ICS 35.030
CCS M 10

中华人民共和国国家标准

GB/T 44462.3—2024

工业互联网企业网络安全 第3部分：标识解析企业防护要求

Industrial internet enterprise cybersecurity—Part 3：Protection requirements of industrial internet identification resolution enterprise

2024-09-29 发布　　2025-01-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　工业互联网标识解析企业安全防护级别的确定 …… 2
6　工业互联网标识解析企业安全防护范围 …… 2
7　工业互联网标识解析企业安全防护要求 …… 3
7.1　初始级防护要求 …… 3
7.2　基本级防护要求 …… 7
7.3　增强级防护要求 …… 13
附录 A（资料性）　工业互联网标识解析企业安全防护范围示意图 …… 20
参考文献 …… 21

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。

本文件是GB/T 44462《工业互联网企业网络安全》的第3部分。GB/T 44462已经发布了以下部分：

——第1部分：应用工业互联网的工业企业防护要求；

——第2部分：平台企业防护要求；

——第3部分：标识解析企业防护要求。

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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC 485)和全国网络安全标准化技术委员会(SAC/TC 260)共同归口。

本文件起草单位：中国信息通信研究院、国家工业信息安全发展研究中心、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、中国电子技术标准化研究院、中国工业互联网研究院、北京航空航天大学、广东鑫兴科技有限公司、江苏中天互联科技有限公司、北京天融信网络安全技术有限公司、北京启明星辰信息安全技术有限公司、北京东方通网信科技有限公司、郑州信大捷安信息技术股份有限公司、亚信科技(成都)有限公司、中通服咨询设计研究院有限公司、北京神州绿盟科技有限公司、南京中新赛克科技有限责任公司、中移物联网有限公司、国能大渡河大数据服务有限公司、国网河南省电力公司、华北计算机系统工程研究所(中国电子信息产业集团有限公司第六研究所)、中国电信股份有限公司北京研究院、北京信安世纪科技股份有限公司、奇安信科技集团股份有限公司、国网电商科技有限公司、青岛海信通信有限公司、中国船级社、长扬科技(北京)股份有限公司。

本文件主要起草人：魏亮、赵爽、董悦、张倩、柯皓仁、李艺、于广琛、马娟、张瑜、区景安、汪毅、时宗胜、渠立孝、李俊、孙军、余果、马霄、安高峰、刘为华、吴锦涛、唐刚、张嘉欢、崔婷婷、糜靖峰、汤永田、赵梓桐、查奇文、洪晟、刘超、高丽芬、叶建伟、王雷、涂扬举、贺玉彬、党芳芳、李帅、霍朝宾、付军、崔君荣、靳晓雨、张学杰、张煜、张亚京、刘伟。

引　言

工业互联网企业数量众多、信息化发展程度不同且承载业务类型相异，所属行业网络安全防护需求差异化明显，为解决现有网络安全防护要求无法满足工业互联网企业发展实际需求的问题，需实施工业互联网企业网络安全分类分级管理并编制相关标准。

GB/T 44462《工业互联网企业网络安全》是指导工业互联网企业开展网络安全分类分级防护工作的基础性标准，旨在针对应用工业互联网的工业企业、工业互联网平台企业、工业互联网标识解析企业及企业数据安全，提出不同级别的网络安全管理及安全防护技术要求，用于指导企业落实与自身级别相适应的安全防护措施，由于文件的使用者需求不同，由四个部分构成。

——第1部分：应用工业互联网的工业企业防护要求。目的在于提出应用工业互联网的工业企业开展网络安全分类分级防护工作需要落实的安全要求。

——第2部分：平台企业防护要求。目的在于提出工业互联网平台企业开展网络安全分类分级防护工作需要落实的安全要求。

——第3部分：标识解析企业防护要求。目的在于提出工业互联网标识解析企业开展网络安全分类分级防护工作需要落实的安全要求。

——第4部分：数据防护要求。目的在于提出工业互联网企业开展网络安全分类分级防护工作需要落实的数据安全要求。

本文件面向工业互联网标识解析企业，提出了不同级别安全防护要求，指导企业实施工业互联网安全分类分级管理工作，为工业互联网标识解析企业建设、运营及提升节点安全防护能力奠定基础，提升工业互联网安全保障能力。

工业互联网企业网络安全
第3部分:标识解析企业防护要求

1 范围

本文件规定了工业互联网标识解析企业在设备和系统、网络、业务和应用、管理以及物理环境等方面不同级别的网络安全防护要求。

本文件适用于指导工业互联网标识解析企业开展网络安全分类分级防护工作。

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 信息安全技术 术语

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 42021 工业互联网 总体网络架构

GB 50174 数据中心设计规范

3 术语和定义

GB/T 25069 和 GB/T 42021 界定的以及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

工业互联网标识 industrial internet identification

工业互联网中使用的用于唯一识别和定位物理对象或数字对象及其关联信息的字符串。

3.3

标识解析 identification resolution

将标识翻译成与其相关联的信息的过程。

[来源:GB/T 33745—2017,2.4.3,有修改]

3.4

工业互联网标识解析系统 industrial internet identification resolution system

承载工业互联网标识解析服务的信息系统。

3.5

工业互联网标识解析企业 industrial internet identification resolution enterprise

工业互联网标识解析根节点运行机构、国家顶级节点运行机构、标识注册服务机构、递归节点运行

机构等提供工业互联网标识服务的机构。

4 缩略语

下列缩略语适用于本文件。

DDoS:分布式拒绝服务(Distributed Denial of Service)

DNS:域名系统(Domain Name System)

IP:互联网协议(Internet Protocol)

NTP:网络时间协议(Network Time Protocol)

VPN:虚拟专用网络(Virtual Private Network)

5 工业互联网标识解析企业安全防护级别的确定

工业互联网标识解析企业应按照工业互联网企业网络安全定级方法划分级别,由低到高划分为一级、二级、三级,采取不同程度的安全防护。工业互联网标识解析企业的安全防护要求分为初始级防护、基本级防护和增强级防护三个级别,如表1所示,其中:

——一级工业互联网标识解析企业应采取初始级防护措施;

——二级工业互联网标识解析企业应采取基本级防护措施;

——三级工业互联网标识解析企业应采取增强级防护措施。

表1 工业互联网标识解析企业安全防护级别的确定

企业级别	安全防护要求级别
一级	初始级
二级	基本级
三级	增强级

6 工业互联网标识解析企业安全防护范围

工业互联网标识解析企业安全防护范围从设备和系统安全、网络安全、业务和应用安全、安全管理以及物理环境安全要求等方面展开,参见附录A。具体内容包括:

a) 设备和系统安全防护:包括身份鉴别、访问控制、恶意代码防范、入侵防范、安全审计、设备冗余等;

注:设备和系统包括主机/服务器、网络设备、安全设备、终端等硬件及其所包含的底层系统软件,如操作系统、数据库等。

b) 网络安全防护:包括架构安全、访问控制、安全监测、入侵防范、安全审计等;

c) 业务和应用安全防护:包括身份认证与访问控制、应用资源控制、入侵防范、安全审计、业务提供安全等;

d) 安全管理:包括机构管理、制度管理、人员管理、建设管理、运维管理等;

e) 物理环境安全:包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等。

7 工业互联网标识解析企业安全防护要求

7.1 初始级防护要求

7.1.1 设备和系统安全防护要求

7.1.1.1 身份鉴别

本项要求包括：

a) 应对登录用户进行身份标识和鉴别，身份标识具有唯一性；

b) 口令等身份鉴别信息应有复杂度要求，并定期更换；

c) 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登录连接超时自动退出等相关措施。

7.1.1.2 访问控制

本项要求包括：

a) 应为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) 应定期删除或停用多余的、过期的账户，避免共享账户的存在。

7.1.1.3 恶意代码防范

本项要求包括：

应具备恶意代码防范能力并对恶意代码库进行维护和及时更新。

7.1.1.4 入侵防范

本项要求包括：

a) 操作系统、数据库等应遵循最小安装的原则，仅安装标识解析系统相关设备需要的组件和应用程序；

b) 应关闭不需要的系统服务、默认共享和高危端口，包括不限于标识解析服务器应限制只在解析端口上提供标识解析服务，不对其他用户终端开放任何服务。

7.1.2 网络安全防护要求

7.1.2.1 架构安全

本项要求包括：

标识解析系统内部网络应根据安全需求和业务特点划分为不同的安全域，按照统一的管理和控制原则划分不同的子网或网段，设备依照功能划分及其重要性等因素分区部署。

7.1.2.2 访问控制

本项要求包括：

应在网络边界部署网络流量访问控制设备，并启用访问控制功能，保证跨越网络边界的访问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。

7.1.2.3 安全监测

本项要求包括：

应对网络流量信息等进行监测，发生异常访问、异常流量等进行告警并进行相应处置。

7.1.2.4 入侵防范

本项要求包括：

a) 应对进出标识解析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；

b) 应对病毒和恶意软件入侵进行防护。

7.1.3 业务和应用安全防护要求

7.1.3.1 身份认证与访问控制

本项要求包括：

a) 应对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) 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登录连接超时自动退出等相关措施；

c) 应重命名或删除默认账户，修改默认账户的默认登录口令；

d) 应定期删除或停用多余的、过期的账户。

7.1.3.2 应用资源控制

本项要求包括：

应支持对应用的最大并发会话连接数进行限制。

7.1.3.3 入侵防范

本项要求包括：

应定期（至少每月一次）检查标识解析系统及标识应用软件版本等，对软件版本漏洞进行扫描评估，对存在严重漏洞的软件进行更新。

7.1.3.4 业务提供安全

本项要求包括：

标识解析服务器不应提供除了标识查询及解析服务之外的其他服务。

7.1.4 安全管理要求

7.1.4.1 机构管理

本项要求包括：

应设立安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位。

7.1.4.2 制度管理

本项要求包括：

应制定安全工作的总体方针和安全策略，建立适合机构安全工作实际情况的安全管理制度。

7.1.4.3 人员管理

本项要求包括：

a） 应指定或授权特定的部门或人员负责人员录用；
b） 应及时终止离岗员工的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

7.1.4.4 建设管理

7.1.4.4.1 定级

本项要求包括：
a） 应明确本企业的安全等级；
b） 应以书面形式说明企业确定为某安全等级的方法和理由。

7.1.4.4.2 安全方案设计

本项要求包括：
a） 应按照企业等级情况，选择对应级别安全措施，依据风险分析的结果补充和调整安全措施；
b） 应根据安全防护对象的安全防护需求进行安全方案设计。

7.1.4.4.3 产品采购和使用

本项要求包括：
a） 网络关键设备及网络安全产品的采购和使用应符合国家有关规定；
b） 密码产品与服务的采购和使用应符合国家密码管理主管部门的要求。

7.1.4.4.4 软件开发

本项要求包括：
a） 应要求开发单位提供软件设计文档、使用指南及第三方专业机构出具的软件安全性检测报告；
b） 应要求开发单位在软件交付前进行安全性测试，测试内容至少包括恶意代码检测。

7.1.4.4.5 系统交付

本项要求包括：
a） 应在软件交付前进行缺陷和恶意代码等安全检测；
b） 应制定安全性测试验收方案，并依据测试验收方案实施验收，形成验收报告；
c） 应根据交付清单对所交接的设备、软件和文档等进行清点；
d） 应要求开发单位对负责运行维护的技术人员进行相应的技能培训。

7.1.4.4.6 供应链安全

本项要求包括：
a） 应选择安全合规的设备、服务、系统及软件供应商，其所提供的设备、平台系统等应为其所承载的业务提供相应的安全防护能力；
b） 应在服务协议中规定具体服务内容和技术指标；
c） 应在服务协议中规定供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
d） 应与选定的供应商签署保密协议，要求其不应泄露客户数据和业务系统的相关重要信息；
e） 应与选定的供应商签订相关协议，明确供应链各方需履行的安全相关义务。

7.1.4.5 运维管理

7.1.4.5.1 环境管理

本项要求包括：

应对机房的安全管理做出规定，指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。

7.1.4.5.2 资产管理

本项要求包括：

a) 应清晰地识别标识解析相关业务所涉及的资产，编制并维护核心资产清单。清单中应包括所有为从灾难中恢复而需要的资产，相关的资产可能包括：信息资产、软件资产、物理资产、服务、人员、无形资产等；

b) 信息和资产均应指定部门和人员承担责任，资产责任人应确保介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。

7.1.4.5.3 密码管理

本项要求包括：

a) 使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，密码产品应经检测认证合格；

b) 应根据 GB/T 39786 中密码应用基本要求等级，企业涉及的相关业务系统的管理者可根据业务实际情况选择相应级别的密码保障技术能力及管理能力。

7.1.4.5.4 配置管理

本项要求包括：

应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

7.1.4.5.5 连续性管理

本项要求包括：

应为标识解析系统制定解析服务连续性管理的过程，识别可能引起解析服务中断的事态以及这种事态发生的概率。

7.1.4.5.6 安全事件及应急处置

本项要求包括：

a) 应建立网络安全监测预警和信息通报制度，建设工业互联网安全监测技术手段；

b) 应及时向工业互联网安全主管部门报告所发现的安全弱点和可疑事件。

7.1.5 物理环境安全要求

7.1.5.1 物理位置选择

本项要求包括：

a) 工业互联网标识解析相关设备放置场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 工业互联网标识解析相关设备放置场地不宜设在建筑物的顶层或地下室，否则应加强防水和

防潮措施。

7.1.5.2 物理访问控制

本项要求包括：

工业互联网标识解析相关设备放置场地出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

7.1.5.3 防盗窃和防破坏

本项要求包括：

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

b) 应将通信线缆铺设在隐蔽安全处，可铺设在地下或管道中；

c) 主机房或重要设备区域应安装必要的防盗报警设施。

7.1.5.4 防雷击

本项要求包括：

应将各类机柜、设施和设备等通过接地系统安全接地。

7.1.5.5 防火

本项要求包括：

工业互联网标识解析业务相关设备放置场地应设置灭火设备和火灾自动报警系统。

7.1.5.6 防水和防潮

本项要求包括：

应采取措施防止雨水通过机房或场地窗户、屋顶和墙壁渗透。

7.1.5.7 防静电

本项要求包括：

工业互联网标识解析业务相关的关键设备应采用必要的接地防静电措施。

7.1.5.8 温湿度控制

本项要求包括：

工业互联网标识解析业务相关设备放置场地应设置温湿度自动调节设施，使温湿度的变化在设备运行所允许的范围之内。

7.1.5.9 电力供应

本项要求包括：

应在机房供电线路上配置稳压器和过电压防护设备。

7.2 基本级防护要求

7.2.1 设备和系统安全防护要求

7.2.1.1 身份鉴别

除满足 7.1.1.1 之外，还符合以下要求：

应采用密码技术等保障鉴别信息通过网络传输时的机密性和完整性。

7.2.1.2 访问控制

除满足 7.1.1.2 之外，还符合以下要求：

应对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。

7.2.1.3 恶意代码防范

除满足 7.1.1.3 之外，还符合以下要求：

当检测到恶意代码植入时，应对其进行有效阻断或隔离。

7.2.1.4 入侵防范

除满足 7.1.1.4 之外，还符合以下要求：

a) 应支持检测网络入侵行为，记录入侵的源 IP、攻击类型、攻击时间等，并在发生严重入侵事件时提供报警；

b) 应对设备系统中的安全漏洞、配置隐患等定期进行检测，保证不存在已公布的漏洞，或具备补救措施防范漏洞安全风险。

7.2.1.5 安全审计

本项要求包括：

a) 应启用安全审计功能，审计覆盖到所有用户，对重要的用户行为和安全事件进行审计；

b) 应采取手段保证日志无法删除、修改或覆盖，例如，日志集中管理、日志文件权限控制等；

c) 业务服务器、数据库、网络设备、安全设备等关键设备审计记录应采用 NTP 协议或其他技术保持时间上的同步。

7.2.1.6 设备冗余

本项要求包括：

应保证标识解析系统业务相关的关键设备支持冗余功能，在设备运行状态异常时，可通过启用备用部件防范安全风险。

7.2.2 网络安全防护要求

7.2.2.1 架构安全

除满足 7.1.2.1 之外，还符合以下要求：

a) 应采用内外网隔离、专线、加密等保护措施避免远程访问和标识数据在公共互联网的明文传输；

b) 应采用节点分布式架构，支持主备节点或负荷分担，单个主机/虚拟机故障不影响整体性能。

7.2.2.2 访问控制

除满足 7.1.2.2 之外，还符合以下要求：

a) 应优化访问控制列表，并保证访问控制规则数量最小化；

b) 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；

c) 系统内部网络与外部网络之间应采用访问控制机制，禁止任何与内部网络承载的业务无关的

通用网络服务穿越区域边界，如电子邮件服务、万维网服务、文件传输服务等；

d) 应在边界访问控制机制失效时及时进行告警。

7.2.2.3 安全监测

除满足 7.1.2.3 之外，还符合以下要求：

a) 应对标识解析系统中重要网络设备运行状况进行监测，发现异常情况（如系统宕机等）提供告警并进行相应处置；

b) 应通过访问控制技术手段限制只有特定网段和特定人员才能访问安全监测系统，查看监测数据。

7.2.2.4 入侵防范

除满足 7.1.2.4 之外，还符合以下要求：

a) 应在关键网络节点处部署防 DDoS 攻击措施，对针对这些节点的 DDoS 攻击流量进行检测和清洗，保障系统正常运行，并在发生攻击事件时提供告警；

b) 应在系统边界处对发生的网络入侵行为提供有效的检测能力，当检测到入侵行为时，应记录包括不限于攻击源 IP、攻击类型、攻击目的、攻击时间等信息，在发生严重入侵事件时应提供告警。

7.2.2.5 安全审计

本项要求包括：

a) 应在标识解析系统网络边界、重要网络节点进行安全审计，审计覆盖到所有用户，对标识解析系统重要的用户行为、网络流量和安全事件进行审计；

b) 应对审计记录进行留存和保护；

c) 审计记录应采用 NTP 协议或其他技术保持时间上的同步。

7.2.3 业务和应用安全防护要求

7.2.3.1 身份认证与访问控制

除满足 7.1.3.1 之外，还符合以下要求：

a) 应使用密码技术对身份认证数据进行机密性和完整性保护；

b) 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；

c) 应提供访问控制功能，对使用应用程序的用户分配账户及相应的访问操作权限；

d) 标识解析系统应配置基于密码技术的可信认证体系。

7.2.3.2 应用资源控制

除满足 7.1.3.2 之外，还符合以下要求：

a) 应支持对单个用户、终端、IP 地址的多重并发会话进行限制；

b) 应支持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；

c) 当通信双方中一方在一段时间内未作响应，另一方能够自动结束会话；

d) 应对请求标识解析业务并发量进行限制，保证标识解析业务的正常运行。

7.2.3.3 入侵防范

除满足 7.1.3.3 之外，还符合以下要求：

a) 应能够采取安全策略和措施，抵御缓冲区污染、防范反射/放大攻击、DNS 劫持、递归攻击等攻击行为；
b) 存在缓存服务的标识节点，应能够防范“中间人攻击”行为。

7.2.3.4 安全审计

本项要求包括：
a) 应记录包括不限于系统日志、错误日志、注册日志和解析日志等，日志记录的内容应包括但不限于事件的日期、时间、类型、主体标识、客体标识和结果等；
b) 应采取日志集中管理、日志文件权限控制等手段保证日志无法删除、修改或覆盖。

7.2.3.5 业务提供安全

除满足 7.1.3.4 之外，还符合以下要求：

系统要求不间断运行，在排除不可抗因素的情况下，按月统计解析服务可用性监测结果，系统业务可用性均应大于 99.99%。

7.2.4 安全管理要求

7.2.4.1 机构管理

除满足 7.1.4.1 之外，还符合以下要求：
a) 应设立网络安全管理工作的职能部门，具体承担网络安全管理工作，组织制定和落实网络安全管理制度，落实网络安全技术防护措施，开展网络安全宣传教育培训，执行网络安全监督检查等；
b) 应设立安全负责人岗位，以及系统管理员、网络管理员、安全管理员等专职人员岗位，并明确部门、各负责人和专职人员的岗位职责，明确授权审批事项、审批部门和批准人等；
c) 加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理安全问题；
d) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程；
e) 应加强与工业互联网安全主管部门、各类供应商、业界专家等合作与沟通，建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

7.2.4.2 制度管理

除满足 7.1.4.2 之外，还符合以下要求：
a) 应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
b) 应指定或授权专门的部门或人员负责安全管理制度的制定；
c) 根据工业互联网标识解析业务功能及安全工作总体方针和安全策略，建立适合机构安全工作实际情况的安全管理制度，覆盖机构和人员、物理和环境、安全建设和安全运维等层面的管理内容；
d) 安全管理制度应通过正式、有效的方式发布，并进行版本控制；
e) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

7.2.4.3 人员管理

除满足 7.1.4.3 之外，还符合以下要求：

a) 应对被录用人员的身份、背景、专业资格和资质等进行审查；
b) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
c) 应确保在外部人员接入受控网络访问系统前先提出书面申请；
d) 应确保在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
e) 应确保在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案，外部人员离场后应及时清除其所有的访问权限。

7.2.4.4 建设管理

7.2.4.4.1 定级

同 7.1.4.4.1。

7.2.4.4.2 安全方案设计

除满足 7.1.4.4.2 之外，还符合以下要求：

应组织安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

7.2.4.4.3 产品采购和使用

同 7.1.4.4.3。

7.2.4.4.4 软件开发

除满足 7.1.4.4.4 之外，还符合以下要求：

应要求外包开发合同中包含开发单位、供应商对所提供设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专用等方面的约束条款。

7.2.4.4.5 系统交付

除满足 7.1.4.4.5 之外，还符合以下要求：

应提供建设过程中的文档和指导用户进行运行维护的文档。

7.2.4.4.6 供应链安全

除满足 7.1.4.4.6 之外，还符合以下要求：

a) 应在服务协议中规定服务合约到期时，完整地返还客户信息，并承诺相关信息均已清除；
b) 应确保供应链安全事件信息或威胁信息能够及时传达到客户；
c) 应确保外包运维服务商的选择符合国家的有关规定；
d) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

7.2.4.5 运维管理

7.2.4.5.1 环境管理

除满足 7.1.4.5.1 之外，还符合以下要求：

应不在标识解析计算服务及数据存放等区域接待来访人员。

7.2.4.5.2 资产管理

除满足 7.1.4.5.2 之外，还符合以下要求：

a) 应对信息和资产在物理传输过程中的人员选择、打包、交付等情况进行控制，并对归档和查询等进行登记记录；
b) 应记录相关设备的状态（包括外观、电量、指示灯等信息），对设备进行现场维护（除尘、充电、修理等）；
c) 应对设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；
d) 应明确资产变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

7.2.4.5.3 密码管理

同 7.1.4.5.3。

7.2.4.5.4 安全审计

本项要求包括：

a) 应对标识解析相关业务系统、安全设备等启用安全审计功能，对工作人员及企业用户（如托管企业用户等）、个人用户行为和重要安全事件进行审计；审计记录应包括事件（如注册、解析等服务事件）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；
b) 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；审计记录中应避免明文记录敏感数据，如用户口令等；
c) 依法记录并留存标识注册日志、标识解析日志、维护日志等网络日志，日志留存时长不少于 6 个月。

7.2.4.5.5 配置管理

除满足 7.1.4.5.4 之外，还符合以下要求：

应根据监管部门及电信管理机构要求，配置监管数据的上报接口。

7.2.4.5.6 连续性管理

除满足 7.1.4.5.5 之外，还符合以下要求：

应为标识解析系统制定解析服务连续性计划，来保持解析服务的可用性，在解析服务中断的情况下能够在要求的时间内恢复系统的服务。

7.2.4.5.7 安全事件及应急处置

除满足 7.1.4.5.6 之外，还符合以下要求：

a) 应明确安全事件的报告和处置流程，制定安全事件报告和处置管理制度；
b) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据并记录处理过程；
c) 应制定网络安全事件应急预案，包括应急处理流程、系统恢复流程等内容，并根据实际情况适时进行评估和修订，原则上每年进行一次评估和修订；
d) 应定期开展网络安全事件应急预案宣贯培训及应急演练，确保相关人员熟悉应急预案。

7.2.5 物理环境安全要求

7.2.5.1 物理位置选择

同 7.1.5.1。

7.2.5.2 物理访问控制

除满足 7.1.5.2 之外，还符合以下要求：

工业互联网标识解析业务相关的重要服务器、数据库等设备所在区域宜采取视频监控等手段。

7.2.5.3 防盗窃和防破坏

同 7.1.5.3。

7.2.5.4 防雷击

同 7.1.5.4。

7.2.5.5 防火

同 7.1.5.5。

7.2.5.6 防水和防潮

除满足 7.1.5.6 之外，还符合以下要求：

应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

7.2.5.7 防静电

同 7.1.5.7。

7.2.5.8 温湿度控制

同 7.1.5.8。

7.2.5.9 电力供应

除满足 7.1.5.9 之外，还符合以下要求：

应在机房供电线路上配置稳压器和过电压防护设备。

7.2.5.10 电磁防护

本项要求包括：

电源线和通信线缆应隔离铺设，避免互相干扰。

7.3 增强级防护要求

7.3.1 设备和系统安全防护要求

7.3.1.1 身份鉴别

除满足 7.2.1.1 之外，还符合以下要求：

a) 应采取手段限制只允许管理员从特定终端登录进行管理；

b) 应选择两种或两种以上组合的鉴别技术对用户进行身份认证管理，且其中一种鉴别技术至少应使用密码技术来实现。

7.3.1.2 访问控制

除满足 7.2.1.2 之外，还符合以下要求：

a) 应对工业互联网标识解析涉及的多主体对象的身份权限进行统一管理，对用户访问过程实行严格的权限控制；
b) 应采用基于身份的策略、基于角色的策略、基于规则的策略等访问控制策略和访问控制列表、访问控制许可、密码技术等访问执行机制实现主机的用户或用户进程与设备、文件等对象间的访问控制。

7.3.1.3 恶意代码防范

除满足 7.2.1.3 之外，还符合以下要求：
a) 应对防范恶意代码机制进行统一管理，如统一升级和更新等。
b) 更新前应在离线环境中进行安全性和兼容性测试，必要时应在离线环境中进行安全验证，以保证配置变更不会影响服务器的正常运行；

7.3.1.4 入侵防范

除满足 7.2.1.4 之外，还符合以下要求：
a) 远程控制维护应采用 VPN 等加密通道，并具备日志记录能力；
b) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供告警。

7.3.1.5 安全审计

除满足 7.2.1.5 之外，还符合以下要求：
a) 应对审计进程进行保护，防止未经授权的中断；
b) 应对分散在各个网络设备上的审计数据进行收集汇总和集中分析。

7.3.1.6 设备冗余

除满足 7.2.1.6 之外，还符合以下要求：
a) 关键网络设备、重要线路、网络设备的重要部件应采用冗余的保护方式；
b) 应保证服务器、网络设备、安全设备等硬件设备的业务处理能力具备冗余空间。

7.3.2 网络安全防护要求

7.3.2.1 架构安全

除满足 7.2.2.1 之外，还符合以下要求：
a) 不应将标识注册、解析业务服务器直接连接外部系统或网络，系统内各功能区域间采取可靠的技术隔离手段；
b) 依据安全域内业务系统重要性，应采用基于物理原理通信的隔离交换技术，保障域间数据交换安全性；
c) 系统应具有过负荷保护功能，确保系统在过负荷时，重要业务能正常运行。

7.3.2.2 访问控制

除满足 7.2.2.2 之外，还符合以下要求：
a) 应在标识解析系统关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制；
b) 应限制无线网络的使用，确保无线网络通过受控的边界防护设备进行防护，使用无线接入认证技术。

7.3.2.3 安全监测

除满足 7.2.2.3 之外，还符合以下要求：

a) 应能够对系统内部网络中的用户或网络设备非授权连接到外部网络或因特网的行为进行限制或检查，并对其进行有效阻断；

b) 应在标识解析系统与外部系统之间的节点处部署异常检测、流量分析等技术手段，针对异常行为和指令可按需实现报警、阻断等功能，并保留攻击溯源样本；

c) 应能对网络中发生的各类安全事件进行识别、报警和分析。

7.3.2.4 入侵防范

除满足 7.2.2.4 之外，还符合以下要求：

a) 应具备相应技术能力，可以根据实际情况对特定地址/网段采取技术手段防止地址欺骗；

b) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

7.3.2.5 安全审计

除满足 7.2.2.5 之外，还符合以下要求：

a) 应对网络审计数据进行收集汇总和集中分析；

b) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

c) 应对标识解析系统进出流量和访问操作进行安全审计；

d) 应采取手段保证日志无法删除、修改或覆盖，例如，日志集中管理、日志文件权限控制等。

7.3.3 业务和应用安全防护要求

7.3.3.1 身份认证与访问控制

除满足 7.2.3.1 之外，还符合以下要求：

a) 应在系统边界部署访问控制设备，并启用访问控制功能，具有根据 IP 和端口为数据流提供明确的允许/拒绝访问的能力，并设置为默认拒绝，而只根据业务需要对特定网段开放访问权限；

b) 应支持双向身份认证，确保访问请求来自可靠的签名证书或可靠渠道；

c) 应对重点标识信息进行特别标记，并采取措施严格控制用户对重点标识信息的操作。

7.3.3.2 应用资源控制

同 7.2.3.2。

7.3.3.3 入侵防范

除满足 7.2.3.3 之外，还符合以下要求：

应对身份鉴别信息采取增加时间因子等手段，防止发生重放攻击。

7.3.3.4 安全审计

除满足 7.2.3.4 之外，还符合以下要求：

a) 应对标识业务服务情况进行监测，如服务解析量异常、解析状态异常、解析时延异常等，能够对业务上的安全事件进行识别、预警和分析；

b) 应提供对标识系统日志记录进行统计、查询、分析及生成审计报表的功能，并利用此功能定期（至少每月一次）对日志记录进行审计，出具审计报告；

c) 应采取手段保证日志无法删除、修改或覆盖，例如，日志集中管理、日志文件权限控制。

7.3.3.5 业务提供安全

除满足 7.2.3.5 之外，还符合以下要求：

a) 系统要求不间断运行，应采用冗余架构、多点任播分布或类似技术措施提高系统的可用性；
b) 应设置重点工业互联网标识清单，并对重点工业互联网标识的解析结果进行正确性监控，如发现解析结果异常，应及时告警。

7.3.4 安全管理要求

7.3.4.1 机构管理

除满足 7.2.4.1 之外，还符合以下要求：

a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
b) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

7.3.4.2 制度管理

除满足 7.2.4.2 之外，还符合以下要求：

a) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系；
b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
c) 应确定安全检查内容，汇总安全检查数据，形成安全检查报告，根据安全检查结果进行整改。

7.3.4.3 人员管理

除满足 7.2.4.3 之外，还符合以下要求：

a) 应配备专职安全管理员，不可兼任，关键事务岗位应配备备用管理人员；
b) 应对被录用人员所具有的技术技能进行考核，应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
c) 人员离岗时，应办理严格的调离手续，并承诺调离后的保密义务后方可离开；
d) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训，应定期对不同岗位的人员进行技能考核；
e) 获得系统访问授权的外部人员应签署保密协议，不应进行非授权操作，不应复制和泄露任何敏感信息，对关键区域或关键系统不准许外部人员访问。

7.3.4.4 建设管理

7.3.4.4.1 定级

同 7.2.4.4.1。

7.3.4.4.2 安全方案设计

除满足 7.2.4.4.2 之外，还符合以下要求：

a) 应根据标识解析企业的安全防护需求及与其他防护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
b) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和

审定，经过批准后才能正式实施。

7.3.4.4.3 产品采购和使用

除满足 7.2.4.4.3 之外，还符合以下要求：

a) 应预先对产品进行选型测试，确定产品候选范围，并定期审定和更新候选产品名单；

b) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

7.3.4.4.4 软件开发

除满足 7.2.4.4.4 之外，还符合以下要求：

a) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；

b) 自行进行软件开发时，应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

c) 自行进行软件开发时，应制定代码编写安全规范，要求开发人员参照规范编写代码；

d) 自行进行软件开发时，应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制；

e) 自行进行软件开发时，应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

f) 自行进行软件开发时，应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

7.3.4.4.5 系统交付

除满足 7.2.4.4.5 之外，还符合以下要求：

系统安全测试报告应包含密码应用安全性测试相关内容。

7.3.4.4.6 供应链安全

除满足 7.2.4.4.6 之外，还满足以下要求：

a) 应定期评审和审核供应商提供的服务，并对其变更服务内容加以控制；

b) 应保证供应商的重要变更及时传达到客户，并评估变更带来的安全风险，采取有关措施对风险进行控制。

7.3.4.5 运维管理

7.3.4.5.1 环境管理

除满足 7.2.4.5.1 之外，还符合以下要求：

a) 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等；

b) 应加强对工业互联网设备部署环境的机密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

7.3.4.5.2 资产管理

除满足 7.2.4.5.2 之外，还符合以下要求：

a) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

b) 应对信息分类与标识方法做出规定，并对信息的使用、传输和存储等进行规范化管理；

c) 信息处理设备应经过审批后带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要及核心数据应加密处理；

d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用；
e) 应建立资产变更的申报和审批程序，依据程序控制所有的变更，记录变更实施过程；
f) 应建立中止资产变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

7.3.4.5.3 密码管理

同 7.2.4.5.3。

7.3.4.5.4 安全审计

除满足 7.2.4.5.4 之外，还符合以下要求：
应能对远程访问企业内部网络的用户行为进行行为审计和数据分析。

7.3.4.5.5 配置管理

除满足 7.2.4.5.5 之外，还符合以下要求：
a) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库；
b) 应实现标识业务系统、安全设备、关联系统的管理员权限分离，分别设置安全管理员、系统管理员、审计管理员。

7.3.4.5.6 连续性管理

同 7.2.4.5.6。

7.3.4.5.7 安全事件及应急处置

除满足 7.2.4.5.7 之外，还符合以下要求：
a) 应建设完善工业互联网安全监测技术手段，宜接入国家级或省级工业互联网安全监测平台；
b) 应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
c) 应定期开展网络安全应急演练，检验应急预案的可操作性，并结合应急演练结果，对应急预案进行评估和适用性修订；
d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对基础设施中断服务的应急保障要求等。

7.3.5 物理环境安全要求

7.3.5.1 物理位置选择

除满足 7.2.5.1 之外，还符合以下要求：
a) 在机房选址及设计时，满足 GB 50174 的相关规定；
b) 确保工业互联网标识解析服务器及运行关键业务和数据的物理设备位于境内。

7.3.5.2 物理访问控制

除满足 7.2.5.2 之外，还符合以下要求：
a) 应对工业互联网标识解析系统相关设备放置场地划分区域并在不同区域之间设置物理隔离装

置，在重要区域前设置交付或安装等过渡区域；

b） 应在工业互联网标识解析系统相关设备放置场地设置有专人值守的视频监控系统。

7.3.5.3 防盗窃和防破坏

除满足 7.2.5.3 之外，还符合以下要求：

应对工业互联网标识解析系统相关设备放置场地设置监控报警系统。

7.3.5.4 防雷击

同 7.2.5.4。

7.3.5.5 防火

除满足 7.2.5.5 之外，还符合以下要求：

a） 工业互联网标识解析系统相关设备放置场地应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

b） 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

7.3.5.6 防水和防潮

除满足 7.2.5.6 之外，还符合以下要求：

应安装对水敏感的检测仪表或元件，对工业互联网标识解析系统相关设备放置场地进行防水检测和报警。

7.3.5.7 防静电

除满足 7.2.5.7 之外，还符合以下要求：

应采取措施防止静电的产生，例如，采用静电消除器、佩戴防静电手环等。

7.3.5.8 温湿度控制

同 7.2.5.8。

7.3.5.9 电力供应

除满足 7.2.5.9 之外，还符合以下要求：

应设置冗余或并行的电力电缆线路为工业互联网标识解析系统供电。

7.3.5.10 电磁防护

同 7.2.5.10。

附 录 A
（资料性）
工业互联网标识解析企业安全防护范围示意图

图 A.1 给出了工业互联网标识解析企业安全防护范围示意图。

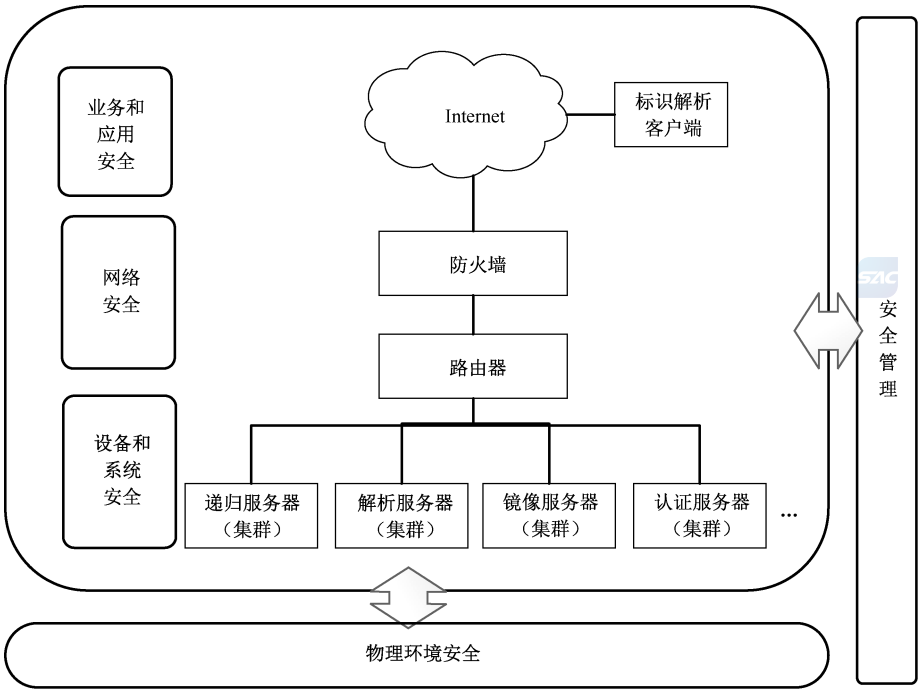

图 A.1 工业互联网标识解析企业安全防护范围示意图

参 考 文 献

[1] GB/T 22239 信息安全技术 网络安全等级保护基本要求
[2] GB/T 33745—2017 物联网 术语
[3] 工业互联网安全分类分级管理办法(工信部网安〔2024〕68号)
[4] 工业互联网标识管理办法(工信部信管〔2020〕204号)