ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团 体 标 准

T/XXX XXXX—XXXX

风电企业绿色供应链信息管理平台 第 3 部分： 系统和数据安全要求

Green Supply Chain Information Management Platform of wind power companies
Part 3: System and data security 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。

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中国信息协会 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。

本文件由中国信息协会提出并归口。

本文件起草单位：

本文件主要起草人：

风电企业绿色供应链信息管理平台
第 3 部分： 系统和数据安全要求

1 范围

本文件规定了风电企业绿色供应链信息管理平台的系统安全要求和数据安全要求。

本文件适用于风电企业绿色供应链信息管理平台的系统和数据安全建设。其他组织的绿色供应链信息管理平台可参照执行。

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 2887-2011 计算机场地通用规范

GB/T 9361-2011 计算机场地安全要求

GB 50174-2017 数据中心设计规范

3 术语和定义

本文件没有需要界定的术语和定义。

4 系统安全要求

4.1 软硬件安全

系统应充分考虑在实际应用中可能出现的软硬件异常，针对可能出现的异常应具备恢复能力，同时软件方面应能够提供详细的日志信息。

a) 系统发生硬件或者软件故障时，现场数据采集器应能支持对数据不低于 7 天的存储需求，待恢复后正常进行数据重传。数据采集设备应具备良好的自恢复能力，出现异常时，可自动重连，恢复通信能力，可根据需要进行远程系统修改和升级。

b) 系统具有自诊断能力，当系统发生硬件或软件故障时，应能提供详细的故障信息和地理定位。当出现故障无法恢复的情况下，应有备用的设备可自动启用，最大程度确保系统不间断运行。

4.2 采集数据传输安全

能耗数据报文由采集器发送至云计算中心的接口服务器，接口服务器在进行数据接收前应对采集器进行身份验证，发送端对报文进行加密后传输。

a) 身份认证过程

接口服务器使用MD5算法应进行数据采集器身份认证，密钥长度为128位，具体过程如下：

1) 传输控制协议（TCP）连接建立后，数据采集器向接口服务器发送身份认证请求；
2) 接口服务器向数据采集器发送一个随机序列；
3) 数据采集器将接收到的随机序列和本地存储的认证密钥组合成一连接串，计算连接串的 MD5 值，并发送给接口服务器；
4) 接口服务器将接收到的 MD5 值和本地计算结果相比较，如果一致则认为成功，否则认证失败。

认证密钥存储在接口服务器和数据采集器的本地文件系统中，接口服务器可通过网络对数据采集器的认证密钥进行更新。

b) 数据加密

使用高级加密标准（AES）加密算法应对可扩展标记语言（XML）数包进行加密，密钥长度为128位。加密密钥存储在接口服务器和数据采集器的本地文件系统中，接口服务器可通过网络对数据采集器的加密密钥进行更新。

4.3 云计算中心安全

4.3.1 网络安全

应从总体层面来统一设计、建设和管理，在网络和系统层面为绿色供应链云计算中心云计算平台提供安全保护功能的统一支撑，主要保护云平台网络、系统和终端的安全，包括区域边界划分、区域边界防护两部分。

安全局和网络访问控制：覆盖网络层面，应从整体上规范网络架构，进行安全局划分，并进行边界隔离与访问控制，解决网络层面的网络结构和访问控制问题。

网络通信防护：应加强入侵防护、入侵检测等安全技术措施，为云平台提供边界防护。

4.3.2 监控与审计

统一监控与审计：应主要覆盖网络、系统层面，解决网络、系统和部分应用软件的监控和审计问题，为用户提供监控和审计技术手段。

4.3.3 防病毒

防病毒管理：应覆盖用户终端和服务器，解决网络层防病毒、终端病毒统一管理问题。

4.3.4 云安全综合管控平台

云安全综合管控平台是云计算中心的一个安全子系统，其覆盖各个层面，主要提供统一的云安全管理功能。云安全综合管控平台，是承载整个安全体系的支撑平台，整合策略体系、组织体系、技术体系和运行体系，支持和承载整体安全工作的软件和工作流支撑平台。

4.3.5 用户认证授权

统一认证与授权管理平台（CA系）应由云计算中心统一规划建设，主要覆盖应用层面，也持网络层、系统层和终端。根据等级保护中对于身份鉴别的要求，针对用户身份的标识，应采用PI/CA识别等技术进行身份鉴别，通过网络登录应对身份鉴别过程信息进行加密保护，且PI/CA的建设符合电子政务信息安全等级保护相关要求，有效保证绿色供应链云计算中心信息系统数据访问的机密性、完整性及不可抵赖性，同时解决了目前身份认证和访问管理问题，规范多业务系统认证和授权方式同时为提高访问管理能力、监控和审计能力提供基础保障。

4.3.6 数据备份与容灾

数据备份与容灾是云计算中心的重要组成部分，为本项目提供相应的数据备份与容灾服务，应覆盖数据层面，解决一些重要系统的数据备份和容灾存在的问题，保障重要数据的完整性和可用性。

4.3.7 应用系统安全

应从总体层面来统一设计、建设和管理，在应用和数据层面为绿色供应链云计算中心云计算平台提供安全护功能的统一支撑，应主要保护云平台应用、云计算平台和数据的安全，针对绿色供应链云平台各应用系统及云平台独特或无法形成统一平台的安全技术措施，此部分主要增加各应用系统的安全、加固与改造。

4.3.8 云边界防护

应建立可信安全前置系统，增强虚拟化应用系统边界安全，确保云计算平台及相关系统在发生严重事件和严重攻击的情况下都能保证提供正常服务，系统运行符合设计目标，异常事件不能导致对被保护目标的损害，另外，在服务过程中，应用系统若发生局部或部件崩溃，能快速恢复，以及在系统运行时具有抵抗各种干扰和部件故障的能力。

4.3.9 互联网技术（IT）设备安全

互联网技术（IT）设备安全配置与加固，解决目前各系统加固问题，涉及系统、主机、网络、数据库和应用等方面的加固工作。

4.3.10 环境安全

机房建设应符合GB/T 2887-2011、GB 50174-2017、GB/T 9361-2011的要求，应具有防震、防盗、防水、防电、防静电和温度、湿度调节措施。

区位布局、区域防护，关键部位应安装门禁、监视系统，严格控制人员进入机房。

4.4 系统访问安全

在业务应用登录上，应采用基于认证对操作及来访问者身份鉴别，或通过集中认证措施，实现统一的身份鉴别、访问控制身份管理及审计。应用系统的软件设计中应充分考虑不同角色、不同用户对应的权限级别。

a) 系统使用有权限管理的用户和密码访问，密码在数据库中加密存储。对共享或者对外提供的数据资料应严格按照用户级别及权限的规定来授权用户对资料访问，防止越权访问。数据加密算法可以依据部署要求选取而不需修改文件。

b) 提供授权的访问方式，以保障系统管理的安全性。登录过程中服务器应自动识别用户在服务器上的注册信息，用户的权限应由管理员分配。例如，管理员级用户可实现计量器具的维护、建筑基础信息维护等高级功能；一般用户仅可使用系统管理员分配的功能，如在线监测、查询数据、统计分析等。对于客户级的用户，登录系统后应只能看到与之相关的授权区域内用能管理的数据。

5 数据安全

5.1 安全要求

5.1.1 数据源安全

确保传感器或端侧设备收集到的数据安全，一般是在广域内网中完成。

5.1.2 数据采集过程安全

在进行数据采集时，应对数据采集源进行识别和标识。可采取数据标签的形式，确保数据唯一性。应对数据采集源进行身份鉴别，防止数据源假冒和伪造。包括但不限于使用用户名/口令认证等鉴别方式。应采取加密和完整性校验技术保证数据安全。包括但不限于安全套接字协议（SSL）等。

5.1.3 数据传输过程安全

数据传输过程中，应采取加密和完整性校验技术保证数据安全。包括但不限于安全套接字协议（SSL）等。

5.2 安全控制方法

5.2.1 数据标识

设备在出厂前，应在平台侧分配设备标识，同时会把这个标识烧录到设备端，设备连接应通过标识做认证。

5.2.2 数据安全技术

数据安全技术主要包括：端侧采集数据安全、数据传输的链路安全、物管平台的安全、对外输出应用程序接口（api）安全。