|  |  |
| --- | --- |
| ICS  | 35.240.01 |
| CCS  | L70 |

团 体 标 准

增材制造知识图谱 第3部分：安全管控溯源

Additive manufacturing knowledge graph—Part 3: Securing managing and tracing

XXXX - XX - XX发布

XXXX - XX - XX实施

|  |  |
| --- | --- |
| 中国机械工程学会 | 发布 |

T/CMES XXXXX—2023

目次

[前言 II](#_Toc150518675)

[1 范围 1](#_Toc150518676)

[2 规范性引用文件 1](#_Toc150518677)

[3 术语和定义 1](#_Toc150518678)

[4 安全管控技术架构 1](#_Toc150518679)

[5 增材制造图谱存储要求 2](#_Toc150518680)

[5.1 增材制造知识审查 2](#_Toc150518681)

[5.2 数据安全性 2](#_Toc150518682)

[5.3 性能与扩展性 2](#_Toc150518683)

[5.4 可管理性 2](#_Toc150518684)

[6 增材制造流程权限管理要求 2](#_Toc150518685)

[6.1 增材制造领域用户身份认证 3](#_Toc150518686)

[6.2 权限分级与专业角色管理 3](#_Toc150518687)

[6.3 数据隐私与访问控制 3](#_Toc150518688)

[7 日志审计要求 3](#_Toc150518689)

[7.1 审计范围 3](#_Toc150518690)

[7.2 审计功能 3](#_Toc150518691)

[7.3 操作日志监控与告警 3](#_Toc150518692)

[7.4 合法性审计 3](#_Toc150518693)

[8 日志溯源要求 4](#_Toc150518694)

[8.1 日志记录 4](#_Toc150518695)

[8.2 日志存储与保护 4](#_Toc150518696)

[8.3 操作链路追踪 4](#_Toc150518697)

[8.4 数据溯源与还原 4](#_Toc150518698)

[9 系统性能要求 4](#_Toc150518699)

[9.1 响应时间与吞吐量 4](#_Toc150518700)

[9.2 数据存储与查询效率 5](#_Toc150518701)

[9.3 并发处理和分布式计算 5](#_Toc150518702)

[9.4 扩展性 5](#_Toc150518703)

[9.5 定制化要求 5](#_Toc150518704)

[9.6 兼容性要求 5](#_Toc150518705)

[图1 增材制造知识图谱安全管控技术架构图 2](#_Toc142057473)

1. 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。

本文件由 提出。

本文件由 归口。

本文件起草单位：XXX、XXX、XXX、

本文件主要起草人： XXX、XXX、XXX、

增材制造知识图谱 第3部分：安全管控溯源

* 1. 范围

本文件规定了增材制造领域知识图谱安全管控与审计溯源系统的技术要求，主要涵盖了数据存储要求、权限管理要求、日志审计要求、日志溯源要求、系统性能要求。

本文件适用于增材制造知识图谱安全管控系统的设计、研发和应用。

* 1. 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 35351 增材制造 术语

GB/T 42131 人工智能 知识图谱技术框架

GB/T 41479 信息安全技术 网络数据处理安全要求

* 1. 术语和定义

GB/T 42131，GB/T 41479和GB/T 35351 界定的术语和定义适用于本文件

* 1. 安全管控技术架构

增材制造领域知识图谱的安全管控技术架构如图1所示，主要包括四个关键部分：数据存储、访问控制、日志记录和审计、以及溯源功能。在数据存储方面，系统需要采用高效、安全的存储技术，确保增材制造知识图谱数据的可靠性和完整性。同时，数据存储应具备高性能和扩展性，以满足大规模数据处理和存储的需求。访问控制是确保只有经过授权的用户和角色能够访问增材制造知识图谱数据的重要环节。系统需要实现灵活的权限管理机制，对不同级别的用户和角色进行精确的权限划分，从而保障知识图谱数据的安全性和保密性。日志记录和审计功能是对知识图谱系统中的操作和访问进行全面记录和监控的关键组成部分。通过详细的日志记录，系统可以追踪用户的操作行为，发现异常操作并进行及时响应。审计功能则对操作日志进行审查和分析，确保知识图谱的操作符合规定，提高系统的可信度和透明度。溯源功能是对知识图谱中数据的来源和变更过程进行追溯的重要特性。系统需要能够准确记录数据的修改历史和来源信息，以便在需要时能够快速溯源数据，保障知识图谱的数据可信度和可溯性。



1. 增材制造知识图谱安全管控技术架构图
	1. 增材制造图谱存储要求
		1. 增材制造知识审查

增材制造知识图谱入库存储之前应由对应领域的增材制造专家进行审查核验，如零部件参数、生产工艺、操作手册等，确保增材制造知识图谱的正确性。

* + 1. 数据安全性
1. 数据加密：对增材制造图谱中的敏感数据和用户信息采用强大的加密算法进行加密，确保数据在传输和存储过程中的安全性；
2. 数据备份与恢复：定期进行增材制造图谱数据的备份，保障数据在灾难或意外情况下能够及时恢复。
3. 数据完整性：确保增材制造图谱数据的完整性，防止数据篡改或损坏。
	* 1. 性能与扩展性
4. 存储性能：确保增材制造图谱存储系统具有高性能，能够快速响应用户的查询和操作请求；
5. 扩展性：增材制造领域数据往往种类繁多，设计图谱存储架构时需考虑扩展性，使系统能够支持不断增长的数据量和用户访问；
6. 负载均衡：采用负载均衡技术，均衡各个节点的压力，提高系统整体性能。
	* 1. 可管理性
7. 可管理性：提供友好的管理界面，方便管理员对增材制造图谱存储系统进行配置、监控和管理；
8. 日志记录：对增材制造图谱数据的操作和访问产生日志文件，便于后续的审计和溯源。
	1. 增材制造流程权限管理要求
		1. 增材制造领域用户身份认证
9. 增材制造专用注册与登录：系统应提供特定于增材制造领域的用户注册和登录功能，确保只有具备增材制造领域专业资格的用户能够访问和使用知识图谱系统；
10. 多因素认证：对于涉及敏感信息，如：生产数据和质量记录等，或权限较高的操作，采用多因素认证方式增加用户身份验证的安全性，应该确保用户数据和用户身份不直接关联。
	* 1. 权限分级与专业角色管理
11. 用户分组与角色定义：根据个人、岗位以及执行任务，将用户划分为不同的专业角色，如普通用户、增材制造工艺专家、材料科学家、质量控制经理、数据库管理员等，根据用户的个人特征、所在岗位以及具体任务的需求，为不同角色分配相应的权限；
12. 专业角色权限控制：为每个角色分配相应的权限，限制其在图谱存储中的操作和访问范围。确保普通用户只能查看图谱中的信息以及部分修改权限，而工艺专家可以编辑和更新增材制造工艺相关的知识，材料科学家可以访问材料属性数据，质量控制经理具有数据质量审核权限等；
13. 动态权限调整：允许系统管理员根据实际需求调整角色权限，确保权限的动态管理。
	* 1. 数据隐私与访问控制
14. 敏感数据访问控制：对图谱中的敏感数据进行特殊保护，仅授权的用户或角色可以访问和查看；
15. 数据访问审批机制：对于某些特定的敏感数据或权限较高的操作，设置审批机制，确保相关访问经过审核和审批。
	1. 日志审计要求
		1. 审计范围
16. 操作审计：对图谱中的所有数据操作行为进行审计，包括查询、编辑、修改、删除等操作。操作的审计由系统管理员进行，针对系统层面判断操作的安全性与可行性，如该操作是否会引起系统异常等。
17. 访问审计：审计用户对图谱的所有访问行为，包括登录、登出、访问时间、IP地址等信息。
18. 数据变更审计：审计图谱数据的变更情况，包括数据的新增、修改、删除等操作，确保数据的完整性和可追溯性。数据变更操作由对应的增材制造领域专家进行，针对数据本身修改的合理性进行审计，如图片或相关词条的修改本身是否正确。
	* 1. 审计功能
19. 日志查询与检索：提供用户友好的查询界面，使管理员能够快速检索特定时间段或特定用户的审计日志；
20. 审计报告：支持生成审计报告，对图谱的操作和访问行为进行统计和分析，以便发现异常和趋势；
21. 实时监控：支持实时监控图谱的操作和访问行为，及时发现异常和安全事件。
	* 1. 操作日志监控与告警
22. 实时监控：建立实时操作日志监控系统，对图谱中的数据操作行为进行实时监控，发现异常操作；
23. 告警机制：设定告警规则，当发现异常操作或访问时，自动触发告警，通知相关管理员或安全团队进行处理。
	* 1. 合法性审计
24. 行为审计：数据库管理员对用户操作行为进行审计，包括数据库的查询、修改等，确保用户操作符合合规性要求，并且未超越其权限范围；
25. 操作内容审计：增材制造领域对数据的合法性要求较高，如相关的生产参数、操作步骤等。增材制造专家需要对在知识图谱中的内容修改行为进行审计，确保其内容的正确性。
	1. 日志溯源要求
		1. 日志记录
26. 操作日志：对图谱中的所有数据操作行为进行详细记录，包括查询、编辑、修改、删除等操作。
27. 访问日志：记录用户对图谱的所有访问行为，包括登录、登出、访问时间、IP地址等信息。增材制造数据包含某些隐私或保密级别较高的数据，如制造工艺、生产方法等，因此需要对所有访问行为进行记录，保证后续追溯的可行性。
28. 数据变更日志：记录图谱数据的变更情况，包括数据的新增、修改、删除等操作，确保数据的完整性和可追溯性。
	* 1. 日志存储与保护

增材制造领域的知识图谱日志存储与保护主要包括以下要求：

1. 安全存储：采用安全的存储技术，确保日志记录不被篡改和删除；
2. 数据加密：对存储的日志进行加密处理，确保日志在传输和存储过程中的安全性和隐私保护；
3. 分布式存储：采用分布式存储技术，将日志数据存储在多个节点上，增加数据的可靠性和抗故障能力。
	* 1. 操作链路追踪
4. 数据操作溯源：对图谱中的每一项数据操作进行溯源，确保每一步的操作都可以追踪到具体的操作者和时间；
5. 操作关联：将数据操作与相应的用户、设备和任务等关联，建立完整的操作历史链，方便后续的数据溯源和审计；
6. 溯源准确性：应确保数据操作的溯源信息准确无误，避免因数据丢失或错误导致的溯源不完整。应有一个灵活的查询语言和接口，来支持用户对融合后的知识图谱进行多维度、多层次、多粒度和多形式的检索和分析。
	* 1. 数据溯源与还原
7. 数据还原：能够根据溯源信息还原历史数据状态，确保数据的完整性和可追溯性。
8. 溯源分析：对溯源信息进行分析和比对，以便发现潜在的数据操作问题和异常行为。
	1. 系统性能要求
		1. 响应时间与吞吐量

响应时间与吞吐量(throughput，单位：Transactions per second, TPS)相关要求包括：

1. 实时响应：系统应能够在即时响应用户的请求，即：从用户发出请求至系统返回第一个数据或完成用户所请求的操作的时间，一般应不超过500毫秒,并能够实时显示操作日志和溯源信息，以便用户能够及时查看数据操作情况；
2. 高吞吐量：系统需处理大量的数据操作和访问请求，能够同时支持多用户、多设备的并发操作，吞吐量至少达到100TPS。单位时间内处理的数据量计算见公式1。

 公式1

其中：

Transactions为系统处理的事务数量，一个事务指用户向系统发出请求且系统完成该请求的过程；

time为系统完成这些事务花费的时间。

* + 1. 数据存储与查询效率

数据存储与查询效率相关要求包括：

1. 数据存储效率：系统应采用高效的存储技术，确保数据在写入和读取时的速度和效率，避免因存储性能导致的延迟问题，数据写入速度不低于20MB/s，数据读取速度不低于40MB/s；
2. 查询效率：能够快速检索和查询操作日志和溯源信息，支持复杂查询和快速定位特定操作，查询响应时间不超过500毫秒。
	* 1. 并发处理和分布式计算
3. 并发处理：系统应具备强大的并发处理能力，能够同时处理多个用户的数据操作请求，至少同时处理100个并发请求，不影响系统的性能和稳定性；
4. 分布式计算：采用分布式计算架构，将负载均衡分配给至少3个节点，提高系统的计算效率和处理能力；
5. 分布式事务：确保分布式环境下的数据一致性和事务处理，防止数据冲突和错误。
	* 1. 扩展性

对增材制造知识图谱安全管控系统的扩展性的要求包括但不限于：

1. 可扩展性：系统应具备良好的可扩展性，能够根据业务需求和数据量的增长进行水平扩展，保持高性能和稳定性；
2. 弹性伸缩：能够根据实际负载情况自动进行弹性伸缩，根据需求调整计算和存储资源，以确保系统的高效运行；
3. 自动化扩展：设置自动化扩展策略，根据预设规则自动进行扩展，降低运维成本和人工干预。
	* 1. 定制化要求
	1. 模块化设计：系统应采用模块化的设计架构，便于根据需求灵活添加新功能和扩展已有功能，满足不同用户的定制化需求；
	2. 多平台支持：确保系统能够运行在不同操作系统和硬件平台上，为用户提供更多选择和兼容性。
		1. 兼容性要求

对增材制造知识图谱安全管控系统的兼容性的要求包括但不限于:

* 1. 兼容主流图查询语言及图分析工具：系统应支持主流的图查询语言，如SPARQL等，并能与常用的图分析工具进行无缝集成，以便用户能够灵活查询和分析知识图谱数据；
	2. 适配多种硬件平台：系统应能够在业界主流硬件平台上正常运行，包括服务器、工作站和云平台等，以满足不同用户的部署需求；
	3. 支持多数据源批量导入与更新：系统宜支持从多种数据源中批量导入和更新知识图谱数据，包括工艺设计手册、加工特征库、加工实例库、增材制造国行标、用户数据等，以确保系统能够整合多样化的数据来源；
	4. 系统应能够兼容多种图数据库引擎, 如Neo4j、JanusGraph等，以便根据需求灵活选择和切换数据库系统；
	5. 数据格式兼容：系统应支持常见的数据格式和标准，例如JSON、XML等，以便与其他系统进行数据交换和集成。

