ICS 35.240.50
CCS L 77

T/EJCCCSE

团　　体　　标　　准

T/EJCCCSE XXXX-XXXX

可信“智慧食安”工业物联网数字化管理平台

Reliable smart food fafety industrial internet of things digital management platform

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中国商业股份制企业经济联合会　发布

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。

本文件由浙江智飧科技有限公司提出。

本文件由中国商业股份制企业经济联合会归口。

本文件起草单位：浙江智飧科技有限公司、杭州玺湖科技有限公司、中厨环保科技（海南）有限公司、苏州工业园区唯亭万亚餐饮服务有限公司、广东吉嘉环保科技有限公司、苏州鸿本机械制造有限公司、江苏神工节能科技有限公司、嘉兴联飧科技有限公司、智康数字产业（海南）有限公司、南通中飧健康科技有限公司、南京维冠商显科技有限公司、苏州市和谐康工业设计有限公司、杭州水讯科技有限公司、江苏安信餐饮管理有限公司、苏州餐艺谋食安科技有限责任公司

本文件主要起草人：杨馥铭、杨镇蔚、高静雯、方金旗、姚春达、鄢中华、王东平、张建峰、顾加荣、徐磊、雷中华、雷保华、管图祥、李士雨、江彩、印德洲、朱建文

可信“智慧食安”工业物联网数字化管理平台

1 范围

本文件规定了可信“智慧食安”工业物联网数字化管理平台（以下简称“平台”）的基本要求、关键场景应用、建设要求、运行维护的要求。

本文件适用于研发、生产、部署和运营的智慧食品安全工业物联网数字化管理平台产品，包括但不限于食品生产、加工、存储、运输、销售等环节的监控和管理。

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 15629.3-2014 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第3部分：带碰撞检测的载波侦听多址访问（CSMA/CD）的访问方法和物理层规范

GB15629.11-2003 信息技术 系统间远程通信和信息交换局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第1号修改单

GB/T 18233.1-2022 信息技术 用户建筑群通用布缆 第1部分：通用要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 25068.5-2021 信息技术 安全技术 网络安全 第5部分：使用虚拟专用网的跨网通信安全保护

GB/T 28452-2012 信息安全技术 应用软件系统通用安全技术要求

GB/T 31240-2014 信息技术 用户建筑群布缆的路径和空间

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信“智慧食安”工业物联网数字化管理平台

指应用“互联网＋”理念，依托物联网、大数据、云计算、区块链、二维码溯源、边缘计算、AI识别、人工智能、电子取证等新一代移动互联网技术，通过传感器感知采集大量的数据为平台提供决策依据，实现全链智慧食安协管。

4 基本要求

4.1 基本原则

4.1.1 保真原则

平台应确保所有数据的真实性和完整性，通过先进的物联网、大数据、区块链等技术，防止数据在传输和存储过程中被篡改或损坏。

4.1.2 确权原则

4.1.2.1 平台应确保数据的合法使用和访问，对数据的来源和使用权进行明确的界定和记录。
4.1.2.2 确权机制应能有效防止数据滥用和非法访问并保障数据的安全性和合规性。

4.1.3 溯源原则

平台应确保食品来源的透明和可追溯性，通过二维码溯源等技术，实现对食品从生产、加工、存储、运输到销售的全程追溯。

4.2 一般要求

4.2.1 可信“智慧食安”工业物联网数字化管理平台框架应满足可集成、兼容主流系统、可扩展、容易维护、安全、系统稳定性和高可能性等性能要求。
4.2.2 可信“智慧食安”工业物联网数字化管理平台总体架构应由平台运行系统环境、数据存储、消息中间件、物联硬件监控、服务中心、业务应用层、API 接口、前端展示、接入终端搭建，打通数据流、信息流、业务流，实现企业安全生产全过程、全要素的连接和优化。
4.2.3 基于工业互联网平台，“工业互联网+食品安全生产”相关软件、硬件系统应能够相互兼容、有机融合，实现数据互联互通及业务集成。
4.2.4 可信“智慧食安”工业物联网数字化管理平台应支持多种通信协议接入（MQTT、HTTP、TCP、私有协议等），支持协议扩展，具备与企业其他系统之间安全、稳定传输各类数据的能力，同时可与上级及其他监管部门等进行数据的交换、汇聚和共享。
4.2.5 可信“智慧食安”工业物联网数字化管理平台应能实现数据的采集、清洗整合、存储、分析，为智能应用提供数据支持。数据可信可靠，真实、产权清晰、可追溯，保密和合规。

4.3 总体架构

4.3.1 平台架构

可信“智慧食安”工业物联网数字化管理平台总体架构应由运行环境、存储、中间件、硬件监控、服务中心、业务应用层、API 接口、前端展示、接入终端搭建，打通数据流、信息流、业务流，实现企业安全生产全过程、全要素的连接和优化。

4.3.2 运行环境层

4.3.2.1 应支持云服务器，并提供简单高效、安全可靠、处理能力可弹性伸缩的计算服务，快速构建更稳定、安全的应用，降低开发运维的难度和整体 IT 成本，包括但不限于阿里云、百度云、天翼云、华为云。
4.3.2.2 宜引入 JVM（Java Virtual Machine）Java 语言虚拟机，具备移植性、成熟、覆盖面等特性。
4.3.2.3
4.3.2.4 平台的网络基础宜基于网络技术建设， 网络设备、结构、布缆、组网等宜按 GB/T 15629.3-2014、 GB 15629.11-2003、 GB/T 18233.1-2022 和 GB/T 31240-2014 的规定执行。
4.3.2.5 安全体系架构宜按 GB/T 22239-2019 中第三级安全保护进行建设，并符合 GB/T 28448-2019 的要求 。
4.3.2.6 主机、存储和安全设备宜按 GB/T 25068.5-2021、GB/T 28452-2012 的规定执行。

4.3.3 存储层

存储层主要由redis缓存、数据库、文件服务器、流媒体服务器等组成。具体要求如下：

a) redis缓存：
   1) redis作为NoSQL数据库，包含多种数据结构、支持网络、基于内存、可选持久性的键值对存储数据库，其具备基于内存运行，性能高效、支持分布式，可以无限扩展、key-value存储系统等特性；
   2) 遵守BSD协议、支持网络、可基于内存亦可持久化的日志型、Key-Value数据库，并提供多种语言的API；
   3) Redis具备 C/S通信模型、单进程单线程模型、丰富的数据类型、操作具有原子性、持久化、高并发读写、支持lua脚本等特性。
b) 数据库：应由主库、从库、备库等保证信息的存储，不会因数据库的损坏，而导致无法运行；
c) 文件服务器：对文件进行管理，功能包括：文件存储、 文件同步、文件访问（文件上传、文件下载）等；
d) 流媒体服务器：适用于直播、录播、视频客服等多种场景，支持RTMP/HLS/FLV，高效、稳定、易用。

4.3.4 中间件

4.3.4.1 主要实现消息队列、Redis、负载均衡等功能。

4.3.4.2 应通过MQ架构设计，就可将紧急重要（需要立刻响应）的业务放到该调用方法中，响应要求不高的使用消息队列，放到MQ队列中，供消费者处理。

4.3.4.3 通过消息整合，大数据的背景下，消息队列还与实时处理架构整合，为数据处理提供性能支持。

4.3.4.4 Java消息服务（Java Message Service，JMS）应用程序接口是一个Java平台中关于面向消息中间件（MOM）的API，用于在两个应用程序之间，或分布式系统中发送消息，进行异步通信。

4.3.5 硬件监测层

通过对设备异构性进行封装,将设备看作无状态资源的访问方法,实现对物联网感知设备数据采集，历史数据查询，设备状态监控，设备数据展示等功能。

4.3.6 服务中心层

4.3.6.1 应能通过集群部署的方式解决服务的高并发访问和单节点故障问题。

4.3.6.2 应能通过特定的负载均衡（Load Balance）算法，将并发访问的请求，分发到不同节点的服务器进行处理，将每一台服务器的负载压力，实现负载均衡。

4.3.6.3 服务中心层宜采用微服务架构（Microservice Architecture），通过将功能分解到各个离散的服务中以实现对解决方案的解耦。

4.3.7 业务应用层

业务应用层中的组件应能提供具体的业务需求服务，业务应用主要包括：

—— 能力平台；
—— 数据处理系统；
—— 楼盘表系统；
—— 采集系统；
—— 权限管理中心；

——　报表中心；
——　配置中心；
——　任务调度中心；
——　日志中心；
——　消息中心；
——　全网搜索；
——　业务构件；
——　服务监控中心。

4.3.8　API 接口层

4.3.8.1　API 接口层应能为 PC 端应用、小程序、微信公众号、IOS、Android 等提供统一的接口。
4.3.8.2　API 接口层应能提供对用户登录态进行必要的检测、控制业务场景的主流程，创建领域业务实例，并进行调用、进行必要的日记纪录、返回接口结果。
4.3.8.3　API 接口层应能提供 API 管理，通过对 API 的设计、创建、测试、部署、集成、管理、运维、下线等全生命周期管理，进一步优化流程。

4.3.9　前端展示

前端展示层应能为 PC 端应用、小程序、微信公众号、IOS、Android、Web 网页端等展示。

4.3.10　接入终端搭建

接入设备应包括 PC、移动终端及相关物联网设备，其中物联网平台设备应包含但不限于：
——　智能体征晨检仪
——　智能体质检测秤；
——　智能工衣消毒柜；
——　智能阳光云秤；
——　智能全自动食品安全快速分析仪；
——　智能仓库恒温恒湿；
——　智能添加剂管控柜；
——　智能中心温度检测仪；
——　智能留样管控；
——　智能食用油温监测；
——　智能食用油品质检测仪；
——　专区智能温度监测；
——　智能行为分析告警器；
——　智能前置油烟处理器；
——　智能餐饮污水处理器；
——　智能紫外灯管控精灵；
——　智能瓦斯监控；
——　智能积水监控；
——　智能安全阀门管控；
——　智能油温在线监测；
——　智能水质监测器；
——　智能环境消毒管控；

——　智能多功能节能燃具；
——　智能餐厨垃圾处理器；
——　智能车载记录仪。

5　关键场景应用

5.1　概述

针对食品安全数字化管理的关键应用场景，提出数字化管理、网络化协同和智能化管控相关要求，推动实现食品安全工作全方位、全过程、全天候、全链条的态势感知，强化风险分级管控隐患排查治理和动态监测预警，创新食品安全工作机制，完善食品安全保障体系。

5.2　入口

入口应能管理包括但不限于以下功能：
——　人脸识别门禁；
——　智能测温门；
——　手触式消毒测温机；
——　餐厅客流量采集；
——　智能档口拥挤预警；
——　智能配餐溯源。

5.3　办公室

办公室应能管理包括但不限于以下功能：
——　亮证经营；
——　智慧晨会溯源；
——　AI 行为识别与检测；
——　智能管理日志；
——　智慧信息化电子台账；
——　智慧云告警看板；
——　智能日常检查与飞行监督；
——　智慧食安协管指挥中心。

5.4　厨房入口

厨房入口应能管理包括但不限于以下功能：
——　标准化预警提示；
——　智能体温检测门禁；
——　智能手部识别；
——　智能病史核查；
——　智能多班考勤；
——　智能开门闭门；
——　智能全身消杀；
——　不明人员抓怕。

5.5　快检验

快检验应能管理包括但不限于以下功能：

——　智能农残检测；
——　智能兽残检测；
——　智能重金属检测；
——　ATP 检测溯源；
——　全自动信息化台账；
——　营养膳食配置。

5.6　仓库

仓库应能管理包括但不限于以下功能：

——　挡鼠板离位监测；
——　智能三离监测；
——　智能常温检测；
——　超声波驱鼠器；
——　智能云称重溯源；
——　一物一码管控；
——　索票索证管控；
——　先进先出管控；
——　食材临期管控；
——　最低采购量管控；
——　智能实时库存报表。

5.7　清洗浸泡

清洗浸泡应能管理包括但不限于以下功能：

——　智能清洗溯源；
——　农残处理监测；
——　智能浸泡管控；
——　智能食材净化管控；
——　地面积水监测。

5.8　切配间

切配间应能管理包括但不限于以下功能：

——　智能刀具砧板柜；
——　智慧切配看板；
——　智慧色标管控；
——　智慧营养搭配；
——　智慧禁食管控。

5.9　保鲜缓存

保鲜缓存应能管理包括但不限于以下功能：

——　智慧低温监测；
——　智慧重量溯源；
——　智慧净菜率分析；

——　智慧保鲜管控；
——　智慧临期预警。

5.10　烹饪间

烹饪间应能管理包括但不限于以下功能：
——　智能瓦斯监测；
——　AI 食用油温监控；
——　智能动火离人监测；
——　智能油水分离器；
——　AI 安全阀门监测管控；
——　智能油烟在线监测；
——　智能油烟前置净化处理；
——　菜品中心温度监测；
——　智慧膳食标签。

5.11　二更间

二更间应能管理包括但不限于以下功能：
——　智能双手消毒溯源；
——　智能全身消毒溯源；
——　刷脸进出自动开门闭门。

5.12　分餐间

分餐间应能管理包括但不限于以下功能：
——　智能雾化环境消毒；
——　智能杀菌灯管控；
——　智能门窗闭合监测；
——　全自动打饭机；
——　全自动打汤机；
——　环境温湿监测；
——　AI 留样销样溯源。

5.13　餐具回收、配送

餐具回收、配送应能管理包括但不限于以下功能：
——　智能固液分离；
——　智能粉碎压榨；
——　智能餐余生化处理；
——　AI 餐具洗消溯源；
——　智慧智能快速结算；
——　车裁温湿在线监测；
——　车载轨迹查询；
——　异常开门告警溯源。

6　建设要求

6.1 主要建设内容

主要建设平台见图 1 。各平台又内设子系统和多个应用程序。各个平台及子系统既可分工独立运行，实现食品安全全程全域的互联互通。

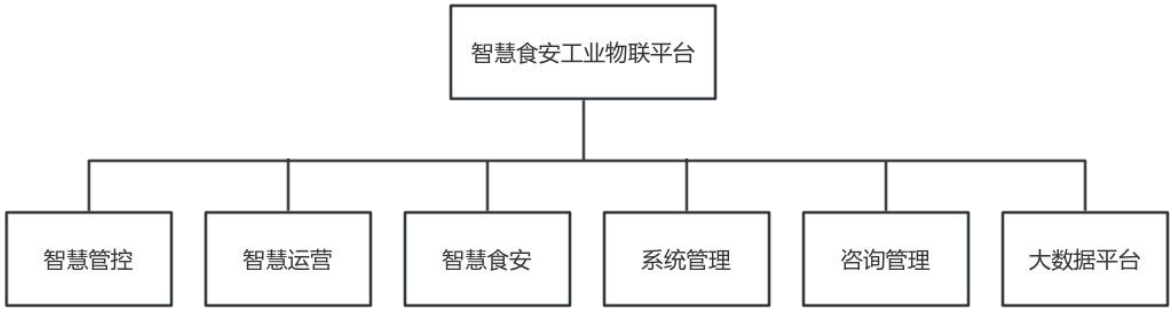

图 1 智慧食安工业物联网平台

6.2 功能要求

6.2.1 智慧管控

智慧食安工业物联网平台的智慧管控子系统宜包含以下功能模块：

a) 公司资讯：
   1) 公司资讯；
   2) 公司证照。
b) 公司管理：
   1) 组织架构；
   2) 部门制度。
c) 人力资本：
   1) 考勤管理；
   2) 班次管理；
   3) 工作日志；
   4) AI 设备监测；
   5) AI 违规识别；
   6) AI 违规统计；
   7) 不明人员抓拍；
   8) 不明人员统计。
d) 流程审批；
e) 安全生产：安全培训/培训记录；
f) 检测管理：
   1) 安全检查记录；
   2) 自检和抽检。
g) 区域管理：
   1) 区域管理；
   2) 实景展示。
h) 晨会管理：晨会记录；

i） 陪餐管理：
1） 陪餐排班表；
2） 陪餐记录。
j） SOP 流程：
1） 泔水回收记录；
2） 废油回收记录；
3） 剩饭剩菜记录。

6.2.2 智慧运营

智慧食安工业物联网平台的智慧运营子系统应包含以下功能模块：
a） 菜谱管理：
1） 发布菜谱；
2） 发布记录。
b） 智慧仓储：
1） 仓库管理；
2） 库存管理；
3） 库存明细；
4） 出库单；
5） 入库单；
6） 采购订单；
7） 预采购订单；
8） 领用订单；
9） 采购退货单；
10） 库存调拨；
11） 报表管理。
c） 清洗浸泡：
1） 清洗浸泡管理；
2） 清洗设备监测；
3） 食材清洗记录；
4） 清洗违规记录；
5） 食材清洗称重；
6） 食材风干称重。
d） 切菜配菜：切配称重；
e） 智能烹饪：
1） 菜品烹饪；
2） 烹饪称重。

6.2.3 智慧食安

智慧食安工业物联网平台的智慧食安子系统应包含以下功能模块：
a） 食安检测：食材检测；
b） 智能消杀：
1） 专间消杀；
2） 手部消杀；

3) 人体消杀；
4) 餐具消杀。

c) 环境监测：
1) 低温在线检测；
2) 燃气在线检测；
3) 三离设备管理；
4) 挡鼠板管理；
5) 高温在线检测；
6) 冰箱留样管理；
7) 常温在线检测。

6.2.4 系统管理

智慧食安工业物联网平台的系统管理子系统应包含以下功能模块：

a) 权限管理：
1) 员工管理；
2) 权限管理。

b) 食材管理：
1) 食材分类管理；
2) 食材管理。

c) 菜品管理：菜品管理；

d) 合作单位管理：
1) 领用单位管理；
2) 供应商管理。

6.2.5 咨询管理

智慧食安工业物联网平台的咨询管理子系统应包含以下功能模块：

a) 个人消息管理；
b) 异常报警管理；
c) 公告管理。

6.2.6 大数据平台

智慧食安工业物联网平台的大数据平台子系统应包含以下功能模块：

a) 数据采集；
b) 数据清洗；
c) 数据分析；
d) 数据可视化。

6.3 性能要求

6.3.1 用户操作

平台未来需要面向的用户分为三大类：政府监管用户、企业用户和公众用户。具体如下所示：

a) 政府监管用户：市、县市场监管局、监管所；
b) 企业用户：食品农产品生产、流通、消费环节食品企业；
c) 公众用户：消费者。

6.3.2 系统性能指标

6.3.2.1 根据业务需求，系统性能是至关重要的因素，主要满足以下指标内容：

a) 响应时间：对于确切条件的查询，响应时间不超过 3 s；
b) 数据交换能力：根据信息流量预测，每秒交换数据量不低于 40 MB；
c) 数据备份：全备份在 48 h 内完成，增量备份在 12 h 内完成；
d) 系统应具有高可用性，支持负载均衡、集群，保持系统运行稳定
e) 系统能支持系统主机、操作系统、网络、数据库 7×24 h 平稳运行；
f) 系统运行要支持双机热备，单台设备的故障不影响业务进行，实现故障恢复不中断业务服务；
g) 系统宜采用大量的数据冗余技术，有效提高数据的存取速度；
h) 系统在可靠性、 易用性和可扩展性等方面， 需满足以下内容：
   1) 可靠性要满足系统 7×24 h 不间断服务的要求；
   2) 系统可用率 ≥ 99.9%， 即每年的不可用时间小于 9 h；
   3) 采用标准接口、界面友好、使用方便；
   4) 网络结构、硬件结构、软件结构、 数据库等方面的设计能满足功能不断扩展， 以及系统容量和用户数量不断增长的要求。

6.3.3 部署环境需求

6.3.3.1 网络

宜确保互联网与内部局域网之间用防火墙隔离，禁止外界用户直接访问内部局域网。

6.3.3.2 机房

建有独立机房的，宜在机房内放置平台服务器及相关硬件设备，并制定完善的机房安全管理制度。

6.3.3.3 服务器

服务器宜至少配置以下内容：

a) 部署应用中间件和发布应用程序；
b) 部署数据库系统；
c) 数据交换需求。

6.4 安全要求

6.4.1 一般要求

可信“智慧食安”工业物联网数字化管理平台应采取全面的安全保护措施，在操作系统、依赖的第三方服务、程序应用、端口开发管理等方面完成服务器的安全策略；从身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制等方面进行安全设计，提高服务器在应用过程中安全抵御能力。

6.4.2 物理安全

应对机房环境、机房建设、机房管理、防静电措施、设备供电与接地、电磁干扰等方面进行排查，排查问题包括但不限于：

a) 自然灾害、物理损坏和设备故障；
b) 电磁辐射、乘机而入、痕迹泄漏；
c) 操作失误、意外疏漏。

6.4.3 网络安全

应对网络防病毒措施、系统业务处理能力网络边界设备的访问控制、各子系统子网划分、用户身份鉴别等方面进行排查，使系统中的数据受到保护，不因偶然的或者恶意的原因而遭受破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

6.4.4 主机安全

应对登录系统和数据库用户身份鉴别、权限分配、防病毒软件安装等方面进行排查，具体要求如下：

a) 建设漏洞主动发现机制：可以通过渗透测试结合漏洞扫描来实现涵盖系统漏洞、应用漏洞的自动化、周期性安全风险监测、检出能力。主动检测安全问题，发现未知漏洞，对安全问题进行及早预防，先黑客一步检测出安全问题并修复；

b) 增强网络攻击主动发现能力：如何有效地发现各种网络攻击行为，增强网络攻击主动发现能力，成为在实际的网络安全建设、运营、保障过程中需要重点考虑的问题。通过部署 WAF/IDS 等网络安全设备，可第一时间对攻击行为进行发现阻断保护系统不被入侵；

c) 对主机进行安全防护：主机安全防护系统可以及时发现主机层的漏洞和不安全的配置，也可以在黑客尝试爆破或检测到入侵行为进行告警，隔离等操作，是主机入侵防御的最后一道保障。针对未部署安全防护系统的场景及核心业务主机，部署主机安全产品，可以有效规避安全事件的影响；

d) 加强配置策略设置：如果密码等用户身份被轻易破解，那么再强的防护系统也形同虚设。通过配置密码错误多次禁止 IP 的策略，SSH 使用密钥登录等安全策略，来保证不会因为风险策略而导致的入侵事件发生。

6.4.5 应用安全

6.4.5.1 应对登录用户的身份鉴别能力、登录失败处理措施、文件自动保护及服务预警措施等方面进行排查。

6.4.5.2 管理员通过服务器报警策略、用户密码策略、用户安全策略、访问控制策略和时间策略来保证服务器的稳定性以及限用户安全访问应用程序的安全设置。

6.4.6 数据安全

数据备份与恢复、重要业务数据完整性保护措施、主要网络设备与传输通道冗余等方面进行排查并建立良好的安全制度，制度内容应包含：

a) 对应用系统使用、产生的介质或数据按其重要性进行分类，对存放有重要数据的介质，应备份必要份数，并分别存放在不同的安全地方（防火、防高温、防震、防磁、防静电及防盗），建立严格的保密保管制度；

b) 保留在机房内的重要数据（介质），应为系统有效运行所必需的最少数量，除此之外不应保留在机房内；

c) 根据数据的保密规定和用途，确定使用人员的存取权限、存取方式和审批手续；

d) 重要数据（介质）库，应设专人负责登记保管，未经批准，不得随意挪用重要数据（介质）；

e) 在使用重要数据（介质）期间，应严格按国家保密规定控制转借或复制，需要使用或复制的须经批准；

f) 对所有重要数据（介质）应定期检查，要考虑介质的安全保存期限，及时更新复制。损坏、废弃或过时的重要数据（介质）应由专人负责消磁处理，秘密级以上的重要数据（介质）在经过保密期或废弃不用时，要及时销毁；

g) 机密数据处理作业结束时，应及时清除存储器、联机磁带、磁盘及其他介质上有关作业的程序和数据；
h) 机密级及以上秘密信息存储设备不得并入互联网。重要数据不得外泄，重要数据的输入及修改应由专人来完成。重要数据的打印输出及外存介质应存放在安全的地方，打印出的废纸应及时销毁。

6.4.7 管理安全

应建立良好的网络安全管理制度、系统操作人员管理、网络安全培训、软件升级审批等。

7 运行维护

7.1 运维管理

可信“智慧食安”工业物联网数字化管理平台具备运维管理功能。

7.2 运维管理内容

可信“智慧食安”工业物联网数字化管理平台应负责系统对接与生产切换服务，对系统软件及功能模块进行日常的管理和维护，及时修复相关软件漏洞，排除故障，保障软件层面的正常稳定、安全高效运行。

7.3 运维管理流程

7.3.1 为保证运行维护体系的高效、协调运行，宜依据管理环节、管理内容、管理要求制定统一的运行维护工作流程，实现运行维护工作的标准化、规范化。运行维护流程包括的环节有：日常运行维护、用户的运维请求、故障处理、问题跟踪等。
7.3.2 运维等级及响应处理时间应符合表 1 的规定。

表 1 运维等级及响应处理时间

序号	故障等级	故障描述	响应时间	恢复时间	支持方式
1	一级	非平台故障引起的一般性使用问题	≤ 30 min	≤ 24 h	远程
2	二级	次要功能无法使用或概率性出现问题，影响用户使用	≤ 30 min	≤ 6 h	远程/现场
3	三级	核心功能无法使用，影响业务开展	≤ 15 min	≤ 2 h	远程/现场

7.4 运维管理制度

为确保运行维护工作正常、有序、高质地进行，针对运行维护的管理流程和内容，应制定相应的运行维护管理制度，实现各项工作的规范化管理。运行维护管理制度可分为：

a) 网络管理制度；
b) 系统和应用管理制度；
c) 安全管理制度；
d) 存储备份管理制度；
e) 故障管理制度；
f) 人员管理制度；
g) 质量考核制度。