

# 电科院设备状态监测与评价系统自主可控改造

## 技术规范书



广州供电局电力科学研究院

2026年3月

## 1. 总则

1.1 本招标技术文件适用于广州供电局的电科院设备状态监测与评价系统自主可控改造项目技术服务，它提出了该服务的技术要求、功能要求、性能要求等方面的技术要求。

1.2 本招标技术文件提出的是最低限度的技术要求。凡本招标技术文件中未规定，但在相关信息系统的行业标准、国家标准或 IEC 标准中有规定的规范条文，投标方应按相应标准的条文进行系统开发。对国家有关安全、环保等强制性标准，必须满足其要求。

1.3 如果投标方没有以书面形式对本招标技术文件的条文提出异议，则意味着投标方提供的技术服务完全符合本招标技术文件的要求。如有任何异议，都应在报价书中以“对招标技术文件的意见和同招标技术文件的差异”为标题的专门章节中加以详细描述。

1.4 本招标技术文件所使用的标准如遇与投标方所执行的标准不一致时，按较高标准执行。

1.5 本招标技术文件经买、卖双方确认后作为订货合同的技术附件，与合同正文具有同等的法律效力。

1.6 本招标技术文件未尽事宜，由买、卖双方协商确定。

1.7 投标方在应标技术文件中应如实反映应标产品与本招标技术文件的技术差异。如果投标方没有提出技术差异，而在执行合同的过程中，招标方发现投标方提供的产品与其应标招标技术文件的条文存在差异，招标方有权利要求解除合同，根据严重程度在对下一批次招评标工作中进行综合评标分扣减或暂停投标资格。

1.8 投标方应在应标技术部分按本招标技术文件的要求如实详细的填写技术方案，并按此方案进行报价，如发现二者有矛盾之处，将以报价表的配置为准。

1.9 投标方应充分理解本招标技术文件并按本招标技术文件的具体条款、格式要求填写应标的技术文件，如发现应标的技术文件条款、格式不符合本招标技术文件的要求，则认为应标不严肃，在评标时将有不同程度的扣分。

1.10 标注“★”的条款为关键条款，必须满足；标▲的技术要求如有不符将被扣分，以上两项作为评标时打分的重点参考。

## 2. 通用技术要求

### 2.1. 设计原则

为实现本项目的建设目标，应预留扩展与升级空间。本项目建设除应按引用规范执行外，还应符合国家、电力行业、南方电网公司现行的有关标准规定。

#### 1) 先进性要求

本项目硬件需具备先进、成熟、可靠的特点；软件需要采用适合本项目的软件体系结构，采用符合相关标准的数据格式，具有较强的可维护性。

其体系架构应符合南方电网公司、广东电网公司和广州供电局相关规范，系统数据接入方案需满足南方电网公司、广东电网公司和广州供电局要求。

#### 2) 开放性要求

系统需要支持跨平台的移植和运行，并能方便地进行数据的迁移和系统切换；要考虑与其它系统的接口，并且能够提供二次开发；能够全面整合广州供电局在相关技术领域开发的软件。

#### 3) 系统安全性要求

系统应根据分层管理的原则进行权限控制，提供严密的扩展功能，身份验证、访问控制、数字签名、多层次的保密手段等措施，确保系统和数据的安全性和完整性。系统需充分考虑网络数据安全，满足广州供电局信息安全防护要求，系统应符合广州供电局网络安全三同步管理要求。

#### 4) 稳定性要求

系统应保证在硬件运行正常的前提下，服务器在长时间运行后，系统性能不会出现大的下降，前台应用和后台服务系统不应出现崩溃现象。

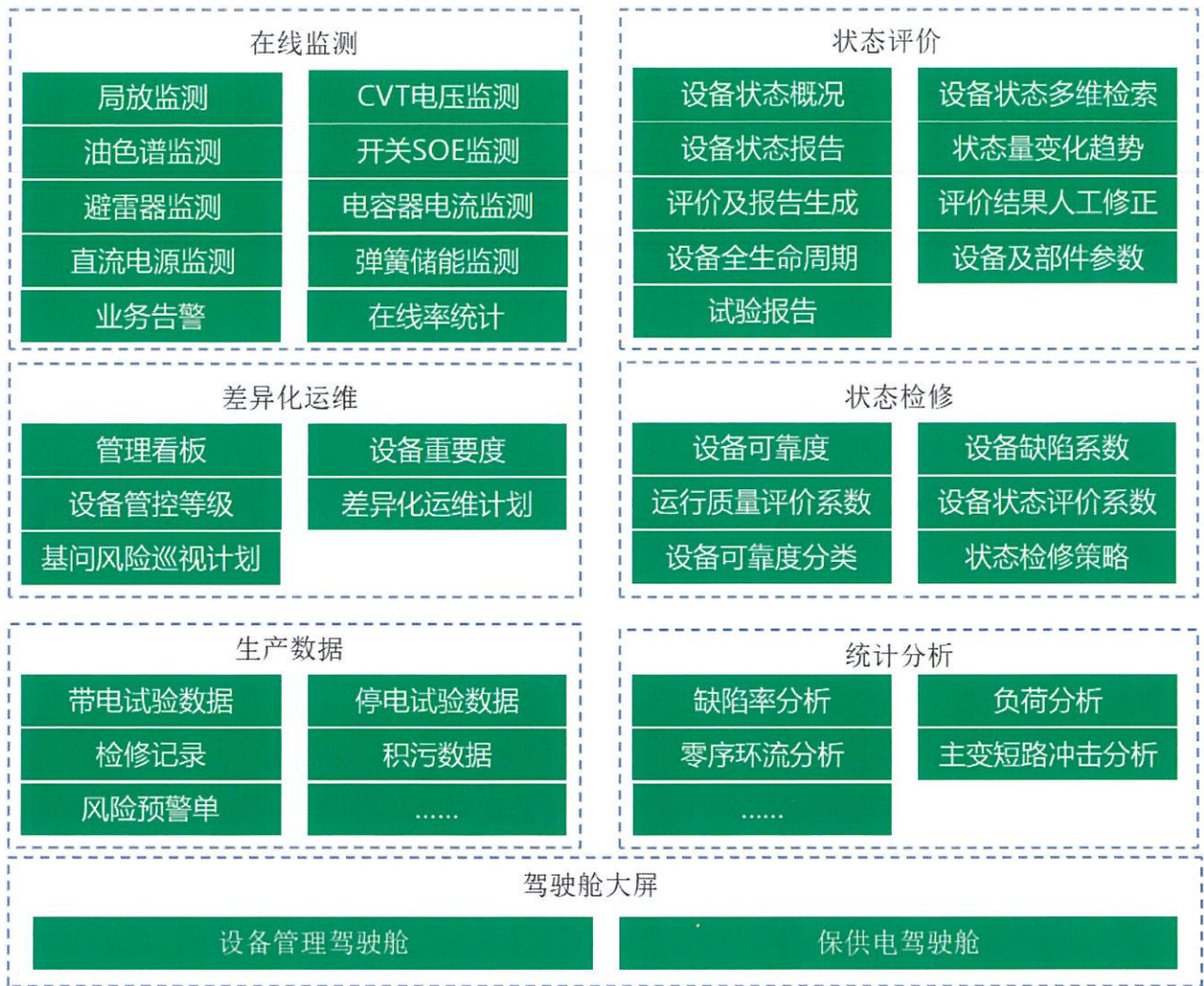
#### 5) 易操作要求

用户接口及界面设计将充分进行优化设计，界面友好、美观，操作符合日常工作流程需要，易学习、易操作，系统提示和帮助信息准确、及时。

#### 6) 网络安全要求

系统建设与试运行阶段均满足系统网络安全要求，采用的系统数据库、操作系统、中间件应满足自主可控要求，应支持通过数认登录。

## 2.2.应用架构

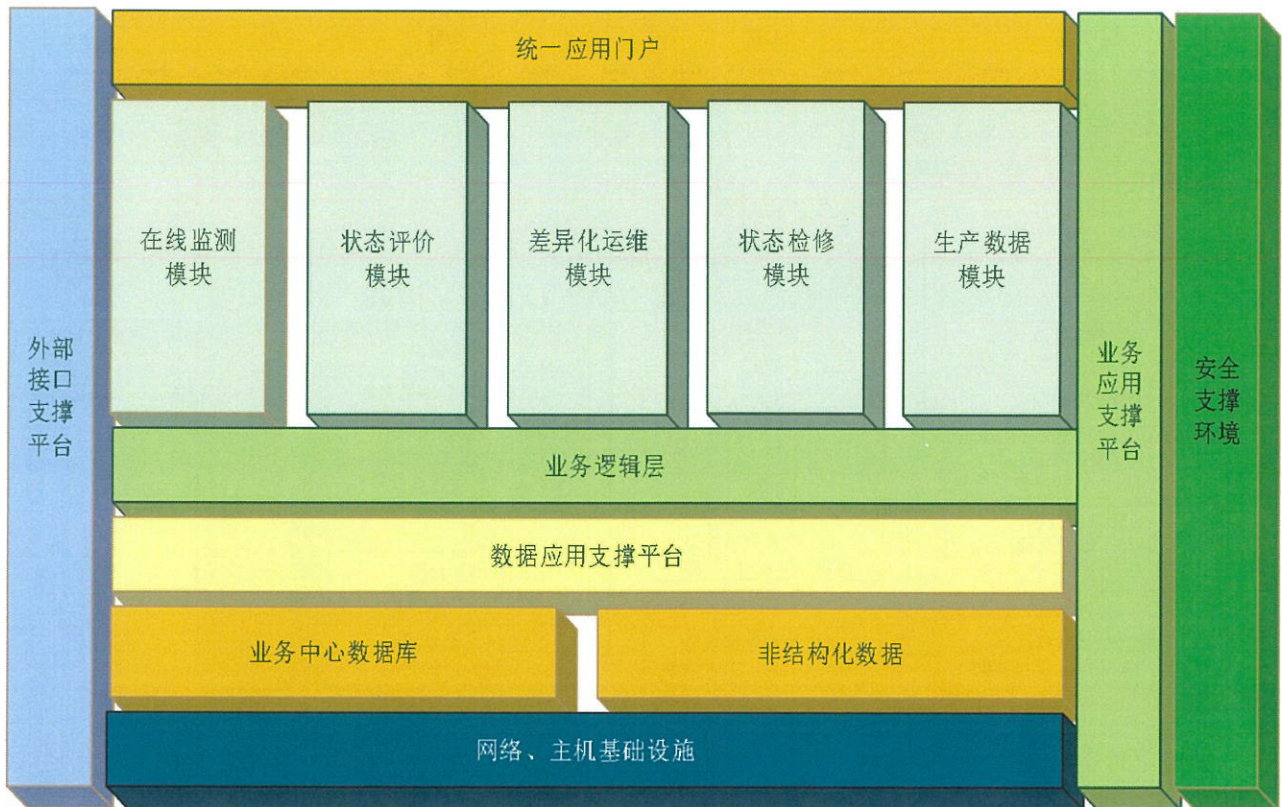


状态状态监测与评价系统分成 Web 端和大屏端两部分。

Web 端主要包括在线监测、状态评价、差异化运维、状态检修、生产数据、统计分析等几部分；

大屏端主要包括：设备管理驾驶舱、保供电驾驶舱。

### 3.2.平台架构



平台采用分层架构设计和开发，满足当前设计的前提下，方便未来对系统进行扩展。

基础设施层：底层由通用的网络、主机等基础设施提供硬件环境；

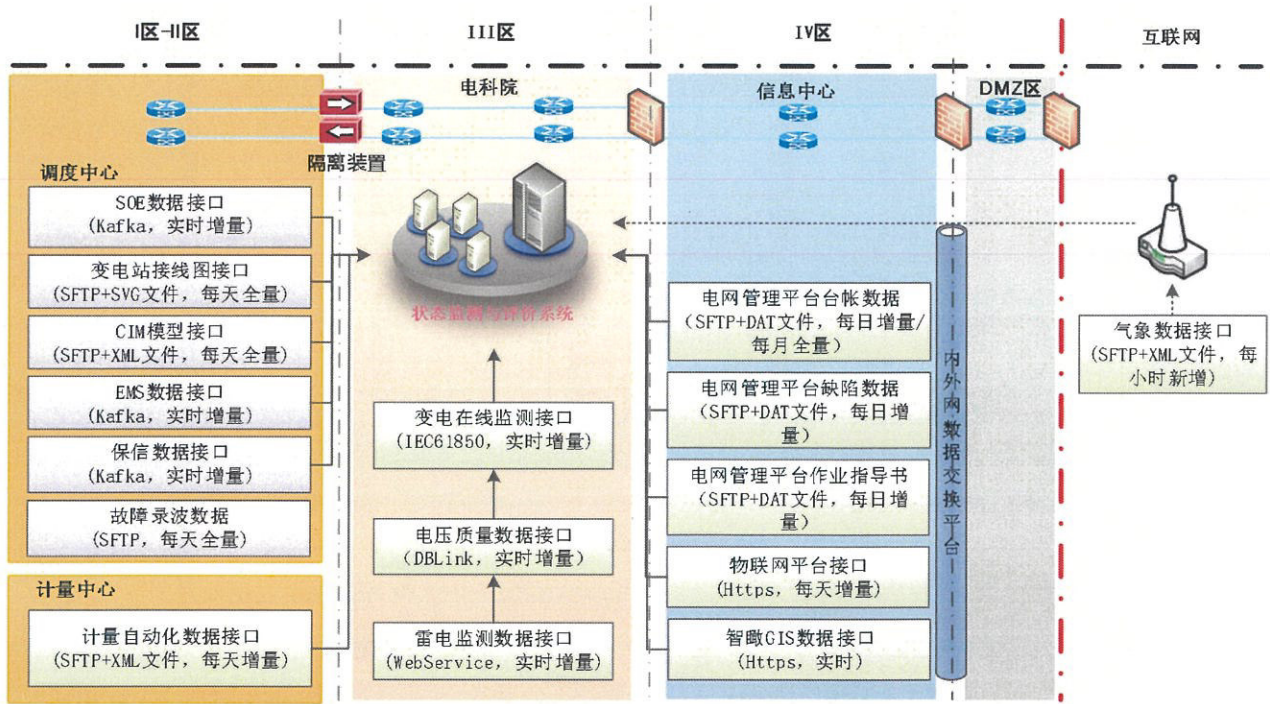
数据存储层：由通用的 RDBMS 系统和文件服务器对业务中的结构化数据和非结构数据进行存储管理；

数据支持层：提供标准统一的数据接口和数据处理算法，方便业务层实现对复杂业务的高性能计算和数据处理；

业务逻辑层：对各种业务规则进行实现和计算；

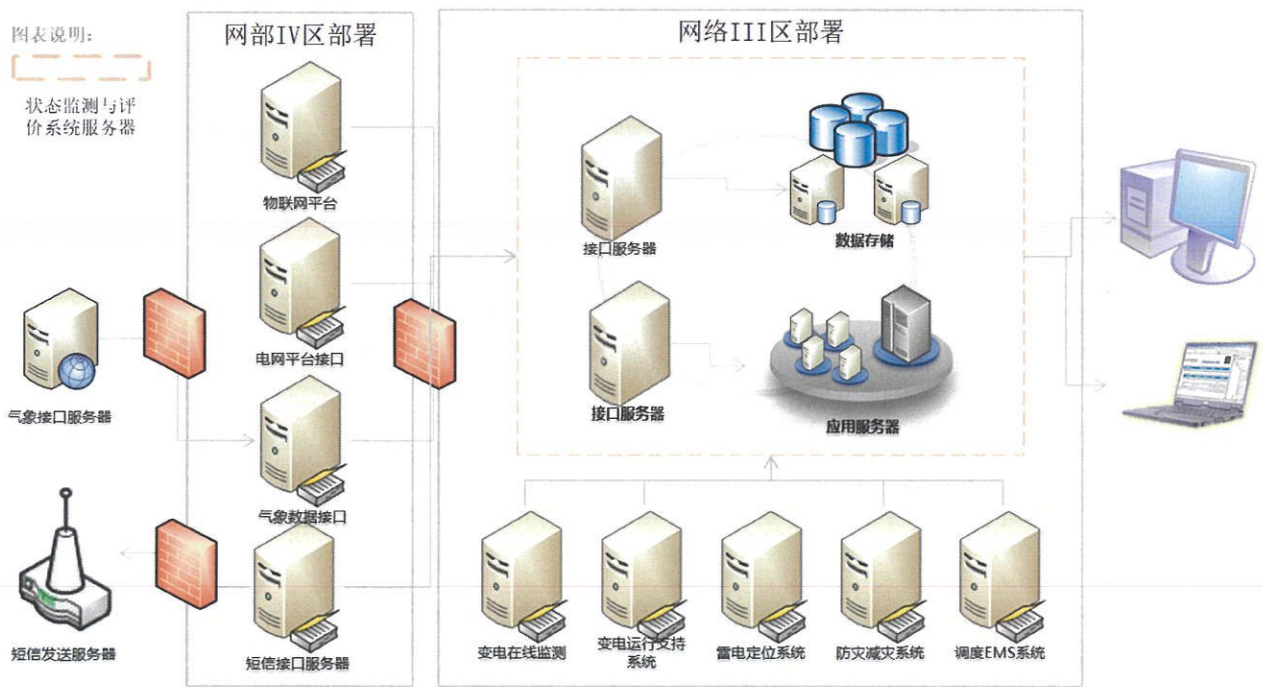
应用展示层：将各个子模块以统一风格的 Web 方式进行可视化展示。

## 2.4.数据架构



状态评价中心系统需要与II区、III区、IV区多个系统进行数据交互，根据业务需求实现实时或全量数据接入，实现数据融合，支撑系统应用功能建设。

## 2.5.部署架构



系统在网络 III 区、网部 IV 区均有相应服务器部署；  
 使用两台服务器部署主数据库，使用一台服务器部署监视器，确保数据安全存储。  
 应用服务器采用集群方式，确保系统的稳定和高可用性。

## 2.6.性能指标

采用基于 RDBMS 技术实现数据的存储和管理；

支持基于 HTTPS 数据传输协议方式，进行 SSL 加密信道传输；

基于 IEC61850、MQTT、Kafka、SFTP 等协议构建数据通信，实现数据传输的安全管控功能，以满足数据传输过程中的管控要求；

文件类数据通过专业的文件服务器进行存储，尽量通过压缩减少存储空间，确保存储 3 年以上的数据；

一般展示类业务响应时间<3 秒，峰值时间<5 秒；统计分析类业务响应时间<15 秒，峰值时间<30 秒。

峰值在线用户 50，平均在线用户 10；

最大宕机时间 1 小时，平台支持常用备份软件，提供备份系统和无单点故障，系统应满足 7×24 小时可以使用。

### 3.功能要求

#### 3.1.以可靠性为中心的变电设备状态检修的功能升级改造

##### 3.1.1.数据接口功能改造

★状态评价主要从电网平台接入相关数据，包括设备台帐、缺陷、作业计划、作业指导书、试验数据、组织机构数据等，并且完成数据结构化，支持以设备为中心的大数据分析。

##### ★3.1.2.状态评价待办任务

###### 3.1.2.1.基于缺陷生成评价待办任务并自动复归状态

根据接入的电网平台的缺陷数据，将缺陷数据与设备关联，并生成一个待评评价任务，状态评价专责可以方便的对此设备的进行扣分操作。

当电网平台中的缺陷数据消缺后，系统后台能自动对扣分操作进行恢复，并对设备状态进行自动变更。

###### 3.1.2.2.基于试验数据生成评价待办任务并自动复归状态

根据接入的电网平台的试验数据，将试验数据与设备关联，并生成一个待评评价任务，状态评价专责可以方便的对此设备的进行扣分操作。

当电网平台中的试验数据变正常值之后，系统后台能自动对扣分操作进行恢复，并对设备状态进行自动变更。

##### ▲3.1.3.设备状态评价中心

设备状态评价中心是基于南方电网公司主网一次设备状态评价导则，结合设备状态大数据分析结果，实现了设备状态综合评价与自动推送，评价覆盖基本所有变电一次设备，是掌握设备运行状态的重要手段。

###### 3.1.3.1.模块总览

通过图表展示各类设备的严重、异常、注意、异常四种状态的设备数量。

### 3.1.3.2. 变压器设备状态评价

根据变压器的状态评价导价，对某个变压器进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与变压器相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

### 3.1.3.3. 电抗器设备状态评价

根据电抗器的状态评价导价，对某个电抗器进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与电抗器相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

### 3.1.3.4. GIS 设备状态评价

根据 GIS 设备状态评价导价，对某个 GIS 设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与 GIS 设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

### 3.1.3.5. 断路器设备状态评价

根据断路器设备状态评价导价，对某个断路器设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与断路器设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

### 3.1.3.6. 隔离和接地开关设备状态评价

根据隔离和接地开关设备状态评价导价，对某个隔离和接地开关设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与隔离和接地开关设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.3.7. 避雷器设备状态评价

根据隔离和接地开关设备状态评价导价，对某个隔离和接地开关设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与隔离和接地开关设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.3.8. 电容器设备状态评价

根据电容器设备状态评价导价，对某个电容器设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与电容器设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.3.9. 电流互感器设备状态评价

根据电流互感器设备状态评价导价，对某个电流互感器设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与电流互感器设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.3.10. 电压互感器设备状态评价

根据电压互感器设备状态评价导价，对某个电压互感器设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与电压互感器设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.3.11. 试验报告的录入与展示

展示接入的 20 多类作业指导书中的试验数据，包括：预试类、间隔类、检修类等数据，后台可以进行

修改和录入。

### 3.1.3.12. 设备相其它数据的关联与展示

包括监造信息、安装验收信息、缺陷信息、检修维护等信息。

将上述信息分别进行录入和展示，并关联到电网一次设备。

### 3.1.4.风险评估中心

风险评估中心是参考电网风险、设备价值、重要用户等要素，开展一次设备风险评估。

#### 3.1.4.1. 风险评估中心总览

总览用于展示关键、重要、关注、一般的设备数量。

#### 3.1.4.2. 设备的重要度清单和明细

每年初始化所有设备的年度基准重要度。

根据设备名称、设备厂家、设备类型、投运年限、电压等级、所属变电站、设备状态、重要度等级、管控等级等信息，查找设备重要度的清单。

支持年度基准重要度、当时重要度的变更与恢复。

#### 3.1.4.3. 基于问题的设备风险巡视

★根据调度每日的停电计划，解析设备的名称、当前重要度，对设备的重要度进行变更，并生成基于问题的设备风险的巡视计划。

#### 3.1.4.4. 基于电网风险的差异化运维

★根据调度每周发布的电网风险总表，解析其中的设备名称、设备重要度变化，对本系统中的设备的重要度进行变更，并生成基于电网风险的差异化运维计划。

### 3.1.5.运维管控中心

★运维管控中心是以设备状态评价和风险评估结果为基础，利用设备风险矩阵对全局设备进行管控定级，并推送差异运维计划到电网管理平台，以满足高效、个性化的设备管理需求。

#### 3.1.5.1. 运维管控中心总览

根据管控等级统计各级设备的数量。

根据管控等矩阵，统计各矩阵内的设备数量。

展示巡视策略、试验策略、大修技改策略、品控策略的基本要求。

#### 3.1.5.2. 设备的管控等级清单和明细

各个设备的管控等级，要设备状态、设备重要度的变化，进行相应变更。

~~根据设备名称、设备厂家、设备类型、投运年限、电压等级、所属变电站、设备状态、重要度等级、~~

管控等级等信息，查找不同管控等级的设备清单。

不同种类的设备，有自己不同的管控策略，可以通过设备进行查看策略的详细内容。

### 3.1.5.3. 每日风险变化情况

计算每个设备当前的状态、重要度、管控等级，与昨天、年度的对比，找出变化的设备。

可以根据间隔导出变化的设备清单。

### ▲3.1.6. 状态检修设备评价

设备检修设备评价是基于南方电网公司的设备状态检修评价导则，实现了设备状态评价与自动推送，评价覆盖基本所有变电一次设备，是掌握设备运行状态的重要手段。

#### 3.1.6.1. 模块总览

通过图表展示各类设备的严重、异常、注意、异常四种状态的设备数量。

#### 3.1.6.2. 变压器设备状态评价

根据变压器的状态评价导价，对某个变压器进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与变压器相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.3. 电抗器设备状态评价

根据电抗器的状态评价导价，对某个电抗器进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与电抗器相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.4. GIS 设备状态评价

根据 GIS 设备状态评价导价，对某个 GIS 设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与 GIS 设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.5. 断路器设备状态评价

根据断路器设备状态评价导价，对某个断路器设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与断路器设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.6. 隔离和接地开关设备状态评价

根据隔离和接地开关设备状态评价导价，对某个隔离和接地开关设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与隔离和接地开关设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.7. 避雷器设备状态评价

根据隔离和接地开关设备状态评价导价，对某个隔离和接地开关设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与隔离和接地开关设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.8. 电容器设备状态评价

根据电容器设备状态评价导价，对某个电容器设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与电容器设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.9. 电流互感器设备状态评价

根据电流互感器设备状态评价导价，对某个电流互感器设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与电流互感器设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.10. 电压互感器设备状态评价

根据电压互感器设备状态评价导价，对某个电压互感器设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与电压互感器设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.11. 换流阀设备状态评价

根据换流阀设备状态评价导价，对某个换流阀设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与换流阀设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

#### 3.1.6.12. 换流阀冷却系统设备状态评价

根据换流阀冷却系统设备状态评价导价，对某个换流阀冷却系统设备进行评价。

根据导则的状态量，自动计算扣分值，并保存每次的扣分原因。

可根据总扣分值自动计算设备状态。

保存每次评价的状态及结果，可以查看历史状态及扣分情况。

展示与换流阀冷却系统设备相关的试验数据，通过趋势图展示试验数据的值的变化趋势。

### 3.1.7. 统计分析中心

#### 3.1.7.1. 设备规模分析

统计内容包括：

- 按电压等级统计变电站的数量
- 按电压等级统计主变设备的数量
- 按电压等级统计 GIS 设备的数量
- 按设备厂家统计设备数量的前 10 厂家

- 按运行年限统计各年段的设备数量
- 根据电压等级统计一次设备的数量

### 3.1.7.2. 年均缺陷率分析

★对全局设备十余万条缺陷数据、6万余条台账数据的清洗，按照缺陷描述定义缺陷类型，对厂家、型号、批次等数据进行人工校核，针对不同厂家、型号、批次设备的不同缺陷计算年均缺陷率。建立缺陷率数据查询模块，支持多维度查询，结果以柱状图进行展示，可以下钻查询。

### 3.1.7.3. 试验数据分析

★对全局40年试验数据进行数据清洗，剔除异常数据，计算每一台设备的纵横比、显著性差异等指标并进行数据可视化。对40年历史试验数据按照试验指标进行正态分布统计，计算每一项试验指标的均值与标准差，并进行可视化展示。对不同厂家的试验指标分布规律进行可视化。计算各项试验数据指标的增长率。

## 3.1.8. 后台管理模块

### 3.1.8.1. 评态评价导则管理

包括导则基本信息、设备部件、状态量等信息的维护。

### 3.1.8.2. 运维管控策略管理

实现对十多类主设备的运维管控策略的增删改查。

### 3.1.8.3. 推送电网平台功能

★开发专用数据接口，实现向电网管理平台推送如下数据。

- 推送每日设备状态

每日设备状态发生变化时，系统自动推送变化的设备信息及状态给电网管理平台。

- 推送年度设备状态

每年末，需要把所有设备的当前设备状态，进行归档并导出年度状态评价报告，然后统一推送到电网管理平台，作为年度设备状态。

- 推送每日设备重要度变化

每日设备的重要度生成变化时，系统自动推送变化的设备信息和最新重要度给电网管理平台。

- 推送基于问题的设备风险巡视计划

根据每日上传的停电计划生成的基于问题的设备风险巡视计划，每日将计划推送到电网平台。

- 推送差异化运维计划

根据每周上传的设备风险总表，生成的差异化运维计划，并将计划推送到电网平台。

- 推送防污闪计划

每年的 10 月到 2 月，根据气象的降雨情况，计算变电站的积污期，生成防污闪计划，并推送的电网平台。

### ★3.1.9.历史数据迁移

#### 3.1.9.1. 设备台帐及状态数据的迁移

包括设备台帐的基本信息，如台帐、功能位置、设备状态、重要度、管控等级等数据。

#### 3.1.9.2. 历史试验数据的迁移

包括 70 多类试验数据的迁移，并转换成新版试验作业指导书的格式。

#### 3.1.9.3. 检修维护记录的迁移

设备的历史的检修维护记录的数据，迁移到新的数据库。

#### 3.1.9.4. 历史缺陷数据的迁移

设备的历史的缺陷记录数据，迁移到新的数据库。

### 3.2.变电设备在线监测模块的自主可控改造

#### 3.2.1.数据接口功能改造

##### 3.2.1.1. IEC61850 在线监测数据接入

###### 3.2.1.1.1. 二区采集功能

★开发二区在线监测数据采集功能，包括采集变电站在线监测遥测、遥信数据、谱图文件、通信状态的数据接入功能。

###### 3.2.1.1.2. 二区到三区的跨区发送/接收功能

★把二区采集到的各类数据，通过正反向隔离装，发送到三区，在三区的接收处理。

###### 3.2.1.1.3. 三区数据入库功能

★三区接收的遥测、遥信数据、谱图文件、通信状态的数据，保存在关系型数据库或通过网络文件进行存储，方便后续的使用。

###### 3.2.1.2. 调度 E 文件的数据接入

★实现对调度 E 文件数据的接入，包括广州电网开关类设备位置、设备电压电流等数据。

###### 3.2.1.3. 调度 SOE 数据接入

★实现对调度 SOE 数据的接入。

###### 3.2.1.4. 保信录波数据接入

▲实时接入的保信系统的录波文件数据。

### 3.2.1.5. 外部供数据接口

#### 3.2.1.5.1. 变电在线监测装置台帐接口

包括在线监测的装置台帐，以及运行监测的装置台帐的信息。主要是：局放、油色谱、CVT、电容器、SOE、油温绕温变压器的台帐数据。

#### 3.2.1.5.2. 变电在线监测遥测数据

包括局放、油色谱、避雷器、铁芯夹件、直流电源等各类监测的遥测数据，以准实时的方式提供给下游。

#### 3.2.1.5.3. 变电在线监测遥信数据

包括局放、油色谱、避雷器、铁芯夹件、直流电源等各类监测的遥信数据，以准实时的方式提供给下游。

#### 3.2.1.5.4. 变电在线监告警信数据

告警数据的来源主要是两个：

1、根据 IEC61850 协议接入的变电在线监测的遥信数据（如：局放、油色谱……等），在线监测系统根据业务要求生成告警。

2、根据从调度主站接入的 SOE 和 E 文件数据（如：CVT 电压、开关 SOE、电容器电流……），在线监测系统根据业务要求生成的告警。

#### 3.2.1.5.5. 变电在线监谱图文件数据

二区接入的在线监测的局部放电、油色谱的谱图文件，提供实时的数据接口。

#### 3.2.1.5.6. 状态评价业务数据

获取变电设备台帐信息、重要度等级、状态等级、管控等级、扣分原因等信息，以及对应的电网平台的台帐信息。

#### 3.2.1.5.7. 不停电试验接口台帐接口

包括局放监测的间隔、油色谱监测的变压器、500kV 避雷器、CVT、电容器、油温绕温变压器六类不停电预测设备的台帐及相关的监测信息。

### 3.2.2. 在线监测

在线监测模块主要针对电科院负责安装维护的变电站的监测装置，这些装置基于 IEC61850 协议上送监测数据和谱图。

监测数据从二区接入，传入三区主站，在后台分析处理后，由 WEB 系统进行展示。

### 3.2.2.1. 局放监测

局放监测包括特高频局放、超声局放、高频局放三种类型，详情包括：台帐信息、时分钟曲线图、监测数据列表、趋势分析图、告警列表、谱图分析、关注日志。

★接入变电站传过来的局放监测数据进行展示、自动分析告警。时分钟曲线图通过曲线直观地查看监测数据变化，趋势分析图通过曲线直观地观察监测数据趋势分析。

当局放监测数据超过预设阈值时，自动触发告警，提醒运维人员及时处理。监盘人员发现监测异常的设备可记录于关注日志，追踪设备监测数据变化情况和运维情况。

### 3.2.2.2. 油色谱监测

油色谱监测详情包括监测列表、实时曲线、历史曲线、告警、关注日志、偏差比对。

★接入变电站传过来的油色谱监测数据进行展示、自动分析告警。实时曲线、历史曲线通过曲线直观地展示数据变化及趋势。

当气体含量或变化率超过预设阈值时，自动触发告警，提醒运维人员及时处理。

偏差比对通过对比不同维度的数据差异，识别设备的异常状态。监盘人员发现监测异常的设备可记录于关注日志，追踪设备监测数据变化情况和运维情况。

### 3.2.2.3. 避雷器监测

避雷器监测详情包括监测列表、历史曲线、告警、关注日志。

接入变电站传过来的避雷器监测数据进行展示、自动分析告警。历史曲线图通过曲线直观地查询监测数据变化。

当避雷器监测数据超过预设阈值时，自动触发告警，提醒运维人员及时处理。监盘人员发现监测异常的设备可记录于关注日志，追踪设备监测数据变化情况和运维情况。

### 3.2.2.4. 变压器铁芯接地电流监测

通过数据接口实时接入变电运行支持系统的铁芯接地电流监测数据。

## 3.2.3. 运行监测

运行监测模块主要接入调度监测数据，对接入的调度监测数据进行数据清洗和处理。通过页面查看调度 CVT 电压监测数据、调度电容器电流监测数据、开关分合闸监测、开关弹簧储能监测、变压器油温绕组监测等数据。

对每类监测数据进行接口开发及解析，运用算法实现对监测数据自动分析告警。

### 3.2.3.1. CVT 电压监测

CVT 电压监测详情包括电压数据、告警数据、关注设备日志。

实时接收调度系统传输的监测数据，并进行分类存储。

以图形化界面（如波形图、趋势曲线、柱状图等）展示监测数据，支持多参数、多维度同时展示，方便运维人员直观了解 CVT 的运行状态。

对监测数据进行统计分析、趋势分析和对比分析，能够自动识别电压参数的异常变化。

★通过电网拓扑和开关、刀闸位置，自动寻找与被监测 CVT 电气相连的设备参考电压，包括通过变压器变比折算的方式，当监测到 CVT 电压与参考电压偏差率超过设定阈值时，系统能够通过展示告警信息等方式及时发出告警信号，并记录告警信息，包括告警时间、告警类型、告警值等。用户可根据需要导出数据，包括监测数据、告警信息等。

监盘人员发现监测异常的设备可记录于关注日志，追踪设备监测数据变化情况和运维情况。

### 3.2.3.2. 电容器电流监测

电容器电流监测详情包括数据列表、数据曲线、告警数据、关注设备日志。

实时接收调度系统传输的监测数据，对数据进行校验和解析后，按照预设的格式进行分类存储，支持数据的快速查询和检索。以数据曲线展示电容器的电流参数等信息，方便运维人员直观了解电容器运行状态。

★当被监测电容器组三相电流比值数据超过设定阈值或出现异常趋势时，系统通过展示告警信息等方式发出告警信号，并记录告警时间、告警类型、告警值等信息，支持告警信息的查询和处理跟踪。

用户可根据需要导出数据，包括监测数据、告警信息等。

监盘人员发现监测异常的设备可记录于关注日志，追踪设备监测数据变化情况和运维情况。

### 3.2.3.3. 开关分合闸监测

开关分合闸监测包括分合闸监测、开关动作记录、分合闸统计、录波数据接入。

分合闸监测包括保护分合闸时间、遥控分合闸时间、控制回路断线分合闸时间、分合闸时差，详情包括监测指标、告警数据、关注设备日志。

★对全部开关的历史分合闸相关报文数据进行大数据分析，计算出每一台开关的保护分合闸时间、遥控分合闸时间、控制回路断线分合闸时间、分合闸时差，当上述指标超出阈值时应自动进行发送告警信息。

开关动作记录详情包括监测指标、告警数据、关注设备日志。

分合闸统计包括开关分合闸延时情况、保护分合闸延时情况、开关三相不同时期时间分布、保护跳闸时延。

用户可根据需要导出数据，包括监测数据、录波数据等。

### 3.2.3.4. 开关弹簧储能监测

开关弹簧储能监测详情包括储能动作、基准值样本、告警数据、关注设备日志。

开关设备（如断路器）通常采用弹簧储能机制来实现快速断开或闭合电路。当电力设备（如断路器）需要切换时，弹簧储能装置提供必要的能量以驱动开关动作。

开关弹簧储能时间分析功能基于采集的调度 SOE 数据，包括 10kV 馈线开关弹簧未储能动作、弹簧未储能复归数据，并结合调度 SOE 数据中的开关调试数据来判断其有效性的数据处理分析功能。该功能通过数据库存储过程和数据库 Job 定期处理数据，并将结果存储到结果表，为 Web 系统的展示提供数据支持。

### 3.2.3.5. 并列运行线路状态监测

整理输电线路的台帐，分析处理找出并列运行线路。

实时接收调度系统传输的监测数据，并进行分类存储。

根据并行线路的状态监测算法，设置预警值，超出预警值则触发告警。

### 3.2.3.6. 保信录波跳闸数据接入

实现保信系统（保护动作、告警）与录波装置（电压、电流波形）数据的同步采集与关联存储。

### 3.2.3.7. 变压器中性点监测

变压器中性点监测详情包括数据列表、数据曲线、告警数据、关注设备日志。

### 3.2.3.8. 母联分段监测

母联分段监测详情包括数据列表、数据曲线、告警数据、关注设备日志。

### 3.2.4. 告警管理

实现设备监测告警的接收、分析、处理及闭环管理。

### 3.2.5. 统计查询

#### 3.2.5.1. 信息汇聚查询

★根据设备名称关键字，查询设备的台帐信息、健康状态、缺陷、油色谱监测、局放监测、CVT 监测、开关动作等信息，在这些信息进行汇聚展示，用于跳闸辅助业务分析。

#### 3.2.5.2. 在线监测装置在线率

★计算在线监测装置的在线率，按装置进行查询展示。

#### 3.2.5.3. 在线监测变电站在线率

★按变电站计算在线监测装置的在线率，按变电站进行查询展示。

#### 3.2.5.4. CVT 在线率

计算 CVT 设备的在线情况，可以查询导出。

#### 3.2.5.5. 电容器在线率

计算电容器设备的在线情况，可以查询导出。

### 3.2.5.6. 电容器可用率

计算电容器的可用率，可以查询导出。

### 3.2.5.7. 电抗器可用率

计算电抗器的可用率，可以查询导出。

## 3.2.6.关注日志

实现设备监测关注日志的统一存储、查询和管理。

### ▲3.2.6.1. 关注日志

监盘人员发现监测异常的设备记录于关注日志，追踪设备监测数据变化情况和运维情况。

实现设备监测关注日志的统一存储、查询和管理，支持多种查询方式，如按监测类型、时间范围、是否需要跟踪监测等。

### ▲3.2.6.2. 预警通知书

用户可以根据关注日志，把有缺陷隐患的设备记录下来，生成预警通知书，并推送生产运行支持系统。

本模块实现预警通知书的维护和查询。

## 3.2.7.台帐管理

### 3.2.7.1. CVT 台帐管理

CVT 台帐的信息维护。

★同时实现每个 CVT 与调度测点的挂接。

### 3.2.7.2. 电容器台帐管理

电容器台帐的信息维护。

★同时实现每个电容器与调度测点的挂接。

### 3.2.7.3. 母联分段台帐管理

母联开关台帐的信息维护。

同时实现每个母联开关与调度测点的挂接。

### 3.2.7.4. 中性点直流台帐管理

实现中性点直流台帐的信息维护。

同时实现每个中性点直流台帐与调度测点的挂接。

### 3.2.7.5. 变压器台帐管理

实现油温绕组温监测的变压器台帐的信息维护。

同时实现每个变压器与调度测点的挂接。

### 3.2.7.6. 在线监测装置台帐管理

★实现局放、油色谱等基于 IEC61850 协议接数的在线监测装置的台帐，并实现与电网平台的台帐数据关联。

### 3.2.8.通信监测

显示基于 IEC61850 协议接数的在线监测的局放、油色谱装置的通信情况，准实时更新，并可以查看历史通信记录。

### 3.2.9.系统配置

#### 3.2.9.1. 油色谱偏差标准配置

油色谱分析是监测变压器内部运行状态的重要手段。通过检测油中溶解气体的成分和含量，可以有效发现设备内部的潜伏性故障，如过热等。而设置油色谱偏差标准，旨在为设备运行状态的评估提供量化依据。当油色谱监测数据与标准值的偏差超出设定范围时，系统能够及时发出预警，提示运维人员设备可能存在异常，以便采取进一步的检测和维护措施，保障电力设备的安全稳定运行。

#### 3.2.9.2. 装置在线率剔除配置

在线监测装置在线率是衡量电力设备在线监测装置运行效能的重要指标，而实际运行中存在多种非故障性离线情况，若不进行合理剔除，会导致在线率统计失真。通过装置在线率剔除配置，可确保统计数据能真实反映装置的有效运行状况，为设备管理决策提供依据。

#### 3.2.9.3. 状态监测与评价日报自动生成功能

传统的状态监测与评价日报依赖人工汇总、整理和分析数据，不仅耗时费力，还容易出现数据遗漏、计算错误等问题。实现日报自动生成功能，能够快速整合各类监测数据，及时生成准确的评价报告，为管理层和运维人员提供及时、可靠的决策支持，提升工作效率和管理水平。

### ★3.2.10.历史数据迁移

#### 3.2.10.1. 在线监测台帐迁移

包括在线监测的装置台帐，以及运行监测的装置台帐的信息。主要是：局放、油色谱、CVT、电容器、SOE、油温绕温变压器的台帐数据。

#### 3.2.10.2. 在线监测遥测、遥信、告警数据迁移

包括局放、油色谱等各类监测的遥测、遥信数据。

告警数据包括局放、油色谱、CVT、电容器、开关监测……等。

#### 3.2.10.3. 在线监测谱图文件迁移

包括历史的局放、油色谱的谱图文件。

#### 3.2.10.4. e 文件数据迁移

包括历史的 e 文件数据中的十多类数据表的迁移、转换。

#### 3.2.10.5. SOE 数据迁移

包括历史的 SOE 数据表的迁移、转换。

#### 3.2.10.6. 保信录波数据迁移

包括保信系统的录波文件，以及解析后数据表的迁移。

#### 3.2.10.7. 气象数据迁移

包括历史的气象实况数据的迁移。

### ▲3.3. 设备驾驶舱

#### 3.3.1. 保供电驾驶舱

通过可视化方式展示设备状态总览、缺陷总览、实时告警、保供电场所、气象监测、低电压台区等内容。

##### 3.3.1.1. 保供电地图

在地图上展示变电站、保供电场所所有地理分布。

可以查看每个保供电场所对应的电网设备及供电链路，以及设备对应的状态、缺陷等信息。

##### 3.3.1.2. 保供电设备状态总览

统计保供电设备的严重、异常、注意的设备数量。

##### 3.3.1.3. 保供电设备缺陷总览

统计保供电设备的紧急、严重、一般的缺陷数量。

##### 3.3.1.4. 保供电设备实时告警

显示保供电设备最新的告警信息。

##### 3.3.1.5. 保供电场所

按类型和保供电等级，统计保供电场所的数量。

##### 3.3.1.6. 气象监测

显示重点保供电场所的气象实况信息。

##### 3.3.1.7. 低电压台区

显示电压系统的低电压台区的信息。

#### 3.3.2. 状态监测总览

##### 3.3.3.1. 地图总览

包括变电线、线路的地理分布图，提供多类图层选择，如：变电站图层、输电线路图层、地闪密度图、

污区图层。

统计变电站积污信息清单、输电杆塔积污信息清单，并能导出相关数据。

### 3.3.2.2. 电网设备数量

根据电网平台的数据，统计出输电、变电、配电主要一次设备数量，并能定时自动更新。

### 3.3.2.3. 设备状态重要度及管控等级

展示设备状态、设备重要度、管控等级的三个统计图。

### 3.3.2.4. 近三年缺陷明细及统计

展示近三年缺陷的明细清单，以及根据变电所进行缺陷数量统计图。

### 3.3.2.5. 监测装置覆盖情况

统计局放、油色谱、CVT、电容器、开关 SOE、视频摄像头的装置数量，以及覆盖的变电站的数量。

### 3.3.2.6. 监测预警指标

包括局放监测、油色谱监测、CVT、电容器、开关的监测装置的在线率、覆盖率两类指标。

### 3.3.2.7. 输电线路跳闸信息

展示近三年输电线路跳闸的明细清单，以及根据输电所进行跳闸原因的数量统计图。

## 4.服务要求

(1) 在保修期内发现平台问题（包括系统漏洞整改、系统运行异常等），可随时向供方提出通知，供方保证 48 小时内必须到达现场。

(2) 供方向需方交付使用说明书及相关资料。

★ (3) 自项目验收完毕投入运行之日起（需方出具验收报告），供方向需方提供不少于 36 个月的无条件全免费保修。

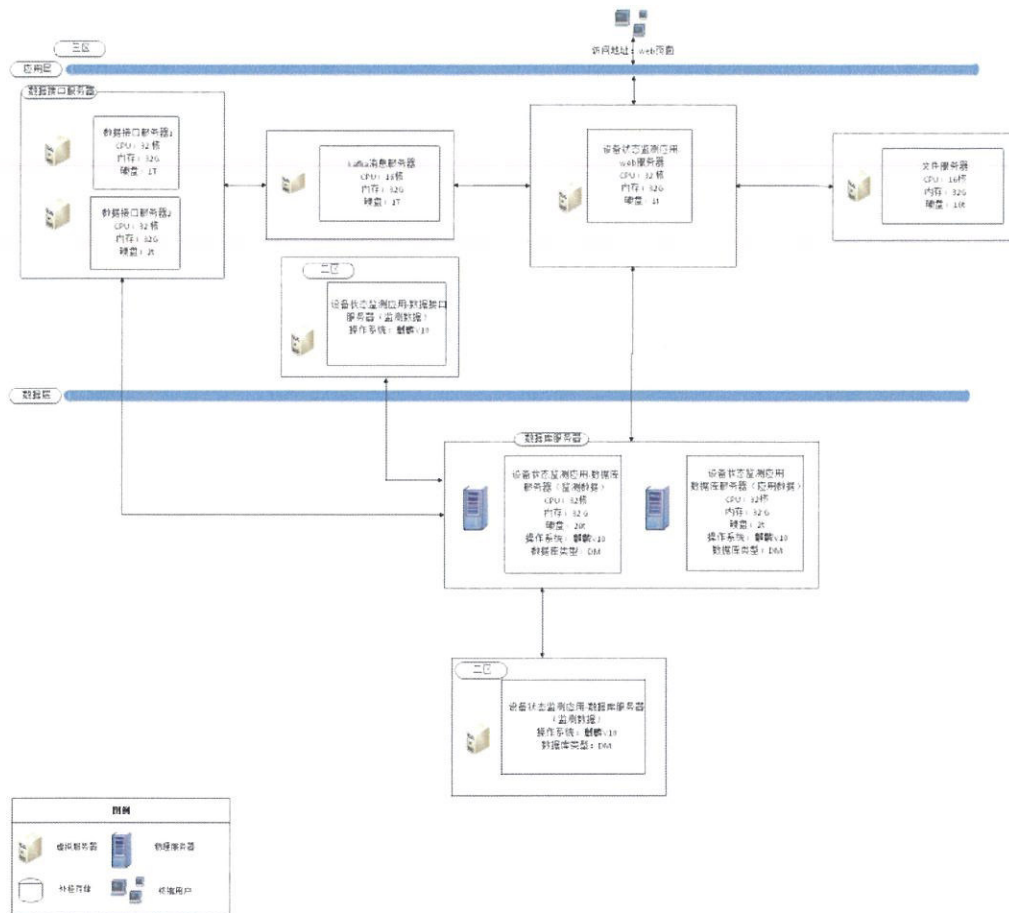
(4) 供方向需方提供终身维修和技术支持，免费提供培训；供方根据需方要求进行不少于 1 次技术培训，供方发生的费用由供方承担，时间由供需双方协商确定。

★ (5) 项目实施期间，供应方应安排至少 6 名技术人员驻点开发，时间不少于 1 年，项目运行期间，供应方应安排至少 4 名技术人员驻点开发，时间不少于 1 年。

## ★5.网络安全相关要求

### 5.1.系统部署完整性

1、项目基于设备状态监测与评价系统现有部署架构进行部署，部署于 II、III 区，服务于广州局各变电所、电科院、生产指挥中心的用户。部署架构及新增服务器资源如下图所示：



## 5.2.安全责任单位完整性

1、原则上自主运维。如确实需要外包运维的，需与选定的外包运维服务商签订服务协议，明确约定外包运维的范围、工作内容及工作要求。

## 5.3.系统安全等级准确性

1、根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）以及《南方电网管理信息系统安全等级保护标准》要求，电科院设备状态监测与评价系统的安全等级保护拟定为2级。并需要按照中华人民共和国国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）进行系统的安全防护。

2、电科院设备状态监测与评价系统不属于关键信息基础设施。

## 5.4.数据保护合规性

- 1、系统建设包括信息系统数据安全需求、数据安全等集成需求。
- 2、电科院设备状态监测与评价系统数据不涉及商业机密。
- 3、系统数据不涉及个人信息。

## 5.5.安全设计完整性

### 1、网络和通信安全

为保证网络层的安全性，需要合理设计网络拓扑结构，并实施网络边界控制措施。

### 2、网络拓扑结构

网络结构安全保证网络设备的业务处理能力具备冗余空间和链路负载均衡能力，满足业务高峰期需要。

根据本系统的安全属性，其部署在信息内网。并按照“三级（及以上）系统独立成域、二级（及以下）系统集成成域”的原则，通过虚拟化网络技术或者 SDN 技术实现本系统单独设域，与其他系统实现逻辑隔离，在不同网段之间进行路由控制，建立安全的访问路径，实行针对性、差异化防护。

涉及 Internet 的应用，须部署在信息外网区，使用统一集中的互联网出口，并通过信息安全交换平台实现强逻辑隔离。

要求采用冗余技术设计网络拓扑结构，确保路由冗余。

网络优先级配置：根据本系统的重要性设置带宽分配级别，保证在网络发生拥堵的时候优先本系统服务连续性。

网络设备冗余配置，避免存在网络单点故障，确保网络设备高可靠性。

### 3、网络边界防护

通过 ACL 技术或防火墙技术，在网络边界或区域之间根据访问控制策略设置访问控制规则，对本系统域实现端口级访问控制，默认情况下除允许通信外受控接口拒绝所有通信；应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。并对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出，保证信息及网络资源不被非法使用和访问。

通过入侵监测技术，在网络边界处监视如端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击行为，并给警告警以及响应和处理。

在网络边界及核心业务网段处对恶意代码进行检测和清除；及时实现恶意代码库升级和检测系统更新。

通过网络安全扫描工具，利用优化系统配置和打补丁等各种方式最大可能地弥补最新的安全漏洞和消除安全隐患。

### 4、网络安全审计

通过信息安全运行预警系统，实现对网络设备、安全设备运行状况、网络流量、用户行为等进行日志信息实时采集、集中监控及实时预警。审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

## 5、网络安全加固

- 1.对登录网络设备的用户进行身份鉴别。
- 2.禁止采用默认的管理员账号和密码。
- 3.对网络设备管理员登录的地址进行限制。
- 4.通过支持国密算法的 U-key 认证方式登录，key 证书具有唯一性。
- 5.网络设备账号满足密码复杂度设置，并定期进行更新，存储为加密存储方式。
- 6.具有登录失败处理功能，登录 5 次失败后，采取结束会话的措施。
- 7.采取 SSH 加密协议远程管理网络设备。
- 8.已通过服务器区防火墙进行限制，只对系统的：8000/8001/8002/8003/8004/8005/8006/8007 等端口进行开放。

## 6、硬件安全

采用服务器设备具备冗余配置（包括双机热备等）；具备不间断电源保障，具备服务器运行状态监控，确保本系统处理性能要求。

对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；当进行远程管理时，应采取加密措施。

## 7、操作系统安全

操作系统原则上采用 Linux，加强操作系统账号管理、认证授权、安全日志等功能，实现从身份鉴别，访问控制，安全审计入侵防范，恶意代码规范，资源控制几个方面进行主机安全基线加固。

## 8、中间件安全

从身份鉴别，访问控制，安全审计，通信完整性，通信保密性，软件容错，资源控制几个方面进行中间件安全基线加固，选用安全可控的中间件。

## 9、数据库安全

禁止采用默认的管理员账号和密码，避免非法用户进入到网络后通过直接调用监控末端设备查看相关信息，选用安全可控的数据库。

电科院设备状态监测与评价系统采用达梦数据库。达梦数据库作为国产自研的高安全数据库标杆，构建了以权限制衡为核心，覆盖身份鉴别、访问控制、全链路加密、细粒度审计、数据安全防护的全方位安全体系。其默认支持三权分立、可选配四权分立架构，从根源杜绝超级管理员权限滥用，同时融合自主访问控制与强制访问控制双重机制，搭配行级、列级精细化权限管控，满足不同密级场景的访问需求。

## 10、数据安全

采用身份认证、权限控制、加密存储、加密传输、数据防泄密等技术，加强本系统数据机密性及安全性防护：

1.通过对数据库表设置完整性约束，如 Check、NOT NULL、Unique、Primary、Foreign key 来保证数据的完整性。

2.使用国产密码技术对本系统数据库表访问权限进行控制。

3.采用国产密码技术对本系统的重要数据进行加密存储，防止数据库被黑客攻击导致系统机密泄漏。

4.使用国产密码技术保证本系统重要数据传输过程中的机密性及完整性。

5.仅采集和保存业务必需的用户个人信息；禁止未授权访问、使用用户个人信息。

6.通过数据防泄密网关，减少敏感数据泄密。

7.采用数据本地备份或者数据灾备技术，确保本系统核心数据安全，确保在某个存储设备故障或灾害发生时，数据不会丢失。

8.存储设备报废前按照规定通过消磁粉碎一体机进行信息彻底清除，确保数据不能被恢复、还原。

9.确保本系统日志信息保持 6 个月以上。并采用国产密码技术实现本系统日志信息完整性保护。

10.采用国产密码技术实现本系统的加载和卸载安全控制。

11.实现数据库访问审计。

## 11、应用安全

1.采取三权分立，本系统应具备完善的权限管理，贯穿全系统的分级授权和界面信息操作控制，完整的应用程序日志记录和审计机制。

2.提供访问控制功能，通过角色划分实现各层各级人员对于功能页面的访问控制；依据安全策略控制用户对文件、数据库表等客体的访问；访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；授权主体配置访问控制策略，并严格限制默认帐户的访问权限。

3.实现对登录用户的统一身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证本系统用户身份的真实性。

4.启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

1) 用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用户在第一次登录系统时修改分发的初始口令，口令长度不得小于 8 位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；

应用软件不得明文存储口令数据；

- 2) 提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
- 3) 授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
- 4) 及时删除或停用多余的、过期的账号，避免共享账号。
- 5.采用基于国产密码的数据验签技术保证通信过程中数据的完整性。
- 6.通过基于国产密码的加解密技术，实现对重要数据的传输安全防护。
- 7.通过基于国产密码的加解密技术实现数据有效性检验功能。
- 8.加强数据有效性检查，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。
- 9.关闭不需要的端口及服务。
- 10.通过负载均衡技术，确保在突发数据流的情况下，本系统依然可以提供适当的服务能力。
- 11.当通信双方中的一方在一段时间内未作任何响应，另一方自动结束会话；对系统的最大并发会话连接数进行限制；对单个账号的多重并发会话进行限制。
- 12.通过防病毒系统，实现统一控制台对应用系统病毒防范，包括统一的分发、维护、更新和报警等。
- 13.通过对用户的登录、退出、增加用户、修改用户权限等进行应用审计。
- 14.通过信息安全运行预警系统，实现对本系统的运行状态、用户体验等的实时监控与预警。
- 15.要求通过支持国产密码的堡垒机等技术，实现对本系统运维的统一管控，避免对网络和服务器资源的直接访问，对不合法命令进行命令阻断，过滤掉所有对目标设备的非法访问行为，减少和恶意攻击，拦截非法访问，并实现运维操作行为审计。

## 12、终端安全设计

- 1.要求通过桌面终端准入控制，加强桌面终端监控审计管理，重点提高移动存储介质使用管理能力与病毒、木马检测防护、桌面终端行为监控审计能力等建设。
- 2.通过上网行为管理系统，加强信息外网办公终端 Internet 访问控制，如网络应用控制、带宽流量管理、上网行为分析等。对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。
- 3.存储设备报废前按照规定通过消磁粉碎一体机进行信息彻底清除，确保数据不能被恢复、还原。
- 4.对访问的移动终端进行安全防护，通过沙箱等技术确保本地数据安全存储，通过身份认证及权限控制技术确保访问安全；通过加密技术实现传输安全了通过设备远程控制技术，如设备定位、设备远程数据擦除、锁定、更改密码等确保重要数据一键式擦除。

### 13、代码安全

- 1.代码审查：实施严格的代码审查流程，确保每一行代码都经过至少一个其他开发者的检查。
- 2.静态代码分析：使用静态代码分析工具来检测潜在的安全漏洞和编码错误。
- 3.动态分析：进行动态安全测试，如渗透测试和模糊测试，以发现运行时的漏洞。
- 4.安全编码规范：制定并遵守安全编码标准，如 OWASP Top Ten 等。
- 5.依赖管理：定期更新第三方库，并检查这些库是否存在已知的安全漏洞。
- 6.版本控制：使用版本控制系统（如 Git）来跟踪代码变更，并保持清晰的历史记录。

### 14、组件安全

- 1.组件选择：选择信誉良好且维护活跃的开源或商业组件。
- 2.安全配置：按照最佳实践配置所有使用的组件，避免使用默认设置。
- 3.补丁管理：及时应用组件的安全更新和补丁。
- 4.隔离原则：尽可能将不同功能的组件隔离开，限制它们之间的交互，减少攻击面。
- 5.最小权限原则：为每个组件分配最小必要的权限，以降低潜在风险。

### 15、接口安全

- 1.认证与授权：实现强认证机制（如 OAuth, JWT），并对访问 API 的用户或服务进行细粒度的授权。
- 2.输入验证：对所有外部输入进行严格验证，防止 SQL 注入、XSS 等攻击。
- 3.输出编码：在返回响应之前对输出数据进行适当的编码，防止注入攻击。
- 4.限流与防滥用：通过速率限制和访问控制防止接口被滥用。
- 5.日志记录：详细记录所有接口调用，以便于审计和异常检测。
- 6.加密传输：使用 TLS/SSL 等协议加密敏感信息的传输，保护数据不被截取。

## 5.6.安全集成合规性

1、电科院设备状态监测与评价系统自主可控改造项目接入其他系统时，根据接入要求完成接入，同时确保数据交互通道安全。

2、业务系统接入电科院设备状态监测与评价系统自主可控改造项目时，要制定详细的接入文档，同时接口添加权限校验，确保能拦截非法接入，数据传输要使用安全传输协议。

## 5.7.自主可控要求合规性

1、优先使用《南网云平台技术白皮书》所发布的服务与组件，采用南网云平台的中间件、数据库组件、计算、存储资源等技术或开源技术保证自主可控。

2、项目建设阶段，要求围绕《南方电网公司全栈自主可控技术路线目录（2024）》开展产品差异分析及设计，设计方案参考《南方电网公司系统自主可控适配典型设计参考（2024版）》，且后续根据上述文件同步更新迭代。

3、本项目涉及的所有应用和软硬件产品必须符合自主可控要求，且本项目涉及的所有应用能够适配未来自主可控环境潜在变化需求，目前南方电网公司 CPU、操作系统、数据库、中间件、计算机终端、浏览器、开源软件及关键组件等自主可控选型适配设计情况包括但不限于：

1) CPU：计算机终端 CPU 要求兼容自主可控 CPU（ARM、MIPS、X86、ALPHA 等）架构，根据项目业务需求选择自主可控 CPU（如龙芯、兆芯、飞腾、鲲鹏、申威、海光等）。服务器 CPU 要求兼容自主可控 CPU（ARM、MIPS、X86、ALPHA 等）架构，选型要求确保系统的稳定性、可靠性以及满足特定的性能需求，包括不限于飞腾、鲲鹏、海光等产品。

2) 操作系统：兼容国内主流桌面、服务器自主可控操作系统（如统信 UOS、银河麒麟、麒麟信安等）。

3) 数据库：要求兼容国内主流自主可控数据库（包括不限于达梦、金仓等）。

4) 中间件：兼容国内主流自主可控中间件（如：中创等）。

5) 浏览器：兼容统信浏览器、麒麟奇安信浏览器、360 安全浏览器、搜狗浏览器、红芯浏览器等自主可控浏览器，应用系统可与支持国密算法的国产浏览器加密通信。

6) 开源软件及关键组件：要求开源软件及关键组件自主可控，选型过程中评估这些组件与现有系统的兼容性和可替代性。

# 电科院设备状态监测与评价系统自主可控 改造项目技术规范书 (网络安全相关内容)

## 一、系统部署完整性

1、项目基于设备状态监测与评价系统现有部署架构进行部署，部署于II、III区，服务于广州局各变电所、电科院、生产指挥中心的用户。部署架构及新增服务器资源如下图所示：

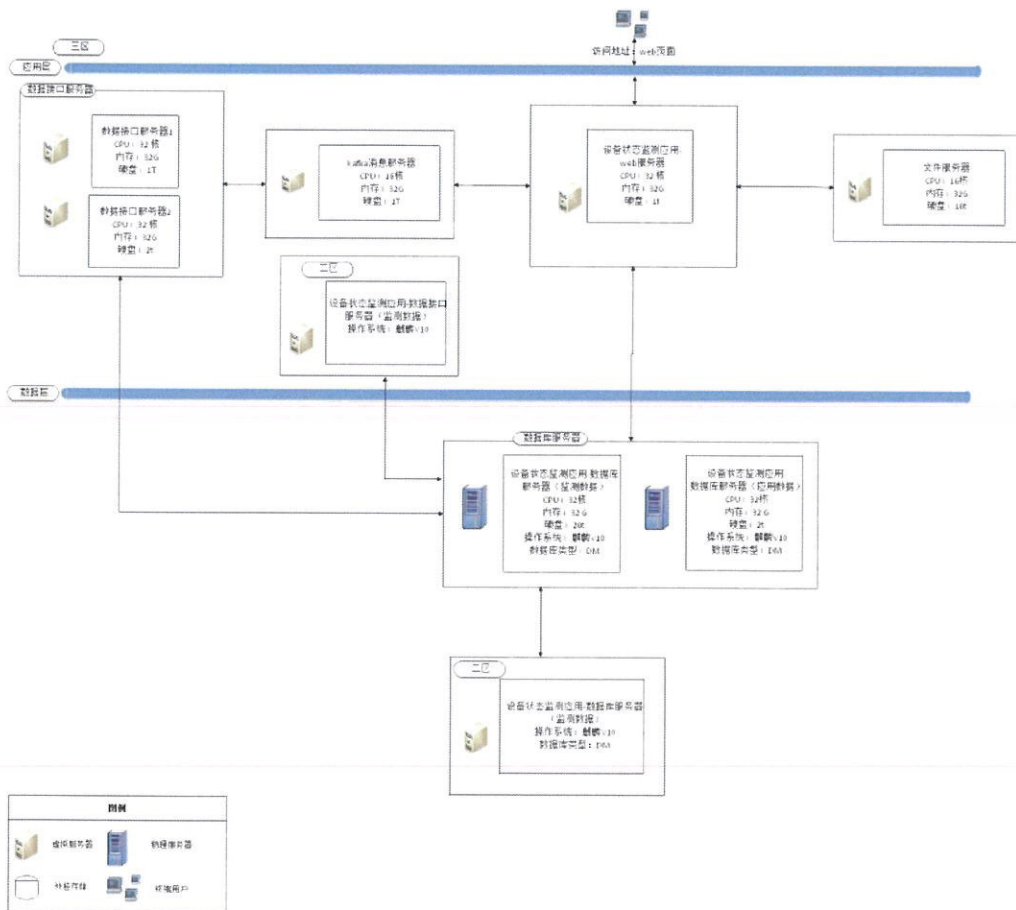


图 1-1 网络拓扑图

## 二、安全责任单位完整性

1、原则上自主运维。如确实需要外包运维的，需与选定的外包运维服务商签订服务协议，明确约定外包运维的范围、工作内容及工作要求。

### **三、系统安全等级准确性**

1、根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）以及《南方电网管理信息系统安全等级保护标准》要求，电科院设备状态监测与评价系统的安全等级保护拟定为 2 级。并需要按照中华人民共和国国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）进行系统的安全防护。

2、电科院设备状态监测与评价系统不属于关键信息基础设施。

### **四、数据保护合规性**

1、系统建设包括信息系统数据安全需求、数据安全等集成需求。

2、电科院设备状态监测与评价系统数据不涉及商业机密。

3、系统数据不涉及个人信息。

### **五、安全设计完整性**

#### **1、网络和通信安全**

为保证网络层的安全性，需要合理设计网络拓扑结构，并实施网络边界控制措施。

#### **2、网络拓扑结构**

网络结构安全保证网络设备的业务处理能力具备冗余空间和链路负载均衡能力，满足业务高峰期需要。

根据本系统的安全属性，其部署在信息内网。并按照“三级（及以上）系统独立成域、二级（及以下）系统集成成域”的原则，通过虚拟化网络技术或者 SDN 技术实现本系统单独设域，与其他系统实现逻辑隔离，在不同网段之间进行路由控制，建立安全的访问路径，实

行针对性、差异化防护。

涉及 Internet 的应用，须部署在信息外网区，使用统一集中的互联网出口，并通过信息安全交换平台实现强逻辑隔离。

要求采用冗余技术设计网络拓扑结构，确保路由冗余。

网络优先级配置：根据本系统的重要性设置带宽分配级别，保证在网络发生拥堵的时候优先本系统服务连续性。

网络设备冗余配置，避免存在网络单点故障，确保网络设备高可靠性。

### **3、网络边界防护**

通过 ACL 技术或防火墙技术，在网络边界或区域之间根据访问控制策略设置访问控制规则，对本系统域实现端口级访问控制，默认情况下除允许通信外受控接口拒绝所有通信；应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。并对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出，保证信息及网络资源不被非法使用和访问。

通过入侵监测技术，在网络边界处监视如端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击行为，并给警告警以及响应和处理。

在网络边界及核心业务网段处对恶意代码进行检测和清除；及时实现恶意代码库升级和检测系统更新。

通过网络安全扫描工具，利用优化系统配置和打补丁等各种方式最大可能地弥补最新的安全漏洞和消除安全隐患。

### **4、网络安全审计**

通过信息安全运行预警系统，实现对网络设备、安全设备运行状

---

况、网络流量、用户行为等进行日志信息实时采集、集中监控及实时预警。审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

## 5、网络安全加固

1. 对登录网络设备的用户进行身份鉴别。
2. 禁止采用默认的管理员账号和密码。
3. 对网络设备管理员登录的地址进行限制。
4. 通过支持国密算法的 U-key 认证方式登录，key 证书具有唯一性。
5. 网络设备账号满足密码复杂度设置，并定期进行更新，存储为加密存储方式。
6. 具有登录失败处理功能，登录 5 次失败后，采取结束会话的措施。
7. 采取 SSH 加密协议远程管理网络设备。
8. 已通过服务器区防火墙进行限制，只对系统的：8000/8001/8002/8003/8004/8005/8006/8007 等端口进行开放。

## 6、硬件安全

采用服务器设备具备冗余配置（包括双机热备等）；具备不间断电源保障，具备服务器运行状态监控，确保本系统处理性能要求。

对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；当进行远程管理时，应采取加密措施。

## 7、操作系统安全

操作系统原则上采用 Linux，加强操作系统账号管理、认证授权、安全日志等功能，实现从身份鉴别，访问控制，安全审计入侵防范，恶意代码规范，资源控制几个方面进行主机安全基线加固。

## 8、中间件安全

从身份鉴别，访问控制，安全审计，通信完整性，通信保密性，软件容错，资源控制几个方面进行中间件安全基线加固，选用安全可控的中间件。

## 9、数据库安全

禁止采用默认的管理员账号和密码，避免非法用户进入到网络后通过直接调用监控末端设备查看相关信息，选用安全可控的数据库。

电科院设备状态监测与评价系统采用达梦数据库。达梦数据库作为国产自研的高安全数据库标杆，构建了以权限制衡为核心，覆盖身份鉴别、访问控制、全链路加密、细粒度审计、数据安全防护的全方位安全体系。其默认支持三权分立、可选配四权分立架构，从根源杜绝超级管理员权限滥用，同时融合自主访问控制与强制访问控制双重机制，搭配行级、列级精细化权限管控，满足不同密级场景的访问需求。

## 10、数据安全

采用身份认证、权限控制、加密存储、加密传输、数据防泄密等技术，加强本系统数据机密性及安全性防护：

1. 通过对数据库表设置完整性约束，如 Check、NOT NULL、Unique、Primary、Foreign key 来保证数据的完整性。

2. 使用国产密码技术对本系统数据库表访问权限进行控制。

3. 采用国产密码技术对本系统的重要数据进行加密存储，防止数

---

据库被黑客攻击导致系统机密泄漏。

4. 使用国产密码技术保证本系统重要数据传输过程中的机密性及完整性。

5. 仅采集和保存业务必需的用户个人信息；禁止未授权访问、使用用户个人信息。

6. 通过数据防泄密网关，减少敏感数据泄密。

7. 采用数据本地备份或者数据灾备技术，确保本系统核心数据安全，确保在某个存储设备故障或灾害发生时，数据不会丢失。

8. 存储设备报废前按照规定通过消磁粉碎一体机进行信息彻底清除，确保数据不能被恢复、还原。

9. 确保本系统日志信息保持6个月以上。并采用国产密码技术实现本系统日志信息完整性保护。

10. 采用国产密码技术实现本系统的加载和卸载安全控制。

11. 实现数据库访问审计。

## **11、应用安全**

1. 采取三权分立，本系统应具备完善的权限管理，贯穿全系统的分级授权和界面信息操作控制，完整的应用程序日志记录和审计机制。

2. 提供访问控制功能，通过角色划分实现各层各级人员对于功能页面的访问控制；依据安全策略控制用户对文件、数据库表等客体的访问；访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；授权主体配置访问控制策略，并严格限制默认帐户的访问权限。

3. 实现对登录用户的统一身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证本系统用户身份的真实性。

---

4. 启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

1) 用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用户在第一次登录系统时修改分发的初始口令，口令长度不得小于8位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；应用软件不得明文存储口令数据；

2) 提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

3) 授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

4) 及时删除或停用多余的、过期的账号，避免共享账号。

5. 采用基于国产密码的数据验签技术保证通信过程中数据的完整性。

6. 通过基于国产密码的加解密技术，实现对重要数据的传输安全防护。

7. 通过基于国产密码的加解密技术实现数据有效性检验功能。

8. 加强数据有效性检查，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

9. 关闭不需要的端口及服务。

10. 通过负载均衡技术，确保在突发数据流的情况下，本系统依然可以提供适当的服务能力。

11. 当通信双方中的一方在一段时间内未作任何响应，另一方自

动结束会话；对系统的最大并发会话连接数进行限制；对单个账号的多重并发会话进行限制。

12. 通过防病毒系统，实现统一控制台对应用系统病毒防范，包括统一的分发、维护、更新和报警等。

13. 通过对用户的登录、退出、增加用户、修改用户权限等进行应用审计。

14. 通过信息安全运行预警系统，实现对本系统的运行状态、用户体验等的实时监控与预警。

15. 要求通过支持国产密码的堡垒机等技术，实现对本系统运维的统一管控，避免对网络和服务器资源的直接访问，对不合法命令进行命令阻断，过滤掉所有对目标设备的非法访问行为，减少和恶意攻击，拦截非法访问，并实现运维操作行为审计。

## **12、终端安全设计**

1. 要求通过桌面终端准入控制，加强桌面终端监控审计管理，重点提高移动存储介质使用管理能力与病毒、木马检测防护、桌面终端行为监控审计能力等建设。

2. 通过上网行为管理系统，加强信息外网办公终端 Internet 访问控制，如网络应用控制、带宽流量管理、上网行为分析等。对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查。

3. 存储设备报废前按照规定通过消磁粉碎一体机进行信息彻底清除，确保数据不能被恢复、还原。

4. 对访问的移动终端进行安全防护，通过沙箱等技术确保本地数据安全存储，通过身份认证及权限控制技术确保访问安全；通过加密

技术实现传输安全了通过设备远程控制技术，如设备定位、设备远程数据擦除、锁定、更改密码等确保重要数据一键式擦除。

### 13、代码安全

1. 代码审查：实施严格的代码审查流程，确保每一行代码都经过至少一个其他开发者的检查。

2. 静态代码分析：使用静态代码分析工具来检测潜在的安全漏洞和编码错误。

3. 动态分析：进行动态安全测试，如渗透测试和模糊测试，以发现运行时的漏洞。

4. 安全编码规范：制定并遵守安全编码标准，如 OWASP Top Ten 等。

5. 依赖管理：定期更新第三方库，并检查这些库是否存在已知安全漏洞。

6. 版本控制：使用版本控制系统（如 Git）来跟踪代码变更，并保持清晰的历史记录。

### 14、组件安全

1. 组件选择：选择信誉良好且维护活跃的开源或商业组件。

2. 安全配置：按照最佳实践配置所有使用的组件，避免使用默认设置。

3. 补丁管理：及时应用组件的安全更新和补丁。

4. 隔离原则：尽可能将不同功能的组件隔离开，限制它们之间的交互，减少攻击面。

5. 最小权限原则：为每个组件分配最小必要的权限，以降低潜在风险。

---

## 15、接口安全

1. 认证与授权：实现强认证机制（如 OAuth, JWT），并对访问 API 的用户或服务进行细粒度的授权。
2. 输入验证：对所有外部输入进行严格验证，防止 SQL 注入、XSS 等攻击。
3. 输出编码：在返回响应之前对输出数据进行适当的编码，防止注入攻击。
4. 限流与防滥用：通过速率限制和访问控制防止接口被滥用。
5. 日志记录：详细记录所有接口调用，以便于审计和异常检测。
6. 加密传输：使用 TLS/SSL 等协议加密敏感信息的传输，保护数据不被截取。

## 六、安全集成合规性

- 1、电科院设备状态监测与评价系统自主可控改造项目接入其他系统时，根据接入要求完成接入，同时确保数据交互通道安全。
- 2、业务系统接入电科院设备状态监测与评价系统自主可控改造项目时，要制定详细的接入文档，同时接口添加权限校验，确保能拦截非法接入，数据传输要使用安全传输协议。

## 七、移动应用安全合规性

- 1、电科院设备状态监测与评价系统自主可控改造项目不涉及移动应用。

## 八、安全设计准确性

- 1、电科院设备状态监测与评价系统与数认平台的集成的统一账号管理、统一授权管理、统一认证管理、统一审计管理。

## 九、自主可控要求合规性

1、优先使用《南网云平台技术白皮书》所发布的服务与组件，采用南网云平台的中间件、数据库组件、计算、存储资源等技术或开源技术保证自主可控。

2、项目建设阶段，要求围绕《南方电网公司全栈自主可控技术路线目录（2024）》开展产品差异分析及设计，设计方案参考《南方电网公司系统自主可控适配典型设计参考（2024版）》，且后续根据上述文件同步更新迭代。

3、本项目涉及的所有应用和软硬件产品必须符合自主可控要求，且本项目涉及的所有应用能够适配未来自主可控环境潜在变化需求，目前南方电网公司 CPU、操作系统、数据库、中间件、计算机终端、浏览器、开源软件及关键组件等自主可控选型适配设计情况包括但不限于：

1) CPU：计算机终端 CPU 要求兼容自主可控 CPU（ARM、MIPS、X86、ALPHA 等）架构，根据项目业务需求选择自主可控 CPU（如龙芯、兆芯、飞腾、鲲鹏、申威、海光等）。服务器 CPU 要求兼容自主可控 CPU（ARM、MIPS、X86、ALPHA 等）架构，选型要求确保系统的稳定性、可靠性以及满足特定的性能需求，包括不限于飞腾、鲲鹏、海光等产品。

2) 操作系统：兼容国内主流桌面、服务器自主可控操作系统（如统信 UOS、银河麒麟、麒麟信安等）。

3) 数据库：要求兼容国内主流自主可控数据库（包括不限于达梦、金仓等）。

4) 中间件：兼容国内主流自主可控中间件（如：中创等）。

5) 浏览器：兼容统信浏览器、麒麟奇安信浏览器、360 安全浏览器、搜狗浏览器、红芯浏览器等自主可控浏览器，应用系统可与支持国密算法的国产浏览器加密通信。

6) 开源软件及关键组件：要求开源软件及关键组件自主可控，选型过程中评估这些组件与现有系统的兼容性和可替代性。