附件 2

项目类别：信息安全

编　　号：

河南省 BB 公司郑州市公司
创新项目申报书

项　目　类　别	信息安全
项　目　名　称	数字孪生技术在 BB 信息安全领域的探索与应用
归口申报单位	河南省 BB 公司郑州市公司
主要承担单位	河南省 BB 公司郑州市公司
协　作　单　位	
申　报　日　期	2023 年　5 月 22 日

河南省 BB 公司郑州市公司

填 报 说 明

一、申请河南省BB公司郑州市公司管理创新项目必须填报本“申报书”。

二、“申报书”要求打印，A4纸装订。

三、请按栏目要求，实事求是，逐条认真填写，概念、术语、表达简洁明确，符合规范，并使用标准计量单位。

四、需选择填写的栏目请在类别题目前圆圈中划勾，本“申报书”可以复印使用，栏目空格不够填写时可以加页，但要加贴整齐 。

五、申报书所列归口申报单位为各直属单位，市局机关各部门申报项目，不需填报归口申报单位。

六、“申报书”编号由郑州市BB公司科技管理部门填写。

七、本“申报书”一式贰份或根据要求份数填写。

一、项目名称（<25 字）

数字孪生技术在 BB 信息安全领域的探索与应用

二、项目类别

○卷烟营销	○专卖管理	●信息安全	○大数据
○物流管理	○人事劳资	○党建群团	○科技管理
○安全管理	○规范管理	○财务审计	○经济运行
○企业文化	○其它类_____		

三、项目起止日期

2023 年 3 月至 2024 年 2 月

六、项目经费预算表

经费来源预算（万元）		经费支出预算（万元）			
科　目	总预算数	科　目	市公司拨付经费	自筹经费	总预算数
来源预算合计	28.1	支出预算合计	28.1		28.1
（一）市公司拨付经费		（一）直接经费			
其中：2022 年	0	1. 设备费			
2023 年	28.1	2. 材料费			

<table>
<tr><td colspan="2">2024 年</td><td></td><td>3. 测试化验加工费</td><td>13</td><td></td><td>13</td></tr>
<tr><td colspan="2">（二）自筹经费</td><td></td><td>4. 燃料动力费</td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">1. （单位名称）</td><td>小计：</td><td></td><td>5. 会议/差旅/国际合作交流费</td><td>2.1</td><td></td><td>2.1</td></tr>
<tr><td>____年：
____年：
____年：</td><td></td><td>6. 出版/文献/信息传播/知识产权事务费</td><td>3.2</td><td></td><td>3.2</td></tr>
<tr><td rowspan="2">2. （单位名称）</td><td>小计：</td><td></td><td>7. 劳务费</td><td></td><td></td><td></td></tr>
<tr><td>____年：
____年：
____年：</td><td></td><td>8. 专家咨询费</td><td>8.2</td><td></td><td>8.2</td></tr>
<tr><td rowspan="2">3. （单位名称）</td><td>小计：</td><td></td><td>9. 外协合作费</td><td></td><td></td><td></td></tr>
<tr><td>____年：
____年：
____年：</td><td></td><td>10. 其他支出</td><td>1.6</td><td></td><td>1.6</td></tr>
<tr><td rowspan="3">4. （单位名称）</td><td>小计：</td><td></td><td rowspan="2">（二）间接经费</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td rowspan="2">____年：
____年：
____年：</td><td rowspan="2"></td></tr>
<tr><td colspan="2">1.....</td><td></td><td></td><td></td></tr>
<tr><td colspan="2"></td><td></td><td>2.....</td><td></td><td></td><td></td></tr>
</table>

自筹经费包括直属单位及系统外单位配套经费。

直接经费测算说明：

1. 设备费：

2. 材料费：

3. 测试化验加工费：13 万元

用于相关软件测试和接口对接等费用，虚拟化平台部署实施费 5 万元，系统设备对接及调试费用 5 万元，软件测试费用 3 万元，合计 13 万元。

4. 燃料动力费：

5. 会议/差旅/国际合作交流费：2.1 万元

用于项目调研、学习考察的差旅费用 5 万元，开展需求调研至少 2 次，每次调研 6 人，预计调研 5 天，差旅标准以 350 元/天测算，2*6*5*350=2.1 万元。

6. 出版/文献/信息传播/知识产权事务费：3.2 万元

(1)软件著作产权登记 2 项，每项 2000 元，合计 2000 元×2 项=0.4 万元。

(2)申请专利 1 项，每项 6000 元，合计 6000×1 项=0.6 万元。

(3)发表 2 篇核心论文，按 6000 元/篇，合计 6000 元*2=1.2 万元。

(4)项目研究过程中发生的资料制作、整理等,以及成果推广印制宣传册，课题资料出版制书等费用，预计 1 万元。

7. 劳务费：

8. 专家咨询费：8.2 万元

用于专家指导和咨询费用，具体参照郑州市 BB 公司咨询费发放标准支付。预计邀请创新管理专家就自动化运维、数字孪生管理模式等开展咨询辅导 2 次，每次时间 2 天，按照行业外高级职称标准 2500 元/天计算，2500×2×2=1 万元。

邀请架构建设、技术研发、前端设计、软件设计等技术专家 4 名，开展咨询辅导 3 次，每次时间 4 天，按照行业外中级职称标准 1500 元/天计算，1500×4×3×4=7.2 万元。

9. 外协合作费：

10. 其他支出：1.6 万元

(1)项目评审、验收等费用，预计 1 万元；

(2)购买项目研究相关书籍，预计 0.1 万元；

(3)用于资料印制等其他费用，预计 0.5 万元。

间接经费测算说明：

七、项目内容摘要（<200 字）

针对当前网络安全形势日益严峻和企业提升网络安全信息安全的需求，市局在运维管理方面存在多方面问题，如人员不足、机房结构复杂、设备各类多样、分布广泛、各系统独立运行、时效性要求高、管理难度大、协同处置困难等困境。郑州市局拟采用数字孪生仿真、C4D 模型设计、MBD 模型设计理念、MBE 数字企业技术对网络环境和安全状况进行数字定义、建模和展示，以完善对网络空间安全状态的认知。同时，通过数据分析，使用自动化运维技术实现各种运维场景流程，自动进行网络空间的安全评估、预测性防护、应急演练等，扩充网络安全态势感知的范围和智能化程度，促进网络空间安全方案的改进，进一步推动 BB 行业信息安全数字化转型升级，用数字驱动数据安全、数据驱动智能决策，为 BB 信息安全管理数字化赋能提供有力保障，加快 BB 行业信息安全转型步伐。近年来数字孪生模型逐渐得到人们的重视，该模型对 BB 信息安全系统进一步优化具有积极作用，本文在此背景下对数字孪生模型在 BB 信息安全系统中的应用进行探索。

八、项目预计解决的主要问题与意义简述

（一）预计解决的主要问题

1．解决运维人员和业务人员不足、日常运维繁琐、处理效率低，无法及时响应网络安全问题，以及提升解决信息化安全问题的整体技术能力。

2．解决安全设备单点作战，处于被动式的单点防御模式，无法整合多台设备联机作战防护网络安全问题。

3．解决未能及时识别分析响应网络告警事件，未能有效快速处理能力，导致攻击受害资产的问题。

4．解决全区设备资产盘点不直观、不规范、工作量大、实物不符、闲置浪费和资产流失，以及设备运行告警无法统一管理问题。

（二）项目研究意义

保护信息安全，能够有效地保护企业的信息资产和资源，避免机密信息泄露、数据丢失、网络攻击等风险；优化企业信息安全运维管理流程，提高企业工作效率和业务创新能力，增强信息安全意识，提高信息安全管理水平。

数字孪生技术可以实时的数据处理和分析，可以帮助信息安全领域更好的管理和监测网络系统的安全状态，及时发现和预测的安全威胁和攻击，提高网络系统的安全性和可靠性，保护企业的信息资产和资源，避免经济损失和法律责任。

数字孪生技术在信息安全领域中有广泛的应用,可以提供更好的安全保障和风险管理。以下是数字孪生技术在信息安全领域中的一些应用：

1．威胁建模和分析:通过建立数字孪生模型，可以对网络和系统进行威胁建模和分析。这有助于识别潜在的威胁和漏洞，并预测可能的攻击路径和后果。通过模拟攻击和漏洞利用过程，可以评估系统的弱点，并采取相应的防御措施。

2．安全策略优化:数字孪生技术可以用于优化安全策略和控制措施。通过模拟和仿真不同的安全策略,可以评估其对系统性能和安全性的影响,并找到最佳的安全策略配置。这有助于提高系统的安全性和响应能力，同时减少对业务流程的不必要影响。

3．安全事件响应和演练:数字孪生技术可以用于模拟和演练安全事件的响应过程。通过构建数字孪生环境，可以模拟各种攻击场景和安全事件，让安全团队能够实时演练和调整应对策略。这有助于提高安全团队的应急响应能力和协同工作效率。

4．跨部门合作和信息共享:数字孪生技术可以促进不同部门之间的安全协作和信息共享。通过共享数字孪生模型和实时数据，不同部门可以更好地协调工作，共同应对安全威胁。这有助于加强整个组织的安全防御能力，并提高对威胁的感知和应对速度。

5．安全培训和意识提升:数字孪生技术可以用于安全培训和意识只提升。通过建立逼真的数字孪生环境,可以模拟各种安全事件和攻击场景,让员工在虚拟环境中进行实践和培训，提高对安全风险的认知和应对能力。

总结而言，数字孪生技术在信息安全领域中的应用可以提供更好的安全防御、风险管理和安全意识培养。它使安全团队能够更好地预测、应对各种威胁和攻击，提高企业的整体安全水平。

九、主要研究内容

（一）主要研究内容

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 BB 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。

1．研究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。

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。

3．研究自动化运维场景开发

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。

4．研究网络化协同业务开发

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。

（二）技术路线

十、项目成果呈现形式与预期达到的研究目标

（一）成果呈现形式

1. 基于数字孪生技术建立信息安全数字孪生体系，该项目包含 AI 人工智能自动化运维、数字孪生可视化大屏、网络化协同应用、智能化管理安全设备。

2. 申请软件著作权登记 2 项。

3. 申请发明专利 1 项。

4. 公开发表论文 2 篇。

（二）预期研究目标

实现业务自动化运维，网络安全设备集成，数据集中可视化，便捷操作和可追溯的管理，可以实时监控机房设备动态，有助于推动工作更好的开展。

十一、预期达到的目标与现状的对比分析

（一）预期目标

建设信息安全数字孪生系统预期达到目标主要包括以下几方面：

1．提高安全监测能力：数字孪生可以通过实时监测和诊断市局全区系统的各种指标，如网络设备状态、流量、端口、协议等，来及时发现和预测潜在的安全威胁和攻击，提高安全监测能力。

2．提高安全防御能力：数字孪生可以通过对市局全区的网络系统的历史和实时数据进行分析，识别出潜在的安全威胁和攻击，提前做好防范和应对措施，提高安全防御能力。

3．提高安全效率：数字孪生可以通过自动化分析和处理大量数据，提高安全监测和分析的效率，减少人工干预和操作成本，提高安全效率。

4．降低安全风险：数字孪生可以通过实时监测和诊断网络系统的安全状态，及时发现和响应安全事件，减少损失和影响，降低安全风险。

5．优化安全管理：数字孪生可以通过数字化技术手段，实现对各类资源和业务的数字化管理，优化安全管理流程和机制，提高安全管理效率和质量。

总之，数字孪生在信息安全应用可以帮助企业提高网络系统的安全性和可靠性，保护信息和数据的安全，提高安全监测、分析效率和准确性，帮助企业更好地管理

和控制信息安全风险。

（二）现状

1．运维人员不足：目前信息中心主要技术人员有 2 名，负责解决全区网络、终端、VPN 用户等千台终端使用的问题，问题较繁琐，造成信息中心在此繁琐工作中占用大量的时间。

2．护网防御不足：现网中设备类型有防火墙、上网行为管理、终端准入、终端杀毒、态势感知、负载均衡、SSL VPN、路由器、交换机等不同品牌不同型号设备近百台，基本都是单设备单点作战，无法整合多台设备联合作战。

3．监控分析不足：依据相关政策要求在重保期间要对全网安全设备进行实时监控，并统计设备监控告警信息，包括 web 应用防火墙、态势感知、防病毒、防火墙等安全设备，现阶段通过人工进行统计监控无法做到 24 小时实时或定时统计分析。

4．资产管理不足：目前全区设备资产需通过人工统计，不能清晰反映出设备资产数量、类型、品牌，以及使用状态，更不能实时进行设备运行情况健康监控。

通过对比可以看出，数字孪生技术在信息安全中还存在一些问题和挑战，需要加强安全保障和管理，完善技术标准，提高安全意识和防范能力。同时，也需要充分发挥数字孪生技术的优势，补足现状的缺陷，加强数据保护和应急响应能力，降低安全风险，提高信息安全管理水平。

十二、项目实施方案

1. 需求调研阶段（2023 年 6 月）

主要任务：调研全区信息网络安全的情况，梳理总结当前运维管理网络存在的问题；结合实际情况运用数字孪生仿真、C4D 模型设计、MBD 模型设计理念、MBE 数字企业技术；初步形成项目可行性研究报告及需求规格说明书。

2. 方案设计阶段（2023 年 7 月）

主要任务：确定信息安全数字孪生系统建设方案，以及系统实现的技术总体可行性方案。

3. 应用系统研发阶段（2023 年 8 月-2024 年 2 月）

主要任务：明确项目研发需求和技术架构，研发信息安全数字孪生系统所包含的功能，以及对接全区网络安全设备到平台。

4. 测试应用、上线阶段（2024 年 3 月）

主要任务：进行软件和硬件测试和试运行，跟踪应用实施效果，收集反馈信息，及时调整优化，通过后投入使用。

5. 推广应用阶段（2024 年 4 月-2024 年 6 月）

主要任务：开展项目推广应用，在全市范围进行推广。积极获得省局相关部门认证，筹备开展兄弟单位间的成果交流。

6. 成果巩固阶段（2024 年 7 月）：

主要任务：总结提炼项目开展过程的亮点和经验，制作完善项目资料。

十三、年度进度安排及考核指标

（一）2023 年 6 月-2023 年 12 月进度安排

1. 需求调研阶段计划进度：调研郑州市局及各县区网络信息安全的情况，梳理总结当前运维管理网络存在的问题；结合实际情况如何运用数字孪生仿真、MBD 模型设计、MBE 数字企业技术。

2. 方案设计阶段计划进度：确定信息安全数字孪生系统建设方案，以及系统实现的技术总体可行性方案。

3. 应用系统研发阶段计划进度：明确项目研发需求和技术架构，研发信息安全数字孪生系统所包含的功能，以及对接全区网络安全设备到平台。

2023 年度考核指标：

1. 需求规格说明书 1 份。

2. 技术总体方案设计 1 份。

3. 信息安全数字孪生系统建设方案 1 份。

（二）2024 年 1 月-2024 年 7 月进度安排

1. 测试应用、上线阶段计划进度：对开发的软件和硬件进行测试和试运行。

2. 推广应用阶段计划进度：向省局（公司）或兄弟单位推广介绍项目成果，实现成果推广应用，发表论文 1-2 篇。

3. 成果巩固阶段主要任务：系统梳理总结项目成果，撰写结题资料。

2024 年度考核指标：

1. 信息安全数字孪生系统软件 1 套。

2. 信息安全数字孪生系统测试报告 1 份。

3. 信息安全数字孪生系统使用手册及应急手册 1 份。

4. 推广应用总结报告 1 份。

5. 软件著作权或软件著作权受理书 1 份，发明专利 1 份，项目结题资料 1 套。

十四、项目推广应用方案

（一）推广目的

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。

（二）推广内容

1. 自动化运维：利用人工智能自动化运维技术，将全区全网网络安全设备结合运维业务场景处置网络安全信息事件，以及常态化运维。

2. 数据可视化大屏：利用数字孪生仿真技术、C4D 模型设计、MBD 模型设计理念、MBE 数字化企业技术，实现了全区全网安全态势感知、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的数据可视化大屏。

（三）推广主体

河南省 BB 公司郑州市公司专门成立成果推广小组，组长由本项目负责人担任，成员由项目研究人员组成。

（四）推广对象

全省、全市或部分兄弟单位。

（五）推广进度安排

为了保证成果推广工作达到预期目的，将成果推广分为三个阶段。

1. 试点应用阶段（2024.4-2024.5）。确定郑州市局（公司）为试点单位，通过全市单位的参观交流，推广至各地市应用测试。

2. 省内推广阶段（2024.6）。在全省范围内进行推广应用，通过对应用信息安全数字孪生系统平台和自动化场景应用的成果介绍，并通过数字孪生可视化技术，介绍信息安全数字孪生系统平台的优势逐步全省范围内推广应用。

3. 常态化全面推广：利用行业、兄弟单位交流调研活动，宣传推广项目成果，推动项目成果在兄弟单位的推广应用。

（六）推广方法

1. 组织召开座谈会、交流会、研讨会等。

2. 在国家级期刊发表相关学术论文。

3. 在行业平台上发表管理经验文章。

十五、项目协作单位的现有基础条件与主要负责人学术背景

河南省BB公司郑州市公司，目前通过部署防火墙、入侵防御、上网行为管理、态势感知等网络安全设备构建自己的安全防御体系，但随着安全体系建设的日趋完善，相应的问题点也随之暴露，涉及人员不足、技术能力薄弱；设备品类多、功能各异；设备单点作战、协同处置困难等情况，在当前及未来的网络安全形势下，需要我们具有快速、协同处置能力，一旦发现攻击，立即采取相应阻断手段，现网安全体系往往已经部署有预警、阻断等设备，如何快速、有效进行协同处置是下一步网络安全建设的一个重要环节，本项目旨在打造一套快速、高效的协同智慧指挥平台，实现各网络安全设备的协同处置能力。

十六、项目承担单位、协作单位任务分工

（两家以上承担单位、或有协作单位的项目填写）

第一承担单位：

第二承担单位：

协作单位：

十七、项目承担单位意见

签 章

年　　月　　日

十八、郑州市 BB 公司科技主管部门审查意见

经办人（签字）

年　　月　　日