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1部分： 总体要求

Green supply chain information management platform of Wind power companies
part 1: General 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 1 部分： 总体要求

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总体架构、设计原则、系统框架、能源管理系统功能分担、能源数据分析及数据传输、系统安全、平台建设、环境、硬件服务器配置、存储配置等要求。

本文件适用于风电企业绿色供应链信息管理平台的设计、开发，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 17167-2006 用能单位能源计量器具配置和管理通则

GB 50174-2017 数据中心设计规范

T/CIIA BBBB-2022 风电企业绿色供应链信息管理平台 第2部分：能源数据采集要求

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能够实现产品设计、采购、生产、流通、回收处置等供应链环节相关绿色信息的收集、处理、分析、共享及披露功能的信息平台。

3.2

综合能耗 comprehensive energy consumption

在统计报告期内生产某种产品或提供某种服务实际消耗的各种能源实物量，按规定的计算方法和单位分别折算后的总和。。

[来源：GB/T 2589-2020，3.5]

3.3

绿色供应链 green supply chain；GCS

将环境保护和资源节约的理念贯穿于企业从产品设计到原材料采购、生产、运输、储存、销售、使用和报废处理的全过程，使企业的经济活动与环境保护相协调的上下游供应关系。

[来源：GB/T 33635-2017,3.3]

4 缩略语

下列缩略语适用于本文件。

BBV：位流虚拟参考解码器（Bitstream Buffer Verifier）

DCS：分散控制系统（Distributed Control System）

HMI：人机接口（Human Machine Interface）

MES：生产制造过程执行系统（Manufacturing Execution System）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

RFID：射频识别（Radio Frequency IDentification）

TPC：传输控制协议（Transmission Control Protocol）

OLE：对象连接与嵌入（Object Linking and Embedding）

OPC：用于过程控制的OLE （OLE for Process Control）

SCADA：数据采集与监视控制系统（Supervisory Control And Data Acquisition）

5 总体架构

绿色供应链信息平台由企业端信息管理系统和中心端信息管理系统构成，系统层级结构图见图1。

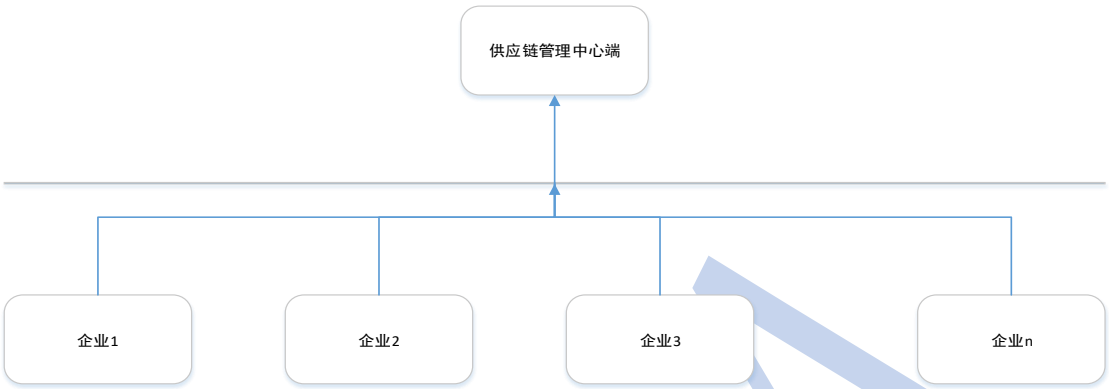

图1 绿色供应链信息平台示意图

绿色供应链信息平台采用“绿色供应链信息管理平台+供应链企业端系统”的架构，各供应链企业需按照GB 17167-2006要求配备计量仪表。绿色供应链信息管理平台总体架构见图2。

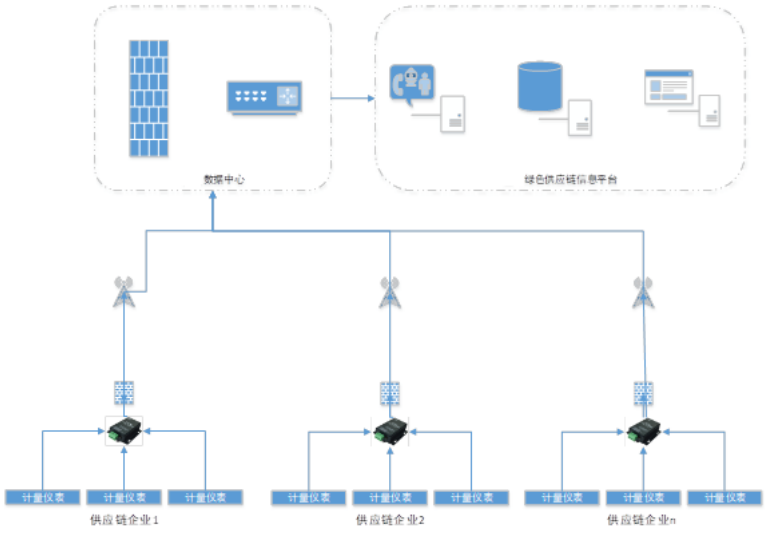

图2 绿色供应链信息管理平台总体架构

绿色供应链信息管理平台主要功能是接入、汇总、存储、分析各供应商上传数据，为能源分析等工作提供服务，可为各供应商企业提供数据接口，实现信息共享。

用能单位端系统一般由能耗在线监测端设备、计量器具、工业控制系统、生产监控管理系统、管理信息系统、通信网络及相应的管理软件等组成，部署在用能单位内部，由用能单位负责建设，主要为用能单位提供能源管理服务。用能单位端系统应具备一端双发的能力，通过互联网以安全方式将采集到的数据上传至绿色供应链信息管理平台。

6 设计原则

6.1 先进性、成熟性和实用性

根据能源系统的工艺特点，采用当今成熟并具有良好发展前景的新技术、新设备，使得各个子系统具有较长的生命周期。不盲目追求高档次，既能满足当前的需求，又能适应未来的发展（包括设备和技

术两方面内容）。设计兼顾与已有生产调度系统的总体集成，以方便系统集成和维护。网络架构层次结构符合企业分层架构模式。能源管理中心系统满足国家工信部[2009]365号要求，达到国内同类企业先进水平。

6.2 安全可靠性

高效稳定的系统，能提供全年365天，全天24小时的连续运作；对于安装的服务器、终端设备、网络设备、控制设备与布线系统，能适应严格的工作环境，全部设备采用工业级设备，以确保系统稳定；系统采取各种安全技术措施和管理手段，确保系统不被侵扰。

6.3 可操作性

先进且易于使用的图形人机界面功能，提供信息共享与交流、信息资源查询与检索等有效工具。提供易于使用的数据库功能，让使用者能随时查询信息及制作所需的报表。

6.4 高效率性

注重各子系统的信息共享，提高整个系统高效率的传输与运行能力。采用高效的国际标准通讯规约，提高通讯效率和网络规范性。

6.5 实时性

设备和终端反应快速，充分配合实时性的需求。

6.6 完整性

提供与相关外界系统的通信功能，并在整体系统的运作上确保信息的完整性。满足能源供需平衡、调度管理和能源计量管理、成本核算的需求。

6.7 可扩展性

能源管理系统将在设计时应考虑实现系统扩展和在线扩展的技术。

6.8 可维护性

从应用系统的设计、硬件设备的选型等方面考虑通用性、开放性，在系统局部发生故障时，运行维护人员能尽快发现并能及时处理，避免故障扩大并快速恢复正常运行。

6.9 经济性

考虑良好性价比、便利的技术和备件支持服务。

7 系统框架

7.1 系统功能框架

整个能效服务体系的建设是一个逐步发展的过程，因此能源和设备管控开发时不仅应满足可用性、安全性、可靠性还应具备一定可扩展性。系统架构六个层次的架构包括以下几个方面。

a) 表现层：系统直接面向操作用户的部分。
b) 应用层：实现具体业务逻辑，是系统主站的核心层，根据系统的应用特点，应用层分为系统管理模块、能耗/能效分析模块、分类/分项计量模块、采集管理模块、报表模块等。
c) 服务层：提供全局通用的数据库访问服务、消息服务、权限服务等基础服务，并实现本系统专用的业务逻辑服务，为应用层提供通用的技术支撑。
d) 数据层：信息的存储、访问、整理，为系统提供数据的管理支持。
e) 网络层：支持有线、无线多种网络通信方式，通过网络层实现数据交互，主要有窄带物联网（NB-IoT）技术、增强机器类通信（eMTC）技术，以及局域网蓝牙、WiFi、可编辑逻辑控制器（PLC）逻辑控制器等。
f) 感知层：包括二维码标签和识读器、RFID 标签和读写器、摄像头、GPS、传感器、M2M 终端、传感器网关等，主要功能是识别物体、采集信息。

7.2 系统基本功能

信息管理系统应包含以下基本功能。

a) 系统管理：管理系统运行的基础信息以及-用户的基础信息。包括系统安全管理、系统日志管理、系统信息管理、设备及参数设置功能、报警设置以及用户信息维护功能。
b) 采集管理：负责数据采集及相关的设置。
c) 能耗监测：可对能耗信息进行在线监测，可对用能损耗统计与超标预警，能效指标统计与偏差报警，并可以按能源类型以及能源用途分别进行分类与分项统计；对于系统的历史数据可以按相关条件进行综合查询。
d) 能耗/能效分析：分析用户的能耗与能效相关的信息。主要包括：用能单元能耗/能效分析、组织单元能耗/能效分析、节能项目能耗分析、用户能耗和能效专项分析、用户综合能耗/能效分析、能耗趋势和同环比及对比分析等扩展。
e) 报表功能：生成满足用户自身需求以及外部要求的相关报表。
f) 报警管理：系统可对报警类型、报警阈值以及报警方式等进行设置。
g) 档案管理：设备台账及其它文档信息管理。设备档案管理。

7.3 平台数据库结构

7.3.1 概述

能耗监测系统是一个整体，但考虑到各个成员企业平台自主开发的状况，需要针对各成员企业平台数据库结构进行统一规范，各成员企业的自主开发应遵照执行，以确保各系统数据含义的一致性。

7.3.2 关系型数据库

采集记录业务逻辑数据应采用传统的关系型数据库存储，应采用支持集群部署的关系型数据库类型，确保数据存储的稳定性。关系型数据库选型可采用但不限于以下几种：

a) MySQL 开源数据库；
b) PostgreSQL 开源数据库；
c) Oracle 商业数据库；
d) MS SQLServer 商业数据库。

7.3.3 缓存数据库

运行和计算数据应采用缓存数据库存储，应采用支持集群部署的缓存数据库类型，确保数据存储的稳定性。缓存数据库选型应可用但不限于以下几种：

a) Reids 开源缓存数据库；
b) Memcached 开源缓存数据库。

7.3.4 消息队列化数据存储

采集数据交换过程或消除异构问题应采用消息队列化数据库存储，应采用支持集群部署的消息队列化数据库类型，确保数据存储的稳定性。消息队列化数据库选型可采用但不限于以下几种：

a) Kafka 开源消息队列；
b) RabbitMQ 开源消息队列；
c) RocketMQ 开源消息队列；
d) ActiveMQ 开源消息队列；
e) ZeroMQ 开源消息队列。

7.3.5 非结构化数据存储

采集非结构化数据应采用非结构化数据存储，应采用支持集群部署的非结构化数据系统，确保数据存储的稳定性。非结构化数据选型可采用但不限于以下几种：

a) MinIO 开源分布式文件存储；
b) FastDFS 开源分布式文件存储。

7.4 平台开放性和扩展性

能耗监测系统应具备良好的开放性和扩展性，可与已建成的相关系统进行功能对接或数据交换，不断吸收计算机软硬件技术、电子监测技术、无线数据传输技术等先进技术的最新发展成果，改进成员企业用能模型和分项能耗拆分算法，提高系统的准确性和实用性。

8 能源管理系统

8.1 I/O服务器

根据系统负荷，设置1台I/O 服务器采集数据。此服务器完成与现场所有的modbus 、DL/T 645、101/103等协议系统的通讯，进行数据采集，并完成中间量计算、累积量计算、趋势、报警、数据短时归档、向数据库站传送数据等功能。实现与其他单元的通讯，并保存操作信息记录。

考虑到高并发，I/O服务器宜采用支持高并发的消息队列。

8.2 人机接口操作站（HMI）

在能源和设备管控中心设置人机接口操作站（HMI），作为整个系统的操作界面，对有关的能源数据和设备进行监控。这些操作站完成潮流监视、生产实时监视、设备状态显示、信息显示、实时曲线、语音报警等功能。在操作站上还可进行数据查询、报表查询、参数设置等工作。

8.3 应用服务器

应用服务器完成数据的长时归档、数据压缩、数据备份、与企业其他信息化管理系统的数据交换。与企业其他信息化管理系统的数据交换通讯协议采用网络通讯协议（TCP/IP）。归档数据从实时数据采集服务器送到数据库服务器。在实时数据采集服务器内对数据先进行初步运算和整理。如对流量的积算、电量的累积等。

运行有管理类的应用软件，包括在线监测、基本能源管理、安全应急管理、协同管理、数据查询、报表查询和打印、能源预测等应用软件。

保存报警、事件、操作记录、趋势等信息，能源管理的分析数据以此为基础。

9 能源数据采集

能源数据采集按照T/CIIA BBBB-2022执行。

10 能源数据分析

10.1 总体要求

能源和设备管控系统开发平台应集成和充分利用目前工业企业各种能耗监控设备和仪器采集到的各种能耗数据。本系统的分析和决策支持功能的设计应基于国家有关行业标准、标准的指标体系、标准的指标定义、标准的数据接口的原则，实现系统能在国内其他区域的能耗分析中具有可比性、代表性、和领先性。

10.2 能耗监测要求

能耗监测系统中应包含以下各种能耗，在实际部署实施中需结合企业实际用能状况而定：

a） 综合能耗；
b） 电能耗；
c） 水能耗；
d） 气体能耗；
e） 冷热能耗；
f） 其他能耗，如焦炭、原油等。

10.3 能耗分析要求

企业能耗在线分析应包含以下功能：

a） 能耗排名；
b） 能耗占比；
c） 能耗分布；
d） 能耗趋势；
e） 分类能耗分析（可再生能源占比等）。
f） 能耗折算碳排放分析。

10.4 能效分析要求

在实现能耗数据采集后，针对重点用能设备在具备数据采集的条件下，应对设备能效和负载进行分析：

a） 负载分析；
b） 设备能效；
c） 能源费用；
d） 单位能效；
e） 设备用电对比；
f） 峰平谷分析。

10.5 电能质量要求

针对电力数据，应具备以下功能分析：

a） 功率因数；
b） 谐波含量；
c） 电力和电能质量统计。

10.6 报表分析要求

针对各种能耗数据，应具备以下能耗报表：

a） 综合能源消耗统计；
b） 历年综合能耗；
c） 电量统计；
d） 气耗统计；
e） 水耗统计；
f） 能耗费用分析；
g） 单位产品或产值能耗。

10.7 能源管理要求

能耗在线监测和分析系统应该对用能异常及数据异常具备以下功能：

a） 能源异常；
b） 用能安全；
c） 监测点管理；
d） 工艺流程图；
e） 能源网络图。

10.8 节能普及要求

中心平台应提供对节能新技术、新方向、新路线等方面的宣传推广：

a） 节能新技术；
b） 合理化建议；
c） 节能宣传。

11 数据传输

11.1 概述

中心系统的数据传输需求包含数据上传和数据接收两部分。数据包括成员企业基本信息、成员企业能耗数据、系统消息等内容。

11.2 数据上传

成员企业数据中心需要向集团数据中心上传数据，部署在企业内部的采集器需要向企业中心上传数据，且每一步骤应记录操作日志。成员企业数据中心的数据上传工作流程见图3。

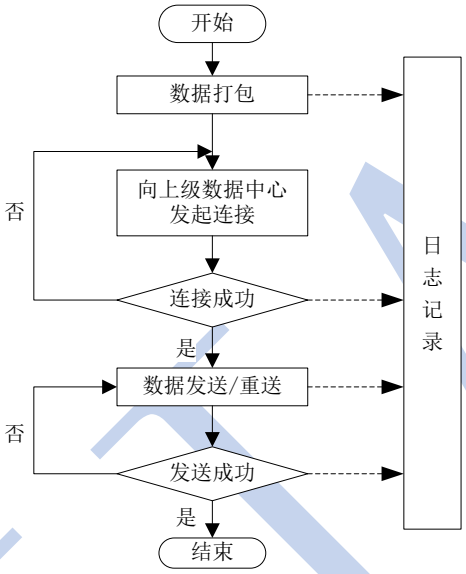

图3 数据上传工作流程图

a） 数据打包

定时启动数据打包程序，从数据库中抽取需要上报的数据，按照通信双方约定的协议、报文格式封装成TCP格式的数据包，并压缩数据包。

b） 发起连接

向上一级数据中心服务器发送握手消息，建立连接状态。如果连接不成功则再次发起连接。

c） 数据发送

调用上一级数据中心的数据接收网络服务（Web Services），基于TCP传输协议将压缩后的TCP数据包发送出去。如因网络故障或繁忙等原因造成的发送失败则定时重新发送，直到发送成功。

目前约定各级数据中心分时段集中上传上一日的数据包。今后随着数据中心增多、各数据中心监测数据量增大等情况变化，可加大数据传输频率，减小数据包容量。

11.3 云边平台通讯规约

在综合智慧能源物联网体系中，边平台与云平台通讯根据物理链路及数据类型不同，一般宜使用以下几种规约。

a） MQTT 规约

MQTT是物联网常用传输规约，基于发布/订阅（publish/subscribe）模式，所有的物联网终端都通过TCP连接到云端，云端通过主题的方式管理各个设备订阅的通讯内容，并实现设备与设备之间消息的转发，为远程设备提供实时可靠的消息服务。

作为一种低开销、低带宽占用的即时通讯协议，在物联网、小型设备、移动应用等方面有较广泛的应用。

b） Coap 规约

Coap（Constrained Application Protocol）是一种在物联网世界的类Web规约，它的详细规范定义在 RFC 7252。Coap规约占用资源比较少，可使用在资源受限的物联网设备上，在无线网络场景下有广泛应用。

c） SFTP/FTP 规约

SFTP/FTP规约是文件类传输规约，适用于风电场内功率预测、故障录波、振动监测等以文件形式传输数据的场景。

d） DDS 规约

DDS（Data Distribution Service for Real-Time Systems），面向实时系统的数据分布服务，这是OMG组织提出的协议。DDS很好地支持设备之间的数据分发和设备控制，设备和云端的数据传输，同时DDS的数据分发的实时效率非常高，能做到秒级内同时分发百万条消息到众多设备，在服务质量（QoS）上也提供非常多的保障途径。

e） IEC 60870-5-104 规约

IEC 60870-5-104规约由国际电工委员会制定为远动信息的网络传输提供了通信规约依据。

11.4 数据传输质量

数据采集和传输中，应提供相应的保护措施，努力提高数据的质量，尽量消除因为采集和通讯对系统使用的不良影响。

在数据质量的统计分析中，主要包括但不限于阀值范围检查、数据丢失检查、增量值域（跳变）检查。各检查之间相互独立，互不影响，数据应可以同时被赋予多种检查属性。

11.5 数据处理

系统的数据治理工作，应能对数据进行存储、插补、清洗、计算，并统一标准和口径，形成标准数据，建立基础模型、融合模型和挖掘模型。数据治理的范围主要针对从控制系统（SCADA）以后的数据流（含部分机型可编程逻辑控制器（PLC）直连）。数据采集应包含场站各种类型的实时采集，场站数据到中心侧系统的转发，以及中心侧系统的实时接收和数据入库等环节。数据采集质量直接影响数据传输稳定性及数据质量，其标准化应包含底层标准化、中间层标准化和上层标准化。

数据采集处理措施应包括但不限于：设备接入认证措施、数据传输防误措施、边缘计算措施、高可用措施、风机数据采集疑难问题处理措施、数据采集接入措施等。

11.6 数据接收

数据中心应接收各供应链企业上传的数据，且每一步骤应记录操作日志。平台中心系统的数据接收工作流程见图4。

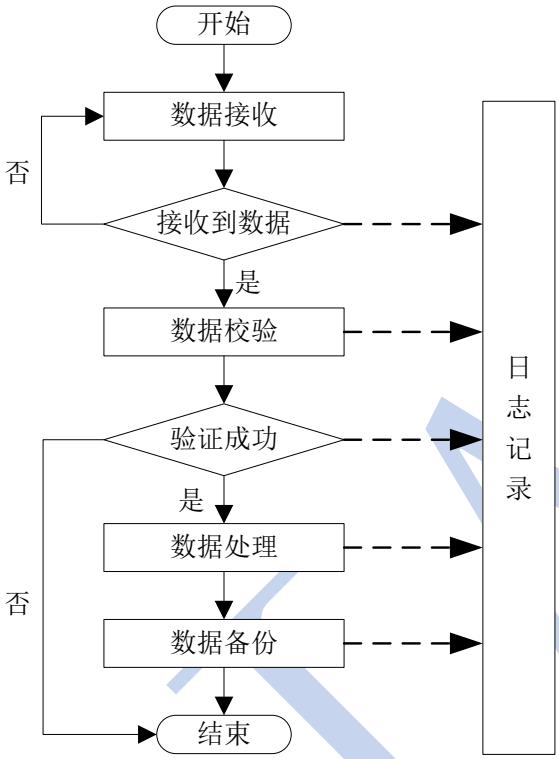

图4　数据接收工作流程图

a)　数据接收

数据接收方式为被动接收，采用网络服务（Web Services）技术实现，基于Socket包传输协议。向下级数据中心返回接收成功与否的消息。接收成功后将数据包解压缩，还原为标准格式的TCP数据包。

b)　数据校验

数据校验包括两个方面：数据格式校验以及数据内容校验。数据格式校验主要对上传的成员企业与能耗信息进行TCP校验，校验应符合相关文件中对于成员企业与能耗信息TCP格式的规定；数据内容校验主要对上传的成员企业与能耗信息中包含数据的规范性及合理性进行检测与分析。校验成功后进行数据处理，失败则结束本次接收操作。

c)　数据处理

对上传的成员企业与能耗信息的TCP数据进行解析以及数据存储至数据库，并调用数据分析功能对上传数据进行统计分析，生成数据仓库记录。

d)　数据备份

历史数据库，对接收到的成员企业和能耗数据以及附件进行备份。

11.7　数据上传的 TCP 接口要求

应对上传数据的TCP接口进行统一规范，各成员企业自主开发的上传数据协议应遵照执行，以确保各系统数据的可交换性。

12　系统安全

12.1　概述

系统的安全包含访问控制安全、数据安全和网络安全。

12.2　访问控制功能

系统访问控制功能应符合以下基本要求：

a） 系统超级管理员：权限应包括后台流程配置、数据库维护、为其他用户授权；
b） 能源管理者：应具有最高使用权限，可以浏览所有报表；
c） 局域管理者：应具有相关负责区域的管理权限；
d） 一般用户：应只限于综合或者汇总后的数据。

12.3 数据安全控制

应保证信息资料和能耗数据资料的安全性，所有入库的数据资料应有相应的备份策略和安全策略，对外共享或者对外提供的数据资料要严格按照“用户级别及权限” 的规定来授权用户对资料的访问，防止越权访问。

应有系统数据定期备份和灾难恢复机制，有条件者可实行数据异地备份。

12.4 网络安全控制

信息管理平台应进行网络安全控制。

13 数据中心建设要求

13.1 总体要求

本系统建设应充分利用现有先进、成熟技术和考虑长远发展需求，统一规划、统一布局、统一设计、规范标准、突出重点、分步实施，在实施策略上，应根据实际需要及投资金额，统一领导、统筹规划、标准化及核心业务重点推进，注重信息的共享和安全体系建设，保证系统建设的完整性和投资的有效性，建设先进而实用的重点用能单位能耗在线监测系统。

13.2 平台建设原则

13.2.1 标准化和规范化原则

从业务、技术、运行管理等方面对项目的整体建设和实施进行设计，充分体现标准化和规范化。

13.2.2 开放性和可扩展性原则

系统结构应按照开放性和可扩展性原则设计。系统应采用开放性、标准化的平台设计以尽可能地利用已有的设备、软件及信息资源；另一方面，系统对于未来可能增添的新的功能、新的用户预留接口和二次开发应用程序编程接口（API），系统可以随形势的发展而不断扩展。

13.2.3 技术的先进性和成熟性原则

在设计理念、技术体系、产品选用等方面考虑先进性和成熟性的统一，以满足系统在很长的生命周期内有持续的可维护性和可扩展性。

13.2.4 可靠性原则

系统从系统结构、技术措施、设备选型和安装校验等方面综合考虑，确保系统整体运行的可靠性和安全性。

关键设备考虑备份与冗余措施，软件考虑维护保障能力、容错能力。

13.3 环境要求

信息平台中心机房的建设，应符合GB 50174-2017的要求。

机房关键设备应按冗余要求进行配置，在设备冗余能力范围内，不会因故障原因而导致数据中心信息系统运行中断。机房环境条件如下：

a） 机房环境温度： 18℃～27℃；
b） 机房湿度：35%～60%；
c） 安保系统：具备视频监控及出入口权限控制；
d） 应具备灭火应急系统。

13.4 服务器配置要求

为保障信息管理系统的正常运行，服务器的选型配置应符合以下要求：

a) 服务器应选用当前国内先进的、主流的机型，要具有较高的性能价格比，同时系统应符合标准化，开放式系统互连的原则，易于开发维护，还要具有较强的网络通信和数据库管理功能和较强的扩充能力；
b) 服务器支持对称多处理方式（SMP）和服务器集群 Cluster 方式；
c) 服务器的设计必须确保其高效、可靠及安全性(如带错误检查和纠正（ECC）校验，对数据的奇偶校验，热切换等)，同时又能极大简化维护工作；
d) 服务器要具有良好的性能，具有较高的系统吞吐量（TPS）值；
e) 服务器在设计上最好采用模块化及通用件设计，易于扩充，以胜任网络及应用的扩展；
f) 服务器厂商具有良好的售后服务和技术支持；
g) 虚拟化宿主机每台服务器内存应不低于 128G，中央处理器（CPU）不低于 2 颗，每颗 CPU 不少于 6 核。

13.5 存储配置要求

存储配置应符合以下基本要求：

a) 存储阵列控制器，应配置精简指令集计算机（RISC）架构双活控制器，应具有独立的磁盘冗余阵列（RAID）校验芯片；
b) 前端主机接口，应配置不少于 8 个 16 GB/s FC 型光纤端口，支持扩展不少于 4 个 1GB 的 iSCSI 端口；
c) 磁盘列阵配置容量应满足监测数据需求及未来 10 年内的扩展性要求。
d) 磁盘扩展能力，最大可扩展磁盘数量应不少于 110 块；
e) RAID 级别支持，应支持 RAID 0/1/1+0/3/5/6；
f) 支持磁盘类型，应支持 SAS，NL_SAS 及固态硬盘（SSD）等类型；
g) 应配置后备锂电池，支持 BBU、flash、控制器缓存镜像等三重数据保护；
h) 应支持后台介质扫描、RAID 级别在线迁移、LUN 在线扩容，需支持卷快照、卷复制、卷远程镜像功能，需支持自动精简功能；
i) 应配置相应数量的路径冗余软件,并支持 I/O 通道故障切换和链路负载均衡(Windows/Linux)；
j) 应配置冗余电源,风扇；
k) 应支持 Windows、Linux、UNIX 等操作系统。

13.6 网络配置要求

13.7 总体要求

交换机、防火墙不应为同一品牌。所有设备均应从设备性能、可靠性、协议、安全性、服务质量、易管理性、可扩展性等方面考虑。

13.8 隔离区 DMZ 区-接入交换机

网络交换机应符合以下基本要求：

a) 应支持堆叠的三层交换机，全部端口支持千兆，支持 10GE 扩展模块；
b) 整机 10/100/1000M 电接口应不少于 48 个，10GE 光纤接口应不少于 2 个；
c) 单台支持可扩展插槽应不少于 1 个，扩展模块支持在线热拔插；
d) 交换容量应不低于 160 Gbps；
e) 转发性能应不低于 120 Mpps，应可实现端口全线速交换转发；
f) 局域网 MAC 地址表应不低于 32K，支持 MAC 地址自动学习和老化；
g) 应支持 4000 个虚拟局域网（VLAN），支持基于 MAC/协议/IP 子网/策略/端口的 VLAN；
h) 应支持静态路由、RIP V1/2、OSPF、IS-IS、BGP；
i) 双电源，可插拔，交流供电；
j) 端口配置：48 个 10/100/1000 BASE-T 端口。

13.9 核心业务区-核心交换机

核心业务交换机应符合以下要求：

a） 要求为框式交换机，业务插槽应不少于 3 个；
b） 交换容量应不低于 540 Gbps；
c） 转发性能应不低于 360 Mpps，要求实现端口全线速交换转发；
d） 应支持虚拟局域网（VLAN）交换，支持 QinQ、增强型灵活 QinQ；
e） 应支持局域网 MAC 地址自动学习和老化；
f） 应支持 RIP、OSPF、ISIS、BGP 等 Ipv4 动态路由协议；
g） 应支持 RIPng、OSPFv3、ISISv6、BGP4+等 Ipv6 动态路由协议；
h） 应支持组播、多协议标签交换（MPLS）、服务指令（QoS）功能；
i） 一体化总装机箱,双主控板,双交流电源；
j） 端口配置：48 个千兆以太网接口（GE）电口。

13.10 核心业务区—接入交换机

接入交换机应符合以下要求：

a） 应支持堆叠的三层交换机，全部端口支持千兆，支持 10GE 扩展模块整机；
b） 10/100/1000M 电接口应不少于 48 个，10GE 光纤接口应不少于 2 个；
c） 单台支持可扩展插槽应不少于 1 个，扩展模块支持在线热拔插交换容量应不低于 160Gbps 转发性能不低于 120Mpps，要求实现端口全线速交换转发 MAC 地址表应不低于 32K；
d） 应支持 MAC 地址自动学习和老化；
e） 应支持 4000 个 VLAN；
f） 应支持基于 MAC/协议/IP 子网/策略/端口的 VLAN 支持静态路由、RIP V1/2、OSPF、IS-IS、BGP 双电源，可插拔，交流供电；
g） 端口配置：48 个 10/100/1000BASE-T 端口。

14 安全配置要求

14.1 防火墙

防火墙应符合以下要求：

a） 百兆防火墙，应采用专用设计的硬件平台，支持冗余电源；
b） 每秒新建会话能力应不少于 35000 个；
c） 最大并发连接数应不少于 30 万；
d） 最大吞吐量应不低于 4G；
e） 最大入侵防御系统（IPS）吞吐量应不少于 1G；
f） 最大访问控制策略应不少于 20000 条；
g） 具有访问控制，入侵防御系统 IPS 防护，应用层攻击保护功能；
h） 支持远程管理、维护。
i） 设备应配置 6 个千兆电接口；
j） 配置内存应不少于 2GB。

14.2 堡垒主机

堡垒主机应符合以下要求：

a） 含单交流电源，2 个 USB 接口，1 个 RJ45 串口，1 个 GE 管理口，4 个 GE 电口，应不小于 2T SATA 硬盘。缺省授权管理 100 台设备；
b） 支持证书、口令、短信、动态字符等多种认证方式，可基于角色和安全等级的动态授权；
c） 支持虚拟网关和虚拟防火墙；
d） 可支持不少于 500 个并发用户。

14.3 网络安全审计系统

网络安全审计系统应符合以下要求：

a) 含交流冗余电源，标准配置提供一路监听，应支持对未注册的用户终端实施自动阻断网络的功能；
b) 应支持对用户的进程审计、服务审计、主机资源审计、主机端口审计、主机账号审计、主机文件操作审计；
c) 应支持客户端媒体介质控制，并进行日志记录与审计；
d) 应支持客户端 IP 与 MAC 绑定控制管理；
e) 支持吞吐量应不少于 1.0Gbps；
f) 并发会话数应不少于 80 万；
g) 并发用户数应不少于 2000 个；
h) 设备接口应不少于 4 个千兆电口；
i) 磁盘容量应不小于 500G。

14.4 漏洞扫描

漏洞扫描应符合以下要求：
a) 含交流单电源，1 个 RJ45 串口，1 个 GE 管理口，4 个 10M/100M/1000M 自适应以太网电口扫描口，标准配置提供 1 路授权扫描端口，IP 点授权，授权可扫描总数量不多于 512 个无限制范围的 IP 地址或域名，应支持能对扫描目标的安全脆弱性进行全面检查，检查内容包括缺少的安全补丁、暴露的危害信息、不安全的服务配置等；
b) 漏洞库的数量应不低于 2000 条，应支持国际 CVE 标准；应支持对主流数据库包括：Sybase、SQLServer、Oracle、MySql、DB2 等的扫描检测功能；
c) 支持的最大并发扫描 IP 应不少于 30 个，单个 IP 的最大并发扫描线程应不少于 30 个，单个 IP 的平均扫描时间不大于 30s，扫描 IP 数量 500 个以上。

14.5 入侵检测系统（IDS）

入侵检测系统应符合以下要求：
a) 百兆入侵检测系统，应大于 4 个 10/100M 以太网口，1 个异步控制口；
b) 含交流冗余电源模块，2 个 USB 接口，1 个 RJ45 串口，2 个 GE 管理口；
c) 漏洞特征库能自动或者手动升级；
d) IPS 防护对像包括防护服务器和防护客户端两种，防护的类型包括蠕虫、木马、后门、DoS、DDoS 攻击探测、扫描、间谍软件、利用漏洞的攻击、缓冲区溢出攻击、协议异常、IPS 逃逸攻击等；IPS 能对应用服务器信息进行隐藏，且能对服务器进行扫描，评估服务器对漏洞的防护能力。

14.6 安全认证网关

安全认证网关应符合以下要求：
a) 应支持基于 Linux、Windows 等操作系统的企业端设备 CA 数字证书的身份认证和传输加密，满足国家信息中心的数字证书信任链验证及证书黑名单验证，符合相关接入要求；
b) 最大并发连接数 400 个；
c) 最大新建连接数 60 次/s，每秒完成交易数(TPS)1000 次；
d) 最大流量应不小于 50Mbps；
e) 系统可设置是否需要用户提交用户证书；
f) 系统可自动、动态更新黑名单，不需要重新启动服务，支持 LDAP、HTTP 等多种方式更新，支持 B64、DER 等多种格式；
g) 系统可拥有多个站点证书，不同的服务可拥有不同的站点证书；
h) 一个安全套接字层（SSL）服务中可同时配置多条证书链，验证不同 CA 的用户证书；
i) 应支持主流数字证书认证体系，且支持接入国家电子政务外网信息体系中；
j) 系统可将用户证书信息包括扩展项信息传送给应用系统；
k) 应支持 B/S 应用；支持 FTP、telnet、远程桌面以及通用的 C/S 应用，系统可创建多个 SSL 服务，保护不同的应用服务，也可采用同一个 SSL 服务保护多个应用服务（需客户端）；
l) 系统将真正应用服务的地址隐藏，用户仅知道网关地址；

m） 在有防火墙 NAT 映射的情况下应正常访问有重定向的网站；
n） 可独自完成基于数字证书的身份认证；
o） 国密算法支持：应支持 RSA1024 及 2048 位算法；应支持商用密码非对称算法 SM2；应支持商用密码杂凑算法 SM3；应支持商用密码对称算法 SM4；应支持扩展国密对称加密算法 SM1；
p） 能提供浏览、下载等日志管理功能，且可与第三方审计系统进行关联功能；
q） 应支持串联、并联等多种部署方式，适用不同的网络环境和应用需求；
r） 应拥有公安部销售许可证。

14.7 Web 防火墙（WAF ）设备

Web防火墙设备应符合以下要求：
a） 标准配置含 SQL 注入/XSS 防护、Web 常规攻击防护、扫描防护、Cookie 安全防护、URL ACL、CSRF 防护、HTTP 协议防护、ARP 欺骗防护、非法下载防护、非法上传防护、Web 内容安全防护、网页盗链、爬虫防护等功能；
b） 应提供网页篡改防护以及服务器侧恶意代码过滤功能；
c） 含交流单电源，1 个 RS232 串口，1 个 FE 管理口，4 个 100/1000 M 自适应电口（Bypass）；
d） 标准配置提供 1 路电口 WAF 防护，应支持 Bypass。

14.8 VPN 网关

SSLVPN与IPSECVPN 均可实现由互联网企业监测端到系统平台服务端的加密访问，实现证书的验证和传输加密，下面提供两类产品的要求及参数：
a） SSLVPN：
1） 应支持基于 CA 数字证书，实现互联网企业监测端到系统平台服务端的身份验证和加密通信。
2） 应支持互联网企业监测端到系统平台服务端的传输加密；
3） 应支持第三方数字证书认证，支持硬件加速，提供 C/S 应用支持；
4） 最大并发连接数应不少于 400 个；
5） 并发客户端数应不少于 2000 个；
6） 系统能对用户连接数、应用访问情况，系统资源占用等信息进行详细统计，为更好了解应用及调节资源提供基础；
7） 系统实现客户端策略的统一下发，用户无需对客户端进行任何配置；
8） 对于特定应用，系统应采用用户映射技术，将证书映射为原有系统中的账户，并进行自动登录，在后台应用无需修改的情况下实现单点登录；
9） 系统通过特有的 cookie 技术将用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息；
10） 系统应支持国密 SM1/SM2/SM3 算法；
11） 实现 URL 级别的访问控制，对于不同用户、不同角色应实现不同的控制；
12） 应支持单点登录功能（SSO）。
b） IPSECVPN:
1） 应支持基于 CA 数字证书,实现互联网企业监测端到系统平台服务端的身份验证加密通信；
2） 应支持第三方数字证书认证，支持硬件加速，提供 C/S 应用支持；
3） 加密速度应不低于 280 Mbps；
4） 并发客户端数应不少于 2000 个；
5） 应支持虚拟化远程应用发布；
6） 应支持单点登录功能（SSO）；
7） 系统对于认证错误可重定向到用户指定页面，增强友好性。

14.9 数据库安全审计系统

数据库安全审计系统应符合以下要求：
a） 电源硬件冗余，配置双交流电源；
b） 性能指标，检测能力应不低于 100 Mbps；

c） 最大并发 TCP 连接数应不少于 1 万个；
d） 每秒新增 TCP 并发连接数应不少于 1000 个；
e） 应支持对不少于 2000 在线用户进行审计；
f） 端口配置应不少于 4 个 10/100/1000 M 电口；
g） 系统要求，模块化设计，应具有良好的可扩展性；
h） 旁路方式或透明方式接入网络；
i） 审计引擎应支持不同的操作系统类型（Windows、Linux、Unix 等）；
j） 应支持同时审计多种数据库及跨多种数据库平台操作，例如：ORALCE、SQL SERVER、MYSQL、DB2、Sybase、Postpresql 等各类主流数据库系；
k） 系统应支持基于 IP 地址、时间、用户/用户组、数据库用户名、数据库类型、数据库表名、字段名、关键字等组合数据库审计策略；
l） 应支持实时审计用户对数据库系统所有操作，如：登录、注销、插入、删除、执行存储过程、用户自定义操作等，支持分析、提取 SQL 语句中绑定变量，并可完全监测还原 SQL 操作语句包括源 IP 地址、目的 IP 地址、访问时间、MAC 地址、数据库用户名、客户端类型、数据库操作类型、数据库表名、字段名等；
m） 应支持对邮件系统的审计，支持 SMTP、POP3、WEBMAIL 等协议，支持基于邮箱地址、邮件主题、邮件内容、附件名的关键字审计功能；
n） 日志管理，应支持按时间、级别、源\目的 IP、源\目的 MAC、协议名、源\目的端口为条件进行查询；
o） 应支持日志自动备份；
p） 应支持日志归并；
q） 应具备分级管理功能，满足分级管理的要求；
r） 应支持对审计数据的多种查询方式；
s） 应提供多种形式的审计报表，数据格式报表可以保存为 EXCEL、TXT、WORD、HTML 等多种文件类型；
t） 应具备对外接口，可将审计结果上报给安全管理平台或其它安全产品。