ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

制造业数据资产脱敏和交换管理规范

Manufacure process data masking and exchange management specification

（征求意见稿）

（本草案完成时间：2023-08-14）

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 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　体系结构 2
4.1　软件架构图 2
4.2　架构说明 2
5　功能要求 3
5.1　数据存储层 3
5.2　数据处理层 3
5.3　数据交换层 4
5.4　数据应用层 5
5.5　数据行为日志 5
6　建设要求 5
6.1　集成要求 5
6.2　实施要求 6
6.3　应用要求 6

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。

本文件由中共辽宁省委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：沈阳航科智能系统有限公司、上海颐健互联网科技有限公司、上海数瞳信息科技有限公司、沈阳罗泰智能系统有限公司、沈阳开鑫投网络科技有限公司、大连优欣光科技股份有限公司、北方重工集团有限公司、沈鼓集团股份有限公司。

本文件主要起草人：张时乐、赵永生、刘宏、滕代友、赵海鑫、邱秉伟。

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：沈阳市和平区光荣街26号甲，联系电话：024-81680033

本文件起草单位通讯地址：辽宁省沈阳市浑南区上深沟村863-9号沈阳国际软件园D09，联系电话：024-86085890

引　言

制造业数据资产脱敏和交换管理的概念由来已久。本文件就是这样一种基于制造业数据资产脱敏和交换管理的数据处理过程的标准。

制造业数据资产脱敏和交换管理标准涉及数据脱敏和数据交换的基础概念，以及制造业数据资产脱敏和交换管理标准的体系结构。本文件比较系统、完整地反映制造业数据资产脱敏和交换管理标准的技术术语、体系结构、业务需求和功能要求。

本标准的目的并非：

- 建议只有一种方式可以实现制造业数据资产脱敏和交换管理；
- 强迫用户放弃他们现有的数据资产脱敏和交换管理方案。

使用本标准所带来的潜在收益有：

- 在制造业企业内部建立基于制造业数据资产脱敏和交换管理的共同语境；
- 建立第三方应用供应商基于制造业数据资产脱敏和交换管理的共同语境；
- 帮助制造业企业第三方应用供应商理解和描述制造业数据资产脱敏和交换管理的需求；
- 帮助供应商提供满足制造业企业需求的制造业数据资产脱敏和交换管理的产品和服务。

制造业数据资产脱敏和交换管理标准

1 范围

本文件规定了制造业数据资产脱敏和交换管理标准的术语和定义、体系结构、系统功能要求、与应用系统的集成要求、项目实施要求和应用要求。

本文件适用于制造业信息技术服务组织及咨询服务机构、独立软件测评机构、安全审计机构；同时，制造业数据资产脱敏和交换管理业务应用的实施和咨询服务机构以及制造业数据资产脱敏和交换管理的使用者均可参考使用。

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。

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据生命周期 data lifecycle

将原始数据转化为可用于行动的知识的一组过程。

3.2

加密 encryption

对数据进行密码变换以产生密文的过程。

3.3

制造流程 Manufacture process

制造流程，又叫生产流程、工艺流程或加工流程，是指在生产工艺中，从原料投入到成品产出，通过一定的设备按顺序连续地进行加工的过程。 也指产品从原材料到成品的制作过程中要素的组合。

3.4

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性。

3.5

数据脱敏 Data Masking

数据脱敏（脱敏）：屏蔽敏感数据，在使用某些敏感数据前，通过脱敏规则进行数据的变形，实现隐私数据的可靠保护。

3.5

资源 resource

系统中可供访问的客体，例如：应用、系统、接口、服务、数据等。

3.6

接口集成 interface integration

在应用或者其他软件系统中，嵌入对制造业数据资产脱敏和交换管理系统的调用，以便实现高安全的需求。

3.7

数据集成 data integration

在应用或者其他软件系统中，需要与制造业数据资产脱敏和交换管理系统进行数据的交互，以便实现快速集成的需求。

3.8

版本 version

用于记录本文件的数据格式变更的标识。

4 体系结构

4.1 软件架构图

制造业数据资产脱敏和交换管理是基于制造业组织业务数据高安全和数据交换需求处理规范性的平台软件，其软件架构应采用分层结构，见图1。

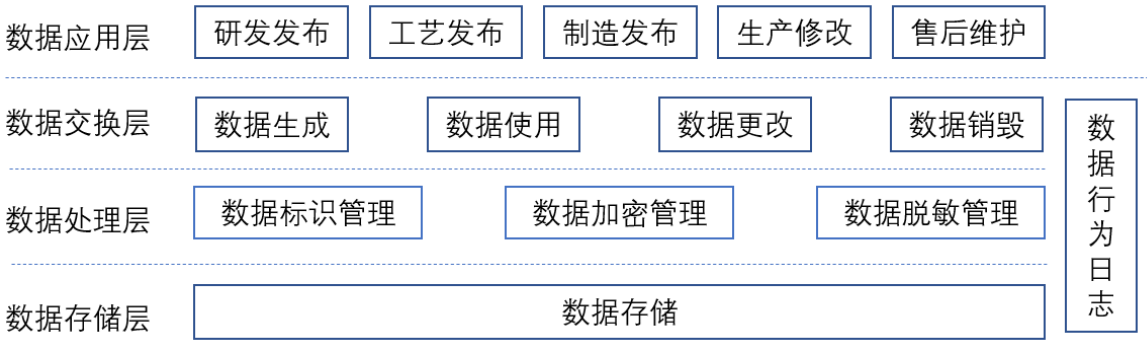

图1 制造业数据资产脱敏和交换管理软件架构

4.2 架构说明

4.2.1 数据存储层

数据存储层支持以任何格式进行物理存储或云存储。

4.2.2 数据处理层

数据处理层由下列内容组成：

a） 数据标识管理用于唯一标识数据的统一的标识管理；

b） 数据加密管理用于对达到一定安全要求的数据实施加密；

c） 数据脱敏管理用于对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私和安全数据的可靠保护。

4.2.3 数据交换层

数据交换层由下列内容组成：

a） 数据生成用于管理业务系统内部生成的新数据，或者从外部系统收集来的数据；
b） 数据使用用于管理业务系统或组织中的角色对数据的使用；
c） 数据更改用于针对数据进行计算并调整或者更正的对数据的处理过程；
d） 数据销毁用于在数据不在业务系统中使用时，对数据的归档和销毁操作。

4.2.4 数据应用层

包括制造业数据资产脱敏和交换管理相关的组织应用和其他专业应用系统。

制造业数据资产脱敏和交换管理的数据应用层包括研发发布过程应用、工艺发布过程应用、制造发布过程应用、生产修改过程应用以及售后维护等过程的应用。

4.2.5 数据行为日志

支持记录数据处理和交换过程的日志。

5 功能要求

5.1 数据存储层

制造业组织业务涉及的数据存储层主要存储以下数据：

a） 业务流程中产生的数据：如图纸、生产物料清单、工程设计关键计算结果等结构化和非结构化数据类型；
b） 工艺发布所产生的数据：如工艺卡、质检卡、装配卡和生产过程中的质检数据等结构化和非结构化数据类型；
c） 制造发布过程中所产生的数据：如加工计划、加工单据、物料签收等流程结构化数据类型；
d） 生产过程中所产生的数据：如修改工艺，修改加工流程，退工、不良品等结构化数据类型；
e） 制造业售后维护中所产生的数据：如维修单，现场检测单据、诊断结果等结构化和非结构化数据类型。

5.2 数据处理层

5.2.1 数据标识管理

数据标识管理应实现以下功能：

a） 支持数据的唯一标识的存储；
b） 支持基于标识的数据的查询；
c） 支持行为日志分析与标识的关联查询。

5.2.2 数据加密管理

数据加密管理实现基于可选的加密算法对关键数据的加密处理。数据加密处理应实现以下功能：

a） 支持对数据包含的关键数据进行加密处理；
b） 支持基于部门、业务以及基于数据标识的数据的访问授权；
c） 支持访问授权后数据的自动解密访问。

5.2.3 数据脱敏管理

数据应用层的应用只能得到数据脱敏后的数据进行使用，以隔绝其对原始数据集的操作。数据脱敏管理应实现以下功能：

a） 支持静态数据脱敏，即将敏感数据从生产环境脱敏完毕，再在非生产环境使用。使得脱敏后的数据与生产环境隔离，满足业务需要的同时又保障了生产数据的安全；
b） 支持动态数据脱敏，即访问敏感数据时实时进行脱敏，有时在不同情况下对于同一敏感数据的读取，需要做不同级别的脱敏处理；
c） 支持完全脱敏，即针对部分敏感数据，可以替换为随机的数字和字母；
d） 支持部分脱敏，即针对部分敏感数据，可以保留敏感数据的一部分，替换其他部分为随机的数字和字母；
e） 支持按照不同部门、不同业务、不同数据级别进行脱敏策略设置，即根据不同情况采用动态和静态脱敏以及完全和部分托名；
f） 脱敏后的数据会按使用次数和时间限制销毁。

5.3 数据交换层

5.3.1 数据生成

数据生成用于数据应用层创建业务系统内部的新数据，或者封装从外部系统收集来的数据。数据生成应实现以下功能：

a） 支持制造业组织需要的通用的、常见的数据格式；
b） 支持建立生成的数据与数据标识的关联关系；
c） 生成的数据应包含销毁时间以及敏感信息标识；销毁时间应支持依据制造业不同部门以及应用的业务进行自动设置；
d） 支持关键字段或者关键词查询；
e） 生成的数据应包含格式的版本标识。

5.3.2 数据使用

数据使用用于数据应用层使用数据生成模块生成的数据。数据使用应实现以下功能：

a） 支持通过数据标识或者关键字段和关键词查询获得需要的数据；
b） 支持通过获得数据对应的数据格式读取对应的信息；
c） 支持数据敏感信息依据访问者及访问模块进行数据自动脱敏。

5.3.3 数据更改

数据更改用于数据应用层变更数据内容。数据更改应实现以下功能：

a） 支持数据按照时间序列生成变更历史记录，并记录到数据行为日志中；
b） 支持对应关键数据的更改，支持采用数字签名等手段标识更改人；
c） 支持数据更好完毕，需审核后发布生效。

5.3.4 数据销毁

数据销毁用于数据应用层执行数据销毁或者数据由于生成或者更改导致的自动销毁。数据销毁应实现以下功能：

a） 应支持基于不同部门、不同业务等数据的销毁时长配置；
b） 支持数据销毁后归档的处理；
c） 支持归档周期、以及归档时限的设定；
d） 支持基于销毁时间或者其他触发条件的自动销毁；
e） 支持数据应用层授权后手工销毁的处理；
f） 支持销毁处理过程的数据行为日志记录。

5.4 数据应用层

数据应用层应支持一下应用类型：

a） 桌面端应用；
b） 浏览器端应用；
c） 移动端应用。

5.5 数据行为日志

数据行为日志分析应实现以下功能：

a） 支持数据生成、数据使用、数据更改以及数据销毁过程操作的记录；
b） 支持数据更改过程中，记录更好后的数据与原始数据的追溯关系；
c） 支持基于数据标识的数据生命周期周期中各个环节的操作和内容的查询。

6 建设要求

6.1 集成要求

6.1.1 概述

制造业数据资产脱敏和交换管理是制造业组织应用系统高安全和有效使用的核心组合部分，应支持企业中需要高安全及相关数据的集成。根据制造业数据资产脱敏和交换管理系统集成内容的不同，应提供以下两种集成方法：

a） 接口集成，制造业数据资产脱敏和交换管理系统应提供接口中间件，以简化不同应用系统对制造业数据资产脱敏和交换管理系统的功能集成；
b） 数据集成，用于支持应用系统制造业数据资产脱敏和交换管理系统之间进行数据的交换，制造业数据资产脱敏和交换管理系统应提供统一的数据交换格式；

6.1.2 日志系统接口需求

日志系统接口系统中原有的日志系统应该与制造业数据资产脱敏和交换管理系统中数据行为日志部分提供的接口对接完成与制造业数据资产脱敏和交换管理系统的集成。

日志系统接口应提供以下功能：

a） 支持根据访问资源的结果实现对资源的访问的记录；
b） 支持相关资源针对访问边界值的预警功能。

6.2 实施要求

6.2.1 概述

本实施要求规定制造业数据资产脱敏和交换管理的项目实施目标、阶段划分、阶段完成的任务及成果。

6.2.2 实施目标

通过制造业数据资产脱敏和交换管理项目的实施，应达成以下目标：

a） 实现基于原有业务系统管理体系的平滑升级；

b） 通过数据权限库的分级分类多维度的建立，积累了企业的安全保证措施，进一步保障了资源的访问安全性、规范性、正确性；

c） 实现了企业内和企业间协同的高安全性，降低由于不安全额外带来的时间和投入成本；

d） 实现针对以数据为中心的方法对数据分类，并由外部访问机制实现数据分类服务；

e） 实现工业互联等级保护2.0 和等级保护3.0 规范。

6.2.3 实施过程注意事项

基于制造业数据资产脱敏和交换管理实施项目，实施过程应遵循如下标准：

a) 团队组建中，应确定组织层面领导小组。重点是加入对组织生产高敏感性数据和数据使用规范要求高的关键领导；

b) 项目启动时，应明确项目对安全和高敏感型的定义和验证方法。

6.3 应用要求

6.3.1 网络环境

充分考虑到制造业业务系统高安全和数据量交互比较大的环境，并需要考虑到峰值业务访问，需建设与企业业务应用规模和未来发展规划相配套的网络环境。

6.3.2 数据与系统安全

数据与系统安全方面应遵循下列要求：

a） 制定清晰的数据使用规范与数据敏感定义，以便实施数据脱敏和使用与交换方法；

b） 利用制造业数据资产脱敏和交换管理的行为日志，及时发现数据使用的漏洞。

6.3.3 专职人员

6.3.3.1 系统管理员

系统管理员对制造业数据资产脱敏和交换管理的可靠运行必不可少。系统管理员要确保系统环境、网络环境的长期、安全和稳定高效。

6.3.3.2 安全审计员

采用制造业数据资产脱敏和交换管理的系统一定是需要高安全保障的系统，安全审计员要及时发现数据行为日志产生的信息，及时审核相关业务和数据的使用策略，保证系统数据按照既定策略有效执行相关的访问。

6.3.4 数据质量

6.3.4.1 数据正确性

确保进入制造业数据资产脱敏和交换管理的数据的正确性是制造业数据资产脱敏和交换管理成功的关键要素。数据创建者和提供者需要以高度负责的态度对检查数据的正确性，数据审核环节也应该尽责。

6.3.4.2 数据实时性

确保制造业数据资产脱敏和交换管理不影响业务的高效运行，需做到业务系统内部的实时制造业数据资产脱敏和交换管理响应。需要做到如下数据处理时的毫秒级响应：

a) 数据脱敏的处理速度；
b) 数据通过标识获取的响应速度。

6.3.4.3 数据完整性

进入制造业数据资产脱敏和交换管理的相关数据具有完整性要求,此类相关数据进入系统要尽可能的完整。

6.3.5 业务持续优化

6.3.5.1 流程引入

在制造业数据资产脱敏和交换管理引入初期，不应基于提出各种想法，应首先用开放的心态接受这种新的安全管理思路。以便制造业数据资产脱敏和交换管理能在短时间内顺利引入。

6.3.5.2 流程改进

随着制造业数据资产脱敏和交换管理的逐渐深入和使用，可以开始审查对现有业务的影响，哪些使用方法不够合理，是否可以优化，并尝试一定的改进。改进应在测试环境进行，成熟后一定到正式环境。

6.3.5.3 拓展业务范围

随着企业业务变化，或者增加新的业务。可以开始考虑将制造业数据资产脱敏和交换管理的安全策略和系统移植都新的业务中来，进一步扩大制造业数据资产脱敏和交换管理的使用范围。

6.3.6 持续推动业务应用

6.3.6.1 管理层重视

业务系统的安全对相关业务的开展的重要性要求组织高层必须持续关注和推动制造业数据资产脱敏和交换管理在组织内的应用。高层需要在人、财、物和政策等多方面给与重视和支持。

6.3.6.2 纳入安全战略

组织需要明确制造业数据资产脱敏和交换管理是组织安全战略和数据使用规范的基础设施，有效的实施对组织核心资产的安全必不可少。

6.3.7 维护与升级

6.3.7.1 安全策略维护

经常性维护制造业数据资产脱敏和交换管理关联的各类资源的安全策略，并针对已经发生的安全事故进行策略调整，以便提高系统的安全性。

6.3.7.2 采购安全服务

可以考虑采购相应的售后服务，获得专业保障。

6.3.7.3 及时升级

及时升级到合适的版本是保障系统安全可靠、数据使用规范化的必要措施。

参 考 文 献

[1] GB/T 5271.18-2008 《信息技术 词汇 第 18 部分：分布式数据处理》[2] GB/T 11457-2006 《信息技术 软件工程术语》

[2] GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》[6] GB/T 20520—2006 《信息安全技术 公钥基础设施 时间戳规范》

[3] GB/Z 28828—2012 《信息安全技术 公共及商用服务信息系统个人信息保护指南》[8] GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》

[4] ISO/IEC 9804-1998 《信息技术 开放系统互连 托付、并发和恢复服务元素 Information technology -- Open Systems Interconnection -- Service definition for the Commitment, Concurrency and Recovery service element》

[5] IEEE P2418.2 《数据格式规范 Data Format for Blockchain Systems (C/SAB/DBC)》