

CECS

T/CECS xxx-202x

中国工程建设标准化协会标准

建设工程数字化施工管理系统技术规程

（征求意见稿）

Technical Specification for Digital Construction Management
System of Construction Projects

中国 xx 出版社

中国工程建设标准化协会标准

建设工程数字化施工管理系统技术规程

Technical Specification for Digital Construction Management
System of Construction Projects

T/CECS xxx-202x

主编单位：XXXXXX

批准单位：中国工程建设标准化协会

施行日期：202x 年 x 月 x 日

中国 xx 出版社

202x 北 京

前 言

《建设工程数字化施工管理系统技术规程》（以下简称规程）是根据中国工程建设标准化协会《关于印发<2025 年第一批协会标准制订、修订计划>的通知》（建标协字[2025]22 号）的要求进行编制。编制组经广泛调查研究，认真总结实践经验，参考国内外有关标准，并在广泛征求意见的基础上，制定本规程。

本规程共 8 章和 2 个附录，主要技术内容包括：总则、术语和缩略语、基本规定、数据、系统功能及接口、系统运行环境、系统运维、系统安全等。

本规程某些内容可能涉及一种施工管理系统相关专利（专利号：ZL 2024 1 0263671.0）、一种施工任务单创建方法、存储介质以及计算机程序产品相关专利（专利号：ZL 2025 1 0059124.5）、工程施工验收单生成方法、系统和存储介质相关专利（专利号：ZL 2024 1 0869163.7）、一种记工预警系统相关专利（专利号：ZL 2024 1 0169374.X）、一种施工进度管理方法、系统、装置和存储介质相关专利（专利号：ZL 2024 1 0080350.7）、一种存储项目文档的方法、系统及存储介质相关专利（专利号：ZL 2025 1 0474190.9）、一种施工任务单处理方法、系统及介质相关专利（专利号：ZL 2024 1 0713323.9）的使用。涉及专利的具体技术问题，使用者可直接与专利持有人（单位或人员）协商处理。除上述专利外，本规程的某些内容仍可能涉及专利，本规程的发布机构不承担识别这些专利的责任。

本规程由中国工程建设标准化协会建筑与城市信息模型专业委员会归口管理，由一智科技（成都）有限公司负责具体技术内容的解释。执行过程中如有意见或建议，请反馈给一智科技（成都）有限公司（地址：四川省成都市高新区天府五街 200 号菁蓉汇 1A-10 层，邮政编码：610095，电话 028-XXXXXXX，邮箱：niexian@axzo.cn）。

主编单位：一智科技（成都）有限公司

中国建筑科学研究院有限公司

参编单位：中国五冶集团有限公司

四川华西集团有限公司

西南交通大学

成都建工集团有限公司

四川路桥建设集团股份有限公司

成都倍特建筑安装工程有限公司

主要起草人：刘勇刚 刘俊杰 杜磊堂 聂 贤 赵 焱
陈洪辉 朱礼敏 王振兴 谭小聪 夏 天
杨依然 杨根明 陈 艳 丁云波 张剑峰
何 希 陈 伟 李文焕 余志祥 田永丁
廖文杰 庄 重 向柏霖 饶 丹 高 杨
成 蕾 向正松 席呈虎 黎 倩 丁广林
代付全

主要审查人：

目 次

1 总则	1
2 术语和缩略语	2
2.1 术语	2
2.2 缩略语	4
3 基本规定	6
3.1 系统架构	6
3.2 数据共享	7
4 数据	9
4.1 一般规定	9
4.2 基础数据	10
4.3 业务数据	11
4.4 其他数据	14
5 系统功能及接口	15
5.1 一般规定	15
5.2 实名制管理子系统	16
5.3 任务管理子系统	17
5.4 进出场管理子系统	18
5.5 记工管理子系统	19
5.6 发薪管理子系统	19
5.7 评价管理子系统	20
5.8 质量管理子系统	21
5.9 安全管理子系统	22
5.10 进度管理子系统	23
5.11 技术管理子系统	24
5.12 成本管理子系统	27
6 系统运行环境	29
6.1 一般规定	29
6.2 网络环境	29
6.3 数据采集设备	30
7 系统运维	34
7.1 一般规定	34
7.2 系统监控	34
7.3 日志管理	34

7.4 数据库备份与恢复	35
7.5 数据库灾备管理	36
7.6 数据更新维护	37
8 系统安全	38
8.1 一般规定	38
8.2 网络安全	39
8.3 数据安全	39
8.4 安全保密	40
附录 A 基础能力要求	41
附录 B 数据合理性控制标准	46
用词说明	48
引用标准名录	49

Contents

1 General Provisions	错误！未定义书签。
2 Terms and abbreviations	错误！未定义书签。
2.1 Terms	错误！未定义书签。
2.2 Abbreviations	错误！未定义书签。
3 Basic requirements	错误！未定义书签。
3.1 System architecture	39
3.2 Data sharing	错误！未定义书签。
4 Data	错误！未定义书签。
4.1 General provisions	错误！未定义书签。
4.2 Basic data	错误！未定义书签。
4.3 Business data	错误！未定义书签。
4.4 Other data	错误！未定义书签。
5 System functions and interfaces	15
5.1 General provisions	15
5.2 Real-name system management subsystem	15
5.3 Task management subsystem	17
5.4 Entry and exit management subsystem	错误！未定义书签。
5.5 Work recording management subsystem	18
5.6 Salary payment management subsystem	19
5.7 Evaluation management subsystem	20
5.8 Quality management subsystem	21
5.9 Safety management subsystem	22
5.10 Progress management subsystem	23
5.11 Technical management subsystem	24
5.12 Cost management subsystem	26
6 System operating environment	28
6.1 General provisions	28
6.2 Network environment	28
6.3 Data collection equipment	29
7 System operation and maintenance	32
7.1 General provisions	32
7.2 System monitoring	32
7.3 Log management	32
7.4 Database backup and recovery	33
7.5 Database disaster recovery management	34
7.6 Data update and maintenance	35

8 System security	36
8.1 General provisions	36
8.2 Network security	错误！未定义书签。
8.3 Data security	37
8.4 Security and confidentiality	错误！未定义书签。
Appendix A: Basic capability requirements	39
Appendix B: Data rationality control standards	44
Explanation of terms used	45
List of cited standards	46

1 总则

1.0.1 为推进建设工程数字化施工管理转型，提升多组织协同效率，规范施工现场数据采集与共享机制，强化施工质量安全管控，优化进度、技术与成本管理水平，助力工程建设全流程精细化管理和政府高效监管，促进建设工程高质量发展，制定本规程。

1.0.2 本规程适用于建设工程的数字化施工管理系统建设。

1.0.3 建设工程数字化施工管理系统除应符合本规程外，尚应符合国家现行有关标准和现行中国工程建设标准化协会有关标准的规定。

2 术语和缩略语

2.1 术语

2.1.1 项目协同组织 Project Collaboration Organization

由建设工程相关单位或组织共同参与，通过明确的协同机制、职责分工及数据交互，实现项目目标的组织协作形式。

2.1.2 任务项 Task Item

将建设工程领域需完成事项从分部分项工程逐级拆解至最细粒度的工序，每个细粒度工序被称为工人需要完成的任务项。

2.1.3 任务特征 Task Characteristics

用于反映施工任务项复杂度、技术难度、安全风险、消耗成本和工期的任务内在属性，常用特征包括规格、型号、材料、温度、湿度、高度等。

2.1.4 任务单 Task Order

用于明确描述施工区域、施工任务项、作业交底、安全交底、工期、履约对象、计价方式、预估工程量、预估金额、付款方式的单据，形成派单与接单双方的微合约。

2.1.5 进出场 Entry and Exit

在本规程内主要指工人进入施工现场和离开施工现场，应与工人在项目注册、退出项目组织区分开。

2.1.6 进度单元 Progress Unit

由施工区域与进度节点组成，是某区域施工进度节点达成情况的管理单元。

【条文说明】例如“3#楼 10 层的砌体完成”，3#楼 10 层是施工区域，砌体完成是一个进度节点。

2.1.7 生产单元 Production Unit

由施工区域与任务项组成，是某区域施工生产任务项分配、检查、验收的管理单元。

【条文说明】例如“3#楼 10 层的顶口封砌工序”，3#楼 10 层是施工区域，顶口封砌工序是一个任务项。

2.1.8 访问控制 Access Control

访问控制是一种安全机制，用于限制对系统资源（如文件、数据库、应用程序）的访问权限。通过设置用户角色和权限，确保只有授权人员可以查看、修改或删除特定的数据。

2.1.9 系统日志 System Log

系统日志记录了系统的运行状态和各类事件，包括系统启动、关闭、接口调用、异常信息等。

2.1.10 专户 Project-Specific Account

专户的全称是农民工工资专用账户，是指总包单位在工程建设项目所在地银行业金融机构开立的，用于支付工资的专用存款账户。

2.1.11 人工费 Labor Cost

人工费是支付给直接从事建筑安装工程施工作业的生产工人的各项费用。

2.1.12 动态拨付 Dynamic Appropriation

拨付是人工费拨付的简称，是建设单位向总包单位专用账户拨付工资款的行为。动态拨付则指在工程建设过程中，根据项目记工金额和专户余额的差值变化，对人工费金额实现按需拨付的弹性拨付机制，从而区别于传统的固定周期或一次性拨付方式。

2.1.13 限制人员 Restricted Personnel

指在特定时间、区域或条件下，被限制通行或操作权限的人员。该人员因安全、管理等要求，受到相应的出入或行为限制。

2.1.14 电子围栏考勤 Electronic Fence Attendance

利用电子围栏技术，通过设定虚拟地理边界，对人员进出特定区域的行为进行自动识别和记录，实现考勤管理。系统在人员进入或离开考勤区域时，按要求进行考勤打卡，则采集考勤数据并触发相应处理。

2.1.15 人脸识别验证 Facial Recognition Verification

用人脸生物特征进行身份识别和认证的技术。系统通过采集和比对人脸图像，实现对人员身份的自动确认和访问控制。

2.1.16 合约引擎 Contract Engine

一种用于规范施工任务派发与计价管控的核心模块，通过预设任务内容范围、计价单价区间、工程量单位及产能阈值等规则，约束任务派发行为，避免无序派单与定价乱象，提升任务派发规范性与效率。

2.1.17 边缘计算 Edge Computing

在数据产生源或网络边缘侧（如传感器、采集终端、网关等）就近提供计算能力的分布式计算模式。其特点是在靠近设备的一端对数据进行实时处理和分析，仅将结果或必要的原始数据上传至中心系统，从而降低网络带宽压力、提升响应速度和系统稳定性。

2.1.18 OPC UA Open Platform Communication Unified Architecture

一种面向工业自动化的数据交换标准，提供跨平台、跨厂商、跨系统的互操作性。其特征包括统一的地址空间模型、安全的数据传输机制，以及支持从现场设备到上层应用的多层级通信，常用于智慧工地的数据采集设备对接与集成。

2.1.19 RP6 Salt Spray Test Level RP6

设备在盐雾腐蚀试验中的防护等级要求，RP6 等级表示设备需能在规定浓度和时间条件下经受盐雾环境考验而不发生明显锈蚀、起泡、开裂等损坏，通常用于户外环境设备的耐腐蚀性能评价。

2.2 缩略语

BIM（Building Information Model）建筑信息模型

CDN（Content Delivery Network）内容分发网络

CPU（Central Processing Unit）中央处理单元

DBA（Database Administrator）数据库管理员

HTTPS（Hyper Text Transfer Protocol Secure）超文本传输安全协议

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

IK（Impact Protection）抗冲击等级

IP（Ingress Protection）防护等级

JSON（JavaScript Object Notation）JavaScript 对象表示法

MQTT（Message Queuing Telemetry Transport）消息队列遥测传输协议

OPCUA（Open Platform Communications Unified Architecture）开放平台通信统一架构

PaaS（Platform as a Service）平台即服务

RFID（Radio Frequency Identification）射频识别

RP（Resistance to Salt Spray）盐雾试验等级

RPO (Recovery Point Objective) 恢复点目标

RTO (Recovery Time Objective) 恢复时间目标

TCP/IP (Transmission Control Protocol / Internet Protocol) 传输控制协议/网
际协议

VPC (Virtual Private Cloud) 虚拟私有云

3 基本规定

3.1 系统架构

3.1.1 建设工程数字化施工管理系统架构（图 3.1.1）应包括基础设施层、数据层、业务应用层、用户层。

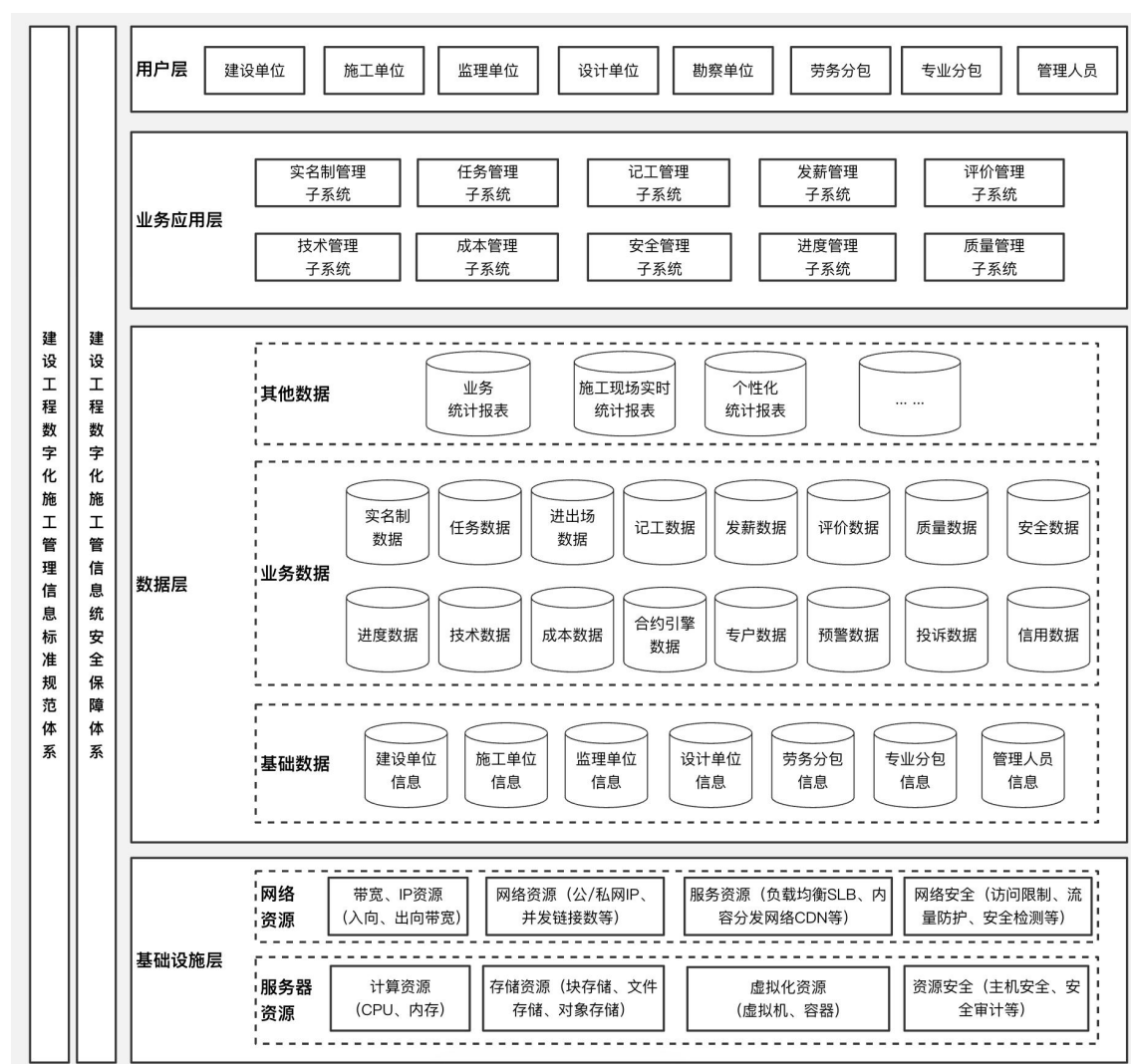


图 3.1.1 系统架构图

【条文说明】建设工程数字化施工管理系统总体架构由基础设施层、数据层、业务应用层和用户层构成。基础设施层提供系统运行的底层支撑；数据层统一管理基础数据与业务数据；业务应用层部署质量、安全、进度、成本管理等各业务功能；用户层面向工程项目各层级参与角色、系统管理员及数据维护人员提供信息服务。

3.1.2 基础设施层应包含基础软件、机房环境、硬件设备（服务器、存储等）、安全防护设施、网络及通信设备等关键组件。宜采用云计算技术，通过云服务（如IaaS（Infrastructure as a Service）基础设施即服务、PaaS（Platform as a Service）平台即服务）及云存储形式实现。

【条文说明】基础设施层为信息系统提供运行所需的底层支撑环境。

3.1.3 数据层应包括基础数据、业务数据和其他数据，并符合下列规定：

1 基础数据宜包括建设工程施工项目信息、各方责任主体信息、人员信息、设备信息；应包括建设单位、施工单位、监理单位、设计单位、勘察单位的管理人员信息，应包括劳务分包、专业分包的管理人员信息；

2 业务数据宜包括任务数据、实名制数据、进出场数据、记工数据、发薪数据、评价数据、质量数据、安全数据、进度数据、技术数据、成本数据等；

3 其他数据包括非基础和业务类数据，如报表、日志类数据等。

3.1.4 业务应用层应由各业务应用系统组成，宜包括任务管理子系统、实名制管理子系统、记工管理子系统、发薪管理子系统、评价管理子系统、质量管理子系统、安全管理子系统、进度管理子系统、技术管理子系统、成本管理子系统。

【条文说明】业务应用层部署质量、安全、进度、成本管理等各业务功能。

3.1.5 用户层宜包括主管部门、建设单位、施工单位、监理单位、设计单位、勘察单位、分包单位、班组、工人等相关角色、系统管理员和数据维护人员等。宜为没有智能手机的用户提供的临时处理工作流的固定设备，主要用于工人接单、确认记工、访客登记。

【条文说明】用户层面向工程项目各层级参与角色、系统管理员及数据维护人员提供信息服务。

3.1.6 建设工程数字化施工管理系统应具备技术标准规范体系和安全保障体系。

3.1.7 建设工程数字化施工管理系统的密码使用和管理应符合国家现行有关标准的规定。

3.2 数据共享

3.2.1 建设工程数字化施工管理系统应符合现行国家标准《信息安全技术—数据安全能力成熟度模型》GB/T 37988 的有关规定。数据共享应符合下列规定：

1 系统宜为监管部门系统提供可访问的接口,并提供可集成外部系统数据的能力;

2 系统内部各子系统之间应实现数据共享;

3 数据接口的标准应符合本规程附录 C.0.3 (数据接口技术参数表)的有关规定。

3.2.2 数据共享应符合现行国家标准《信息安全技术 网络安全等级保护基本要求》GB/T 22239 的有关规定,进行分级权限管理。

3.2.3 外部系统或用户应在系统指定入口提交共享数据使用申请,经系统数据管理员审批同意后才能使用。

3.2.4 系统应建立共享监控机制,记录数据共享交换过程的信息,包括发起方、接收方,采用的共享和交换规则、策略的运行情况等。系统应通过比对发送日志和接收日志以验证发送、接收数据的一致性。

3.2.5 系统数据共享接口的元数据编制、数据报文设计、数据传输方式需符合现行国家标准《信息安全技术 网络安全等级保护基本要求》GB/T 22239 及《全国一体化政务大数据体系第 2 部分:数据共享交换要求》GB/T 45800.1-2025 的有关规定,其中与外部系统共享的接口需包含身份认证、数据校验、日志记录等功能模块,确保共享过程可追溯、可审计。

【条文说明】分级权限管理:工程数字化施工管理系统的数据应按照敏感程度及重要性划分成不同等级,同时和系统用户的角色或岗位类型相匹配,确保敏感数据受控访问,避免数据泄露。

4 数据

4.1 一般规定

4.1.1 建设工程数字化施工管理系统的数据宜包括基础数据、业务数据及其他数据。数据的格式应符合国家现行有关标准的规定。

【条文说明】建设工程数字化施工管理系统的数据库可按照不同的标准进行划分,在本规程中划分了三大类:基础数据、业务数据和其他数据。三大类数据又可进一步细分为工程基础数据、地理空间数据、任务数据、实名制数据、进出场数据、记工数据、发薪数据、评价数据、质量数据、安全数据、进度数据、技术数据、成本数据、业务统计报表数据、施工现场实时统计报表数据等十五类数据。

4.1.2 建设工程数字化施工管理系统基础数据中的地理空间数据应采用统一的时空基准。

【条文说明】建设工程数字化施工管理系统的部分子系统带有地图应用功能,使用了电子地图等基础地理数据,因此采用相同的时空基准才能保证数据的共享。

4.1.3 建设工程数字化施工管理系统业务数据应随工程的施工过程同步生成;应采取安全措施,原始数据不得被修改、截留和泄露。

【条文说明】建设工程数字化施工管理系统涉及建设工程的施工全过程,例如派工、考勤、质量、安全、验收、记工、发薪等诸多方面。目前一些地方的建设工程施工过程数据仍采用人工填报的形式,部分还存在事后补报的现象,施工管理过程数据存在被人为修饰或篡改的潜在风险,因此为了保障建设工程施工管理过程数据的真实性和及时性,本规程要求施工业务数据应随工程的施工过程同步生成,杜绝事后补报行为;同时要采用实时上传或加密存储等安全措施,保证施工过程产生的原始数据不被修改、截留、泄露。

4.1.4 建设工程数字化施工管理系统业务数据宜作为工程档案保存,保存期限应符合现行行业标准《建设电子文件与电子档案管理规范》CJJ/T 117的有关规定。

【条文说明】按照现行行业标准《建设电子文件与电子档案管理规范》CJJ/T 117的要求,对列入城建档案管理机构接收范围的工程,应在国家规定的期限内,将建设工程电子档案与纸质档案同步向当地城建档案管理机构移交。建设工程数字化施工管理系统应结合建设工程电子档案资料的存档要求,做好数据的接口,支

持从建设工程数字化施工管理系统中直接提取业务数据，生成建设工程施工全过程的电子档案资料，既减轻了建设单位整理档案资料的负担，又能确保档案资料的真实性，还可减少城建档案管理机构对非标电子档案数据进行档案整编的工作量。系统业务数据的保存期限可参照建设工程电子档案管理的相关规定。在具体实施时，系统可根据保存期限要求来做好前端设备和服务器设备的设计与部署。

4.2 基础数据

4.2.1 建设工程数字化施工管理系统的基础数据应包括工程基础数据和地理空间数据等。

【条文说明】工程基础数据、地理空间数据属于建设工程数字化施工管理系统数据库的基础数据，也是各子系统可共享使用的公共数据。

4.2.2 工程基础数据应包括建设工程施工项目信息、各方责任主体信息、人员信息、设备信息；应包括建设单位、施工单位、监理单位、设计单位、勘察单位的管理人员信息，以及劳务分包、专业分包的管理人员信息。

【条文说明】工程基础数据的内容包括建设工程项目信息、各方责任主体信息、人员信息、设备信息等。工程项目信息一般包括项目名称、项目地点、建筑面积、工程造价、建筑用途、项目状态、开工日期、竣工日期、工程结构类型等信息。工程基础数据一般需要由基础数据管理子系统统一管理，并提供给各个子系统共享使用，避免各个子系统分别录入工程基础数据，导致同一项目信息在不同子系统数据库中存在差异，从而给施工现场的协同造成困难。各地、各部门在设计建设工程数字化施工管理系统时，可以根据需要对工程基础数据的内容进行扩展。

4.2.3 地理空间数据应包括建筑工地位置数据、项目电子围栏数据、施工区域数据。

【条文说明】系统数字化管理中应包括地理空间数据。系统地理空间数据一般包含以下三类：建筑工地位置数据、项目电子围栏数据、施工区域数据。地理空间数据一般需要由基础数据统一管理，并提供给各子系统共享使用，避免各子系统因为位置、区域差异，无法正常使用。其他的专题地图，如建设主管部门、建设单位、施工单位、监理单位等的位置分布图，以及现场人员位置监控数据（即人员轨迹图）等可结合管理需要拓展。

4.3 业务数据

4.3.1 业务数据应包括实名制数据、任务数据、进出场数据、记工数据、发薪数据、评价数据、质量数据、安全数据、进度数据、技术数据、成本数据等。还应包含基于以上业务产生的预警数据，包括预警工程信息、预警事件信息、预警处办信息。预警工程信息宜包括工程名称、工程类别、施工许可证等；预警事件信息宜包括预警事项、预警指标、风险等级、预警开始时间、预警结束时间等；预警处办信息宜包括整改要求、处理状态、处理进度、处理人员等。

【条文说明】系统业务数据主要指建设工程数字化施工过程中所产生的各类数据。根据施工过程的不同阶段，业务数据又可分为实名制数据、任务数据、进出场数据、记工数据、发薪数据等多种类别，在具体实施时，每种类别的业务数据又可分为多个小类，各地可根据实际需要进行扩展。此外，系统应提供各核心业务的预警处办能力，为施工管理人员提供管理抓手，完成预警监控与处办闭环，产生的预警数据应进行结构化设计。

4.3.2 实名制数据应包括人员身份信息、注册认证信息、关联的施工单位信息以及信用信息等。人员身份信息宜包括姓名、身份证号、岗位信息、所属单位、人员入职离职、面部图像信息以及身份证的其他基础信息等内容。人员信用信息应包括人员姓名、身份证号、联系方式、参建工程、风险记录信息等。

【条文说明】系统应对实名制数据进行规范化管理。实名制数据是保障施工现场人员身份唯一性与合法性的关键基础，须确保其信息的准确性与完整性。数据内容包括人员基本身份信息及相关认证信息。通过实名制管理，可有效防范冒名顶替、无证上岗等现象，维护现场管理的合规性与安全性。

4.3.3 任务数据应包括工程的施工区域、施工图纸、施工任务项、交底、工期、履约对象、单价、预估工程量、任务预估金额数据等。

【条文说明】任务数据采用结构化存储方式，涵盖施工区域定位、图纸关联、任务项分解、工艺标准、工期节点、执行主体、计价基准、预估工程量及任务预估金额计算等要素。任务数据作为进度跟踪、成本核算及施工调度的核心依据，支撑现场作业的规范化执行。

4.3.4 进出场数据应包括人员进场信息、人员出场信息。进场信息应包括人员实名制信息、人员身份信息、进场时间、进场地点、进出区域、通行方式等；出场

信息应包括出场时间、出场地点、通行方式等。

【条文说明】系统需对进出场数据进行结构化设计，采集并存储人员的进出场记录。进出场数据主要包括进场信息和出场信息，其中进场信息包括人员身份标识、进场时间及地点，出场信息涵盖出场时间及地点，以及进出区域的在场时长。进出场数据是施工现场人员、考勤核验和安全管控的重要基础，完善的进出场数据有助于实现施工现场的动态监管，提升现场安全与管理效率。

4.3.5 记工数据应包括班组管理人员信息（姓名、所属班组）、工人信息（姓名、工种）、出勤日期、施工作业内容、完成工程量、单价、记工金额；宜包括操作日志记录。

【条文说明】记工作为发薪的重要凭证，需关联工人指定周期内的工作任务、考勤数据，同时基于以上数据，输出记工金额供发薪使用；在记工操作过程中，为确保数据操作可追溯，需要存储记工单内数据变动的过程。

4.3.6 发薪数据应包括专户数据、从业人员实名制备案与用工花名册信息、从业人员进出场信息、从业人员任务与记工信息、项目工资支付专用账户信息、从业人员发薪账单信息以及从业员工资支付信息。宜包括银行流水、账户余额等信息。其中，专户数据应包括专户基本信息、银行开户信息、工程项目信息、总包单位信息、建设单位信息、人工费拨付信息、专户交易信息。专户基本信息宜包括专户名称、专户账号、专户类型等；银行开户信息宜包括银行名称、开户时间、销户时间等；工程项目信息宜包括工程名称、工程类别、施工许可证号等；总包单位、建设单位信息宜包括企业名称、统一社会信用代码等；人工费拨付信息宜包括拨付规则、拨付周期、拨付金额等；专户交易信息宜包括专户余额、专户流水等。

【条文说明】发薪数据主要依赖于考勤、任务、记工等数据，基于以上数据生成发薪数据，根据相关审批流程完成工资支付。此外，专户作为用于支付工资的专用存款账户，系统需要提供专户相关的各项信息，供相关部门和企业及时了解专户内款项的来龙去脉。

4.3.7 评价数据应包括评价场景、评价人、评价时间、评价对象、评价结果等数据。

【条文说明】评价是建设工程各参与方对他人在施工过程中的表现所给出的主观意见，评价数据是对评价行为的记录。基于评价数据，管理人员可以对项目上的

人员进行更有效地管理，例如，对于质量安全意识评价结果不佳的人员，可及时提供质量安全相关技能培训，提升其质量安全意识，保障工程施工质量。

4.3.8 质量数据应包括质量检查记录、质量验收记录、质量整改问题、质量整改记录等数据。

【条文说明】质量功能模块应全面覆盖施工任务相关环节，根据任务阶段进行质量检查、质量验收、质量整改，形成相应的信息记录。

4.3.9 安全数据应包括安全检查记录、安全整改问题、安全整改记录、危大工程清单、危大工程相关资料、危大工程检查记录、重大危险源清单等数据。

【条文说明】施工安全是在建设工程的施工过程中，为保障施工现场人员的生命安全以及现场设备、材料和周边环境的安全，采取的一系列预防和防控措施，安全数据是对这些预防和防控措施采取的管理行为所产生的过程记录。这些管理行为往往涉及施工任务的事前、事中和事后管控，因此系统应对这些管理数据进行如实记录，以便于施工管理人员制定安全防控方案，如遇安全风险可及时干预和控制。

4.3.10 进度数据应包括进度节点、关键工序、节点完成条件、计划完成时间、进度节点完成度等数据。

【条文说明】进度是对建设工程在施工过程中各项工作任务进展的描述，进度数据则是对每项工作完成情况的真实记录。基于进度数据，管理人员可以及时了解建设工程的施工进展，并与进度计划进行对比分析，对与进度计划有偏差的任务及时干预和调整，确保工程按期交付。

4.3.11 技术数据应包括施工区域、施工任务项、作业交底、安全交底、质量通病、安全风险、规范图集、施工图纸。宜包括施工日志、安全日志等信息。

【条文说明】技术数据涵盖施工区域、任务项、作业交底、安全交底、质量通病库、安全风险库、规范图集索引及图纸。可扩展存储施工日志、安全日志等过程记录数据。技术数据为施工工艺控制、风险预警及合规性校验提供基础支撑。

4.3.12 成本数据应包括合约引擎数据、盈亏账本数据和变更签证数据。合约引擎数据应包括任务内容、控制单价、控制工程量、控制产能要求数据。盈亏账本数据应包括任务预估金额、记工金额、已发薪金额数据。变更签证数据应包括基本信息和关联信息，基本信息包括施工任务单、发起人、受影响的施工单位、佐证材料、审批流程以及预估金额信息，关联信息包括整改单、图纸信息、洽商记录

等。

【条文说明】合约引擎需根据合约对任务派发进行精细化管控，对任务内容设置控制单价、控制工程量、控制产能要求。系统需对变更签证数据进行结构化设计，并开展变更签证的数据的采集、建库等。变更签证的基本信息内容包括施工任务单、发起人、受影响的施工单位、佐证材料、审批流程以及预估金额信息，关联信息，根据需要，允许关联包括整改单、图纸信息、洽商记录等信息。盈亏账本根据任务预估数据、已施工完成任务金额、记工金额、已发薪金额生成账本数据，为拆分任务和推送工人记工提供判断依据。

4.4 其他数据

4.4.1 系统应包括业务统计报表、施工现场实时统计报表等其他数据。

【条文说明】系统的其他数据主要满足建设工程施工过程中不同层级和角色管理人员对项目的管理需求，提供面向企业管理人员、项目管理人员的多维度统计报表。由于建设工程的施工过程涉及的主体较多，不同的组织或参建单位，以及项目上不同岗位管理人员的管理职能有所不同，丰富的统计报表数据有利于各职能管理人员快速发现作业异常并及时处理，以确保工程有序开展。

4.4.2 业务统计报表应包括用工统计报表、任务统计报表、考勤统计报表、记工统计报表、发薪统计报表、评价统计报表、质量统计报表、安全统计报表、进度统计报表、成本统计报表、预警统计报表等。

【条文说明】系统业务统计报表可帮助相关管理人员主动或被动地了解建设工程的施工过程整体现状，分析施工过程中存在的问题与风险，并及时处理。

4.4.3 施工现场实时统计报表数据应包括人员实时进出场打卡报表、在场班组报表、在场访客报表、在场工人报表、在场管理人员报表、疲劳作业工人报表、施工中危大和超危大任务报表等功能。

【条文说明】施工现场实时统计报表是对施工现场的人员进出场情况以及现场作业安全情况进行实时数据统计的报表。由于建设工程的施工现场环境复杂且存在诸多安全隐患，对现场人员的管理以及施工作业安全的管理就显得尤为重要，因此宜为现场安全管理人员提供实时的可视化报表，以便及时了解现场人员动态，对疲劳作业、危大作业人员进行有效管理，以确保工程安全有序开展。

5 系统功能及接口

5.1 一般规定

5.1.1 建设工程数字化施工管理系统应支持与第三方平台进行数据交换，应提供开放标准的数据接口，满足与外部系统集成需求。数据接口的标准应符合本规程附录 C.0.3（数据接口技术参数表）的有关规定。

【条文说明】数据接口功能应支持数据对接与同步，满足系统集成要求，减少人工重复录入操作。

5.1.2 建设工程数字化施工管理系统应支持内部各子系统间进行数据交换。

5.1.3 建设工程数字化施工管理系统应具有预警管理功能，并提供预警规则、预警事件、预警处办等配置功能，应符合下列规定：

1 预警规则配置选项应包括预警工程类别、预警指标及预警阈值、风险等级、预警周期、预警时间、通知对象、通知内容。

2 预警事件管理应支持对预警事件提供筛选、查看、统计、分析的功能。

3 预警处办应包括下发整改、预警督办、取消预警的功能。

【条文说明】预警管理需通过任务、考勤、记工、发薪等数据整合和规则配置，构建“监测、预警、处办”的闭环管理流程，防范化解风险，变被动响应为主动预防。系统需实现以下核心功能：（1）系统需提供配置预警规则、进行预警监测的功能。系统需面向不同的预警场景（如人工费未足额发放、人员考勤数据异常等）给定可预警的监控指标（如发薪率、考勤率等指标），从而监测项目是否有对应的风险。系统需采用分级预警机制，支持“黄橙红”三级预警。当指标数值低于规则配置的阈值时，系统需自动生成对应风险等级的预警事件，并通知至相应人员角色。（2）系统需提供已生成预警事件的筛选、查看、统计、分析功能，供预警管理人员把握风险态势，了解风险情况。（3）系统需提供预警管理人员针对预警事件的处办功能，支持预警管理人员向产生预警的工程项目所属企业下发整改，并进行督办，直至预警消除。通过提前干预的方式，化解风险隐患，避免问题事故。

5.1.4 系统接口设计应符合下列标准规定：

1 与外部政务监管平台、银行专户系统的数据交互接口，应符合《全国一体

化政务大数据体系第2部分：数据共享交换要求》GB/T 45800.1-2025 中关于数据字段定义、传输频率及安全校验的要求；

2 与 BIM 模型、图纸引擎的数据对接接口，应符合现行标准《建筑信息模型应用统一标准》GB/T 51212 中关于模型数据格式、解析与传输的要求；

3 接口通信架构应符合《信息技术 开放系统互连 基本参考模型》GB/T 9387，优先采用 TCP/IP 协议栈、HTTPS 加密传输方式，确保跨系统兼容性与数据安全性。

5.2 实名制管理子系统

5.2.1 实名制管理子系统应包含实名信息管理、身份识别验证、信用管理、预警分析功能模块。

5.2.2 实名信息管理功能应符合下列规定：

1 应支持从业人员身份证号、姓名、岗位、技能证书等基础信息的录入、变更与归档；

2 应记录从业人员入职、离职、岗位变更等状态变更信息，并形成日志；

3 应支持通过人员身份鉴别采集设备自动采集人员信息；

4 应采集并存储从业人员的面部图像信息。

【条文说明】实名信息管理是实名制管理的基础，系统应支持从业人员自入职至离职期间的信息采集、维护和归档。身份证信息采集可提高数据准确性，面部图像数据应满足后续识别验证的技术要求。

5.2.3 身份识别验证功能应符合下列规定：

1 应在施工现场部署人脸识别终端、人员身份鉴别采集设备等验证设备，或支持基于具有人脸识别验证的电子围栏考勤方式；

2 应支持通过物理闸机或虚拟电子围栏方式进行身份识别和进出信息采集；

3 应记录每次验证的时间、位置、验证方式、验证结果；

4 应保存验证记录并支持按人员、时间段等条件查询、导出。

【条文说明】系统应支持规范执行身份识别验证操作，覆盖多种现场识别手段，包括人脸识别终端、电子围栏等。验证数据应完整留存，用于支持后续的考勤数据生成及进出管理应用

5.2.4 预警分析功能宜对从业人员出勤异常、连续未出勤、超时加班等情况进行识别和提示，并应具备数据展示、自动推送、历史记录留存等功能。

【条文说明】预警分析功能应基于考勤数据识别异常情况，并提供提示与记录功能。应结合历史数据和规则逻辑进行自动识别，识别后推送预警告知项目管理人员。

5.2.5 信用管理功能应实现信用数据录入、信用等级查询的管理功能，并应符合下列规定：

1 应具有风险人员和风险企业管理功能，应支持人员、企业的风险记录数据录入，宜支持提供风险人员、风险企业警示信息。

2 应提供人员、企业信用等级的查询、统计及分析功能。

【条文说明】针对存在不良行为的个人和企业，需提供风险人员、风险企业的名单录入功能。系统在展示人员、企业信息时，若人员、企业处于风险名单中，则展示风险警示信息，提示风险内容。系统需提供信用记录的查询功能。在提供企业信用记录时，除需提供风险记录数据、统计分析结果外，还需提供企业的营业执照、施工资质、施工许可证等电子证照，作为基础材料和重要依据。其中电子证照系统需满足本规程附录 A.0.2（电子证照的技术标准和性能标准）的规定。

5.3 任务管理子系统

5.3.1 任务管理子系统应预留扩展接口，提供与记工管理、考勤管理、人工费管理、质量管理、安全管理、成本管理、进度管理、技术管理等其他功能模块数据交互功能。

【条文说明】任务单作为业务驱动核心数据，需满足考勤、人工费、进度等模块在数据调用与流程触发中的要求，确保系统间协同一致。

5.3.2 任务管理子系统应提供任务单在不同层级的项目协同组织之间流转的功能，并应符合下列规定：

1 应提供总包单位、专业分包单位、劳务分包单位、班组、小组、工人按合约逐级派发或拆分任务单的功能；

2 应提供下级单位或个人对任务单接受或驳回的功能；

3 应提供配置自定义派发与验收流程的功能。

【条文说明】任务管理子系统需支持多组织多层级的任务单流转，需要满足不同工程类别与组织模式下的派发与协同需求，适配多类协作流程。

5.3.3 任务管理子系统应提供任务单关联单据及操作记录查询功能。

5.3.4 任务管理子系统应具备数据合理性校验功能，并根据校验结果对流程进行预警或拦截，合理性校验的标准应符合本规程附录 B.0.1（任务单风控标准）的有关规定。

【条文说明】任务单是建设工程数字化施工管理系统中所有业务单据的源头单据，需要具备真实性、完整性、合理性的校验机制。本条所列风控规则用于控制任务单数据在真实性、完整性、合理性维度的偏差，保障任务单全生命周期中关键要素的可追溯性与一致性。

5.4 进出场管理子系统

5.4.1 进出场管理子系统应包括通行权限管理、进出规则配置、通行记录管理、限制人员管理、异常行为识别预警、设备集成与接口对接等功能。

5.4.2 通行权限管理功能应满足根据进出场规则动态授予或回收通行权限的要求，并应记录权限的调整日志。

5.4.3 进出规则配置功能应读取施工任务数据、人员备案数据、记工确认数据、限制人员清单数据、访客数据等，并根据各模块数据灵活配置通行权限授予规则。

【条文说明】通过配置进出规则，可约束进出行为，提升现场人员管理的规范性。

5.4.4 通行记录管理功能应实时记录人员通行方向、进出时间、通道位置，并与实名制系统关联自动生成人员考勤数据、考勤报表。

【条文说明】通行记录功能应与实名信息和考勤数据关联，实现数据间的信息匹配与应用支撑。

5.4.5 限制人员管理功能应支持项目、企业、主管部门在所辖范围内手动录入限制人员名单，并支持限制人员名单逐级推送或上报，经审核后扩大限制范围。

【条文说明】自定义限制人员包含安全违规未处理人员，系统应支持限制人员名单的同步接入与管理，并记录相关拦截及提醒信息。

5.4.6 异常行为识别功能宜支持识别滞留人员、限制人员非授权通行、非实名制通道进场等异常行为，并可触发预警提示。

【条文说明】系统应识别异常行为事件并提供提示功能，以支持现场人员管理。

5.4.7 系统集成功能应符合下列规定：应支持门禁闸机数据对接，宜结合视频监控系统，对通行画面进行实时抓拍，同时应与实名制考勤系统共享通行数据，宜具备与第三方监管平台或劳务管理系统的对接能力。

【条文说明】系统集成功能应支持将不同系统连接起来，支持门禁设备与实名信息、通行记录系统的数据交互与联动操作。

5.5 记工管理子系统

5.5.1 记工管理子系统应通过记工单实现班组为工人记录工作量并推送工人确认记工、工人驳回记工的功能。

5.5.2 记工管理子系统应读取考勤子系统的工人进出场数据生成出勤日期、工作时长数据，应读取任务管理子系统的任务信息生成工作内容并记录工作量。

【条文说明】为工人记工时，为确保信息真实可溯源，需记录清楚工人在什么时间做了什么事情，花了多少时间等关键信息。

5.5.3 记工管理子系统应具备数据合理性校验功能，并根据校验结果对流程进行预警或拦截，应符合本规程附录 B.0.2（记工单风控标准）的有关规定。

5.5.4 记工管理子系统应实现向建设单位、监理单位、总包单位、专业分包单位、劳务分包单位等提供查看并处理异常记工信息的功能。

【条文说明】记工单作为发薪前的最后环节，需要提供风险识别的规则配置能力，避免不合理的记工单产生。比如：通过行业工种收入行情植入系统做初步判断，触发预警后，施工现场的总分包管理人员做评估审批等。

5.6 发薪管理子系统

5.6.1 发薪管理子系统应具有专户管理功能，应支持绑定、编辑、查询、删除专户，应与各专户银行对接申请开户、申请销户、校验工程项目信息准确性、查询开户和销户结果、查询专户余额、查询专户流水的功能。

【条文说明】项目在取得施工许可证或完成备案报批后，总包单位需在合作银行开立工资专用账户。总包单位通过系统提交专户开立申请，系统生成唯一申请编号；银行在受理开户时，需通过系统接口校验工程项目信息（如施工许可证号、

备案状态)及企业资质(如总包单位信用记录);核验通过后,银行完成专户开立,并将专户账号、开户时间等关键信息传回系统。系统存入专户与工程项目的关联信息,并更新企业专户台账。因项目竣工或项目出现异常必须终止时,需对项目工资专户进行销户处理。银行处理销户时,需向系统发起工程项目信息校验,校验通过后完成专户销户,同时需将销户信息回传至系统中。

5.6.2 发薪管理子系统应具有人工费动态拨付规则配置功能,应包括选择动态拨付计算规则、设置动态拨付周期、自动计算拨付金额的功能。

【条文说明】为减少企业在专户中的资金沉淀,提高资金使用效率,在建设单位向专户拨付人工费时,系统需提供动态拨付规则配置功能。配置内容需包括选择动态拨付计算规则和设置动态拨付周期,支持配置从项目产生记工数据的第二个月开始,建设单位每月根据项目上月实际记工金额进行人工费动态拨付。若专户余额充足或上月未产生记工数据,则无需拨付。从而避免企业资金过度积压,提升企业资金利用效率。

5.6.3 发薪管理子系统应具备发薪流程管理功能,应包括流程配置、发薪申请、发薪审批、发薪明细查询、发薪日志查询、发薪依据查询等功能,并符合下列要求:

1 发薪申请应基于记工单数据创建,每一笔发薪记录需与任务单、考勤信息、记工单关联。

2 发薪日志包括提交申请人员、审批人员、时间、状态、驳回的情况等信息。

【条文说明】发薪流程管理参与方多、审批流程长,参与方可能有:建设单位、监理单位、总包单位,专业分包单位,劳务分包单位,班组,工人,需要满足不同项目的发薪申请要求和审批流程要求。

5.6.4 预付回款应能实现预付单位依据预付记录数据生成可回款金额,根据相关审批流程,付款方和收款方双方确认后,完成预付回款支付。

【条文说明】需要给不同层级管理人员提供权限范围内的预付回款申请、查看预付和回款记录,预付回款申请金额支持按照预付单支持多笔提交。

5.7 评价管理子系统

5.7.1 评价管理子系统应支持对项目参建人的任务履约情况和个人工作表现进行

评价、查看和管理评价结果。

5.7.2 评价管理子系统应支持管理人员、班组长、工人之间的相互评价，并提供匿名评价功能。

【条文说明】匿名评价仅适用于涉及敏感问题的投诉类反馈，且匿名仅针对评价对象不可见评价人信息，有限制权限的管理员可验证评价内容并确保评价人身份可追溯。

5.7.3 评价管理子系统应提供可修改期限的配置，并支持在期限内修改、删除评价内容。

5.7.4 评价管理子系统应提供汇总查看本人发起的所有评价数据、所有被评价数据的功能。

5.7.5 评价管理子系统应基于任务履约情况提供派发人和履约人相互评价的功能，并满足以下条件：

1 班组长完成任务自检后，班组长可基于工人任务单评价工人。

2 管理人员完成任务验收后，管理人员可基于班组任务单评价班组长，或基于工人任务单评价工人。

3 班组长确认记工信息后，工人可基于工人任务单评价班组长。

5.7.6 评价任务履约情况应包含工作态度、质量意识、安全意识、诚信意识、专业能力、行为习惯等评价维度。

【条文说明】“工作态度”需要通过工作配合情况、工作主动性、沟通能力等维度衡量；“质量意识”需要通过技术资料的执行情况、成品观感、材料使用、质量通病防治等维度衡量；“安全意识”需要通过安全规定执行情况、安全设备使用情况、专业器材使用情况等维度衡量。

5.7.7 评价个人工作表现应包含正向评价和负向评价维度。

5.8 质量管理子系统

5.8.1 质量管理子系统应将作业交底传递至任务管理子系统，并应在任务单中查询任务项对应的作业交底文件。

【条文说明】质量管理要求以技术交底的形式触达工人层级，让工人熟知施工要求，在过程中通过对任务单的检查以控制质量，最后通过验收、整改责任到人形

成闭环。

5.8.2 质量管理子系统应具备过程检查、任务验收的功能，并应提供检查单、验收单的在线创建与流转，并将检查单、验收单关联对应任务单。

5.8.3 质量管理子系统应具有发起整改、整改回复、整改验收的功能，并将整改单与检查单、验收单、任务单等单据关联。

【条文说明】关联单据可提升验收过程的可追溯性。验收单与任务单的数据可互相查询，确保数据完整。

5.8.4 质量管理子系统应将检查、验收、整改数据传递至任务管理子系统、记工管理子系统，并提供检查不通过、验收不通过或整改未完成则任务无法结束的规则配置功能，提供任务未结束无法推送记工单的功能。

【条文说明】质量检查结果通过限制任务单后续流程，直接影响工人利益，促使工人严守质量规范。线上发起整改功能需要明确相关人员，确保整改责任清晰。

5.9 安全管理子系统

5.9.1 安全管理子系统应将安全交底传递至任务管理子系统，并应在任务单中查询任务项对应的安全交底文件。

5.9.2 安全管理子系统应具备过程检查功能，并应提供检查单的在线创建与流转，并将检查单关联对应任务单。

5.9.3 安全管理子系统应具有发起整改、整改回复、整改验收的功能，并将整改单与检查单、任务单等单据关联。

【条文说明】关联单据可提升验收过程的可追溯性。验收单与任务单的数据可互相查询，确保数据完整。

5.9.4 安全管理子系统应将检查、整改数据传递至任务管理子系统、记工管理子系统，并提供检查不通过、整改未完成则任务无法结束的规则配置功能，提供任务未结束无法推送记工单的功能。

5.9.5 安全管理子系统应能实现重大危险源管理功能，应将重大危险源信息与施工区域、任务项、图纸等信息关联，应提供重大危险源的监控、预警、过程记录等功能。

【条文说明】绑定关联功能可精准定位风险，监控和预警可及时处理隐患，记录

过程确保可追溯。

5.9.6 安全管理子系统应能实现危大工程管理功能，应符合下列规定：

- 1 需支持清单创建并绑定任务项与施工区域，关联图纸、交底信息并实现查看；
- 2 可上传专项方案及专家论证报告并支持预览；
- 3 需与任务单系统双向互通、向形象进度系统同步信息，同时对接巡检系统以推送提醒及创建记录，形成全流程关联与信息互通。

【条文说明】本条对危大工程管理功能说明如下：（1）危大工程需要涵盖任务项和施工区域，可通过任务项、施工区域与任务单进行绑定。（2）危大工程需支持关联系统中的其他子系统，如图纸、交底，任务单、形象进度、巡检等，支持危大工程的在相关流程中体现出警示作用。（3）危大工程需支持关联施工方案，在施工方案中上传审核通过的专项方案和专家论证通过的论证报告文件，且可在危大工程中查看。

5.9.7 安全管理子系统应能实现工人安全资料管理功能，并应符合下列规定：

- 1 应提供工人安全资料模板，并支持资料上传功能。
- 2 应支持工人在线签署安全资料，并能对已签署资料进行归档管理。
- 3 应记录工人安全资料的更新时间、更新内容及更新人等信息，形成完整的更新轨迹。
- 4 应可配置资料完整性校验规则，对缺失或不符合要求的资料进行提示。

【条文说明】工人安全资料包含三级安全教育记录卡、员工入场安全教育考试、农民工进场确认书、劳动合同、体检报告、安全风险告知书、员工消防安全工作承诺书、安全生产目标分解责任书、出行遵守交通安全承诺书、进场施工人员身体健康承诺书、农民工维权告知书等。

5.10 进度管理子系统

5.10.1 进度管理子系统应从任务管理子系统获取任务状态数据，并根据任务完成情况更新对应进度单元。

【条文说明】进度管理需要以施工任务单为依据，是实现施工进度全流程管理的基础条件，因为任务单能够提供具体的施工信息，确保数据准确性、实时性与可

追溯性，需在系统设计中明确其核心作用。将施工进度管理细分为多个功能模块，是提高管理效率与覆盖度的有效方法，因为每个模块对应具体的管理需求，需要规定功能模块的组成与职责分工。

5.10.2 进度管理子系统应包括施工进度节点管理、进度计划管理、形象进度管理等功能。

【条文说明】形象进度是以二维或三维的形式，直观展示项目整体及各施工区域，在各进度节点的施工进展及完成情况。

5.10.3 施工进度节点管理应包含进度节点创建、排序，节点关联的关键工序定义，及节点完成条件定义等功能。

【条文说明】进度节点管理需要根据工程类别，和楼栋、地下室、室外、基坑等施工区域类型为维度定义节点。每个进度节点需要关联多个关键施工任务项，进度节点的达成条件，可基于多个任务项全部完成或任一完成进行判断。

5.10.4 进度计划管理功能应提供进度计划制定方式。进度计划应能基于施工区域和进度节点维度，按照周期制定生产计划。宜提供实时调整进度计划、进度计划与任务单关联的功能。

【条文说明】进度计划需要按项目、楼栋、楼层、区域等维度，以周、月为维度制定。

5.10.5 形象进度管理功能的基础形式，应将区域和进度节点组成进度单元进行管理。应通过二维或三维形式展示不同颗粒度的进度单元完成情况

【条文说明】进度单元的完成情况应提供关键任务项完成度、任务单完成比例、工日消耗等多种衡量方式。关键任务项完成度需要获取 5.10.2 中进度节点管理里设置的关键任务项完成条件，以及任务单的工序完成情况数据得出。任务单完成百分比按已验收合格任务单数量占计划任务单总数的百分比计算得出。工日消耗按已验收合格任务单工日总数占计划任务单工日总数的百分比计算得出。

5.10.6 进度单元应能查看详细情况，包括计划工期、实际工期、关联单据和文档等信息。应能通过进度单元的计划工期、实际工期等信息进行比对分析，并基于同楼栋不同楼层的历史施工数据分析计算，实际进度偏差是否超过阈值。

5.11 技术管理子系统

5.11.1 技术管理子系统应包括生产单元管理、行业知识管理、图纸管理、现场日志管理、文档管理及方案管理。

【条文说明】本条规定了技术管理子系统包含的功能模块，用于施工过程中的技术资料组织、应用与记录。

5.11.2 技术管理子系统应输出数据至任务管理子系统，并符合下列规定：

- 1 在任务单应能查看和使用生产单元、行业知识及图纸数据；
- 2 在日志管理和文档管理模块应能查看和使用任务单、验收单、整改单等过程数据。
- 3 技术管理子系统应在任务单创建时自动向任务管理子系统推送关联的生产单元、图纸等数据；若数据传输失败，系统应即时生成预警并记录日志，由技术管理员排查处理。

【条文说明】本条规定了技术管理子系统与任务类数据的交互要求，任务执行中所需的图纸、知识和区域信息应可被调取，过程产生的数据可在日志与文档模块进行查看。

5.11.3 生产单元管理功能应符合下列规定：

- 1 应以施工区域与施工任务项的组合为生产单元进行管理；
- 2 应支持施工区域的创建、拆分与维护；
- 3 应支持为任务项配置任务特征信息。

【条文说明】本条规定了生产单元管理的结构组织方式，要求系统以任务项与施工区域的组合方式建立施工管理单元，并支持任务数据的分层维护与结构化配置。

5.11.4 行业知识管理功能应符合下列规定：

- 1 应支持管理质量通病、安全风险、规范图集等知识类型，可基于知识类型进行知识点的添加、维护、查看；
- 2 宜支持在任务项及任务特征上查看各类知识点。

【条文说明】本条规定了行业知识管理功能要求，应支持多类型知识资料的组织管理，并与任务数据进行结构化绑定，用于辅助任务单的创建与执行前置准备。

5.11.5 现场日志包括施工日志、安全日志、监理日志等类型，应基于当日施工任务数据自动生成日志，支持按日期、施工区域查看和检索日志内容，应支持移动端及 PC 端查看与编辑日志。

【条文说明】现场日志模块应结合任务数据进行生成，减少人工干预所引发的数

据风险，并提供日志的统计分析能力，为项目过程管理提供支撑数据。日志内容包括天气、人员出勤、进度、施工内容、安全问题及措施等。

5.11.6 文档管理应为不同地区、不同单位提供针对性的文档目录、文档模板以及归档功能。

【条文说明】文档管理需要基于各地城乡档案馆备案要求提供文档目录，避免大量文档生成后，文档与地方档案馆不一致。文档模板需要提供符合国家及地区备案要求的文档模板，避免自动生成文档时，模板不一致，导致提交档案馆时反复校对。

5.11.7 专项方案管理应符合下列规定：

- 1 应支持创建专项方案，专项方案应支持上传资料文件，并可查看文件内容；
- 2 应支持专项方案信息输入危大工程系统，在危大工程中查看对应的专项方案；
- 3 应支持在危大工程未上传必要资料（如专项方案、专家论证报告、交底等资料）时阻止派发与危大工程绑定的任务单。

【条文说明】为解决传统方案停留在纸面的问题，专项方案可以进行线上存储，并支持专项方案与危大工程和任务单之间需建立绑定关系，能够满足专项方案不完善的情况下禁止派发任务单的要求。

5.11.8 技术管理子系统应实现对图纸、模型相关的解析、查看、批注、管理功能，并应符合下列规定：

- 1 应具有图纸、模型的上传、解析及在线查看功能。模型引擎应符合本规程附录 A.0.5（BIM 轻量化引擎的技术标准和性能标准）的规定，且模型导入/导出接口应符合《建筑信息模型应用统一标准》GB/T 51212；图纸引擎应符合本规程附录 A.0.6（图纸引擎的技术标准和性能标准）的规定，图纸解析接口应支持 DWG 格式按《信息技术 开放系统互连 基本参考模型》GB/T 9387 实现跨平台传输；
- 2 宜具有识别 dwg 图纸文件的图框和图签信息的能力，图签信息包括但不限于：图名、图号、子项、专业、图纸类型。
- 3 应具有在线标注、测量图纸的功能，并支持基于图纸评论的回复。
- 4 应具有支持用户确认图纸有效性及下发至指定组织的功能，系统应记录不同版本图纸对应操作的时间、人员等信息。
- 5 宜具有显示不同版本图纸之间差异的功能。

【条文说明】本条对图纸、模型中相关的功能做了规定。图纸、模型是项目中的重要文件，为提升其管理效率，需要将其上传、解析，并为用户提供在线查看、测量、标注等功能，为此需要有专门的图纸、模型引擎。而图框图签信息能指征图纸文件的图名、图号，其识别能提升图纸管理的自动化程度和准确性。

5.12 成本管理子系统

5.12.1 成本管理子系统应包括合约引擎、盈亏账本、变更签证等功能。

5.12.2 合约引擎应支持对单工序、多工序组合配置对应控制单价、控制工程量、控制产能要求，并在任务派发时提供预警、审批功能；宜从技术管理子系统自动读取对应任务项关联的作业交底、安全交底、规范图集、质量通病、安全风险等行业知识。

5.12.3 盈亏账本应实现单个任务允许超额派发、超额记工功能；提供实时数据以及历史数据查看，盈亏统计分析与统计报表等用户服务功能。宜满足拆分任务、推送工人记工实时获取盈亏数据并同时触发对应预警规则。

5.12.4 变更签证管理应包括创建单据、群聊沟通、立项申请和价款确认等功能，并应符合下列规定：

1 创建功能支持填写受影响施工方、施工区域信息以及施工项等信息，及上传附件、并可由图纸管理子系统中获取图纸信息。

2 应支持群聊沟通过程信息留存和归档，并与对应单据关联；

3 立项申请功能应提供跨组织和跨层级的审批、存证，应支持线上电子签章。电子签章应符合附录 A.0.1（电子签名和印章应符合表）的规定；

4 价款确认功能支持上传变更签证影响的进度款项计算依据、签证费用明细、相关计价凭证等资料，为价款核算与确认提供依据。

【条文说明】变更签证的创建、群聊洽商、立项申请和价款确认属于建设工程施工现场的过程管理信息，为避免变更带来的纠纷，需要提供整个生命周期的管理、存档、存证功能。本条对变更签证功能进行说明：（1）变更签证的创建功能一般包括发起方、受影响的施工方、佐证材料、施工区域信息以及施工任务项等信息。提报内容一般需要由发起方填写，佐证材料和申请材料宜支持文档、图片，提报内容应不支持修改，避免经办方前后内容不一致，造成各方经济损失。（2）

变更签证的群聊洽商过程一般包括线上即时通讯沟通，沟通过程的各方意见可以统一留存，避免处办方前后沟通不一致，造成反复沟通、渎职等管理事故。（3）变更签证的立项申请，需要支持多组织的签证审批和存证，多组织一般包括项目内的施工单位、监理单位、设计单位、勘察单位、专业分包单位和劳务分包单位等单位，需要支持统一流程处办，避免各单位分别处办，从而给施工现场管理协同造成困难，签字方式需要采用线上电子签章的方式实现。（4）变更签证的价款确认过程，需要支持多组织的审批和存证，多组织一般包括项目内的施工单位、监理单位、设计单位、勘察单位、专业分包单位和劳务分包单位等单位，需要支持统一流程处办，避免各单位分别处办，从而给施工现场管理协同造成困难，签字方式需要采用线上电子签章的方式实现。需要提供进度款项的关联管理，可根据实际项目需要对关联事项内容进行扩展。

6 系统运行环境

6.1 一般规定

6.1.1 系统运行环境应包括网络、应用服务器、计算与存储设备、数据库、显示设备、从业人员实名制监管数据采集设备、视频监控设备、业务应用系统软件、业务中间件软件、安全保障设备等。

【条文说明】系统运行环境是整个业务系统运行所需要的软硬件环境，包括提供数据传输通道的网络环境，运行业务系统的应用服务器，处理数据运算与持久化的计算与存储设备；业务数据存储的数据库；从业人员信息采集和身份核验的从业人员实名制监管数据采集设备；提供系统间通信及服务集成能力的业务中间件；防护网络攻击与数据泄露的安全保障设备（含防火墙、入侵检测系统）等。

6.1.2 系统运行环境应由明确的组织或角色负责，确保环境满足系统运行要求。

【条文说明】系统运行环境需要由运维、DBA 和业务系统研发人员共同负责管理和维护，确保运行环境正常运行。

6.1.3 系统运行环境应满足预期的性能指标要求，系统所使用的设备应完全符合系统建设的设计规格与容量需求。

【条文说明】系统运行所需的基础资源（包括 CPU、内存、磁盘存储）及网络组件（带宽、CDN 服务、操作系统等），必须满足业务负载对计算能力、存储容量与流量吞吐的性能要求。

6.1.4 系统运行环境应采用云架构。非云架构下的系统应向云平台升级迁移，由云服务提供商负责底层资源的管理，可以是公有云、私有云或混合云。

【条文说明】系统部署在云上，硬件维护、网络带宽分配、物理安全等基础设施管理由云厂商提供管理能力，借助云厂商的管理平台，结合虚拟化、容器化技术进行资源管理、分配和回收。

6.1.5 系统应具有向下兼容性。低版本系统的数据应能无损迁移到高版本系统。

【条文说明】系统任何一次需求上线，版本升级迭代，系统需要自动进行业务流程和数据兼容处理，不影响升级之前发布的功能使用。

6.2 网络环境

6.2.1 网络环境应符合国家现行有关标准的规定，且应具有开放性、可扩充性、可靠性和安全性。

【条文说明】网络基础架构须严格遵循国家现行标准（如网络安全等级保护要求），确保开放性（支持多系统异构集成）、可扩充性（预留物理/逻辑扩容接口）、可靠性（冗余设计与故障容错）及安全性（数据传输加密与访问控制）。

6.2.2 系统应采用具备高度可扩展性和平滑演进能力的组网方案，应支持多种网络拓扑结构的适配。在扩展硬件环境时，应支持从最小配置到最大容量的无中断或低影响扩容。

【条文说明】组网方案需要具备拓扑灵活性，既支持云上以 VPC 为核心划分业务域的组网方式，也能适配本地化部署。在硬件扩容时需要实现无缝升级，避免因容量增长导致业务中断。

6.2.3 用于从业人员实名制监管数据采集设备总带宽应不低于：上行 20M，下行 100M。在专网环境上下行带宽应不低于 50M。

【条文说明】针对从业人员实名制监管场景，数据采集设备带宽设定依据业务特性差异化配置。

6.3 数据采集设备

6.3.1 数据采集设备应覆盖施工现场的人员、机械设备、环境、安全与材料等要素，并应支持统一接入数字化施工管理系统。

【条文说明】数据采集设备是智慧工地的前端感知层，覆盖施工全过程关键对象，确保数据真实、全面，并为后端分析与决策提供依据。

6.3.2 人员数据采集设备应符合以下规定：

1 设备应支持人脸识别、身份证识别及考勤计量功能，并与实名制管理系统实时传输数据；

2 设备应支持定位功能或者应具备定位模块扩展；

3 设备应支持自检功能或者具备自检模块扩展接口；

4 设备应满足户外使用环境要求，工作温度范围-10℃～60℃、湿度范围0%～90%，防护等级不低于 IP65，盐雾等级不低于 RP6，防爆等级不低于 IK06，具备防腐蚀、防爆、防尘、防潮能力；

5 设备的身份证识别、人脸认证识别准确率不低于 99%，人脸认证应支持活体检测，具备防伪造能力（如防照片、视频、3D 面具），并适配眼镜、口罩、安全帽、光照等因素。人脸识别系统应符合附录 A.0.4（人脸识别应符合表）的要求。

6 设备应支持不少于 1000 人并发认证，身份识别数据与考勤计量数据应实时互通；

7 设备应具备本地存储、备份和恢复功能，本地容量不少于 10000 张人脸图像和 50000 条记录；

8 设备应支持远程终端控制、管理端参数配置、状态查看和数据调取，支持在线升级功能（固件、算法、参数）；

9 数据传输应支持 TCP/IP 通信、HTTPS 协议和 JSON 格式，实时照片上传延时不超过 10 秒，考勤数据应支持脱机存储 ≥ 3 天并自动补传；

10 设备平均无故障时间不低于 10000 小时，应支持访问控制和基于角色的权限管理；

11 设备应生成、存储和查看系统日志，记录所有数据读写和操作行为，包括时间、操作人、操作类型；

12 设备应安装于人员进出场出入口，并能与门禁装置联动。

【条文说明】从业人员实名制设备是人员管理的核心，要求涵盖硬件可靠性、环境适应性、身份识别准确性及系统安全性，确保实名制管理落地执行。设备监测可防止因违规操作或设备故障引发的安全事故，其中塔吊、施工升降机等大型设备的监测数据接口需符合《信息安全技术—工业控制系统信息安全分级规范》GB/T 36324，确保设备与系统间数据传输的实时性（延迟不超过 1 秒）与安全性（采用 SM4 加密算法）；车辆管理设备的识别数据接口需符合《物联网 系统接口要求》GB/T 35319，支持车牌号、装载情况等数据以 JSON 格式实时上传。

6.3.3 机械与车辆数据采集设备宜符合以下规定：

1 塔吊、施工升降机等大型机械设备宜配置运行监测装置，采集吊重、风速、倾角、限位等指标，并与数字化施工管理系统实时互通；

2 施工车辆宜配置车辆识别与监测设备，采集车牌号、进出时间、装载情况等信息。

【条文说明】设备监测可防止因违规操作或设备故障引发的安全事故。车辆管理

设备有助于控制施工物料运输秩序，减少超载和违规运输。设备监测可防止因违规操作或设备故障引发的安全事故，其中塔吊、施工升降机等大型设备的监测数据接口需符合《信息安全技术—工业控制系统信息安全分级规范》GB/T 36324，确保设备与系统间数据传输的实时性（延迟不超过 1 秒）与安全性（采用 SM4 加密算法）；车辆管理设备的识别数据接口需符合《物联网 系统接口要求》GB/T 35319，支持车牌号、装载情况等数据以 JSON 格式实时上传。

6.3.4 环境数据采集设备应符合以下规定：

1 施工现场应配置环境监测设备，采集扬尘、噪声、气体浓度、温湿度等指标；

2 环境监测设备宜与喷淋、降噪装置联动，并在超标后自动预警与处置。

【条文说明】环境监测满足绿色施工与环保监管的要求。自动联动有助于提升环境治理的及时性和智能化水平。

6.3.5 安全数据采集设备应符合以下规定：

1 视频监控设备应覆盖施工现场出入口、重点作业面和危险区域，并应支持与 AI 识别系统联动。

2 视频监控设备宜实现对安全帽、反光衣佩戴情况的自动识别与报警。

【条文说明】视频监控是安全监管的重要手段，AI 分析可提升自动化识别能力。AI 监测可提前发现违规行为，减少人为疏漏。

6.3.6 材料数据采集设备宜符合以下规定：

1 材料进出场宜采用 RFID、二维码等识别设备，采集物料批次、来源、检测报告等信息；

2 材料采集设备宜与质量管理子系统数据互通。

【条文说明】材料设备保障质量可追溯，减少使用不合格材料的风险。与仓储系统联动可形成材料进出、存储、使用的完整闭环。

6.3.7 数据集成与接口应符合以下规定：

1 数据采集设备应支持与数字化施工管理系统的统一接入，并具备跨设备、跨厂商的互联互通能力，接入接口应符合《物联网 系统接口要求》GB/T 35319 中关于设备注册、数据上报、指令下发的规范；

2 数据采集设备传输的数据应采用统一的数据格式与通信协议，宜采用 JSON、MQTT、OPC UA 等标准协议，协议实现应符合《物联网 系统接口要求》

GB/T 35319 的相关技术参数；

3 塔吊、施工升降机等工业级机械设备的监测接口，应符合《信息安全技术—工业控制系统信息安全分级规范》GB/T 36324 中关于设备数据加密、访问控制的要求，防止数据传输过程中被篡改或泄露；

4 数据采集设备宜具备边缘计算能力，对采集数据进行预处理，并支持将结果与原始数据一并上传；

5 数据采集设备应支持远程统一管理，包括设备状态监控、固件升级、配置调整及安全策略下发。

【条文说明】不同厂商的设备类型众多，统一接入要求可做到数据互通，提升系统扩展性。同时，采用标准协议便于快速对接，降低系统集成和运维成本。

7 系统运维

7.1 一般规定

7.1.1 系统运维应符合现行国家标准《信息技术服务运行维护第 1 部分：通用要求》GB/T 28827.1 的有关规定。

7.1.2 系统运维应包括用户管理、系统监控、日志管理、数据更新维护、数据备份恢复、数据库灾备管理。

7.1.3 系统运维应制定标准运维流程，并明确负责的组织或角色。针对不同的运维对象，宜制定不同的运维流程。

7.1.4 系统运维标准流程应满足可执行、可量化、可追溯的要求。

【条文说明】系统运维需要细化成不同的模块，针对每个模块，需要分别制定标准操作流程（SOP）和操作规范，明确责任主体。同时，必须实施严格的权限管控，确保无权限人员无法执行运维操作。所有运维操作均须完整记录日志，并确保日志在指定周期内可长期追溯，以便在出现问题时进行精准回溯定位。

7.2 系统监控

7.2.1 系统监控内容应覆盖资源使用情况监控（CPU 使用率、内存使用率、磁盘空间），流量监控，可用性监控，稳定性监控以及调用链监控。

7.2.2 系统监控应有告警机制，按告警紧急程度分类分级，并基于级别设置告警规则。

7.2.3 系统监控应覆盖应用系统、数据库、服务器、网络和存储设备。

【条文说明】在系统的运行过程中，需要通过监控工具对系统的运行状态进行全面的监控，监控内容覆盖硬件、网络、应用程序及安全事件维度，实时采集 CPU 使用率、内存使用率、磁盘空间、网络带宽、业务接口可用性与稳定性指标。监控系统自动触发异常告警，通过短信、邮件或 App 推送通知研发人员和运维人员。

7.3 日志管理

7.3.1 系统应记录所有关键操作的日志，包括用户行为日志、系统运行日志、业务操作日志、设备接口日志。

7.3.2 系统日志应分为三种类别，包括审计日志、业务日志、运行日志，不同的类别应分类存储。

7.3.3 系统日志宜分为四种等级：致命、错误、警告、信息，为不同等级日志制定差异化的应急响应机制，明确各等级对应的处置时效、动作流程及责任主体。

7.3.4 系统日志宜用集中式日志平台统一采集、存储、查看、管理和分析。

7.3.5 系统日志备份保留周期宜符合：业务日志不少于一年，审计日志不少于半年，运行日志不少于 30 天，且应与数据库备份周期协同匹配。

【条文说明】系统日志是记录运行状态和操作行为的关键数据，对故障追溯与安全审计至关重要，需通过日志管理系统统一收集、归类和分析，并确保其完整性，防止未经授权的篡改。日志应实时生成并分类存储，以支持高效的后期审计和故障排查。对于关键操作及安全事件，系统应自动触发预警并通知运维人员。

7.4 数据库备份与恢复

7.4.1 数据库备份内容应包括结构定义、全量数据、增量数据、触发器、存储过程、用户权限信息等关键内容。

【条文说明】数据库备份与恢复是保障系统数据安全与业务连续性的核心措施。为确保数据的完整性与可靠性，备份内容应涵盖所有关键数据元素，必须包括表结构、全量数据、增量数据、存储过程、触发器和用户权限等。

7.4.2 数据库应支持全量备份、增量备份、日志备份，并能根据业务需求配置备份策略；数据库全量备份周期应与日志备份周期保持协同，确保数据恢复时可结合日志实现精准的时间点恢复。

【条文说明】备份策略需要具备灵活性，支持全量备份、增量备份及日志备份，并允许根据具体业务需求配置不同的备份频率和策略。

7.4.3 数据库备份应具备周期性自动执行机制，支持每日/每周/每月自动计划备份，并具备失败重试及异常告警机制。

【条文说明】备份过程必须具备周期性自动执行机制，确保数据按时备份，并具备失败重试及告警功能，及时发现问题。

7.4.4 数据库备份数据应存储在独立存储设备或备份服务器上，与生产数据库的存储资源隔离。

【条文说明】备份数据必须存放在独立的存储介质或备份服务器上，避免与生产环境共用存储资源，从而保证数据的安全性和恢复的可靠性。

7.4.5 数据库应支持基于时间点恢复的能力。

【条文说明】基于时间点恢复功能的支持能够确保在数据损坏或丢失的情况下，根据备份数据恢复到指定的历史时刻，确保系统恢复到业务正常状态，减少数据损失。

7.5 数据库灾备管理

7.5.1 数据库应部署主备架构或高可用集群架构，支持故障自动切换，保障业务连续性。

【条文说明】鉴于数据是核心资产，为避免数据丢失或系统崩溃引发重大业务中断，系统需要采用高可用技术架构，确保在故障发生时能快速切换，保障业务连续性。

7.5.2 灾备系统应至少包含两个异地备份副本，位于不同可用区或物理位置，防止地域性故障导致数据不可用。

【条文说明】灾备系统必须配置至少两个异地备份副本，分别存储于不同可用区或物理位置，以规避自然灾害、网络中断等区域性故障导致的数据不可访问风险。

7.5.3 数据恢复应设定明确的恢复目标：RTO（恢复时间目标）不超过 6 小时；RPO（恢复点目标）不超过 1 小时。

【条文说明】为确保灾难恢复效果，需要明确设定恢复时间目标（RTO）和恢复点目标（RPO），如：RTO 不超过 6 小时，RPO 不超过 1 小时，避免系统长期中断或数据严重丢失。

7.5.4 系统宜每半年进行一次数据库灾备演练，内容包括数据恢复验证、主备切换测试、故障模拟；演练后应形成评估报告，明确演练中发现的问题及整改措施，并跟踪整改落实情况，持续优化灾备方案。

【条文说明】需要每半年执行一次灾备演练，涵盖数据恢复验证、主备切换测试及故障模拟等内容，以检验灾备方案的可行性和操作流程的有效性。

7.5.5 灾备环境应与生产环境保持版本、结构一致，在切换时数据库能无缝衔接业务系统。

【条文说明】为实现业务系统在灾备切换时的无缝衔接，灾备环境需要与生产环境在版本和数据结构上保持一致。

7.5.6 灾备系统应具备实时或准实时同步机制，确保数据一致性。

【条文说明】数据库系统需要采用实时或准实时同步机制，如 binlog 同步或逻辑复制，以保障主备数据的一致性。

7.6 数据更新维护

7.6.1 系统应建立数据更新审批机制。所有数据更新应经过审批同意后进行，并应对数据更新结果进行检查。

【条文说明】数据更新维护是保证系统数据准确性、完整性和安全性的关键措施。为确保更新操作不影响系统稳定性，所有数据更新必须经过严格的审批流程，避免未经授权的修改，并明确每次更新的责任人和批准人。此外，更新完成后需对结果进行验证检查，确认更新成功且未对系统功能产生负面影响。

7.6.2 系统数据变更宜在非主要业务时间进行。技术支持人员应按预先方案进行测试验证，验证通过后，走正式审批流程后执行变更操作。

【条文说明】为最大限度减少对业务运营的影响，数据更新操作安排在非高峰时段执行，严格规避业务高峰期进行可能增加系统负载的操作。技术支持人员执行更新前，需要按预定方案完成充分的测试验证，确保变更可正确执行并达成预期效果；验证通过后，方可提交正式审批。

7.6.3 系统的数据更新应进行日志记录，各操作过程应具有可追溯性。

【条文说明】为了保证操作的透明性和追溯性，系统需要对每一次数据更新操作进行详细的日志记录，确保每一项操作都能够追溯到具体的人员和时间。此举不仅有助于问题的追踪和排查，还能为系统维护提供重要的审计依据。

8 系统安全

8.1 一般规定

8.1.1 系统网络安全要求应通过安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心以及安全管理制度等方面保障系统安全，满足现行国家标准《信息安全技术 网络安全等级保护基本要求》GB/T 22239 中三级等保的安全控制项要求，各子系统应根据数据敏感度与业务重要性分级落实安全防护，具体应符合下列规定：

1 涉及核心敏感数据的子系统（含实名制管理子系统、发薪管理子系统、成本管理子系统），应按等保三级要求建设，重点强化数据传输加密、访问权限管控及操作日志审计，保障人员身份信息、工资专户数据、成本合约数据的安全性；

2 涉及业务流程管理的子系统（含任务管理子系统、质量管理子系统、安全管理子系统、进度管理子系统、进出场管理子系统、记工管理子系统），应按等保三级要求建设，聚焦业务数据完整性校验、操作行为追溯及风险预警能力，确保施工任务、质量安全、人员考勤等核心业务流程可控可追溯；

3 涉及常规信息交互的子系统（含评价管理子系统、技术管理子系统），应按等保二级要求建设，落实基础安全防护措施，包括账户密码复杂度管控、常规数据备份及基础访问控制，满足非敏感业务的安全管理需求。

8.1.2 系统应按照国家标准《数据安全技术 数据分级分类规则》GB/T 43697 中的有关规定，对系统收集、存储、处理、传输的信息数据进行分级分类，识别核心数据、重要数据、一般数据，并对不同级别的数据进行分级保护。

8.1.3 若系统涉及处理国家秘密信息，应严格遵守相关的国家安全保密管理规定，建立完善涉密信息系统分级保护制度，实施物理隔离、严格的访问控制、身份鉴别、审计追踪等专项保护措施。

【条文说明】国家实行网络安全等级保护制度，因此系统必须满足对应等保定级的相关安全控制项（安全物理环境、通信网络、区域边界等）要求。国家建立数据分级分类保护制度，因此系统首先需要对数据进行分类分级，然后建立相应的数据安全保护措施。存储、处理国家秘密的计算机信息系统（以下简称涉密信息系统）按照涉密程度实行分级保护，因此系统必须实施相关安全保密措施。

8.2 网络安全

8.2.1 系统所在物理环境的安全保护应符合现行国家标准《电子信息系统机房设计规范》GB/T 50174 的有关规定，实施门禁监控、防火防潮、电磁屏蔽等物理防护措施。

8.2.2 系统网络架构应划分不同安全域，安全域边界应实施访问控制和入侵防护。

8.2.3 系统应采用访问密码、数字证书等方式，进行统一身份认证，实现分权分域管理。

8.2.4 系统应实施统一安全管理，对网络设备和安全事件进行集中监测、监控及审计，存储时间不少于六个月，并对资产管理、漏洞与风险管理、网络和系统安全管理、密码管理、备份与恢复管理、安全事件处置等做出明确规定。

【条文说明】《电子信息系统机房设计规范》GB/T 50174 将机房分为三个等级，系统需要按照对应级别要求，实施相应的机房安全措施。按照《信息安全技术 网络安全等级保护基本要求》GB/T 22239，系统需要划分不同安全域，并在边界实施访问控制与入侵防护。需要实施身份标识和鉴别技术，同时针对建筑工程的多角色场景，增强统一身份认证与分权分域管理。需要集中监测、集中管控系统网络安全风险，按照《中华人民共和国网络安全法》要求，相关日志存储时间不得少于 6 个月。需要制定资产管理、漏洞和风险管理等一系列管理制度要求。

8.3 数据安全

8.3.1 系统在处理个人信息时应符合国家标准《信息安全技术 个人信息安全规范》GB/T 35273 的有关规定，规范个人信息收集、存储、处理、共享及销毁，对于安装的图像采集、个人身份识别设备，应设置显著的提示标识。

8.3.2 系统应实现关键数据增量备份和全量数据定期备份，并至少每半年开展一次备份恢复演练，留存验证记录报告；对于核心业务数据，可根据数据重要程度适当提高演练频率。

【条文说明】系统作业场景中涉及对个人信息进行处理，因此需要符合国家标准《信息安全技术 个人信息安全规范》GB/T 35273 的有关规定。系统发薪、监管等作业场景中存在数据共享行为，因此按照国家标准要求，对共享的评估、告知、责任约定、安全保护等进行明确要求。

8.4 安全保密

8.4.1 系统密码应用应满足现行国家标准《信息安全技术 信息系统密码应用基本要求》GB/T 39786 的有关规定，优先采用国产密码模块，禁止使用已知存在漏洞的密码算法，涉及使用的商用密码技术，应遵循国家密码管理部门相关规定。

8.4.2 涉密系统与非涉密网络应实行物理隔离，涉密文件、资料、数据不得进入国际互联网传播或存储，确需与企业网络连接的，应制定和采取相应的安全技术措施，确保系统的安全。

【条文说明】系统作业场景涉及传输加密、存储加密，因此相关密码使用需要满足国家相关标准，以及商用密码管理要求，且禁止使用已知存在漏洞的密码算法。如系统涉及处理涉密信息，则需要做好涉密与非密环境的物理隔离，以及安全导出控制。

附录 A 基础能力要求

A.0.1 电子签名和印章应符合表 A.0.1 的规定：

表 A.0.1 电子签名和印章的技术标准和性能标准

序号	一级分类	二级分类	要求
1	技术标准	安全性	应采用加密算法保证电子签名的安全性。签名过程中应生成不可篡改的数字指纹，确保签名内容的完整性。
2		认证机制	电子签名应结合实名认证技术，确保签名人员的身份真实可靠并且配合身份验证系统双重认证，如银行卡认证、身份证认证、面部识别等多重验证措施。
3		法律效力	电子签名应符合相关法律法规，如《中华人民共和国电子签名法》规定，能够在法律上与传统手写签名具有同等效力。
4		存证机制	应支持多种文件格式（如 PDF、Word、Excel 等）的签署，并能够有效保存签署过程的时间戳、签署人信息等日志记录，以便后续审计。
5	性能标准	响应时间	用户发起电子签名请求到签名完成的响应时间不应超过 2 秒；在并发场景下（例如每秒 100 次请求），响应时间不应超过 3 秒。
6		吞吐量与并发处理能力	系统应支持至少 100 个并发用户请求，且在高负载下仍能保证稳定签名处理；系统每天应能够处理 1 万次签名请求。

【条文说明】电子签名和印章具备不可篡改、可追溯的特性，能够提高文件签署过程的效率与透明度，减少纸质文件带来的时间和空间限制。故需要规定电子签名和印章的生成、存储、验证等环节都应符合行业标准和法律要求，确保其在法律诉讼中具备法律效力，并且签名过程要有详细的审计日志记录。

A.0.2 电子证照应符合表 A.0.2 的规定：

表 A.0.2 电子证照的技术标准和性能标准

序号	一级分类	二级分类	要求
1	技术标准	数字化存储	电子证照应按照标准格式进行数字化存储，确保证照的完整性和不可篡改性。支持 PDF、JPG、PNG 等常见文件格式。
2		验证机制	应采用电子签名、二维码等验证手段，确保证照的真实性和有效性，并且支持扫码、在线验证等方式对证照进行即时验证。
3		安全性	电子证照的存储和传输过程中应使用加密技术，确保其不被未经授权的人员篡改或泄露。

4		存储机制	证照数据应加密存储,所有存储的数据应符合政府或行业标准的存储与管理要求(例如数据加密存储,定期备份)。
5	性能标准	响应时间	在网络正常的情况下,1MB 以内证照图片上传、下载请求的响应时间应小于 1 秒。
6		数据一致性	系统应保证数据的一致性和实时性,所有证照数据的更新与修改必须实时同步到所有查询端,支持至少 99.9%的数据一致性保障。
7		吞吐量与并发处理能力	系统应支持大规模证照数据的存储和检索,确保在高并发情况下,系统能够稳定运行,快速响应用户查询。应支持多用户并发访问、下载和验证,保证证照的实时性与可用性。

【条文说明】电子证照能将传统的纸质证照数字化,便于存储、查询和验证,同时能避免纸质证照丢失或损毁的风险。故需要规定电子证照的存储、传输和验证过程必须经过加密保护,并且具备自动化的验证和查询能力,以确保证照信息的安全性、准确性和及时性。

A.0.3 区块链存证应符合表 A.0.3 的规定。

表 A.0.3 区块链存证的技术标准和性能标准

序号	一级分类	二级分类	要求
1	技术标准	双层区块链结构	底层为公链,主要负责存储数据的哈希值等不可变记录;上层为私链,负责存储具体的数据内容。通过这种双层结构,能够有效减轻公链的负担,提升系统处理高并发事务的能力。
2		共识机制	选择适合高并发、高吞吐量的共识机制,以提升系统的交易处理速度。
3		数据存证	区块链应能够存储施工过程中的关键数据,如工程合同、审批文件、施工日志、质检记录等,确保数据不可篡改,且可追溯。
4	性能标准	响应时间	区块链存证请求的响应时间应不超过 5 秒,包括数据提交、区块生成及确认等过程。双层区块链结构的交易确认时间应不超过 30 秒。
5		吞吐量	系统应能处理至少 1000 笔交易/秒,满足高并发场景下的交易存证需求。高峰时段(如大型项目验收期),系统应支持至少 1,000,000 次存证请求。
6		高并发处理	双层区块链架构应支持高并发环境下的交易提交和确认,支持在 1,000,000 交易的高峰期依然稳定运行。

【条文说明】区块链存证能够保障数据在传输和存储过程中的安全性。故需要规定系统应采用双层区块链结构来应对高并发和大数据量场景,确保每一笔存证数

据的完整性、透明性和合法性，且能够支持系统内部和外部数据的无缝对接和验证。

A.0.4 人脸识别应符合表 A.0.4 的规定。

表 A.0.4 人脸识别的技术标准和性能标准

序号	一级分类	二级分类	要求
1	技术标准	识别精度	系统应具备较高的识别精度，能够在不同光照、角度、距离下准确识别人员身份。误识率应低于 1%，拒识率应低于 1%。
2		多场景适应能力	应支持不同场景下的人脸识别，包括施工现场的远程身份验证、进出门禁的考勤记录等。
3		实时性	系统应支持实时识别，并且在秒级时间内完成比对与识别，并快速反馈结果。
4		数据隐私与安全性	人脸数据应加密存储；系统应具备访问控制，确保只有授权用户才能访问和使用人脸数据。
5	性能标准	响应时间	人脸识别过程中的验证时间应小于 1 秒，包括采集、识别及验证的整个过程。系统应支持 100 个并发识别请求，并保证每个识别请求的响应时间不超过 2 秒。
6		识别准确率	人脸识别的准确率应不低于 99%，识别错误率控制在 1%以下。系统应支持多种环境下的识别，包括弱光、遮挡和不同角度等，确保识别准确性。
7		吞吐量	系统应能支持至少 100 个并发识别请求，并能够在全网高并发的情况下进行稳定处理。

【条文说明】人脸识别能够通过生物特征进行精准验证，减少人为操作的误差，提升身份认证的安全性。故需要规定人脸识别系统应具备高准确率、高并发能力和抗干扰能力，确保在不同光照、角度和背景下都能实现稳定识别，且能够快速响应，提供良好的用户体验。

A.0.5 BIM 轻量化引擎应符合表 A.0.5 的规定。

表 A.0.5 BIM 轻量化引擎的技术标准和性能标准

序号	一级分类	二级分类	要求
1	技术标准	多平台支持	BIM（Building Information Modeling）轻量化引擎应支持 Web、移动端等多平台。
2		文件格式支持	支持 IFC、RVT、NWD 等常见的 BIM 文件格式，并能够对其进行有效加载、渲染和交互。
4		存储与压缩	BIM 数据应进行压缩存储，确保在云环境下能够高效存储和快速访问。

5	性能标准	响应时间	BIM 模型（模型大小 500M 以内）的加载时间应小于 30 秒。
6		吞吐量与并发处理	系统应能支持至少 1000 个并发用户查看 BIM 模型。

【条文说明】BIM 轻量化引擎能够将传统的重型 BIM 文件转化为适合快速浏览和分析的轻量化模型，方便多方协同工作。故需要规定 BIM 轻量化引擎必须具备较高的文件加载和渲染速度，能够支持大规模项目的数据处理，确保在不同终端和网络条件下都能流畅展示，提升设计人员的协同效率和决策能力。

A.0.6 图纸引擎应符合表 A.0.6 的规定。

表 A.0.6 图纸引擎的技术标准和性能标准

序号	一级分类	二级分类	要求
1	技术标准	图纸格式支持	应支持常规工程图纸格式，如 DWG 等，并能够进行图纸的查看、批注等操作。
2		图纸结构化识别	支持图纸识别图框以及图签内容。识别准确率应不低于 98%。
3		图纸比对功能	能够支持不同版本图纸的比对，自动标识出差异
4		文件管理与存储	图纸文件应支持压缩和分割存储，以便高效管理大文件，并提供快速查找和提取功能。
5		唯一性标识	应设计对文件进行唯一标识命名，防止文件被覆盖和篡改。
6		数据一致性与协作	系统应具备图纸版本管理能力，确保历史版本的备份与恢复。
7		任务队列	应实现任务队列机制，防止大批量图纸解析任务同时运行导致系统负载过高，确保系统运行的稳定性。
8		监控机制	应建立实时任务监控机制，对超时未完成解析的文件及时进行超时处理并发出警告，确保解析服务的正常运行。
9	性能标准	响应时间	图纸（图纸大小 100M 以内）加载时间应控制在 5 秒以内，支持大规模图纸文件快速加载。图纸其它操作时其响应时间应不超过 2 秒，保证用户快速查看。
10		吞吐量与并发处理	系统应能够同时处理 5000 张图纸的查看。高并发访问下，系统应能够支持至少 100 个并发编辑操作，并保持性能稳定。

【条文说明】图纸引擎是支持建筑和工程图纸高效查看、标注和共享的重要工具，因为它能够确保图纸在不同设备上精准展示，方便项目成员进行协作和修改。故需要规定图纸引擎应支持常见的图纸格式，且具备快速渲染、精准标注和云端协

作功能，以使用户能够在任意时间、地点查看和编辑图纸内容，提高项目实施过程中的协同效率。

附录 B 数据合理性控制标准

B.0.1 任务单应符合表 B.0.1 的规定。

表 B.0.1 任务单风控标准

一级分类	二级分类	要求
真实性	关联单据	应可在合约清单中进行任务单的创建，提升创单效率。
	区块链存证	应通过区块链存证的方式防止任务单被任意方篡改，区块链存证的技术标准和性能标准应符合本规程附录 A.0.3 的规定。
完整性	层级完整	应为每个相关单位提供接单、拆单、派单、验收的基本功能。
	任务完整	应提供各工程类别、各项目阶段、各颗粒度级别的全部施工任务项，如从分部分项工程到工序。
	区域完整	宜提供各工程类别、各颗粒度级别的全部施工区域，如从单位工程到楼层、功能间，宜精确至部品部件。
合理性	施工区域	下级任务单的施工区域不应超过上级任务单。
	施工图纸	施工图纸应与施工区域对应。
	施工任务项	下级任务单的施工任务项不应超过上级任务单。
	交底	施工交底应与施工任务项对应。
	工期	下级任务单工期不应超过上级工期。
	履约对象	履约对象的经营范围、档期应与任务项对应。
	单价	应提供基于任务项的单价合理区间。
	预估金额	下级任务单的预估金额不应高于上级任务单金额。

B.0.2 记工单应符合表 B.0.2 的规定。

表 B.0.2 记工单风控标准

一级分类	二级分类	要求
真实性	关联单据	应建立记工单与其他业务单据的关联关系，通过单据的互相依赖提升创单效率。
	区块链存证	应通过区块链存证的方式防止记工单被任意方篡改，区块链存证的技术标准和性能标注应符合本规程附录 A.0.3 的规定。
完整性	层级完整	记工单应经过多方确权方能存证。
	要素完整	应确保记工单核心要素完整。
合理性	工作量	宜建立工作量与工种、考勤时长的关联关系。
	记工金额	应建立记工金额与工种、考勤时长、任务单金额的关联关系。

B.0.3 接口应符合表 B.0.3 的规定。

表 B.0.3 数据接口技术参数表

接口类型	适用场景	通信协议	数据格式	安全要求	响应时效	依据标准
政务平台对接接口	与住建、人社等监管平台数据交互	HTTPS	JSON	支持 OAuth2.0 身份认证, SM3 数据校验	≤3 秒	GB/T 45800
工业设备监测接口	塔吊、施工升降机等数据上传	MQTT/OPCUA	二进制/JSON	SM4 加密, 访问权限分级控制	≤1 秒	GB/T 36324
物联网设备接入接口	人脸识别终端、环境传感器	MQTT	JSON	设备证书认证, 数据传输加密	≤2 秒	GB/T 35319
BIM 模型交互接口	BIM 轻量化模型导入/导出	HTTP/HTTPS	IFC/RVT	模型文件哈希校验, 权限管控	≤30 秒 (500M 内)	GB/T 51212
子系统内部共享接口	任务管理→记工管理数据同步等	内部 API	JSON	接口调用日志记录, 数据一致性校验	≤1 秒	GB/T 9387

用词说明

为便于在执行本规程条文时区别对待,对要求严格程度不同的用词说明如下:

1 表示很严格,非这样做不可的:

正面词采用“必须”;反面词采用“严禁”;

2 表示严格,在正常情况下均应这样做的:

正面词采用“应”;反面词采用“不应”或“不得”;

3 表示允许稍有选择,在条件允许时首先这样做的:

正面词采用“宜”;反面词采用“不宜”;

4 表示有选择,在一定条件下可以这样做的,采用“可”。

引用标准名录

本规程引用下列标准。其中，注日期的，仅对该日期对应的版本适用于本规程；不注日期的，其最新版适用于本规程。

- 《信息安全技术 网络安全等级保护基本要求》GB/T 22239
- 《信息技术服务 运行维护 第1部分：通用要求》GB/T 28827.1
- 《信息安全技术 个人信息安全规范》GB/T 35273
- 《信息安全技术 数据安全能力成熟度模型》GB/T 37988
- 《信息安全技术 信息系统密码应用基本要求》GB/T 39786
- 《数据安全技术 数据分级分类规则》GB/T 43697
- 《电子信息系统机房设计规范》GB/T 50174
- 《建设电子文件与电子档案管理规范》CJJ/T 117
- 《信息安全技术—工业控制系统信息安全分级规范》GB/T 36324
- 《信息技术 开放系统互连 基本参考模型》GB/T 9387
- 《物联网 系统接口要求》GB/T 35319
- 《建筑信息模型应用统一标准》GB/T 51212
- 《全国一体化政务大数据体系第2部分：数据共享交换要求》GB/T 45800.1