基于数字孪生技术在AA信息安全领域的探索与应用
项目技术支持服务项目合同

甲方： 河南省AA公司郑州市公司

乙方： 郑州BB科技有限公司

依据《中华人民共和国民法典》的规定，协议双方就基于数字孪生技术在AA信息安全领域的探索与应用项目技术支持服务项目的合作事宜，本着友好合作、长远发展的目的，在互利互惠的原则下，经协商一致，签订本合同。

1. 服务内容、形式和要求

受甲方委托，乙方向甲方提供基于数字孪生技术在AA信息安全领域的探索与应用项目技术支持服务项目技术服务，具体内容见附件技术要求。

2. 乙方的责任

1．乙方负责按甲方规定的内容和时间进度，安排相关人员进行开发工作。

2．乙方按甲方的规定，在甲方的协助下完成各阶段的工作成果。

3．乙方承诺在本合同及其相关附件的履行过程中，乙方所使用的相关资料、方法、工具、手段和工作成果不存在侵犯他人合法权益及违反与第三方之间约定的情况。

3. 甲方的责任

1．与乙方协商确定《基于数字孪生技术在AA信息安全领域的探索与应用项目》的实施计划，协调内部资源，配合和协助乙方开展工作，为乙方提供必要的工作条件。

2．甲方需对项目实施过程进行监督和管控，确保项目按计划推进并达到预期效果。

3．有关本合同之签订、履行、变更、解除、终止等相关事宜以及与之对应的合同附件等相关法律文件，只有加盖甲方公章或者合同专用章的情况下才是甲方的真实意思表示。

4. 验收标准和方式

合同签订后30个工作日完成项目验收，甲方出具加盖印章或授权人签字的验收意见。

验收标准：乙方完成虚拟化平台部署实施，提供相关证明材料；乙方完成对接设备的调试

及相关技术测试，提供相关证明材料。

5. 合同金额及其支付方式

1．本合同金额总计（大写）人民币 ：拾万陆仟元整（小写：¥106000.00）。合同明细如下：

序号	名称	描述	单价	数量	小计	备注
1.	虚拟化平台部署实施	对支撑服务运行的虚拟化平台进行部署，满足服务运行要求，提供相关软件授权等。	40000	1 项	40000	
2.	设备对接及调试	完成与数据中心相关安全设备的对接调试工作，包括防火墙、防病毒等，并完成相关功能调试。	40000	1 项	40000	
3.	软件测试	对项目所涉及软件进行功能测试、稳定性测试等。	26000	1 项	26000	
合计					106000	

2．支付方式

项目验收合格 15 日内，乙方向甲方开具全额增值税专用发票，技术服务增值税税率 6%，甲方收到发票后 10 个工作日内给乙方支付合同总金额 100％款项,共计人民币拾万陆仟元整（小写：¥106000.00）。

6. 违约条款

1．任何一方未履行本合同约定的任何一项条款均被视为违约，甲方有权按照技术协议中的相关条款追究违约责任。

2．若乙方逾期完成基于数字孪生技术在 AA 信息安全领域的探索与应用项目，每逾期一周，需支付合同金额 1% 的违约金，逾期超过 90 天，甲方有权单方解除合同，乙方需要在解除合同后的 20 个工作日内退回甲方已经支付的合同价款。

3．任何一方在收到对方的具体说明违约情况的书面通知后，应在 5 个工作日内对此确认或提出书面异议或补充说明，否则视为其接受书面通知所述内容。在此情形下，双方应对此问题进行协商，协商不成的，按本合同第八条之约定解决。

7. 风险责任的承担

若一方因不可抗力（包括：战争、地震、洪水、瘟疫、恐怖活动）不能履行本合同的，不承担本合同中确定的违约责任，但因不可抗力不能履约的一方，必须及时将该情况以正式书面形式于不可抗力发生日起 5 个工作日内通知对方。否则，应承担相应的法律责任。

8. 解决协议纠纷的方式

在履行本合同的过程中发生争议，双方当事人和解或调解不成，双方同意采用以下第 2 种方式解决纠纷：

1．双方同意由 / 仲裁委员会仲裁。

2．双方约定向 甲方所在地 人民法院起诉。

9. 知识产权

双方确定，因履行本合同所产生的研究开发成果及其相关知识产权权利归属，按下列方式处理：

履行本合同产生的成果归 甲 方所有。

10. 保密条款

双方均有责任对项目进行过程中了解到的对方资料信息和商业秘密严格保密。

乙方参与本项目的人员应遵守国家、客户、甲方有关保密的法律法规和规定，在本项目执行前、执行期间以及执行后，对所接触和知悉的国家秘密和客户商业秘密都负有保密义务。

双方均不得将本项目的成果物向第三方组织或个人提供。

11. 其它

1．本合同任何一方给另一方的通知，都应以书面形式（信函、传真、电子邮件）发送至对方。

2．项目执行过程中，若甲方提出增加其它与本项目工作计划所规定之外的咨询内容、或者本合同所确定的服务费用不足以完成整个项目，经双方协商后另行签订补充协议书或单项协议书。

3．未尽事宜，双方协商一致签署补充协议，经与本合同同等生效程序后，与本合同具有

同等法律效力。

4．本合同自双方签字、盖章之日起生效。本合同一式 肆 份，甲乙双方各执 贰 份，具有同等法律效力。

12.

13. 附件：技术要求

13.1. 项目背景

鉴于当前网络安全形势愈发严峻，且企业有提升网络安全及信息安全水平的需求，市局在运维管理方面面临诸多问题，包括人员短缺、机房结构复杂、设备种类繁多且分布广泛、各系统独立运行、时效性要求高、管理难度大以及协同处置困难等状况。郑州市局计划采用数字孪生仿真、C4D 模型设计、MBD 模型设计理念以及 MBE 数字企业技术，对网络环境和安全状况进行数字定义、建模与展示，从而完善对网络空间安全状态的认知。同时，借助数据分析，运用自动化运维技术实现各类运维场景流程，自动开展网络空间的安全评估、预测性防护、应急演练等工作，拓展网络安全态势感知的范围，提升其智能化程度，推动网络空间安全方案的改进，进一步促进 AA 行业信息安全数字化转型升级，以数字驱动数据安全，以数据驱动智能决策，为 AA 信息安全管理数字化赋能提供有力保障，加速 AA 行业信息安全转型进程。

依据《“十四五”软件和信息技术服务业发展规划》和《“十四五”信息化和工业化深度融合发展规划》文件要求，设计仿真系统软件，突破三维几何建模引擎、约束求解引擎等关键技术，探索开放式工业软件架构、系统级设计与仿真等技术路径，基于模型的系统工程产品研发。优化信息技术服务，面向数字化、网络化、智能化应用需求，加强典型场景下的算法服务，推进企业级业务连续性管理（BCM）相关技术创新。围绕数字化管理咨询、一体化集成、智能运维等，完善信息技术服务体系，提升 AA 行业专业化信息技术服务能力。支撑构建具备感知力、控制力和决策力的信息技术服务生态。

数字孪生技术是以物理实体真实场景数据为依托，以真实和仿真模型运行数据实时交互优化为机制，自运行的虚拟空间映射模型，对大到城市、小到设备原件的实物均可虚拟化表示，因此完全可以根据虚拟模型对物理资产进行管理。其主要价值体现在描述、分析、诊断、预测四个方面，描述价值指的是数字孪生技术可以对物理资产的数据进行虚拟化描述，有利于对物理资产进行实时监测；分析价值指的是虚拟化数字孪生模型可以直接根据物理资产数据分析其中的不足，有利于改进物理资产的性能；诊断价值指的是虚拟化模型能够对历史数据中的相关关系进行分析，有利于发现某些问题的真实原因；预测价值指的是虚拟化模型能够在数字孪生技术的支持下预测物理资产未来的发展状态，有利于管理人员对管理策略进行优化。

信息安全数字孪生系统数据可视化大屏基于数字孪生仿真、C4D 模型设计、MBD 模型设计理念、MBE 数字企业技术，实现了全网安全态势感知、关键网络安全设备状态、机房动力及环境、设备资产等设备 24 小时实时智能化监管。

自动化运维方面依据信息安全数字孪生系统数据可视化大屏数据决策，基于人工智能技术，实现了全网网络安全事件自动化运维应用场景，数据中心无人值守，保障机房环境及设备安全高效运行，实现了数据中心的管理自动化、运行智能化和决策科学化。

13.1.1. 验证数字化运维管理模式

数字化运维管理模式是随着数字化时代的到来而兴起的一种新型运维管理模式。它主要通过运用数字化技术手段，实现对各类资源和业务的数字化管理，从而提高运维效率、降低运维成本、提高业务的可靠性。数字化运维管理模式的核心是对数据的处理和分析，通过对海量的数据的采集、处理和分析，可以实现对业务状态的实时监测和预警，及时发现和解决潜在的问题。数字化运维平台可以通过提供各种智能化服务（自动化控制、智能化决策等），提高运维管理效率和业务创新能力。

13.1.2. 打通全区网络安全设备

通过智能传感、物联网 SNMP 协议和 SYSLOG 协议等技术，实现全区设备数据链的打通，以实现全业务链数据的实时采集和全面贯通。利用数字孪生技术绘制的三维仿真显示高度还原机房、机柜、设备的结构细节，同时支持网络监控、主机监控、存储监控等系统集成，可实时监测网络设备运行状态，对设备运行异常（故障、过载、过温等）进行实时预警告警。同时，可下钻查看设备具体参数、运行状态、端口详情、网络接口、设备资产负责人等详细信息，辅助运维人员更加直接高效地掌握设备运行情况。

13.1.3. 验证自动化运维场景联动

利用自动化运维技术，可以将全网网络安全设备结合运维业务需求，形成多种应用场景，包括护网、双机设备应急演练、自动化病毒上报处置、安全漏洞自动化管理、自动化巡检、一键断网、防火墙联动封禁等。在实际应用中结合数字孪生可视化大屏联动场景，以便更好地处置安全事件。

13.1.4. 验证网络化协同业务应用

利用数字孪生技术，可以真实地再现物理机房的整体空间环境、设备设施布局和网络拓扑结构图。通过贯通机房动力及环境、设备运行和设备资产等多个维度的数据互融互通，实现网络安全设备的智能管理，从而构建出适应实际运维场景需求的业务应用。数字孪生体管理赋能了数据中心资源监测、机房全景概览、设备运行监测、设备资产监管、网络拓扑结构可视化、动环态势监测、态势感知监测、病毒查杀监测、运维场景执行回执、应急协同处置等业务，使其更加高效便捷。

13.2. 附件 1：虚拟化平台部署实施

13.2.1. 需求调研与分析

与甲方进行深入沟通，全面了解项目的业务需求、服务运行要求以及现有 IT 基础设施状况，包括服务器硬件配置、网络拓扑结构、存储资源等方面的信息。

对收集到的信息进行深入分析，评估天融信超融合软件在甲方环境中的适用性，确定虚拟化平台的规模（如虚拟机数量、资源配置需求等）、性能要求（如 CPU、内存、存储和网络带宽需求）以及安全需求（如网络隔离、数据加密等），为后续制定详细的部署方案提供依据。

13.2.2. 技术方案设计

依据需求调研结果，制定具有针对性的虚拟化平台部署技术方案，涵盖天融信超融合软件的版本选择、服务器硬件配置建议（如 CPU 核心数、内存容量、硬盘类型和容量等）、网络架构设计（如物理网络拓扑、虚拟网络配置、IP 地址规划等）、存储方案规划（如本地存储配置、分布式存储策略等）以及高可用性和备份恢复策略的制定。

明确部署实施计划，将整个部署过程划分为多个阶段，为每个阶段设定明确的任务、责任人、时间节点和交付成果，确保部署工作有序推进。同时，制定详细的测试计划，包括功能测试、性能测试、稳定性测试和兼容性测试等内容，以验证虚拟化平台部署后的各项指标是否符合项目要求。

13.2.3. 环境准备

协助甲方进行服务器硬件环境的准备工作，按照技术方案的要求对服务器进行硬件安装、固件升级、BIOS 设置调整等操作，确保服务器硬件处于最佳状态，满足天融信超融合软件的安装要求。

准备网络环境，依据网络架构设计方案对网络设备（如交换机、路由器）进行配置，包括 VLAN 划分、端口配置、IP 地址分配、路由策略设置等，确保网络通信稳定顺畅，为虚拟化平台的部署提供良好的网络基础。

确认存储资源的可用性和配置情况，按照存储方案规划对本地存储或外部存储设备进行初始化配置，创建存储池、设置存储策略等，为虚拟化平台提供可靠的存储支持。

13.2.4. 软件安装与配置

在准备好的服务器上安装天融信超融合软件，依照软件安装向导进行操作，确保安装过程顺利完成，软件组件正确安装并注册。

对天融信超融合软件进行初始化配置，包括设置节点信息、管理 IP 地址、管理员账号密码等基本参数，配置网络连接（如虚拟交换机设置、VLAN 绑定等）、分配存储资源（如创建存储卷、设置挂载点等）以及设置安全策略（如访问控制规则、防火墙策略等），使虚拟化平台具备初步运行条件。

13.2.5. 虚拟机部署与配置

根据甲方业务需求，创建并部署虚拟机，包括选择合适的操作系统模板、配置虚拟机的硬件资源（如 CPU 核心数、内存大小、硬盘容量和网络连接方式等）、安装操作系统和应用程序，确保虚拟机能够正常运行业务服务。

对虚拟机进行个性化配置，如设置主机名、IP 地址、DNS 服务器、安全组规则等，优化虚拟机的性能（如调整操作系统参数、启用内存优化技术等），使其满足业务系统的运行要求。同时，建立虚拟机的备份和恢复策略，确保虚拟机数据的安全性和可恢复性。

13.2.6. 功能测试与验证

按照测试计划，全面测试虚拟化平台的各项功能，包括虚拟机的创建、启动、停止、暂停、迁移等基本操作功能，网络通信功能（如虚拟机之间的网络连接、虚拟机与外部网络的通信），存储功能（如数据存储、快照功能、克隆功能等），高可用性功能（如虚拟机故障自动迁移、节点故障切换等）以及安全功能（如访问控制、数据加密、入侵检测等）。

对测试结果进行详细记录和分析，及时发现并解决功能缺陷或异常情况。对于发现的问题，进行分类整理，制定问题解决方案，并跟踪问题解决进度，确保所有问题得到妥善解决，使虚拟化平台功能完全符合项目要求。

13.2.7. 性能测试与优化

使用专业的性能测试工具，模拟实际业务场景下的负载情况，对虚拟化平台的性能进行测试。性能测试指标包括虚拟机的响应时间、吞吐量、并发连接数，以及虚拟化平台的 CPU 使用率、内存利用率、存储 I/O 性能、网络带宽利用率等。

根据性能测试结果，分析性能瓶颈所在，如服务器硬件资源不足、虚拟化软件配置不合理、网络延迟过高、存储性能瓶颈等。针对性能瓶颈问题，采取相应的优化措施，如升级服务器硬件、调整虚拟化软件参数（如内存分配策略、CPU 调度算法等）、优化网络配置（如增加网络带宽、调整网络拓扑结构等）、优化存储架构（如更换高性能存储设备、调整存储策略等），提高虚拟化平台的整体性能，确保服务在虚拟化环境下能够高效稳定运行。

13.2.8. 稳定性测试与保障

进行长时间的稳定性测试，模拟虚拟化平台在持续运行状态下的各种情况，观察平台是否出现故障、虚拟机是否异常退出、数据是否丢失等问题。稳定性测试时间应根据项目实际需求确定，一般不少于 72 小时。

在稳定性测试过程中，实时监测虚拟化平台的运行状态，记录各项性能指标和日志信息。对出现的问题及时进行分析和处理，采取有效的措施保障平台的稳定性，如优化服务器散热条件、调整系统资源分配、修复软件漏洞等。确保虚拟化平台在长时间运行过程中能够稳定可靠地工作，为业务系统提供持续的服务支持。

13.3. 附件 2：设备对接及调试

13.3.1. 设备对接及调试清单

设备分布	设备清单
	深信服办公网防火墙主、深信服办公网防火墙备、天融信内网防火墙主、天融信内网防火墙备、深信服上网行为管理、天泰 WEB 应用防火墙、山石互联网防火墙主、山石互联网防火墙备、互联网出口负载、运维区防火墙、天融信数据库审计、盈高安全准入、深信服 VPN 主、深信服 VPN 备、带外管理、网御漏洞扫描、深信服无线控制器、奇安信流量探针、奇安信天眼态势感知、帕拉迪堡垒机、工控主机安全监管平台、VPN 外置数据中心、AC 外置数据中心、奇安信杀毒平台、天融信日志审计、市局负载、Security-SW。
	卷烟配送中心防火墙、工控防火墙、工业审计系统、工控日志审计、工控堡垒机、工控入侵检测、锐捷交换机、省局路由器 h3c56-60－主、省局路由器 h3c56-60－备、核心交换机-主、核心交换机-备、办公网汇聚交换机、huawei5720-10#、huawei5720-9#、huawei5720-8#、huawei5720-7#、huawei5720-6#、huawei5720-5#、huawei5720-4#、huawei5720-3#、huawei5720-2#、huawei5720-1#、1F_S3352_1、1F_S3352_2、1F_S3328_3、2F_S3352_1、2F_S3352_2、2F_S3328_1、3F_S3352_1、3F_S3352_2、3F_S3328_1、4F_S3352_1、4F_S3352_2、4F_S3328_3、5F_s5700_1、5F_S3352_2、5F_S3328_3、6F_S3352_1、6F_s3352_2、6F_S3328_3、6F_S5700_4、7F_S3352_1、7F_S3352_2、7F_S3328_3、8F_S3352_1、8F_S3328_2、9F_S3352_1、物流中心、DMZ-SW。
	负载
	负载
	负载
	负载
	负载
	负载
	负载
	负载
	负载
	负载

13.3.2. 需求调研与分析

与甲方进行深入沟通，全面了解数据中心的现有网络架构、业务系统布局、安全策略要求以及已部署安全设备的状况，包括设备品牌、型号、配置信息和运行状态等。

对收集到的信息进行深入分析，评估设备对接及调试的可行性和潜在风险，确定项目的技术难点和重点关注领域，为后续制定详细的技术方案提供依据。

13.3.3. 技术方案设计

根据需求调研结果，制定针对性的设备对接及调试技术方案，包括设备选型与配置建议（如防火墙策略配置、防病毒软件部署方案等）、网络拓扑调整计划、数据交互与同步机制设计、安全功能联动策略制定等。

明确测试计划和验收标准，测试计划应涵盖功能测试、性能测试、稳定性测试、兼容性测试等方面，确保设备对接后各项功能正常、性能满足业务需求、系统稳定可靠且与现有环境兼容良好；验收标准应具体、可量化，明确规定各项测试指标的合格范围。

13.3.4. 设备安装与初始化配置

协助甲方进行防火墙、防病毒等安全设备的安装工作，确保设备安装位置恰当、硬件连接牢固且电源供应正常，严格遵循设备厂商的安装规范和最佳实践准则。

对安全设备实施初始化配置，具体包括设置设备名称、IP 地址、子网掩码、默认网关、管理员账号密码等基本参数，同时进行系统时间同步以及日志存储位置设置等操作，为设备后续的对接调试工作奠定基础。

13.3.5. 网络连接与配置

依据数据中心网络拓扑结构，合理规划安全设备在网络中的接入位置，确保设备与服务器、终端等设备之间的网络连接稳定可靠。针对网络设备（如交换机、路由器）开展配置工作，涵盖 VLAN 划分、端口配置、IP 地址分配、路由策略设置等内容，实现安全设备与网络环境的无缝衔接。

优化网络配置参数，例如调整 MTU（最大传输单元）大小、缓冲区设定、QoS（Quality of Service）策略等，以提升网络性能和数据传输效率，保障安全设备在网络中的正常运行不受网络拥塞或延迟的影响。

13.3.6. 设备间数据交互与联动调试

配置防火墙、防病毒等安全设备之间的数据交互接口和协议，确保设备能够精准采集并传输相关安全数据，如网络连接信息、访问日志、病毒事件信息等，实现数据的实时或定时同步，

保证网络安全智慧指挥中心系统能够及时获取最新的安全信息。

制定设备间的联动策略，依据安全事件的类型和严重程度，实现防火墙与防病毒设备之间的协同工作。比如，当防病毒设备检测到病毒爆发时，联动防火墙阻止感染源的网络访问；当防火墙发现异常流量时，通知防病毒设备加强对相关流量的扫描和检测。全面测试联动功能，模拟各类安全事件场景，验证联动的及时性和准确性。

13.3.7. 功能测试与验证

按照测试计划，全面测试设备对接后的各项功能。功能测试内容包括但不限于防火墙的访问控制功能（验证策略是否生效，能否正确阻止非法访问并允许合法访问）、NAT（网络地址转换）功能（测试地址转换的正确性和有效性）、VPN（虚拟专用网络）功能（测试隧道建立、数据加密传输、用户认证等功能）、防病毒设备的病毒检测与清除功能（运用已知病毒样本和模拟病毒感染场景，验证设备的检测和清除能力）、设备间联动功能（检查联动是否依策略执行，能否有效应对安全事件）等。

详细记录并深入分析测试结果，及时察觉并解决功能缺陷或异常状况。针对发现的问题进行分类整理，拟定问题解决方案，并跟进问题解决进程，确保所有问题均得到妥善处置，使设备功能完全符合项目要求。

13.3.8. 性能测试与优化

运用专业的性能测试工具，模拟实际业务场景中的网络流量和负载状况，对设备对接后的整体性能展开测试。性能测试指标涵盖防火墙的吞吐量（设备在单位时间内能够处理的数据量）、并发连接数（设备能够同时处理的网络连接数量）、延迟（数据从发送端到接收端所需的时间）、防病毒设备的扫描速度（单位时间内能够扫描的文件数量或数据量）、系统资源利用率（如 CPU 使用率、内存占用率等）等。

依据性能测试结果，剖析性能瓶颈所在之处，诸如设备硬件配置不足、软件配置不当、网络带宽受限等。针对性能瓶颈问题，实施相应的优化举措，如升级设备硬件、调整设备配置参数（如缓冲区大小、连接超时时间等）、优化网络拓扑结构（增加网络带宽、优化路由策略等），提升设备对接后的整体性能，确保系统在高负载情况下仍能稳定运行，满足业务需求。

13.3.9. 稳定性测试与保障

开展长时间的稳定性测试，模拟设备在持续运行状态下的各类情形，观察设备是否发生故障、性能是否下降、数据是否丢失等状况。稳定性测试时长应依据项目实际需求确定，通常不少于 72 小时。

在稳定性测试期间，实时监控设备的运行状态，记录设备的各项性能指标及日志信息。对出现的问题及时予以分析与处理，采取有效措施确保设备的稳定性，如优化设备散热条件、调整系统资源分配、修复软件漏洞等。保证设备在长时间运行过程中能够稳定可靠地工作，为业务系统持续提供安全防护。

13.4. 附件 3：软件测试

13.4.1. 测试及验证功能清单

序号	模块	二级菜单
1.	工作台	
2.	智慧运维	运维计划
3.		运维任务
4.		场景管理
5.		流程管理
6.		处置报告
7.		任务下派
8.	场景市场	新建模板
9.		模板管理
10.	智慧展示	指挥中心大屏
11.		机房动环监控大屏
12.		全区大屏
13.		重保大屏
14.	数据分析	态势感知
15.		网络病毒
16.		告警中心
17.		护网分析
18.		告警处置
19.	工单管理	提交工单
20.		审批中心
21.		数据管理

22.		工单模板
23.	设备管理	设备台账
24.		配置管理
25.		SNMP 管理
26.		关联场景
27.	智慧库	新建文档
28.		文档管理
29.		草稿箱
30.		类型管理
31.		安全报告
32.	人员管理	用户管理
33.		角色管理
34.		组织管理
35.	重保管理	重保大屏
36.		重保管理
37.	消息推送	推送管理
38.		渠道管理
39.		推送记录
40.	系统管理	全局参数
41.		操作日志
42.		企业定制

13.4.2. 测试计划制定

于项目启动阶段，依据项目需求文档、设计文档以及相关标准，制定详尽的软件测试计划。测试计划需涵盖测试目标、测试范围、测试策略、测试资源分配、测试进度安排、风险评估与应对措施等内容，以保障测试工作具备明确的方向与规划。

清晰明确功能测试和稳定性测试的具体目标与重点。功能测试的目标在于确保软件系统各项功能契合需求规格说明书之要求，全面覆盖所有功能模块与业务流程，包括正常业务场景、异常业务场景以及边界值情形等。稳定性测试的目标则是评估软件系统于长时间运行及高负载状况下的稳定性与可靠性，确保系统不会出现内存泄漏、资源耗尽、崩溃或异常退出等问题。

13.4.3. 功能测试

13.4.3.1. 测试用例设计

依据需求规格说明书，运用等价类划分、边界值分析、因果图、决策表等测试用例设计方法，为各功能模块设计全面且详细的测试用例。测试用例应包含测试场景描述、输入数据、预期输出结果、执行步骤以及实际测试结果等信息，以保证对软件功能实现全面覆盖与精确验证。

针对项目中的数字孪生技术应用，专门设计测试用例，用于验证数字孪生模型与物理实体之间的数据交互与同步是否精准实时，模型能否真实反映物理实体的状态变化，以及基于数字孪生模型的数据分析和应用功能是否正确实现，例如网络流量分析、安全评估、预测性防护等功能的准确性与有效性。

13.4.3.2. 功能测试执行

测试人员严格依照测试用例执行功能测试，详尽记录测试过程中所发现的问题，包括问题描述、发现时间、出现频率、所属功能模块等信息。对于发现的缺陷，及时提交至缺陷管理工具中，予以跟踪和管理。

在测试过程中，着重对软件界面的友好性、操作的便捷性以及数据的准确性和完整性展开检查。确保软件系统便于使用，用户操作流程符合逻辑，数据在各个功能模块之间的传递与处理准确无误，不会出现数据丢失、篡改或不一致的情形。

13.4.3.3. 缺陷管理与跟踪

建立严格的缺陷管理流程，对提交的缺陷实施分类、分级和优先级排序。缺陷分类可涵盖功能缺陷、界面缺陷、性能缺陷、兼容性缺陷等；分级可依据缺陷的严重程度划分为致命、严重、一般和轻微等级别；优先级则根据缺陷对业务的影响程度及修复的紧急程度予以确定。

及时将缺陷分配给开发人员进行修复，并跟踪缺陷的修复进度。在缺陷修复后，开展回归测试，验证缺陷是否已被彻底解决，确保修复过程未引入新的问题。对缺陷的处理过程与结果进行详细记录，形成缺陷报告，为项目质量评估及后续改进提供依据。

13.4.4. 稳定性测试

13.4.4.1. 测试环境搭建

模拟真实生产环境构建稳定性测试环境，确保测试环境与实际运行环境在硬件配置、操作系统、数据库系统、中间件、网络环境等方面具备高度的一致性与兼容性。涵盖服务器硬件参数（如 CPU 型号、内存大小、硬盘类型和容量等）、操作系统版本及补丁级别、数据库软件及其配置、应用服务器及相关组件的设置等，尽可能还原软件系统在实际运行中的各类条件。

配置测试工具，如性能测试工具中的负载生成器、监控代理等，确保测试工具能够精准模拟多用户并发访问和高负载场景，并且能够实时采集与分析系统的性能数据。

13.4.4.2. 稳定性测试方案设计

设计合理的稳定性测试方案，确定测试的持续时间、负载模式和负载级别。持续时间应足够长，以充分暴露软件系统在长时间运行过程中可能出现的稳定性问题，一般建议不少于 72 小时；负载模式应模拟实际业务场景中的用户行为模式，如并发用户登录、数据查询与更新、文件上传下载等操作的混合模式；负载级别应逐步递增，从低负载至高负载，直至达到或超越系统设计的最大负载能力，观察系统在不同负载条件下的稳定性表现。

针对项目中的数字孪生系统，考虑在稳定性测试过程中模拟大量设备数据的实时采集、传输、处理和分析场景，以及各类安全事件的频繁触发情况，确保数字孪生系统于复杂业务环境下的稳定性与可靠性。

13.4.4.3. 稳定性测试执行与监控

依照稳定性测试方案执行测试，在测试过程中，实时监控软件系统的各项性能指标，如 CPU 使用率、内存占用、磁盘 I/O、网络流量、响应时间、事务处理成功率等。借助性能监控工具生成性能曲线和报表，直观呈现系统性能随时间的变化趋势，及时察觉性能瓶颈和潜在的稳定性问题。

同时，密切留意系统的日志信息，记录系统在运行过程中出现的任何异常情况，如错误日志、警告信息等。对系统出现的崩溃、异常退出、无响应等严重问题进行详细剖析，收集相关的内存转储文件、日志文件和系统状态信息，为问题定位与解决提供依据。

13.4.4.4. 稳定性问题分析与解决

对稳定性测试过程中发现的问题展开深入分析，确定问题的根本原因。问题分析可能涉及多个方面，如软件代码缺陷、资源竞争、内存管理问题、配置不当、外部接口异常等。通过代码审查、调试工具、性能分析工具等手段，逐步排查问题，定位问题所在的代码模块或系统组件。

针对稳定性问题制定有效的解决方案，可能包含代码优化、调整资源配置、修复软件漏洞、改进系统架构等措施。在问题解决后，进行再次稳定性测试，验证问题是否已得到彻底解决，确保软件系统的稳定性和可靠性得到有效提升。

13.5. 附件 4：技术服务文档交付

乙方提供的技术服务文档包括：

1. 虚拟化平台部署实施技术文档
2. 设备对接及调试技术文档
3. 测试报告