ICS 35.020
CCS L80

DB21

辽　宁　省　地　方　标　准

DB21/TXXXX—XXXX

工业互联网　安全要求

（征求意见稿）

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 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　设备安全 2
4.1　设备身份鉴别 2
4.2　设备访问控制 2
4.3　运维用户身份鉴别 2
4.4　运维用户访问控制 3
4.5　入侵防范 3
4.6　系统升级安全 3
4.7　硬件接口安全 3
4.8　冗余备份恢复安全 3
5　控制安全 3
5.1　控制协议完整性保护 3
5.2　控制软件用户身份鉴别 4
5.3　控制软件用户访问控制 4
5.4　入侵防范 4
5.5　资源控制 4
6　网络安全 4
6.1　工厂内部网络安全防护 4
6.2　工厂外部网络安全防护 5
6.3　边界防护 5
6.4　应用安全防护 6
7　标识解析安全 7
7.1　运行环境安全 7
7.2　身份安全 8
7.3　服务运营安全 9
7.4　数据安全 ..... **错误！未定义书签。**

8 平台安全 9
8.1 边缘层安全防护要求 9
8.2 平台 IaaS 层安全防护要求 11
8.3 平台 PaaS 层安全防护要求 14
8.4 平台 SaaS 层安全防护要求 18
9 数据安全 24
9.1 数据保密性保护 24
9.2 数据完整性保护 24
9.3 访问控制 25
9.4 数据抗抵赖 25
9.5 数据备份恢复 25
9.6 数据销毁 25
9.7 数据溯源 25

前　言

本文件按照GB/T1.1-2020《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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：沈阳华睿博信息技术有限公司等。

本文件主要起草人：邵华等。

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。

归口管理部门通信地址：辽宁省沈阳市皇姑区北陵大街45-2号。

归口管理部门联系电话：024-86913384。

标准起草单位通讯地址：辽宁省沈阳市和平区青年大街386号华阳国际大厦2396。

标准起草单位联系电话：18698849086。

工业互联网 安全要求

1 范围

本文件规定了工业互联网设备安全、控制安全、网络安全、标识解析安全、平台安全以及数据安全等方面的要求。

本文件适用于工业互联网安全监管部门、运营单位等组织开展安全防护工作，为工业互联网安全防护提供指导。

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 22239-2019 信息安全技术 网络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

YD/T 2439-2012 移动互联网恶意程序描述格式

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业互联网 industrial internet

新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，通过对人、机、物、系统等的全面连接,构建起覆盖全产业链、全价值链的全新制造和服务体系。

[来源：GB/T 42021-2022,3.1]

3.2

工业互联网平台 industrial internet platform

面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系，支撑制造资源泛在连接、弹性供给、高效配置的载体。

3.3

工业应用程序 industrial application

可实现包括工业设计、生产、管理、服务等在内能力的工业业务系统或移动应用程序。

3.4

工厂内部网络 enterprise internal network

在工厂内部，用于生产要素互联及企业 IT 管理系统之间连接的网络。

3.5

工厂外部网络 enterprise external network

以支撑工业全生命周期各项活动为目的，用于连接企业上下游之间、企业与智能产品、企业与用户之间的网络。

3.6

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、入侵、干扰、破坏和非法使用以及意外事故，使网络处于可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239-2019,3.1]

4 缩略语

下列缩略语适用于本文件。

FTP：文件传输协议（File Transfer Protocol）

HMI：人机接口（Human Machine Interface）

IP：网络协议（Internet Protocol）

5 设备安全

5.1 设备身份鉴别

设备身份鉴别要求如下：

a） 应采用鉴别机制对接入工业互联网中的设备身份进行鉴别，确保数据来源于真实的设备；

b） 若存在需要对接入工业互联网中的设备进行远程管理的，应采取必要措施，防止身份鉴别信息在网络传输过程中被窃听。

5.2 设备访问控制

应通过制定安全策略如访问控制列表，实现对接入工业互联网中设备的访问控制。

5.3 运维用户身份鉴别

运维用户身份鉴别要求如下：

a） 应对登录设备进行运维的用户进行身份标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；

b） 对于登录设备进行运维的过程应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

5.4 运维用户访问控制

运维用户访问控制要求如下：

a） 应对登录设备进行运维的用户分配账户和权限；

b） 应重命名或删除默认账户，修改默认账户的默认口令；

c） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d） 应对登录设备进行运维的用户授予其所需的最小权限，并实现对不同类型运维用户的权限分离。

5.5 入侵防范

入侵防范要求如下：

a） 应遵循最小安装的原则，仅为设备安装需要的组件和应用程序；

b） 设备生产商应明示设备中使用的端口与服务列表及用途，并关闭设备中不需要的端口与服务；

c） 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

d） 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。

5.6 系统升级安全

系统升级安全要求如下：

a） 应保障关键设备具有系统升级功能；

b） 应保障系统升级操作的安全，如更新时机和更新权限；

c） 应能检测升级软件的真实性和完整性。

5.7 硬件接口安全

所有用于生产、调试和维修的接口要求默认禁用且普通用户不可激活，厂商应具有相关安全防护接入机制。

5.8 冗余备份恢复安全

关键部件应支持冗余功能，在设备运行状态异常可能影响网络安全时，可通过启用备用部件防范安全风险。

6 控制安全

6.1 控制协议完整性保护

对于控制协议应采取完整性保证机制，确保控制协议中的各类指令不被非法篡改和破坏。

6.2 控制软件用户身份鉴别

控制软件用户身份鉴别要求如下：

a） 应对登录控制软件进行操作的用户进行身份标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；

b） 对于登录控制软件进行操作的过程应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

6.3 控制软件用户访问控制

控制软件用户访问控制要求如下：

a） 应对登录控制软件进行运维的用户分配账户和权限；

b） 应重命名或删除默认账户，修改默认账户的默认口令；

c） 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

6.4 入侵防范

入侵防范要求如下：

a） 控制软件应遵循最小安装的原则，仅安装需要的组件；

b） 控制软件生产商应明示控制软件中使用的端口与服务列表及用途，并关闭控制软件中不需要的端口与服务。

6.5 资源控制

应限制单个用户或进程对系统资源的最大使用限度。

7 网络安全

7.1 工厂内部网络安全防护

7.1.1 区域划分与隔离

工厂内部网络应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。

7.1.2 数据传输完整性保护

应采用适应工厂内部网络特点的完整性校验机制，实现对网络数据传输完整性保护。

7.1.3 网络异常监测

应对网络通讯数据、访问异常、业务操作异常、网络和设备流量、工作周期、抖动值、运行模式、各站点状态、冗余机制等进行监测，发生异常进行报警。

7.1.4 无线网络攻击的防护

应对通过无线网络攻击的潜在威胁和可能产生的后果进行风险分析，并对可能遭受无线攻击的设备的信息发出(信息外泄)和进入（非法操控)进行屏蔽。

7.1.5 网络入侵防范

应在关键网络节点处部署入侵防范措施，对针对这些节点的入侵行为进行检测，并在发生严重入侵事件时提供报警。

7.2 工厂外部网络安全防护

7.2.1 数据传输完整性保护

应采用常规校验机制检验网络数据传输的完整性，并能发现其完整性被破坏的情况。

7.2.2 数据传输保密性保护

应采用密码技术支持的数据保密机制，实现对网络中传输数据的保密性保护。

7.2.3 网络入侵防范

应在关键网络节点处部署入侵防范措施，对针对这些节点的入侵行为进行检测，并在发生严重入侵事件时提供报警。

7.3 边界防护

7.3.1 网络边界隔离

工厂内部网络与工厂外部网络之间应划分为两个区域，区域间应采用技术隔离手段。

7.3.2 网络边界访问控制

网络边界访问控制要求如下：

a） 应在网络边界根据访问控制策略设置访问控制规则，保证跨越网络边界的访询和数据流通过边界防护设备提供的受控接口进行通信，默认情况下受控接口拒绝所有通信；

b） 应删除多余或无效的访问控制规则，优化访问控制列表,并保证访问控制规则数量最小化；

c） 应根据网络边界访问控制规则，通过检查数据包的源地址、目的地址、源端口、目的端口、协议等，确定是否允许该数据包通过该区域边界；

d） 工厂内部网络与工厂外部网络之间应采用访问控制机制，不应有任何穿越区域边界的E-Mail、Web、Telnet、Rlogin、FTP等通用网络服务；

e） 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

f） 工程师站、操作员站、HMI等位于工厂内部网络的重要控制节点不应在无安全防护措施的情况下直接与工厂外部网络建立连接。

7.4 应用安全防护

7.4.1 用户身份鉴别

用户身份鉴别要求如下：

a） 应对使用工业互联网平台与工业应用程序的用户身份进行标识和鉴别，身份标识应具有唯一性，身份鉴别信息应具有复杂度要求并定期更换；

b） 工业互联网平台及工业应用程序的登录过程应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施:

c） 应使用密码技术对鉴别数据进行保密性和完整性保护；

d） 应强制用户首次登录时修改初始口令；

e） 用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全。

7.4.2 访问控制

访问控制要求如下：

a） 应提供访问控制功能，对使用工业互联网平台及工业应用程序的用户分配账户及相应的访问操作权限；

b） 应重命名或删除默认账户，修改默认账户的默认登录口令；

c） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d） 工业互联网平台应为工业应用程序提供访问控制授权能力；

e） 应根据访问控制策略，对工业互联网平台开发者、工业应用程序及其用户调用工业互联网平台开发接口实施访问控制。

7.4.3 合规性检查

对于工业互联网平台及工业应用程序应提供数据合规性检验功能(如验证数据类型是否正确、数据大小或长度是否超出范围等)，保证通过人机接口输入或通过通信接口输入的内容符合其设定要求。

7.4.4 应用管控

应用管控要求如下：

a） 工业应用程序供应商不应通过捆绑安装、自动启动等技术手段对用户自主选择安装或运行应用程序的权利进行限制；

b） 应设置针对工业应用程序的白名单功能,根据应用程序白名单控制应用程序的安装、运行；

c） 应具有应用程序权限控制功能，应能控制应用程序对终端设备中资源的访问；

d） 应只允许可靠证书签名的应用程序安装和运行。

7.4.5 应用来源保证

应用来源保证要求如下：

a） 工业互联网平台运营商应保证终端设备安装、运行的工业应用程序来自可靠证书签名或可靠分发渠道；

b） 工业互联网平台运营商应保证终端设备安装、运行的工业应用程序由可靠的开发者开发；

c） 工业互联网平台运营商应验证开发工业应用程序的签名证书的合法性。

7.4.6 应用健壮性保证

在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施。

7.4.7 应用资源控制

应用资源控制要求如下：

a） 工业互联网平台及工业应用程序应具备会话超时自动结束功能,当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b） 应能够对工业互联网平台及工业应用程序的最大并发会话连接数进行限制；

c） 应能够对单个账户的多重并发会话进行限制；

d） 应能够对用户或进程对终端设备系统资源的最大使用限度进行限制，防止终端设备被提权。

7.4.8 应用上线前检测

应在工业互联网平台及工业应用程序上线前对其安全性进行测试，对可能存在的缺陷与恶意代码等进行检测。

8 标识解析安全

8.1 运行环境安全

8.1.1 物理环境安全防护

物理环境安全防护要求如下：

a） 应建立机房安全管理制度，对机房所在区域采取访问授权、视频监控等物理安全防护措施并定期巡查通信线路；

b） 应对核心软硬件所在区域采取安全域隔离、访问控制、视频监控、专人值守等物理安全防护措施。防火、防盗、防静电、温湿度控制、防尘、电力供应、电磁防护。

8.1.2 设备及软件系统安全防护

设备及软件系统安全防护要求如下：

a） 应建立标识解析系统基础设施资产清单，做好资产分类、定级与标识管理，及时修复重要系统的安全漏洞；

b） 应建立恶意代码防护及其相应的维护机制，通过手动或自动方式及时更新，防止非特权用户绕过；

c） 应密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需对补丁进行严格的安全评估和测试验证。

8.1.3 网络安全防护

网络安全防护要求如下：

a） 应做好安全域划分，分离安全区域，通过网络边界防护设备对边界进行安全防护，通过防火墙、网闸等防护设备对安全区域之间进行逻辑隔离安全防护；

b） 应对核心系统（如标识解析节点服务系统）搭建独立的计算平台、存储平台、内部网络环境及相关维护、安防、电源等设施，并经由受控边界与外部网络相连；

c） 应做好入侵防范，建设端口扫描、木马后门、DDoS、缓冲区溢出等网络入侵行为检测及报警能力，并记录攻击源IP、攻击类型、攻击时间；

d） 应对进出关键系统的数据信息进行过滤，并能根据系统能力对网络流量及并发数进行限制，对关键入侵行为进行阻断；

e） 应做好安全审计，对重要设备运行情况、网络流量信息、系统管理及维护等信息进行记录，对记录进行留存并加以保护，防止篡改和未授权访问，以支持将来的调查和访问控制监视。

8.2 身份安全

8.2.1 组织机构安全

应加强机构实体身份认证，对于新申请加入的组织机构做好相关身份与资质审查，建立身份信息标识，保证操作过程身份可校验，防止机构身份伪造。

8.2.2 终端安全

终端安全要求如下：

a） 应通过防伪、标识绑定等技术防止被动及主动标识载体中的标识编码被篡改、伪造；

b） 应通过软件安全防护技术，防止客户端被破坏，避免其身份被篡改、伪造、恶意利用。

8.2.3 协议安全

应采用具有认证机制的通信协议，在各级节点间、客户端与服务端间等通信过程中，对主体身份、消息进行安全认证，支持配套的认证密钥建立。

8.2.4 平台系统安全

平台系统安全要求如下：

a） 应建设支持多种认证方式的身份与权限管理平台，对工业互联网标识解析涉及的多主体对象的身份及权限进行统一管理；

b） 应对用户访问的全过程实行严格的向正确的用户实行相应的权限控制，包括从登入到登出的过程。

8.3 服务运营安全

服务运营安全要求如下：

a） 应对标识解析注册机构、运营服务机构、监管方、安全服务提供方、安全运营方等制定相应的管理制度和运营规范，明确各机构的职责、权益工作流程；

b） 应针对物理环境、终端设备、软件系统、网络设施等对象，在服务及运维等过程采取多样安全防护技术，建设立体化防护体系；

c） 应加强标识解析注册与服务机构的认证和管理，做好解析节点授权管理及标识资源使用，利用云计算、大数据等新手段实现数据资源共享、机构高效协同、责任边界明确的标识解析服务协作机制；

d） 应对每个用户账号的操作、行为、标识资源使用情况、系统重要安全事件进行审计，留存记录并加以保护；

e） 应在标识解析系统运营维护、配置和补丁管理、系统升级、主机登录、标识解析服务资源访问等过程中使用身份认证管理；

f） 应对关键设备、系统和平台的访问采用多因素认证；

g） 应对所有的通信会话提供真实性保护，防止中间人攻击、会话劫持；

h） 应依据安全策略控制业务用户、管理用户对系统文件、数据库、标识资源等客体的访问，对重要信息资源设置敏感标记，并依据安全策略控制用户对有敏感标记重要信息资源的操作，实现规范化的技术应用、体系化的运营管理、立体化的安全保障。

9 平台安全

9.1 边缘层安全防护要求

9.1.1 网络架构

网络架构要求如下：

a） 应设置单独的接入安全区域，并分配已规划的地址空间；

b） 避免接入设备与重要信息系统直接互连，可通过信息交换系统或者共享系统来进行数据的交互。

9.1.2 传输保护

传输保护要求如下：

a） 应能够对非授权设备的接入行为进行告警和阻断；

b） 对于有线和无线接入，应确保通过受控的边界防护设备或者其上的指定端口接入网络。

9.1.3 边界防护

边界防护要求如下：

a） 工厂内部网络与工厂外部网络的边界应该具有隔离措施；

b） 应能够对非授权设备的接入行为进行告警和阻断。

c） 对于有线和无线接入，应确保通过受控的边界防护设备或者其上的指定端口接入网络。

9.1.4 访问控制

访问控制要求如下：

a） 应确保接入网络边界网关只开放接入服务相关的端口；

b） 应确保边界安全网关通过ACL检测机制对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据进出；

c） 应对接入网络数据进行深度包检测；

d） 应采用白名单控制方式，只允许合法设备接入网络；

e） 应采用IP-MAC绑定、802.1x、证书、标识码等技术对接入的PC机、便携机、智能终端等设备进行注册认证；

f） 终端接入后，应限制该终端的访问权限，并限制其他设备与该终端的非授权通信；

g） 在一个非活动时间周期后，应通过自动方式或者手动方式终止用户远程连接。

9.1.5 入侵防范

入侵防范要求如下：

a） 应能够检测接入设备发起的DDoS等网络攻击行为；

b） 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间在发生严重入侵事件时应能够告警；

c） 应能够对未知威胁进行分析和防范。

9.1.6 安全审计

安全审计要求如下：

a） 应对接入用户的重要安全事件和重要行为进行审计；

b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d） 审计日志应符合相关法律法规要求；

e） 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。

9.2 平台 IaaS 层安全防护要求

9.2.1 服务器安全防护要求

9.2.1.1 身份鉴别认证

身份鉴别认证要求如下：

a） 应对登录服务器的用户进行身份标识和鉴别；

b） 服务器管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

c） 应启用登录失败处理功能，可采取结束会话、限制非法登陆次数和自动退出等措施；

d） 应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用；

e） 当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃取。

9.2.1.2 访问控制

访问控制要求如下：

a） 应采用技术措施对允许访问服务器的终端地址范围进行限制；

b） 应关闭服务器不使用的端口，防止非法访问；

c） 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

9.2.1.3 安全审计

安全审计要求如下：

a） 审计范围应覆盖到服务器上的每个用户；

b） 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等重要的安全相关事件；

c） 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d） 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等；

e） 应支持按用户需求提供与其相关的审计信息及审计分析报告；

f） 应能够根据记录数据进行分析，并生成审计报表；

g） 应保护审计进程，避免受到未预期的中断；

h） 应能汇聚服务范围内的审计数据，支持第三方审计。

9.2.1.4 资源控制

资源控制要求如下：

a） 应根据安全策略，设置登录终端的会话数量；

b） 应根据安全策略设置登录终端的操作超时锁定；

c） 应对重要服务器进行性能监测，包括服务器的CPU、硬盘、内存、网络等资源的使用情况，发现异常情况提供告警，并进行相应处置。

9.2.1.5 恶意代码防范

恶意代码防范要求如下：

a） 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

b） 应支持对防恶意代码的统一管理。

9.2.1.6 入侵防范

入侵防范要求如下：

a） 所使用的操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新；

b） 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

c） 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

9.2.2 虚拟化安全防护要求

9.2.2.1 虚拟机安全

虚拟机安全要求如下：

a） 应支持虚拟机之间、虚拟机与宿主机之间的隔离；

b） 应支持虚拟机部署防病毒软件；

c） 应具有对虚拟机恶意攻击等行为的识别并处置的能力；

d） 应支持对虚拟机脆弱性进行检测的能力；

e） 应保证虚拟机迁移过程中数据和内存的安全可靠，保证迁入虚拟机的完整性和迁移前后安全配置环境的一致性；

f） 应确保虚拟机操作系统的完整性，确保虚拟机操作系统不被篡改，且确保虚拟机实现安全启动；

g） 应对虚拟机镜像文件进行完整性校验，确保虚拟机镜像不被篡改；

h） 应提供最新版本的虚拟机镜像和补丁版本；

i） 应支持发现虚拟机操作系统漏洞的能力，支持漏洞修复。

9.2.2.2 虚拟网络安全

虚拟机安全要求如下：

a） 应部署一定的访问控制安全策略，以实现虚拟机之间、虚拟机与虚拟机管理平台之间、虚拟机与外部网络之间的安全访问控制；

b） 应支持采用VLAN或者分布式虚拟交换机等技术，以实现网络的安全隔离；

c） 应支持不同租户之间的网络隔离；

d） 应支持对虚拟网络的逻辑隔离，在虚拟网络边界处实施访问控制策略；

e） 应对虚拟机网络出口带宽进行限制；

f） 可支持用户选择使用第三方安全产品。

9.2.2.3 虚拟化平台安全

虚拟机安全要求如下：

a） 应保证每个虚拟机能获得相对独立的物理资源，并能屏蔽虚拟资源故障，确保某个虚拟机崩溃后不影响虚拟机监控器及其他虚拟机；

b） 应保证不同虚拟机之间的虚拟CPU指令隔离；

c） 应保证不同虚拟机之间的内存隔离，内存被释放或再分配给其他虚拟机前得到完全释放；

d） 应保证虚拟机只能访问分配给该虚拟机的存储空间（包括内存空间和磁盘空间）；

e） 应对虚拟机的运行状态、资源占用等信息进行监控；

f） 应支持发现虚拟化平台漏洞的能力，支持漏洞修复。

9.3 平台 PaaS 层安全防护要求

9.3.1 数据分析服务安全防护要求

9.3.1.1 数据挖掘

数据挖掘安全要求如下：

a） 针对不同接入方式的数据挖掘用户，应采用不同的认证方式。需要检查使用数据的合法性和有效性；

b） 挖掘算法在使用前，必须申报算法使用的数据范围、挖掘周期、挖掘目的、以及挖掘结果的应用范围等内容。算法提供者必须对算法的安全性和可靠性提供必要的验证与测试方案；

c） 在数据挖掘过程中，应对挖掘算法使用的数据范围、数据状态、数据格式、数据内容等进行监控；

d） 挖掘算法不应对数据存储区域内的原始数据进行增加、修改、删除等操作，以保证原始数据的可用性和完整性；

e） 不应将挖掘算法产生的中间过程数据与原始数据存储于同一空间，以防数据使用的混乱、加大数据存储的管理难度。同时，应周期性的检查用户操作数据的情况，统一管理数据使用权限；

f） 不同应用之间应进行数据关联性隔离，防止不同应用之间的 ECA 分析产生数据泄露；

g） 应对挖掘内容、过程、结果、用户进行安全审计。主要包括挖掘内容的合理性、挖掘过程的合规性、挖掘结果的可用性，以及挖掘用户的安全性；

h） 应对源数据和挖掘结果进行签识，防止数据被恶意删除、随意篡改、无约束的滥用；

i） 如需将收集到的信息共享给第三方应用，应对信息进行脱敏处理，严格保护用户隐私不被泄露。

9.3.1.2 数据输出

数据输出安全要求如下：

a） 应对应用数据的各种操作行为、操作结果予以完整记录，确保操作行为的可追溯；

b） 应对所有输出的数据内容都进行合规性审计，审计范围包括数据的真实性、一致性、完整性、归属权、使用范围等；

c） 应对数据输出的接口进行规范管理，管理内容包括数据输出接口类型加密方式、传输周期、使用用途、认证方式等；

d） 如需将数据输出到平台以外的实体时，在输出前应对数据进行脱敏操作，确保输出的数据满足约定的要求且不泄露敏感信息；

e） 应对所有审计行为留有记录并独立存储，严禁在任何情况下开放对审计结果的修改与删除权限。

9.3.2 微服务组件安全防护要求

9.3.2.1 身份鉴别

身份鉴别要求如下：

a） 应对管理微服务组件的用户进行身份标识和鉴别；

b） 管理微服务组件的用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

c） 应启用登录失败处理功能，可采取结束会话、限制非法登陆次数和自动退出等措施；

d） 应采用安全方式防止用户鉴别认证信息泄露而造成身份冒用；

9.3.2.2 访问控制

在微服务组件权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

9.3.2.3 安全审计

安全审计要求如下：

a） 审计范围应覆盖到使用微服务组件的每个用户；

b） 审计内容应包括重要用户行为、微服务组件资源的异常使用和重要操作命令的使用等重要的安全相关事件；

c） 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d） 保护审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等；

e） 应支持按用户需求提供与其相关的审计信息及审计分析报告。

9.3.2.4 开放接口

开放接口要求如下：

a） 微服务组件应有与外部组件或应用之间开放接口的安全管控措施，接口协议操作应通过接口代码审计、黑、白名单等控制措施确保交互符合接口规范；

b） 应对开放接口调用有认证措施；

c） 应对关键接口的调用情况进行技术监控，如调用频率、调用来源等；

d） 应用开放接口生成的业务应用或应用程序在供用户下载之前应通过安全检测；

e） 应制定开放接口管理机制和网络安全应急管理制度。

9.3.3 平台应用开发环境安全防护要求

9.3.3.1 身份鉴别

身份鉴别要求如下：

a） 对保留用户个人信息或用户服务信息的业务，应对登录用户进行身份标识和鉴别；

b） 对要求提供登录功能的开发环境，应提供并启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

c） 对要求提供登录功能的开发环境，应提供并启用用户身份标识唯一检查功能，保证开发环境中不存在重复用户身份标识。应提供并启用用户鉴别信息复杂度检查功能，保证身份鉴别信息不易被冒用；

d） 应采用加密方式存储用户的账号和口令信息；

e） 需要登录访问的开发环境，应对用户访问和操作的有关环节（如注册、登录操作、管理、浏览等）提供有效的保护措施（如对用户注册口令进行强度检查用户检测和账号保护、以图形验证码保护各类提交信息、对用户重要操作进行确认和验证、授权访问页面使用安全连接等）。

9.3.3.2 访问控制

访问控制要求如下：

a） 应由授权主体配置访问控制策略，并严格限制默认用户的访问权限；

b） 应严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

9.3.3.3 安全审计

安全审计要求如下：

a） 审计范围应覆盖到每个用户的关键操作；

b） 审计内容应包括对用户的重要行为、资源使用情况等重要事件；

c） 应保护审计记录，保证无法删除、修改或覆盖等；

d） 相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等，并且根据相关法律法规要求保留一定期限。

9.3.3.4 资源控制

资源控制要求如下：

a） 当用户和开发环境的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b） 应根据需要对用户与开发环境之间相关通信过程中的全部报文或整个会话过程提供必要的保护（如进行通信数据加密），并提供对相关访问、通信等数据的防抵赖功能；

c） 应定义服务水平阈值，能够对服务水平进行监测，并具备当服务水平降低到预先规定的阀值时进行告警的功能。

9.3.3.5 信息保护

信息保护要求如下：

a） 开发环境中各功能的提供、控制与管理过程应保护用户隐私，未经用户同意，不能擅自收集、修改、泄漏用户相关敏感信息；

b） 应保护相关信息的安全，避免相关数据和页面被篡改和破坏；

c） 不应有不必要的内嵌网络服务，不应在用户端自动安装恶意软件和插件；

d） 应对通信过程中的敏感信息字段进行加密；

e） 应对敏感信息（如用户信息、订单信息、应用软件下载路径等）进行加密存储；

f） 应对开发环境相关功能的关键数据（如业务数据、系统配置数据、管理员操作维护记录、用户信息、业务应用与应用程序购买、下载信息等）应有必要的容灾各份；

g） 应能对诈骗、虚假广告等信息建立处理机制，防止类似信息的扩散；

h） 与开发环境中的重要功能相关的数据应进行异址备份；

i） 开发环境应提供数据自动保护功能，当发生故障后应保证开发环境能够恢复到故障前的业务状态。

9.3.3.6 恶意代码防范

应提供有效的恶意代码检测和过滤技术手段，对开发环境向用户提供的各类信息（如用户发布和上传的文件、资源站点可供下载的立件、即时通信用户间传送的文件、电子邮件附件）进行必要的安全检查和过滤。

9.3.3.7 上线前检测

上线前检测要求如下：

a） 开发环境应在业务应用与工业应用程序上线前对其进行安全审核，以确保其不包含恶意代码、恶意行为等，经过安全审核后才能进行上线处理正式发布；

b） 开发环境可提供用户数据同步功能，但开发环境同步的用户数据不应保存在位于境外的服务器上；

c） 开发环境应支持对工业应用程序的移动代码签名机制，对应用程序检测审核后，对其进行数字签名。移动终端在下载安装工业应用程序之前，对经过签名的应用程序进行签名验证，只有通过签名验证的应用程序才能被认为是可信的，继而被安装到终端上；

d） 开发环境应对已经上线的业务应用与工业应用程序进行拨测抽查，并记录拨测过程及结果，针对违规行为、可疑行为等进行相应的处理。业务应用与工业应用程序拨测应采用自动拨测与人工拨测相结合的方式进行；

e） 开发环境应要求开发者在提交业务应用与工业应用程序时声明其调用的API，并对业务应用与工业应用程序调用终端API的行为进行检测。业务应用与工业应用程序不应调用与其业务功能无关的API以及在其声明范围之外的API；

f） 业务应用与工业应用程序在上线前或升级后应进行代码审计，形成报告，并对审计出的问题进行代码升级完善；

g） 业务应用与工业应用程序应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考CVE、CNVD等）。

9.4 平台 SaaS 层安全防护要求

9.4.1 业务应用安全防护要求

9.4.1.1 身份鉴别

身份鉴别要求如下：

a） 应采用一种或一种以上组合的鉴别技术来进行身份鉴别；

b） 应采用两种或两种以上组合的鉴别技术来进行身份鉴别，并保证一种身份鉴别机制是不易伪造的；

c） 应具备防范暴力破解等攻击的能力。

9.4.1.2 访问控制

访问控制要求如下：

a） 应严格限制用户的访问权限，按安全策略要求控制用户对业务应用的访问；

b） 应严格限制应用与应用之间相互调用的权限，按照安全策略要求控制应用对其他应用里用户数据或特权指令等资源的调用。

9.4.1.3 安全审计

安全审计要求如下：

a） 审计范围应覆盖到用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件；

b） 应对审计记录进行保护，有效期内避免受到非授权的访问、篡改、覆盖或删除等；

c） 应定期针对审计日志进行人工审计；

d） 应支持按用户需求提供与其相关的审计信息及审计分析报告；

e） 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能；

f） 应具备自动化审计功能，监控明显异常操作并响应；

g） 应能汇聚服务范围内的审计数据，支持第三方审计。

9.4.1.4 资源控制

资源控制要求如下：

a） 应限制对应用访问的最大并发会话连接数等资源配额；

b） 应提供资源控制不当的报警及响应；

c） 应在会话处于非活跃一定时间或会话结束后终止会话连接。

9.4.2 工业应用程序安全防护要求

9.4.2.1 逻辑安全

9.4.2.1.1 身份鉴别

身份鉴别要求如下：

a） 应提供专门的登录控制模块对登录用户进行身份标识和鉴别，并保证用户身份标识的唯一性；

b） 应提供并启用用户登录口令复杂度检查功能，保证身份信息不易被冒用；

c） 应提供并启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d） 应采用加密方式存储用户的登录口令信息；

e） 登录验证模块应能防止身份鉴别暴力攻击（如登录模块应采用随机验证码进行验证，并且保证验证码不易被自动预测、识别）；

f） 加强密码复杂度要求，应不含有常用字符组合、数字组合、键盘顺序等可预测密码组合；

g） 应采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

9.4.2.1.2 访问控制

访问控制要求如下：

a） 应由经过授权的主体配置访问控制策略，严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问；

b） 应严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击措施的能力（如限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定）；

c） 当进行业务权限更改时（如密码重置、密码找回等），应设置相关策略，防止暴力破解攻击；

d） 业务订购、变更、退订流程应根据实际业务需求，应采用“认证码”或“二次短信认证”等方式加强安全性，应限定同一用户每日业务订购次数；

e） 工业应用程序管理后台不应暴露在公网，管理接口通信内容不应使用明文协议。

9.4.2.1.3 安全审计

安全审计要求如下：

a） 审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件（如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作）；

b） 应保护审计记录，保证无法删除、修改或覆盖等；

c） 业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等；

d） 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能。

9.4.2.1.4 其他要求

其他要求如下：

a） 当工业应用程序和平台服务的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b） 应能对含有恶意代码链接的信息建立发现和处理机制，防止类似信息的扩散；

c） 工业应用程序运行时，未经用户同意，不得擅自为用户自动开启其他服务功能（如定位等）；

d） 应定义服务水平阈值，能够对服务水平进行检测，并具备当服务水平降低到预先规定的阙值时进行告警的功能；

e） 应保证工业应用程序中使用的第三方软件、运维软件无已知后门、漏洞；

f） 应提供有效的病毒和攻击检测过滤技术手段，能够对用户之间传送的文件进行必要的安全检查和过滤。

9.4.2.2 原生应用及后台系统安全

9.4.2.2.1 输入验证

应对输入数据做严格验证，默认所有输入都可能包含恶意信息。

9.4.2.2.2 身份认证

身份认证要求如下：

a） 应确保身份认证模块不能被非法绕过；

b） 软件的用户身份鉴别模块应对用户身份鉴别信息进行保护，防止泄露。

9.4.2.2.3 会话管理

应采取会话保护措施保障工业应用程序与平台服务之间的会话不可被窃听、篡改、伪造、重放等。

9.4.2.2.4 数据存储

应确保工业应用程序配置信息、用户认证信息等敏感数据采用加密方式存储。

9.4.2.2.5 日志记录

日志记录要求如下：

a） 后台日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件（如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作）；

b） 不应在后台以及客户端日志中记录用户登录口令等敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理；

c） 应防止日志欺骗，如果在生成后台日志时需要引入来自非受信源的数据则需要进行严格校验，防止日志欺骗攻击；

d） 应确保后台日志数据的安全存储并严格限制日志数据的访问权限，可对后台日志记录进行签名来实现防篡改。

9.4.2.2.6 其他要求

其他要求如下：

a） 工业应用程序不应含有移动互联网恶意程序。移动互联网恶意程序的判定依据见YD/T 2439-2012的相关要求；

b） 应确保软件内存管理不存在逻辑缺陷，如未释放资源、敏感信息驻留内存等；

c） 应确保软件不非法操作与自身功能不相关的文件（如图片、通信录、其他应用软件等）；

d） 客户端软件应进行代码变量隐藏。

9.4.2.3 Web 应用及后台系统安全

9.4.2.3.1 输入验证

输入验证要求如下：

a） 应对输入数据（如文件路径、URL地址等）做安全验证，默认所有输入都可能包含恶意信息，并尽量使用白名单验证方法；

b） 应在服务器端进行输入验证，避免客户端输入验证被绕过；

c） 关键参数应直接从服务器端提取，避免从客户端输入，防止关键参数被篡改。

9.4.2.3.2 身份认证

身份认证要求如下：

a） 不应明文传输用户密码，可采用SSL/TLS加密隧道确保用户密码的传输安全；

b） 不应在数据库或文件系统中明文存储用户密码，可采用单向散列值在数据库中存储用户密码，降低存储的用户密码被字典攻击的风险；

c） 不应在COOKIE中保存明文用户密码；

d） 不应采取措施防止暴力破解、恶意注册、恶意占用资源等行为；

e） 应对关键业务操作进行二次鉴权，例如修改用户认证鉴权信息（如密码、密码取回问题及答案、绑定手机号码等），避免用户身份被冒用；

f） 应避免认证错误提示泄露信息，在认证失败时，应向用户提供通用的错误提示信息（如不应区分是账号错误还是密码错误），避免这些错误提示信息被攻击者利用；

g） 应支持密码策略设置，从业务系统层面支持强制的密码策略，包括密码长度、复杂度、更换周期等，特别是业务系统的管理员密码；

h） 应支持账号锁定功能，系统应限制连续登录失败次数，在客户端多次尝试失败后，服务器端需要对用户账号进行短时锁定，且锁定策略支持配置解锁时长；

i） 应确保用户不能访问到未授权的功能和数据，未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权。

9.4.2.3.3 会话管理

会话管理要求如下：

a） 应确保会话的安全创建。在用户认证成功后，应为用户创建新的会话并释放原有会话；创建的会话标识应满足随机性和长度要求，避免被攻击者猜测；会话与IP地址可绑定，降低会话被盗用的风险；

b） 应确保会话数据的存储安全。用户登录成功后所生成的会话数据应存储在服务器端，并确保会话数据不能被非法访问:当更新会话数据时，要对数据进行严格的输入验证，避免会话数据被非法篡改；

c） 应确保会话数据的传输安全，防止泄露会话标识；

d） 应确保会话的安全终止。当用户登录成功并成功创建会话后，应在Web应用系统的各个页面提供用户登出功能，登出时应及时删除服务器端的会话数据；当处于登录状态的用户直接关闭浏览器时，需要提示用户执行安全登出或者自动为用户完成登出过程，从而安全的终止本次会话；

e） 应设置合理的会话超时阈值，在合理范围内尽可能减小会话超时阈值，可以降低会话被劫持和重复攻击的风险，超过会话超时阈值后立刻销毁会话，清除会话的信息；

f） 应限制会话并发连接数，限制同一用户的会话并发连接数，避免恶意用户创建多个并发的会话来消耗系统资源，影响业务的可用性；

g） 在涉及到关键业务操作的Web页面，应为当前Web页面生成一次性随机令牌，作为主会话标识的补充。在执行关键业务前，应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配，以避免跨站请求伪造等攻击。

9.4.2.3.4 数据存储

数据存储要求如下：

a） 对于不同类别的数据，比如日志记录和业务数据，应采取相应的隔离措施和安全保护措施。

b） 不应在客户端本地存储用户敏感数据，如用户密码、身份信息等。

c） 应避免在代码中硬编码密码(即在代码中直接嵌入密码，会导致密码修改困难，甚至密码的泄露)，可从配置文件载入密码。

d） 在配置文件中不应明文存储数据库连接密码、FTP服务密码、主机密码外部系统接口认证密码等。

9.4.2.3.5 数据传输

应确保通信信道的安全，在客户端与Web服务器之间使用并正确配置SSL/TLS，应使用SSL3.0/TLS1.0以上版本，对称加密密钥长度不少于128位非对称加密密钥长度不少于1024位，单向散列值位数不小于128位。

9.4.2.3.6 日志记录

日志记录要求如下：

a） 后台日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件，如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作；

b） 不应在后台日志中记录用户密码等敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理；

c） 应防止日志欺骗，如果在生成后台日志时需要引入来自非受信源的数据则需要进行严格校验，防止日志欺骗攻击；

d） 不应将后台日志保存到Web目录下，确保日志数据的安全存储并严格限制日志数据的访问权限，可对日志记录进行签名来实现防篡改。

9.4.2.3.7 其他要求

其他要求如下：

a） 应有技术手段检测和避免 Web 业务系统域名、访问链路的异常、访问延迟、解析错误等情况，并有应急处理能力；

b） 应避免存在常见的Web漏洞（如SQL注入、跨站脚本、跨站请求伪造等）；

c） 应能检测挂马、暗链等 Web 业务系统入侵事件，并有应急处理能力。

10 数据安全

10.1 数据保密性保护

数据保密性保护要求如下：

a） 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

b） 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

c） 应使用密码技术确保工业互联网平台迁移过程中，重要数据的保密性，防止在迁移过程中的重要数据泄露。

10.2 数据完整性保护

数据完整性保护要求如下：

a） 应采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

b） 应采用校验码技术或密码技术保证重要数据在存储过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

c） 应使用校验码或密码技术确保工业互联网平台迁移过程中，重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。

10.3 访问控制

访问控制要求如下：

a） 应结合工业互联网业务用户的角色与数据敏感程度的不同确定针对特定数据的访问控制级别:

b） 应使用订阅/分发模式实现特定来源数据的访问控制。

10.4 数据抗抵赖

在工业互联网平台及可能涉及法律责任认定的工业应用程序中,应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

10.5 数据备份恢复

数据备份恢复要求如下：

a） 工业互联网平台应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

b） 工业互联网平台应提供重要数据处理系统的热冗余，保证系统的高可用性；

c） 应保证不同工业互联网平台用户的审计数据隔离存放；

d） 应为工业互联网平台用户将业务系统及数据迁移到其他平台和本地系统提供技术手段，并协助完成迁移过程；

e） 工业互联网平台运营商的数据存储服务应确保平台用户数据存在若干个可用的副本，各副本之间的内容应保持一致；

f） 工业互联网平台应建立异地灾难备份中心，提供业务应用的实时切换。

10.6 数据销毁

数据销毁要求如下：

a） 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除；

b） 工业互联网平台应提供基于数据分类分级的数据销毁机制，并明确销毁方式和销毁要求。

10.7 数据溯源

数据溯源要求如下：

a） 应跟踪和记录数据采集、处理、分析和挖掘等过程，确保溯源数据能重现相应过程；

b） 溯源数据应能支撑数据业务要求和合规审计要求；

c） 应采用技术手段保证溯源数据真实性和保密性。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[2] GB/T 23031.2-2023 工业互联网平台 应用实施指南 第2部分：数字化管理

[3] GB/T 23031.3-2023 工业互联网平台 应用实施指南 第3部分：智能化制造

[4] GB/T 23031.4-2023 工业互联网平台 应用实施指南 第4部分：网络化协同

[5] GB/T 23031.5-2023 工业互联网平台 应用实施指南 第5部分：个性化定制

[6] GB/T 23031.6-2023 工业互联网平台 应用实施指南 第6部分：服务化延伸

[7] YD/T 3865-2021 工业互联网数据安全保护要求