ICS 35.030
CCS M10

团 体 标 准

T/CCSA 527—2024

工业互联网企业网络安全分类分级评估方法

Industrial Internet enterprise cybersecurity classification and grading evaluation method

2024－04－10 发布　　2024－04－10 实施

中国通信标准化协会　　发 布

版权声明

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。

本文件由中国通信标准化协会提出并归口。

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、北京天融信网络安全技术有限公司、南京中新赛克科技有限责任公司、杭州安恒信息技术股份有限公司、北京启明星辰信息安全技术有限公司、鹏城实验室、郑州信大捷安信息技术股份有限公司。

本文件主要起草人：魏亮、谢玮、林美玉、张倩、田慧蓉、柯皓仁、于广琛、马娟、李艺、孟烨、王吉、吴昊、张瑜、刘晓曼、杨春瑞、官文杰、柴月飞、刘晓喆、陈杰、吴诗雨、李诗婧、郭茜、陕言、余果、樊佩茹、孔同、马霄、安高峰、曹家腾、糜靖峰、汤永田、李兴刚、周升宝、谷宝晶、张凡、赵娟、刘为华。

引　言

为适应信息通信业发展对标准文件的需求，由中国通信标准化协会组织制定“中国通信标准化协会团体标准”，推荐有关方面采用。有关对本标准的建议和意见，向中国通信标准化协会反映。

根据工业和信息化部工业互联网安全分类分级管理相关文件，提出工业互联网企业定期开展符合性评测等工作要求。目前，工业互联网企业落实分类分级防护要求后，缺乏开展符合性评测的标准化指导，评估内容、流程和要求尚未统一规范，评估结论和判定结果多样，无法有效引导企业提升网络安全防护水平。

本文件以《中华人民共和国网络安全法》、《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》、《加强工业互联网安全工作的指导意见》等法律法规及政策文件为指引，根据工业和信息化部工业互联网安全分类分级管理相关文件及配套的标准规范要求，为工业互联网企业、工业互联网安全评估机构、相关主管部门等提供工业互联网企业网络安全分类分级评估的实施方法。

工业互联网企业网络安全分类分级评估方法

1 范围

本文件规定了工业互联网企业网络安全分类分级评估的工作流程、实施要求、分析评价以及结果输出等。

本文件适用于指导开展工业互联网企业网络安全分类分级评估工作，为评估实施、分析评价和结果输出等各环节提供工作指引。

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 25069-2022 信息安全技术 术语

GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

GB/T 25069-2022界定的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

工业互联网企业 industrial Internet enterprise

包括应用工业互联网的工业企业、工业互联网平台企业和工业互联网标识解析企业。

3.3

应用工业互联网的工业企业 Internet industrial enterprise

将新一代信息通信技术与工业系统深度融合，推动开展数字化研发、智能化制造、网络化协同、个性化定制、服务化延伸等的工业企业，本文件中简称“联网工业企业”。

3.4

工业互联网平台企业 industrial Internet platform enterprise=

面向制造业数字化、网络化、智能化需求，基于云平台等方式对外提供工业大数据、工业APP等资源和公共服务的企业，本文件中简称“平台企业”。

3.5

工业互联网标识解析企业 industrial Internet identity 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，本文件中简称“标识解析企业”。

3.6

安全评估 security assessment

按安全标准及相应方法，验证某一安全可交付件与适用标准的符合程度及其安全确保程度的过程。

[来源：GB/T 25069-2022，3.19]

4 缩略语

下列缩略语适用于本文件。

APP：应用程序（Application）

CVE：通用漏洞披露（Common Vulnerabilities & Exposures）

CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）

CNNVD：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）

NVDB：工业和信息化部网络安全威胁和漏洞信息共享平台(National Vulnerability Database)

5 评估原则

工业互联网企业网络安全分类分级评估应遵循以下原则：

a) 最小影响：评估过程中，对于需要进行攻击性测试的工作内容，应与用户沟通并进行应急备份，同时选择避开业务的高峰时间运行，保障评估委托单位业务系统的稳定运行；

b) 客观公正：评估应建立在评估单位和评估委托单位诚信的基础之上，评估委托单位在访谈过程中应如实陈述自身的安全防护情况，评估方在评估过程中应客观公正地记录和分析评估委托单位的安全防护情况；

c) 范围完整：应按照相关安全防护标准规范，从不同层面全面评估其安全防护水平与安全风险隐患；

d) 信息保密：评估人员应严格遵守保密原则，对于接触到的业务数据、系统数据及其他敏感信息等，不得泄露给第三方，损害评估委托单位利益。

6 评估流程

6.1 工作准备

6.1.1 组建项目组

在工作启动阶段，评估单位首先应组建评估工作项目组，明确项目经理以及项目组成员。项目经理应了解项目组成员技术能力，保证项目实施过程顺利开展。评估单位应依据委托评估协议书、委托评估项目合同等，获取委托单位业务情况、资产配备情况、安全建设情况、安全防护情况、基础硬件设施情况、安全人员配备情况等基本信息，为评估实施做好准备。

6.1.2 开展评估调研

评估单位通过查阅评估对象已有资料或使用评估调研问卷的方式，了解企业网络架构、系统资产、网络安全防护以及安全管理制度等相关情况，为编写评估方案、开展安全评估工作奠定基础。如在调研过程中发现获取信息存在不准确、不完善或相互矛盾的情况，评估单位应与评估委托单位相关人员进行沟通和确认，必要时安排一次调查，与相关人员进行面对面的沟通和确认，确保信息的准确性和完整性。

6.1.3 制定评估方案

评估方案是评估工作开展的基础，为评估工作提供实施指导，包括评估对象、评估指标、评估内容、评估方法及评估计划等重点内容。

6.1.3.1 确定评估对象

根据评估调研情况，应明确评估委托单位的分类分级结果，包括企业类型与企业级别。通过分析其业务范围、关键业务流程、相关业务特点等，确定评估对象范围。

联网工业企业评估对象包括：工控设备、工业控制软件、工业APP、工业主机及服务器操作系统、应用软件、数据库软件、网络设备、安全设备等。

平台企业评估对象包括：通用组件、通用接口、容器、虚拟机、服务器操作系统、数据库、网络互联设备、安全设备、平台应用等。

标识解析企业评估对象包括：标识解析系统、服务器操作系统、数据库、网络互联设备、安全设备等。

6.1.3.2 确定评估指标

根据评估委托单位的企业类型与级别确定本次评估的指标项。企业类型包括联网工业企业、平台企业、标识解析企业，企业级别包括一级、二级、三级，指标选取按照相关工作要求以及《工业互联网企业网络安全 第1部分：应用工业互联网的工业企业防护要求》、《工业互联网企业网络安全 第2部分：平台企业防护要求》、《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》等防护标准规范要求进行。

6.1.3.3 确定评估内容

评估内容依据相关防护规范，将评估指标和评估对象结合起来，即将评估指标映射到各评估对象上，同时结合评估对象的特点，说明对各评估对象采取的评估方法，由此构成可以具体实施的评估内容。

6.1.3.4 确定评估方法

根据实际情况选取人员访谈、文档审查、基线核查、技术评估等方式开展评估工作。

a) 人员访谈：通过与评估委托单位的相关人员进行交谈和问询，了解评估对象技术和管理方面的基本信息；
b) 文档审查：通过查阅文档的方式，审查评估委托单位网络安全建设、安全管理制度、制度执行情况记录等文档的完整性，以及这些文件之间的内部一致性等；
c) 配置核查：对被评估单位相关的评估对象，包括主机类设备、网络设备、安全设备、控制设备、系统软件、应用软件等进行安全配置的检查；
d) 技术评估：通过使用专用的评估工具进行主机层面、设备层面、软件层面、应用层面等的技术评测，包括漏洞扫描、渗透测试、恶意代码扫描等。技术评估的要求包括：
   1) 技术评估环境应根据被测系统的实时性要求，选择生产环境或与生产环境各项安全配置相同的测试环境；
   2) 技术评估应充分考虑网络边界安全防护设备等对于技术评估的影响，根据实际情况选择合适的工具接入点（互联网接入、内部局域网接入、设备直连接入等）以及接入方式（无线网络、有线网络、虚拟专用网络）。

6.1.3.5 制定评估计划

根据前期得到的信息进一步估算评估工作量，并结合评估项目组成员配置与时间节点要求等，编制具体评估工作计划。

6.1.3.6 形成评估方案

评估单位汇总评估对象、评估指标、评估内容、评估方法、评估计划等，形成评估方案，提交至评估委托单位进行内容确认。

6.2 评估实施

6.2.1 召开启动会

评估单位组织项目组成员与评估委托单位召开评估启动会。会上，评估单位应介绍评估工作安排，相关方针对评估方案进行沟通。评估相关方确认评估需要的各种资源，包括评估需要的配备的人员和评估环境等。

评估委托单位应协助评估单位获得评估对象相关方的评估授权。

评估单位应签订保密承诺书，严格保守评估过程中获取的相关信息，保护评估委托单位信息不被泄露。评估单位应与评估委托单位签订风险告知书，使评估委托单位了解评估过程中存在的安全风险，做好相关应急和备份工作。

6.2.2 开展评估实施

评估人员按照评估方案实施安全技术评估与安全符合性评估，具体要求符合第7章。

6.2.3 确认评估结果

评估单位在评估完成后，首先应汇总评估记录，对漏掉和需进一步验证的内容实施补充评估。并与评估委托单位对评估过程中得到的评估原始记录进行沟通和确认。完成评估原始记录信息确认后，评估单位应归还评估过程中借阅的所有文档资料，并由评估委托单位文档资料提供者确认。

6.3 结果研判

6.3.1 安全符合性评估结果

评估单位针对原始记录表中的不符合项及部分符合项，采取逐条判定的方法，分析与该评估项相关的其他评估项之间可能存在的关联关系，以及这些关联关系产生的作用是否可以“弥补”该评估项的不足或“削弱”该评估项的影响，判断该评估项的评估结果是否会影响与其有关联关系的其他评估项的评估结果。即从评估委托单位的工业互联网安全整体层面考虑，复核修正单项评估结果，进而计算得出安全符合性评估分数，计算方法详见8.1。

6.3.2 安全风险分析结果

评估单位应采用风险分析的方法，对评估中不符合项与部分符合项存在的安全问题进行分析，确定安全风险与风险等级，判定方法详见8.2。

6.3.3 评估结论

评估单位根据评估信息，得出评估委托单位安全符合性评估分数与风险分析结果。

6.4 报告编制

评估单位整理评估成果，参考附录B编制评估报告，并针对评估委托单位存在的安全隐患，从系统安全角度提出相应的改进建议，编制评估报告的问题整改建议部分。

评估报告编制完成后，评估单位内部根据委托评估协议书、委托评估项目合同、评估委托单位提交的相关文档、评估原始记录和其他辅助信息，对评估报告进行评审，评审通过后，由评估单位盖章并提交给评估委托单位。

7 实施要求

7.1 安全评估总体要求

7.1.1 工具要求

评估单位应提供安全评估中涉及到的工具清单，并保证评估工具本身不存在恶意程序、漏洞及其他安全缺陷。

对于评估工具可能带来的风险及后果应明确提出，并给出相应风险规避措施及应急处置措施。

7.1.2 过程要求

评估委托单位应提供满足评估工作要求的接入环境，并提供评估工作所需要的相关信息。评估单位应将评估过程中获取信息进行详细、准确记录，形成原始记录表单。

评估单位应在评估过程中规避危害或可能带来风险的动作，避免因评估工作对被评估系统运行造成不良影响。评估单位应保证评估过程中的相关数据不被泄漏。在评估工作完成后，评估单位应删除评估痕迹，如若存在无法删除的痕迹，应及时告知委托评估单位。

7.1.3 人员要求

评估单位应选派具备相关评估资质的安全评估人员开展评估工作。评估工作负责人应具备工业互联网安全评估经验。

7.2 安全技术评估要求

7.2.1 漏洞扫描

基于漏洞库，使用端口服务扫描、主机扫描、Web应用扫描、APP扫描等工具对指定的远程或者本地的网络设备、主机、业务系统等进行漏洞扫描，并通过使用人工手动验证或工具自动化验证的手段，验证漏洞扫描过程中发现的各类漏洞。

7.2.2 渗透测试

通过流量抓取、协议分析等方式，深入分析评估对象自身或业务应用业务逻辑层面可能存在设计缺陷、配置不足等安全风险，进行模拟攻击以检测系统或应用程序的防护能力。应从不同的安全区域，如内网接入或外网接入开展渗透测试，从而验证网络安全策略的有效性。

7.2.3 恶意代码扫描

基于恶意代码特征库，通过自动化扫描工具对评估委托单位的相关网络、服务器、终端等进行恶意代码扫描，发现潜伏在网络、主机或存储设备中的恶意代码。

7.3 安全符合性评估要求

7.3.1 联网工业企业安全符合性评估

按照联网工业企业安全防护相关标准规范实施，评估应根据企业定级级别选择相应级别防护指标项开展。

7.3.2 平台企业安全符合性评估

按照平台企业安全防护相关标准规范实施，评估应根据企业定级级别选择相应级别防护指标项开展。

7.3.3 标识解析企业安全符合性评估

按照标解析企业安全防护相关标准规范实施，评估应根据企业定级级别选择相应级别指标项开展。

8 分析评价

8.1 概述

首先针对评估委托单位的安全符合性评估结果进行分数计算，其次结合安全技术评估与安全符合性评估结果，围绕评估委托单位所承载的核心业务资产，通过关联影响分析，判定其存在的高风险、中风险、低风险及可接受风险。

8.2 安全符合性评估分数计算

8.2.1 分数说明

评分总分值为100分，每类企业安全符合性评估算分均从技术、管理维度进行，技术类占比50%，管理类占比50%，指标分类详见附录A。

每个评估项对应四类评估结果，包括“符合”“部分符合”“不符合”“不适用”。其中，“符合”“部分符合”“不符合”对应评分分别为100分、50分、0分，“不适用”项不计入分数计算。

8.2.2 权重分配

指标项划分权重，具体操作如下：

设置指标项【权重】为λ，默认λ为1；

将评估项根据重要性分为一般项、重要项与关键项，三类指标的【权重】取值范围分别为：0.5≤λ＜1、λ=1、1＜λ≤2；

8.2.3 评估得分计算

评估得分计算公式：

$$S_{技/管}=\frac{\sum_{i=1}^{M} Xi\,\lambda i}{\sum_{i=1}^{M} \lambda i} \quad \cdots\cdots (1)$$

式中：

M——指标个数；

Xi——指标得分；

λi——指标对应的权重。

注：仅计算已评价的指标项，不适用指标不参与计算。

分别计算技术类总分$S_{技}$、管理类总分$S_{管}$，进而得出安全符合性评估总分：

$$S_{总} = 0.5S_{技} + 0.5S_{管} \quad (2)$$

8.3 安全风险等级判定

对评估实施过程中安全技术评估发现的漏洞、安全符合性评估发现的问题进行风险判定。

针对安全技术评估过程发现的安全漏洞，宜根据NVDB、CVE、CNVD、CNNVD等漏洞库平台标注的漏洞级别进行风险等级判定；或者按照GB/T 30279-2020进行风险等级判定，其中，超危和高危漏洞风险等级均为“高风险”、中危漏洞风险等级为“中风险”，低危漏洞风险等级为“低风险”。

针对安全符合性评估发现的问题，应采用风险分析的方法进行风险等级判定，即根据安全问题的关联资产，以及资产已有安全措施，分析安全问题被利用的难易程度（被利用等级，见表1）和安全问题导致安全事件产生影响的影响程度（事件影响等级，见表2），综合评价其所能造成的安全风险（风险等级，见表3）。

在安全技术评估过程中发现安全漏洞的风险等级，可通过风险分析方法进行调整。

注：对评估发现的高风险，应第一时间进行整改。

表1 被利用等级赋值

序号	利用等级	描述
1	容易	结合安全问题关联资产以及已有安全措施分析，安全问题可通过网络/本地/物理等方式被利用，触发资源很容易被获取，并且利用成本很低或通过不可抗力因素触发
2	一般	结合安全问题关联资产以及已有安全措施分析，安全问题可通过网络/本地/物理等方式被利用，触发所需的部分资源比较容易获取，成本不高，在现有条件基础上通过一定的技术、资源投入可以触发安全问题或偶然通过自然条件触发
3	较难	结合安全问题关联资产以及已有安全措施分析，安全问题可通过网络/本地/物理等方式被利用，触发需要的资源多，成本高，难于获取或不容易通过自然条件触发

表2 事件影响等级

序号	事件影响等级	描述
1	重大影响	触发安全问题会对系统资产、业务运行以及企业管理等造成严重影响，例如:对环境中大部分资产造成影响，通常高于 50%；或造成业务停止运行超过 4 小时以上；或者受影响实体处于参考环境的重要位置，或者具有重要作用
2	一般影响	触发安全问题会对系统资产、业务运行以及企业管理等造成中等程度的影响，例如:对环境中相当部分资产造成影响，通常介于 10%-50%；或者受影响实体处于参考环境的比较重要位置，或者具有比较重要的作用
3	较小影响	触发安全问题会对系统资产、业务运行以及企业管理等造成轻微的影响，例如:只对环境中小部分资产造成影响，通常低于 10%；或者受影响实体处于参考环境的不重要位置，或者具有不重要作用
4	无影响	触发安全问题不会对系统、资产等造成任何资产损失

表3 风险等级赋值

序号	利用等级	影响等级	风险等级
1	容易	重大影响	高风险
2	容易	一般影响	高风险
3	容易	较小影响	中风险

表 3（续）

序号	利用等级	影响等级	风险等级
4	一般	重大影响	高风险
5	一般	一般影响	中风险
6	一般	较小影响	中风险
7	较难	重大影响	中风险
8	较难	一般影响	低风险
9	较难	较小影响	低风险
10	较难	无影响	可接受风险

9 结果输出

评估应出具完整的工业互联网企业网络安全分类分级评估报告，包括评估基本情况、评估实施情况与评估结论分析等:

a) 评估基本情况包括评估委托单位基本情况、安全管理情况、自主定级情况、评估对象（系统）情况、评估时间、评估地点、评估方法、评估工具、评估指标项与评估单位等。

b) 评估实施情况与评估结论分析主要包括以下部分，详见附录 B。

1) 对评估中发现的安全问题进行总结说明，包含安全管理、设备安全防护要求、网络安全防护、控制安全防护、物理和环境安全、漏洞隐患情况等，给出整体安全状况的描述与评价；

2) 评估情况说明要以表格形式整合原始记录信息，对各安全子类符合情况进行结果记录说明，给出单项指标的符合性结果，结果包括“符合”、“不符合”、“部分符合”、“不适用”。重点对不符合项、部分符合项以及不适用项进行详细的情况说明；

3) 根据评估结果分析安全问题，对企业存在的主要安全威胁、安全漏洞、安全隐患进行详细描述，对评估中发现的具体安全问题进行描述；

4) 针对全部不符合项和部分符合项对应的安全问题给出详细的整改建议；

5) 对评估委托单位网络安全情况进行整体分析，给出综合评估结论。

附 录 A
（资料性）
评估指标项分类

联网工业企业、平台企业、标识解析企业指标项分类见表A.1。

表A.1 联网工业企业、平台企业、标识解析企业指标项

企业类型	技术类指标项	管理类指标项
联网工业企业	设备安全类、工业控制安全类、网络安全类、应用平台软件安全类	安全管理类、物理和环境安全类
平台企业	接入层安全类、基础设施层安全类、平台层安全类、应用层安全类	安全管理类、物理和环境安全类
标识解析企业	设备和系统安全类、网络安全类、业务和应用安全类	安全管理类、物理和环境安全类

附 录 B
（资料性）
工业互联网企业网络安全分类分级评估报告模板

[可添加企业logo]

报告编号：XXXXXXX

【报告编号说明：评估单位应制定本单位的报告编号规则，如前两位为评估委托单位类型，联网工业企业LW、平台企业PT、标识解析企业BS；中间两位为年份，如2024年为24；后三位为报告编号可从001开始；示例LW24001】

工业互联网企业网络安全分类分级评估报告

对象名称：_____

委托单位：_____

评估单位：_____

报告时间：XXXX 年 XX 月 XX 日

[可添加企业 logo]

报告编号：XXXXXXX

基本信息及评估结果				
企业级别	一级/二级/三级	安全防护要求级别		
企业类型	联网工业企业/工业互联网平台企业/工业互联网标识解析企业			
对象名称				
评估地点				
评估周期	XXXX 年 XX 月 XX 日~XXXX 年 XX 月 XX 日			
评估得分				
风险情况	XX 高风险、XX 中风险、XX 低风险、XX 可接受风险			
评估委托单位信息				
单位名称				
单位地址			邮政编码	
联系人	姓名		邮箱	
	所属部门		电话	
评估单位信息				
单位名称				
通信地址			邮政编码	
联系人	姓名		邮箱	
	所属部门		电话	
项目评估工程师				
审核批准	编制人	(签名)	编制日期	
	审核人	(签名)	审核日期	
	批准人	(签名)	批准日期	

[可添加企业 logo]

报告编号：XXXXXXX

声 明

【填写说明：声明是评估单位对评估报告的有效性前提、评估结论的适用范围以及使用方式等有关事项的陈述。针对特殊情况下的评估工作，评估单位可在以下建议内容的基础上增加特殊声明。】

本报告是针对[评估委托单位]的分类分级评估报告。

本报告安全评估结论的有效性建立在评估委托单位提供相关证据的真实性基础之上。

本报告中给出的安全评估结论仅对被评估业务当时的安全状态有效。当安全评估工作完成后，由于业务发生变更而涉及到的业务构成组件（或子业务）都应重新进行安全评估，本报告不再适用。

本报告中给出的安全评估结论不能作为对业务内部署的相关业务构成组件（或产品）的结论。

在任何情况下，若需引用本报告中的安全评估结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

评估单位名称:

XXXX 年 XX 月 XX 日

（盖章）

[可添加企业 logo]

报告编号：XXXXXXX

报 告 摘 要

【填写说明：报告摘要通过文字描述项目报告的摘要信息，包括但不限于项目信息、评估对象、评估依据、评估过程、各层面已有安全措施情况和安全问题情况、综合评估结论等内容。】

[可添加企业 logo]

报告编号：XXXXXXX

目 录

[可添加企业 logo]

报告编号：XXXXXXX

1 项目概述

1.1 项目背景

【填写说明：简述评估项目背景和项目目标等。】

1.2 评估依据

【填写说明：分类列出开展工业互联网企业网络安全评估活动所依据的标准、文件和合同等。如果依据了国家、行业标准的，列出最新标准。】

■ ……

1.3 评估过程

【填写说明：描述评估工作流程、各阶段完成的关键任务和工作的时间节点等内容。】

1.4 企业定级情况

【填写说明：参考工业互联网企业网络安全分类分级定级要素以及定级规则，对当前企业的定级情况以及级别进行描述，并根据企业自主定级结果填写下表中的定级要素得分和企业级别。】

企业类型	定级要素得分	企业级别
联网工业企业/平台企业/标识解析企业	需对各定级要素得分及总分进行说明	一级/二级/三级

[可添加企业 logo]

报告编号：XXXXXXX

2 业务情况

2.1 承载业务情况

【填写说明：承载业务情况对评估范围内评估对象的业务情况进行了解，并且评估对象的业务情况进行描述，对业务的保密性、可用性、实时性等方面进行分析。】

2.2 网络结构情况

【填写说明：网络结构是对评估对象的网络结构进行分析，包括网络结构的区域划分、边界识别、防护情况等进行分析；如涉及多个评估对象应分别分析网络结构情况；附网络拓扑结构图和文字说明。】

2.3 业务资产构成

2.3.1 主机/存储类设备

表 1 服务器/主机设备清单

序号	服务器/主机名称	IP 地址	操作系统版本	虚拟机/物理机	虚拟机填写虚拟化技术	评估对象
1						是/否
2						

2.3.2 网络设备清单

表 2 网络设备清单

序号	网络设备名称	品牌型号	IP 地址	评估对象
1				
2				

[可添加企业 logo]

报告编号：XXXXXXX

2.3.3 安全设备清单

表 3 安全设备清单

序号	安全设备名称	品牌型号	IP 地址	评估对象
1				
2				

2.3.4 工控设备清单

表 4 工控设备清单

序号	工控设备名称	品牌型号	IP 地址	评估对象
1				
2				

2.3.5 平台接入设备清单

表 5 平台接入设备

序号	设备名称	品牌型号	操作系统	IP 地址	评估对象
1					
2					

2.3.6 应用程序清单

表 6 应用程序清单

序号	应用软件名称	登录地址（B/S 架构请填写 IP 地址或 url）	评估对象
1			
2			

[可添加企业 logo]

报告编号：XXXXXXX

2.3.7 数据库清单

表 7 数据库清单

序号	数据库名称	版本	IP 地址及端口	用途	评估对象
1					
2					

2.3.8 微服务组件清单

表 8 微服务组件清单

序号	组件名称	版本	IP 地址	主要用途	评估对象
1					
2					

2.3.9 资源管理平台清单

表 9 资源管理平台清单

序号	应用软件名称	版本/型号	登录地址（B/S 架构请填写 IP 地址或 url）	评估对象
1				
2				

2.3.10 物理环境

表 10 物理环境

序号	物理环境名称	物理环境位置	评估对象
1			
2			

[可添加企业 logo]

报告编号：XXXXXXX

2.3.11 安全相关人员

表 11 安全相关人员

序号	姓名	岗位/角色
1		
2		

2.3.12 管理制度列表

表 12 管理制度相关材料清单

序号	分类	制度名称
1		
2		

3 评估范围

3.1 评估指标

【填写说明：评估指标按照企业类型、企业级别、安全防护要求级别情况参考《工业互联网企业网络安全 第 1 部分：应用工业互联网的工业企业防护要求》《工业互联网企业网络安全 第 2 部分：平台企业防护要求》《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》标准相关要求，选择相应的评估指标，并按照下表方式进行填写。】

序号	一级指标	二级指标	三级指标（数量）	备注

[可添加企业 logo]

报告编号：XXXXXXX

3.2 评估方法

【填写说明：评估方法是开展工业互联网企业网络安全分类分级评估工作过程中所适用的评估方法，如下评估方法共参考，评估单位可根据实际情况撰写。】

- 人员访谈

通过与评估委托单位的相关人员进行交谈和问询，了解评估对象技术和管理方面的一些基本信息。

- 文档审查：

通过查阅文档的方式，审查评估委托单位网络安全建设、安全管理制度、制度执行情况记录等文档的完整性，以及这些文件之间的内部一致性等。

- 基线核查

通过人工的方式，对被评估单位相关的评估对象，包括主机类设备、网络设备、安全设备、控制设备、系统软件、应用软件等进行安全配置的检查。

- 技术评估

通过使用专用的评估工具进行主机层面、设备层面、软件层面、应用层面等的技术评估，包括漏洞扫描、渗透测试、恶意代码扫描等。

3.3 评估工具

【填写说明：评估工具是开展工业互联网企业网络安全分类分级评估工作过程中所使用的评估工具，工具包括主动探测类、自动化扫描工具、验证类工具等等，根据实际工具使用情况填写下表。】

序号	工具名称	型号/版本号	主要用途
1			
2			

[可添加企业 logo]

报告编号：XXXXXXX

4 安全符合性评估结果

符合情况判定根据“评估指标”的要求，结果完全满足时，符合情况为“符合”，结果部分满足时，符合情况为“部分符合”，结果完全不满足时，符合情况为“不符合”，“评估指标”当前环境下不适用时，符合情况为“不适用”。

评估指标根据重要性分为一般项、重要项与关键项，三类指标的权重取值范围分别为：0.5≦λ＜1、λ=1、1＜λ≦2；权重默认取值为 1。

安全评估内容包括“3.1 评估指标”中涉及的安全分类中要求，具体内容结果记录如下。

4.1 一级指标

4.1.1 二级指标

评估对象	三级指标	评估指标	结果记录	符合情况	权重

4.1.2 二级指标

评估对象	三级指标	评估指标	结果记录	符合情况	权重

4.1.3 二级指标

评估对象	三级指标	评估指标	结果记录	符合情况	权重

[可添加企业 logo]

报告编号：XXXXXXX

4.2 一级指标

4.2.1 二级指标

评估对象	三级指标	评估指标	结果记录	符合情况	权重

4.2.2 二级指标

评估对象	三级指标	评估指标	结果记录	符合情况	权重

4.3 一级指标

4.3.1 二级指标

评估对象	三级指标	评估指标	结果记录	符合情况	权重

4.3.2 二级指标

评估对象	三级指标	评估指标	结果记录	符合情况	权重

4.4 一级指标

4.5 一级指标

……

[可添加企业 logo]

报告编号：XXXXXXX

5 安全技术评估结果

【填写说明：安全技术评估包括漏洞扫描、渗透测试等，测试说明应阐述测试对象、测试范围、测试所用工具、测试环境、接入点选择以及测试过程保障等；测试结果应体现不同测试对象所发现的安全漏洞数量，可绘制表格统计；安全漏洞应根据 NVDB、CVE、CNVD、CNNVD 等漏洞库平台标注的漏洞级别进行风险等级判定；或者按照 GBT 30279-2020《信息安全技术 网络安全漏洞分类分级指南》对发现的漏洞进行风险等级判定；详细测试漏洞信息参见附录。

安全漏洞风险等级作为评估结论判定因素之一。

若由于用户原因无法开展验证测试，应将用户签章的“自愿放弃验证测试声明”作为报告附件。】

5.1 漏洞扫描

5.1.1 漏洞扫描测试说明

5.1.2 漏洞扫描测试结果

5.2 渗透测试

5.2.1 渗透测试测试说明

5.2.2 渗透测试测试结果

5.3 恶意代码扫描

5.4 ……

[可添加企业 logo]

报告编号：XXXXXXX

6 安全符合性评估得分

(1) 分数说明

分值划分：企业评分总分值为 100 分制，每类企业安全符合性评估算分均从技术、管理（含物理和环境）、数据三个维度进行，技术类总分为 50 分，管理类总分为 50 分。

(2) 权重分配

1) 设置指标项【权重】为λ，默认λ为 1；（具体权重在“安全符合性评估结果”中给出）

2) 将评估指标根据重要性分为一般项、重要项与关键项，三类指标的【权重】取值范围分别为：$0.5 \leqq \lambda < 1$、$\lambda = 1$、$1 < \lambda \leqq 2$；

3) 评估指标结果包括“符合”“部分符合”“不符合”“不适用”，其中，“符合”“部分符合”“不符合”对应评分分别为 100 分、50 分、0 分，“不适用”指标不参与分数计算。

(3) 公式计算

（1） 评估指标计算公式：

$$S_{技/管} = \frac{\sum_{i=1}^{M} Xi\,\lambda\,i}{\sum_{i=1}^{M} \lambda\,i}$$

其中，M 为指标个数，Xi 为指标得分，λ i 为指标对应的权重。

注：仅计算已评价的指标项，不适用指标不参与计算。

分别计算技术类总分 $S_{技}$、管理类总分 $S_{管}$，

$$S_{总}=0.5S_{技}+0.5S_{管}$$

[可添加企业 logo]

报告编号：XXXXXXX

7 安全风险分析

【填写说明：结合第“4 安全符合性评估结果”中的不符合项和部分符合项，按照《工业互联网企业网络安全分类分级评估方法》中风险判定操作方法进行风险分析，判断安全问题的风险等级“高风险”“中风险”“低风险”“可接受风险”

风险分析结果作为评估结论判定因素之一

以下段落为建议书写内容，评估单位可调整下述内容】

风险分析是根据安全问题的关联资产，以及资产已有安全措施，分析安全问题被利用的难易程度和安全问题导致安全事件产生影响的严重程度，判定安全问题的风险等级。

表：安全问题风险分析表

序号	问题描述	关联资产	被利用分析	利用等级	事件影响分析	影响等级	风险等级
1							高风险/中风险/低风险/可接受风险
2							
3							

[可添加企业 logo]

报告编号：XXXXXXX

8 综合评估结论

【填写说明：综合分析安全符合性评估得分与风险分析情结果，综合说明评估情况。】

[可添加企业 logo]

报告编号：XXXXXXX

9 安全问题整改建议

【填写说明：结合第“4 安全符合性评估结果”和“5 安全技术评估结果”中存在安全问题项和漏洞情况进行安全问题描述给出安全整改建议】

问题编号	安全类	问题描述	安全整改建议

附录 A：

此页为报告最后一页

参 考 文 献

[1]GB/T 19001 质量管理体系要求
[2]GB/T 41479-2022 信息安全技术 网络数据处理安全要求
[3]GB/T 42021-2022 工业互联网 总体网络架构
[4]《工业互联网安全分类分级管理办法（公开征求意见稿）》