ICS 35.020
CCS L 70

团　　体　　标　　准

T/CIIA 032.3—2022

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 enterprises—Part 3：Requirements system and data security

2022-12-23 发布　　2023-03-23 实施

中国信息协会　发布
中国标准出版社　出版

目　　次

前言 ……
引言 ……
1　范围……
2　规范性引用文件……
3　术语和定义……
4　系统安全……
4.1　硬件安全 ……
4.2　软件安全 ……
4.3　系统访问安全 ……
4.4　云计算中心安全 ……
5　数据安全……
5.1　安全要求 ……
5.2　安全控制 ……

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。

本文件是T/CIIA 032《风电企业绿色供应链信息管理平台》的第3部分。T/CIIA 032已经发布了以下部分：

——第1部分：总体要求；

——第2部分：能源数据采集要求；

——第3部分：系统和数据安全要求。

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：新疆金风科技股份有限公司、北京蓝象标准咨询服务有限公司、山西天宝集团有限公司、北京金风科创风电设备有限公司、中天科技海缆股份有限公司、伊莱特能源装备股份有限公司、山西富兴通重型环锻件有限公司、定西高强度紧固件股份有限公司、沁阳市锦辉风电科技有限公司、江西华伍制动器股份有限公司、上海电气风电集团股份有限公司、重庆工业大数据创新中心有限公司、中国船舶重工集团海装风电股份有限公司、哈电风能有限公司、上海核工程研究设计院有限公司、苏州天顺风能设备有限公司、祥博传热科技股份有限公司、苏州朗高电机有限公司、南京安维士传动技术股份有限公司、北京协合运维风电技术有限公司、北京神州绿盟科技有限公司、唐山文丰重工有限公司、德力佳传动科技(江苏)有限公司、泛中能源建设有限公司、上海华能电子商务有限公司、山西环冠重工集团有限公司、中联信达(天津)科技发展有限公司、嵩嘉标准化技术服务(北京)有限公司。

本文件主要起草人：甘旭超、段小莉、张德保、胡大为、俞黎萍、蔡炳余、王子源、闫鹏涛、李伟、孙富、陈海江、熊莉荣、蒋勇、胡小林、罗璐、宋晓萍、于淼、孙占锋、夏波涛、江安乐、吴伟强、胥佳、王晓鹏、郭尧、刘建国、郭婧、李俊华、闫泽康、许晓东、王历亮、张硕、闫江涛、张雁玲、王永栋、朱永峰、张立生、吴孔威、聂振荣、熊凡凡、马建红、乔华阳。

引　言

2019年4月4日，国家发展和改革委员会办公厅、市场监督管理总局办公厅印发《关于加快推进重点用能单位能耗在线监测系统建设的通知》，推动各地区全部重点用能单位的接入端系统建设，并实现数据每日上传。我国新能源战略把大力发展风力发电作为重点，绿色供应链信息管理平台的建立可实现供应商与企业在能源使用、环境排放、产品材料等方面的信息资源共享，建立上下游良好的系统绿色生态链条，但不同供应链信息管理平台之间只有保持数据格式一致、平台接口统一等，才能保证信息流通共享，因此亟需根据风电企业绿色供应链的特点制定信息管理平台相关文件进行规范。

T/CIIA 032《风电企业绿色供应链信息管理平台》由3个部分构成：

——第1部分：总体要求。旨在为风电企业绿色供应链信息管理平台的设计、开发等提供指导。

——第2部分：能源数据采集要求。旨在为风电企业绿色供应链信息管理平台的数据全生命周期管理提供指导。

——第3部分：系统和数据安全要求。旨在为风电企业绿色供应链信息管理平台系统和数据的安全保障提供指导。

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系统和数据安全要求。

本文件适用于风电企业绿色供应链信息管理平台系统和数据应用，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 计算机场地通用规范

GB/T 9361 计算机场地安全要求

GB 50174 数据中心设计规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

绿色供应链信息管理平台 green supply chain information management platform

基于信息技术和生命周期理念构建的实现产品设计、采购、生产、流通、回收处置等供应链环节绿色信息收集、处理、分析、共享及披露功能的信息平台。

4 系统安全

4.1 硬件安全

能源数据采集器应符合下列要求：

a) 应根据实际使用环境要求，选用符合传输安全等要求的采集器；

b) 宜选用具有数据存储和断点续传功能的数据采集器；

c) 企业端应用系统服务器应根据业务需求和系统架构配置要求确定，宜采用冗余配置，并应根据实际需要，建立数据备份机制；

d) 企业端网络设备应根据业务需求和网络建设需求确定，应用管理系统与外网之间宜采用防火墙隔离。

4.2 软件安全

系统软件应根据实际应用中可能出现的运行异常，具备恢复能力，系统软件应提供日志信息，并应

符合下列要求：

a) 系统发生硬件或软件故障时，现场数据采集器应支持对数据不低于 7 d 的存储需求，待恢复后应正常对数据重传；数据采集设备应具备自恢复能力，出现异常时，可自动重连，恢复通信能力，完成恢复数据校核，可根据需要对远程系统进行修改和升级；

b) 系统应具有自诊断能力，系统发生硬件或软件故障时，应显示故障类型及故障位置，自动记录故障信息，并满足故障分析需求；自诊断系统应采用冗余设计。

4.3 系统访问安全

业务应用登录，应采取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。应用系统软件设计应根据不同角色、不同用户对应权限级别确定，并应符合下列要求。

a) 系统使用有权限管理的用户和密码访问，密码应在数据库中加密存储。对共享或对外提供的数据资料应按用户级别及权限的规定授权用户对资料访问。数据加密算法可按部署要求选取而不需修改文件。

b) 应提供授权访问方式，并应符合下列要求：

1) 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，用户权限应由管理员分配；

2) 管理员级用户可实现计量器具维护、建筑基础信息维护等高级功能；

3) 一般用户可使用在线监测、查询数据、统计分析等系统管理员分配功能；

4) 对于客户级用户，登录系统后应只看到与之相关的授权区域内用能管理数据。

4.4 云计算中心安全

4.4.1 网络安全

网络安全应符合下列要求：

a) 应从总体层面统筹确定，网络和系统层面应为云计算中心、云计算平台提供安全保护功能，应保护云平台网络、系统和终端安全，以及区域边界划分和防护；

b) 安全局和网络访问控制应覆盖网络层面，应规范网络架构，对安全局划分，并对边界隔离与访问控制；

c) 网络通信防护应采取入侵防护、入侵检测等安全措施，应为云平台提供边界防护。

4.4.2 监控与审计

监控与审计应覆盖网络、系统层面，应解决网络、系统和应用软件监控和审计问题。

4.4.3 防病毒

防病毒管理应覆盖用户终端和服务器。

4.4.4 云安全综合管控平台

云安全综合管控平台宜提供云安全管理功能；应整合策略体系、组织体系、技术体系和运行体系，支持和承载安全软件和工作流支撑平台。

4.4.5 用户认证授权

用户认证授权应符合下列要求：

a) 统一认证与授权管理平台(CA 系统)应由云计算中心统筹确定，宜覆盖应用层面，也应支持网络层、系统层和终端；

b） 身份鉴别应根据等级保护中身份鉴别要求，通过网络登录对身份鉴别过程信息加密保护，应符合信息安全等级保护要求。

4.4.6 数据备份与容灾

数据备份与容灾应提供数据备份与容灾服务，应覆盖数据层面，应保障数据完整性和可用性。?

4.4.7 应用系统安全

应用系统安全应从总体层面统筹确定，应用和数据层面应为云计算中心、云计算平台提供安全护功能，应保护云平台应用、云计算平台和数据安全。

4.4.8 云边界防护

云边界防护应符合下列要求：

a） 应建立可信安全前置系统，增强虚拟化应用系统边界安全，应确保云计算平台及系统发生严重事件和严重攻击时提供正常服务；

b） 服务过程中，应用系统发生局部或部件崩溃时，应能快速恢复，系统运行时应具有抵抗干扰和部件故障的能力。

4.4.9 互联网技术设备安全

互联网技术设备安全配置与加固，应解决系统、主机、网络、数据库和应用等加固问题。

4.4.10 环境安全

环境安全应符合下列规定：

a） 机房建设应符合 GB/T 2887、GB 50174、GB/T 9361 的规定，应有防震、防盗、防水、防电、防静电和温度、湿度调节措施；

b） 区位布局、区域防护，关键部位应安装门禁、监视系统。

5 数据安全

5.1 安全要求

5.1.1 数据源安全

数据源应确保传感器或端侧设备收集到的数据安全，宜在广域内网中完成。

5.1.2 数据采集安全

数据采集过程安全应符合下列要求：

a） 数据采集时，应对数据采集源识别和标识，可采取数据标签形式；

b） 应对数据采集源身份鉴别，可使用用户名/口令认证等鉴别方式；

c） 应采取加密和完整性校验技术，可包括安全套接字协议(SSL)等。

5.1.3 数据传输安全

数据传输安全应符合下列要求。

a） 数据传输过程中，应采取 SSL 等加密和完整性校验技术。

b） 能耗数据报文应由采集器发送至云计算中心接口服务器，接口服务器数据接收前应对采集器

身份验证，发送端应对报文加密后传输。

c) 身份认证过程中，接口服务器应使用报文摘要算法 5(MD5)对采集器身份认证，密钥长度应为 128 位，并按下列步骤执行：

1) 传输控制协议(TCP)连接建立后，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) 接口服务器将接收的 MD5 值和本地计算结果相比较，一致应确认成功，否则应确认失败；
5) 认证密钥应存储在接口服务器和采集器本地文件系统中，接口服务器可通过网络对采集器认证密钥更新。

d) 数据加密应使用高级加密标准(AES)加密算法对可扩展标记语言(XML)数包加密，密钥长度应为 128 位。加密密钥应存储在接口服务器和采集器本地文件系统中，接口服务器可通过网络对采集器加密钥更新。

5.2 安全控制

5.2.1 数据标识

设备出厂前，应在平台侧分配设备标识，正式启用前应与平台侧完成设备注册。

5.2.2 数据安全技术

数据安全技术宜包括端侧采集数据安全、数据传输链路安全、物管平台安全、对外输出应用程序接口(api)安全技术。