ICS 91.140.90
C 73

DB33

浙 江 省 地 方 标 准

DB33/T XXXXX—XXXX

产业大脑工业APP安全基本要求

Industrial brain Industrial APP security basic requirements

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

浙江省市场监督管理局　发布

目　次

前　言

本标准按照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》给出的规则起草。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由浙江省经济和信息化厅提出并归口。

本标准起草单位：

本标准主要起草人：

引　言

随着两化融合的逐步深入及工业互联网平台的逐步成型，传统的工业信息系统正在加快云化改造迁移，最终工业APP都将汇聚至工业互联网平台。数字经济系统建设是浙江省数字化改革的重要支柱，产业大脑是数字经济系统的核心业务组成部分。为深入贯彻落实浙江省数字化改革大会精神和省委、省政府决策部署，支撑数字经济领域改革，基于省产业大脑和“1+N”工业互联网平台体系，以及省委主要领导关于数字经济的重要指示和要求，组织编制本标准。

产业大脑工业 APP 安全基本要求

1 范围

本标准规定了工业APP安全防护与安全保障的技术要求和管理要求。

本标准适用于工业APP上线产业大脑时的安全性评估。

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 25069-2010 信息安全技术 术语

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1 产业大脑 Industrial brain

产业大脑是以工业互联网为支撑，以数据资源为核心，运用新一代信息技术，综合集成产业链、供应链、资金链、创新链，融合企业侧和政府侧，贯通生产端和消费端，为企业生产经营提供数字化赋能，为产业生态建设提供数字化服务，为经济治理提供数字化手段，是着力推动相关产业质量变革、效率变革、动力变革的集成开放赋能平台。

3.2 工业 APP Industrial Application

工业 APP 是基于松耦合、组件化、可重构、可重用思想，面向特定工业场景，解决具体的工业问题，基于平台的技术引擎、资源、模型和业务组件，将工业机理、技术、知识、算法与最佳工程实践按照系统化组织、模型化表达、可视化交互、场景化应用、生态化演进原则而形成的应用程序，是工业软件发展的一种新形态。

4 缩略语

下列缩略语适用于本文件：

APP　　应用软件（APPlication）

5 概述

产业大脑工业APP属于产业大脑总体架构中的数字经济应用部分。本标准从信息安全方面规范了上线产业大脑的工业APP的安全基本要求，包括技术要求和管理要求。技术要求包

括程序保护要求、身份认证要求、口令安全机制要求、访问控制要求、安全审计要求、数据安全要求、安装要求、卸载要求和升级要求，管理要求包括资质要求和上架要求。

6 技术要求

6.1 程序保护要求

a) 工业 APP 应不存在已公布的高风险安全漏洞,例如跨站脚本漏洞、注入类漏洞、文件上传漏洞、逻辑漏洞、反序列化漏洞、安全配置错误、不安全的第三方组件等。

6.2 身份认证要求

a) 工业 APP 应提供专用的登录控制模块对登录用户进行身份标识和鉴别,用户身份标识唯一，登录控制模块具有鉴别信息长度、复杂度检查、登录失败处理功能；
b) 工业 APP 用户身份认证应具备认证超时功能,当空闲时间超过设定时间应自动终止认证过程并进行重新认证；
c) 工业 APP 重要参数修改、配置下发等操作前应进行身份鉴别。

6.3 口令安全机制要求

a) 在使用过程中不应以明文形式显示和存储；
b) 修改或找回口令时，应具备验证机制，如短信验证、邮箱验证等。

6.4 访问控制要求

a) 用户访问的内容不应超出授权的范围（如管理后台向低权限用户开放）；
b) 应限制工业 APP 用户账户的多重并发会话；
c) 应支持用户权限分配和互斥机制。

6.5 安全审计要求

a) 工业 APP 应具有安全审计功能，审计覆盖工业 APP 中所有用户，对重要的用户行为和重要安全事件进行审计；
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，日志保存时间不少于六个月；
c) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，具有良好可读性。

6.6 数据安全要求

6.6.1 数据采集要求

a) 未向用户明示并经用户同意，工业 APP 不得收集用户工业数据,不得开启收集地理位置、读取通讯录、使用摄像头、启用录音等与服务无关的功能，不得捆绑安装应用无关的应用程序；
b) 应采用数据校验机制，对采集数据的完整性进行验证。

6.6.2 数据传输安全要求

a) 应采取技术手段保证重要数据在传输过程中的保密性；
b) 应采用技术手段保证重要数据在传输过程中的完整性。

6.6.3 数据存储安全要求

a) 应支持对重要数据的存储完整性校验；
b) 应对服务器中所存储的重要数据进行加密，对重要数据加密应当使用未曝出安全隐患的加密算法或采用符合国家密码管理局要求的加密算法；
c) 应对存储在服务器的重要数据提供互相隔离技术。

6.6.4 数据处理要求

a) 工业 APP 在处理重要数据前，应明确提示用户，并由用户再次确认是否处理该数据（如删除数据前，应明确提示用户，由用户再次确认是否删除数据）。

6.6.5 数据备份与恢复要求

a) 应提供用户有选择的备份重要数据的功能；
b) 应提供用户按自我信息备份所保留的信息进行数据恢复的功能。

6.6.6 数据销毁要求

a) 工业 APP 用户退出或关闭浏览器时，应清除在内存、硬盘等介质中非必需留存的数据（例如用户身份鉴别信息）；
b) 工业 APP 删除数据或注销用户后，服务端内存、硬盘等介质的文件系统中不应残留任何与用户相关的敏感信息。

6.7 安装要求

a) 应包含 APP 供应者或开发者的签名信息、软件属性信息（如名称、版本信息和描述等）；
b) 应提示用户对其使用的终端资源和终端数据进行确认。

6.8 卸载要求

a) 应完全删除其安装及使用生成的资源文件、配置文件和用户数据；
b) 应不影响承载平台其他应用的正常使用。

6.9 升级要求

a) 应提供软件的升级功能；
b) 应提供保证升级的时效性（如自动升级、更新通知等）和准确性（如完整性校验）的安全机制。

7 管理要求

7.1 资质要求

a) 由具有依法在境内设立的企事业法人资质的机构研发；

b) 拥有对该软件产品的完全知识产权，具有规范化的软件名称、完善的使用手册，并已通过评估登记；

c) 符合法律、行政法规规定的其他条件。

7.2 上线要求

a) 应通过行业产业大脑或工业 APP 创新中心等渠道上架；

b) 工业 APP 上架产业大脑前应由具备资质的第三方机构，依据本标准 6.技术要求条款进行规范化测评，并出具合格报告。

参考文献

[1] GB/T 20984-2007 信息安全技术 信息安全风险评估规范

[2] GB/T 25069-2010 信息安全技术 术语

[3] GB/T 28452-2012 信息安全技术 应用软件系统通用安全技术要求

[4] GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南

[5] GB/T 34975-2017 信息安全技术 移动智能终端应用软件安全技术要求和测试评价方法

[6] GB/T 25058-2019 信息安全技术 信息系统安全等级保护实施指南

[7] GB/T 28448-2019 信息安全技术 信息系统安全等级保护测评要求

[8] GB/T 35273-2020 信息安全技术 个人信息安全规范

[9] T / CESA1046-2019工业APP分类分级和测评

[10] 工业数据分类分级指南（试行），中华人民共和国工业和信息化部，2021年2月

[11] 工业APP白皮书(2020)，工业互联网产业联盟(Alliance of Industrial Internet)，2021年5月

[12] 产业大脑建设方案（试行），浙江省经济和信息化厅，2021年4月