查、工程单位变换、模拟数据变化及越限检测等，并根据规定产生报警和报告。

5.2.2 状态数据处理：

应包括防抖滤波、状态输入变化检测，并根据规定产生报警和报告。

5.2.3 事件顺序数据处理：

应记录各个重要事件的动作顺序、事件发生时间（年、月、日、时、分、秒、毫秒）、事件名称、事件性质，并根据规定产生报警和报告。

5.2.4 计算数据：

- a. 功率总加；
- b. 脉冲累积、电度量或分时电度量的累计；
- c. 主辅设备动作次数和运行时间等维护管理统计；
- d. 水量、耗水率、效率等计算（任选项）。

5.2.5 主要参数趋势分析处理（任选项）。

5.2.6 事故追忆处理（任选项）。

5.2.7 相关量处理（任选项）。

5.3 控制与调节

监控系统按照电厂当前运行控制方式和预定的决策参数进行控制调节，以满足电力调度发电控制要求。

5.3.1 对运行设备控制方式的设置：

- a. 远方调度端/电站（级）控制方式设置；
- b. 电站（级）/现地控制单元（级）控制方式设置；
- c. 机组单控/联合控制运行方式设置；
- d. 运行设备自动/手动控制方式设置。

5.3.2 对单台被控设备人工操作：

运行人员通过电站（级）或现地控制单元的操作屏（台）进行操作，完成对单台设备的控制与调节。

5.3.3 机组单元的控制调节：

机组单元在现地人工控制或电站（级）远方控制均应具有以下控制调节功能：

- a. 机组顺序控制；

- b. 机组转速及有功功率调节；
- c. 机组电压及无功功率调节。

5.3.4 厂内自动发电控制或有功功率联合控制的调节准则：

- a. 按系统调度给定的日负荷曲线调整功率；
- b. 按系统 AGC 定周期设定值自动调整功率（任选项）；
- c. 按运行人员给定总功率调整功率；
- d. 按水位控制方式；
- e. 按等功率、等开度或等微增率等优化方式进行有功功率的自动分配和调整。

5.3.5 厂内自动发电控制：

监控系统根据给定的电站功率，考虑调频和备用容量的需要，计算当前水头下电站最佳运行的机组数；根据电站供电的可靠性、设备（特别是水轮发电机组）的当前安全和经济状态，确定应运行机组台号；在应运行机组间实现负荷的经济分配；校核各项限制条件，如机组汽蚀振动区、下游最小流量、下游水位变化、用水量计算等，不满足时进行各种修正。

5.3.6 厂内自动电压控制或机组无功功率联合控制的调节准则：

- a. 按系统调度给定的电厂高压母线电压日调节曲线进行调整；
- b. 按运行人员给定的高压母线电压值进行调节；
- c. 按发电机出口母线电压给定值进行调节；
- d. 按等无功功率或等功率因数进行调节。

5.3.7 低频控制和高频控制（任选项）：

监控系统根据系统频率降低和升高的程度以及机组的运行方式，自动改变机组的运行方式以恢复系统的频率正常。

5.4 人机联系及操作要求

监控系统均通过以下接口设备完成画面显示、打印制表、设置参数及操作控制等人机联系功能。

- a. 电站级运行人员控制台；
- b. 现地操作台（屏）；
- c. 工程师/程序员工作台；
- d. 模拟屏。

5.4.1 电站级运行人员控制台基本功能及操作要求：

作为电厂运行人员监视和控制电厂运行的主要手段，运行人员与计算机监控系统的交互作用将通过运行人员控制台使用 CRT、汉字打印机、键盘或跟踪球等来实现。

5.4.1.1 人机联系原则：

- a. 运行人员控制台只允许完成对电厂设备运行监视、控制调节和参数设置等操作，而不允许修改或测试各种应用软件；
- b. 人机联系应有汉字显示和打印功能，汉字应符合国家一级汉字库标准；
- c. 人机联系操作方法应简便、灵活、可靠，对话提示说明应清楚准确，在整个系统对话运用中保持一致；
- d. 有关控制操作的人机联系，应充分利用具有被控对象显示画面、键盘（或跟踪球等）及画面对话区提示三者相结合的方式；操作过程中应有必要的可靠性校核及闭锁功能；

- e. 画面调用方式应满足灵活可靠、响应速度快的原则；
- f. 应给不同职责的运行管理人员提供不同安全等级操作权限。

5.4.1.2 CRT 功能：

- a. 画面显示；
- b. 画面实时刷新（包括设备状态、运行参数及实时时钟的刷新）；
- c. 报警与操作信息报告显示；
- d. 人机对话提示以及操作命令出错信息提示；
- e. 光标显示与控制（应能通过键盘或跟踪球等进行控制）；
- f. 画面窗口变换与局部放大；
- g. 画面的平移与滚动。

5.4.1.3 画面显示：

运行人员通过键盘或跟踪球选择和召唤画面显示。画面内容应精炼、清晰、直观，以便于监视和改善动态特性。可以显示的主要画面包括：

- a. 各类菜单（或索引表）显示；
- b. 电厂电气结线图；
- c. 机组及其风、水、油等主要辅助设备状态模拟图；
- d. 机组运行状态转换顺序流程图；
- e. 各类棒图；
- f. 各类曲线图；
- g. 各类记录报告；
- h. 各类运行报表；
- i. 操作票及操作指导（任选项）；
- j. 事故处理指导（任选项）；
- k. 计算机系统设备运行状态图；
- l. 各类维护管理报表。

5.4.1.4 屏幕显示画面的编排：

- a. 时间显示区；
- b. 画面静态及动态信息主显示区；
- c. 报警信息显示区；
- d. 人机对话显示区。

5.4.1.5 画面图符及显示颜色定义：

- a. 电气结线图中各电气设备图符应符合《水利水电工程制图标准》；
- b. 电气结线图中各电压等级颜色应符合 NDGJ8—89 有关规定；
- c. 电气结线图中机组、断路器、隔离开关、接地开关图符动态刷新颜色定义；
 - 机组发电状态：红色；
 - 机组调相状态：蓝色；
 - 机组停机备用状态：黄色；
 - 机组停机检修状态：白色；
 - 机组水泵状态：粉红色；
 - 断路器、隔离开关、接地开关合闸状态：红色；

断路器、隔离开关、接地开关分闸状态：绿色；

d. 报警与操作信息显示颜色定义：

报警事故信息：红色；

故障信息：黄色；

复归信息：白色；

操作信息：绿色；

e. 参数刷新颜色定义：

参数正常：绿色；

参数越限：红色（或闪光）（越上上限或下下限）；

黄色（越上限或下限）。

5.4.1.6 键盘操作与控制：

运行人员通过键盘或跟踪球进行选择画面和屏幕管理操作之外，主要是完成 5.3 条款中的操作控制任务。功能设计上应采取下述措施：

a. 充分利用人机联系方式、采用键盘（专用键或动态键）和画面对话区显示一致控制的原则，以保障操作安全可靠；

b. 操作前，首先调用有关控制对象的画面，进行对象选择，在画面上，所选择的被控对象应有显示反映及选择无误的提示，运行人员确认选择的目标后，方可执行有关操作；

c. 被控对象的选择和控制只能在同一个控制台上进行；

d. 控制操作步骤应尽可能少，但应有必要复核检查。

5.4.1.7 各种参数的设置（或修改）：

运行人员在控制台上应能方便准确地设置或修改运行方式、负荷给定值及运行参数限值等等。

5.4.1.8 报警处理：

a. 当对象达到事故和故障状态，应立即发出报警音响和显示信息。报警音响应将事故和故障区别开来。声音可手动或自动解除。

b. 报警显示信息应在当前画面上显示报警语句（包括报警发生时间、对象名称、性质等）。显示颜色应随报警信息类别而改变。若当前画面具有该报警对象，则该对象标志（或参数）闪光及其颜色变化。闪光信号应在运行人员确认后方可解除。

c. 对于确认的误报警，运行人员可以退出该报警点。

5.4.1.9 命令无效处理与删除：

a. 任何人机联系请求无效时应显示出错信息；

b. 任何操作命令进行到某一步时，如不进行下一步操作（在执行之前）则应能自动删除或人工删除。

5.4.1.10 制表打印与记录：

a. 各类操作记录；

b. 各类事故及故障记录；

c. 报表打印；

d. 曲线打印（任选项）；

e. 趋势记录（任选项）；

f. 事故追忆及相关量记录（任选项）；

- g. 各种典型操作票（任选项）；
- h. 画面拷贝（任选项）。

上述记录报表应能自动（定时、随机）或由运行人员在控制台上选择和控制打印机打印。

5.4.2 现地操作屏（台）基本功能：

- 5.4.2.1 运行人员应能在现地通过操作屏（台）上的功能按钮或 CRT 键盘选择测量或控制。
- 5.4.2.2 操作屏（台）应具有远方（电站级）和现地控制方式的切换功能，在现地方式进行控制操作时，远方命令不起作用，但不影响数据采集和传送到电站（级）。
- 5.4.2.3 各种整定值和限值的设置或修改。
- 5.4.2.4 功能按钮或键盘的操作应作到安全、可靠和简便。

5.4.3 工程师/程序员工作台基本功能：

- a. 系统生成和启动；
- b. 系统管理维护和故障诊断；
- c. 应用软件的开发和修改，以及数据库修改、图形显示和报告格式的生成。

5.4.4 模拟屏（任选项）。

5.5 电厂设备运行管理及指导

- a. 历史数据存储；
- b. 自动统计机组工况转换次数及运行、备用、检修时间累计；
- c. 被控设备操作动作次数累计以及事故动作次数累计；
- d. 峰谷负荷时的发电量分时累计；
- e. 运行参数及经济指标等计算（任选项）；
- f. 操作指导（任选项）；
- g. 事故处理指导（任选项）。

5.6 系统通信

5.6.1 监控系统与各调度级的调度自动化系统间的通信：

为满足调度自动化系统对电厂的遥测、遥信、遥调及遥控功能，监控系统应可随时接受各级调度的命令信息，并向它们发送电厂实时工况、运行参数及有关信息。

5.6.2 监控系统与电厂其它计算机系统之间的通信：

- a. 与水情自动化测报系统的通信（任选项）；
- b. 与厂内办公室管理系统的通信（任选项）。

5.6.3 监控系统内电站级与现地控制单元的通信：

- a. 数据采集；
- b. 传送操作控制命令；
- c. 通信诊断。

5.6.4 时钟同步控制：

监控系统（电站级和现地控制单元级）的时钟同总调度自动化系统的时钟应能进行同步控制。

5.7 系统自诊断及自恢复

监控系统在线运行时，应对本系统内的硬件及软件进行自诊断，自诊断内容包括以下几类：

- 5.7.1 计算机内存自检。
- 5.7.2 硬件及其接口自检，包括外围设备、通信接口、各种功能模件等。当诊断出故障时，应自动发出信号；对于冗余设备，应自动切换到备用设备。
- 5.7.3 自恢复功能包括软件及硬件的监控定时器（看门狗）功能。
- 5.7.4 掉电保护。
- 5.7.5 双机系统故障检测及自动切换。

5.8 培训仿真

监控系统内可配置培训仿真台，在离线时，用以仿真电厂实际运行，培训运行操作人员进行各种操作及维护（任选项）。

监控系统内也可不专门配制培训仿真台，可利用工程师工作台对运行人员进行简单的操作培训。

6 硬件基本技术要求

6.1 设备分类

本系统设备按布置可划分为两大类：电站（级）设备和现地控制单元（级）设备；
本系统设备按通用组件可划分为三大类：计算机设备及外部设备、接口设备和电源设备。

6.2 计算机和存贮器

用于本系统的计算机应是适合实时控制，能满足系统功能和性能要求的机型。

6.2.1 电站级计算机：

6.2.1.1 电站级配置计算机（或处理器）应具备如下技术性能：

- a. CPU 字长： ≥ 32 位（含准 32 位）；
- b. 时钟频率： $\geq 16\text{MHz}$ ；
- c. 浮点处理：硬件。

6.2.1.2 计算机内的主存贮器应有足够的容量，存贮容量分配中应留有 40% 以上的余量。

6.2.2 是站级计算机系统的辅助存贮器：

6.2.2.1 支持实时控制系统工作的辅助存贮器以温盘机为宜。应有足够存贮能力，以支持实时控制系统的资源文件、应用文件和历史数据（包括日、月、年累加信息量）的存贮管理工作。最低容量应大于 80MB。

6.2.2.2 支持管理工作的辅助存贮器可配置温盘机或小型磁带机。

6.2.3 现地控制单元级计算机（处理机、存贮器）：

6.2.3.1 对工业控制微机类型的技术性能要求：

- a. 处理器字长： ≥ 16 位；
- b. 时钟频率： $\geq 8\text{MHz}$ ；

- c. 存储器容量： $\geq 512\text{kB}$ ；
 - d. 硬件中断： ≥ 8 级；
 - e. 具有硬件 WATCHDOG；
 - f. 机内总线标准化；
 - g. 具有局部网通信接口；
 - h. 具有现地终端接口（含 CRT、打印机）或面板接口；
 - i. 能实现时钟同步校正，其精度应与事件分辨率配合。
- 6.2.3.2 对可编程控制器类型的基本性能要求：
- a. 扫查率： $\leq 5\text{ms/K}$ ；
 - b. 存储容量： $\geq 16\text{kB}$ ；
 - c. 具有较强功能的指令系统；
 - d. 具有局部网通信接口；
 - e. 允许接入 DI/O 和 AI/O 点的容量应大于实际可能使用容量，且留有足够贮备；
 - f. 当有 SOE 点时，应能实现时钟同步校正，其精度应与事件分辨率配合。

6.3 数据和控制接口

数据和控制接口为本系统设备中与被监控设备进行电气连接的部件。

6.3.1 模拟信号输入接口：

6.3.1.1 模拟信号接口回路宜采用差分连接，输入直流放大器应具有足够电压的电气隔离。

6.3.1.2 多路模拟信号输入共用模数转换电路时宜采用悬浮电容双端切换技术。

6.3.1.3 用于温度测量的模拟输入接口应能直接或经变送器与电阻温度探测器（RTD）连接。

6.3.1.4 对模拟输入接口宜提供模数变换精度自动检验或校正。

6.3.1.5 模拟输入接口参数：

- a. 信号范围：
电流型 $4\sim 20\text{mA}$ ；
电压型 $\pm 5\text{V}$ 、 $0\sim 5\text{V}$ 、 $0\sim 10\text{V}$ ；
- b. 输入阻抗：
电流型 $\leq 250\Omega$ 或 $\leq 500\Omega$ ；
电压型 $\geq 5\text{k}\Omega$ ；
- c. 模数转换分辨率： 12 位（可含符号位）；
- d. 最大转换误差（ 25°C 时）： $\pm 0.25\%$ （从变送器取信号，包括失调、标度变换以及 6 个月周期以上的检验误差）；

注：当直接从电流互感器（CT）、电压互感器（PT）、RTD 取信号时为 $\pm 0.5\%$ 。

- e. 最大温度误差： $\pm 0.01\%/^\circ\text{C}$ （正常输入信号范围 2mA 的百分比）；
- f. 共模电压： 200V DC 或 AC 峰值；
- g. 共模抑制比（CMRR）：
 $\geq 80\text{dB}$ （直流到交流 50Hz ；测试信号从端子加入）；
 $\geq 90\text{dB}$ （直流到交流 50Hz ）；
- h. 常模抑制（NMRR）： $\geq 60\text{dB}$ （交流 50Hz ）。

6.3.2 数字信号输入接口：

6.3.2.1 数字信号输入宜采用空（干）接点，且输入回路应由独立电源供电。

6.3.2.2 数字信号输入接口一般采用光电隔离和浪涌吸收回路。

- 6.3.2.3 每一数字输入端口宜有发光二极管(LED)显示其状态。
- 6.3.2.4 数字输入接口参数：
- a. 信号范围：电压：12V DC、24V DC、48V DC；
电流： $\leq 10\text{mA}$ ；
 - b. 最小变态检测时间：2ms；
 - c. 最大变态检测时间：30ms；
 - d. 接点电阻： $< 100\Omega$ (包括电缆芯线)；
 - e. 在工作电压条件下接点泄漏电阻： $> 50\text{k}\Omega$ (包括电缆芯线)。
- 6.3.3 模拟信号输出接口：
- 6.3.3.1 模拟信号输出接口回路宜采用差分连接。
- 6.3.3.2 模拟输出接口参数：
- a. 信号范围：电流型 4~20mA；
电压型 0~10V；
 - b. 负载阻抗：电流型 $\leq 500\Omega$ ；
电压型 $\geq 500\Omega$ ；
 - c. 最大转换误差： $\pm 0.25\%$ 、 $\pm 0.5\%$ ；
 - d. 数模转换分辨率：12位(含符号位)、10位(含符号位)；
 - e. 转换时间： $\leq 0.15\text{s}$ 、 $\leq 0.55\text{s}$ ；
 - f. 共模电压：200V DC 或 AC 50Hz。
- 6.3.4 数字信号输出接口：
- 6.3.4.1 数字信号输出接口应采用光电隔离或继电器隔离。
- 6.3.4.2 数字信号输出回路应由独立电源供电。
- 6.3.4.3 每一路数字输出宜有LED显示其状态。
- 6.3.4.4 数字输出接口参数：
- a. 信号电压范围：电子式 0~30V DC；
接点式 220V DC、110V DC、48V DC、24V DC、220V/380V AC；
 - b. 信号电流范围：电子式 0~50mA；
接点式 1A、2A、5A；
 - c. 信号持续时间：可控和锁存；
 - d. 接点开断容量：感性负载 30W；
 - e. 继电器固有动作时间范围：吸合 2~30ms、释放 10~30ms。
- 6.3.5 脉冲累加信号输入接口：
- 6.3.5.1 脉冲累加信号输入宜采用空接点或OC门，且输入回路应采用光电隔离。
- 6.3.5.2 每一脉冲累加信号输入应有独立的计数器。
- 6.3.5.3 脉冲累加信号输入接口参数：
- a. 信号电压：5V DC、12V DC、24V DC；
 - b. 信号电流： $\geq 10\text{mA}$ ；
 - c. 最小变态检测时间：30ms、50ms。

6.4 通信接口

6.4.1 本系统与调度系统的通信接口：

6.4.1.1 本系统通信接口带调制解调器或外加数据通信设备后，应能与微波设备、电力载波设备、光缆设备或专用通道连接。

6.4.1.2 系统通信接口应能满足调度要求的通信方式：

- a. 异步串行半双工通信；
- b. 异步串行全双工通信；
- c. 同步串行半双工通信；
- d. 同步串行全双工通信。

6.4.1.3 通信接口设备所包括的通信适配器或通信控制器以及连接器或调制解调器彼此应适应于统一的规程特性和参数。

6.4.1.4 本系统应配备接受卫星、无线电台或电网自动化系统的校正同步时钟精度的设备。

6.4.1.5 通信接口设备与外部调制解调器（在数据通信设备中）连接时的特性要求：

- a. 接口信号电气特性应符合所采用规程的接口标准；
- b. 信号重复率：符合调度要求；
- c. 信号质量和噪声极限应符合美国电子工业协会标准 RS—334（串行数据传输的数据处理终端设备与同步数据通信设备接口处信号质量）或 RS—363、RS—404（数据终端设备与非同步数据通信设备间的起止信号的质量标准）标准。

6.4.1.6 通信接口设备包含调制解调器的特性要求：

- a. 信号阻抗：当信号速率需要标准音频级通道时，全部输入和输出应采用平衡的 $600\Omega \pm 10\%$ 阻抗；
- b. 信号电平：输入（接收）电平的范可低到 -30dB （基准值 1mW ）；输出（发送）电平不得超过 0dB （基准值 1mW ），输出电平和接收灵敏度按最多 4dB 档调整；
- c. 信号稳定性：全部输入和输出应稳定在 $\pm 1\text{dB}$ 内；
- d. 信号线性：输出（发送）信号的线性是指在容许的频率和电平范围内应不超过 $\pm 1\text{dB}$ ，输入信号的线性和延迟失真按通道类型和数据速率的要求分别规定；
- e. 信号失真：当信号速率需要标准音频通道时，全部输入和输出所包含的均方根谐波成份在 0dB 时不超过 2% ；
- f. 信号载波：应满足调度系统规定的中心频率和带宽。

6.4.1.7 调制解调器与外部通道连接宜采用变压器隔离，耐压 15kV 直流或峰—峰交流。

6.4.2 电站级与现地控制单元级间，或主控制级多机间的通信接口：

6.4.2.1 当本系统为分布控制系统结构时，其相互间的通信连接宜按局域网来考虑，而且应尽可能选择适合于工业控制的局域网。局域网结构，通信规程，信息格式，数据传输速率，传输介质和传输距离等除应考虑下述款项一般要求外，还应满足系统功能和性能的有关要求。

6.4.2.2 通信接口应采用光电隔离或变压器隔离，其隔离电压等级应大于器件上可能出现的最大地电位差和 6.8.3 条规定的浪涌（或传导干扰）抑制能力（SWC）的允许值。

6.4.2.3 点对点星形网通信接口：

- a. 通信方式：异步或同步串行数据传输；
- b. 接口标准：符合美国电子工业协会标准 RS—422—A（非平衡电压数字接口电路的电气特

性)、RS-232-C (采用串行二进制数据交换的数据终端设备与数据通信设备之间的接口) (带调制解调器) (单端);

符合美国电子工业协会标准 RS-423-A (平衡电压数字接口电路的电气特性)、RS-485 (差分)、20mA 电流环;

- c. 传输速率: $\geq 1200\text{bps}$;
- d. 传输距离: 使用电缆时一般不应大于 1km;
- e. 传输介质: 聚乙烯绝缘对绞铜带绕包屏蔽电缆或光缆。

6.4.2.4 总线网接口:

- a. 通信方式: 令牌 (标记) 传输或竞争式 (广播、点对点);
- b. 接口标准: IEEE802.4 或 IEEE802.3 (数据通信中局域网的一种标准);
- c. 传输速率: 10Mbps (以太网);
- d. 传输距离: 500m (可加中继器延长);
- e. 传输介质: 50 Ω 或 75 Ω 同轴电缆 (或光缆);
- f. 结点数: 1024。

6.5 人机接口

人机通信接口设备应为运行操作员和程序员提供人机通信手段, 它应包括电站级运行人员控制台、模拟屏、工程师/编程员工作台和现地操作台 (屏) 等设备。

6.5.1 对电站级运行人员控制台的要求:

6.5.1.1 对显示器的要求:

- a. 显示器屏幕尺寸不小于 51cm (19");
- b. 分辨率不低于 640 \times 400;
- c. 显示颜色: 8 种以上;
- d. 显示器场频: 50Hz \pm 0.2%;
- e. 图象闪烁、晃动和失真应限制在不易察觉的程度内。

6.5.1.2 对键盘的要求:

a. 操作键盘应由功能键和数字 (或含字母) 键组成, 所使用的按钮应具有良好的机械性能和电气性能, 文字标记要美观清晰;

b. 控制台上显示器光标控制应优先采用鼠标器或跟踪球, 跟踪球转动应与光标移动成比例;

c. 操作键盘的键定义及数量根据需要确定。

6.5.1.3 对打印机的要求:

- a. 打字速度: 最少 120 字符/s;
- b. 字符: ASCII 码、国标一级汉字库 (自带);
- c. 缓冲存贮容量: $\geq 7\text{kB}$;
- d. 打印行长: 80 个字符、132 (136) 个字符。

6.5.1.4 对控制台的要求:

a. 彩色显示器布置不得有碍操作人员对模拟屏的监视;

b. 彩色显示器方位、角度、距离应给操作人员最佳监视效果, 显示器应有遮除眩光的措施;

- c. 操作键盘应布置在合适的高度，和显示器方位应该一致；
- d. 当有常规监视和控制器件布置在同一控制台上时，宜考虑分区布置并加以协调；
- e. 控制台上应有一定的平面给操作人员搁置文件；
- f. 控制台上的人机接口设备及电缆连接应能方便地拆卸更换；
- g. 必要时，控制台上应能布置调度电话。

6.5.2 对模拟屏接口的基本要求：

6.5.2.1 当模拟屏信号由计算机监控系统提供时，选择模拟屏的对外接口类型应综合考虑计算机监控系统的接口能力。

6.5.2.2 对自带驱控设备的模拟屏，本系统应提供合适的通信接口设备。

6.5.2.3 对不带驱控设备的模拟屏，本系统提供的驱控器组件中数字输出和模拟输出接口应与模拟屏信号参数匹配。

6.5.3 工程师/程序员工作台一般包括终端设备（或工作站）以及打印机等设备。

6.5.4 现地控制单元级的人机接口设备可配置便携式工作站、固定式工作站（或终端设备）、或屏面操作板等型式中之一种。

6.6 电源

6.6.1 本系统设备用不间断电源（UPS）、稳压电源等应在下列外电源电压范围内正常工作和不遭损坏：

厂内交流电源： 220/380V±10%单相或三相 50Hz±2%；

厂内蓄电池直流电源： 176~253V（220V 额定值）；

88~127V（110V 额定值）；

42~58V（48V 额定值）；

21~29V（24V 额定值）。

6.6.2 在外电源内阻小于 0.1Ω 时，由本系统设备所产生的电噪声（1~100kHz）在电源输入端上的峰—峰值电压应小于外部电源电压的 1.5%。

6.6.3 当输入电压下降到下限以下或正负极性颠倒时，本系统设备不应遭到破坏。

6.6.4 本系统电站级应配置不间断电源，现地控制单元级宜配置不间断电源或由厂内直流蓄电池供电的逆变电源。

6.6.5 不间断电源（或逆变电源）除满足 GB7260 有关规定外还要满足下列具体要求：

- a. 额定容量：按 1.5~2 倍正常负载容量考虑；
- b. 输入电压：满足 6.6.1 条的要求；
- c. 输出电压：AC220V±2%；
- d. 输出电压波形：正弦波 50Hz±1%；
- e. 波形失真：<5%；
- f. 电压超调量：<10%额定电压（当负载突变 50%时）；
- g. 不间断电源备用电池维持时间：20min 或 30min。

6.6.6 系统内部直流稳压电源应有过压过流保护及电源故障报警信号。电源配置应满足接口隔离要求。

6.6.7 本系统设备的电源输入回路应有隔离变压器和抑制噪声的滤波器。

6.7 机柜

6.7.1 本系统设备所用机柜应适合水电厂使用环境。机柜的电磁屏蔽特性应保证本系统能正常工作和不影响电厂其它设备的正常工作。放于现场的机柜应有屏蔽、防尘、通风和防潮设施，以便适应现场环境。

6.7.2 机柜的结构尺寸，开门位置，密封和冷却，端子排或接线盒的型式及布置，电线引入位置，内部布线和连接，油漆和颜色以及外壳安装等应满足用户要求。

6.8 一般电气特性

6.8.1 绝缘电阻：

6.8.1.1 交流回路外部端子对地的绝缘电阻应不小于 $10M\Omega$ 。

6.8.1.2 不接地直流回路对地的绝缘电阻应不小于 $1M\Omega$ 。

6.8.2 介电强度：

6.8.2.1 500V 以下，60V 及以上端子与外壳间应能承受交流 2000V 电压 1min。

6.8.2.2 60V 以下端子与外壳间应能承受交流 500V 电压 1min。

6.8.3 浪涌（或传导干扰）抑制能力（SWC）：

6.8.3.1 本系统所有电源设备、数据和控制接口设备、通信接口设备的 SWC 应使用如下技术标准：

a. 1~1.5MHz 衰减振荡： 1级 0.5kV；

2级 1kV；

3级 2.5kV；

b. 1.2/50 μ s 冲击波： 1级 1kV；

2级 3kV；

3级 5kV。

6.8.3.2 大型水电厂的计算机监控系统接口设备的 SWC 应满足 2 级或 3 级要求。

6.8.4 无线电干扰（RI）：

6.8.4.1 本系统中无线电干扰采用如下技术标准：

30~500MHz： 1级 1V/m；

2级 3V/m；

3级 10V/m。

6.8.4.2 对本系统设备的电磁干扰（Electromagnetic Interference—EMI）和电磁兼容性（Electromagnetic Compatibility—EMC）分别采用的射频干扰（Radio Interference）等级应按其工作环境提出。一般情况下可采用 1 级。

6.8.5 静电干扰（Electro—Static Discharge）：

6.8.5.1 本系统中采用如下 ESD 标准：

ESD 150pF—150 Ω ： 1级 2kV；

2级 4kV；

3级 8kV。

6.8.5.2 本系统设备应按所采用元件类型选择 ESD 标准进行设计和测试处理。

6.9 接地

6.9.1 本系统接地应该使用水电厂公用接地网接地。

6.9.2 为了避免产生接地环流或地噪声干扰，同时为了设备的安全防护，本系统设备的外壳、交流电源、逻辑回路、信号回路和电缆屏蔽层必须按如下原则接地：

- a. 设备外壳或裸露的非载流的金属部分必须接地；
- b. 经过隔离的交流电源电压超过 150V 时必须接地；
- c. 未隔离的所有计算机直流电路（包括直流电源、逻辑回路、信号回路）中一般只应有一个接地点；
- d. 未隔离的所有计算机直流电路中共地回路如有两点或多点接地时，其任意两接地地点的地电位差在任何时候均不能大于设备所允许的噪声；
- e. 任一机柜（或一套装置）内全部对外接口设备有隔离时，机柜外壳、交流电源、计算机直流电路和电缆屏蔽层可在该机柜内共一点接地；计算机逻辑回路在机柜内应只有一个点同机柜的公共接地点连接；
- f. 在一个设备中，或在邻近设备中的接地不应有两个独立的接地网；
- g. 信号和电缆屏蔽层的接地应考虑相应传感器或其它连接设备的接地点，避免两点接地，并且应尽可能选择本系统接收设备端一点接地。

6.9.3 本系统所属设备柜内接地连线应尽量短，柜内的公共接地板应采用截面大于 35mm^2 的铜条。

6.9.4 机柜或箱壳的接地点必须有良好耐久的金属接触点接地。

6.9.5 本系统所属设备使用测试仪器时，该设备应为测试仪器提供电源连接和接地连接。

7 软件基本技术要求

7.1 操作系统

7.1.1 提供的操作系统应是实时多重任务执行程序系统、交互式分时操作系统或多道程序通用目标虚拟存贮器系统。

7.1.2 操作系统应满足如下要求：

- a. 操作系统在所提供的硬件构造中应有实用成功的经验；
- b. 对计算机设备制造单位支持的实时操作系统不宜进行修改，对其未使用部分可进行删节；
- c. 为提高计算机利用率和响应时间，操作系统应具有以优先权为基础的任务调度执行，资源管理分配以及任务间通信和控制手段，优先级至少有 32 级；
- d. 应具有输入输出设备的直接控制能力；
- e. 应能有效地执行高级语言程序；
- f. 能执行诊断检查，故障自动切除；
- g. 对系统的启动、终止、监视、组态和其它联机活动应有交互式语言和命令程序支持；
- h. 应通过任务名称、数据名称和操作标号实现软件相互连接；
- i. 为系统生成提供服务。

现地控制单元级的操作系统应根据实际应用环境对上述要求进行简化。

7.2 支持程序和实用程序

7.2.1 系统服务软件中应该配备成熟适用的支持程序和实用程序。

7.2.2 应提供的支持程序和实用程序及其特性要求如下：

a. 具备有效的编译软件，以进行应用软件的开发。这些编译软件包括标准的汇编语言编译程序、高级语言编译程序、交互式数据库编译程序、交互式图象编译程序、交互式报告编译程序等；

b. 具有容易使用和代码汇编的连接装配程序；

c. 具有对应用软件进行检验和修改的实用程序；

d. 具有存贮器转贮的实用程序。

7.3 数据库

集中式或分布式数据库应能满足如下要求：

a. 数据库的结构定义应包括电厂监控和管理所需要的全部数据项；

b. 支持快速存取和实时处理；

c. 能控制数据的完整性和统一性；

d. 能在线设定或修改数据；

e. 有专门软件支持数据库建立和修改；

f. 能对模拟输入量进行测量死区、零读数死区、报警死区和越限检查处理；

g. 能对模拟输入量进行工程单位变换处理；

h. 为改善实时数据处理能力，在实时数据库中采用报警允许或控制闭锁等相关数据计算项。

7.4 数据采集软件

7.4.1 数据采集软件应配合数据库提供检测和处理电厂监控和管理所需数据的能力。

7.4.2 数据采集软件应能满足如下要求：

a. 按周期方式和请求方式实现电站设备的实时数据采集；

b. 对需要计算的实时数据进行实时处理；

c. 对当前产生的报警和控制点进行计算处理；

d. 对各种限制值的点进行校核处理；

e. 对状态点变化进行监视处理；

f. 对实时数据异常点进行监视处理；

g. 对外部链路数据实现采集和处理；

h. 按周期方式或请求方式实现规定的的数据输出；

i. 数据采集和处理速度应满足实时性要求。

7.5 人机接口软件

7.5.1 人机接口软件的设计应满足系统功能设计要求。

7.5.2 人机接口软件应使用户能按使用手册增加或修改显示画面、报表和系统配置。

7.6 通信软件

用于本系统的通信软件应尽可能采用开放系统互连（Open Systems Interconnection—OSI）协议或适于工业控制的标准协议。

7.6.1 局域网络通信规约：

a. 星形网络宜采用高级数据通信控制步骤（Advanced Data Communication Control Procedure—ADCCP）、同步数据链路控制（Synchronous Data Line Control—SDLC）、高级数据链路控制规程（High Level Data Link Control Procedures—HDLC）、分组性公用数据网（X.25）、二进制（二元）同步通信（Binary Synchronous Communications—BISYNC）等主要型式的数据链路层协议，或采用TTY、循环数字传送（CDT）等通信规约；

b. 竞争式总线网宜采用 IEEE802.2 和 IEEE802.3 标准协议；

c. 令牌总线网络宜采用 IEEE802.4 标准协议。

7.6.2 电站级计算机与调度级计算机间所采用的远程通信协议应该服从调度端的要求。

7.6.3 在通信协议规定的数据块传送结构中，报文类型定义宜按报警点数据、事件顺序记录点数据、状态点数据、模拟点数据、脉冲累加点数据、控制及校核数据等划分。

7.6.4 通信软件应能监视通信通道故障，并进行故障切除（停止通信）和报警。

7.6.5 局域网通信交换数据量及其频度应满足功能要求和特性要求。

7.7 诊断软件

为了提高系统可利用率和可维修性，应该配置完备的诊断软件。

7.7.1 周期在线诊断软件：

a. 对电站级计算机及外围设备应提供周期在线诊断软件；

b. 对现地控制单元级处理器及接口设备应提供周期在线诊断软件；

c. 对通信网络及接口设备应提供周期在线诊断软件；

d. 在线诊断发现的故障信息应有报警显示和记录。

7.7.2 在系统在线运行及人机对话控制下，对系统中某一外围设备能使用请求在线诊断软件进行测试检查。

7.7.3 应提供离线诊断软件或工具，对系统中的计算机设备或组件进行查找故障的诊断。

7.8 应用软件

7.8.1 监控系统应提供用于完成第5章所述功能的应用软件。

7.8.2 应用软件应采用结构式模块化软件，功能软件模块或任务模块应具有一定的完整性和独立性。

7.8.3 应用软件环境的设计应使用户能安全地实现应用软件的补充、修改或移植。

8 环境条件

8.1 气候环境

8.1.1 环境温度：

- a. 电站级计算机房：
 - 夏季 $23\pm 2^{\circ}\text{C}$
 - 冬季 $20\pm 2^{\circ}\text{C}$
 - b. 现地控制单元： $0\sim 40^{\circ}\text{C}$ ；
 - c. 允许温度变化率： $5^{\circ}\text{C}/\text{h}$ 。
- 8.1.2 相对湿度：
- a. 电站级计算机房： $45\%\sim 65\%$ ；
 - b. 现地控制单元： $20\%\sim 90\%$ （无凝结）。
- 8.1.3 尘埃：
- 8.1.3.1 本系统设备应根据不同的使用场地考虑防尘措施，一般应采用密闭机柜和带过滤器的通风孔。
- 8.1.3.2 设备安装场地的尘埃应尽可能减少，特别是在初期施工中应采取临时保护措施。
- 8.1.3.3 设备使用场地尘埃参数的参考值如下：
- a. 电站级计算机房：尘埃粒度大于 0.5μ 的个数小于 3500 粒/L；
 - b. 现地控制单元：尘埃粒度大于 0.5μ 的个数小于 18000 粒/L。
- 8.1.4 海拔高度不大于 2500m。
- ## 8.2 振动和冲击
- a. 电站级计算机房：振动频率在 $5\sim 200\text{Hz}$ 范围内，加速度不大于 $5\text{m}/\text{s}^2$ ；
 - b. 现地控制单元：振动频率在 $10\sim 500\text{Hz}$ 范围内，加速度不大于 $10\text{m}/\text{s}^2$ 。
- ## 8.3 地震
- 本系统设备用于地震多发地区时，设备的结构应有相应的特殊考虑。
- ## 8.4 防雷防护
- 如有遭受雷电侵入损坏设备的可能时，应在通道进入设备机柜的端口加装防雷保护元件，如气隙放电管、压敏电阻或两者的组合。气隙放电管击穿电压约 300V 并能抑制约 5kA 脉冲电流。压敏电阻击穿电压约 250V 并能抑制约 5kA 脉冲电流。
- ## 8.5 噪声限制
- 8.5.1 本系统设备的噪声应控制在不造成人员伤害、疲劳或干扰通话的程度内。
 - 8.5.2 本系统设备发出的噪声，在中央控制台处测量应小于 60dB。
 - 8.5.3 设备在正常工作时，距离设备 1m 处所产生的噪声应小于 70dB。
- ## 8.6 电磁干扰（EMI）和电磁相容性（EMC）
- 8.6.1 电磁干扰极限应满足在离设备机壳 1m 处测量其电磁辐射不超过 6.8 条规定的数值。为了限制电磁场辐射量，设备制造单位应采用衰减技术，如隔离、屏蔽、接地、密封和滤波等措施。
- 8.6.2 电磁相容性极限应满足本系统设备当其所处环境的无线电干扰不超过 6.8 条中所取的某一等级时能正常工作。当安装环境的辐射超过了设备允许的电磁相容性极限时，则应改善安装环境，使设备安装处的辐射场在允许限值内，或者由制造单位采取特殊措施提高设备的电磁相容

性极限值，以适应特殊环境的要求。

8.6.3 对磁场极敏感的设备，应贮存在限制了磁通密度的环境中，磁带和磁盘装置的典型贮存极限在 $50 \times 10^{-4} \sim 70 \times 10^{-4} \text{T}$ 范围内，显示器放置处磁通密度不大于 $1 \times 10^{-4} \text{T}$ 范围内。

9 系统特性

9.1 实时性

9.1.1 现地控制单元级装置的响应能力应该满足对于生产过程的数据采集时间或控制命令执行时间的要求。

9.1.1.1 数据采集时间分类如下：

- a. 状态和报警点采集周期：1s 或 2s；
- b. 模拟点采集周期：电量 1s 或 2s；
非电量 1~30s；
- c. 事件顺序记录点 (SOE) 分辨率：
 - 1 级： $\leq 20\text{ms}$ ；
 - 2 级： $\leq 10\text{ms}$ ；
 - 3 级： $\leq 5\text{ms}$ 。

9.1.1.2 现地控制单元级装置接受控制命令到开始执行的时间应小于 1s。

9.1.1.3 供事件顺序记录使用的时钟同步精度应高于所要求的事件分辨率。

9.1.2 电站级的响应能力应该满足系统数据采集、人机接口、控制功能和系统通信的时间要求。

9.1.2.1 电站级数据采集时间包括单元级数据采集时间和相应数据再采入电站级数据库的时间，后者应不超过 1~2s。

9.1.2.2 人机接口响应时间分类如下：

- a. 调用新画面的响应时间：
 - 半图形显示： $\leq 2\text{s}$ (90%画面)；
 - 全图形显示： $\leq 3\text{s}$ (90%画面)；
- b. 在已显示画面上实时数据刷新时间从数据库刷新后算起不超过 1~2s；
- c. 操作员执行命令发出到控制单元回答显示的时间不超过 1~3s；
- d. 报警或事件产生到画面字符显示和发出音响的时间不得超过 2s。

9.1.2.3 电站级控制功能的响应时间分类如下：

- a. 有功功率联合控制任务执行周期可取 3~15s；
- b. 无功功率联合控制任务执行周期可取 6s、12s、3min；
- c. 自动经济运行功能处理周期时间可取 5~15min。

9.1.2.4 电站级对调度系统数据采集和控制的响应时间应满足调度的要求。

9.1.2.5 双机切换时间：

- a. 热备用时：保证实时任务不中断；
- b. 温备用时： $\leq 30\text{s}$ ；
- c. 冷备用时： $\leq 5\text{min}$ 。

9.2 可靠性

9.2.1 系统中任何设备的单个元件故障不应造成关键性故障（或使外部设备误动作）。

9.2.2 要防止设备或组件中的多个元件或串联元件同时发生故障。

9.2.3 本系统设备的 MTBF 应满足如下要求：

主控计算机（含磁盘） >8000h；

现地控制单元装置 >16000h。

9.3 可维修性

9.3.1 可维修性参数平均修复时间（MTTR）由制造单位提供，当不包括管理辅助时间和运送时间时，一般可取 0.5~1h。

9.3.2 可维修性的基本要求：

- a. 设备应具有自诊断和寻找故障程序，按照现场可更换部件水平来确定故障位置；
- b. 应有便于试验和隔离故障的断开点；
- c. 应配置合适的专用安装拆卸工具；
- d. 互换件或不可互换件应有措施保证识别；
- e. 预防性维修应使磨损性故障尽量减少；
- f. 应提高硬件的代换能力。

9.4 可用性（或可利用率）

9.4.1 本系统在电厂验收的可用性指标分为 99.9%、99.7%和 99.5%三档，其计算方法见附录 A。

9.4.2 对不同的系统结构或类型应采用不同的可用性指标。

9.5 系统安全

9.5.1 对操作安全性的基本要求：

- a. 对系统每一功能和操作提供校核；
- b. 当操作有误时能自动或手动地被禁止并报警；
- c. 自动或手动操作可作存贮记录或作提示指导；
- d. 根据需要在人机通信中设操作员控制权口令；
- e. 按控制层次实现操作闭锁，其优先权顺序为：现地控制单元级最高，电站级第二，远方调度级第三。

9.5.2 对通信安全性的基本要求：

- a. 系统设计应保证信息中的一个信息量错误不会导致系统关键性故障（使外部设备误动作，或造成系统主要功能的故障或系统作业的故障等）；
- b. 本系统与调度系统的远程通信的信息出错控制应与通信规约一致；
- c. 电站级和现地控制单元级装置的通信包括控制信息时，应该对响应有效信息或没有响应有效信息有明确肯定的指示。当通信尝试失败时，发送站应能自动重新发出该信息，直到超过重发计数（一般为 2~3 次）为止。当个别通道超过重发极限时，应发出适宜的警报；
- d. 为证实通道正常，应该定期地通过测试信息检查或通过正常使用进行校核；

e. 本系统内部通信的信息错误码检测能力及编码效率应有较高的指标。

9.5.3 对硬件、软件和固件设计安全的基本要求：

- a. 应有电源故障保护和自动重新启动；
- b. 能预置初始状态和重新预置；
- c. 有自检能力，检出故障时能自动报警；
- d. 设备故障自动切换或切除并能报警；
- e. 系统中任何地方单个元件的故障不应造成生产设备误动；
- f. 硬软件中相关的标号（如地址）必须统一；
- g. CPU 负载应留有适当的裕度，在重载情况下，其最大负载率不宜超过 70%；
- h. 磁盘的使用时间应尽可能低，正常情况下，在任一个 5min 周期内，其平均使用率应低于 50%；
- i. 系统设计或系统性能应考虑到重载和紧急临界情况。

9.6 可扩展性

9.6.1 为了确定和实现系统的扩充，制造单位应给出系统可扩充性的限制，其主要限制包括如下：

- a. 电站级或现地控制单元级装置点容量或存储器容量的极限；
- b. 使用有关例行程序、地址、标志或缓冲器的极限；
- c. 数据速率极限；
- d. 增添部件时，接口修改或部件重新定位等设计和运行的限制。

9.6.2 对系统扩充的基本要求：

- a. 根据需要预留一定数量的备用点、布线点和空位点设备；
- b. 电站级计算机存储器容量应有 40% 以上的余度；
- c. 应留有扩充现地控制装置、外围设备或系统通信的接口；
- d. 通道容量应留有足够余度，期望的通道利用率宜小于 50%。

9.7 可变性

对电站级和现地控制单元级装置中点设备的参数或结构配置应容易实现改变。对点的可变性要求：

- a. 点说明的改变；
- b. 模拟点工程单位标度改变；
- c. 模拟点限值改变；
- d. 模拟点限制值死区改变；
- e. 控制点时间参数改变。

10 试验和检验

10.1 试验和检验阶段

本系统所使用的设备和部件应是通过了型式试验的合格产品；在设备生产和安装各个阶段

应该分别进行规定的试验和检验；最后的系统验收阶段分别为：

- a. 出厂试验和检验，这一试验阶段是在制造单位厂家完成设备出厂前的型式试验和预验收试验后，由制造单位和用户共同进行的系统设备出厂试验；
- b. 现场试验和检验，现场试验和检验是在设备到现场之后，由用户和制造单位厂家共同进行的安装投运的试验和检验；
- c. 可用性检验，当用户要求在现场实行这项检验时，其最终验收可于本系统设备投运时间满一年后进行。

10.2 试验和检验项目（内容）

出厂试验和现场试验阶段的试验和检验项目不需要全部重复。出厂试验项目应尽可能全面完整，包括有完整仿真的控制和调整试验，工厂试验能够替代现场试验的项目，在现场试验阶段可以考虑减免。

某些试验项目，如温度、湿度、耐冲击电压能力、抗干扰能力、满载或过载等，一般可能已在别的阶段或其它同样设备上进行，根据试验记录的完整性和真实性，在出厂试验和现场试验可能免除。当用户要求进行这些项目的试验时，应在有关文件中明确规定。

10.2.1 硬件设备试验和检验项目：

- a. 试验和检验文件的检查；
- b. 质量保证措施及检验报告的检查；
- c. 试验和检验记录和缺陷处理记录的检查；
- d. 设备工艺质量检查；
- e. 设备配置检查；
- f. 一般电气性能试验；
- g. 定义的功能和性能试验。

10.2.2 软件功能试验和检验项目：

- a. 试验和检验文件的检查；
- b. 设计文件、操作手册和维护手册的检查；
- c. 预验收记录和缺陷处理记录的检查；
- d. 数据库软件测试；
- e. 数据采集软件测试；
- f. 人机接口软件测试；
- g. 应用软件测试；
- h. 通信软件测试；
- i. 诊断软件测试；
- j. 系统性能测试；
- k. 系统维护测试。

11 标志、包装、运输和储存

11.1 标志

本系统的每个独立装置的产品标志应符合国家标准相应的有关规定。除此之外，为了安全和识别的需要，本系统设备以及主要组件还应该加上下列合适的标志。

11.1.1 每台设备都应加上识别的标志，以便与说明文件对照。识别标志在整个系统中应该一致，其可为色码、标签、部件号等。识别标志应牢固地固定在它所确定的部件上。

11.1.2 为了使用安全需要注意和特别说明的地方，应该使用警告标志或安全指示。

11.2 包装

11.2.1 产品应有内包装和外包装。装箱应有防潮、防霉、防振、防辐射等措施。

11.2.2 包装箱上应清楚地标注产品名称、型号和重量等。

11.2.3 包装箱内应附有产品合格证、装箱清单以及文件资料。

11.3 运输

制造单位应指明设备适用的运输工具和运输时的要求。

11.4 储存

11.4.1 包装好的设备应储存在环境温度为 $-25\sim 55^{\circ}\text{C}$ ，湿度不大于85%，无腐蚀性和爆炸性气体的室内。

11.4.2 制造单位应指明设备储存期限及超过规定期限后应采取的措施。

12 文件

12.1 一般要求

12.1.1 制造单位为本系统设备提供的文件应包括五个基本部分：设计文件、安装文件、操作文件、维护文件和试验文件。

12.1.2 制造单位提出的文件内容应详尽、完整、统一，文图工整清晰，印刷装订美观。

12.1.3 制造单位执行用户要求的初步设计和出厂验收文件应经用户审批。

12.1.4 制造单位所提供的全部最终文件要反映设备验收时的真实情况。设备投运后的全部更改应该由用户进行文件修订记录。用户修订记录应尽量完整，以便满足第9章中性能质量的检验。

12.2 设计文件

由制造单位提供的设计文件是制造单位根据用户的设计文件、技术规范书或招标书，进行系统设备制造所编制的图纸和说明书。它们应该包括：

- a. 硬件系统框图（或配置图）及设备清单；

- b. 模件原理图；
- c. 机柜的设备布置图及布线图；
- d. 软件系统结构设计文件；
- e. 系统软件和应用软件清单；
- f. 操作系统、支持程序、实用程序、数据库、数据采集软件、人机接口软件及通信软件使用说明；
- g. 应用软件流程图（顺控）、源程序及说明；
- h. 全部外购设备所附文件。

12.3 安装文件

- a. 端子图及内部连接图；
- b. 设备安装开孔和固定连接图；
- c. 设备接地连接图；
- d. 安装说明书。

12.4 操作文件

制造单位应为运行操作员编制使用本系统设备的操作说明书。

12.5 维护文件

制造单位应为程序员编制维护文件，包括下列内容：

- a. 正常维护说明书；
- b. 故障检查及修复说明书。

12.6 试验文件

制造单位应提供系统设备在工厂和现场各试验阶段的文件。

附录 A

考核系统可用性的计算表达式为：

$$A = \frac{\text{可使用时间(h)}}{\text{可使用时间(h)} + \text{维修停机时间(h)}} \%$$

式中 A——可用性；

可使用时间=考核（试验）时间（h）—维修停机时间（h）。

考核（试验）时间，本系统设备在现场正确可靠地工作达到规定的试运期后，即可开始进入可用性试验的考核时间，如采用有关运行和维护记录数据计算可用性，其考核时间宜取 8760h；如采用专门的试验，考核时间可选为 400h。

关于维修停机时间的定义：

- a. 维修停机时间应包括故障维护时间、影响设备使用的预防性维修时间和扩充停机时间；
- b. 故障维修时间仅计算检查故障和处理故障设备使其恢复正常运行时间，它不包括通知和安排维修人员时间，也不包括等待备件和修理工具的时间。但对于重复性故障，其故障维修时间应取故障发生到处理结束的全部连续时间；
- c. 维修停机时间中所含现地控制单元的故障维修时间应按所有现地控制单元故障维修时间总和除以现地控制单元总个数的商进行计算；
- d. 可不计入故障维修时间的设备故障有：非关键性故障（不影响监控运行或不需要停机维修的故障）、冗余部件中不影响功能的故障；
- e. 维修停机时间应按规定的考核时间范围进行统计。

附加说明：

本标准由电力工业部标准化技术委员会提出。

本标准由电力工业部水电站自动化设备标准化技术委员会归口。

本标准主编单位：水利部长江水利委员会设计局

中国水利水电科学研究院自动化研究所

本标准主要起草人：胡家驹 陈美林 苏开佛 高光华 柳宇强

本标准校阅人：叶钟黎 顾景芳