ICS 35.020
CCS L 70

团　体　标　准

T/CESA XXXX-202X

工业互联网平台边云智能协同系统防护技术要求

Industrial Internet platform edge cloud intelligent collaborative system protection technology 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。

已授权的专利证明材料为专利证书复印件或扉页，已公开但尚未授权的专利申请证明材料为专利公开通知书复印件或扉页，未公开的专利申请的证明材料为专利申请号和申请日期。

202X-XX- XX 发布　　202X-XX- XX 实施

中国电子工业标准化技术协会　发布

目　次

工业互联网平台边云智能协同系统　防护技术要求

1. 范围

本标准规定了工业互联网平台边云智能协同系统防护技术要求的要素，提供了工业互联网平台边云智能协同系统防护技术要求的指导体系和操作方法。

本标准适用于工业互联网平台边云智能协同系统涉及的平台应用，并针对基于工业互联网平台边云智能协同系统延申的平台系统提供指导。

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 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

GB/T 20271-2006 信息安全技术 信息系统通用防护技术要求

GB/T 25068.3-2010 信息技术 安全技术 IT 网络安全第 3 部分：使用安全网关的网间通信安全保护

GB/T 25068.4-2010 信息技术 安全技术 IT 网络安全第 4 部分：远程接入的安全保护

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 35279-2017 信息安全技术 云计算安全参考架构

GB/T 37044-2018 信息安全技术 物联网安全参考模型及通用要求

GB/T 9361-2011 计算机场地安全要求

GB 50174-2017 数据中心设计规范

GB/T 32400-2015 信息技术 云计算 概览与词汇

GB/T 36324-2018 信息安全技术 工业控制系统信息安全分级规范

GB/T 5271.8-2001 信息技术 词汇 第8部分：安全

GB/T 25056-2010 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 28452-2012 信息安全技术 应用软件系统通用防护技术要求

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 29246-2017 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 25058-2010 信息安全技术 信息系统安全等级保护实施指南

GB/T 21052-2007 信息安全技术 信息系统物理防护技术要求

3. 术语和定义

GB/T 42562-2023 和 GB/T 41870-2022 界定的以及下列术语和定义适用于本文件。

3.1.

边缘计算 edge computing

在网络边缘对数据进行存储和处理的分布式计算。

3.2.

边缘应用 edge computing application

运行在边缘节点上的应用程序。

3.3.

边缘基础设施 edge computing infrastructure

承载边缘计算服务的硬件设备、系统软件以及用于监控或管理边缘节点的软件工具等基础设施。

3.4.

边缘网络 edge computing network

边缘计算系统中端层、边层和云层之间的通信网络。

3.5.

边缘数据 edge computing data

在边缘计算过程中，由边层、端层和云层采集、生成、处理或存储的数据。

3.6.

云计算 cloud computing

一种通过网络将将可伸缩、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模式。

3.7.

云计算服务 cloud computing service

通过云计算已定义的接口提供的一种或多种能力。

3.8.

云服务租户 cloud service tenant

对一组物理和虚拟资源进行共享访问的一个或多个云服务用户。

3.9.

云计算基础设施 cloud computing infrastructure

由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施。

注：硬件资源包括所有的物理计算资源，包括服务器（CPU、内存等）、存储组件（硬盘等）、网络组件（路由器、防火墙、交换机、网络链接和接口等）及其他物理计算基础元素。

3.10.

云计算平台 cloud computing platform

云服务商提供的云基础设施及其上的服务软件的集合。

3.11.

控制设备 control equipment

工业生产过程中用于控制执行器以及采集传感器数据的装置，包括分布式控制系统（DCS）的现场控制单元、可编程逻辑控制器（PLC）以及远程终端单元（RTU）等进行生产过程控制的单元设备。

3.12.

工业主机 industrial host

工业生产控制各业务环节涉及组态、工作流程和工艺管理、状态监控、运行数据采集以及重要信息存储等工作的设备载体，包括工程师站、操作员站、服务器、存储设备等。

3.13.

代码安全审计 Code Security Audit

一种以发现代码安全缺陷和违反代码安全规范为目标的源代码安全性分析。

3.14.

信息系统 information system

信息系统由计算机及其相关的配套部件、设备和设施构成，按照一定的应用目的和规则对信息进行采集、加工、存储、传输、检索等的人机系统。

3.15.

信息系统物理安全 physical security forinformation system

为了保证信息系统安全可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施(包括机房建筑、供电、空调)、环境、人员及系统等采取适当的安全措施。

3.16.

设备物理安全 facility physical security

为保证信息系统的安全可靠运行，降低或抑制人为或自然因素对硬件设备安全可靠运行带来的安全风险，对硬件设备及部件所采取的适当安全措施。

4. 缩略语

以下缩略语适用于本文件。

PLC：可编程逻辑控制器

DCS：分布式控制系统

RTU：远程终端单元

5. 概述

本标准依据 GB/T 22239-2008，GB/T 20271-2006，GB/T 25068.4-2010，GB/T 35279-2017，GB/T 37044-2018，GB/T 9361-2011，GB/T 28452-2012，GB/T 21052-2007 综合提出信息系统防护技术要求。本标准给出了工业互联网边云智能协同系统的防护技术要求，

其安全要求主要包括云计算安全防护、边缘计算安全、代码安全审计等 3 个主要的技术要求。

6. 云计算安全防护技术要求

6.1. 概述

云计算安全防护技术要求用于定义和评价云服务提供商在工业互联网平台边云智能协同系统建设中云端的安全防护能力，根据 GB/T 22239-2008，GB/T 20271-2006，GB/T 25068.3-2010，GB/T 25068.4-2010，GB/T 35273-2020，GB/T 35279-2017，GB/T 25056-2010，GB/T 20984，云计算安全防护技术要求被分为系统与通信保护、访问控制、数据保护、应急响应、安全审计、风险评估与持续监控 6 个方面。

6.2. 系统与通信保护

6.2.1. 边界保护

云服务商的边界保护应满足以下要求：

a）在连接外部网络或外部信息系统的边界以及内部关键边界上，对通信进行监控。

b）将允许外部公开直接访问的组件，划分在一个与内部网络逻辑隔离的子网络上，如 DMZ 区（隔离区），确保允许外部人员访问的组件与允许客户访问的组件在逻辑层面实现严格的网络隔离。

c）确保与外部网络或信息系统的连接只能通过严格管理的接口进行，该接口上应部署有边界保护设备。

6.2.2. 传输保密性和完整性

云服务商应采用密码技术保证通信过程中数据的保密性和完整性。

6.2.3. 网络中断

云服务商应采取有关措施，确保在应用层通信会话结束时或在[赋值：云服务商定义的不活动时间]之后，云计算平台终止有关网络连接。例如，对基于 RAS（远程访问服务）的会话，可将不活动时间定义为 30min；对于非交互式用户，可将不活动时间定义为 30 到 60min。

6.2.4. 可信路径

云服务商应采取有关措施，确保在云计算平台用户和系统安全功能之间建立一条可信的通信路径，安全功能至少应包括：系统鉴别、再鉴别、服务分配和回收。

6.2.5. 密码使用和管理

云服务商应按照国家密码管理有关规定使用和管理云计算平台中使用的密码设施，并按规定生成、使用和管理密钥。

6.2.6. 设备接入保护

云服务商应在远程运维终端接入云计算平台前对其进行安全检查，确保安全状态符合云计算平台要求后，才可接入云计算平台。

6.2.7. 恶意代码防护

云服务商在恶意代码防护方面应满足以下要求：

a）在网络出入口以及系统中的主机、移动计算和存储设备上实施恶意代码防护机制。

b）建立相应维护机制，确保恶意代码防护机制得到及时更新，如升级病毒库。

c）及时对恶意代码告警记录进行检查和分析，并分析误报对信息系统可用性的潜在影响。

6.3. 访问控制

6.3.1. 用户标识与鉴别

云服务商在用户标识与鉴别方面应满足以下要求：

a）对信息系统的用户进行唯一标识和鉴别。

b）对特权账号的网络访问实施多因子鉴别。

6.3.2. 鉴别凭证管理

云服务商在鉴别凭证管理方面应满足以下要求：

a）通过以下步骤管理鉴别凭证：

1）验证鉴别凭证接收对象（个人、组、角色或设备）的身份。

2）确定鉴别凭证的初始内容。

3）确保鉴别凭证能够有效防止伪造和篡改。

4）针对鉴别凭证的初始分发、丢失处置以及重置，建立和实施管理流程。

5）强制要求用户更改鉴别凭证的默认内容。

6）明确鉴别凭证的最小和最大生存时间限制以及再用条件。

7）对[赋值：云服务商定义的鉴别凭证]，强制要求在[赋值：云服务商定义的时间段]之后更新鉴别凭证。

8）保护鉴别凭证内容，以防泄露和篡改。

9）采取由设备实现的特定安全保护措施来保护鉴别凭证，如：由设备生成证书或密码。

10）当组或角色账号的成员资格发生变化时，变更该账号的鉴别凭证。

b）对于基于口令的鉴别：

1）设立相关机制，能够强制执行最小口令复杂度，该复杂度满足[赋值：云服务商定义的口令复杂度规则]。

2）设立相关机制，能够在用户更新口令时，强制变更[赋值：云服务商定义的数目]个字符，确保新旧口令不同。

3）对存储和传输的口令进行加密。

4）强制执行最小和最大生存时间限制，以满足[赋值：云服务商定义的最小生存时间和最大生存时间]。

c）对于基于硬件令牌的鉴别，定义令牌安全质量要求，并部署相关机制予以满足，如基于 PKI 的令牌。

6.3.3. 密码模块鉴别

云服务商应确保系统中的密码模块对操作人员设置了鉴别机制，该机制应满足国家密码管理的有关规定。

6.3.4. 账号管理

云服务商在账号管理方面应满足以下要求：

a）指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。

b）标识账号类型（如个人账号、组账号、访客账号、匿名账号和临时账号）。

c）当下述情况出现时，通报账号管理员：

1）当临时账号不再需要时。

2）当用户离职或调动时。

3）当变更信息系统用途时。

d）按照[赋值：云服务商定义的频率]，检查账号是否符合账号管理的要求。

6.3.5. 访问控制的实施

云服务商在访问控制的实施方面应满足以下要求：

a）对云计算平台上信息和系统资源的逻辑访问进行授权。

b）在对访问进行授权时应符合[赋值：云服务商定义的职责分离规则]。

6.3.6. 未成功的登录尝试

云服务商在未成功的登录尝试方面应满足以下要求：

a）将[赋值：云服务商定义的时间段]内连续登录失败的上限限定为[赋值：云服务商定义的次数]。

b）当登录失败次数超过上限时，系统将锁定账号，直至[选择：达到[赋值：云服务商定义的时间段]；由管理员解锁]。

6.3.7. Web 访问安全

云服务商在 Web 访问安全方面应满足以下要求：

a）支持 web 代码安全机制的能力，包括对输入输出进行有效性检查，以及采取防范认证漏洞、权限漏洞、会话漏洞、web 服务漏洞、注入漏洞等代码漏洞的措施。

b）支持对用户通过 web 访问资源进行访问控制的能力。

c）支持 web 远程访问安全传输能力。

6.4. 数据保护

6.4.1. 数据安全管理

云服务商在数据安全管理方面应满足以下要求：

a）通过与客户签订合同等形式，声明未经客户授权不得收集、使用或处理客户数据。

b）提供重要数据的备份与恢复功能。

c）支持由租户设置数据备份和数据导出权限的能力。

d）支持由租户设置数据重置权限的能力。

6.4.2. 个人信息保护

云服务商应根据客户需求，通过合同等形式与客户确定应满足的个人信息安全要求，并按照 GB/T35273 等提供相应的个人信息保护机制。

6.4.3. 数据共享

云服务商在数据共享方面应满足以下要求：

a）允许授权用户判断共享者的访问授权是否符合[赋值：云服务商定义的信息共享环境]中的数据访问限制策略，以促进数据共享。

b）使用自动机制或人工过程，协助用户作出数据共享决策。

6.4.4. 介质访问和使用

云服务商在介质访问和使用方面应满足以下要求：

a）限制介质访问权限，根据服务模式和业务需求，仅允许特定人员、角色或信息系统组件访问存储客户数据的介质。

b）[选择：限制；禁止]在[赋值：云服务商定义的系统或组件]中使用[赋值：云服务商定义的介质]。

6.4.5. 服务关闭和数据迁移

云服务商在服务关闭和数据迁移方面应满足以下要求：

a）在客户与其服务合约到期时，能够安全地返还云计算平台上的客户数据。

b）在客户定义的时间内，删除云计算平台上存储的客户数据，并确保不能以商业市场的技术手段恢复。

c）为客户数据迁移提供技术手段，并协助完成数据迁移，包括：

1）具备在相同云计算平台上将客户服务快速迁入或迁出的能力。

2）具备在异构云计算平台上将客户服务迁入或迁出的能力。

3）针对客户数据量大等可能导致迁移过程执行受阻的因素，制定应对措施。

4）数据格式应支持主流硬件厂商的硬件平台和操作系统平台使用的典型数据库产品，如 Oracle、Sybase、SQLServer 等，支持异构数据库间的数据集成与协同，并保证多数据库（异构或同构）之间的全局事务一致性。

6.5. 应急响应

6.5.1. 事件处理计划

云服务商在事件处理计划方面应满足以下要求：

a）制定云计算平台的事件处理计划，该计划应：

1）说明启动事件处理计划的条件和方法。

2）说明本组织内与事件处理有关的组织架构。

3）定义需要报告的安全事件。

4）提供事件处理能力的度量目标。

5）定义必要的资源和管理支持。

6）由[赋值：云服务商定义的人员或角色]审查和批准。

b）向[赋值：云服务商定义的人员、角色或部门]，发布事件处理计划。

c）按照[赋值：云服务商定义的频率]，审查事件处理计划。

d）如系统发生变更或事件处理计划在实施、执行或测试中遇到问题，及时修改事件处理计划并通报[赋值：云服务商定义的人员、角色或部门]。

e）防止事件处理计划非授权泄露和更改。

6.5.2. 事件处理

云服务商在事件处理方面应满足以下要求：

a）为安全事件的处理提供必需的资源和管理支持。

b）协调应急响应活动与事件处理活动，并与相关外部组织（如供应链中的外部服务提供商等）进行协调。

c）将当前事件处理活动的经验，纳入事件处理、培训及演练计划，并实施相应的变更。

6.5.3. 应急响应计划

云服务商在应急响应计划方面应满足以下要求：

a）制定云计算平台的应急响应计划，该计划应：

1）标识出云计算平台的基本业务功能及其应急响应需求。

2）进行业务影响分析，标识关键信息系统和组件及其安全风险，确定优先次序。

3）提供应急响应的恢复目标、恢复优先级和度量指标。

4）描述应急响应的结构和组织形式，明确应急响应责任人的角色、职责及其联系信息。

5）由[赋值：云服务商定义的人员或角色]审查和批准。

b）将应急响应计划向[赋值：云服务商定义的人员、角色或部门]进行通报。

c）按照[赋值：云服务商定义的频率]更新应急响应计划。

d）如云计算平台发生变更或应急响应计划在实施、执行或测试中遇到问题，及时修改应急响应计划并向[赋值：云服务商定义的人员、角色或部门]及客户进行通报。

e）防止应急响应计划非授权泄露和更改。

f)在发生安全事件时,确保应急响应计划的实施能够维持云计算平台的基本业务功能，并能最终完全恢复信息系统且不消弱原来的安全措施。

g）当本组织的管理架构、云计算平台或运行环境发生变更时，及时更新应急响应计划。

6.5.4. 信息系统备份

云服务商在信息系统备份方面应满足以下要求：

a）具备系统级备份能力，按照[赋值：云服务商定义的频率]，对信息系统中的系统级信息进行备份，如系统状态、操作系统及应用软件。

b）防止通过备份过程访问客户的明文数据。

c）为用户提供多种备份方案。

d）在存储位置保护备份信息的保密性、完整性和可用性。

e）具有验证信息系统备份连续有效的方法，并按照[赋值：云服务商定义的频率]进行验证。

f）向客户提供下列信息，以支持客户制定其自身的备份策略和规程：

1）备份的范围。

2）备份方式和数据格式。

3）验证备份数据完整性的规程。

4）恢复备份数据的规程。

6.5.5. 支撑客户的业务连续性计划

云服务商在支撑客户的业务连续性计划方面应满足以下要求：

a）具备灾难恢复能力，确保客户业务可持续。

b）对云计算服务为客户业务连续性带来的风险进行评估，包括云计算服务失败、云服务商和客户之间网络连接中断、云计算服务终止等，并将相关的风险信息告知客户。

c）将应急响应计划、灾难恢复计划及支撑客户实施业务连续性计划的有关措施告知客户，并根据客户的业务连续性计划的需要，对应急响应计划、灾难恢复计划进行调整。

6.6. 风险评估与持续监控

6.6.1. 风险评估

云服务商在风险评估方面应满足以下要求：

a）至少每年开展一次风险评估，在云计算平台建设、发生重大变更（包括发现新的威胁和漏洞）时，或者在出现其他可能影响系统安全状态的条件时，重新进行风险评估。

b）将评估结果记录在风险评估报告中，并将风险评估结果发布至[赋值：云服务商定义的人员或角色]。

c）根据风险评估报告，有针对性地对云计算平台进行安全整改，将风险降低到可接受的水平。

6.6.2. 持续监控

云服务商在持续监控方面应满足以下要求：

a）根据自身及客户在持续监控方面的需要，制定持续监控策略，明确监控的度量指标和监控频率。

b）根据持续监控策略，对已定义的度量指标进行持续的安全状态监控。

c）对评估和监控产生的安全相关信息进行关联和分析。

d）对安全相关信息分析结果进行响应。

e）按照[赋值：云服务商定义的频率]向信息安全责任部门和相关人员报告信息系统安全状态。

7. 边缘计算防护技术要求

7.1. 概述

边缘计算防护技术要求用于定义和评价边缘计算产品和服务在工业互联网平台边云智能协同系统建设中的安全防护能力，根据 GB/T 22239-2008，GB/T 20271-2006，GB/T 25068.3-2010，GB/T 25068.4-2010，GB/T 37044-2018，GB/T 28452-2012，GB/T 21052-2007，边缘计算防护技术要求分为应用安全、网络安全、数据安全、基础设施安全、安全运维、安全支撑、端边协同安全和云边协同安全 8 个方面。