目 次

1 总则 1
2 术语 2
3 基本规定 4
4 总体设计 5
5 信息基础设施 6
5.1 信息交换与采集 6
5.2 通信网络 6
5.3 计算资源 7
5.4 存储资源 7
6 数据资源建设及应用 9
6.1 数据资源建设 9
6.2 数据应用 10
7 应用支撑 11
7.1 基础应用支撑 11
7.2 算法模型 11
7.3 三维仿真引擎 11
7.4 知识库与知识引擎 13
8 业务应用系统 14
8.1 工程通用要求 14
8.2 水库枢纽工程 15
8.3 调水工程 17
8.4 水（船）闸工程 17
8.5 泵站工程 18
8.6 灌溉工程 19
8.7 河湖工程 20
8.8 蓄（滞）洪区工程 21
8.9 圩区工程 22
9 实体运行环境 23
9.1 一般要求 23
9.2 集控（总调）中心 23
9.3 数据中心 23
9.4 会商室及会议系统 23
10 信息资源共享 25
10.1 共享对象 25
10.2 数据共享 25
10.3 资源共享 25
10.4 共享方式 26
11 网络安全 27
11.1 保护对象和等级 27
11.2 安全物理环境 27
11.3 安全通信网络 27

11.4 安全区域边界 28
11.5 安全计算环境 28
11.6 安全管理平台 29
11.7 安全扩展要求 29
12 系统集成与运维 30
12.1 系统集成 30
12.2 运行维护 30
附录 A 工程信息系统典型逻辑架构图 31
A.0.1 工程信息系统在工程里的定位 31
A.0.2 工程信息系统典型逻辑架构图 31
标准用词说明 32
条文说明 33

1 总则

1.0.1 为明确水利水电工程信息系统设计要求，做到安全、可靠、实用、先进、高效的水利信息化建设，制定本标准。

1.0.2 本标准适用于水利水电工程的信息系统设计。

1.0.3 本标准引用下列标准：

GB/T 2887	计算机场地通用规范
GB/T 22239	信息安全技术 网络安全等级保护基本要求
GB/T 22240	信息安全技术 网络安全等级保护定级指南
GB/T 36340	防静电活动地板通用规范
GB/T 39204	信息安全技术 关键信息基础设施安全保护要求
GB/T 39786	信息安全技术 信息系统密码应用基本要求
GB 50174	数据中心设计规范
GB 50872	水电工程设计防火规范
SL 715	水利信息系统运行维护规范
SL/T 803	水利网络安全保护技术规范

1.0.4 水利水电工程信息系统设计应符合本标准外，尚应符合国家现行有关标准的规定。

2 术语

2.0.1 工业控制系统 industrial control system

工业生产中使用的控制系统，包括数据采集与监视控制系统（SCADA）、分散控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC）。

2.0.2 网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

2.0.3 数据安全 data security

数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。数据安全包括数据的可用性、完整性和保密性。

2.0.4 云计算平台 cloud computing platform

云计算平台也称为云平台，是指计算、存储、网络等基础设施和其上服务软件资源的集合。

2.0.5 自主可控 autonomous and controllable

自主可控是指依靠自身研发设计，全面掌握产品核心技术，实现信息系统从硬件到软件的自主研发、生产、升级、维护的全程可控，实现核心技术、关键零部件、各类软件，不受制于人。自主可控是保障网络安全、信息安全的前提。

2.0.6 数据仓库 data warehouse

数据仓库，是为决策制定过程提供所有类型数据支持的战略集合。它是单个数据存储，出于分析和决策支持目的而创建。

2.0.7 数据归档 data archiving

数据存档是一个数据管理流程，可以将很少被访问的、不活跃的、但仍有价值的业务数据迁移出生产环境长期保存，并提供查询和迁回这些数据的能力。

2.0.8 数据挖掘 data mining

数据挖掘是指从大量的数据中通过算法发现隐藏于其中信息的过程。

2.0.9 数据治理 data governance

数据资源及其应用过程中相关管控活动、绩效和风险管理的集合。

2.0.10 数字签名 digital signature

采用非对称密钥加密技术对数据的摘要（定长字符串）进行加密，用以验证数据的完整

性和来源，达到保护数据和抗抵赖的目的。

2.0.11 缩略语

下列缩略语适用于本文件。

BIM：建筑信息模型（Building Information Modeling）

GIS：地理信息系统（Geographic Information System）

API：应用程序接口（Application Programming Interface）

SDH：同步数字体系（Synchronous Digital Hierarchy）

AR：增强现实（Augmented Reality）

LPWAN：低功率广域网络（Low-Power Wide-Area Network）

IaaS：基础设施即服务（Infrastructure as a Service）

3 基本规定

3.0.1 水利水电工程信息系统设计应以提升水旱灾害防御能力、加强水资源节约集约利用和生态环境保护、保障工程安全高效建设和运行为目标。

3.0.2 应按照“需求牵引、应用至上、数字赋能、提升能力”的要求，结合工程实际需求和工程所在流域数字孪生建设情况，确定工程信息系统建设的技术路线。

3.0.3 水利水电工程信息系统设计方案应与工程的调度运用方式、监视和控制对象数量等相匹配。关系到系统功能和性能的重要技术方案，应通过技术经济比选确定。

3.0.4 水利水电工程信息系统设计方案应满足工程业务功能、系统性能、网络安全防护的需求，也应满足系统未来合理的扩展需要。

3.0.5 当采用数字孪生工程技术路线建设工程信息系统时，建设方案应兼顾工程运管单位的运维能力，系统应易于使用和迭代升级。

3.0.6 信息系统的“预报、预警、预演、预案”功能应与工程业务结合，并根据各业务系统实际需求进行设计。

3.0.7 工程信息系统应在网络安全、数据安全的前提下，对工程各类自动化系统的数据、软件功能、硬件资源进行集成整合，并优先使用工程已建私有云平台、工程所在地统一建设的水利云平台或政务云平台提供的计算、存储、网络等资源服务。

3.0.8 工程信息系统应为行业内的数据共享提供便利条件，数据共享过程应遵循数据分类分级和数据安全防护要求。

3.0.9 工程信息系统宜通过水利专业模型或人工智能算法实现工程自主分析、辅助决策和优化控制。在准确、及时的预报和预警基础上，通过数字空间下的多工况预演，指导工程调度预案的制定。

3.0.10 工程信息系统的建设不应以增加工程运行维护负担为代价，且不应将系统建成为单纯的线上展示系统。

3.0.11 工程信息系统建设内容应以用户常用功能为主，偶尔或长周期重复使用（如每年或多年 1 次）的功能，宜优先采用购买服务的方式。

3.0.12 工程信息系统应与工程主体同时设计、同时建设、同时投运，水利水电工程应配置具备相应技术能力的系统运行维护人员，人员数量应与工程管理设计相衔接。

4 总体设计

4.0.1 水利水电工程信息系统设计范围一般可界定为除现地端工业控制系统外的生产系统、管理信息系统及其运行环境设施的设计，如附图 A.0.1。

4.0.2 工程信息系统典型逻辑架构一般可分为七层，如附图 A.0.2，分别为实体工程层、信息采集层、网络通信层、计算存储层、数据资源层、应用支撑层、业务应用层和系统展示层。

4.0.3 应结合工程建设期、运行期的业务特点进行工程信息系统总体设计。可分别对建设期和运行期提出架构解决方案，也可将其作为连续的整体系统提出一个全生命期的架构解决方案。

4.0.4 应通过技术经济比选，选定符合工程建设和运行过程中各方面需求的系统开发技术路线，推荐采用安全自主可控的技术和产品。

4.0.5 宜对照系统建设需求，通过统一建模语言，从多个角度对系统功能以及构成系统的各个组件的逻辑关系进行设计说明。

4.0.6 应结合工程建设管理单位在工程建设和运行维护阶段的职责，分析建设管理、监视控制、调度决策、运行维护等核心业务流程，提出信息系统主要功能。

4.0.7 工程信息系统设计应统筹存量资源和增量需求，充分整合利用已建信息基础设施、数据资源和应用系统。

5 信息基础设施

5.1 信息交换与采集

5.1.1 工程信息系统应采用开放体系结构，便于系统或平台之间的数据交换和交互操作。

5.1.2 应根据工程建设和运行管理业务应用的需求采集所需数据。数据来源包括自动化采集设备、人工录入以及外系统接入。

5.1.3 工程信息系统所需外部数据如水文数据、气象数据、水环境数据、视频数据、三维空间、墒情数据等宜优先采用与流域、区域等外部系统交换方式获取。

5.1.4 工程内部的监测数据应通过集成计算机监控系统、设备状态在线监测系统、视频监视系统、水文测报系统、安全监测系统、水环境监测系统等获取。

5.1.5 应根据数据的应用方式，确定交换和采集的数据格式、频次，以及传输通道是否加密。

5.1.6 分布分散且远离电网电源的各类监测设施宜选用低功耗、无线通信的自动化设备，有条件的地区对小容量用电设施推荐采用光伏或风光互补供电装置供电。

5.1.7 对接工程内部各系统的接口程序开发、无线接收平台开发、数据的检查检验及存储入库等工作应视为数据采集工作。对于已有历史监测数据的工程项目，数据采集工作还可包括历史数据的数字化、清洗及存储入库等。

5.1.8 对接工程外部系统的接口程序开发工作应视为数据交换工作，包括对侧数据的读取、检查检验以及本侧存储入库的环节。

5.2 通信网络

5.2.1 通信网络设计包括通信传输网络设计和计算机网络设计。

5.2.2 监测信息的通信接入方式宜采用有线接入为主，实施确实困难时可采用无线通信方式。当采用北斗卫星短消息方式接入时，通信设备注册、报文格式以及报文加密方式等应经水利行业主管部门审批。

5.2.3 系统中实时性要求较高的下行控制命令，宜通过有线方式传送，经技术确认网络通信时延满足要求时，也可采用公网无线通信网络。

5.2.4 骨干通信网络拓扑结构应安全可靠、便于管理，在发生单一故障时应具备自愈能力，网络切换时间应满足业务运行要求。

5.2.5 承载实时控制业务的通信传输网络应具备通信路由和通信设备的 1+1 保护能力。

5.2.6 计算机网络应采用分层、分区结构，网络核心节点应进行高可用设计。

5.2.7 应分网络、分业务估算工程未来 5 年的网络业务承载能力，并据此选定网络设备。

5.2.8 根据通信传输距离、业务容量，通信骨干网络可采用基于 SDH 的光传输方式或光纤以太网组网方式，当工程运行期的通信业务有较大增长量时，可采用基于波分复用的光传输方式。

5.2.9 通信传输网络应充分利用公共通信资源。经技术经济比选采用长距离光缆时，宜设置光缆线路在线监测系统，实时监测光缆运行状态、快速准确定位故障。

5.2.10 长距离通信光缆敷设宜充分利用工程设施，可利用的设施包括长距离输水隧洞、输水管道或者专用架空输电线路等。

5.2.11 当通信站点设置储能供电装置作为备用电源时，储能装置供电时间应根据主电源可靠性和运维人员抵达现场维修的时间综合确定，备用供电时间不少于 4 小时。

5.2.12 通信传输和计算机网络应配套建设网络管理系统。

5.3 计算资源

5.3.1 宜基于系统的信息访问量、业务并发量以及业务应用本身对算力资源需求、算力冗余需求和经济等因素，估算各类服务器数量，并选定处理器、内存等核心器件的技术指标。

5.3.2 工业控制系统中的业务应用宜部署在物理服务器或物理服务器集群中。

5.3.3 应通过技术经济比选，选定信息系统的计算资源形式，并参考以下要求：

1 对于小型水利工程，系统中的监测、事务管理等应用可在工程本地部署，也可基于区域集中部署。

2 对于大、中型水利工程，应综合考虑应用系统部署规模、系统负载、系统时效、运维人员技术能力等因素，系统计算资源宜采用本地物理机或本地虚拟化平台部署。

3 当有政务云平台或水利行业云平台可供使用时，工程中的分析、模拟、事务管理等应用，宜优先基于属地政务云或行业云平台部署。

4 应根据工程的业务和硬件资源扩展需求，综合经济因素，选择硬件解耦的计算设备、超融合设备或云计算服务。

5.3.4 应配置相应工具对计算资源进行运行监视和调度管理。

5.4 存储资源

5.4.1 综合考虑系统数据量、读写性能、数据安全、运维人员技术能力等因素，通过技术经济比选，选定存储系统架构及数据存储设备。

5.4.2 综合考虑系统建设初期数据量、年度数据增量情况、数据安全、备份数据等因素，估算系统数据存储容量。新建系统存储容量至少满足工程运行 5 年的业务数据量。

5.4.3 应确定系统数据备份及恢复方式。对于大型及重要中型水利工程，宜提出容灾备份方案。

5.4.4 应根据工程的业务和硬件资源扩展需求，综合经济因素，选择硬件解耦的存储设备、超融合设备或云存储服务。

5.4.5 应配置相应工具对存储资源进行运行监视和调度管理。

6 数据资源建设及应用

6.1 数据资源建设

6.1.1 应根据业务架构，建立工程业务数据库，并根据业务系统的实时性、重要性以及数据的保密性、完整性、可用性需求，进行相应的高可用和加密存储设计。

6.1.2 应建立工程基本特征属性的基础信息数据库，工程基础信息数据应对行业主管部门共享。

6.1.3 应建设工程数据仓库，运用数据分析技术对业务数据进行分析、挖掘，辅助支撑业务系统运行和决策。

6.1.4 应建立数据归档机制，对超出 5 年的调度、运行数据进行归档。

6.1.5 建筑物信息模型（BIM）数据宜按以下要求建设：

1 主体工程建构筑物，安全监测设施设备，机电辅助设备及管路、桥架，清污机、启闭机、桥机、门机等金属结构设施设备，工程区地质构造和地层结构，模型精细度等级不低于 LOD2.0。

2 水库泄水建筑物主要结构，水轮发电机组、水泵电动机组、变压器、机组进水阀等主要机电设备，拦污栅、闸门等主要金属结构设施设备，威胁人员和建筑物安全的边坡或滑坡体，影响主体工程安全的坝区地质构造和地层结构，模型精细度等级不低于 LOD3.0。

3 不参与空间分析及三维仿真分析的工程附属建筑物、建筑物附属结构、防护边坡、厂区、景观等，可以适当精度的三维实景模型替代 BIM 模型。

6.1.6 三维地理空间模型数据宜按以下要求建设：

1 对工程的管理范围和工程影响范围创建对应 L3 级的数字正射影像模型、数字高程模型和水下地形。

2 枢纽工程影响范围一般是指工程到防洪保护对象之间的河段；当下游有紧邻水库工程时，下游影响范围为工程到下游水库库尾之间河段。大型枢纽工程下游影响范围特别大的，可在满足分析计算精度要求的前提下适当降低建模精度。

3 水下地形精度应满足水动力模型分析和泥沙淤积分析计算需求；蓄滞洪区内长期有水的湖泊、河道可不建设水下地形模型。

4 地下工程对应的地表三维空间模型应采用共享（免费）资源。

6.1.7 工程三维实景模型数据宜按以下要求建设：

1 地面建筑物、厂区等可通过倾斜摄影、激光点云等方式建立实景模型，与三维地理

空间模型进行平滑拼接。

2　线性工程如河道和湖泊的堤防，输水渠道和管道应建立 BIM 模型，不宜建设三维实景模型。

6.1.8　应建设工程建筑信息模型、三维地理空间模型和三维实景模型数据的更新、维护等工具软件。

6.1.9　工程中的地理信息数据应不涉及国家秘密，或采用经国家认定的地理信息保密处理技术脱密后使用。在工程中公开使用经保密技术处理的地理信息，应依法进行地图审核。

6.2 数据应用

6.2.1　应结合业务需求，梳理工程数据资源应用方案，开展数据资源应用设计。

6.2.2　宜建设数据资源目录，并对工程数据进行分类、分级管理。

6.2.3　数据应用包括数据挖掘、数据服务、数据共享等内容，也可包括数据汇聚、数据治理等数据应用前的准备工作。

6.2.4　宜结合数据应用方案，选定或开发用于数据汇聚、数据治理、数据分析、数据挖掘、数据可视化、数据共享的软件工具，相应软件工具的功能应灵活、操作应便捷。

6.2.5　数据共享服务宜采用网络应用程序接口（Web API）方式。

7 应用支撑

7.1 基础应用支撑

7.1.1 应用支撑平台中的组件应采用跨平台技术进行开发，便于各类系统的集成、复用、互操作和迁移。

7.1.2 宜在控制网和管理信息网分别设置统一认证和鉴权服务。

7.1.3 工程信息系统应建立数字签名服务，采用数字签名技术为调度指令、应急预案等关键调度控制信息提供完整性验证和身份验证服务。

7.1.4 系统应建立实现业务数据可视化和格式文本生成的报表与图形服务组件。

7.1.5 宜采用中间件技术为系统的消息传递、数据集成、应用互操作和应用的负载均衡等提供服务。

7.2 算法模型

7.2.1 算法模型一般包括基于水利专业知识的算法模型和基于机器学习的智能算法模型。需要单独开发图像、视频或音频识别算法的，也可包括图像、视频与音频的智能识别模型。

7.2.2 用于图像、视频、音频等的智能识别模型，若属于定型产品已嵌入设备中的，应在设备选型设计时确定其功能及参数。

7.2.3 应根据工程特点和业务应用需求建设算法模型，并明确算法模型的建设原则、模型应用范围、边界条件、精度要求、参数率定方案，需要三维仿真的还应确定算法与三维仿真引擎的交互要求。

7.2.4 根据工程布局和调用运用需求，可建设工程全局多目标水量优化调度模型、梯级水电厂/梯级泵站（群）优化调度模型、工程联合调度模型。

7.2.5 应建立工程安全监测分析评价和预测模型、主要机电和金属结构设备的状态分析评价和预测模型。

7.2.6 系统应能在工程试运行期间，提供足够用于机器学习算法训练和验证的数据，且系统应具备对算法模型持续训练的功能。

7.2.7 工程核心业务已配置专业模型的，若搭建智能算法模型，需与专业模型功能形成互补或提供辅助支撑。非核心业务已配置专业模型的，可不再建立对应功能的智能模型。

7.3 三维仿真引擎

7.3.1 按照数字孪生工程技术路线建设的信息系统，应建设三维仿真引擎。

7.3.2 三维仿真引擎主要功能应包括根据工程数据（状态量或状态量时间序列），即时对水体、建筑物、机电及金属结构设备等三维模型构建的虚拟场景进行渲染和仿真模拟。

7.3.3 三维仿真引擎性能应满足对工程现实物理状态的即时响应要求。

7.3.4 应根据已监测数据、计算成果和推理分析成果对以下水体状态进行即时渲染模拟：

1 水库、水池、渠道、渡槽、隧洞、调压井（室）、船闸闸室里的水位和水体流动方向。

2 河流、湖泊、蓄滞洪区的水位、流动方向及淹没范围。

3 有压管道或有压隧洞里的水体压力和流动方向。

4 当有水体污染溯源任务时，可对污染物扩散过程进行渲染仿真。

7.3.5 应根据已监测数据、计算成果和推理分析成果对下列建筑物和设备的状态进行即时渲染模拟：

1 建筑物安全监测状态。

2 发电机组、水泵机组、变压器、高压配电装置、开关柜、控制柜、柴油发电机组、封闭母线、气体绝缘封闭母线（GIL）的非电量参数及告警状态。

3 水闸、船闸及其启闭机工作状态；输水、供水主回路的阀门工作状态。

4 油、气、水系统核心设备的工作状态；安装有流量、压力变送器的主管道流体状态。

5 通风空调设备工作状态、照明系统工作状态、火灾报警及消防设备工作状态。

6 视频监视画面与三维模型的融合渲染。

7.3.6 对人员和设备位置渲染应按以下要求设计：

1 根据可穿戴设备等的定位信息即时定位显示现场当值运维人员、施工作业人员位置；也可通过实时的巡更打卡信息显示当值人员在巡查巡检工作过程中的移动轨迹。

2 对无人机、无人船、无人潜航器、机器人、大型施工机械等重要可移动设备进行定位和追踪。

3 非当值工作人员不进行定位和轨迹追踪。

7.3.7 在工程的三维虚拟空间中应实现距离、面积、体积等的空间分析功能。

7.3.8 三维仿真引擎应能实现大场景三维模型和与工程三维模型的无缝集成，实现不同分辨率、不同大小数据的自动融合、投影变换以及数据裁切，制作任意分辨率真实质感三维场景。

7.3.9 三维仿真引擎应能实现三维地图服务的加载、三维场景漫游、图层管理、视点功能、标注标绘、空间测量，以及属性查询和空间查询等功能。

7.4 知识库与知识引擎

7.4.1 工程信息系统宜按以下要求建设预案库及预案管理工具：

1 预案库一般包括工程防汛和抗旱应急预案、工程调度预案、应急抢险工作预案等。

2 应提供预案管理工具，具备对各预案动态管理的能力。

3 宜实现与预警信息联动推送预案的功能。

7.4.2 工程信息系统宜按以下要求建设规则库及规则管理工具：

1 规则库可包括工程调度规则、工程建筑物安全评价规则（标准）、设备状态评价规则（标准）等。

2 提供规则管理工具，对规则库各项规则动态管理。

3 规则库对所有规则的触发事件进行记录，用于历史事件查询匹配。

7.4.3 应建设支撑工程安全、运行维护、故障诊断等相关业务的知识图谱，工程不单独建设常识性、科普性知识库。

7.4.4 知识引擎应具备知识推理计算功能，并可集成在信息系统中。当被业务应用流程调用时，可返回知识计算的结果。

7.4.5 知识引擎应具备知识库管理功能，功能应包括对预案、规则、知识图谱等的管理维护和可视化表达。

8 业务应用系统

8.1 工程通用要求

8.1.1 应视工程施工需要，设置建筑物和堆渣场的施工期安全自动监测及预报预警功能、水雨情自动监测及预报预警功能，监测数据记录应平顺衔接到工程运行维护阶段。

8.1.2 可利用信息技术加强对工程关键建筑物、关键施工工法的质量控制和监督管理，施工过程数据应按照电子档案管理。

8.1.3 涉及地下洞室施工的工程可采用物联网等技术提升对施工人员和施工设备的安全作业管控能力。实时对地下洞室施工环境进行视频监视和安全监测，安全监测项目根据需要应包括（但不限于）粉尘、毒害气体、地应力、放射性元素、环境温度、排（涌）水量等。

8.1.4 根据隧洞地质条件确有必要设置超前地质预报系统的，信息系统可集成地质条件远程在线诊断系统。

8.1.5 建设期对影响质量、进度、安全、环境的关键变量进行趋势分析和预警。

8.1.6 建设期宜对关键施工方案进行优化仿真分析，优化分析的目标函数宜为施工质量最优、施工用时最短、施工费用最省或施工能耗最低等。

8.1.7 工程运行监测类应用宜具备工程运行状态在线安全评估和预警功能。

8.1.8 水资源调度决策类应用应具备包含节水、降耗、生态流量保障等约束条件的优化决策功能。

8.1.9 水库、电站、闸站、泵站、河湖水域及堤防、蓄（滞）洪区等工程中的重点区域宜布设高清智能视频监视设备，鼓励在实现传统视频记录功能的基础上，采用新算法实现水位辅助识别、水质监测、车流人流统计、人脸识别、周界报警、火灾探测、温度探测等功能，合理拓展视频监视系统的应用范围。

8.1.10 工程视频监视系统宜与工程主要设备的操作、故障报警、火灾报警、安防系统等实现联动。

8.1.11 经分析确有必要时，应对工程中旋转、振动的重要机电设备进行振动监测和振动模式识别，监测对象包括（但不限于）水轮机、发电机、水泵、电动机、调流阀等。

8.1.12 设有过鱼设施的工程，应设置过鱼设施监测控制系统，对过鱼种类、数量进行监测，并宜实现过鱼效果的统计评估功能。

8.1.13 应对主要机电设备操作动作次数、在线运行时长等进行统计和分析。

8.1.14 宜对电化学防腐设施的运行状态进行监测，设施数量较多时可选取典型区域的进行

监测。

8.1.15 鼓励针对管理类业务开发移动应用系统。可采用语音输入、图像识别等智能技术辅助提升移动应用的便捷性。

8.1.16 宜建设工程智能巡检系统。巡检手段可选择具有音视频及通信功能的手持式移动终端。

8.1.17 无人机、无人船、机器人作为巡视巡查工具，宜优先采用社会服务，经分析确有必要时，也可自行配置。无人机的使用应严格遵守相关法律法规的规定。

8.1.18 工程各级管理机构配置的设备规模、系统功能应与工程管理机构职能相匹配。

8.1.19 对入库径流、河库关键断面水位、洪水过程等进行预报，多泥沙河流宜对入库泥沙及淤积情况进行预报；有冰凌风险的水库工程宜结合危害程度酌情开展凌汛预报。

8.1.20 对工程主要建筑物安全、关键机电设备运行状态、威胁人员和工程安全的地质灾害等进行安全预警；河湖、水库工程应对水位、洪水进行预警，承担城镇供水任务的工程还应对供水水质进行预警；承担防洪、行蓄洪任务的工程还应对淹没范围内的人员进行预警。

8.1.21 对洪水过程、工程调度方案、水力学过渡过程、淹没范围等进行数字空间下的全过程预演。

8.1.22 通过多工况下的预演，分析建立工程应急抢险、工程应急调度等预案，并具备预案管理功能。

8.2 水库枢纽工程

8.2.1 大型及重要中型水库枢纽工程应按照数字孪生技术路线建设工程信息系统。

8.2.2 大、中型水电站宜配置水轮发电机组、主变压器（110kV 及以上或 100MVA 及以上）、高压配电装置（110kV 及以上）、发电机电压设备等主设备的在线状态监测装置及健康诊断系统，运用声、光、电等多种监测方式实时监测主要设备运行健康状况，实现状态检修的目的。避雷器在线监测宜采用数字化的采集和传输方式。

8.2.3 兼有多项开发任务的枢纽工程，宜开发水资源优化调度系统，对枢纽工程各项开发任务进行全局优化调度管理，节约集约利用水资源。水电站监控系统、船闸（升船机）监控系统、过鱼设施监控系统宜为工程信息系统提供综合调度管理所需的实时运行信息。

8.2.4 承担防洪任务的水库枢纽工程，应与当地省（市）防汛指挥系统共享必要的水雨情监测和预报数据。多个水库枢纽联合承担防洪任务的，宜在水库防洪调度的集控中心实现多库联合防洪调度。

8.2.5 承担城镇供水任务的枢纽工程，应按环境保护设计要求设置水质自动监测设备，监测数据宜与测站所在省级水行政主管部门共享。

8.2.6 承担生态供水、农业灌溉供水任务的枢纽工程，应按环境保护设计要求对水库分层水温及出库水温进行实时监测，并在供水过程中满足水温敏感对象对水温的要求。

8.2.7 承担拦沙减淤任务的枢纽工程，应研究配置库底及坝前淤积监测设施的必要性。经分析确有必要时，淤积监测系统宜具备水库泥沙淤积数值分析和预报功能。

8.2.8 水库枢纽工程应对下放生态流量进行监测，监测数据应与省级水行政主管部门共享。

8.2.9 枢纽工程的水情自动测报系统应具备准确性、可靠性的自修正或可维护能力，为实现水库汛期运行水位的动态调控提供支撑。

8.2.10 同时具有主电站及生态流量电站的枢纽工程，宜设置电站集控中心，集控中心优先考虑与其中一座水电站的中控室合并布置。运行管理另有要求的，视运行管理要求而定。

8.2.11 应对枢纽机电设备的运行能耗进行实时监测，并尽可能地采用高效、节能的运行方式运行。

8.2.12 枢纽电站厂房、坝体廊道、地下洞室宜采用智能照明系统。

8.2.13 枢纽电站地下厂房及有水淹厂房危险的地面或半地面厂房，应设置专用水位监测报警系统。

8.2.14 枢纽电站应对技术供水水量、渗漏排水水量进行监测和预警。

8.2.15 水库库岸具有崩塌、滑坡风险并可能影响河道行洪、大坝安全或电站发电运行的，应设置边坡稳定自动监测预警系统。

8.2.16 水库枢纽蓄水可能对地下水环境造成不利影响的，经分析确有必要时，宜按相关专业要求设置受影响区地下水监测系统、确定监测项目，地下水监测数据应与国家地下水监测系统共享。

8.2.17 枢纽水库为饮用水源地的，水库大坝管理区出入口及内部主要道口宜设置高清智能视频监视系统对来往车辆和行人进行监视；在水库上游主要支流入库口设置高清智能视频系统对水面漂浮物、人员进行监视。

8.2.18 经分析确有必要进行大尺度的地质、水土保持、环境和生态监测监视的，可研究采用卫星遥感或无人机监测，监测分析成果应作为枢纽调度决策和后评价的依据。

8.2.19 枢纽工程如确有必要，可采用增强现实（AR）技术辅助工程巡检。适宜的场所也可采用机器人自动巡检，与监控系统形成功能互补。

8.3 调水工程

8.3.1 大型和重要中型调水工程应按照数字孪生技术路线建设工程信息系统。重要的中型调水工程主要包括承担城镇或工业供水任务的调水工程。

8.3.2 承担城镇供水任务的大、中型调水工程，应设置骨干工程全线集控中心。承担城镇供水任务且全线无在线水量调蓄能力的长距离调水工程，宜论证设置备用集控中心的必要性。备用集控中心应结合工程现场设施或现场管理机构布置。

8.3.3 调水工程监控系统含全线集中监控层、现地集中控制层在内，监控层级不宜超过 3 级。

8.3.4 水资源优化调度、控制系统在满足供水需求、供水安全和生态流量的前提下，一般以全线水量损耗最小、能耗量最小或运行费用最低为优化目标，根据需要也可以最短控制调节时间为优化目标。

8.3.5 应在输水线路关键调节控制断面设置水情自动监测设备，水位、压力、流量等监测数据接入工程监控系统，监测精度应满足工程运行调度分析计算要求。

8.3.6 调水工程取水口、沿线泵站、重要闸站、余能回收电站、柴油发电机房、沿线重要供配电设施、重要通信设备、水质自动测站、调蓄水库（池）、险工险段、重要交叉建筑物等重点部位以及人员不易巡视的部位应设置视频监视设备。

8.3.7 输水线路沿线小容量用电设施供电困难或经济上极不合理时，可采用分布式光伏或风光互补电源供电，同时宜对电源运行状态进行远程监视，可采用公网无线通信（3G、4G 等）、低功耗广域网通信（LPWAN）、北斗卫星通信等无线通信方式。

8.3.8 调水工程中的余能回收电站宜在电站现地进行发电运行控制，并同时接受调水工程集控中心的输水运行监视。运行管理另有要求的，视运行管理要求而定。

8.3.9 应集中对全线工程安全自动监测数据进行监视，并宜实现工程安全在线评估功能。

8.3.10 包含深埋长隧洞的调水工程，宜对隧洞进出水温差进行监测，具备条件的也可结合安全监测设施加测重要隧洞洞段的水温。

8.3.11 承担城镇供水的调水工程，应按环境保护设计要求在水源地和调蓄水库（池）设置水质自动监测设备。

8.3.12 输水隧洞需要停水进人检修的，现场检修作业的进度状态及人员信息宜及时上传至工程集控中心。

8.4 水（船）闸工程

8.4.1 大型水闸及其附属通航建筑物应按照数字孪生技术路线建设工程信息系统。参与河湖数字孪生流域或蓄滞洪区仿真分析的中型水闸，应纳入数字孪生流域建设。

8.4.2 水闸工程宜对工程机电设备运行能耗进行监测，并采用节能的运行方式运行。

8.4.3 船闸工程应对船闸耗水量和机电设备运行能耗进行监视，并通过运行方式的优化达到节水、节能运行。

8.4.4 长期挡水运行或进行流量调节的大中型工作闸门宜装设闸门运行状态在线监测装置，并将其中影响闸门运行安全的关键数据接入闸门计算机监控系统。

8.4.5 经分析确有必要时，可设置闸门门前淤积监测系统。

8.4.6 位于河流、湖泊的闸坝工程，闸门运行状态应与河流、湖泊（流域）管理单位实时共享。条件成熟时，宜建立河流、湖泊流域控制性建筑物的综合优化调度系统。综合优化调度系统应尽可能兼顾防洪、供水、水生态、水环境、灌溉、航运的要求。

8.4.7 闸坝坝顶兼做公共交通道路的，宜设置智能视频监视系统对道路交通流量、重载机动车进行监视，同时闸坝安全自动监测系统应具备安全预警功能。

8.5 泵站工程

8.5.1 大型及重要中型泵站工程应按照数字孪生技术路线建设工程信息系统。重要的中型泵站工程主要包括长期运行的供水泵站、河湖沿岸重要的排涝泵站、蓄滞洪区主要的排涝泵站等。

8.5.2 承担供水任务的泵站或泵站群（组），应根据业务需求建设集成化的水资源优化调度系统，在满足各类用户需水量的前提下优化机组（或泵站群）运行方案，尽可能降低运行能耗。

8.5.3 承担灌溉、排涝任务的大、中型泵站或泵站群（组），宜接受灌溉、排涝调度中心的统一调度，经分析确有必要远程集中控制的，宜在集控中心实现泵站远程控制。

8.5.4 灌溉、排涝集控中心宜设置在其中一座泵站的中控室，或泵站群（组）的管理单位。

8.5.5 泵站群或具有梯级泵站的工程，应建立以节能、节水为约束条件的梯级优化调度模型。

8.5.6 大型泵站应具备主设备状态检修功能，宜配置机组、主变压器、高压配电装置、起动装置、调速装置等主设备的在线状态监测设备，运用声、光、电等多种监测方式实时监测设备运行健康状况。避雷器在线监测宜采用数字化采集和传输方式。

8.5.7 泵站主机组流道出口工作闸门及事故闸门应设置闸门开度监测，并根据闸门型式设置防止闸门卡阻的纠偏装置。

8.5.8 泵站计算机监控系统应对技术供水水量、渗漏排水水量进行监测。泵站有水淹厂房危险的应设置防水淹厂房的专用监测报警系统。

8.5.9 泵站计算机监控系统应对机组效率、泵站能耗进行实时监测，并由系统辅助引导采用高效、节能的运行方式。

8.5.10 泵站厂房、地下洞室宜采用智能照明系统。

8.5.11 大中型泵站如确有必要，可采用增强现实（AR）技术辅助巡检。适宜的场所也可采用机器人自动巡检。

8.5.12 从水库、河流、湖泊取水或向水库、河流、湖泊排水的泵站，其运行流量及水量应与水库或河湖管理单位实时共享。

8.6 灌溉工程

8.6.1 控制灌溉面积 30 万亩及以上的灌溉工程应开展工程信息系统设计。灌区引水工程参照调水工程要求开展数字孪生工程建设。

8.6.2 大型灌溉工程应建设工程综合信息管理系统，功能包括（但不限于）水雨情监测、供水计量、工程安全监测、土壤墒情、需水分析、水量调度及决策支持、防汛抗旱预警、工程运行维护等系统。

8.6.3 灌溉工程宜设置灌区集控中心。大型灌区如确有必要按行政区划分区独立管理时，可按分区分别设置控制中心，但各分区相同业务的应用服务应统一开发、统一部署。灌溉工程一般不设备用集控中心。

8.6.4 灌区中小型泵站应结合泵站运用方式合理选定现地监控系统规模，推荐采用简化的现地监控系统配置，并接受灌区集控中心远程控制。大型泵站可设置中央控制室进行现地集中控制。

8.6.5 农用灌溉机井管径在 20cm 及以上的，应安装计量设施，管径在 20cm 以下的，可采用以电折水等计量方法计量。地下水超采区应在以上要求基础上结合实际进一步提升机井计量覆盖面。

8.6.6 结合灌区实际需求，可设置或完善气象、墒情、水雨情等监测站，气象预报应优先采用接入专业气象预报服务；对兼顾城镇供水功能的灌溉工程，宜按环境保护设计要求设置水质监测站。

8.6.7 灌区骨干工程的闸（阀）门宜采取集中监视，并结合灌区实际情况对重要闸（阀）门采取集中或分区域集中控制。

8.6.8 渠系闸门孔口规模较小时，可结合经济性分析采用测控一体化闸门，并在闸门开度和水位监测基础上根据运行需要合理集成视频监视、流量监测等功能。

8.6.9 灌溉工程应在重要控制性建筑物及安防点安装视频监视设备，可结合视频图像识别技术提高监管水平。

8.6.10 如确有必要对灌区地下水水位、水质等进行监测，监测数据宜与国家地下水监测系统共享。

8.6.11 当灌区田间工程采用滴灌、微喷、渗灌、喷灌等精细化（或水肥一体化）灌溉方式时，宜对灌溉设备供水量、施肥量进行监测统计。

8.6.12 零散分布在灌区中的各类监测设施宜优先选用低功耗无线传输方式。

8.6.13 灌区水量自动监测系统宜实现水量和水费自动计收管理。

8.6.14 如确有必要可采用无人机进行灌溉工程的巡检。

8.7 河湖工程

8.7.1 宜以河湖流域为单元建设河流、湖泊综合信息管理系统；大江大河大湖及主要支流、重点流域已开展数字孪生流域建设的，流域内的河湖工程应为所在流域数字孪生平台提供数据支撑。

8.7.2 工程以整条河流、整个湖泊为单元建设时，宜建设数字孪生流域信息平台，在数字空间下以水利模型、水利知识驱动流域的水资源调配、水灾害防御、水环境修复、城市水系统智慧调度、灌区高效用水调控等具有四预功能智慧决策系统。

8.7.3 河流、湖泊综合信息管理系统依托 GIS 技术标定河道管理范围边界，整合堤防管理、监测项目、已建及在建水利设施等基础信息。跨省河流流经省份依据合理的权限共享同一信息管理平台数据。

8.7.4 应充分利用国家防汛抗旱指挥系统工程及河道现有水文站网数据资源，实现对河道干流关键控制断面水位、流量、冰厚（北方）等的监测。

8.7.5 河湖年许可水量 50 万 m^3 及以上的取水口，原则上均应安装在线计量设施，水资源短缺、地表水过度开发的地区，应结合实际扩大在线监测覆盖范围。取水监测数据应共享至取水口所属省级水行政主管部门。

8.7.6 一级、二级堤防工程应设置堤防工程安全监测系统，监测数据应共享至河流、湖泊管理单位。经分析确有必要时，也可同步采用遥感影像技术对河湖岸线、堤防开展监测与分析。

8.7.7 河湖堤防安全监测系统宜结合流域水情监测及预报成果实现河湖智能综合防汛预警

功能。

8.7.8 根据水环境风险分析，必要时可对河道或湖泊底泥进行监测，监测项目视风险因素而定。

8.7.9 水质问题突出的河段和湖泊，可以省（或流域）为单元建立水质分析数学模型，进行流域水质分析、预报计算，计算成果宜在流域范围内共享。

8.7.10 河道的重点闸坝工程、堤防险工险段、穿堤建筑物区域应设置视频监视系统；水质问题突出的河段和湖泊，视频监视系统宜兼顾覆盖治理范围内的重要污水排放口；堤顶道路作为公共交通道路的宜在关键道口设置视频监视设备监视重载车辆通行情况；重点防洪城市的城区防洪堤，宜优先共享该城市已有的视频监视信息。

8.7.11 在水土流失风险较大的河道，可结合相应水文站开展河道含沙量监测。

8.7.12 应建设堤防防汛物资管理系统，对防汛、抢险物资进行数字化调度管理。

8.7.13 人员密集区的堤防工程宜配合堤防视频监视系统设置应急广播系统。

8.7.14 河湖日常管理确有需要时，可选用无人机或无人船对河流、湖泊进行巡检。

8.7.15 在信息化基础设施及监测感知体系建设方面，鼓励河湖工程与城市景观、生态文旅等领域有机融合、共建共享。

8.8 蓄（滞）洪区工程

8.8.1 蓄（滞）洪区工程应按照数字孪生技术路线建设工程信息系统，并与所在流域的数字孪生平台相衔接。

8.8.2 蓄（滞）洪区工程的监测、监视、控制设备宜优先采用集成化程度较高的设备，也可考虑利用已有监测、监视、控制设备。

8.8.3 蓄（滞）洪区工程监控网络宜优先采用公网有线或无线通信方式。蓄滞洪水时，公网通信有中断风险的，可自建通信网络，建设方案应通过技术经济比选后确定。

8.8.4 蓄（滞）洪区的进、退洪闸、主要排涝泵站宜统一接受市级或省级水行政主管部门监视，并接受防汛指挥部门的调度。

8.8.5 蓄（滞）洪区的进洪、退洪（排涝）设施以及安全区重要邻水部位确有需要时，应设置视频监视设备，视频信息应共享至水行政主管部门、防汛指挥部门。

8.8.6 蓄（滞）洪区应建设淹没分析与灾损评估系统，推荐以 BIM+GIS 技术为支撑，辅助防洪调度决策。具备飞行条件的地区，可采用无人机对汛情进行监视。

8.8.7 应建设通信预警系统，确保可采用多途径及时有效地发布预警预报信息。

8.8.8 应建设蓄（滞）洪区巡检系统、行洪预案管理系统。

8.8.9 应建设防汛物资管理系统，对防汛、抢险物资进行数字化调度管理。

8.8.10 蓄（滞）洪区管理单位设有视频会商系统的，应接入所属市级或省级水行政主管部门和防汛指挥部门的视频会商系统。

8.9 圩区工程

8.9.1 应根据相邻河湖水系、水利工程的数字孪生建设情况，合理选择圩区信息系统建设定位，结合工程运行管理方式选定是否将圩区信息系统纳入流域孪生平台。

8.9.2 对于圩区内部设置的大、中型泵站应满足 8.5 泵站工程规定的相关要求。

8.9.3 对于圩区内部设置的大、中型水闸应满足 8.4 水（船）闸工程规定的相关要求。

8.9.4 宜对泵、闸站的进、出圩区的流量进行实时监测，并汇总至集控中心。

8.9.5 工程等别为Ⅰ等、Ⅱ等、Ⅲ等的圩区工程宜设置圩区集控中心。其中的小型泵、闸站推荐采用简化的现地监控系统配置，并接受集控中心远程控制。

8.9.6 圩区工程宜按需设置雨水情监测系统、工程安全监测系统、防汛预警系统、工程运行维护系统等。

8.9.7 宜对圩区重点堤防的临水侧进行视频远程监视，视频监视系统的建设应充分评估保护区内施工条件、运营商资源等因素。

8.9.8 工程等别为Ⅰ等、Ⅱ等、Ⅲ等的圩区工程宜构建流域水文水动力模型进行计算分析，为确定排涝流量和优化泵闸站开启顺序提供决策支持。

8.9.9 工程等别为Ⅰ等、Ⅱ等、Ⅲ等的圩区工程宜对圩外、圩堤、圩内的防洪风险进行动态评估，预测圩外水位情况，评估堤防失稳风险，绘制圩内动态风险图，为工程调度提供决策支持。

9 实体运行环境

9.1 一般要求

9.1.1 工程信息系统的实体运行环境一般包括集控（总调）中心控制室、数据中心、会商室，其他的设备运行环境应遵循相关标准设计。

9.1.2 集控（总调）中心控制室、数据中心应设置门禁系统和视频监视设备对进入人员进行管控。

9.1.3 集控（总调）中心控制室、数据中心、会商室宜优先选择与工程设施结合布置。

9.1.4 集控（总调）中心控制室、数据中心、会商室应避开强磁场、强震动和强噪音的干扰，并采取防尘、防潮、防噪音、防静电、防火等措施。

9.2 集控（总调）中心

9.2.1 梯级水电站、实施水资源联合调度的水库群或泵站群、联合调度的闸群宜设置工程联合调度中心进行集中调度；运行管理需要实施远程控制的，应具备工程集中控制功能。

9.2.2 梯级水电站、承担城镇供水任务且无在线调蓄能力的大（Ⅰ）型调水工程宜设置备用集控中心，接管集控中心的集中控制功能，备用集控中心应结合工程现场设施布置。

9.2.3 大中型水电站和梯级水电站集控中心、水库群集控中心、大型泵站和泵站群集控中心、水闸集控中心和调水工程集控中心宜配置用于运行监视的大屏幕显示系统。

9.2.4 用于运行监视的大屏幕显示器整体分辨率应不低于 2K。

9.2.5 根据工程规模，工程集控（总调）中心控制室面积宜为 80～120m²。

9.3 数据中心

9.3.1 水利水电工程数据中心应根据 GB 50174《数据中心设计规范》设计。

9.3.2 在已建的管理机构部署数据中心时，应对建筑物荷载进行复核。

9.3.3 机柜总数小于 5 的通信或数据中心机房也应配置 UPS、空调、防雷接地等设施，同时宜根据现场条件配置简化的动环监测设施，包括温湿度监测、烟雾探测、视频监控系统、门禁系统等内容。

9.3.4 工程数据中心、重要通信节点机房的动环监测信息应上传至工程集控（总调）中心。

9.4 会商室及会议系统

9.4.1 大型和重要中型水利工程宜设置会商室，面积宜为 80～150m²。会商室大屏幕、音控、视频会议等设备配置应根据会商对象、使用频率及参会人员规模合理确定。小型水利工程必

要时根据现场条件配置用于视频会议的桌面终端和视频会议软件。

9.4.2 除集控（总调）中心外，工程其他各级控制分中心参与会商的人员少于 8 人时，会商室可与中控室合并。

9.4.3 根据工程管理要求设有控制（调度）分中心的工程，集控中心与分中心以及重要的单位工程之间可配置视频会议系统。

9.4.4 工程的视频会议系统不宜与业务系统融合建设。

9.4.5 视频会议系统应支持 H.323 和 SIP 协议。

10 信息资源共享

10.1 共享对象

10.1.1 根据工程信息系统中数据的情况，信息共享的外部对象可包括：

1 水利部、流域管理机构和地方水行政主管部门。

2 工程所在地相关的生态环境、自然资源、交通、公安等部门。

3 社会公众。

10.1.2 流域管理机构在水利工程建设项目中统筹建设的信息基础设施和算法模型服务，其共享的外部对象可包括：

1 流域下属管理机构。

2 流域管理范围内的水利工程。

10.2 数据共享

10.2.1 大型水库的大坝以及最大坝高不低于 70m 的大坝监测数据、大坝安全诊断及预警指标宜接入全国大型水库大坝安全监测监督平台。省（市）级水行政主管部门有监管要求的，也应按要求接入。

10.2.2 设有自动安全监测设施的中型水库和小型水库，其大坝安全监测信息宜接入省级水行政主管部门相关信息平台中。

10.2.3 跨越省界或流域范围的工程采集的水位、流量、雨量、气象、墒情、水质、含沙量等水利基础数据应通过工程信息系统同步交换到所属省、流域的信息平台中。

10.2.4 水利水电工程中针对河流、湖泊、蓄滞洪区、圩区采集建立的地理空间数据应与水行政主管单位实现数据共享。

10.2.5 拦河建筑物、堤防、穿堤建筑物的建筑信息模型，若用于数字孪生流域三维空间模型建设和三维仿真分析的，应与水行政主管单位实现数据共享。

10.2.6 工程业务应用宜与水行政主管单位的政务系统实现数据共享，为流域、区域的水利公共服务提供数据支撑。

10.3 资源共享

10.3.1 水利水电工程新建、改建信息系统应充分利用工程运行管理单位已建计算、存储、网络等资源，当已建资源不足时，应在工程影响范围内进行改扩建。

10.3.2 同一运行管理单位下的不同水利水电工程，宜建设共享的计算、存储资源平台。

10.3.3 水利水电工程中建设的计算、存储、网络等资源应得到充分利用，在资源充足且满足相应网络安全等级保护的防护要求时，可以共享给工程运行管理单位的其他工程使用。

10.3.4 水利水电工程中可通用的算法模型服务应对外共享。

10.4 共享方式

10.4.1 水利水电工程信息共享应符合水利数据分类分级管理要求。

10.4.2 应通过工程信息系统的数据资源共享组件（或平台）统一向外共享信息和服务。

10.4.3 信息系统的数据资源共享组件（或平台）宜支持多种常见数据交换协议。

10.4.4 数据资源共享组件（或平台）应支持下列数据共享方式：

1 服务接口共享，将数据或算法模型服务封装成 Web API，供外部用户调用。

2 文件共享，通过文件在线下载方式共享。

10.4.5 数据资源共享组件（或平台）应对工程信息资源的共享过程进行管控，并宜对数据、算法模型服务接口的运行状态进行实时监控。

10.4.6 工程中可对外共享的计算、存储、网络等设施资源，宜以云服务（IaaS）的方式对外共享。

11 网络安全

11.1 保护对象和等级

11.1.1 工程信息系统应合理划分网络安全保护对象，根据 GB/T22240 确定各保护对象的安全保护等级。

11.1.2 大、中型水利工程的信息系统保护对象可按工业控制系统与管理信息系统划分。管理信息系统保护对象还可划分为服务于生产管理的应用和用于综合办公的应用。

11.1.3 大型和重要中型水利工程，当实现集中控制时，其集中控制系统的网络安全保护等级可确定为第三级，各现地控制系统安全保护等级应根据系统遭破坏或信息泄露后的后果确定。小型和其他中型水利工程可参照第二级设计。

11.1.4 大型和重要中型水利工程的管理信息系统中，服务于生产管理的应用可按照不低于第二级设计，具体等级应根据系统遭破坏或信息泄露后的后果确定。综合办公类的应用可参照第二级设计，小型和其他中型水利工程管理信息系统可不高于第二级。

11.1.5 工程信息系统应按照 GB/T 39786《信息安全技术 信息系统密码应用基本要求》同步开展密码应用，密码应用等级可参照网络安全等级保护定级结果。网络安全保护等级确定为第三级的系统，应进行密码应用安全性评估。

11.1.6 工程信息系统可能被确定为关键信息基础设施的，其安全防护要求可参照 GB/T 39204《信息安全技术 关键信息基础设施安全保护要求》及 SL/T 803 执行。

11.2 安全物理环境

11.2.1 应根据 GB/T 22239 和工业控制系统相关安全防护要求进行物理环境的安全防护设计。

11.2.2 系统运行所需的物理环境包括数据中心、接入和汇聚网络通信设备机房、通信线路敷设环境等，相应环境的安全设计均应满足其网络安全等级对应的技术要求。

11.2.3 工程信息系统部署在泵站、水电站副厂房时，相应物理环境在满足计算机监控系统需求基础上，还应满足信息系统对电力供应、电磁防护和安防等的要求。

11.2.4 工程信息系统各个现地运行环境的物理安全监测信息应接入工程统一的网络安全管理平台。

11.3 安全通信网络

11.3.1 应根据 GB/T 22239 和工业控制系统相关安全防护要求进行通信网络的安全防护设

计。

11.3.2 水电站、船闸、调水工程、供水泵站、具有防洪功能的大型水闸工程监控系统的网络应采用分层分区结构，并按安全分区、专网专用、横向隔离、纵向认证（加密）的原则进行设计。其他类型的工程监控网络根据具体安全需求灵活设计。

11.3.3 水利水电工程通信网络宜划分为控制网和管理信息网。控制网主要承载水电站、泵站、重要闸（阀）门等设施的实时监测控制业务；管理信息网主要承载控制网业务以外的其他业务，并可根据需要对管理信息网进一步划分安全域。

11.3.4 承载控制业务的通信和计算机网络应采用加密认证技术实现身份认证、访问控制和加密传输。承载安全等级为第三级的管理信息时，通信和计算机网络也应采用加密传输方式。

11.3.5 管理信息网可采用自建 CA 服务或采用第三方提供的 CA 服务。

11.4 安全区域边界

11.4.1 应根据 GB/T 22239 和工业控制系统相关安全防护要求进行系统区域边界的安全防护设计。

11.4.2 工程的控制网和管理信息网应采用物理上相互独立的网络设备组网，控制网与管理信息网之间应设置单向安全隔离装置。

11.4.3 应将业务系统完整地置于一个安全分区内，当业务系统有跨安全分区通信要求时，应通过统一的安全隔离设施通信。

11.4.4 水利水电工程的水情自动测报、短期水文预报、中长期水文预报、发电计划、优化调度、设备状态监测与分析、工程运行评价、继电保护信息管理、电能量计量等应用宜部署在控制网，并与控制网中的实时控制系统进行逻辑隔离。

11.4.5 水利水电工程的安全监测、防汛抗旱决策支持、设备状态检修、安防联动、仿真分析等应用宜部署在管理信息网。

11.5 安全计算环境

11.5.1 应根据 GB/T 22239 和工业控制系统相关安全防护要求进行系统计算环境的安全防护设计。

11.5.2 涉及工程运行控制安全的实时控制信息应存储在工程自建的存储系统，不宜上传至省、流域水利云中心，更不应存储在公有的云计算中心。

11.5.3 水利水电工程信息系统应制定数据备份及恢复机制，数据备份异地存储时，存储位置应结合工程设施选定。

11.5.4 当工程使用政务云、行业云平台时，宜在工程管理单位本地保存业务数据的备份。

11.5.5 工程信息系统仅采集必须的用户个人信息，且能禁止未授权的访问。

11.5.6 工程信息系统安全审计应覆盖每个用户，应对审计记录进行保护和备份。

11.6 安全管理平台

11.6.1 工程的控制网及管理信息网宜分别设置网络安全管理平台。

11.6.2 网络安全管理平台应对工程的网络安全总体状态进行统一监视，当识别到入侵攻击、恶意操作、越权访问等行为时，管理信息网的安全管理平台应及时报警并进行阻断，工业控制网的安全管理平台应及时报警，并持续监视和记录。

11.6.3 网络安全管理平台应通过安全通信链路对安全设备进行远程配置管理。

11.6.4 网络安全管理平台应对安全管理员进行身份鉴别，并能对其操作行为进行审计。

11.7 安全扩展要求

11.7.1 当采用云平台时，平台的基础设施及运维地点均应在中国境内。使用政务云、行业云平台时，应确保其网络安全等级满足工程信息系统的要求。

11.7.2 工程采用移动互联网或无线网络传输数据的，无线接入设备应具备接入认证功能，并可接受访问控制管理侧的远程管控。

11.7.3 经论证，工程运维工作及智能移动设备的使用确有必要自建无线网络的，宜参照独立内网建设，自建无线网不应与工业控制网有相互连接。

11.7.4 与电力监控系统有信息传输需求的工业控制系统安全防护应符合电力监控系统安全防护总体方案要求。

11.7.5 工程建设期的移动互联网、物联网、云计算安全防护方案，应随施工进度的变化及时调整。

12 系统集成与运维

12.1 系统集成

12.1.1 系统集成主要实现工程中各类应用、平台之间功能整合和业务协同，将各分项系统按总体设计的要求组装为一个有机的整体。

12.1.2 工程建设期、运行期新建系统之间宜采用应用程序接口（API）实现功能集成或采用中间件实现数据集成。

12.1.3 经评估，工程中已有业务系统可继续使用时，宜采用界面集成或数据集成的方式将系统整合纳入新建系统，并完善相应网络安全防护措施。

12.1.4 当工程新建少量业务应用，并拟集成到工程现有信息平台时，应优先采用数据集成的方式。

12.2 运行维护

12.2.1 应根据软件系统、硬件设施部署情况，明确运行维护任务、维护方式以及运维工具。

12.2.2 应根据信息系统的重要程度确定运行维护对象的服务等级，宜划分为四个级别，级别由高到低分别为一级、二级、三级、四级。

12.2.3 重要的工程信息系统（安全保护等级为三级及以上）运行维护服务等级应不低于二级，其他信息系统服务级别宜为三级。

12.2.4 系统应设立与生产环境相互独立的测试环境，系统新功能上线前应在测试环境中进行测试验证。

12.2.5 大型水利水电工程应建设统一的信息系统运维管理平台，对系统软硬件设施设备的运行状态进行实时监控，并可实现对设备的远程配置管理。中小型工程信息系统可使用独立的、由软件系统或设备自带的网络管理、安全管理功能进行运维管理。

12.2.6 运维管理平台宜具备自动化运维能力， 并可对系统进行补丁管理、变更管理、软件版本管理等。

12.2.7 工程信息系统的运维管理宜设置专职管理机构，配置专职技术人员。

附录 A　工程信息系统典型逻辑架构图

A.0.1 工程信息系统在工程里的定位

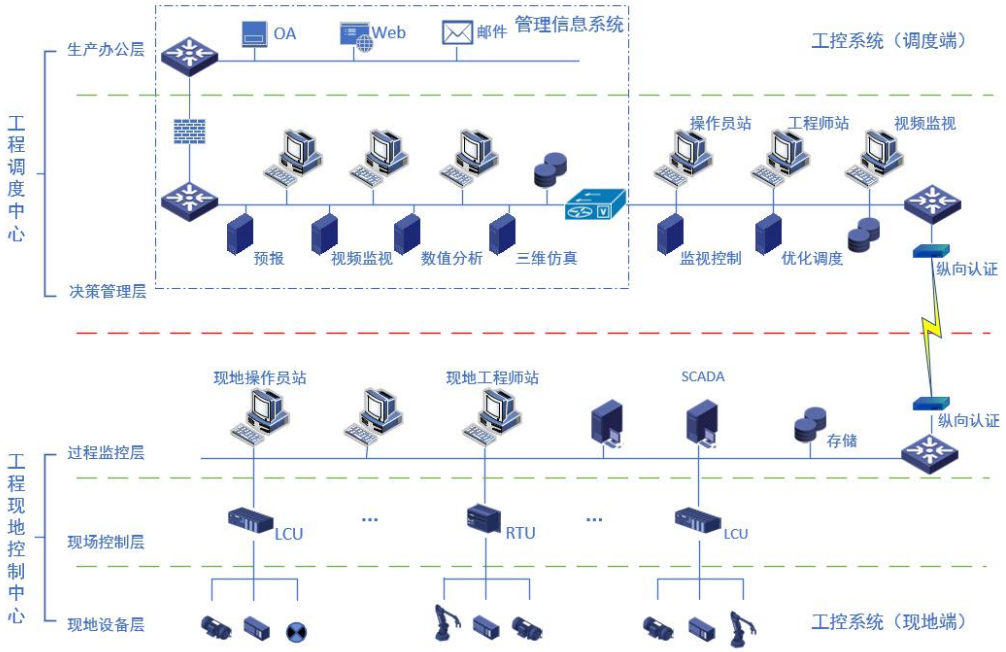

图 A.0.1 工程信息系统与工程自动控制系统的关系

A.0.2 工程信息系统典型逻辑架构图



图 A.0.2 工程信息系统典型逻辑架构图

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/737146136010010001