 **T/CECS XXX-202X**

**中国工程建设标准化协会标准**

**建设工程试验检测管理信息系统技术规程**

**Techinical specification for management information system**

**of consruction engineering test and detection**

**（征求意见稿 ）**

**2021.10**

　　　　　　　　　　　　　　　**前　 言**

　　根据中国工程建设标准化协会《关于印发<2019年第二批协会标准制订、修订计划>的通知》（建标协字【2019】22 号）的要求，标准编制组经过深入调查研究，认真总结实践经验，参考国内外的有关标准，并在广泛征求意见的基础上，制定了本标准。

本标准共分9章，主要技术内容包括：1.总则； 2.术语；3.基本规定；4. 系统运行环境要求；5. 检验检测功能； 6. 日常管理功能；7. 系统质量特性要求；8. 系统安全要求；9. 系统验收与维护。

本标准由中国工程建设标准化协会检测与试验专业委员会归口管理，由北京市建设工程质量第三检测所有限责任公司负责具体技术内容的解释。在执行过程中如有意见或建议，请将意见和有关资料寄送北京市建设工程质量第三检测所有限责任公司（地址：北京市西城区百万庄大街3号；邮编：100037）以供修订时参考。

本标准主编单位：北京市建设工程质量第三检测所有限责任公司、北京市市政工程研究院。

本标准参编单位：贵州华岩试验检测技术有限公司、北京九通衢检测技术股份有限公司、湖南建研信息技术股份有限公司、北京智博联科技股份有限公司、广东鸿翔工程检测咨询有限公司、北京市道路工程质量监督站、北京市建设工程安全质量监督总站、北京轨道交通建设管理有限公司、北京市首都公路发展集团有限公司公路资产管理分公司、北京市城市道路养护管理中心、北京铁科工程检测有限公司、中国建筑科学研究院有限公司、中交路桥检测养护有限公司、国家电子政务系统质量监督检验中心（北京新国信软件评测技术有限公司）、北京建业通工程检测技术有限公司、中国合格评定国家认可中心、北京城市快轨建设管理有限公司、北京城市副中心站综合枢纽建设管理有限公司。

主要起草人：田春艳、李欣、郭晗、王军民、胡越胜、李金涛、刘野、张岚、方清华、王彤、胡隽、王晓东、田行宇、王建春、王国华、李海燕、梁志广、董雨明、沈孛、彭国荣、寇彦青、易小明、聂建成、袁艺匀、王璐、赵欣淮、孔梦妍、崔丽、李东海、张磊、郑德粮、游筱琳、胡运，刘江红、闫卫坡。

主要审查人：

目 次

[1　总则 1](#_Toc85037335)

[2　术语 2](#_Toc85037336)

[3　基本规定 3](#_Toc85037337)

[4 系统运行环境要求 5](#_Toc85037338)

[4.1 一般规定 5](#_Toc85037339)

[4.2 硬件配置 5](#_Toc85037340)

[4.3 软件产品 6](#_Toc85037341)

[4.4 网络体系结构 7](#_Toc85037342)

[5 检验检测功能 8](#_Toc85037343)

[5.1 一般规定 8](#_Toc85037344)

[5.2 委托/合同管理 9](#_Toc85037345)

[5.3 室内试验 10](#_Toc85037346)

[5.4 现场检测 11](#_Toc85037347)

[5.5 报告管理 12](#_Toc85037348)

[6 日常管理功能 15](#_Toc85037349)

[6.1 基本信息管理 15](#_Toc85037350)

[6.2 人员管理 15](#_Toc85037351)

[6.3 设备管理 16](#_Toc85037352)

[6.4 标准管理 18](#_Toc85037353)

[6.5 质量管理 18](#_Toc85037354)

[6.6 权限管理 19](#_Toc85037355)

[6.7 统计与查询 19](#_Toc85037356)

[7 系统质量特性要求 21](#_Toc85037357)

[7.1 系统性能要求 21](#_Toc85037358)

[7.2 系统可靠性要求 21](#_Toc85037359)

[7.3 系统易用性要求 21](#_Toc85037360)

[7.4 系统兼容性要求 22](#_Toc85037361)

[7.5 系统维护性要求 23](#_Toc85037362)

[8 系统安全要求 24](#_Toc85037363)

[8.1 系统安全总体框架 24](#_Toc85037364)

[8.2 物理安全 24](#_Toc85037365)

[8.3 网络安全 25](#_Toc85037366)

[8.4 应用安全 26](#_Toc85037367)

[8.5 数据安全 27](#_Toc85037368)

[9 系统验收与维护 29](#_Toc85037369)

[9.1 系统验收 29](#_Toc85037370)

[9.2 系统维护 29](#_Toc85037371)

[附录A 验收指标评分表 31](#_Toc85037372)

[附录B 系统运维指标 32](#_Toc85037373)

[本标准用词说明 34](#_Toc85037374)

[引用标准名录 35](#_Toc85037375)

附：条文说明 36

Contents

[1 General Provisions 1](#_Toc85037335)

[2　Terms 2](#_Toc85037336)

[3　Basic Requirements 3](#_Toc85037337)

[4 System Operating Environment Requirements 5](#_Toc85037338)

[4.1 General Regulation 5](#_Toc85037339)

[4.2 Hardware Configuration 5](#_Toc85037340)

[4.3 Software Products 6](#_Toc85037341)

[4.4 Network Architecture 7](#_Toc85037342)

[5 Inspection and Detection Function 8](#_Toc85037343)

[5.1 General Regulation 8](#_Toc85037344)

[5.2 Entrusting/ Contract Management 9](#_Toc85037345)

[5.3 Laboratory Test 10](#_Toc85037346)

[5.4 Field Test 11](#_Toc85037347)

[5.5 Report Management 12](#_Toc85037348)

[6 Daily Management Function 15](#_Toc85037349)

[6.1 Basic Information Management 15](#_Toc85037350)

[6.2 Personnel Management 15](#_Toc85037351)

[6.3 Equipment Management 16](#_Toc85037352)

[6.4 Standards Management 18](#_Toc85037353)

[6.5 Quality Management 18](#_Toc85037354)

[6.6 Authority Management 19](#_Toc85037355)

[6.7 Statistics And Query 19](#_Toc85037356)

[7 System Quality Characteristic Requirements 21](#_Toc85037357)

[7.1 System Performance Requirements 21](#_Toc85037358)

[7.2 System Reliability Requirements 21](#_Toc85037359)

[7.3 System Usability Requirements 21](#_Toc85037360)

[7.4 System Compatibility Requirements 22](#_Toc85037361)

[7.5 System Maintenance Requirements 23](#_Toc85037362)

[8 System Security Requirements 24](#_Toc85037363)

[8.1 System Security Overall Framework 24](#_Toc85037364)

[8.2 Physical Security 24](#_Toc85037365)

[8.3 Network Security 25](#_Toc85037366)

[8.4 Application Security 26](#_Toc85037367)

[8.5 Data Security 27](#_Toc85037368)

[9 System Acceptance And Maintenance 29](#_Toc85037369)

[9.1 System Acceptance 29](#_Toc85037370)

[9.2 System Maintenance 29](#_Toc85037371)

[Supplement A Acceptance Index Score Chart 31](#_Toc85037372)

[Supplement B System Operation and Maintenance Index 32](#_Toc85037373)

[Explanation of Wording in This Code 3](#_Toc28898)4

[List of Quoted Standards](#_Toc22867) 35

[Addition：Explanation of Provisions 36](#_Toc26358)

**1**总 则

1.0.1 为规范建设工程检验检测信息管理系统的开发、使用与维护，促进检验检测管理工作信息化，提高管理水平和效率，制定本规程。

1.0.2 本规程适用于建设工程检验检测机构应用的信息管理系统。

1.0.3 建设工程检验检测信息管理系统除应符合本规程外，尚应符合国家现行有关标准的规定。

**2**术 语

2.0.1 建设工程检验检测机构construction engineering test and detection organization

通过室内试验、现场检测等手段对在建工程进行质量检验与评定，或对既有工程、既有技术状态进行鉴定评估的机构。

2.0.2 建设工程检验检测信息管理系统 management information system for construction engineering test and detection organization

由计算机及其相关配套设备、设施（含网络）和软件构成，以实现建设工程检验检测机构获得的数据和信息（计算机及非计算机系统保存的）管理，具有根据建设工程检验检测管理规则对数据和信息进行采集、记录、报告、存储、传输、检索、统计、分析等处理功能。

2.0.3 项目 project

每个试验检测或监测项目，与委托或者合同一一对应，是委托或者合同流程的后续流程，用来上传及审批方案，并与数据集进行关联。

2.0.4 子项目subprojects

若项目较为复杂存在多个子项目或需要一个项目需要申请多个报告号时，可根据需要在工程处申请子项目，其与项目为隶属关系，但功能与项目相同，且每个子项目对应一个数据集。

2.0.5 权限 jurisdiction

指在信息系统中某一用户的访问级别和权利，包括所能够执行的操作及所能访问的数据。

2.0.6 冗余redundancy

指人为增加重复部分，其目的是用来对原本的单一部分进行备份，以达到增强其安全性的目的。

**3**基本规定

3.0.1 系统功能应能满足国家、行业、地方工程建设和主管部门对建设工程试验检测工作的相关规定。

3.0.2 建设工程检验检测机构宜根据自身规模、业务性质和管理模式等，建立或应用实用、可靠、高效的检验检测信息管理系统。

3.0.3 系统应具备检验检测业务流程管理、质量控制、资料电子化归档以及统计、分析等功能。

3.0.4 系统宜采用开放式的开发模式，使机构可根据自身情况增减、组合功能模块，基本框架见图3.0.4。

图3.0.4 系统框架示意图

3.0.5 系统应根据业务情况、人员架构及安全保密要求分级设置管理权限。

3.0.6 系统可在数据安全的前提下进行数据共享，并符合以下要求:

1 内部各功能模块之间实现充分的数据共享；

2 为工程建设或其他行业主管部门的管理平台提供可访问的接口；

3 与客户方的管理系统实现数据交互传输；

4 外部提交数据查询申请，经机构审批同意后方可进行；

5 需外部报送数据时，可提供符合报送要求的数据形式;

6 应根据需求设计数据共享接口，并符合国家现行相关标准的规定。

3.0.7 系统应能保证试验检测原始数据在上传后不被篡改、遗漏，应保证所有信息的输入、修改、删除以及异常情况处理过程均留有痕迹可以查询。

3.0.8 系统运行环境应符合国家信息安全保密管理的规定。

**4** 系统运行环境要求

**4.1 一 般 规 定**

4.1.1 系统的运行环境方案应根据处理能力、可靠性、响应速度、系统结构、数据管理方式等因素进行设计，运行环境应满足以下方面因素：

1 满足系统规模、数据容量、数据处理方式与速度、安全性要求以及系统的架构，由此选择系统硬件和外设配置，应具有通用性，并易于升级。

2 满足系统功能要求，由此选择系统软件配置。

3 满足用户量、数据分布和数据处理速度，由此选择系统网络配置。

4 技术上要求稳定可靠，同时也遵循投资少、见效快、立足现在并顾及将来发展的原则。

4.1.2 系统体系架构的选择宜符合下列要求：

1 工作地点集中、网络安全要求高、用户固定、数据维护量大的系统宜采用客户/服务器模式。

2 工作地点分散、网络结构复杂、客户端操作系统多样、用户分布面广且对数据编辑和分析要求不是很高的系统宜采用浏览器/服务器模式。

3 外部用户只需要检索、查询操作，内部用户需要发布、修改等交互性强的操作，系统宜采用浏览器/客户/服务模式。

4.1.3 系统的部署可根据实际情况选择自建服务器或云平台服务商，应按照《信息安全技术网络安全等级保护基本要求》GB/T 22239中规定的的第二级及以上要求进行自建服务器或选择云平台。

4.1.4 系统部署、运维的机房建设应符合《计算机场地通用规范》GB/T 2887中C级及以上要求，物理环境应符合《信息安全技术 信息系统物理安全技术要求》GB/T 21052中第二级物理安全技术要求。

**4.2 硬 件 配 置**

4.2.1 系统应包括计算机、服务器、交换机、数据存储设备与备份设备和不间断电源等硬件设备。

4.2.2 服务器硬件指标应符合《信息安全技术服务器安全技术要求》GB/T 21028中第二级及以上安全要求。

4.2.3 存储设备应具有良好的稳定性、扩充性和高传输速率。

4.2.4 系统主机资源，包括CPU、内存和存储系统等的利用情况，在事物处理高峰时应保持在总体资源满负荷的70%以下。

4.2.5 备份设备应具有灵活的备份和恢复策略，当系统出现意外损害时，应能快速及时地进行系统和数据恢复。

**4.3 软 件 产 品**

4.3.1 系统应包括操作系统软件、基础软件、应用服务器中间件、应用软件等软件产品。

4.3.2 操作系统软件既要与所选计算机服务器相匹配，又要支持所选系统基础软件。

4.3.3 系统基础软件应满足以下技术要求：

1 具有数据采集、输入、存储与管理和输出的功能；

2 具有构建拓扑关系及空间分析的功能；

3 具有良好的用户界面开发工具、支持汉字处理、具有二次开发功能；

4 具有良好的开放性、兼容性及与其他系统数据的可交换性；

5 性能可靠，软件技术支持服务号功能；

6 具有模块化或组件化功能和较高的性价比。

4.3.4 4.3.4 应用服务器中间件应满足以下技术要求：

1 满足对应用的部署、调试和卸载，能提供对系统性能进行监控和调优、日志管理的管理工具，宜提供支持Web组件开发的可视化集成开发工具；

2 可支持保证数据源恢复和保证事物一致性的系统故障恢复能力；

3 能对进出的网络数据流实时监控；

4 能对登录用户进行身份标识和鉴别；

5 支持访问控制功能，控制用户对服务器数据的访问；

6 不存在隐蔽接口，不加载能够禁用安全机制或绕过安全机制的组件。

4.3.5 应用软件应满足以下技术要求：

1 能与基础软件兼容或能以控制的方式连接；

2 可提供支持多种浏览器的插件；

3 能提供对文件进行加密的选项；

4 不存在隐蔽接口，不加载能够禁用安全机制或绕过安全机制的组件。

**4.4 网 络 体 系 结 构**

4.4.1 系统应根据网络拓扑结构、网络的逻辑设计、网络操作系统等因素进行选择网络环境，宜选用网络速度快、安全性高、可靠性高的计算机网络架构。

4.4.2 系统的网络体系结构方案设计宜包括以下内容：

1 产品选型、拓扑结构、基本部件与配件、传输介质、接口、通信协议、约束条件、结构化布线等方案；

2 画出网络结构图；

3 说明服务器/客户机的作用、配置和具体位置；

4 说明拟采用的网络安全保护技术，如防火墙等。

4.4.3 系统的网络设施应包括主要网络设备和主要安全设备。

**5** 检验检测功能

**5.1 一 般 规 定**

5.1.1 检验检测基本流程见图5.1。

图5.1 检验检测业务流程示意图

5.1.2 检验检测部分宜包含下列功能模块：

1 委托管理/合同管理；

2 收样管理/项目管理；

3 任务分配；

4 数据采集与记录；

5 数据处理与分析；

6 报告管理；

7 台账管理；

8 其他。

5.1.3 系统在数据采集过程应保证数据的原始性和真实性，并满足下列要求：

1 采用自动采集设备时系统宜设置数据接口，保证数据全程记录并点对点上传至系统服务器，不得存在中间存储或中转程序；

2 对采用自动采集设备且尚不具备直接上传的条件时，应使数据在采集设备中保存完好，由具有规定权限的检验检测人员向系统录入数据；

3 对非自动采集设备，应采用专用记录纸做好数据记录，应设置接口由具有规定权限的试验人员向系统录入数据，也可将纸质原始记录通过拍照、扫描等方式上传系统。

5.1.4 系统应建立数据库用于存储试验检测原始数据，保存年限应符合相关标准、规定的要求。根据实际情况可以采用服务器存储数据，也可以采用云存储的方式，但都应采取充分措施保证数据的安全。

5.1.5 系统应能自动筛查检验检测的不合格结果，生成不合格结果台账，并给与提示。

5.1.6 系统各个模块之间相关联的内容宜能互相链接，通过点击调阅相关信息。

5.1.7 当系统采用电子签名功能时，所有人员的电子签章均应按国家相关规定进行备案，电子签章与持有人应进行有效绑定，系统应设置流程防止签章被混用、盗用。

5.1.8 系统在委托单与合同拟定、方案编制、任务下发等阶段，自动筛查其中所列检测内容和标准依据是否在机构受控范围内，当发现超出范围时进行提示。

**5.2 委 托 / 合 同 管 理**

5.2.1 委托/合同管理模块宜包括合同审批、委托单办理、委托编号分配、收样管理、台账与资料管理、统计与查询等功能。

5.2.2 根据业务类型、项目规模、客户要求的不同，与客户签订的委托协议有委托单、合同等不同形式，系统可根据需求设置不同的管理流程。

5.2.3 系统应按机构对合同审批流程的规定设置审批环节，审批通过后方能签订正式合同。

5.2.4 委托单办理环节包括委托单填写、审核、打印、签订等，委托单的信息应至少包括：

1 委托单位名称与联系方式；

2 工程名称、样品或检测对象等基本信息；

3 试验检测内容、方法与依据的标准；

4 委托日期、委托人姓名；

5 承接人姓名、约检日期；

6 委托和承接方经手人签字与单位有效公章；

7 唯一性委托标识编码。

5.2.5 合同或委托单经各方确认无误后正式签署，可以应用电子签名，加盖双方机构电子公章；或线下签订协议，并加盖双方公章后扫描上传。

5.2.6 合同或委托单正式签署后，系统应自动生成台账并将相关电子资料归档，必要的纸质资料可扫描后上传。

5.2.7 委托单或合同签订后系统应具有自动分配和人工设置唯一性委托编号的功能。

5.2.8 系统宜收集委托或合同的相关信息建立信息档案，并对信息进行分析，包括客户类型、项目规模、检测内容、中标方式等。

5.2.9 系统在收样管理环节应实现下列功能：

1 登记工程信息和委托试验样品信息；

2 按照相关标准要求对样品性状核实检查，对符合要求的样品收样并分配唯一性的样品编号并与委托编号关联；对不符合要求的样品退回并在系统中留有相关记录；

3 宜能扫描识别样品上二维码或芯片信息。

5.2.10 登记工程信息和样品信息，包括以下内容:

1 工程信息应：工程名称、委托单位名称、工程属性、委托类别、施工许可证号、建设地址、所属监督站、报告类型等。

2 样品信息：委托单位、工程名称及部位、样品名称、规格（型号）、样品数量、样品状态、制造厂商（产地）、代表批次、保管方法、检测参数、依据标准、样品处置方式及备注信息。

5.2.11 经复核发现已收样品的信息需要修改，或需删除最终因某种原因未进行试验的样品记录时，应按照人员权限的规定，由指定人员完成，并应保留修改或删除的过程记录。

5.2.12 系统宜能够根据委托编号、工程名称、委托单位、委托人、委托时间、承接人等不同输入查询委托信息，并应能显示委托处理情况。

**5.3 室 内 试 验**

5.3.1 系统在收样环节完成后应进入任务管理环节，并符合下列要求：

1 根据收样信息自动生成任务单，任务单应按年度自动连续编号；

2 一个委托或者合同可根据试验内容的不同下达多个任务单；

3 任务单的信息应包括样品编号、样品数量、样品名称、规格（型号）、样品状态、检测参数、检测/评定标准、任务下达日期及留样方式等信息。

5.3.2 接收任务单的试验人员应对任务单内容确认并签字，完成任务接收后按照任务单的要求完成试验前准备、试验操作、数据采集与记录、数据处理等工作。

5.3.3 数据采集符合本标准5.1.3条的要求。

5.3.4 当经过规定流程核实电子记录确实有误需要修改时，核查人员应按原路径退回到数据提交人处进行检查，并应符合下列要求:

1 前一个版本的电子记录文件应保留；

2 改动后的信息应能清晰识别，且能追溯到改动前的信息，新增加的信息应能和原有信息区分开；

3 应清楚标注修改的理由，修改及批准修改人员的姓名、修改日期，相关人员应签名确认。

5.3.5 系统在数据处理环节应实现下列功能：

1 按照相关标准要求，在系统中为每个试验参数设定合格判别标准，应能根据试验结果自动判定是否合格；

2 试验数据的复核应在系统中按规定流程自动流转，当显示试验人与复核人为同一人时，系统应自动拒绝复核人员的电子签名；

3 为试验数据分配唯一编号。

4 建立数据集存放数据。

5.3.6 系统应对不合格结果进行提示并上报。

5.3.7 系统自动生成试验报告，并为报告分配唯一编号。

5.3.8 系统应能实时查看样品在各个环节流转的状态。

**5.4 现 场 检 验**

5.4.1 工程检测项目在委托工作结束后系统可自动进入项目管理环节，每个委托任务宜对应生成一个项目，并可根据工程规模、检测内容、工期长短及其他需求划分为若干子项目。

5.4.2 系统在项目管理模块应实现如下功能：

1 查看项目进展；

2 检验检测方案编辑或上传、审核与批准；

3 下发检测任务；

4 建立数据集，采集、分析数据；

5 检验检测报告编辑或上传、审核与批准；

6 资料归档。

5.4.3 系统应设置检验检测方案上传、审核、修改与批准的功能。

5.4.4 检测方案审批通过后方可进入任务下发阶段，并完成下列工作：

1 选定符合要求的检测人员；

2 选定检测设备并关联设备出库管理程序；

3 确定检测开始时间、预估完成时间；

4 下发任务单，包括工作内容、工作量和检测方法等信息。

5.4.5 检测人员接受任务单后领取检测设备，至检测现场采集数据，并按照本标准5.1.3条的要求将数据提交传输至系统。

5.4.6 当经过规定流程核实电子记录确实有误需要修改时，应符合本标准5.3.4条的要求。

5.4.7 系统应建立数据集，在确认当前任务已经没有新的数据上传或者资料需添加后，可以确认任务完成提交任务。任务提交后，该任务的所有数据、信息都将无法修改。

5.4.8 对于长期监测项目宜预先设定允许值，当实际数据超出允许值时系统应能给予提示。

5.4.9 系统宜能根据不同时间采集到监测数据进行统计分析，包括绝对值、变化值、变化速率等，做出数据随时间变化曲线、不同测点位置的数据曲线等。

5.4.10 当现场检测工作完成后，可编辑并上传检测报告。

**5.5 报 告 管 理**

5.5.1 报告管理环节可包含下列功能:

1设置不同类型报告模板，便于报告编辑；

2 报告审核、批准与签发；

3 报告查阅与下载；

4 建立报告台账

5 已发布报告变更与补发；

6 资料存档。

5.5.2 系统应为检验检测报告分配唯一性的编号，宜按年度连续编号。

5.5.3 系统宜为检验检测报告选择不同的资质标识，并与检验检测项目对应。

5.5.4 系统应按管理规定设置报告审核层级，并为不同类别报告指定各层级审核人，逐级审批报告。

5.5.5 报告各级审核人提出修改意见时，不宜直接修改报告，系统宜应用在线批注功能或采用其他形式将修改意见退回提交人，由提交人修改完成后再按规定流程重新提交审核。

5.5.6 室内试验报告应采用专用模式，宜包括下列内容:

1 报告名称；

2 委托方名称、工程名称、施工部位；

3 试样接收日期、试验日期及报告日期；

4 试样名称、生产单位、规格型号、代表批量；

5 试验依据及执行标准；

6 试验数据及结论；

7 必要的说明和声明等；

8 试验、审核、批准人等不少于三级人员的签名；

9 检测机构的名称、地址及通讯信息；

10 检测机构的有效印章及相关标识。

11 报告的编号、每页及总页数的标识；

12 其他说明。

5.5.7 现场检验检测报告应采用专用模式，宜包括以下内容:

1 报告名称；

2 委托方名称；

3 工程概况，包括工程名称、地址、结构类型、规模、施工日期与现状及以往检测、维护情况概述；

4 检测目的与检测内容；

5 检测方法、抽样方法与依据的标准；

6 检测数量、结构与构件部位；

7 检测数据、分析结果与检测结论；

8 检测日期、报告完成日期；

9 主检、审核和批准人员的签名；

10检测机构的名称、地址及通讯信息；

11 检测机构的有效印章及相关标识；

12报告的编号、每页及总页数的标识。

13 其他说明。

5.5.8 采用电子签名和电子印章时，审核人员审核认为报告无误后在系统进行电子签名，各级审核均完成后报告由系统加盖电子印章和相应资质标识，完成电子化的报告。

5.5.9 报告宜采用特殊水印、二维码、防伪纸或其他措施防伪。

5.5.10 系统应登记报告领取人姓名、领取时间和领取报告份数等信息。

5.5.11 系统应建立报告台账，包括项目名称、委托编号、任务信息（检测人员、设备、日期）、数据编号以及报告名称与编号等，数据记录与报告文本也应及时归档。

5.5.12 当报告发布后需要变更或补发时，应符合下列要求：

1 满足机构关于报告变更的管理规定；

2 系统具有变更或补发申请、变更审批的功能；

3 更改前、后的报告及变更申请均应保留存档系统并生成变更台账。

**6** 日常管理功能

**6.1 基 本 信 息 管 理**

6.1.1 系统宜对机构基本信息进行设置和维护，包括机构名称、组织框架、主要负责人、试验检测业务范围等，并根据变动情况动态调整。

6.1.2 系统宜对机构取得的各项试验检测许可宜实现下列管理功能:

1 资质证书、附表进行电子化管理，便于查阅；

2 设置到期提醒功能，包括复评审、换证等；

3 对资质标识进行管理。

6.1.3 系统宜具有批量导入、导出功能，数据表宜具有拷贝、粘贴功能。

**6.2 人 员 管 理**

6.2.1 人员管理模块应实现以下功能：

1 建立人员电子档案；

2 基本信息维护；

3 培训与考核；

4 关键人员授权；

5 其他。

6.2.2 系统应建立人员电子档案，完善人员基本信息，包括姓名、出生年月、学业经历、从业经历、职称情况、参加培训情况、相关资质资格证书获得情况、任职与奖惩情况等。

6.2.3 系统应具备人员基本信息维护功能，当遇到人员信息变动应及时更新人员信息。

6.2.4系统应按照求设置离职工作交接功能，完成工作交接后系统应及时收回离职人员的访问权限。

6.2.5 系统宜实现培训全过程信息化管理，并包括以下功能：

1 制定年度培训计划，包括培训内容、培训对象、负责人及考核指标等；

2 按计划监控培训实施情况，当未能如期实施或实施进度较慢时应做出提示；

3 录入考核结果并记录人员信息档案；

4 由相关人员定期对培训计划实施情况进行统计与分析；

5 保存相关培训资料。

6.2.6 系统宜根据岗位职责和要求与人员资质、能力进行匹配，设立关键技术岗位人员授权制度，在任务分配环节根据试验检测项目的要求自动排除不符合条件的人员。

**6.3 设 备 管 理**

6.3.1 设备管理模块应具备下列功能：

1 设备档案管理；

2 采购与验收管理

3 出入库管理；

4 使用管理；

5 校准与功能确认管理；

6 报废管理。

6.3.2 系统应建立设备信息档案，并进行全过程跟踪管理。

6.3.3 设备信息档案的内容应包括：

1 唯一性编号、设备名称、型号规格、生产厂家、出厂编号和日期、供应商、购置日期、主要性能指标等信息；

2 设备验收记录；

3 出厂合格证、说明书或操作手册；

4 历次检定或校准记录、证书以及确认记录；

5 维修、保养记录；

6 其他必要信息。

6.3.4 采购与验收环节系统应实现以下功能：

1 制定年度采购计划；

2 设备采购申请与批准；

3 采购记录资料存档，包括招投标文件、谈判文件、合同、发票等；

4 上传或填写设备验收记录；

5 定期分析采购计划完成情况。

6.3.5 新采购设备的使用培训信息与考核结果，以及重要设备的使用授权情况应上传系统。

6.3.6 设备出入库管理应实现以下功能：

1 在库状态查询；

2 出库申请与审批；

3 入库提醒与验收；

4 实时登记出、入库信息，并进行动态管理。

6.3.7出库时宜在系统登记申请人及所在部门、申请时间、应用项目与任务、计划入库时间等信息。

6.3.8设备入库时应进行状态验收，并在系统登记入库时间、入库状态、经受人等信息。

6.3.9 设备使用前、后应登记使用信息，包括使用时间、使用人、检测项目、检测结构或构件的部位、设备使用前、后的状态等。

6.3.10系统应具备管理设备检定或校准的功能，包括以下方面：

1 制定检定或校准计划，包括设备检定或校准周期、上次检定或校准时间、预估下次检定或校准时间、检定或校准的内容、依据标准、结果评价与确认方法、确认人等。

2 设备检定或校准到期提醒；

3 登记检定或校准结果及确认记录，并更新设备状态信息。

6.3.11应对下列设备制定期间核查计划和方案，并登记核查结果，对不符合要求的设备应提示重新进行检定或校准：

1 使用频繁的设备；

2 使用或储存环境恶劣或发生剧烈变化的设备：

3 使用过程中容易受损或对数据存疑仪器；

4 脱离本机构管理控制后返还的仪器；

5 使用寿命临近到期的仪器；

6 历年检定证书、校准证书示值变动较大的设备。

6.3.12 系统应对设备维护保养状态进行登记管理，当发生故障时应向系统报备，并采取下列措施：

1 设备故障维修管理；

2 初步检查并判定是否需返还厂家或委托专业公司进行维修；

3 进行维修申请与审批；

4 维修后应重新对设备进行检定或校准，合格后可重新使用。

6.3.13当设备达到报废条件时，应进行报废管理：

1 提出报废申请并注明报废理由；

2 由相关人员对设备进行检查，确认符合报废要求；

3 报废申请审批；

4修改设备台账，将报废设备存放于规定区域。

6.3.14系统宜通过二维码等形式对设备进行信息化管理。

**6.4 标 准 管 理**

6.4.1系统宜将机构所有受控的标准列表，形成标准台账。

6.4.2 系统可设定标准的查新周期，自动提醒标准查新与变更，并在系统实时更新信息。

6.4.3 更新标准台账时宜提供批量操作的方式，并保留修改痕迹。

**6.5 质 量 管 理**

6.5.1 系统宜具有质量管理的功能，可包括以下方面：

1 内外部质量控制；

2 日常监督；

3 内审与管理评审；

4 文件控制；

5 不符合/偏离工作；

6 信用评价及客户反馈；

7 其他方面。

6.5.2 系统宜在质量管理方面实现全过程信息化管理，包括计划制定与审批、计划实施、结果评价、记录存档、纠正与改进等：

1 系统可根据机构自身人员组成、设备配置、检测参数、上年质量控制结果等状况，依据相关标准要求如质量管理活动的覆盖率、频率等，初步生成各类质量管理计划；

2 由主管人员对初步计划核查，进行必要的修改、补充、完善，并批准允许实施；

3 系统可根据计划日期，提供不同期限的提醒功能；

4 计划实施过程信息应及时录入系统，包括实施日期、实施人员、实施方式、过程记录、发现的问题、纠正措施与记录、实施结果评价等；

5 系统宜定期对质量管理活动的实施情况和结果进行统计与分析，为质量管理水平提升提供依据，并可自动汇总信息得到年度各项质量管理活动总结报告。

6.5.3 系统宜通过信息化方式进行文件受控管理，包括文件受控申请与审批、受控文件的发放回收、受控文件作废等。

6.5.4 系统宜具备不符合/偏离工作全过程控制管理的功能，包括不符合/偏离工作的确认管理、改进与纠错管理、统计与评价等。

6.5.5 系统宜通过信息化方式收集客户意见并进行全流程管理，包括：受理、调查、处理、反馈、记录电子归档等内容。

**6.6 权 限 管 理**

6.6.1系统应设置权限分级管理制度，权限的划分和角色定位应以组织机构、部门职能定位以及人员内部分工为依据。

6.6.2 系统权限管理应贯穿于委托、收样、方案审批、数据采集和分析、记录、报告审批与签发、资料存档等系统各个部分与环节。

6.6.3 系统权限管理应包括以下方面：

1 账号设置权限；

2 服务器管理权限；

3 浏览、查阅、编辑、修改、上传文档的权限；

4 数据采集、记录、处理、传输、复核、存储的权限；

5 查看、处理进程的权限；

6 电子签章使用权限；

7 其他方面的权限。

6.6.4 系统软件、服务器及其他主要设备应由专职人员负责管理，其他人不得擅自操作网络设备，修改网络参数和服务器等相关设置。

6.6.5 系统分配的口令、密码、电子签章等，相关人员应予以妥善保护，禁止互相借用，防止丢失、被盗，一旦发生应及时申报以便修改或注销。

6.6.6 人员岗位变动或离职，系统赋予的权限应随之变动或收回。

**6.7 统 计 与 查 询**

6.7.1系统宜具有对数据和信息进行智能统计和查询功能。

6.7.2 系统应自动生成各类统计台账，并可根据需求自定义台账。

6.7.3 系统宜具有单独管理模块的统计分析功能，也宜具有在全系统范围统计涉及不同模块的统计分析功能，统计对象包括正在处理及已处理完毕归档的数据和信息。

6.7.4 系统宜具有对数据和信息按关键词自定义统计和组合统计的功能，统计结果应可提供表格和图形等不同展示方式。

6.7.5 系统宜具有基本的统计运算功能，如均值运算、均方差运算、比率运算等。

6.7.6 系统宜具有单一关键词或组合条件查询的功能，系统可提供关键词配置功能，方便自定义查询。

6.7.7 系统宜同时支持精确查询和模糊查询。

6.7.8 系统应将符合条件的查询结果全部列出，点击某个查询结果可直接链接到展示详细信息的相关界面。

6.7.9 系统应具有将查询和统计结果单独存档的功能。

6.7.10 系统应可将查询统计结果导出成电子表格，可供用户二次加工使用。

**7** 系统质量特性要求

**7.1 系 统 性 能 要 求**

7.1.1 系统性能要求宜满足以下要求：

1 系统可支持不小于1GB数据的展示和浏览。

2 系统最大并发用户数应满足机构应用需求，并不少于30。

3 系统对单条件查询的平均响应时间应不大于5s，对多条件查询的平均相应时间应不大于15s；数据更新的平均响应时间应不大于10s；统计报表的平均响应时间应不大于10s；多维分析的平均响应时间应不大于10s。

4 系统数据分类处理时间应不大于5s；支持大数据的快速发布，并保持原有数据格式不变。

7.1.2 系统容量应考虑需求变动情况和变动所引起的数据增加，还应考虑系统的日志、索引和冗余量，数据仓库中需保障20年内的历史记录，过期的记录可移出系统以其他方式保存。

**7.2 系 统 可 靠 性 要 求**

7.2.1 系统应运行稳定，并具有容错能力，防止因意外的操作给系统造成严重损失。

1 系统应支持7×24h的稳定无故障运行。

2 系统应支持数据有效性检验功能，保证输入的数据格式或长度符合系统设定的要求。

3 系统对于用户的“非法”输入或操作不崩溃、不退出。

4 系统应支持自动保护功能，当故障发生时能自动保护当前所有状态，保证系统能够进行恢复。

**7.3 系 统 易 用 性 要 求**

7.3.1 系统的易用性要求包括易理解性、易学性、易操作性、吸引性。

1 易理解性要求系统的文档语言简练、前后一致、易于理解以及语句无歧义；

2 易学性要求系统提供的用户文档（如系统用户手册等）内容详细、结构清晰以及语言准确；

3 易操作性要求系统的人机界面友好、界面设计科学合理和操作简单等；

4 吸引性要求系统具有相互吸引、界面外观易定制性。

7.3.2 系统易理解性设计原则可包括以下内容：

1 用户使用手册对各项功能操作方法描述完整；

2 指导用户使用该系统的演示程序能被简单启动；

3 在操作系统某一功能时，该功能的演示程序能被简单启动；

4 演示程序可解决用户操作过程中遇到的问题；

5 系统的功能在操作过程中方便直观；

6 对系统功能的操作实现便于理解、容易操作；

7.3.3 系统易学性设计原则可包括以下内容：

1 用户能很快完成一项功能或一套操作流程的学习，并能很快学会；

2 用户文档或帮助文档清晰，能有效地帮助用户正确完成各项操作，用户不需要频繁阅读帮助；

3 系统的编辑、选择、快捷键等功能应与常规习惯保持一致。

7.3.4 系统易操作性设计原则可包括以下内容：

1 系统用户界面和功能操作的风格一致；

2 用户能容易地纠正操作过程或及时修正在输入数据过程中的错误；

3 不用依靠手动填写，用户可以选择输入参数值，重复输入不与先前输入混淆；

4 系统出现的提示信息能易于用户理解，系统的提示、警告或错误说明应清楚、明了、恰当，避免歧义；

5 用户能对操作过程中的错误进行纠正或恢复；

6 用户可方便地定制操作规程模板；

7 容易寻找操作按钮，对下一步操作状态有预测性。

7.3.5 系统吸引性设计原则可包括以下内容：

1 系统界面对用户具有吸引性，界面色彩对视觉具有吸引力、界面元素形状舒适、界面元素尺寸合理、布局合理和界面整体效果让用户感觉舒适；

2 界面中能够按用户需求定制满意的外观风格或比例。

**7.4 系 统 兼 容 性 要 求**

7.4.1 系统应具有兼容性与集成性。

1 系统宜公布试验检测设备物联网数据采集接口，兼容第三方仪器设备控制软件获取系统信息与上传检测结果信息；

2 系统应兼容主流的浏览器，在各浏览器内操作界面、计算结果、绘图应保持一致；

3 系统应具有开放式体系结构；

4 系统宜为智慧工地项目管理平台、政府监管平台等外部系统提供可访问的接口，并可集成其他外部系统的数据。

**7.5 系 统 维 护 性 要 求**

7.5.1 在保证信息传输完整性、保密性的前提下，系统具备开放性、共享性。系统应可根据检验检测机构应用与业务的扩展进行系统的扩展，以保证在外界要求发生变化时，可进行二次开发，以较小的代价完成系统调整。

1 系统宜预留各类部署接口，保证系统的可扩展性。

2 系统服务接口宜通过企业服务总线的方式发布，宜支持HTTP+XML方式、HTTP+JSON方式、HTTP+SOAP方式。

3 系统与外部系统集成方式宜支持数据库集成方式、OPC接口方式、OCX控制方式、Web Service方式。

4 系统应支持更新控制文件表单、检测参数、标准、设备等信息时，相应历史数据不受影响。

5 系统应支持扩展开发APP平台模式。

**8** 系统安全要求

**8.1 系 统 安 全 总 体 框 架**

8.1.1 系统应具备第二级及以上安全保护能力，应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。系统安全的技术框架详见图8.1.1。



图8.1.1 系统安全技术框架

**8.2 物 理 安 全**

8.2.1 系统服务器场地安全应满足《计算机场地安全要求》GB/T 9361-2011的要求。

8.2.2 系统服务器所在机房应进行物理访问控制：设置专人值守或配置电子门禁系统，控制、鉴别和记录进入人员。

8.2.3 系统服务器、交换机等主要设备应放置在机房内，设备或主要部件应固定，并设置明显标识；同时应将通信线缆铺设在隐蔽安全处。

8.2.4 系统机房所在建筑应安装避雷装置，并设置交流电源地线。

8.2.5 系统机房应设置灭火设备和火灾自动报警系统，应采取措施做到防水、防潮和防静电，并应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的方位之内。

8.2.6 系统机房供电线路上应配置稳压器和过电压防护设备。

8.2.7 系统机房电源线和通信线缆应隔离铺设，避免互相干扰。

8.2.8 应对系统环境安全、设备安全及截止安全定期威胁评估，分析面临的风险。

**8.3 网 络 安 全**

8.3.1 系统的网络应做到可信接入，主要措施可包括以下内容：

1 可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在监测到其可信性收到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

2 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。

8.3.2 网络应设置访问控制措施，主要包括以下内容：

1系统应用服务器、数据库服务器所在的网络边界应部署防火墙等访问控制设备，根据安全策略提供明确的允许/拒绝访问，控制粒度为网段级。

2系统应用服务器、数据库服务器之间的安全边界应开启访问控制策略，控制粒度为端口级。

3对访问系统网络区域的设备终端，应采取“MAC+端口绑定”等技术方式来防止地址欺骗。

8.3.3 系统网络应进行安全审计，主要包括以下内容：

1 系统应用服务器、数据库服务器所处的网络区域接入交换机，并旁路部署网络安全审计设备，对网络流量、用户行为等进行日志记录。

2 网络安全审计内容应包括事件、日期、用户名、IP地址、事件类型、事件是否成功等。

3 安全审计设备应能保护审计记录，定期备份，避免受到未预期的删除、修改和覆盖等，审计记录至少保持6个月。

4 应定期对审计记录进行分析，及时发现异常行为。

8.3.4 系统网络应能识别入侵行为，并能进行防范，可采取以下措施：

1 应在系统政务外网边界、互联网边界等关键网络节点部署相关设备，以监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击和网络蠕虫攻击等。

2 当监测到攻击行为时，应能够记录攻击源IP、攻击类型、攻击目的、攻击事件，发生严重入侵事件时应提供报警。

8.3.5 系统网络应能进行恶意代码防范，可采取以下措施：

1系统网络边界处等关节网络节点应对恶意代码进行检测和清除，及时维护恶意代码库的升级和检测系统的更新。

2系统服务器应安装计算机信息系统安全专用的防病毒软件，并及时更新软件版本和恶意代码库。

8.3.6 系统服务器与用户双方通信时，应采用校验码技术、特定的文件格式、特定协议或等同强度的技术手段进行传输，以保证通信过程中的数据完整性。

**8.4 应 用 安 全**

8.4.1 系统的应用安全应做到身份鉴别， 可采取以下措施：

1系统应对接入的采集端设备进行可信检验，确保接入平台的采集设备真实可信，防止恶意非法终端接入。

2系统的用户访问应采用基于数字证书等严格的强身份认证措施，系统需提供专用的登录控制模块，或者将登录控制模块集成到统一的门户认证系统中，应对登录用户进行身份标识和鉴别。

3系统应为不同用户分配不同的用户名，不能多人使用同一用户名，并能提供鉴别身份标识唯一性和复杂度的检查功能。

4系统的用户身份鉴别信息应具有不被冒用的特点，口令长度不小于8字符，口令应定期更换，用户名和口令应限制为不同。

5系统应提供登录失败处理功能，可采取结束会话、限制非法登录或自动退出等措施。

6系统进行远程管理时，应采取必要措施防止鉴别信息在网络传输中被窃听。

8.4.2 系统的应用安全应做到访问控制，可采取以下措施：

1 系统应提供统一的门户，门户应具有鉴权机制，依据用户的不同身份展现不同的界面。

2 通过外部网络对系统进行访问时，应使用安全方式接入，宜对用户采用数字证书等强制认证方式，应根据维保部门、使用单位等用户和系统间的的访问规则，决定对系统中资源的访问，访问控制粒度为单个用户。

3 系统应具备身份认证与授权管理，实现用户的统一身份认证及资源的统一授权管理，应能根据用户的角色分配权限，实现用户的权限分离，仅授予用户所需的最小权限。

4 系统应实现操作系统和数据库系统特权用户的权限分离。

5 系统应能重命名或删除默认账户，修改默认账户的默认口令。

6 系统应能检查、提醒、删除多余和过期账户，避免共享账户的存在。

8.4.3 系统的应用安全应做到安全审计及web应用防范，可采取以下措施：

1系统应具备安全审计功能，对系统管理员应审计用户登录、修改配置、操作内容、操作结果等重要行为和系统资源的异常使用；对用户应审计用户登录、操作内容等重要行为。

2审计记录应至少包括事件类型、日期和时间、客户端IP地址、详细描述和结果等。

3系统应保证无法删除、修改和覆盖审计记录，并定期备份，审计记录至少保存6个月。

4系统应具备网页防篡改等应用层防护体系，WEB应用应能够抵抗SQL注入等应用层攻击。

**8.5 数 据 安 全**

8.5.1 系统应采取以下措施保证数据库安全：

1数据服务器与应用服务器应部署在不同服务器，按数据创建时间分离新旧数据，比如3年以上的数据即可进行分离，分离出的数据只允许局域网用户访问 。

2系统应建立数据库操作与使用权限管理制度，防止非法创建、删除数据和访问数据库。

3对数据库的操作系统及时修补漏洞，对非法入侵做出响应和处理。

4系统数据库不应存在隐蔽接口，不应加载能够禁用安全机制或绕过安全机制的组件。

5对工作机密、个人秘密数据做机密性保护，数据存储时对关键数据进行加密后存储。

8.5.2 存储数据应具有完整性，可采取以下措施：

1系统应至少采用RAID1策略来存储数据。

2系统应采用SSLVPN技术确保远程接入用户的通信完整性。

8.5.3 系统数据应以数据库形式提供全系统备份与恢复，系统发生故障时，应能够实现数据的恢复，可采取以下措施：

1系统数据汇聚层存储节点和应用层存储节点应提供数据本地备份与恢复功能。完全数据备份至少每月一次，增量备份至少每天一次。

2系统数据除数据库自动备份外，还应选用硬盘、磁带、光盘等数据备份介质进行分离备份，完全数据备份至少每季度1次。

3应制定数据备份与恢复策略和计划，每年应至少进行1次数据恢复演练。

8.5.4 存储设备应有冗余与冗错功能：

1数据存储设备宜采用冗余设计，应通过一定措施确保当系统出现某些确定的故障情况时，安全功能也能维持正常运行，如系统检测和报告系统的服务水平已降低到预先规定的最小值。

2当系统资源的服务水平降低到预先规定的最小值时，应能检测和发出报告。

3系统应提供维护模式中运行系统的能力，在维护模式下各种安全功能全部失效，系统仅允许系统管理员进入维护模式。

**9** 系统验收与维护

**9.1 系 统 验 收**

9.1.1 系统满足以下基本条件时，可进行验收：

1 已根据检验检测管理需求，建立了相应的组织模式。

2 制定了系统信息化管理办法。

3 建立了与系统管理范围和管理工作量相适应的专业管理队伍。

4 具有完整覆盖检验检测业务范围的功能模块，功能性和安全性均满足要求。

5 系统连续、安全、稳定试运行超过6个月以上。

9.1.2 系统的验收应以双方签署的合同、项目实施方案等有关规定为依据，对系统各项功能和数据的配置要求、性能指标、应用和运行情况，进行全面的整体测试验收。

9.1.3 系统验收可采取预验收和正式验收两个方式进行。

9.1.4 应用系统验收宜包括以下内容：

1 应建立系统运行环境，具备网络、服务器、显示设备、存储及备份设备、安全设备等，安装操作系统、数据库管理系统及应用系统等软件。

2 应用系统的功能宜至少符合第5章和第6章的规定。

3 应具有安全保障功能：用户身份认证、用户访问授权和行为控制、漏洞扫描和入侵检测、数据包过滤和病毒防范、数据加密、系统监控等。

4 应对应用系统进行软件测试。

5 应提供应用系统设计和开发文档，包括需求分析报告、总体设计书、详细设计书、用户手册、维护手册和测试报告等。

9.1.5 运行效果验收宜验收以下内容：

1 运行范围应完整覆盖检验检测业务。

2 涉及检验检测业务管理的部门应全部接入系统。

3 系统应处于正常运行状态。

4 应满足附录A规定的运行效果指标。

**9.2 系 统 维 护**

9.2.1 系统应通过适应性维护和改正性维护来保证数据和信息的准确、完整和安全。

9.2.2 系统运维的对象应包括应用系统、数据库、网络系统、主机服务器系统和机房系统。

9.2.3 建设工程检验检测信息管理系统验收与运维应符合现行标准的相关规定。

9.2.4 系统运维包括日常运维和应急保障运维，日常运维应保证5×8小时电话或远程技术支持，应急保障运维应保证7×24小时电话或远程技术支持。

**附录A** **验收指标评分表**

| **序号** | **一级指标** | **二级指标** | **指标描述** | **测评方式** | **得分** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
|  | **管理模式** | **组织机构建设** | 采用的组织模式与检验检测管理需求一致 |  |  |  |
|  | **制度建设** | 制定了系统信息化管理办法 |  |  |  |
|  | **队伍建设** | 建立了与系统管理范围和管理工作量相适应的专业管理队伍，包括系统管理员、网络管理员、安全管理员、应用管理员 |  |  |  |
|  | **应用系统** | **运行环境** | 硬件、软件系统建设符合4.2、4.3的规定 |  |  |  |
|  | 网络环境应具有开放性、可扩充性、可靠性和安全性的特点，并建立网络管理制度和网络运行保障支持体系 |  |  |  |
|  | 建立灵活的备份和恢复系统，具有集中化的备份策略管理及备份任务监督功能，重要数据采取物理备份 |  |  |  |
|  | 建立安全访问机制，确保系统和数据安全 |  |  |  |
|  | **功能和性能** | 应用系统的功能和性能符合第5章、第6章和第7章的规定 |  |  |  |
|  | 通过了国家认可的第三方软件测试 |  |  |  |
|  | **运行维护** | 制定合理有效的运行维护管理制度 |  |  |  |
|  | 配备系统管理员，或由专门机构或公司托管，监测系统运行状况、数据库状况、数据备份情况等 |  |  |  |
|  | **运行效果** | **范围覆盖率** | 达到实施方案规定的覆盖范围 |  |  |  |
|  | **部门覆盖率** | 涉及检验检测相关业务的专业部门全部接入系统 |  |  |  |
|  | **运行指标** | 运行速度符合7.1要求 |  |  |  |
|  | 业务部门系统使用率不低于90% |  |  |  |
|  | 业务部门按期处置事物率不低于80% |  |  |  |
|  | 事物处置延期总量不超过3% |  |  |  |
|  | 通过数据对比，表明检验检测业务实施信息化管理后，各类业务完成效率显著提高 |  |  |  |
|  | **现场考察** | 现场系统检验检测业务化运行演示流程顺畅，操作熟练 |  |  |  |
|  | 现场随机抽取适量检验检测业务，能清晰显示检验检测各流程情况和完整执行记录 |  |  |  |
|  | 现场随机抽取系统功能模块，能顺利进行多种条件的查询和统计分析，并形成报表 |  |  |  |
|  | 现场随机抽查各权限使用人员，均能熟练操作系统 |  |  |  |
|  | **文档资料** | **建设过程文档** | 系统立项申请与批复 |  |  |  |
|  | 系统实施方案及论证专家评审意见 |  |  |  |
|  | 系统集成相关文档资料，包括招标文件、投标文件、合同、场地机房设计和建设文档、设备和软件到货验收文档、系统集成建设文档、系统集成测试报告等 |  |  |  |
|  | 应用软件需求分析报告、总体设计书、详细设计书、用户手册、维护手册、测试报告等 |  |  |  |
|  | 对系统软件测试、网络及机房硬件环境等方面的专项验收 |  |  |  |

**附录B 系统运维指标**

| **序号** | **运维项目** | **日常运维内容** | **应急保障运维内容** | **备注** |
| --- | --- | --- | --- | --- |
|  | **软件系统运维** | **巡检** | **应用软件** | 1. 每天对应用软件运行情况进行巡检并随时监控，定期对功能模块的有效性进行验证检查；
2. 向使用者解答应用软件使用中出现的问题；
3. 对软件运行日志进行日常跟踪检查、备份；
4. 应定期调出部分数据和信息，检查对录入数据所做的数值计算、逻辑函数，添加备注等过程及结果的完整性和准确性；
5. 应定期抽取一定数量的记录和报告，核对数据和记录文件格式的一致性。
 | 1. 应急预案管理：运维人员应根据系统部署情况，设计专项应急方案并对应急方案进行测试预演，并根据演练效果进行完善；
2. 故障处理：故障发生时，运维人员应及时修复软件故障，如无法修复应重新安装，同时应尽快采取硬件冗余备份、转移到纸质系统等应急措施；
3. 对于防病毒系统，如发生防病毒系统无法解决的病毒，运维人员应对病毒进行手动清除。
 |  |
|  | **系统软件** | 1. 每天对系统软件运行情况进行巡检并随时监控；
2. 解决系统软件使用中出现的问题。
 |  |
|  | **第三方应用软件** | 1. 定期对第三方应用软件运行情况进行巡检和升级，验证第三方应用软件的可用性；
2. 每周对防病毒系统现场巡检一次，包括防病毒系 统部署策略检查、防病毒系统服务运行情况以及与通信点的连接状态检查。
 |  |
|  | **性能优化** | 运维人员应针对软件系统性能下降的问题，给出数据库和中间件优化建设及临时库表清理方案。 |  |
|  | **配置管理** | 软件配置管理应制定软件配置管理方案，保证软件和文档是最新版本，应至少每半年检查一次 |  |
|  | **数据库软件运行管理** | 1. 应及时更新数据备份脚本，定期对数据库日志进行保存，提供数据库日志分析；
2. 应定期对数据库软件的运行状态进行巡查，对数据库运行状态进行监测，监测内容应记录到运维日志；
3. 应及时分析数据库日志，发现数据库运行过程中的异常动作或进程
 |  |
|  | **文档管理** | 运维过程中应形成维护手册、技术文档、应急方案、运维记录表单 |  |
|  | **数据库运维** | **数据备份** | 1. 应定期核查备份数据的完整性及备份介质标识的正确性；
2. 应定期监控备份介质、外围设备、通信设备所处的环境条件，并监控电源及不间断电源情况，断电前采取措施完成数据备份；
3. 应定期核查备份介质及保护设备的有效性，避免各种因素引起的数据损坏。
 | 1. 用户错误操作导致系统不能进行数据回退时、软件功能不完善导致产生的数据错误时、历史数据本身质量有问题时均需要进行数据修复；
2. 数据修复需要填写运维记录单；
3. 系统发生故障造成重要信息丢失、损害后，应利用备份数据进行系统恢复，并对灾难恢复的全过程详细记录。
 |  |
|  | **日志跟踪** | 运维人员应跟踪系统运行日志，发现系统运行过程中出现的异常现象 |  |
|  | **网络系统运维** | **网络设备配置管理** | 1. 当系统变更业务需求时，运维人员应根据相关变更内容，提交配置调整方案，并对最终配置进行本机备份；
2. 应对网络配置进行定期备份
 | 1. 应制定网络应急预案及专项预案；
2. 应组织、参与网络应急预案测试演练及培训；
3. 故障发生时，应及时做出响应，根据故障情况，采取措施，恢复网络系统正常运行
 |  |
|  | **网络状态监控** | 1. 应对网络光纤状态、网络设备资源使用情况、网络流量使用情况进行定期巡检；
2. 应定期备份网络监控记录，为网络问题的分析提供依据。
 |  |
|  | **设备保养** | 应定期对设备进行常规性保养，包括设备清洁、除尘、设备运行环境温湿度检测 |  |
|  | **备品备件** | 当出现硬件、配件损坏情况时，应提供功能相同或幸好一致的设备进行更换 |  |
|  | **主机系统运维** | **巡检** | 应定期对硬件设备进行现场巡检，填写巡检记录 | 1. 应有限实施业务恢复，在恢复业务的前提下进行彻底的故障排除
2. 应了解设备运行情况，核实故障现象，并根据故障现象对设备进行故障分析、测试、诊断，并制定业务恢复和故障解决技术方案
 |  |
|  | **技术资料支持** | 收集产品手册、操作手册及必要的技术资料 |  |
|  | **机房系统运维** | **巡检** | 应定期对配电系统、防雷与接地系统、空气调节系统、给排水系统、综合布线、监控与安全防范进行巡检 | 1. 当机房突然停电时，首先应确认是否为正常停电并预计停电时间，检查不间断电源的电池可供电时间，需在不间断电源供电时效内关闭所有服务器及网络设备
2. 当中心机房无法制冷致使机房内环境温度超过设备规定的运行温湿度要求时，应按顺序关闭所有服务器及网络设备
 |  |
|  | **定期保养** | 定期对机房各系统进行保养 |  |

本标准用词说明

1 为准确辨别和执行本标准条文，对条文中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，在条件许可时首先应这样做的：

 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”。

2 条文中指明应按其他有关标准执行的写法为“应符合……的规定”或“应按……执行”。

引用标准名录

《建筑工程施工现场监管信息系统技术标准》JGJ/T 434

《信息安全技术网络安全等级保护基本要求》GB/T 22239

《计算机场地通用规范》GB/T 2887

《信息安全技术 信息系统物理安全技术要求》GB/T 21052

《信息安全技术服务器安全技术要求》GB/T 21028

《信息安全技术操作系统安全技术要求》GB/T 20272

《信息安全技术 网络交换机安全技术要求》GB/T 21050

《信息安全技术 路由器安全技术要求》GB/T 18018

《信息安全技术 防火墙安全技术要求和测试评价方法》GB/T 20281

《信息安全技术 网络入侵检测系统技术要求和测试评价方法》GB/T 20275

《计算机场地安全要求》GB/T 9361-2011

《检测实验室信息管理系统建设指南》RB/T 029

《实验室信息管理系统管理规范》RB/T 028

《信息技术服务 运行维护第1部分：通用要求》GB/T28827.1

《信息技术服务 运行维护第2部分：交付规范》GB/T28827.2

《信息技术服务 运行维护第3部分：应急响应规范》GB/T28827.3

条文说明

目 次

[1　总则 37](#_Toc85037335)

[3　基本规定 3](#_Toc85037337)7

[4 系统运行环境要求 38](#_Toc85037338)

[4.2 硬件配置 38](#_Toc85037340)

[4.3 软件产品 38](#_Toc85037341)

[4.4 网络体系结构 38](#_Toc85037342)

[5 检验检测功能 39](#_Toc85037343)

[5.1 一般规定 39](#_Toc85037344)

[5.2 委托/合同管理 39](#_Toc85037345)

[5.4 现场检测 40](#_Toc85037347)

[5.5 报告管理 40](#_Toc85037348)

[6 日常管理功能 40](#_Toc85037349)

[6.1 基本信息管理 40](#_Toc85037350)

[6.2 人员管理 40](#_Toc85037351)

[6.3 设备管理 40](#_Toc85037352)

[6.4 标准管理 41](#_Toc85037353)

[6.5 质量管理 41](#_Toc85037354)

[6.6 权限管理 41](#_Toc85037355)

[6.7 统计与查询 42](#_Toc85037356)

[7 系统质量特性要求 42](#_Toc85037357)

[7.1 系统性能要求 42](#_Toc85037358)

[7.3 系统易用性要求 42](#_Toc85037360)

[7.4 系统兼容性要求 42](#_Toc85037361)

[9 系统验收与维护 43](#_Toc85037369)

[9.1 系统验收 43](#_Toc85037370)

[9.2 系统维护 43](#_Toc85037371)

**1**总 则

1.0.1检验检测工作是控制工程质量的重要手段，信息化与试验检测行业相结合是必然的发展趋势，也是对检验检测行业传统管理模式的一次变革。检验检测信息管理系统的作用一是使检验检测工作规范化、制度化、流程化，减少违反规范要求、偏离业务流程的情况，从而提高质量管理水平，降低检验检测机构从业风险；二是通过信息化的应用减少重复性、统计性的工作，降低劳动强度、提高工作效率；三是促进检验检测业务相关各方包括检验检测机构、业主单位、行业主管部门之间数据交换与信息共享，促进检验检测行业的健康发展。

**3**基本规定

3.0.1主管部门对第三方检验检测机构有一些要求，比如对见证取样项目，要求有见证取样记录才能接受委托并且报告加盖“见证取样”章；再比如要求上报试验检测不合格的结果等，应通过精心设计使管理信息系统的功能能够满足这些要求。

3.0.2各个检验检测机构规模大小、组织架构、业务范围、运行机制及管理水平都不尽相同，应用的检验检测信息管理系统应符合机构的运行模式，才能有效的为机构服务，达到高效适用的目的。

3.0.4系统宜采用可增减、组合的开放式模块框架，便于机构根据自身情况调整，可选择的模块还包括招投标管理、成本管理、预算管理、分包管理、供应商管理、安全管理、科研管理、印章管理、风险决策管理、智库管理等多方面

3.0.6

3检测机构的系统实现数据交互传输也是客户方的管理需求，《建筑工程施工现场监管信息系统技术标准》JGJ/T 434-2018第5.2.6条：质量监管子系统宜于检测机构的检测系统接口对接，能自动实现质量检测数据的交互传输功能。

5 宜记录数据共享交换过程信息，包括发起方、接收方，采用的共享/交换规则、策略的运行情况等。

6 数据共享接口的原数据编制、数据库设计、业务代码编制、数据报文设计、数据交换格式设计应符合国家现行相关标准的规定。

3.0.7对于修改和删除信息的操作，应在操作前输入修改、删除原因后方可进行，关键信息应设置审批修改和删除的审批流程与权限，并对修改后的信息做出明显标记如用颜色区分或单独成列，对删除的信息应设置回溯查询功能。

**4** 系统运行环境要求

**4.2 硬 件 配 置**

4.2.1硬件选择的原则包括：

1 性能价格比高，具有通用性和可升级性；

2 运算速度和存储容量等性能指标满足数据管理要求；

3 与其他硬件的兼容性、可连接性、共享性好；

4 与所选软件兼容性、对系统软件和应用软件的适应性好；

5 硬件接口丰富；

6 尽量选用国产品牌。

**4.3 软 件 产 品**

4.3.1软件产品选择的原则为：

1 国产化原则：同等性能价格比条件下宜优先采用国产软硬件系统；

2 开放性和扩展性原则：采用开放性、标准化的软件及信息资源，对于未来可能增添的系统、数据库、功能、新的用户留有接口与二次开发API；

3 先进性和成熟性原则：采用先进性和成熟性的统一的产品，以满足系统在很长的生命周期内有持续的可维护性和可扩展性；

4 可靠性原则：从系统结构、网络结构、技术措施及厂商的技术服务和维护响应能力等方面综合考虑，确保系统整体运行的可靠性。

4.3.2操作系统及操作系统相关部件应符合《信息安全技术操作系统安全技术要求》GB/T 20272中二级以上要求。

**4.4 网 络 体 系 结 构**

4.4.3

1 主要网络设备包括交换机和路由器，分别应符合《信息安全技术 网络交换机安全技术要求》GB/T 21050规定和《信息安全技术 路由器安全技术要求》GB/T 18018中二级要求规定。

2 主要安全设备包括防火墙和入侵检测系统，分别应符合《信息安全技术 防火墙安全技术要求和测试评价方法》GB/T 20281和《信息安全技术 网络入侵检测系统技术要求和测试评价方法》GB/T 20275规定。

**5** 检验检测功能

**5.1 一 般 规 定**

5.1.2检验检测包括室内试验和现场检验检测，系统可根据业务情况和管理流程单独设置试验模块和现场检验检测模块，也可以合并设置。其中第2款收样管理针对室内试验，项目管理针对现场检验检测。

5.1.3目前建设工程检验检测行业越来越多采用自动采集设备，尤其是室内试验，这类情况便于直接设置接口将数据上传系统，但对于现场检验检测仍然有采用非自动采集设备的情况，因此本条分为3种情况描述。

5.1.6如在报告界面，通过点击一份报告可以调阅与其相关联的委托单、工程、任务、数据集、使用的设备及参加检测的人员的界信息，而在设备界面，点击一台设备可以进入与其相关联的记录或报告的界面。

**5.2 委 托 / 合 同 管 理**

5.2.1根据检验检测机构的具体需要，还可以增加招投标管理、分包管理等功能，也可根据预先设置的收费标准或与客户的约定自动计算检验检测费用。

5.2.2委托单为简易合同，信息简单、快捷明了，一般针对材料试验与单项现场检测项目，在实际中应用很广泛；对于大型、综合委托项目，委托单的信息无法满足实际需要，一般需签订正式合同。

5.2.4委托单还可约定试验检测费用及支付方式；当委托内容涉及在建工程时，宜增加设计单位、施工单位、监理单位等信息，当为见证取样项目时，也可增加见证取样单位与见证人信息。

5.2.7当涉及保密工程及其他不宜在系统上显示的项目时，宜采用人工设置委托编号的形式。根据管理流程，可以为委托单和合同分别设立编号，也可以合并一起设置编号，但都需满足编号唯一性、连续性的要求。

5.2.9收样管理指对样品进行性状核实检查后实验室收下或退回样品的过程。

5.2.10在办理委托时，部分工程信息与样品信息已经在系统登记的，可不必重新录入。

**5.4 现 场 检 验**

5.4.3可以将针对整个项目编写检测方案，也可以针对各个子项目分别编写检测方案。

5.4.4当人员、地点与设备等其中一项发生变化时，宜重新发布任务。

**5.5 报 告 管 理**

5.5.1报告审核级别不宜少于三级，如可设置为试验人（检测人）、审核人、批准人。

5.5.5在线批注宜与word批注功能类似，界面显示清晰明了，再次提交的报告可呈现上一次的修改意见以及修改后的内容。

**6** 日常管理功能

**6.1 基 本 信 息 管 理**

6.1.3人员、设备、标准依据等相关信息有时需要大量录入或者输入，具有批量导入、导出及复制、粘贴功能会比较便利。

**6.2 人 员 管 理**

6.2.5

4系统宜具备培训实施情况的统计与分析功能，可按度统计年度培训计划完成率、培训员工数量、培训投入经费、培训工作等级分布等内容，为改进培训工作提供依据。

6.2.6 系统宜根据岗位职责和要求与人员资质、能力进行匹配，设立关键技术岗位人员授权制度，在任务分配环节根据试验检测项目的要求自动排除不符合条件的人员。

**6.3 设 备 管 理**

6.3.4设备验收时应登记验收日期、验收人员、验收结论等必要信息。

6.3.6

3 可根据计划入库日期设置归还提醒功能。

6.3.12

2 对易排除的小故障可以自行维修，当无法自行维修时应将设备返还厂家或委托专业公司进行维修。

6.3.14如通过扫描二维码获得相关管理信息，包括设备技术指标信息、设备购置信息、设备检定/校准信息、设备出入库状态信息、设备日常维护信息和设备使用状态信息等内容。

**6.4 标 准 管 理**

6.4.1一般将经资质评审得到认可、机构可以其中的方法为依据进行试验检测并向社会出具报告的标准称为受控的标准。

**6.5 质 量 管 理**

6.5.1

1 外部质量控制包括能力验证、测量审核、盲样考核、实验室间比对等，内部质量控制包括人员比对、仪器比对、不确定度分析等。

3 内审：实验室或检验检测机构自行组织或以自身名义进行，以确定管理体系满足内部审核准则的程度所进行的系统的、独立的并形成文件的过程。

4 内部文件包括质量手册、程序文件、作业指导书、原始记录表格等，外部文件包括标准规程、行业或行政主管单位的技术质量管理文件等。

6.5.4不符合/偏离工作的确认包括来源、事实描述、依据、责任部门与人员、风险分析与评估；改进与纠错管理包括原因分析、整改方案制定与审核、方案完成期限设置、方案实施提醒、整改工作的有效性评价以及资料的电子归档；系统可自动对不符合/偏离工作信息和整改完成情况统计与评价，包括按工作的类型和内容进行统计，按发生率、重复率、整改及时性、整改质量等多方面进行评价。

**6.6 权 限 管 理**

6.6.3

5 处理进程包括接收、转发、审核、批准、不通过而返回、中止进程等。

**6.7 统 计 与 查 询**

6.7.1智能统计和查询对机构大数据分析和利用特别重要，可以更快捷、有效地在数据库中查询到与用户需求相吻合的数据，进行有针对性的分析和统计，提升机构管理水平及业务能力。

6.7.2系统中所有模块都应具有生成多种类型台账的功能，包括：合同委托台账、工程台账、任务台账、数据统计台账、报告台账、不合格结果台账、设备台账、人员台账、质量管理各类功能台账、权限统计台账等。

6.7.4统计图形可包括散点图、直方图、饼图、折线图等不同表现。

6.7.6可根据不同需求设置不同的的查询关键词，如报告管理模块可自定义权属部门、时间、合同委托单名称和编号、工程名称和编号、任务单编号、报告编号、委托单位、项目负责人、报告审批人、检测项目参数、使用设备类型、耗材编号等单一或组合条件进行查询。

6.7.8例如在报告管理模块查询得到一段时间内所有使用了探地雷达设备的报告的信息，点击其中一台探地雷达设备，即可直接跳转至该设备的信息档案界面。

**7** 系统质量特性要求

**7.1 系 统 性 能 要 求**

7.1.1

4 如1GB的数据在5min内完成网络发布。

**7.3 系 统 易 用 性 要 求**

7.3.1

4 界面布局合理可遵循以下原则：版面布局简洁明了、善用最佳视域和有效视域（注意协调性和分割法则）、合理的版面布局顺序（符合人视觉特点）、屏幕不能拥挤（屏幕总体覆盖率不应超过40%，分组覆盖度不应超过62%）、协调界面的视觉平衡感。

**7.4 系 统 兼 容 性 要 求**

7.4.1

3 系统与专业应用软件之间、系统与其他软件系统之间宜实现集成，并宜与第三方移动办公软件流程兼容、消息互通。

**9** 系统验收与维护

**9.1 系 统 验 收**

9.1.3

1 预验收应组织专家按照基本条件逐一对照检查，对存在的问题提出明确的改进意见；整改后结果应经预验收专家确认合格。

2 正式验收应由不少于5人的专家参与，验收程序包括系统建设和运行情况汇报、系统延时、文档审阅、系统业务化运行现场考察及数据和案例随机抽查。

**9.2 系 统 维 护**

9.2.1

适应性维护是通过对运行环境的适当变更来适应系统变化；改正性维护是为了修正系统运行中出现的错误或潜在风险。

9.2.3依据的标准主要有《检测实验室信息管理系统建设指南》RB/T 029、《实验室信息管理系统管理规范》RB/T 028、《信息技术服务 运行维护第1部分：通用要求》GB/T28827.1、《信息技术服务 运行维护第2部分：交付规范》GB/T28827.2、《信息技术服务 运行维护第3部分：应急响应规范》GB/T28827.3的相关规定。

9.2.4系统运维内容包括以下内容：

1 软件系统日常运维包括巡检、性能优化、配置管理、数据库软件运行管理和文档管理，应急保障运维包括应急预案管理与故障处理，具体运维指标见附表B。

2 数据库日常运维包括数据备份与日志跟踪，应急保障运维包括数据修复与数据修复记录，具体运维指标见附表B。

3 网络系统日常运维包括网络设备配置管理、网络状态监控、设备保养和备品备件，应急保障运维包括应急预案管理和故障处理，具体运维指标见附表B。

4 主机服务器系统日常运维包括巡检和技术资料支持，应急保障运维包括故障排查与业务恢复，具体运维指标见附表B。

5 机房系统日常运维包括巡检和定期保养，应急保障运维包括机房停电保障、机房空调制冷保障、机房漏水保障等内容，具体运维指标见附表B。