

团 体 标 准

T/ CESA 1046—2019

工业 APP 分类分级和测评

Classification、grading and evaluation of industrial APP



2019 - 07 - 01 发布

2019 - 07 - 15 实施

中国电子工业标准化技术协会

发 布

目 次

前言..... II

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 工业 APP 基本特征..... 1

5 工业 APP 分类..... 1

6 工业 APP 命名规则..... 3

7 工业 APP 分级和测评..... 4

附录 A（规范性附录） 工业 APP 安全性等级的确定方法..... 155

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

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这些专利的责任。

本部分由中国电子技术标准化研究院提出。

本标准起草单位：中国电子技术标准化研究院、安世亚太科技股份有限公司、中国船舶重工集团公司第七〇二研究所、江苏极熵物联科技有限公司、苏州同元软控信息技术有限公司、国家应用软件产品质量监督检验中心、浙江中控技术股份有限公司、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、南京大学、山东道普测评技术有限公司、中国汽车技术研究中心有限公司、工业和信息化部电子第五研究所、潍坊北大青鸟华光照排有限公司、航天云网科技发展有限责任公司、上海浦东软件平台有限公司、浙江蓝卓工业互联网信息技术有限公司、南京慕测信息科技有限公司、智能云科信息科技有限公司、上海湃睿信息科技有限公司、海尔家电产业集团、北京汉信信息技术有限责任公司。

本标准主要起草人：刘潇健、张旸旸、于秀明、孟志华、田志峰、焦提兵、黄文君、王威、侯觅、陈振宇、周凡利、杨春立、韩明军、殷建民、侯庆坤、倪浩、张星星、韩庆良、俞海斌、周德营、黄晓昆、王刚、张朔、刘奇、刘增志、曾逢春、谭彰、孔令鹏、梁炬、郭小松、张晓、欧培培、邵进涛、李文鹏、房春荣、白欧、职亮亮、罗银、岑天哲、杨卓峰、于泉、窦德聃、徐天昊、戴勇、周长伦。

工业 APP 分类分级和测评

1 范围

本标准给出了工业APP基本特征、命名规则、分类分级和测评要求。

本标准适用于工业APP潜在需方选择合适的工业APP产品，也可为监管方、评价方提供认定和评价工业APP的依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 11457-2006 信息技术 软件工程术语

3 术语和定义

GB/T 11457-2006中界定的以及下列术语和定义适用于本文件。

3.1

工业应用软件(工业 APP) Industrial application

承载工业知识和经验（最佳实践），面向工业领域，解决研发设计、生产制造、运营维护、经营管理等场景中的特定业务需求的软件。

4 工业 APP 基本特征

4.1 特定性。工业 APP 应是承载了经过验证的工业知识和经验的软件。

4.2 适用性。工业 APP 应针对工业领域特有的业务场景和工业产品的应用场景，能解决特定工业业务问题。

4.3 独立性。工业 APP 应是独立可执行的软件，且软件输入、输出的数据和内容应符合应用需求。依托工业互联网平台或其他平台环境开发和部署的工业 APP，应能发布成为独立可执行的软件。

4.4 扩展性。与其他工业 APP 集成的工业 APP，应有完整的应用开发接口和说明文档，具备可移植性和应用扩展能力。

5 工业 APP 分类

5.1 概述

工业APP应从适用范围、业务环节、知识类型3个维度分别进行分类。

5.2 按照适用范围分类

5.2.1 按照适用范围，工业 APP 分为：

- a) 基础共性工业 APP，面向关键基础材料、核心基础零部件（元器件）、先进基础工艺、产业技术基础等“工业四基”领域的工业 APP，以各种基础的自然科学知识形成的工业 APP。该类工业 APP 在工业应用领域发挥着基础作用，适用范围广；
- b) 行业通用工业 APP，面向具体行业及其细分子行业的工业 APP，例如：汽车、航空航天、石油化工、机械制造、轻工家电、信息电子等，以各种行业通用知识形成的工业 APP。该类工业 APP 适用于特定行业，在行业相关的领域和活动中发挥作用；
- c) 企业专用工业 APP。基于企业专业技术、工程技术等形成的工业 APP。该类工业 APP 是企业核心竞争力，在企业内部发挥作用，适用范围有限。
- d) 其他工业 APP。

5.2.2 按适用范围分类的准则：

- a) 基础共性工业 APP，提供证明或说明，证实工业 APP 作用场景属于“工业四基”领域或基础自然科学领域，至少能在 3 个工业行业进行有效应用；
- b) 行业通用工业 APP，提供证明或说明，证实工业 APP 在特定行业中至少 3 家典型企业进行有效应用；
- c) 企业专用工业 APP，提供证明或说明，证实工业 APP 在特定企业进行有效应用。

5.3 按照业务环节分类

5.3.1 按照业务环节，工业 APP 分为：

- a) 研发设计工业 APP，包括：
 - 1) 产品设计类；
 - 2) 工艺流程设计类；
 - 3) 过程控制设计类；
 - 4) 产线设计与实现类；
 - 5) 仿真类；
 - 6) 试制试验类；
- b) 生产制造工业 APP，包括：
 - 1) 生产计划管理类；
 - 2) 生产作业管理类；
 - 3) 物料管理类；
 - 4) 设备管理类；
 - 5) 工装管理类；
 - 6) 质量管理类；
- c) 运维服务工业 APP，包括：
 - 1) 数据收集监控类；
 - 2) 预测性维护类；
 - 3) 应急处理类；
 - 4) 节能服务类；
 - 5) 健康评价类；

- 6) 售后服务类;
- d) 经营管理工业 APP, 包括:
 - 1) 采购管理类;
 - 2) 产业链协同类;
 - 3) 风险管控类;
 - 4) 销售管理类;
 - 5) 物流管理类;
 - 6) 安全管理类;
 - 7) 认证管理类;
 - 8) 项目管理类;
 - 9) 人才管理类;
 - 10) 组织管理类;
 - 11) 辅助决策类;
 - 12) 企业资产类;
 - 13) 过程优化类。

5.3.2 按业务环节分类的准则:

- a) 在进行分类时, 应提供说明或声明, 指明工业 APP 的类属;
- b) 在认定时, 应依据说明或声明, 结合应用和作用场景的应用情况, 进行分类判定, 特定工业 APP 根据应用和作用场景, 可覆盖多个业务环节类型。

5.4 按照知识类型分类

5.4.1 按照知识类型, 工业 APP 分为:

- a) 业务信息化类。面向企业各实际业务场景, 将业务管理规范、业务流程管控、业务信息流转等以信息化解决手段封装为工业 APP, 实现各项业务的信息化管理。例如, 实现生产制造、库存物流、设备维护等业务环节的基本信息化管理的工业 APP。
- b) 数据分析类。基于企业各业务环节中所产生数据的集成, 将数据挖掘、数据分析、数据处理等方法封装为工业 APP, 实现以数据支撑业务管理与决策优化。例如, 基于工业大数据、工业区块链、人工智能等技术, 实现智能化管控的工业 APP。
- c) 知识建模类。基于特定应用场景下, 将工业活动的运行规则、技术过程、工作原理、分析方法等知识、经验、诀窍, 构建成数学模型, 并进行软件化封装形成的工业 APP。例如, 碰撞分析工业 APP、发动机热分析计算工业 APP、大体积混凝土温度裂缝计算模型工业 APP 等。

5.4.2 按知识类型分类的准则:

- a) 在进行分类时, 应提供说明或声明, 指明工业 APP 的类属;
- b) 在认定时, 应依据说明或声明, 结合所应用的信息技术手段、作用场景、解决工业问题的方式, 进行分类判定, 特定工业 APP 根据应用和作用场景, 可覆盖多个知识类型。

6 工业 APP 命名规则

6.1 工业 APP 名称构成:

适用领域+业务环节+功能用途+“软件”或“工业 APP”或“APP”。

6.2 工业 APP 的名称应满足如下要求：

- a) “适用领域”字段明确工业 APP 适用的范围或作用的工业产品；
 - b) “业务环节”字段明确工业 APP 作用的业务环节类型，见 5.3.1；
 - c) 工业 APP 的名称应与实际功能相吻合；
 - d) 除外销品外，工业 APP 的名称应包含中文，且能清楚表述其功能用途；
 - e) 工业 APP 名称的长度不应超过 40 个英文字符/ASCII 码字符；
- 注：一个汉字对应两个英文字符。
- f) 字段间可用“-”间隔；
 - g) 工业 APP 名称不应侵犯他人权利，包括但不限于著作权、商标权、名誉权；
 - h) 工业 APP 名称不应含有绝对性、宣传性的描述，如“官方”、“精品”、“唯一”、“最”等；
 - i) 工业 APP 不应包含使用频率较少且难以直接输入的符号，包括但不限于专业符号、图文符号、箭头符号、特殊文字、乱码。

7 工业 APP 分级和测评

7.1 概述

工业APP产品同时具有工业产品的属性和软件产品的属性，7.3.1-7.3.6给出工业APP产品作为工业产品的产品要求，考虑工业APP产品解决工业问题的能力以及所封装的工业知识的要求。7.3.7-7.3.19中给出工业APP产品作为软件产品的产品要求，其中7.3.7-7.3.15用于评价工业APP产品作为软件本身的能力；7.3.16-7.3.19用于评价工业APP产品在使用过程中呈现的软件能力。

工业APP产品要求共分五级指标，工业APP应用价值和质量从一级到五级逐级递增。

7.2 工业 APP 测评和分级方法

7.2.1 工业 APP 安全等级的确定

工业APP应用的业务场景决定其在安全性、可靠性等方面的特殊要求。本标准通过安全等级标识工业APP应用过程中可能存在的危险和风险。工业APP安全等级的确定方法见附录A。

工业APP安全等级是确定测评范围的依据之一。本标准针对安全性等级为A或B的工业APP提出了更高的测评要求，见7.3.7、7.3.8、7.3.12、7.3.13、7.3.14。

在开展工业APP测评活动前，应首先确定工业APP的安全等级，并依据安全等级确定7.3.7、7.3.8、7.3.12、7.3.13、7.3.14的测试范围。

7.2.2 测评指标的确定

7.3.2、7.3.4、7.3.9、7.3.14、7.3.15、7.3.17、7.3.19为可选指标，可根据实际情况进行剪裁，并给出剪裁说明。若工业APP产品说明或用户文档等文件中涉及到相关声明，以及工业APP应用过程中涉及相关场景，则应将相应可选指标纳入测评范围。

除可选指标外，其他指标皆应纳入测评范围。

7.2.3 测评方法

针对 7.3.1-7.3.6 的测评主要基于所提供的相关说明阐述材料、应用验证报告、认证证明等，评估待测工业 APP 与各级指标要求的符合性；针对 7.3.7-7.3.15 的测评主要通过软件测试的方式，评估待

测工业 APP 与各级指标要求的符合性;针对 7.3.16-7.3.19 的测评主要通过相关应用报告、用户证明等,评估待测工业 APP 与各级指标要求的符合性。

7.2.4 分级方法

本标准采用由低到高逐级评定的方式,应在满足全部低级指标要求的基础上开展高一级指标的测评。

工业APP需完全符合某级的全部待评指标要求才能被评定为该级。

若某级中存在不符合指标要求的情况,应降级评定。

7.3 工业 APP 产品要求和分级测评表

工业APP产品要求及各级别的测评指标,见表1。



表 1 工业 APP 分级测评表

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
7.3.1 应用范围	<input type="checkbox"/> 解决一般性信息化问题	<input type="checkbox"/> 解决特定企业内关键技术问题或重点问题，不具备行业共性	<input type="checkbox"/> 解决行业共性技术问题，适用于本行业大部分企业	<input type="checkbox"/> 解决行业共性关键技术问题或重点问题	<input type="checkbox"/> 解决技术革新或产业革命所需的重大问题
7.3.2 所解决工业问题的影响范围	<input type="checkbox"/> 无要求	<input type="checkbox"/> 所解决的工业问题影响范围较小，属于单元级问题	<input type="checkbox"/> 所解决的工业问题影响范围较大，属于系统级问题	<input type="checkbox"/> 符合三级要求	<input type="checkbox"/> 所解决的工业问题影响范围涉及多个系统，属于复杂系统级问题
7.3.3 先进性程度	<input type="checkbox"/> 能够重现同类传统工业软件的功能	<input type="checkbox"/> 与国内同类产品相比具有一定功能或性能方面的改善	<input type="checkbox"/> 与国内同类产品相比具有明显的先进性	<input type="checkbox"/> 可局部替代国外同类产品	<input type="checkbox"/> 达到或完全超越国外相关产品，能够促进技术革新或产业升级，实现技术的更新换代
7.3.4 工业知识的创新性	<input type="checkbox"/> 自证明能够解决工业问题	<input type="checkbox"/> 提供相关企业或单位证明，证明包含创新点	<input type="checkbox"/> 通过提供国内相关机构的认证、证明（如查新报告、专利等），证明具有重要或显著的创新点	<input type="checkbox"/> 通过提供国内相关机构的认证、证明（如查新报告、专利等），证明达到国内领先水平	<input type="checkbox"/> 通过提供国际相关机构的认证、证明或国际同行业认可，证明达到国际领先水平

表1 (续)

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
7.3.5 应用验证情况	<input type="checkbox"/> 通过提供验证方法说明、测试报告等材料，自证明工业知识经过了基本的试算或测试验证	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 通过提供企业实践应用报告等材料，证明工业知识经过了少量的实践验证 <input type="checkbox"/> 应用报告应详细阐述工业问题的解决程度和效率、结果的精确性和可靠性等情况	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 通过提供实际用户应用报告等材料，证明工业知识在实际业务场景中经过了实践验证 <input type="checkbox"/> 应用报告应有具体历史数据或详细案例作为支撑	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 通过提供专业的认证（如行业协会、主管部门、权威机构）或企业应用报告等材料，证明工业知识得到国内同行业普遍认可 <input type="checkbox"/> 对所使用的验证方法和评价体系及其科学性应进行说明	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 通过提供专业的认证（如行业协会、主管部门、权威机构）或应用报告等材料，证明工业知识得到国际同行业普遍认可
7.3.6 知识产权	<input type="checkbox"/> 无要求	<input type="checkbox"/> 提供说明或证明材料，证明具有工业知识的使用权或采用公开的知识	<input type="checkbox"/> 提供说明或证明材料，证明具有部分知识产权	<input type="checkbox"/> 提供说明或证明材料，证明具有完全知识产权	<input type="checkbox"/> 符合四级要求
7.3.7 产品文档	<input type="checkbox"/> 有相应的产品说明和用户文档集 <input type="checkbox"/> 明确陈述所有功能以及最终用户能调用的所有功能 <input type="checkbox"/> 明确陈述工业APP针对的问题域，以及具体技术指标	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 产品说明和用户文档应至少阐明功能性、性能效率、有效性等运行应用工业APP所必须的信息，及潜在需方所需了解的其他信息	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 产品说明和用户文档应详细说明工业APP功能性、性能效率、兼容性、易用性、可靠性、信息安全性、维护性、可移植性、有效性、使用效率、	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 文档化所有关键模块在软件结构中的位置、功能、约束、接口等 <input type="checkbox"/> 给出必要的数据库备份和恢复指南	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 文档化所有模块间的功能接口、数据接口等 <input type="checkbox"/> 明确所有的关键数据，及其访问控制属性和安全防护措施

表1 (续)

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
	<input type="checkbox"/> 应对相关法律、法规等规范性文件中的必要功能进行说明	<input type="checkbox"/> 针对安全等级为A或B级的工业APP, 产品说明和用户文档应详细说明工业APP功能性、性能效率、兼容性易用性、可靠性、信息安全性、维护性、可移植性、有效性、使用效率、满意度、抗风险等质量特性, 并明确说明可能存在的风险	满意度、抗风险等质量特性 注: 允许质量特性的剪裁, 但需在文档中进行剪裁说明。 <input type="checkbox"/> 明确说明可能存在的风险, 及所有有风险的功能		
7.3.8 功能性	<input type="checkbox"/> 提供说明或证明材料, 证明工业 APP 的功能性特征与产品说明和用户文档集的表述一致 <input type="checkbox"/> 在给定的限制范围内, 使用相应的环境设施、器材和数据, 工业 APP 应能正确安装, 并且所有功能是可执行的 <input type="checkbox"/> 工业 APP 的功能应是一致且不自相矛盾的	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 工业 APP 的功能设计应与使用目的相协调, 应符合实际使用要求 <input type="checkbox"/> 用户对工业 APP 进行的控制与软件的行为应是一致的 注: 两种完全相同的动作应产生同样的结果。 <input type="checkbox"/> 工业 APP 不应存在功能缺失和严重的功能缺陷	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 提供权威测试机构出具的测评报告, 证明各指标的符合性 <input type="checkbox"/> 针对安全等级为 A 或 B 的工业 APP 应明确哪些模块、类等将实现关键需求, 并将关键的模块与非关键模块隔开	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 应有独立模块负责工业 APP 的安全问题, 并作为关键模块与其他模块隔开	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 为每个关键模块实现差错检测和恢复功能 <input type="checkbox"/> 关键模块之间的接口应实现最小交互

表1 (续)

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
7.3.9 性能效率	<input type="checkbox"/> 提供说明或证明材料,证明工业 APP 的性能效率特征与产品说明和用户文档集的表述一致	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 工业 APP 应满足规定的余量要求,一般要求应有不少于 20%的余量	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 提供权威测试机构出具的测评报告,证明各指标的符合性	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 工业APP关键性能指标和关键功能的余量要求应在最大预期的2倍以上	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 提供证明材料,证明工业 APP性能效率领先于同类产品
7.3.10 兼容性	<input type="checkbox"/> 提供说明或证明材料,证明工业 APP 的兼容性特征与产品说明和用户文档集的表述一致 <input type="checkbox"/> 工业 APP 应能与需要交互的软件或资源进行正确的交互	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 工业 APP 应能与需要同时运行的软件共存	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 提供权威测试机构出具的测评报告,证明各指标的符合性 <input type="checkbox"/> 工业 APP 应能与通用的软件共存	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 软件应能识别出哪个组件负责兼容性	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 提供说明或证明材料,证明工业 APP 提供良好的接口,可与多种环境、多个工业互联网平台或多种类型的工业软件实现互联互通互操作
7.3.11 易用性	<input type="checkbox"/> 提供说明或证明材料,证明工业 APP 的易用性特征与产品说明和用户文档集的表述一致 <input type="checkbox"/> 在看到产品说明或者第一次使用后,用户应能确认产品或系统是否符合其需要	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 借助用户接口、帮助功能或用户文档集提供的手段,最终用户应能够学习如何使用某一功能 <input type="checkbox"/> 有关工业 APP 执行的各种问题、消息、屏幕输入格式、报表、输出和结果等应	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 提供权威测试机构出具的测评报告,证明各指标的符合性 <input type="checkbox"/> 当执行某一功能时,若响应时间超出通常预期限度,应告知所处状态	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 对具有严重后果的功能执行应是可撤销的,或者给出这种后果的明显警告,并且在这种命令执行前要求确认 注: 涉及人身安全、生产安全、重大经济风险、重要数据的删除和盖写以及中断一个	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 工业 APP 应能够提供一定的定制性功能 <input type="checkbox"/> 工业 APP 的交互接口应有误操作防护功能和报警功能

表1 (续)

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
		<p>是清晰且易理解的</p> <p>注：借助以下的手段可以达到易理解性：</p> <ul style="list-style-type: none"> — 恰当地选择术语； — 图形表示； — 提供背景信息； — 由帮助功能解释； — 提供易理解的文字或图形输出； — 提供清晰的音频输出 	<input type="checkbox"/> 相同功能的元素应具有一致的外观	<p>很长的处理操作均具有严重的后果。</p> <p><input type="checkbox"/> 提供说明或证明材料，证明工业 APP 易于安装、简单易用</p>	
7.3.12 可靠性	<input type="checkbox"/> 提供说明或证明材料，证明工业 APP 的可靠性特征与产品说明和用户文档集的表述一致	<p><input type="checkbox"/> 符合一级要求</p> <p><input type="checkbox"/> 在限制范围内使用工业 APP 时，不应存在丢失数据的情况</p> <p>注：该要求即使在下面的情况下也要满足：</p> <ul style="list-style-type: none"> — 利用的容量达到规定的极限； — 试图利用超出规定极限的容量； — 由产品说明中列出的其 	<p><input type="checkbox"/> 符合二级要求</p> <p><input type="checkbox"/> 提供权威测试机构出具的测评报告，证明各指标的符合性</p> <p><input type="checkbox"/> 工业APP应能够识别违反句法条件的输入，并且不作为许可的输入加以处理</p> <p><input type="checkbox"/> 针对安全性等级为 A 或 B 的工业 APP，应有容错和容失效设计</p>	<p><input type="checkbox"/> 符合三级要求</p> <p><input type="checkbox"/> 工业 APP 应具有从致命性错误中恢复的能力，并对用户是明显易懂的</p> <p><input type="checkbox"/> 工业APP应有容错和容失效设计</p> <p><input type="checkbox"/> 针对安全性等级为A或B的工业APP，应建立故障封锁区，以防止软件故障的传播</p>	<p><input type="checkbox"/> 符合四级要求</p> <p><input type="checkbox"/> 工业 APP 的关键模块应实现独立的并行冗余</p>

表1（续）

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
		他软件或由最终用户所造成的不正确输入； 一 违背用户文档集中明示的细则	<input type="checkbox"/> 针对安全性等级为 A 或 B 的工业 APP，关键模块应实现独立的并行冗余		
7.3.13 信息安全性	<input type="checkbox"/> 提供说明或证明材料，证明工业 APP 的信息安全性特征与产品说明和用户文档集的表述一致	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 工业 APP 应能防止对程序和数据的未授权访问（不管是无意的还是故意的） <input type="checkbox"/> 工业 APP 应能按照信息安全要求，对访问权限进行管理 <input type="checkbox"/> 工业 APP 应能对保密数据进行保护，只允许授权用户访问	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 提供权威测试机构出具的测评报告，证明各指标的符合性	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 工业 APP 应能识别出对结构数据库或文件完整性产生损害的事件，且能阻止该事件，并通报给授权用户 <input type="checkbox"/> 针对安全关键等级为 A 或 B 的工业 APP，安全关键点应有因子认证的方式	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 在工业 APP 所有关键模块出入口上实现对关键数据信息安全检查和保护
7.3.14 维护性	<input type="checkbox"/> 提供说明或证明材料，证明工业 APP 的维护性特征与产品说明和用户文档集的表述一致	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 每个模块应有头部注释，至少包含模块的名称、功能、输入输出、参数、调用方法等	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 提供权威测试机构出具的测评报告，证明各指标的符合性 <input type="checkbox"/> 应能识别出每一个基本	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 应能在任何时候都能识别出每一个基本组件的发布号，包括安装的版本，以及对软件特征产生的影响	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 对于高级语言实现的模块，每个模块的代码原则上控制在 200 行以内 <input type="checkbox"/> 每个模块所传递的参数个

表1 (续)

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
		<input type="checkbox"/> 针对安全关键等级为 A 或 B 的工业 APP, 每个模块的圈复杂度一般不大于 10, 扇入扇出一般不大于 7	组件的发布号、相关的质量特性、参数和数据模型 注: 基本组件可能是: — 数据屏幕; — 数据库模型; — 子程序; — 接口。 <input type="checkbox"/> 人工编写的源代码中有效注释的行数一般不得少于源程序行数的 20%	注1: 基本组件可能是: — 数据屏幕; — 数据库模型; — 子程序; — 接口。 <input type="checkbox"/> 每个模块的圈复杂度原则上不大于10, 扇入扇出原则上不大于7 注2: 该指标为参考值, 圈复杂度和扇入扇出与业务逻辑相关, 测评时需具体分析	数原则上不超过6个
7.3.15 可移植	<input type="checkbox"/> 提供说明或证明材料, 证明工业 APP 的可移植性特征与产品说明和用户文档集的表述一致	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 工业 APP 应向用户提供在特定环境下, 安装部署和卸载所有已安装组件的方法 <input type="checkbox"/> 工业 APP 应能在所有指定的环境中成功安装和正确运行	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 提供权威测试机构出具的测评报告, 证明各指标的符合性 <input type="checkbox"/> 工业 APP 能够方便的实现新旧版本的替换	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 工业 APP 应具有内部能力 (例如屏幕域、表、事务量、报告格式等) 的可伸缩性 <input type="checkbox"/> 工业 APP 能够方便的实现指定环境间的业务和数据迁移	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 提供说明或证明材料, 证明工业APP具有多种环境、多个工业互联网平台的部署运行的能力

表1（续）

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
7.3.16 经济和社会效益	<input type="checkbox"/> 提供说明或证明材料，证明工业 APP 的使用有效性特征与产品说明和用户文档集的表述一致	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 提供说明或证明材料，证明工业 APP 期望的业务目标基本实现	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 提供说明或证明材料，证明工业 APP 期望的业务目标实现良好	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 提供说明或证明材料，证明工业APP能够带来明显的经济或社会效益	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 提供说明或证明材料，证明工业 APP 有效地促进了技术革新、模式创新或经济效益的重大提升
7.3.17 费效比	<input type="checkbox"/> 提供说明或证明材料，证明工业 APP 的使用效率特征与产品说明和用户文档集的表述一致	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 提供说明或证明材料，证明工业 APP 在实现业务目标的前提下，安装、部署、使用、维护、培训等过程中的资源消耗在可接受范围内 注：资源包括人力成本、经济成本、环境成本等	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 提供说明或证明材料，证明工业 APP 在实现业务目标的前提下，资源消耗优于预期	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 提供说明或证明材料，证明工业APP在实现业务目标的前提下，资源消耗明显优于预期	<input type="checkbox"/> 符合四级要求
7.3.18 客户满意度	<input type="checkbox"/> 提供说明或证明材料，证明工业 APP 的满意度特征与产品说明和用户文档集的表述一致	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 通过满意度调查问卷，证明客户满意度 <input type="checkbox"/> 满意度调查问卷设计的问题内容全面、指标合理。	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 满意度调查的对象应具有代表性 <input type="checkbox"/> 80%及以上的调查对象的问题	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 满意度调查的对象应覆盖大多数客户 <input type="checkbox"/> 80%及以上的调查对象的问题	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 满意度调查的对象应覆盖所有客户 <input type="checkbox"/> 80%及以上的调查对象的问题

表1（续）

工业APP产品要求	一级要求	二级要求	三级要求	四级要求	五级要求
		满意度调查指标一般分为通用指标和技术指标，通用指标一般包括：易学性、易操作性、有效性、出错率、使用频度、价格等；技术指标一般根据实际业务场景进行设计。调查问卷的结论至少分为优、良、中、差4级	满意度达到“中”及以上水平	满意度达到“良”及以上水平 <input type="checkbox"/> 不存在评价为“差”的调查问卷	满意度达到“优” <input type="checkbox"/> 不存在评价为“差”的调查问卷
7.3.19 抗风险性	<input type="checkbox"/> 提供说明或证明材料，证明工业 APP 的抗风险特征与产品说明和用户文档集的表述一致	<input type="checkbox"/> 符合一级要求 <input type="checkbox"/> 提供说明或证明材料，证明工业 APP 已经过合理的验证	<input type="checkbox"/> 符合二级要求 <input type="checkbox"/> 对于所有有风险的功能，软件应提供特定的确认过程和管理权限	<input type="checkbox"/> 符合三级要求 <input type="checkbox"/> 对于所有有风险的功能，软件应提供日志功能	<input type="checkbox"/> 符合四级要求 <input type="checkbox"/> 对于所有有风险的功能，软件应有审计、追踪、风险识别机制

附 录 A

（规范性附录）

工业 APP 安全性等级的确定方法

A.1 概述

确定工业APP安全等级的步骤主要包括：

- a) 采用初步危险分析（PHA）的方法，确定所在系统潜在的危险；
- b) 分析确定危险的严重性和可能性；
- c) 确定所在系统风险指标；
- d) 确定工业 APP 在系统中执行的控制类别；
- e) 确定工业 APP 安全性等级。

A.2 确定所在系统潜在危险

系统初步危险分析是系统中各层次开展危险分析的前提和基础，也是开展软件系统危险分析、确定工业APP安全等级的前提和基础。通过系统的初步危险分析，列出系统所有的潜在危险，包括危险的原因以及针对危险原因的危险控制等。

A.3 分析、确定潜在危险的严重性和可能性

危险的严重性和可能性主要基于过程的判断得到。危险的严重性可分为四级：灾难的、严重的、轻度的、轻微的，参见表A.1。危险可能性可分为五级：经常、很可能、偶然、很少、极少，参见表A.2。

表 A.1 危险严重性等级定义

危险严重性等级	定 义
灾难的	人员死亡，或系统报废，或基本任务失败，或环境灾难。
严重的	人员严重伤害，或系统严重损坏，或基本任务的主要部分未完成，或环境严重破坏。
轻度的	人员轻度伤害，或系统轻度损坏，或对完成任务有轻度影响，或环境轻度破坏。
轻微的	对人员的伤害和系统的损坏轻于轻度，或虽然执行任务有障碍但是能够完成，或对环境的破坏可忽略
注：决定使命成败的任务为基本任务。	

表 A.2 危险可能性等级定义

危险可能性等级	定 义
经常	危险可能经常发生： $P > 10^{-1}$
很可能	在某一项的生存周期中危险将发生若干次： $10^{-2} < P \leq 10^{-1}$
偶然	在某一项的生存周期中危险可能偶尔发生： $10^{-3} < P \leq 10^{-2}$
很少	在某一项的生存周期中危险发生的可能很少： $10^{-4} < P \leq 10^{-3}$
极少	危险几乎不可能发生： $P \leq 10^{-4}$

表 A.2 (续)

危险可能性等级	定 义
注：P是危险发生的概率。针对不同系统，各级P值的划分可能有别。	

A.4 确定系统的风险指标

根据危险的严重性等级及其可能性等级，确定每种危险的系统风险指标，参见表A.3。

表 A.3 系统风险指标

危险严重等级	危险可能性				
	经常	很可能	偶然	很少	极少
灾难的	1	1	2	3	4
严重的	1	2	3	4	5
轻度的	2	3	4	5	6
轻微的	3	4	5	6	7
注：风险指标中的1表示最高系统风险，7表示最低系统风险。					

其中最高风险的危险（即系统风险指标为1）在系统分析与设计中是不允许存在的。如果存在，系统分析与设计就应重新进行。如果风险指标为6、7，通常可以不考虑安全性工作。

A.5 确定工业APP的控制类别

在系统危险分析的基础上开展软件系统的危险分析，以确定工业APP的控制类别。软件系统危险分析的目的是将与软件相关的风险以及与风险相关的软件标识出来。工业APP的控制类别与对系统的控制程度、控制的复杂性和实时性等有关。

工业APP的控制类别可分为四类：I、II、III、IV，参见表A.4。

表 A.4 工业 APP 的控制类型定义

工业 APP 控制类别	定 义	
I	1	工业 APP 对危险进行部分或全部的自主控制。
	2	包含多个子系统、交互作用的并行处理器或多个接口的复杂系统。
	3	有一些或全部安全关键功能是时间关键的。
II	1	控制危险，但是其他安全系统可以进行部分缓解；检测危险，需要采取安全措施时通知操作员。
	2	包含少量子系统和/或一些接口的中等复杂系统，无需并行处理。
	3	有一些危险控制动作可能是时间关键的，具有临界时间要求，但是不会超过中等熟练程度的操作员说需要的时间或自动系统响应时间。
III	1	若软件发生故障，则有一个或若干个缓解系统防止危险发生；或提供冗余的安全关键信息资源。
	2	稍微复杂的系统，仅包含有限数目的接口。
	3	缓解系统能在任何临界时间内进行相应。

表 A.4 (续)

工业 APP 控制类别	定 义	
IV	1	对危险无硬件控制，并不为操作员提供安全关键数据。
	2	仅带 2-3 个子系统的简单系统，仅包含少量接口。
	3	非时间关键，没有临界时间要求。
注：每个工业APP控制类别都有三种描述，他们之间是“或”的关系，即只要符合一种，就可以确定。		

A.6 确定工业APP的安全性等级

根据每个工业APP的控制类别和系统风险指标确定工业APP的安全性等级。软件安全性等级从高到低为A、B、C、D四个等级。参见表A.5。

表 A.5 工业 APP 安全性等级矩阵

工业 APP 控制类别	系统风险指标			
	2	3	4	5
I	A	B	C	D
II	B	C	D	D
III	C	D	D	D
IV	D	D	D	D

A.7 安全关键工业APP

安全性等级高的工业APP为安全关键软件。通常A、B级的软件为安全关键软件。