ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB 21/T XXXX—XXXX

工业互联网区块链零信任建设要求

Industrial internet zero trust base on block chain standardization

（征求意见稿）

（本草案完成时间：2023-08-08）

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

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

工业互联网安全的概念由来已久，基础的认证、授权、审计的概念以及在业务实现上被普遍接受。但就目前网络环境日趋复杂，工业互联网业务内容不变更新和变化的环境来看，尤其针对高安全要求的系统，传统的基于用户身份的单一的认证、授权、审计的安全模式已经不足以满足当前环境的要求。

针对数字时代下数据安全风险的变化，数据安全理念和方法需要演进，其核心思路就是从静态到动态的转变。数字时代的信息化环境是动态的，业务需求是动态的，风险也是动态的，数据管控需求必然也是动态的，需要用动态的安全思路来应对这些新需求、新挑战，工业互联网区块链零信任建设要求就是这样一种基于动态策略的安全理念和建设规范。

工业互联网区块链零信任建设要求涉及工业互联网区块链零信任的基础概念，以及工业互联网区块链零信任建设要求的参考架构。本文件力求从普遍的工业互联网高安全角度出发，比较系统、完整地反映工业互联网区块链零信任领域的技术术语、体系结构、业务需求和功能要求。

本文件的目的并非：

- 建议只有一种方式可以实现工业互联网区块链零信任；
- 强迫用户放弃他们现有的业务系统安全管理系统和模式。

使用本文件所带来的潜在收益有：

- 在组织内部建立基于零信任接入的共同语境；
- 建立第三方应用供应商基于工业互联网区块链零信任的共同语境；
- 帮助组织第三方应用供应商理解和描述工业互联网区块链零信任的需求；
- 帮助供应商提供满足组织需求的工业互联网区块链零信任的产品和服务。

工业互联网区块链零信任建设要求

1 范围

本文件提出了工业互联网区块链零信任概念模型，规定了工业互联网区块链零信任体系结构、功能要求以及与应用系统的集成、实施、应用等相关要求。

本文件适用于工业互联网区块链零信任的开发、实施组织、咨询服务机构、软件测评机构、安全审计机构，以及工业互联网业务应用的实施和咨询服务机构和工业互联网区块链零信任的使用方。

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 22239 信息系统安全等级保护基本要求

GB/T 42021-2022 工业互联网 总体网络架构

3 术语和定义

GB/T 42021界定的以及下列术语和定义适用于本文件。

3.1

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而形成的分布式账本。

3.2

智能合约 smart contract

以数字形式定义的能够自动执行条款的合约。

3.3

零信任 zero trust

对网络资源的访问，无论访问者（主体）和被访问者（资源）是否可信，主体和资源之间的信任关系都需要从零开始，通过信任评估进行构建，从而实施访问控制，基于此原则建立的安全访问机制称为零信任。

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

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

动态授权 dynamic authorization

在工业互联网区块链零信任中，访问主体在对资源进行访问前，临时获得的对资源的访问权限，访问任务结束时也随之终结。

3.7

接口集成 interface integration

在应用或者其他软件系统中，嵌入对零信任接入系统的调用，以便实现高安全的需求。

3.8

数据集成 data integration

在应用或者其他软件系统中，需要与零信任接入系统进行数据的交互，以便实现快速集成的需求。

3.9

版本 version

用于记录工业互联网区块链零信任系统状态变更的标识。

4 概念模型

4.1 概述

传统应用大多基于身份认证的模式实现授权访问，在工业互联网数据和用户信息实时多变的情况下已经不足以满足工业互联网高安全性的要求，企业需要在满足行业合规以及相关威胁情报的合理处理下，处理相关的资源访问安全性的问题。本文件基于工业互联网高安全要求，引入区块链零信任方法，建立工业互联网区块链零信任标准，目的在于定义一般工业互联网对应的安全验证应遵循的标准和规范。本文件应用的概念模型，见图1。

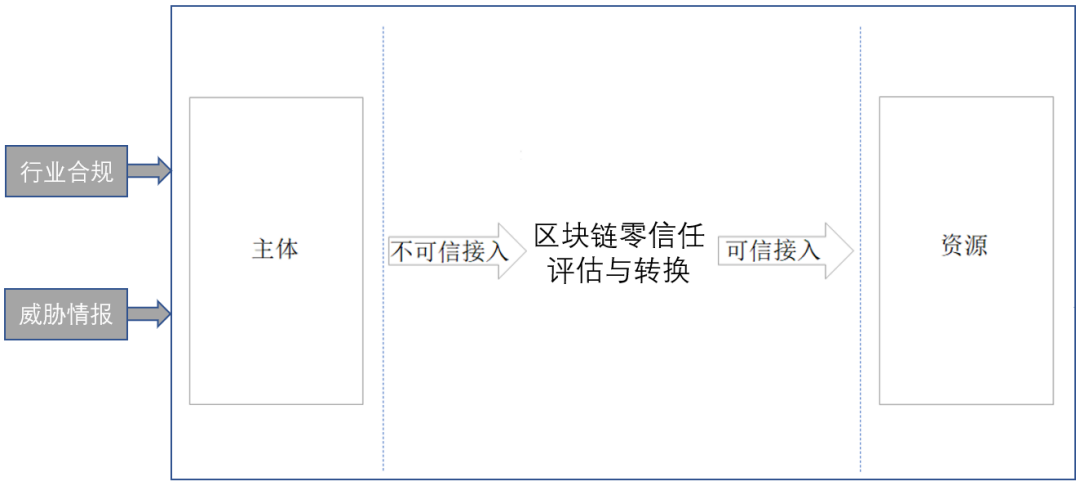

图1 区块链零信任概念模型

如图1所示的概念模型，该模型重点在高安全以及安全性要求与环境动态变化有关的实际场景，如下列典型场景：

a) 资源访问需受网络流量限制：即资源在网络流量过大的情况下需要限制主体的访问。此时传统的用户授权模式已经不可能发生作用，需要依据环境的变化拒绝主体对资源的访问，即不可信接入通过区块链零信任评估与转换，无法转换为可信接入。这类场景还包括网络流量瞬发频次，流量数据量波动，流量 IP 地址和转发流量频次等；

b) 资源的读写次数限制：即资源需要控制在某些场合或者时间范围内的读写次数。此时传统的用户授权模式已经不可能发生作用，需要依据实际对资源的访问情况，控制下一次对资源的访问。

4.2 各部分概念说明

4.2.1 行业合规

企业在经营管理过程中所遵守的法律法规、行为准则、商业伦理道德、企业内部规章制度等方面的要求，要以业务和风险为核心，契合企业治理、运作、文化和价值观。

4.2.2 威胁情报

威胁情报旨在为面临威胁的资产主体（通常为资产所属企业或机构）提供全面的、准确的、与其相关的、并且能够执行和决策的知识和信息。

4.2.3 主体

所有需要对系统中其他资源进行访问的全体构成概念模型中的主体。在实际的环境中，主体会包括软件应用、操作系统、数据库、中间件、服务等。

4.2.4 资源

系统中可供访问的客体的全体构成概念模型中的资源。在实际的环境中，资源会包括软件应用、操作系统、数据库、中间件、服务等。

4.2.5 区块链零信任评估与转换

区块链零信任评估与转换功能示意，如图1。从最初的不可信接入，经过区块链零信任评估与转换的审核，成为可信接入，完成了对资源的访问。本文件认为工业互联网资源在缺省情况下的访问都是不安全的。用户在未经区块链零信任评估与转换的情况下只能进行最小特权访问。本文件体系架构中重点说明区块链零信任评估与转换的实现机制。

5 体系结构

5.1 软件架构图

工业互联网区块链零信任是基于组织内业务系统高安全考虑的平台软件，其软件架构应采用分层结构，见图2。

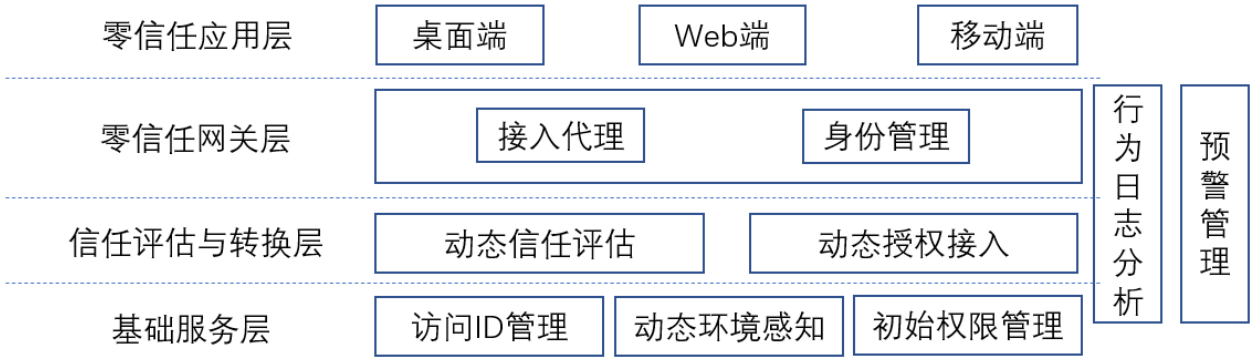

图2　工业互联网区块链零信任软件架构

5.2　架构说明

如图2所示的架构图，其中零信任网关层与信任评估和转换层构成了整个零信任架构的核心，应用层通过零信任网关对工业企业内部的资源进行访问；零信任网关再对访问主体进行信任评估，获得对资源访问的权限后，再对资源进行受限的访问。

5.2.1　基础服务层

基础服务层由下列内容组成：

a）　访问标识管理用于对资源访问过程的记录。主体对资源的每一次访问都会产生唯一的标识，并且是全局统一的标识；

b）　动态环境感知从实际工业互联网业务系统工作环境中，依据工业互联网中关注的安全评估要素，提取出与资源访问有关的信息，如对资源的访问次数，网络当前的瞬间流量等；

c）　初始权限管理记录被访问资源上一次的授权访问情况。

5.2.2　信任评估与转换层

信任评估与转换根据受限访问的资源需要评估的各个因素，以及各个因素的相关信息，计算结果为该接入是否可信，以实现对资源的受限访问。基于动态信任评估，以及动态授权接入实现从最初的不可信接入转换成为可信接入，完成对资源的访问。信任评估与转换层应包含以下内容：

a）　动态信任评估：从多维角度描述系统环境下影响被访问资源信任度计算的各个因素，对模型的各个因素权重进行求解，从而建立主体访问资源这一时刻资源访问的权限评估要素和权重。传统的用户名和密码的验证方式是零信任的最基础模型；

b）　动态授权接入：实际业务系统工作环境中，基于动态的环境变化，动态环境感知从复杂的变化的环境中，依据动态信任评估给出的评估要素提取与资源访问有关的信息。

5.2.3　区块链零信任网关层

零信任安全网关是零信任架构核心的部分，部署在网络入口或应用服务前端，分隔用户和资源，对所有流量强制执行访问控制策略。零信任安全网关包含接入代理、身份管理组件，具备应用访问代理、访问主体多维认证、动态信任评估、行为日志分析等功能，在提高应用访问安全性的同时简化接入过程，提升业务效率。区块链技术可以提供接续控制、用户认证、交易安全，具有可追溯性，可以为零信任机制提供更好的实现架构。区块链零信任网关层应包含以下内容：

a）　接入代理：由接入代理提供应用层的基于授权的访问接入；

b） 身份管理：通过身份管理，获得主体的访问身份，作为后续对资源访问的主体的标识。

5.2.4 零信任应用层

包括零信任接入的组织应用和其他专业应用系统，应包括：

a） 桌面端应用；

b） 浏览器端应用；

c） 移动端应用。

5.2.5 行为日志分析

支持记录行为日志数据，并根据边界行为判断，并能够通知相关系统。

5.2.6 预警管理

支持依据行为日志分析监测，并依据边界行为判断，产生相关预警信息。

6 功能要求

6.1 基础服务层

6.1.1 访问标识管理

支持对资源访问的统一标识管理,即每一次访问都赋予一次唯一访问标识追溯号,应实现以下功能：

a） 支持资源访问的统一标识的存储；

b） 支持访问者与标识的关联；

c） 支持行为日志分析与标识的关联；

d） 支持通过访问者、行为日志、访问标识获取访问者的特征和访问机制。

6.1.2 动态环境感知

动态环境感知支持从变化的环境中，依据动态信任评估给出的评估要素提取与资源访问有关的信息，动态环境感知应实现以下功能：

a） 支持基于动态信任评估的维度给出不同维度的环境参考值；

b） 支持基于智能合约的环境数据感知模式，保证获取的环境数据的一致性和不可篡改。

6.1.3 初始权限管理

初始权限管理应记录被访问资源上一次的授权访问情况，初始的授权应该是无权限访问，初始权限管理应实现以下功能：

a） 支持建立初始行为授权数据库，任何初始接入按照初始授权数据库设定；

b） 支持对资源访问过程中动态授权接入的授权信息获取；

c） 支持授权信息在下一次同样的资源被访问的时候作为初始权限信息被读取。

6.2 信任评估与转换层

6.2.1 动态信任评估

动态信任评估实现评估维度和初始状态的设定，动态信任评估应实现以下功能：

a) 支持从初始权限管理获得本次访问资源的初始权限信息；
b) 支持从多维角度描述系统环境下被访问资源信任度的各个因素；
c) 支持 b）中描述的要素的权重设定；
d) 支持依据区块链智能合约模式制定并执行，保证动态信任评估在零信任接入代理节点执行的效率以及执行条件的一致性；
e) 符合 GB/T 22239 等级保护要求，达到不同等保要求下对资源的访问。

6.2.2 动态授权接入

动态授权接入依据上次对资源访问的结果，根据权限要素及其权重以及动态环境感知该处的评估要素情况，计算本次对该资源的访问权限，实现对该资源的精准管控。动态授权接入应实现以下功能：

a) 支持上次对资源访问的结果的获取；
b) 支持依据该资源权限要素维度及权重计算本次访问权限；
c) 支持对资源的授权访问；
d) 支持依据区块链智能合约模式制定并执行，保证执行资源访问的田间的一致性和访问的可追踪性；
e) 符合 GB/T 22239 等级保护要求，达到不同等保要求下对资源的访问。

6.3 零信任接入代理层

6.3.1 零信任接入代理

零信任接入代理支持组织内其他业务系统通过不同方式实现零信任接入到组织并实现对组织内资源的授权访问。从而实现基于零信任的授权方式。零信任接入代理应实现以下功能：

a) 支持外部不同的接入方式。如桌面端应用、浏览器端应用、移动端应用；
b) 支持对访问端要访问的资源的透明访问。

6.3.2 零信任应用层

包括零信任接入的组织应用和其他专业应用系统。

零信任接入应用层包括桌面端应用、浏览器端应用和移动端应用。这类应用是本文件应支持的各类应用，这些类型的应用应该遵从本文件规范实现相关的安全应用接入。

6.4 行为日志分析

行为日志分析应实现以下功能：

a) 支持通过行为日志数据，找出边界行为，并通知相关系统；
b) 行为日志数据应满足如下要求：
    1) 应记载各种访问的浏览路径；
    2) 应记载访问流程和边界条件，并对每一种访问的边界行为实现记录；
    3) 边界行为应由授权数据库（静态）、行为日志数据（动态）以及边界行为判定比较计算单元计算获得。

6.5 预警管理

预警分析应实现以下功能：

a) 支持预警值信息设定；

b） 支持预警值输出接口。

7 建设要求

7.1 集成要求

7.1.1 概述

工业互联网区块链零信任系统应支持组织中需要高安全访问的业务系统及相关资源对零信任接入系统的集成，根据应用系统与工业互联网区块链零信任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：工业互联网区块链零信任系统应提供接口中间件，以简化不同应用系统对工业互联网区块链零信任系统的功能集成；

b） 数据集成：用于支持应用系统与工业互联网区块链零信任系统之间进行数据的交换，工业互联网区块链零信任系统应提供统一的数据交换格式。

7.1.2 认证系统接口需求

工业互联网业务系统中原有的认证系统应该通过与工业互联网区块链零信任系统中动态信任评估提供的接口对接完成与工业互联网区块链零信任系统的集成，认证系统应至少提供以下信息：

a） 用户标识；

b） 本次访问时间。

7.1.3 授权系统接口需求

工业互联网业务系统中原有的授权系统应该与工业互联网区块链零信任系统中动态授权部分提供的接口对接完成与工业互联网区块链零信任系统的集成。授权系统应实现以下功能：

a） 支持不同资源访问权限边界值的设定；

b） 支持根据获得的授权结果实现对资源的有限访问；

c） 支持记录本次访问的情况。

7.1.4 审计系统接口需求

业务系统中原有的审计系统应该与工业互联网区块链零信任系统中行为分析部分提供的接口对接完成与工业互联网区块链零信任系统的集成。审计系统应实现以下功能：

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。

7.2 实施要求

7.2.1 概述

规定工业互联网区块链零信任项目实施目标、实施过程的重点注意事项。

7.2.2 实施目标

通过工业互联网区块链零信任项目的实施，应达成以下目标：

a） 实现基于原有安全体系的平滑升级；

b） 通过资源权限库的分级分类多维度的建立，积累了组织的安全保证措施，进一步保障了资源的访问安全性、规范性、正确性；
c） 实现了组织内和组织间协同的高安全性，降低由于不安全额外带来的时间和投入成本；
d） 对所有IT和数据资产编目，并基于角色分配访问权限；
e） 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；
f） 对网络分段，以防止外部访问在内网漫游及其他攻击。

7.2.3 实施过程注意事项

基于工业互联网区块链零信任项目实施的高安全性要求，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安全负责的关键领导；
b） 项目启动时，应明确项目对安全的定义和验证方法；
c） 项目执行时，应确认与原有认证、授权、审计系统集成的成果确认。

7.3 应用要求

7.3.1 概述

工业互联网区块链零信任应用要求包括网络环境要求、数据与系统安全要求、外部访问客体要求、内部被访问客体要求、数据质量要求等。

7.3.2 网络环境

工业互联网区块链零信任系统环境交互数据量比较大，考虑到峰值业务访问，需建设与组织业务应用规模和未来发展规划相配套的网络环境。

7.3.3 数据与系统安全

数据与系统安全方面应遵循下列要求：
a） 制定清晰的功能和数据权限体系，以便实施动态信任评估；
b） 利用工业互联网区块链零信任的行为日志和预警管理体系，及时发现资源访问的漏洞；
c） 工业互联网区块链零信任的安全要求执行 GB/T 22239 安全等级保护的相关规定。

7.3.4 专职人员

7.3.4.1 系统管理员

系统管理员应确保工业互联网区块链零信任系统环境、网络环境的长期、安全和稳定高效。

7.3.4.2 安全审计员

安全审计员应采用工业互联网区块链零信任的系统及时发现系统行为日志以及预警系统产生的信息，及时审核相关业务和资源的权限策略，保证系统资源按照既定策略有效执行相关的访问。

7.3.5 外部访问客体

工业互联网区块链零信任主要涉及的系统间安全的边界问题，其外部访问客体包括：
a） 不在本业务所属网段的外部异地信息设备。如远程控制终端，远程维护设备，远程其他需要访问此网段的操作系统等等；

b) 外部的访问人员。如组织成员，供应链上下游组织以及设计研发，第三方验证等相关数据共享者；
c) 外部共享数据的工业互联应用和二次开发应用。如供应链 EDI 数据交换，设备远程维修诊断等系统；
d) 外部信息系统。如工厂门户订阅，工厂与电子销售系统，库存共享系统等等；
e) 政府监管系统。如行业监管对接，环境监管和相关危险品、消防等等系统的监管数据上报机制。

7.3.6 内部被访问客体

工业互联网区块链零信任主要涉及的系统间安全的边界问题，其内部被访问客体包括：
a) 组织内部设备、环境感知需要的所有设备数据，运行数据和生产环境数据；
b) 制造数据系统，管理系统以及环境，人机界面指令和控制命令以及计算汇总结果的结构化、非结构化数据库；
c) 内部信息设备。如工业互联网服务器，工位机，产线大屏，人机交互界面等信息设备，可以输入输出，显示计算工业互联网相关的数据；
d) 自动化设备控制器。如工业生产数据采集，可编程逻辑控制器，边缘计算机以及仪器仪表网络的控制设备和计算单元，这些设备与计算单元负责自动化设备的流程运转控制，设备自动检验检测和设备运维的设置处理等相关数据；
e) 网络接口。如金融、工业互联网网络中其他办公，制造，物联网等不同的网络域和网段。

7.3.7 数据质量

7.3.7.1 数据正确性

确保进入工业互联网区块链零信任的相关数据（如身份数据、环境感知需要的所有设备数据）的正确性是工业互联网区块链零信任成功的关键要素。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。

7.3.7.2 数据实时性

确保工业互联网区块链零信任不影响业务的高效运行，需做到业务系统内部的实时响应。需要做到如下数据时延和分析达到毫秒级响应：
a) 业务系统设备数据；
b) 环境感知需要的所有设备数据；
c) 运行数据和生产环境数据。

7.3.7.3 数据完整性

进入工业互联网区块链零信任的相关数据（如身份数据、环境感知需要的所有设备数据）具有完整性要求,这类数据对被访问资源的权限判断具有很高的重要性。此类相关数据进入系统要尽可能的完整。

7.3.8 业务持续优化

7.3.8.1 流程引入

在工业互联网区块链零信任引入初期，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。以便工业互联网区块链零信任能在短时间内顺利引入。

7.3.8.2 流程改进

随着工业互联网区块链零信任的逐渐深入和使用，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。

7.3.8.3 拓展业务范围

随着组织业务变化，或者增加新的业务。可以开始考虑将工业互联网区块链零信任的安全策略和系统移植都新的业务中来，进一步扩大工业互联网区块链零信任的使用范围。

7.3.9 持续推动业务应用

7.3.9.1 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管理层必须持续关注和推动工业互联网区块链零信任在组织内的应用。高层需要在人、财、物和政策等多方面给与重视和支持。

7.3.9.2 纳入安全战略

组织需要明确工业互联网区块链零信任是组织安全战略的基础设施。

7.3.10 维护与升级

7.3.10.1 安全策略维护

经常性维护工业互联网区块链零信任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。

7.3.10.2 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。

7.3.10.3 及时升级

及时升级到合适的版本是保障系统安全可靠的必要措施。

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

[3] GB/T 25069-2010 信息安全技术 术语

[4] GB/T 32399-2015 信息技术 云计算 参考架构

[5] GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

[6] 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

[6] GB/T 42752-2023 区块链和分布式记账技术 参考架构

[8] ISO/IEC 9804-1998 Information technology -- Open Systems Interconnection -- Service definition for the Commitment, Concurrency and Recovery service element

[9] IEEE P2418.2 Data Format for Blockchain Systems (C/SAB/DBC)