ICS 35.080
CCS L77

DB21

辽 宁 省 地 方 标 准

DB XX/T XXXX—XXXX

应用系统工程 工程架构设计规范

Application system engineering-Engineering architecture design specification

（征求意见稿）

（本草案完成时间：2025-6-17）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：大连昆腾数据科技有限公司、大连市财政事务服务中心、大连市大数据中心、大连市友谊医院、国家计算机网络与信息安全管理中心辽宁分中心、荣科科技股份有限公司、大连市工程咨询协会、大连软件行业协会、中国（辽宁）自由贸易试验区营口片区管委会数字经济发展局、营口自贸区建设发展有限公司、大连华屹工程咨询有限公司、大连新闻传媒集团、大连正润科技有限公司、辽宁雨溪项目管理咨询有限公司、中电云计算技术有限公司、大连市甘井子区大数据中心、大连竹方工程咨询有限公司、大连亿丰科技有限公司。

本文件主要起草人：于锋、王璐、王江、段刚、谭跃、吉长军、贾瑄、赵世宏、赵鹤、武毅、葛文跃、荣宪波、王启章、张文革、马双翼、刘斌、冯艳爽、徐慧、刘俊江、王佳驹、宋悦、吉庆、朱明、时凤燕、娄巍、邢宇、裴鑫、王鹏、田野、杨光、陈春声、智靖淼、曹秀坤、孙建峰、陈晓云、赵志明、朱善彬、宋惠妍。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件归口单位通讯地址：沈阳市北陵大街45-2号，联系电话：024-86913384

本文件起草单位通讯地址：大连市沙河口区星河二街25号1单元38层6-1,5-2号，联系电话：0411-84119516

应用系统工程 工程架构设计规范

1 范围

本文件规定了应用系统工程工程架构设计的基本内容、设计方法、指标体系和图纸要求，适用于新建、扩建和改建的应用系统工程。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

DB21/T 3756-2023 应用系统工程 应用软件工程量清单规范

DB21/T 3757-2023 应用系统工程 工程造价咨询规范

DB21/T 3758-2023 应用系统工程 初步设计文件规范

DB21/T 3759-2023 应用系统工程关键性评价指标

DB21/T XXXX-2024 应用系统工程 应用软件架构设计规范

3 术语和定义

DB21/T 3756-2023、DB21/T 3757-2023、DB21/T 3758-2023、DB21/T 3759-2023界定的以及下列术语和定义适用于本文件。

3.1

工程架构 engineering architecture

应用系统工程的基本概念和属性以及实现和演化原则。

3.2

应用系统 application system

以应用软件为主要建设内容的系统，通常包括应用软件系统、运行环境、外部实体与用户构成。

3.3

极限状态 limit state

应用系统保持可靠、稳定、安全运行时的状态，通常由一组阈值来表示。超过阈值时，应用系统运行可能会出现不稳定、超时、或无法运行等状况。

3.4

正常运行极限状态 limit state of normal operation

运行环境保持良好状态时，应用系统所允许的最大数据处理容量和在线用户访问量。

3.5

承载能力极限状态 ultimate limit state

应用系统运行环境中的主要设备允许达到的最大利用率。

3.6

鲁棒性 ultimate limit state

应用系统抵抗故障和干扰的能力，即在各种故障和干扰情况下，应用系统能够保证功能运行正确且数据能够得到正确处理。

4 基本规定

4.1 一般规定

工程架构设计应符合以下要求：

a) 工程架构设计内容一般应包括：机房选择、计算环境设计、终端环境设计、安全环境设计、网络环境设计、存储备份系统、界面与交互设备设施、验证与测试环境。验证与测试环境以外的内容统称为运行环境或基础设施；
b) 应以应用系统设计使用年限作为确定设备规格的主要依据；
c) 应明确应用系统极限状态指标并以此为基础进行设计；
d) 应设计存储备份系统或提出备份介质保存要求，满足业务数据保存、软件备份以及应用系统迁移、重建、改建需要。长期使用、永久使用的应用系统运行环境以及采用购买第三方服务方式建设应用系统运行环境时，应设计独立的存储备份系统；
e) 应采取临时安全措施，保证应用系统建设期间的数据安全；
f) 应为数据管理系统设计能够独立运行、单独管理的设备设施，以满足年度数据集、数据资产、主数据/参考数据等数据生产、管理与决策支持需求；
g) 对密码技术、数字签名技术、加密设备、安全设备等列入网络关键设备和网络安全专用产品目录的技术与设备，应设计安全隔离措施，明确检测认证要求；
h) 需单独建设验证与测试环境、备份环境或灾备系统时，应作为新建项目或新建应用系统进行设计；
i) 数据中心与机房、土建、智能建筑、综合布线、视频监控、门禁、远程会议等建设内容应按国家现有标准规范进行设计。

4.2 工程架构设计方法

工程架构设计可使用极限状态设计方法。必要时，也可考虑使用限额设计方法、指标设计方法等。

应根据应用系统的数据生产能力、性能效率、操作限制与运行模式、采购限制等实际需求，提出不同的极限状态测度指标，以实现不同的架构设计。

当采用限额设计方法、指标设计方法时，应对非功能需求进行剪裁以实现架构设计。

设计时，工程架构设计过程和应用软件架构设计过程应进行迭代和递归，对数据生产能力、并发用户数、设备资源利用率等指标进行测试和优化，以获得最佳的应用系统架构设计方案。

4.3 极限状态

应用系统的极限状态包括正常运行极限状态和承载能力极限状态。

当工程架构包含多个应用系统时，应分别计算每个应用系统的极限状态。当多个应用系统共用设备时，应考虑虚拟化软件、I/O分配等额外资源消耗。

极限状态测度指标应在应用系统质量检测合格、运行环境下安装调试完成和性能优化后，由具有相应能力的测试机构进行测试。

4.3.1 正常运行极限状态

正常运行极限状态应以保证应用系统的鲁棒性为基本原则，以数据生产能力指标作为核心指标。以下情形应认为超过了正常运行极限状态：

a) 应用软件系统作业完成时间持续性超过最大生产能力，且无法通过技术措施解决；
b) 应用系统出现严重安全隐患并导致应用系统难以保持安全可靠运行状态，且无法通过技术措施解决；
c) 基础设施故障或被破坏，严重影响应用系统数据处理，且无法恢复；
d) CPU/GPU 平均利用率、内存平均使用率、硬盘空余容量、可用带宽等严重影响应用软件系统性能效率。如：作业完成时间和响应时间超过用户最长可忍耐时间；

正常运行极限状态指标包括：

e) 最大数据生产能力、最大在线用户数和最大并发用户数；
f) 在单位时间数据生产能力状态下，主要作业用户最长可忍耐响应时间和最长可忍耐作业完成时间。最长可忍耐响应时间一般不应超过 15 秒。最长可忍耐作业完成时间应根据应用系统数据生产能力进行计算；
g) 主要作业的平均周转时间、平均吞吐量等指标，且不低于单位时间内的数据生产能力；
h) 访问控制性、数据加密正确性、数据完整性、内部数据抗讹误性、缓冲区溢出防止率、数字签名使用率、系统日志保留满足度等信息安全性测度要求；
i) 设备可访问性、数据更新的时间延迟、数据值可跟踪性、数据可用性比率、数据可用概率、数据可恢复性比率等依赖应用系统的数据质量测度要求。

4.3.2 承载能力极限状态

通常，应考虑设备故障或损坏、业务量超过系统设计最大容量等因素，且应用软件系统无法通过降级运行、应急运行等运行模式保证应用系统鲁棒性。以下情形应认为超过了承载极限状态：

a) 应用软件系统因访问量过大或超过计算性能限制而持续性失去响应或响应时间超过用户最长可忍耐时间，且无法采取技术措施缓解或恢复；
b) 应用软件系统经常性出现数据泄露、数据篡改、信息丢失等情况，且无法恢复；
c) 设备故障、被干扰或被破坏，应用软件系统无法正确处理数据或运行状态持续性不稳定，且无法恢复；

承载能力极限状态应重点监控资源利用率方面的指标，以防止出现系统失效或数据破坏。包括：

d) 最大数据生产能力状态下，主要设备的 CPU/GPU 平均使用率、内存平均使用率、I/O 设备平均占用率、平均可用网络带宽、可利用存储容量等。CPU 平均使用率不宜超过 30%，内存平均使用率不宜超过 50%。I/O 设备平均占用率、平均可用网络带宽、可利用存储容量应根据应用系统数据生产能力计算；
e) 按年度计算的平均失效间隔时间、周期失效率、系统可用性、平均宕机时间、平均故障通告时间、平均恢复时间等可靠性测度。

5 工程架构设计

5.1 约束和依赖条件

确定工程架构规格与指标时，首先应明确约束和依赖关系，包括：假设与依赖、约束条件、已有信息资源利用、采购限制等内容。

工程架构设计除符合本文件要求外，还应符合《DB21/T 3758-2023》第6.3.3节要求。

5.1.1 假设与依赖

列出适用于工程架构设计要求的任何假设和依赖，这些条件是设计的基础：

a) 需求假设。利益相关方需求规格说明和系统需求规格说明已经审核，业务需求规格已经验证；
b) 质量假设。质量需求已经基本明确，产品质量、数据质量、使用质量的测度元素已被定义。

5.1.2 约束条件

描述由外部标准、监管要求或项目限制对系统设计施加的约束，包括：

a) 法律依据及主要条文的约束；
b) 监管要求或约束；
c) 应遵循的标准规范名称、条文的约束；
d) 正在执行的标准规范；
e) 已有的主数据/参考数据/数据资产等对系统的限制或要求；
f) 对组织全局数据的可用性和可访问性的可能限制；
g) 描述在成本和时间范围内执行项目的限制；
h) 其他限制，如：技术限制、资源限制、人员限制等。

5.1.3 已有信息资源利用

描述信息资源复用要求，包括：基础设施、存储备份资源技术支持资源、运维资源、管理制度等。

5.1.4 采购限制

提供任何将限制供应商选择的其他项目的总体描述，包括：

a) 硬件限制（例如，信号时序要求）；
b) 与其他应用程序的接口；
c) 质量要求（例如，技术支持、维修期等）；
d) 安全方面的考虑因素；
e) 来自其他系统的限制，包括通过接口从受控系统获取的实时要求。

5.2 工程架构规格

完整的工程架构设计应包括：应用系统说明、运行环境设计、验证与测试环境设计等内容。

5.2.1 应用系统架构说明

应根据《应用系统工程 应用软件架构设计规范》（立项编号2024013）提出的应用系统架构模型，以图表形式体现机房环境、计算环境、终端环境、安全环境、网络环境与应用软件系统之间的关系及构成要素，并描述以下应用软件系统规格特征：

a) 应用软件系统与子系统划分，描述构成元素及其相互关系：算力与存储资源、终端设备、网络链路、逻辑数据库、系统软件与支撑软件等；
b) 描述应用软件系统的主要规格，包括：应用软件系统/子系统名称、数据生产能力、主要性能效率指标、容量指标、外部接口等；
c) 应用软件系统与直接用户的逻辑关系及用户数量，与终端的对应关系及终端数量、信息呈现设备与输入控制设备；
d) 根据应用软件系统的内存资源配置、存储容量配置、带宽要求等资源要求，分别计算最低资源消耗和最高资源消耗范围，给出计算过程及计算结果；
e) 根据应用软件系统定义的极限状态、运行模式，计算主要计算设备、存储设备和终端配置最低配置要求；

f） 描述应用系统网络安全等级保护级别和密码应用保护级别；
g） 如配置了唯一来源的设备/软件，或使用不可替代产品，则应给出说明和理由。

5.2.2 机房环境

描述机房要求，明确核心机房环境、备份环境、终端设备基础设施等内容要求，给出核心机房环境的选择理由和依据，如：数据安全性要求、技术理由、复用资源等。还应说明以下内容：

a） 机房基本情况，如：机房级别、电力供应能力、技术支持能力、综合布线情况、互联网带宽、机房服务模式等；
b） 对存储核心数据、重要数据的基础设施、备份环境，应说明机房环境提供商的资质、管理能力、设备生产商等要求；
c） 应说明数据采集设备、传感器等物联网设备的环境要求，包括：供电方式与供电能力、通信方式与速率、基础结构与防护能力、运行状态监控、维修维护、运行费用来源等；
d） 对移动智能终端设备等终端设备，应简要说明：资产管理与日常维护管理、维修与技术支持方法、运行费用来源等；
e） 描述设备搬迁、系统迁移等情况。

注：核心数据、重要数据是指符合《数据安全法》规定的数据分类分级保护制度要求的数据。

5.2.3 计算环境

定义计算环境概念模型，描述应用软件系统/子系统、设备类型与数量、设备部署等内容：

a） 明确设备上运行的应用软件系统/子系统，描述该设备应配置的系统软件、支撑软件。应对设备分配唯一标识并同需求基线对应；
b） 按照应用软件系统极限状态要求，给出计算设备、存储设备的内存/显存配置、硬盘容量、带宽、网络端口数量等计算过程和结果，并作为最低配置要求；
c） 给出主要设备的技术支持、维修维护等细节，以满足设计使用年限要求；
d） 给出主要设备的物理规格要求、能耗要求和部署位置，包括：物理位置、与其他设备的相互关系等内容；
e） 明确主要设备的系统软件、支撑软件、安装调试技术要求、工作内容与工作量等内容；
f） 如配置了唯一来源的设备/系统软件/支撑软件等，或使用不可替代产品，则应给出说明和理由；
g） 应避免提出技术细节，以保证设计使用年限内设备的可替换性，满足系统生命周期需要。

5.2.4 终端环境

描述应用软件系统/子系统、终端设备类型与数量、设备部署等内容：

a） 明确终端设备上运行的应用软件系统/子系统或主要功能，描述该终端设备应配置的系统软件、支撑软件。应对每种终端设备类型分配唯一标识并同需求基线对应；
b） 应明确单台终端设备的业务量。必要时，应描述对应算力设备上的业务量；
c） 应根据应用软件系统数据值精度要求，给出物联网设备、输入输出设备，如：传感器、打印机、扫描仪等终端设备的精度要求；
d） 说明每种类型的物联网设备环境要求，包括：供电方式与供电能力、基础结构、电磁防护能力、通信方式与速率、运行状态监控、维修维护方式等、运行费用来源等；
e） 给出物联网设备的物理规格要求、能耗要求、技术支持要求、维修维护要求等内容；
f） 明确主要终端设备的系统软件、支撑软件、部署要求、安装调试技术要求、工作内容与工作量等内容；
g） 如配置了唯一来源的终端设备使用不可替代产品，则应给出说明和理由。

5.2.5 安全环境

描述应用软件系统/子系统、终端设备类型与数量、设备部署等内容：

a) 明确设备的主要安全功能、性能和安全防护范围，安全防护范围应描述应用系统名称、用户类型、安全风险等内容。应对安全设备分配唯一标识并同需求基线对应；
b) 按照应用系统极限状态要求，给出安全设备的安全性能、端口性能与数量等计算过程和结果，并作为最低配置要求；
c) 描述安全设备部署特点并估算安装调试工作量；
d) 明确安全设备的验收与测试要求，如：检测报告、自检、试运行要求、知识产权证明文件以及法律法规要求的其他证明文件；
e) 如配置了唯一来源的安全设备，或使用不可替代产品，则应给出说明和理由。

5.2.6 网络环境

定义网络环境概念模型或系统图，描述网络环境划分、设备类型与规格、设备部署等内容：

a) 应描述计算设备、安全设备、终端设备、存储备份系统以及应用系统的逻辑位置和运行区域等内容，清晰完整体现网络区域划分、链路类型、访问路径等内容；
b) 核心数据、重要数据的管理及存储，应设置单独区域并同其他区域隔离；
c) 应合理规划、分配网络地址。当使用 TCP/IP 协议时，应同时支持 IPv4 和 IPv6 协议；
d) 明确网络设备的类型及数量，对设备分配唯一标识并同基线需求表对应；
e) 按照应用系统极限状态要求，给出网络设备的网络性能、端口数量与性能等计算过程和结果，并作为最低配置要求；
f) 给出网络设备的主要物理规格要求并估算安装调试工作量等内容；
g) 如配置了唯一来源的网络设备，或使用不可替代产品，则应给出说明和理由。

5.2.7 存储备份系统

存储备份系统应对程序文件、技术文档、数据库、数据文件等应用系统运行所需要的所有电子文件进行备份，能够实现全量备份、增量备份、差分备份、按时间点恢复、按应用系统恢复、按数据类型恢复等方式。

描述存储备份系统构成、设备类型与数量、设备部署等内容：

a) 存储备份系统由存储设备、管理软件和备份介质构成；
b) 明确存储备份设备的类型及数量，对设备分配唯一标识并同基线需求对应；
c) 按照应用系统极限状态要求，给出存储备份设备的网络性能、端口数量、容量要求等计算过程和结果，并作为最低配置要求；
d) 给出存储备份系统功能规格说明，包括：存储容量与性能、纠错和自愈能力、数据保护能力、可维护能力、数据验证能力、恢复能力、介质类型及最长保存时间、介质数量等；
e) 单独描述应用系统重建、迁移等状况时的技术措施及恢复策略；
f) 给出设备的主要物理规格要求并估算安装调试工作量；
g) 给出主要设备的可替换性和备份介质消耗，满足系统生命周期需要。

5.2.8 界面与交互设备设施

根据应用软件系统的用户界面与交互要求，提出须配置的信息呈现、信息控制等输入输出设备：

a) 信息控制设备，即输入设备，如：键盘、鼠标、定位器、操纵杆、轨迹球、触控板、数位板和覆盖层、触控屏、触控笔和光笔，以及语音和手势控制设备、体感设备等；

b) 信息呈现设备，即输出设备，如：视觉显示设备、听觉输出设备、触觉反馈设备等。

5.2.9 验证与测试环境

验证与测试环境架构设计只考虑满足应用系统的需求验证、质量与进度检查，应描述以下内容：

a) 一般情况下，应充分利用计算环境、终端环境、网络环境、安全环境的相关设备设施及已有资源进行架构设计；
b) 可以设计必要的设备用于数据采集、格式转换、数据标注等用途，并明确应用系统验收后的用途，如：技术培训、技术支持、运维监测检测、软件更新验证等用途；
c) 应考虑采取临时安全措施保证数据安全、信息安全。

5.3 应用系统生命周期

描述应用系统的设计使用年限、运行阶段与退役阶段等概念，明确相关依据及技术支持要求：

a) 明确设计使用年限，给出理由和依据；
b) 明确运行阶段质量保证要求：
    1) 支持机构及技术人员要求；
    2) 技术支持设备、设施与支持软件要求；
    3) 运行环境设备维修及更换标准；
    4) 备品备件要求及供应方法；
    5) 定期检测与维护周期；
    6) 运行阶段培训要求；
    7) 故障数据采集与报告；
c) 明确退役阶段的处置要求：
    1) 描述相关设备设施销毁、储存、回收或再利用等要求；
    2) 资料、数据归档与保存。

5.4 工程架构设计方案选择

通常，至少应考虑两种不同的应用系统架构设计方案。工程架构设计方案评选可以采用专家评审、第三方评估、用户审议等方法。

评选时，应说明架构设计方法，明确每种设计方案的投资估算、建设工期、数据生产能力指标、设计使用年限、预期的用户群体满意度等主要规格。

6 指标体系

通过量化指标体现应用系统的设计与施工质量，称之为应用系统的指标体系。指标体系包括：

a) 数据生产能力；
b) 极限状态；
c) 应用软件系统指标；
d) 系统运行状态与模式；
e) 界面与交互指标；
f) 综合技术经济指标。

6.1 数据生产能力

数据生产能力类指标包括：年数据生产能力、日数据生产能力、单位时间数据生产能力、最大数据生产能力、最小连续生产时间、最大在线用户数、最大并发用户数等指标构成：

a) 应根据《DB21/T 3759-2023 应用系统工程 关键性评价指标》，提出每个应用系统的指标要求；
b) 应提出应用系统的年度数据资产指标和设计使用年限内总数据资产指标；
c) 宜提出主数据、参考数据相关的指标，如：年度主数据数量规模、参考数据贡献规模等。

6.2 极限状态

按照第4.3节要求确定应用系统极限状态指标。

6.3 应用软件系统指标

按照GB/T 25000系列标准确定测度与指标值，包括：产品质量、数据质量和使用质量。

6.4 系统运行模式

描述应用系统支持的运行模式。运行模式包括：常规、降级、备份、批量作业、维护、培训、紧急、飞行模式和空闲模式等。通常，应用系统至少应支持常规、降级、紧急运行模式。应描述每种运行模式的以下内容：

a) 描述对操作时间的限制；
b) 可能受到的安全限制；
c) 对用户操作人数的限制；
d) 对计算资源的限制；
e) 对运行地点或基础设施的限制；
f) 运行模式对应的用户类别、功能、数据处理权限。

6.5 界面与交互指标

描述设计时应提出的应用系统界面与交互指标，包括：

a) 有效性测度，包括：任务完成率、目标实现率；
b) 按用户群体提出效率测度，包括：任务用时与时间效率指标、成本效率；
c) 按用户群体提出满意度测度，包括：总体满意度、特征满意度、自主使用率、特征利用率、用户愉悦性、身体舒适性等。

此外，宜提出运行阶段的用户界面与交互指标，包括：

a) 有效性测度，包括：任务中的差错数、出错任务率、任务差错密度；
b) 按用户群体提出效率测度，包括：生产性时间比、非必要动作率、疲劳影响；
c) 按用户群体提出满意度测度，包括：用户投诉率、具体特征用户投诉率、用户可信性等。

6.6 综合技术经济指标

定义应用系统的综合技术经济指标，包括：按功能规模计算的功能点综合单价指标、按年数据生产能力计算的造价指标、应用软件投资占比、基础设施投资占比等。

给出综合技术经济指标计算公式、计量要求。

7 设计图纸与工程量清单

7.1 设计图纸要求

应按照《DB21/T 3758-20231 应用系统工程 初步设计文件规范》6.2节、6.3节、6.6节、6.7节要求绘制工程架构设计图。

此外，还应遵循《GB/T 1526-1989 信息处理 数据流程图、程序流程图、系统流程图、程序网络图和系统资源图的文件编制符号及约定》。

7.2 工程量清单规格要求

汇总架构设计的成果，以表格的形式明确：应用系统标识、应用软件系统/子系统/作业标识、设备标识、设备类型、数量、计量单位、主要规格、安装调试工作量等信息。

工程量清单规范还应符合《DB21/T 3757-2023 应用系统工程 工程造价咨询规范》第6.2节要求。