ICS 35.030
CCS M10

团 体 标 准

T/CCSA 483.2—2024

工业互联网企业网络安全定级方法 第2部分：平台企业

Cybersecurity grading method of industrial internet enterprise
—Part2: Platform enterprise

2024－04－01 发布　　2024－06－01 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。

T/CCSA 483-2024《工业互联网企业网络安全定级方法》计划发布如下部分：

——工业互联网企业网络安全定级方法 第1部分：应用工业互联网的工业企业；

——工业互联网企业网络安全定级方法 第2部分：平台企业；

——工业互联网企业网络安全定级方法 第3部分：标识解析企业。

本文件是T/CCSA 483-2024《工业互联网企业网络安全定级方法》的第2部分。

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、卡奥斯物联科技股份有限公司、河钢数字技术股份有限公司、上海宝信软件股份有限公司、重庆忽米网络科技有限公司、中移（上海）信息通信科技有限公司、腾讯云计算（北京）有限责任公司、郑州信大捷安信息技术股份有限公司、北京天融信网络安全技术有限公司、江苏金恒信息科技股份有限公司。

本文件主要起草人：李诗婧、秦国英、董悦、柯皓仁、马娟、于盟、孙军、董良遇、张哲宇、王蕊、于广琛、张瑜、吴诗雨、张新硕、申蕾、王斌斌、江虹锋、周威、李俊鹏、刘为华、安高峰、李井先。

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。

本文件是工业互联网企业网络安全相关系列标准之一。T/CCSA 483-2024《工业互联网企业网络安全定级方法》标准作为工业和信息化部开展工业互联网企业网络安全分类分级管理工作的重要支撑，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，规定了不同的定级方法。由于文件的使用者需求不同，由三个部分构成。

——工业互联网企业网络安全定级方法 第 1 部分：应用工业互联网的工业企业。目的在于提出针对应用工业互联网的工业企业的网络安全级别定级方法；

——工业互联网企业网络安全定级方法 第 2 部分：平台企业。目的在于提出针对工业互联网平台企业的网络安全级别定级方法；

——工业互联网企业网络安全定级方法 第 3 部分：标识解析企业防护要求。目的在于提出针对标识解析企业的网络安全级别定级方法。

本文件为第2部分：平台企业，依据工业互联网企业网络安全分类分级管理文件，指导工业互联网平台企业开展网络安全的定级工作。从平台对所服务行业和领域的关联性影响、平台业务规模、平台业务能力、平台发生工业互联网网络安全事件的影响程度等四个方面，提出确定工业互联网平台企业安全级别的方法。为工业互联网平台企业按照工业互联网平台企业网络安全防护要求相关标准，落实与自身安全级别相适应的防护措施，提供基础性指引。

工业互联网企业网络安全定级方法
第2部分：平台企业

1 范围

本文件规定了工业互联网平台企业网络安全的定级方法，针对工业互联网平台企业给出定级要素及说明、评分规则等。

本文件主要适用于工业互联网企业网络安全分类分级管理工作，用于工业互联网平台企业开展自主定级。

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 42021 工业互联网 总体网络架构

3 术语和定义

GB/T 25069、GB/T 42021界定的术语和定义适用于本文件。

3.1

工业互联网 industrial internet

互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态，是工业智能化发展的关键综合信息基础设施。

[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、高效配置的工业云平台。

3.3

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。

4 缩略语

下列缩略语适用于本文件。

APP：应用程序（Application）

PB：拍字节（Petabytes）

5 概述

5.1 定级对象和目标

本规则适用的定级对象为工业互联网平台企业（简称平台企业），包括建设和运营工业互联网平台的企业。通过对平台企业进行安全级别划分，指导平台企业按照网络安全防护要求相关标准，落实与自身安全级别相适应的防护措施，加强平台企业的安全防护能力。

5.2 定级基本原则

同一平台企业建设或运营多个工业互联网平台，企业定级依照其建设或运营的平台中较高级别确定。同时具有联网工业企业、平台企业、标识解析企业中两种及以上属性的企业，应当按照不同类型分别定级。

6 工业互联网企业网络安全分级

6.1 定级流程

定级实施流程如图1所示，定级过程应包括以下内容。

a) 明确定级对象；

b) 对标定级对象，此阶段应明确以下要素：

1) 平台企业对所服务行业和领域的关联性影响；

2) 平台企业业务规模；

3) 平台企业业务能力；

4) 平台企业发生工业互联网网络安全事件的影响程度。

c) 根据级别划分规则确定企业级别。

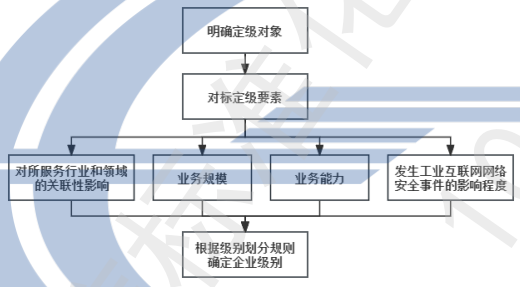

图1 定级实施流程图

6.2 定级要素

6.2.1 平台企业对所服务行业和领域的关联性影响

根据平台企业对所服务的行业网络安全影响程度，由高到低可划分为三类行业、二类行业和一类行业，工业互联网行业网络安全影响程度分类指导目录见附录A。平台企业对所服务行业和领域的关联性影响判定要素及赋值范围如表1所示。

注1：平台服务多个行业，按照服务行业网络安全影响程度的最高级别确定。

注2：如平台服务行业不在行业目录范围内，可参照此项指标自行评分。

表1 平台企业对所服务行业和领域的关联性影响判定要素及赋值表

判定要素	要素描述	赋值范围（本要素满分20分）
对所服务行业和领域的关联性影响	企业有.服务三类行业，或覆盖行业数量≥6个	[18,20]分
	企业有服务二类行业且无三类行业，或覆盖行业数量3至5个	[15,18)分
	企业只服务一类行业，且覆盖行业数量≤2个	[10,15)分

6.2.2 平台企业业务规模

根据平台企业服务用户的数量和工业设备连接数量，将平台企业业务规模分为大、中、小三级。平台企业业务规模判定要素及赋值范围如表2所示。

表2 平台企业业务规模判定要素及赋值表

判定要素	要素描述	赋值范围（本要素满分20分）
业务规模	规模大：用户数≥10万，或工业设备连接数≥100万	[28,30]分
	规模中：用户数＜10万，且10万≤工业设备连接数＜100万	[20,28)分
	规模小：用户数＜10万，且工业设备连接数＜10万	[10,20)分

6.2.3 平台企业业务能力

根据平台企业提供工业APP的数量和承载数据量，对平台企业业务能力进行评分，具体判定要素及赋值范围如表3所示。

表3 平台企业业务能力判定要素及赋值表

判定要素	要素描述	赋值范围（本要素满分20分）
业务能力	工业APP数量≥5000个，或承载数据量≥5PB	[18,20]分
	1000≤工业APP数量＜5000个，或2PB≤承载数据量＜5PB	[15,18)分
	工业APP数量＜1000个，且承载数据量＜2PB	[10,15)分

6.2.4 平台企业发生工业互联网网络安全事件的影响程度

根据发生工业互联网网络安全事件后，对企业生产运行、承载数据安全、社会秩序、经济运行、公共利益甚至国家安全的影响程度，分为重大影响、较大影响、一般影响、轻微影响，判定要素及赋值范围如表4所示。

注1：对于企业生产运行的影响程度：可以从造成生产中断和工业设施损毁程度、企业业务缩减量、企业年均交易额变化量或直接的经济损失大小、企业恢复正常运转的时间和经济代价等方面进行确定。

注2：对于企业平台承载数据安全的影响程度：可以从遭受攻击或间接破坏的关键数据和重要敏感信息的规模或占比、信息恢复周期和费用等方面进行确定。

注3：对于社会秩序、经济运行、公共利益、国家安全的影响程度：可以从对整个行业或国家的总体利益的侵害程度作为判定基准，包括社会影响的范围、深度等。

表4 平台企业发生工业互联网网络安全事件的影响程度判定要素及赋值表

判定要素	要素描述	赋值范围（本要素满分20分）
发生工业互联网网络安全事件的影响程度	重大影响：特别严重影响企业平台运行、造成大量数据资源丢失或被窃取、篡改、假冒，会对社会秩序、经济运行和公共利益造成严重损害，或对国家安全构成严重威胁。	[25，30]分
	较大影响：严重影响企业平台运行、造成较多数据资源丢失或被窃取、篡改、假冒，或对社会秩序、经济运行和公共利益造成较大损害，或对国家安全构成威胁。	[20，25)分
	一般影响：影响企业平台运行、造成较少数据资源丢失或被窃取、篡改、假冒，或对社会秩序、经济运行和公共利益造成较小损害，或对国家安全造成较小影响。	[15，20)分
	轻微影响：局部影响企业平台运行，造成少量数据资源丢失或被窃取、篡改、假冒，或对社会秩序、经济运行和公共利益造成轻微损害，不损害国家安全。	[10，15)分

6.3 级别划分

企业级别划分采用计分方式进行，对平台企业所服务行业和领域的关联性影响、业务能力、业务规模、发生工业互联网网络安全事件的影响程度等4个定级要素分别进行评分，总评分为4个定级要素分值之和，依据表5总评分和级别划分规则，将平台企业网络安全级别由高到低划分为三级、二级、一级。

注1：如平台企业服务的行业或企业，涉及重点监管的危险化工工艺、重点监管的危险化学品和危险化学品重大危险源之一的，至少认定为二级企业。

注2：如平台企业服务的行业或企业，同时涉及重点监管的危险化工工艺、重点监管的危险化学品和危险化学品重大危险源中两者及以上的，认定为三级企业（如：危险化学品重大危险源所涉及的危险化学品在重点监管目录中的，应认定为三级企业）。

表5 总评分和级别划分规则

	总评分划分区间	企业级别
划分规则	80≤总评分≤100	三级企业
	60≤总评分＜80	二级企业
	总评分＜60	一级企业

附 录 A
（规范性）
工业互联网行业网络安全影响程度分类指导目录

表A.1给出了工业互联网企业网络安全影响程度分类指导目录。

表A.1 工业互联网企业网络安全影响程度分类指导目录

序号	行业名称	行业门类及代码
三类行业		
1	钢铁	31 黑色金属冶炼和压延加工业
2	有色	32 有色金属冶炼和压延加工业
3	石化化工	25 石油、煤炭及其他燃料加工业 26 化学原料和化学制品制造业（除日用化学品制造）
4	轨道交通装备	371 铁路运输设备制造 372 城市轨道交通设备制造
5	船舶及海洋工程装备	373 船舶及相关装置制造
6	航空航天装备	374 航空、航天器及设备制造
二类行业		
7	建材	30 非金属矿物制品业（除玻璃制品制造、陶瓷制品制造）
8	废弃资源回收加工	42 废弃资源综合利用业
9	机械	33 金属制品业（除金属制日用品制造） 34 通用设备制造业 35 专用设备制造业 38 电气机械和器材制造业（除电池制造、家用电力器具制造、非电力家用器具制造、照明照具制造） 40 仪器仪表制造业 43 金属制品、机械和设备修理业
10	汽车	36 汽车制造业
11	其他运输设备	375 摩托车制造 377 助动车制造 378 非公路休闲车及零配件制造 379 潜水救捞及其他未列明运输设备制造
12	医药	27 医药制造业
13	电子设备制造	39 计算机、通信及其他电子设备制造业
一类行业		
14	轻工	16 烟草制品业 19 皮革、毛皮、羽毛及其制品和制鞋业 20 木材加工和木、竹、藤、棕、草制品业 21 家具制造业 22 造纸和纸制品业 23 印刷和记录媒介复制业 24 文教、工美、体育和娱乐用品制造业 29 橡胶和塑料制品业 268 日用化学产品制造 305 玻璃制品制造 307 陶瓷制品制造 338 金属制日用品制造 376 自行车和残疾人座车制造 384 电池制造 385 家用电力器具制造 386 非电力家用器具制造 387 照明照具制造 411 日用杂品制造
15	纺织	17 纺织业 18 纺织服装、服饰业 28 化学纤维制造业

表 A.1（续）

序号	行业名称	行业门类及代码
16	食品	13 农副食品加工 14 食品制造业 15 酒、饮料和精制茶制造业
注：分类依据《国民经济行业分类》（GB/T4754-2017）。不属于上述行业门类，但依据《关键信息基础设施安全保护条例》被认定为关键信息基础设施的重要行业领域的，例如公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等，参照三类行业执行。		

参 考 文 献

[1]GB/T 20986-2023 信息安全技术网络安全事件分类分级指南
[2]GB/T 20984-2022 信息安全技术 信息安全风险评估方法
[3]GB/T 4754-2017 国民经济行业分类
[4]AII/004-2018 工业互联网平台 安全防护要求
[5]工业互联网企业网络安全分类分级管理指南（试行）