

T/ZGCMCA

中国移动通信联合会团体标准

T/ZGCMCA 009—2025

工业互联网产品供应链安全评估规范

Assessment specifications for the security of industrial internet product supply chains

2025 - 06 - 25 发布

2025 - 06 - 25 实施

中国移动通信联合会 发布

目 次

前 言 II

1 范围 3

2 规范性引用文件 3

3 术语和定义 3

4 技术要求 5

 4.1 总则 5

 4.2 通用硬件和基础软件 5

 4.3 专用硬件 5

 4.4 嵌入式软件、应用软件和云计算软件 6

5 测评方法 8

 5.1 通用硬件和基础软件 8

 5.2 专用硬件 9

 5.3 嵌入式软件、应用软件和云计算软件 9

 5.4 产品评级规则 10

参 考 文 献 12

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。

本文件由中国移动通信联合会提出并归口。

本标准起草单位：中国工业互联网研究院（工业和信息化部密码应用研究中心）、南方电网科学研究院有限责任公司、西安热工研究院有限公司、安徽继远检验检测技术有限公司、麒麟软件有限公司、软安科技有限公司、兴唐通信科技有限公司、北京东土科技股份有限公司、内蒙古电力（集团）有限责任公司内蒙古电力科学分院、湖北工程职业学院、北京迪力科技有限责任公司、中电科金仓（北京）科技股份有限公司、北京国科环宇科技股份有限公司、上海兆芯集成电路股份有限公司、飞腾信息技术有限公司、中国信息通信研究院、国家工业信息安全发展研究中心、广东省科学院认证有限公司、国网电力科学研究院有限公司、三峡科技有限责任公司、中国石油国际勘探开发有限公司、国网安徽省电力有限公司电力科学研究院、中核武汉核电运行技术股份有限公司、天津市工业和信息化研究院、中国质量认证中心有限公司杭州分公司、先进操作系统创新中心（天津）有限公司、北京凝思软件股份有限公司、浪潮云洲工业互联网有限公司、树根互联股份有限公司、曙光网络科技有限公司、深圳华龙讯达信息技术股份有限公司、联通数字科技有限公司、南京治煜信息科技有限公司、北京鲲鹏联合创新中心有限公司、深圳市三旺通信股份有限公司、北京信尔泰科技股份有限公司、英韧科技股份有限公司、广东云徙智能科技有限公司、宸轩中消检测服务（北京）有限公司、北京中标政联科技有限公司、中标政联标准化技术服务（北京）有限公司、北京计算机技术及应用研究所。

本标准主要起草人：刘如才、郑若楠、薛强、杨春燕、王文庆、靳鑫、张衍顺、谢春刚、高华洁、程远、李勇、鲁捷、邵冬雪、叶慈聪、李壮、张伟、王迥波、刘楠楠、邹俊斌、温树峰、张松、李晓雄、顾广宇、郑明、洪达啸、高巍、李晨斌、靳先奇、巩云雷、雷宇、龙小昂、王思禹、洪中、方田、阳桂林、杜松、杨玉丰、郑成龙、王晓琳、程海艳、于双、刘杰、王辰菲、刘志立、梁继明、刘晓宇。

工业互联网产品供应链安全评估规范

1 范围

本文件规定了工业互联网产品供应链安全要求。

本文件适用于指导开发方、用户方以及第三方等相关组织对工业互联网产品开展供应链安全测试评估工作。

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。

- SJ/T 11939—2024 安全可靠 集中式事务型数据库技术要求
- SJ/T 11938—2024 安全可靠 分布式事务型数据库技术要求
- SJ/T 11937—2024 安全可靠 微型计算机操作系统技术要求
- SJ/T 11936—2024 安全可靠 服务器操作系统技术要求
- SJ/T 11941—2024 安全可靠 服务器技术要求
- SJ/T 11944—2024 安全可靠 一体式台式微型计算机技术要求
- SJ/T 11943—2024 安全可靠 台式微型计算机技术要求
- SJ/T 11942—2024 安全可靠 工作站技术要求
- SJ/T 11940—2024 安全可靠 便携式微型计算机技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业互联网产品 industrial internet product

工业互联网产品是指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产品，支撑工业互联网网络、标识、平台、数据、安全五大功能体系，包括新型工业网络、工业软件、工业操作系统等。根据产品形态，工业互联网产品可划分为通用硬件、基础软件、运行于通用硬件和基础软件环境的应用软件和云计算软件产品、专用硬件及嵌入式软件组成的专用设备。

3.2

供应链安全评估 supply chain security assessment

评估需方和供方在开展工业互联网产品研发、交付、运维和废止等过程中出现的供应关系风险（例如：供应中断、功能受限、服务降级等）以及技术安全风险和知识产权风险（例如：软件漏洞、许可协议不合规等）。

[来源：GB/T 43698-2024，3.7，4，有修改]。

3.3

硬件 hardware

用于处理、存储或传送计算机程序或数据的物理设备。

注：包括通用硬件和专用硬件，通用硬件是指通用计算机系统所需物理设备（包括：服务器、工作站、台式微型计算机、一体式台式微型计算机、便携式微型计算机），专用硬件是指满足工业互联网特定目的或应用场景而设计的嵌入式系统所需物理设备。

[来源：GB/T 11457-2006，2.690，有修改]

3.4

基础软件 basic software

基础软件是指计算机系统中提供底层服务和功能的软件。本规范特指操作系统和数据库产品(包括:服务器操作系统、微型计算机操作系统、分布式事务型数据库、集中式事务型数据库)。

[来源: SJ/T 11936-2024, SJ/T 11937-2024, SJ/T 11938-2024, SJ/T 11939-2024]

3.5

应用软件 application software

设计用于实现用户的特定需要而非计算机本身问题的软件。

注: 包括通用硬件和基础软件环境下部署满足工业互联网场景需求的功能软件, 或介于功能软件与基础软件的中间件(例如: 容器、虚拟软件、消息中间件等)。

[来源: GB/T 11457-2006, 2.71, 有修改]

3.6

云计算软件 cloud computing software

云计算软件是通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的软件。

注: 包括应用能力类、基础设施能力类、平台能力类软件。

[来源: GB/T 32400-2015, 3.2.5, 有修改]

3.7

嵌入式系统 embedded system

置入应用对象内部, 起信息处理或控制作用的专用计算系统。

[来源: GB/T 22033-2017, 2.001]

3.8

嵌入式软件 embedded software

满足嵌入式系统应用环境特殊要求的软件。

注: 这些软件包括嵌入式应用软件和嵌入式系统软件。

[来源: GB/T 22033-2017, 2.004]

3.9

外部组件 external component

由供方以外的组织或人员开发的程序代码、文档或数据, 通常是由二进制程序文件或者源代码程序文件构成。

注: 外部组件包括软件中使用的开源组件和第三方组件。

[来源: GB/T 43698-2024, 3.11]

3.10

元器件 component

设备的组成部分, 在不丧失其特定功能的前提下不能再进行物理细分的最小单元。本规范主要是指组成工业互联网产品硬件设备的最小单元, 包括电气元件、机电元件、电子器件和其他元器件几大类。其中电气元件包括电阻、电容、电感、变压器、电线光缆、熔断器; 机电元件包括开关、电连接器、继电器、微特电机; 电子器件包括集成电路、光电子器件、半导体分立器件、传感器、晶振等; 其他元器件则包括电池、PCB板等。

[来源: GB/T 37963-2019, 3.1.6, 有修改]

3.11

元器件组件 component assemble

由两个或多个半导体分立器件的端子, 散热体和可能带有的其它元器件相连接, 并组装成具有一定电路功能的单元(例如硬盘、内存、网卡、电源、主板、其他模块等)。

[来源: GB/T 2900.32-1994, 2.3.43, 有修改]

3.12

代码自主率 code autonomy rate

软件中自主开发的代码占总代码的比例, 它反映了软件产品的自主创新能力和知识产权保护程度。

[来源: T/ISC 0043-2024, 3.4]

3.13

研制单位 development organization

专门从事工业互联网产品制品及成分研制的单位，其中包括主体研制单位和供应链单位。

注1：主体研制单位是指在产品研制活动中的主要参与者，是产品的技术责任单位。

注2：供应链单位是指在产品研制活动中的各环节（例如：设计、开发、制造、测试等）参与者。

4 技术要求

4.1 总则

工业互联网产品按照通用硬件、基础软件、专用硬件、嵌入式软件、应用软件、云计算软件维度分类，并依据不同技术要求开展供应链安全分级评估。

4.1.1 一级要求

属于基础替代级，初步实现关键元器件组件安全可控和软件成分的自主研发。此阶段产品实现了硬件和软件关键模块的自主替代，降低对外部技术的依赖，提升系统的自主可控能力。

4.1.2 二级要求

属于深化替代级，硬件中关键功能元器件和组件的安全可控比例显著提升，更多的软件核心功能模块实现自主研发。此阶段产品在硬件和软件层面都实现了较大幅度的自主替代，能够满足大部分应用场景的需求。

4.1.3 三级要求

属于核心自研级，硬件电子元器件及组件基本实现安全可控，软件核心算法和功能模块大部分自主研发。此阶段产品在硬件和软件关键层面实现了自主替代，能够为用户提供较为完整的解决方案。

4.1.4 四级要求

属于高度自主级，所有硬件组成均实现安全可控，软件核心功能模块高度自主研发。此阶段产品在硬件和软件层面均达到了高度的自主研发水平，能够替代进口产品满足各类应用场景的需求。

4.1.5 五级要求

属于全面替代级，所有硬件和软件均实现供应链安全可控，并通过实地考察。此阶段产品在生态构建、技术创新等方面引领行业发展，实现了全面自主可控。

4.2 通用硬件和基础软件

4.2.1 通用硬件

通用硬件应满足安全可靠要求如下：

- a) 服务器符合 SJ/T 11941—2024；
- b) 一体式台式微型计算机符合 SJ/T 11944—2024；
- c) 台式微型计算机应符合 SJ/T 11943—2024；
- d) 工作站符合 SJ/T 11942—2024；
- e) 便携式微型计算机符合 SJ/T 11940—2024。

4.2.2 基础软件

基础软件应满足安全可靠要求如下：

- a) 集中式事务型数据库符合 SJ/T 11939—2024；
- b) 分布式事务型数据库符合 SJ/T 11938—2024；
- c) 微型计算机操作系统符合 SJ/T 11937—2024；
- d) 服务器操作系统 SJ/T 11936—2024。

4.3 专用硬件

4.3.1 分级影响因素

专用硬件供应链安全应考虑以下几个影响因素：

- a) 样品实际信息；
- b) 产品研制单位三要素（注册地、投资比例、法定代表人）；
- c) 知识产权（如专利、商标、集成电路布图设计等）；
- d) 实地考察情况。

4.3.2 供应链安全要求

专用硬件应满足供应链安全要求：

- a) 样品整机、元器件组件（适用时）和元器件实际信息与设计内容相符；
- b) 整机及元器件组件（适用时）研制单位应满足表 1 所述的供应链安全分级要求；
- c) 关键功能元器件（如计算、存储、网络、电源、感应等关键功能器件，需根据产品应用场景评审确认）研制单位应满足表 1 所述的供应链安全分级要求；
- d) 除关键功能元器件外，其他元器件研制单位应满足表 1 所述的供应链安全分级要求；
- e) 整机及主板应不存在知识产权风险；
- f) 考察项目、人员、设备设施等应与实际情况相符。

表 1 专用硬件供应链安全分级要求

序号	审查内容	供应链安全等级					备注
		一级	二级	三级	四级	五级	
1	样品实际信息相符	√	√	√	√	√	——
2	整机主体研制单位	√	√	√	√	√	——
3	元器件组件主体研制单位	√	√	√	√	√	√：表示主体研制单位或供应链单位相关的注册地、投资比例、法定代表人信息符合安全可控要求
4	关键功能元器件主体研制单位	——	√	√	√	√	
5	关键功能元器件供应链单位	——	——	——	√	√	
6	其他元器件主体研制单位	——	——	√	√	√	
7	知识产权	——	——	——	——	√	√：表示不存在知识产权风险
8	实地考察	——	——	——	——	√	√：表示需考察项目、人员、设备设施等与实际情况相符

4.4 嵌入式软件、应用软件和云计算软件

4.4.1 分级影响因素

嵌入式软件、应用软件和云计算软件供应链安全应考虑以下几个影响因素：

- a) 研制单位三要素（注册地、投资比例、法定代表人）；
- b) 软件成分和外部组件供应链风险；
- c) 软件代码自主率；
- d) 代码漏洞和软件缺陷；
- e) 知识产权（如专利、商标、著作权等）；
- f) 软件在 4.2 或 4.3 环境下运行质量特性；
- g) 运行所依赖的第三方服务或软件供应链风险；
- h) 实地考察情况。

4.4.2 供应链安全要求

嵌入式软件、应用软件和云计算软件应满足供应链安全要求，包括：

- a) 软件代码研制单位应满足表 2 所述的供应链安全分级要求；
- b) 软件成分应满足供应连续性要求：
 - 1) 软件成分不存在开源许可合规风险；
 - 2) 使用的外部组件不应存在停止维护、长期未更新等供应中断风险；
- c) 不包含操作系统部分的代码自主率应符合供应链安全分级要求；
- d) 不存在已知代码漏洞和软件缺陷；
- e) 不存在知识产权风险；
- f) 嵌入式软件在配套专用硬件环境下运行正常，应符合表 3 规定的质量要求；
- g) 应用软件和云计算软件应在满足 4.2 要求下的通用硬件和基础软件环境运行正常，符合表 3 规定的质量要求；
- h) 软件运行所依赖的第三方服务或软件应不存在停止维护、长期未更新等供应中断风险；
- i) 考察项目、人员、设备设施等应与实际情况相符。

表 2 嵌入式软件、应用软件和云计算软件供应链安全分级要求

序号	审查内容	供应链安全等级					备注
		一级	二级	三级	四级	五级	
1	软件主体研制单位	√	√	√	√	√	√：表示主体研制单位或供应链单位相关的注册地、投资比例、法定代表人信息符合安全可控要求
2	软件供应链单位	——	——	——	√	√	√：表示不存在供应中断风险
3	外部组件供应链风险	——	——	——	√	√	√：不存在开源许可合规风险
4	软件成分开源许可合规风险	——	——	——	√	√	1. 自主率不考虑操作系统部分代码自主率； 2. 根据操作系统部分的供应链安全性做相应等级核减。
5	代码自主率（嵌入式软件）	不低于30%	不低于50%	不低于60%	不低于80%	不低于95%	
6	代码自主率（应用软件和云计算软件）	不低于30%	不低于50%	不低于60%	不低于80%	不低于95%	
7	代码漏洞和软件缺陷	——	——	——	不存在已知高危代码漏洞和软件缺陷	不存在已知代码漏洞和软件缺陷	
8	知识产权	——	——	——	√	√	√：不存在知识产权风险

9	软件质量特性 (嵌入式软件)	√	√	√	√	√	√：表示符合4.3要求的硬件环境下运行正常
10	软件质量特性 (应用软件和云计算软件)	在至少1种通用硬件环境下运行正常	在1种环境下运行正常	在多种环境下运行正常	在多种环境下运行正常	在多种环境下运行正常	本环境指符合4.2要求的软硬件环境
11	运行所依赖第三方服务或软件供应链风险	——	——	——	√	√	√：表示不存在供应中断风险
12	实地考察	——	——	——	——	考察项目、人员、设备设施等与实际情况相符	

表 3 嵌入式软件、应用软件和云计算软件质量要求

序号	类型	项目及要求	
1	功能性	功能完备性	应覆盖需求文档或产品说明中描述的所有功能
		功能正确性	应达到需求文档或产品说明描述的所需精度的正确结果
		功能适合性	功能应按照需求文档、产品说明和用户文档集中规定执行
2	性能效率	时间特性	响应时间、吞吐量应满足需求文档或产品说明中的要求
		资源利用性	CPU、内存、GPU 占用率等各项资源消耗应满足需求文档或产品说明中的要求
		容量	数据处理规模、并发用户数等容量应满足需求文档或产品说明中的要求
3	兼容性	互操作性	数据格式、数据交换协议、API 接口等应满足需求文档或产品说明中的要求
		共存性	应满足与需求文档或产品说明中指明的软件共存，可正常实现所有功能不对其它软件造成负面影响
4	可靠性	稳定性	一定时间内，正常操作情况下稳定运行，缺省 24 小时
		容错性	故障处理、边界条件处理、误操作处理等满足需求文档或产品说明中的要求
		易恢复性	在发生中断或失效时，产品或系统能够恢复直接受影响的数据并重建需求文档或产品说明中指明的系统状态。
5	维护性	软件架构模块化、软件编码质量、系统日志完整性、软件诊断和版本控制等应满足需求文档和产品说明中的要求	
6	易用性	软件界面可辨识性、易学性、易操作性和用户差错防御性等满足需求文档和产品说明中的要求	
7	信息安全性	包括数据加密、安全漏洞、权限控制、认证机制、数字签名、访问控制、审计控制、信息控制等	
8	可移植性	应能够有效适应不同的硬件、软件或者其他运行环境	

5 测评方法

5.1 通用硬件和基础软件

5.1.1 通用硬件

5.1.1.1 测评方法

委托方提供通用硬件样品，产品相关资料，依此开展测评。

5.1.1.2 预期结果

通用硬件符合SJ/T 11940——SJ/T 11944系列标准对应产品要求。

5.1.2 基础软件

5.1.2.1 测评方法

委托方提供基础软件样品，产品相关资料，依此开展测评。

5.1.2.2 预期结果

基础软件符合SJ/T 11936——SJ/T 11939系列标准对应产品要求。

5.2 专用硬件

委托方提供专用硬件整机样品并根据表1所述的供应链安全分级要求提供如下部分或全部资料：

- a) 产品功能、应用场景等基本信息；
- b) 整机、元器件组件、元器件清单及其研制单位信息；
- c) 知识产权资料；
- d) 主板电路版图；
- e) 元器件手册；
- f) 专用硬件样品；
- g) 诚信承诺书：
 - 1) 所提交内容的真实性、完整性承诺；
 - 2) 承诺拥有所送检样品的所有权利，不存在与第三方的产权纠纷。

5.2.1 测评方法

- a) 审查整机、主板是否存在知识产权风险；
- b) 审查整机、元器件组件研制单位是否满足表1所述的供应链安全分级要求；
- c) 根据产品基本信息评审确定关键功能元器件，并审查关键功能元器件研制单位是否满足表1所述的供应链安全分级要求；
- d) 拆机对照元器件手册、主板电路版图审查关键功能器件信息与样品是否相符；
- e) 根据元器件清单审查其他元器件相关研制单位满足表1所述的供应链安全分级要求；
- f) 实地考察（适用时）相关研制单位项目材料、人员配备情况、设备设施状况等材料。

5.2.2 预期结果

- a) 整机及主板不存在知识产权风险；
- b) 整机、元器件组件研制单位满足表1所述的供应链安全分级要求；
- c) 关键功能元器件研制单位满足表1所述的供应链安全分级要求；
- d) 关键功能元器件规格信息、提供资料信息、样品外观一致；
- e) 其他元器件研制单位满足表1所述的供应链安全分级要求；
- f) 实地考察（适用时）项目、人员、设备设施等与实际情况相符。

5.3 嵌入式软件、应用软件和云计算软件

委托方提供样品并根据表2所述的供应链安全分级要求提供如下部分或全部资料：

- a) 产品功能、应用场景等基本信息
- b) 需求文档、产品说明和用户文档集
- c) 代码研制单位信息
- d) 软件源代码，包含代码、配置文件等编译所需内容

- e) 软件知识产权资料
- f) 软件运行所需要的硬件和基础软件环境
- g) 软件运行所依赖的第三方服务或软件清单，包含名称、版本号、厂商、许可等信息
- h) 诚信承诺书：
 - 1) 所提交内容的真实性、完整性承诺；
 - 2) 承诺拥有所送检样品的所有权利，不存在与第三方的产权纠纷。

5.3.1 测评方法

- a) 审查代码研制单位是否满足表 2 所述的供应链安全分级要求；
- b) 通过软件成分分析系统对源代码进行测试：
 - 1) 检查软件成分的开源许可合规风险；
 - 2) 对外部组件进行更新维护情况分析；
 - 3) 对应用软件和云计算软件源代码自主率进行分析；
 - 4) 对嵌入式软件系统软件外的源代码自主率进行分析；
- c) 审查对嵌入式软件的系统软件成分（包括内核、库、服务等）及相关证明材料，查看自研情况；
- d) 通过安全工具扫描是否存在代码漏洞和软件缺陷；
- e) 审查是否存在软件知识产权风险；
- f) 审查软件运行所需要的硬件和基础软件环境是否满足 4.2 或 4.3 要求；
- g) 对软件质量特性进行测试，测试时至少满足功能性和稳定性要求，适用时性能效率、兼容性等其他测试可根据被测软件技术特点和适合性进行增删或裁剪，各质量特性的详细测试内容如表 3 所示。
- h) 审查软件运行所需第三方服务或软件是否存在供应中断风险；
- i) 实地考察（适用时）项目、人员、设备设施是否与实际情况相符。

5.3.2 预期结果

- a) 代码研制单位满足表 2 所述的供应链安全分级要求；
- b) 软件成分不存在开源许可合规风险，不存在停止维护或超过 6 个月未更新的外部组件，源代码自主率应满足表 2 所述的供应链安全分级要求；
- c) 嵌入式软件的系统软件基于国内商业版或超过 50%自研不做等级核减，采用国内开源社区版本做等级核减一级，采用国外开源社区版本做等级核减二级；
- d) 不存在已知代码漏洞和软件缺陷；
- e) 不存在知识产权风险；
- f) 软件运行所需要的硬件和基础软件环境满足 4.2 或 4.3 要求；
- g) 软件质量特性满足表 3 要求；
- h) 软件运行需要的第三方服务或软件不存在停止维护或超过 6 个月未更新情况；
- i) 实地考察（适用时）项目、人员、设备设施与实际情况相符。

5.4 产品评级规则

5.4.1 单一产品评级

依据表1和表2分别对专用硬件、嵌入式软件、应用软件和云计算软件进行符合性评级。

5.4.2 系统产品评级

5.4.2.1 分项得分计算方法

依据5.4.1测评结果，对组成嵌入式系统的专用硬件、嵌入式软件分别进行级别评分。

表 4 嵌入式系统各部分级别评分（单位：分）

	一级要求	二级要求	三级要求	四级要求	五级要求
--	------	------	------	------	------

专用硬件	60	70	80	90	100
嵌入式软件	60	70	80	90	100

5.4.2.2 系统产品得分计算方法

由专家评审确定构成嵌入式系统的专用硬件和嵌入式软件权重占比（邀请多位专家对软件和硬件部分的供应链安全重要性打分确定），并计算定量评价指标值：

$$T = \sum_{j=1}^n T_j \partial_j$$

式中：

T_j ——分项得分；

∂_j ——分项权重，取值为0-1之间。

5.4.2.3 评价得分分级

根据得分给出嵌入式系统整体得分分级：

表 5 嵌入式系统得分分级

指标值T (单位：分)	(70, 60]	(80, 70]	(90, 80]	(100, 90]	100
评级	一级	二级	三级	四级	五级

参 考 文 献

- [1] GB/T 2900.32-1994 电工术语 电力半导体器件
 - [2] GB/T 11457-2006 信息技术 软件工程术语
 - [3] GB/T 22033-2017 信息技术 嵌入式系统术语
 - [4] GB/T 25000.51-2016 系统与软件质量要求和评价（SQuare） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则
 - [5] GB/T 32400-2015 信息技术 云计算 概览与词汇
 - [6] GB/T 37963-2019 电子设备可靠性预计模型及数据手册
 - [7] GB/T 43698-2024 网络安全技术 软件供应链安全要求
 - [8] T/ISC 0043-2024 软件代码自主率测评方法
 - [9] 《工业互联网综合标准化体系建设指南(2021版)》
 - [10] 《工业互联网体系架构2.0》
-