ICS 35.240.50
CCSL70

DB53

云　南　省　地　方　标　准

DB53/T 1409—2025

智能制造区块链数据服务安全规范

2025-05-09发布　　2025-08-09实施

云南省市场监督管理局　　发布

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。

本文件由云南大学提出。

本文件由云南省区块链和数字科技标准化技术委员会(YNTC27)归口。

本文件起草单位：云南大学、云南省工业和信息化厅、云南财经大学、云南省标准化研究院、云南省工业和信息化厅信息中心、云南南天电子信息产业股份有限公司、昆明昆船智慧机场技术有限公司、云南省公路路政管理总队(省综合交通发展中心)、云南省标准化协会。

本文件主要起草人：王金丽、吕宛青、白杰、陈曦、杨璐、景智育、余益民、姚绍文、马骥、谢佳乐、房发科、王晨曦、张璇、朱荣、赵进一、周维、冯立波、成静、马竹仙、朱勋程、李宁、曾学、刘林海、崔鸿刚、唐嘉、袁泽辉、刘俊红、吴鹏、邓显、杨守稳、王培涌、张中捷、刘昕蕊、周建超、陶珊珊、杜镜刚、阳晓金。

智能制造区块链数据服务安全规范

1 范围

本文件规定了智能制造区块链的数据服务安全要求，包括数据采集安全、区块链网络节点安全、数据上链安全、数据上链后的监控与审计安全以及应急与人员管理培训。

本文件适用于基于区块链的智能制造平台数据服务安全的设计与应用。

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。

GB/T 25069-2022 信息安全技术术语

GB/T 40647-2021 智能制造系统架构

GB/T 42570-2023 信息安全技术区块链技术安全框架

GB/T 42571-2023 信息安全技术区块链信息服务安全规范

GB/T 43572-2023 区块链和分布式记账技术术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能制造 intelligent manufacturing

通过综合和智能地利用信息空间、物理空间的过程和资源，贯穿于设计、生产、物流、销售、服务等活动的各个环节，具有自感知、自决策、自执行、自学习、自优化等功能，创造、交付产品和服务的新型制造。

[来源：GB/T 23031.3-2023,3.1.1]

3.2

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源：GB/T 43572-2023,3.12]

3.3

智能制造区块链数据服务 intelligent manufacturing blockchain data service

指利用区块链技术为智能制造领域提供的，涵盖数据采集、处理、存储、传输及共享等全过程的数据管理和服务，旨在保障数据的安全性、隐私性、完整性和可用性。

3.4

上链 record on-chain

将信息写到区块链的过程。

[来源：GB/T 42571-2023,3.5]

3.5

预言机 oracle

使用分布式记账技术系统外部数据更新分布式账本的服务。

[来源：GB/T 43572-2023,3.28]

3.6

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人(例如接收者)伪造的目的地。

[来源GB/T 25069-2022,3.576]

3.7

零知识证明 zero knowledge proof

证明者向验证者证明某个论断的正确性，却不泄露除正确性以外其他信息的密码协议。

[来源：GB/T 42570-2023,3.24]

3.8

同态加密 homomorphic encryption

支持在不解密情况下直接对密文进行有效操作，且其输出对应于明文间运算结果密文的加密方案。

4 缩略语

下列缩略语适用于本文件。

AES: 高级加密标准(Advanced Encryption Standard)

RBAC: 基于角色的访问控制(Role-based Access Control)

IDS: 入侵检测系统(Intrusion Detection System)

IPS: 入侵防御系统(Intrusion Prevention System)

PoW: 工作量证明(Proof of Work)

PoS: 权益证明(Proof of Stake)

DPoS: 委托权益证明(Delegated Proof of Stake)

BFT: 拜占庭容错(Byzantine Fault Tolerance)

KMS: 密钥管理系统(Key Management System)

TLS: 传输层安全性(Transport Layer Security)

SSL: 安全套接层(Secure Sockets Layer)

2FA: 双因素认证(Two-Factor Authentication)

5 智能制造区块链数据服务安全风险及要求

5.1 智能制造区块链数据服务安全风险

在使用区块链技术进行智能制造数据管理和服务时面临各种潜在风险。这些风险包括：

a) 区块链中智能合约和节点基础设施可能存在安全漏洞，从而导致数据泄露或被篡改；

b) 区块链存储的数据是公开透明的，这会与数据隐私保护法规相冲突，尤其是在涉及个人或敏感数据时；

c) 智能制造企业可能面临新技术挑战，如采用新型基础设施、新技术等；

d) 可能会受到网络攻击或其他技术故障，从而导致中断业务运营。

5.2 智能制造区块链数据服务安全要求

智能制造区块链数据服务安全要求旨在确保数据全生命周期的安全性，主要包括：

a) 数据采集的安全；
b) 网络与节点的安全；
c) 数据上链过程的安全；
d) 监控与审计的安全；
e) 应急响应计划与人员的管理和培训。

6 智能制造区块链数据服务安全框架

本文件围绕智能制造区块链数据的采集安全、数据上链网络和节点的安全、数据上链过程的安全、数据上链后的监控与审计以及应急与人员管理培训等五个方面提出安全要求。

智能制造区块链数据服务安全的整体逻辑框架如图1所示。

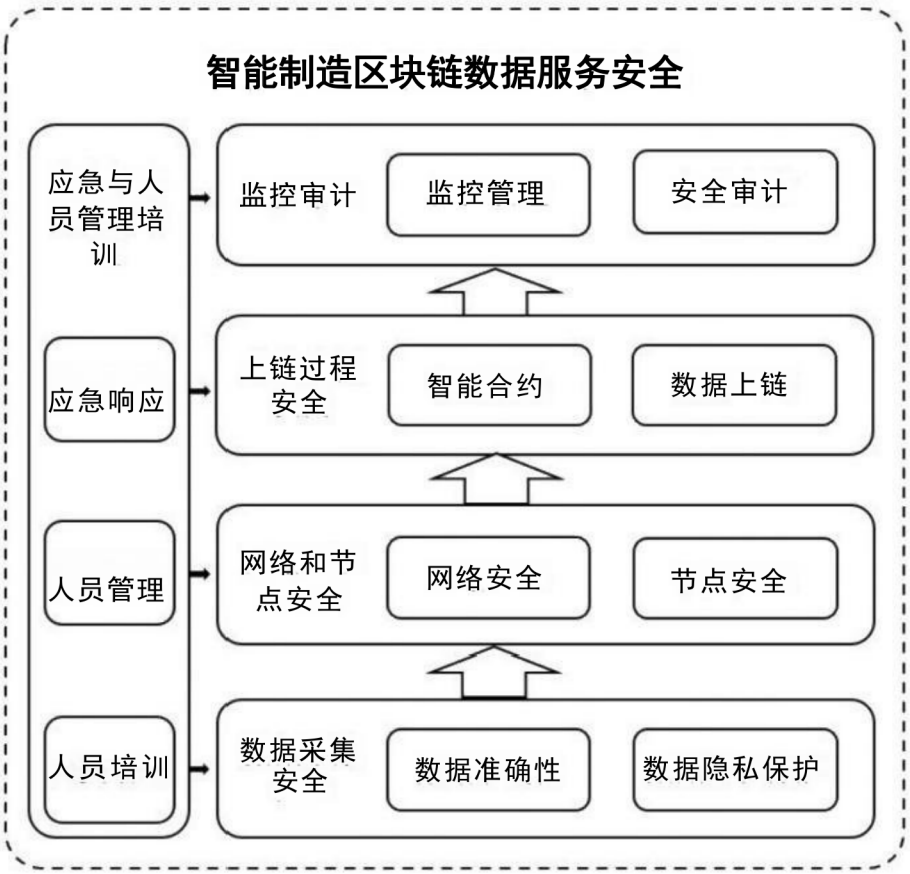

图 1 智能制造区块链数据服务安全的整体逻辑框架图

智能制造区块链数据服务安全具体内容如下：

a) 数据上链前的数据采集安全：包括数据的准确性、数据的隐私保护等；

b) 数据上链网络和节点的安全：包括网络安全、区块链节点安全等；
c) 数据上链过程的安全：包括智能合约安全、数据上链安全等；
d) 数据上链后的监控与审计：包括监控管理、安全审计等；
e) 应急与人员管理培训：包括应急响应、人员管理培训等。

7 数据采集安全

7.1 数据准确性

7.1.1 数据源验证

数据采集时，应核实数据来源的合法性，确保数据来源于已授权和可信的系统或设备。同时应对外部数据源进行认证，确保其提供的数据是准确和经过验证的。

7.1.2 数据采集设备

数据采集时应保证数据采集设备的可靠性，定期对数据采集设备进行校准。

7.1.3 数据验证与清洗

7.1.3.1 数据清洗

必须实施数据清洗过程，确保数据的质量。数据清洗过程包括但不限于去除重复记录(识别并删除重复的数据记录，确保数据的唯一性)、纠正错误(检测并修正数据中的错误，包括拼写错误、格式错误等)、填补缺失值(使用合适的方法填补数据中的缺失值，如插值法、均值填充等)。

7.1.3.2 数据验证

对采集的数据应：
a) 实施数据验证流程，确保数据的一致性和完整性；
b) 使用算法对数据进行验证，包括但不限于数据格式检查、范围检查、逻辑检查等；
c) 记录数据验证的结果，包括验证时间、验证方法和验证结果等信息。

7.1.4 完整性和来源真实性

数据采集时，应对数据进行校验和计算，确保数据在传输过程中未被篡改。同时应采用数字签名技术，验证数据来源的真实性。

7.2 数据隐私保护

7.2.1 数据加密

应使用高强度的加密标准，例如 AES、DES、SM1、SM4等加密算法对采集的敏感数据进行端到端加密，确保数据在传输和存储过程中保持加密状态。

7.2.2 数据匿名化与脱敏处理

在数据采集、分析与共享过程中，为保障个人信息安全，应采取以下措施：
a) 对个人身份信息进行匿名化处理，确保数据中的个人信息不可直接或间接识别；

b) 在数据分析或共享环节，对敏感信息进行数据脱敏处理。采用数据脱敏技术，如数据遮蔽、数据替换、数据泛化等，以隐藏原始数据中的个人信息，确保敏感信息不会被泄露。

7.2.3 访问控制

采集数据时，在访问控制方面的安全要求如下：

a) 实施基于角色的访问控制 (RBAC)， 确保只有授权用户才能访问敏感数据；
b) 采用身份验证和授权机制来访问数据采集系统。

7.2.4 最小化数据采集

在采集数据的过程中，在设计数据采集流程时，遵循数据最小化原则，只采集为实现业务目的所必需的数据，避免收集无关信息。

8 网络和节点安全

8.1 网络基础设施安全

8.1.1 安全配置

网络基础设施的安全配置如下：

a) 更改默认管理员密码；
b) 禁用或删除未使用的服务和端口；
c) 为设备设置唯一的管理员账户；
d) 限制远程访问，如 SSH 或 telnet。

8.1.2 防火墙和 IDS/IPS

针对防火墙和 IDS/IPS， 应：

a) 防火墙仅允许授权用户的入站和出站；
b) 定期审查和更新防火墙；
c) 部署基于网络的 IDS/IPS 来监管流量和行为；
d) 配置 IDS/IPS 自动响应可疑活动，如阻断IP 地址或端口；
e) 定期更新IDS/IPS 签名和规则库。

8.1.3 物理安全

应将设备存放于受控的环境中，如服务器室或数据中心，安装安全摄像头和访问控制系统，同时限制对物理设备的访问，仅允许授权人员进入。

8.2 区块链节点安全

8.2.1 软件安全

应定期更新和维护区块链客户端软件，修复安全漏洞。

8.2.2 数据备份

应定期备份区块链节点数据，防止数据丢失或损坏。

8.2.3 节点身份认证

节点的身份认证安全要求如下：

a) 应实施区块链节点身份验证机制；
b) 应保证只有经过身份验证的节点才能加入网络并进行交易。

8.2.4 共识机制选择

8.2.4.1 网络去中心化程度

根据网络去中心化程度，应：

a) 若追求高度去中心化，可选择PoW或 PoS等共识机制；
b) 若对网络需要有一定的中心化管理，可选择DPoS或其他 BFT类共识机制。

8.2.4.2 安全性能

根据区块链安全要求，应确保共识机制能够抵御各种攻击，如双花攻击、女巫攻击等。

8.2.4.3 能源消耗

根据能源消耗要求，应：

a) 对能源消耗有要求，应选择PoS 或 DPoS 等能耗较低的共识机制；
b) 对能源消耗无要求，应选择PoW 等共识机制，以提供更高的去中心化和强大的安全性。

8.2.4.4 网络规模和节点数量

根据网络规模和节点数量要求，应：

a) 对于拥有大量节点的网络，可选择DPoS、PoW等以提供更好的可扩展性；
b) 对于节点数量较少的网络，可选择BFT类共识机制以更加高效。

9 上链过程安全

9.1 智能合约安全

9.1.1 设计开发

智能合约的设计开发方面的安全要求如下：

a) 在设计智能合约时，应保证交易的可追溯性；
b) 应明确各个角色的功能及其权限；
c) 应具备防篡改和抗抵赖性；
d) 应避免涉及敏感数据；
e) 应不包含随机信息，且运行结果不应对先后顺序有依赖；
f) 应遵循安全编码原则，避免出现安全漏洞。

9.1.2 测试验证

9.1.2.1 常规验证

常规验证要求如下：

a) 若与其他合约有交互，应检查合约与其他合约或区块链组件的交互是否正常工作；
b) 在高并发或高负载条件下保证系统的性能和稳定性；
c) 在发现合约问题时，及时修复和更新。

9.1.2.2 漏洞检测

智能合约的漏洞检测要求如下：
a) 使用静态代码分析工具检查智能合约源代码，避免潜在安全漏洞和逻辑错误；
b) 使用动态分析工具检测运行时智能合约中的漏洞；
c) 应检测智能合约安全性，如重入攻击、整数溢出攻击、时间戳攻击等。

9.1.3 编译部署

9.1.3.1 智能合约编译

智能合约编译阶段的安全要求如下：
a) 应使用安全成熟的编译器；
b) 编译智能合约前，应使用最新版本；
c) 智能合约在编译成字节码后，前后逻辑应保持一致。

9.1.3.2 智能合约的部署

智能合约部署阶段的安全要求如下：
a) 智能合约的部署应由链上节点达成共识，防止产生恶意部署；
b) 可使用脚本进行合约的自动化部署，减少人为干预；
c) 应校验智能合约部署的完整性。

9.1.4 触发运行

9.1.4.1 智能合约触发

智能合约触发阶段的安全要求如下：
a) 智能合约调用接口时，应明确接口名称和功能；
b) 在智能合约相互调用时，应明确智能合约的调用方式；
c) 应使用限定词对智能合约的调用范围进行限定；
d) 在调用预言机时，应确保预言机通过第三方的安全性和可靠性评估；
e) 若发现所使用的预言机提供的数据有误，则应对预言机进行重新评估。

9.1.4.2 智能合约运行

智能合约运行阶段的安全要求如下：
a) 应避免使用严重消耗资源的操作，确保智能合约运行时所消耗的资源在可接受的范围内；
b) 应保证智能合约能在有限的程序步数和时间内完成；
c) 当智能合约需要修改链上数据时，应当提供严格的权限管理机制。

9.1.5 合约维护

9.1.5.1 合约禁用/重启

智能合约禁用、重启阶段的安全要求如下：

a) 应为合约提供禁用功能，当发现合约出现漏洞时可及时禁用合约；
b) 应为合约提供重启功能，当合约漏洞被修复后可重新恢复合约使用；
c) 在使用禁用和重启功能时，应遵循严格的权限管理。

9.1.5.2 合约升级

智能合约的升级阶段的安全要求如下：

a) 应遵循需求分析、设计与开发、单元测试、集成测试、安全审计等流程，确保新合约代码兼容旧合约功能且不影响系统安全性；
b) 应考虑合约升级对系统性能和稳定性的影响，避免升级过程中出现系统故障和数据丢失；
c) 应有明确的通知机制，确保用户和系统的参与者能够及时了解合约的变更；
d) 升级过程应设计可逆机制，确保出现问题时，能够回滚到原来状态；
e) 只有授权的实体才能执行合约升级；
f) 升级过程应当详细记录合约的变更原因、变更时间、操作主体。

9.2 数据上链安全

9.2.1 数据加密及密钥管理

数据上链前，对数据的加密及密钥管理的安全要求如下：

a) 使用强加密算法对数据进行加密；
b) 使用加密算法对数据内容进行加密；
c) 使用密钥管理系统 (KMS) 存储和管理密钥；
d) 定期轮换密钥，当密钥泄露或疑似泄露时立即撤销并更新密钥。

9.2.2 传输协议

数据上链时，对传输协议的安全要求如下：

a) 使用安全协议（如TLS/SSL) 来加密数据传输；
b) 确保使用最新版的TLS;
c) 定期更换TLS证书，确保证书有效性和信任链完整性；
d) 若涉及跨链操作，应保证跨链数据的安全性。

9.2.3 数据隐私

为保护上链数据的隐私，应：

a) 使用零知识证明、同态加密等技术实现交易的验证；
b) 对于敏感数据，使用匿名化或脱敏技术保护个人隐私。

9.2.4 数据验证

数据上链后，应用程序应能够使用零知识证明、环签名等验证方法来验证数据的来源和完整性。

10 监控与审计

10.1 监控管理

10.1.1 人员账户活动及访问权限监控

人员账户活动及访问权限监控安全要求如下：

a) 实施实时监控，记录用户账户的登陆方法、操作和行为；
b) 设置警报系统，检测到可疑行为时应报警；
c) 定期审查账户活动日志，分析潜在的安全威胁；
d) 对人员账户权限变更进行审计跟踪；
e) 监控用户账户访问行为，确保只有授权用户才能访问特定系统和数据。

10.1.2 系统监控

对智能制造区块链系统的监控安全要求如下：

a) 监控区块链节点运行情况，包括节点响应时间、处理能力和资源利用率；
b) 监控网络延迟、宽带利用率，以支持高效的数据传输和区块确认；
c) 监控共识机制的健康状况和异常行为，确保节点一致性和网络的安全性。

10.1.3 智能合约生命周期

对智能合约生命周期的监控安全要求如下：

a) 跟踪智能合约的编写和修改；
b) 监控智能合约的部署过程，确保部署正确且未被篡改；
c) 监控交易的发起、执行和确认，并记录异常交易模式。

10.2 安全审计

10.2.1 数据采集安全审计

对数据采集过程的安全审计，应做好：

a) 审查数据源验证过程，确保数据来源的合法性和可信性；
b) 检查数据采集设备的校准记录，确保测量精准；
c) 评估数据验证与清洗流程的有效性，确保数据一致性和完整性。

10.2.2 数据隐私保护安全审计

对数据隐私保护的安全审计，应做好：

a) 审核数据加密措施，确保敏感数据在传输和存储过程中的安全性；
b) 检查匿名化处理和脱敏技术，确保个人隐私得到保护；
c) 评估访问控制策略和权限管理，确保只有授权用户才能访问敏感数据。

10.2.3 网络和节点安全审计

对网络和节点的安全审计，应做好：

a) 审查网络基础设施的安全配置，包括防火墙规则、IDS/IPS 设置和物理安全措施；
b) 评估共识机制的选择合理性，确保其能够抵御各种攻击，并保持数据一致性；
c) 检查区块链节点的软件安全、数据备份和身份认证机制。

10.2.4 智能合约安全审计

对智能合约的安全审计，应做好：

a) 审查智能合约的设计和开发过程；
b) 评估智能合约的测试验证流程，包括常规验证和漏洞检测；
c) 审核智能合约的编译部署和触发运行过程。

10.2.5 数据上链安全审计

对数据上链的安全审计，应做好：

a) 审查数据加密、密钥管理和数据验证措施，确保数据在上链前的安全性；
b) 评估传输协议和数据隐私保护措施，确保数据在传输过程中的安全性和隐私性。

10.2.6 应急与人员管理培训安全审计

对应急与人员管理的安全审计，应做好：

a) 审查灾难恢复计划的制定和执行情况；
b) 评估人员身份管理和权限管理流程；
c) 审核人员培训计划和操作规程。

11 应急与人员管理培训

11.1 应急响应

11.1.1 灾难恢复计划

为应对突发情况，应做好：

a) 定期对数据进行备份，防止数据因硬件故障或恶意攻击而丢失；
b) 建立备用网络连接，在主网络发生故障或受到攻击时立即接管，确保网络通信不受影响；
c) 定期进行灾难恢复演练，模拟各种灾难场景，测试和验证灾难恢复计划的有效性；
d) 建立专业的技术支持团队，负责监控系统状态、响应紧急情况并提供技术支持；
e) 记录所有灾难恢复活动细节。

11.2 人员管理

11.2.1 身份管理

对人员管理，应做好：

a) 进行人员背景调查，确保符合公司要求。背景调查包括教育背景、工作经历、职业资格、信用记录和犯罪记录等；
b) 及时撤销离职员工的访问权限并删除其账户；
c) 实施强身份认证机制，如密码、2FA(双因素认证)、生物识别等；
d) 确保每个用户都有唯一的身份标识符；

11.2.2 权限管理

对人员权限，应做好：

a) 实施RBAC 模型，根据员工角色授予相应访问权限；
b) 遵循权限最小原则，避免过度授权；

c) 建立权限审批流程，确保权限的授权经过适当的审批和记录；
d) 定期审查员工权限，确保其权限和当前职位需求匹配；
e) 遵循分权原则，确保关键操作和敏感数据访问权限不集中在单一用户手中。

11.3 人员培训

针对企业中的人员，应做好：

a) 定期提供安全意识培训，包括隐私保护、网络安全相关法律法规以及公司的相关安全政策；
b) 定期培训员工如何安全操作智能制造设备和区块链平台；
c) 培训员工如何应对紧急情况；
d) 提供权限管理培训，保证员工能理解权限重要性以及如何正确使用权限；
e) 鼓励员工持续学习新技术，提高员工的安全技能和知识。