



(12) 发明专利申请

(10) 申请公布号 CN 111815132 A

(43) 申请公布日 2020. 10. 23

(21) 申请号 202010596147.7

G06Q 50/06 (2012.01)

(22) 申请日 2020.06.28

(71) 申请人 云南电网有限责任公司电力科学研究院

地址 650217 云南省昆明市经济技术开发区云大西路105号

(72) 发明人 李孟阳 孙暄 唐立军 李踔 王禹

(74) 专利代理机构 北京弘权知识产权代理事务所(普通合伙) 11363

代理人 逯长明 许伟群

(51) Int. Cl.

G06Q 10/06 (2012.01)

G06F 21/46 (2013.01)

G06F 21/62 (2013.01)

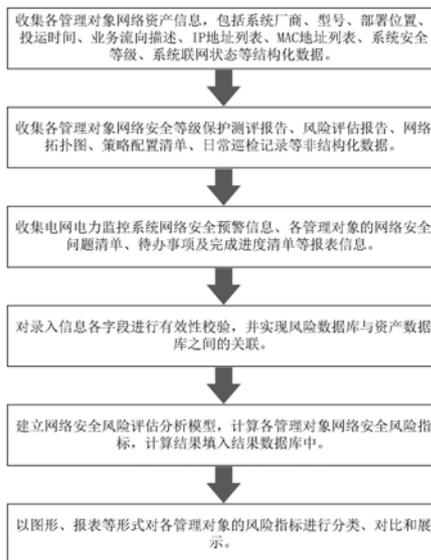
权利要求书2页 说明书5页 附图2页

(54) 发明名称

一种电力监控系统网络安全管理信息发布方法及系统

(57) 摘要

本发明提出一种电力监控系统网络安全管理信息发布方法及系统;用于收集、汇总、分析和展示各供电单位和发电企业电网电力监控系统网络安全态势信息,并面向各单位发布电力监控系统网络安全风险监测预警信息。所述系统由应用服务器、多个网页客户端、信息录入模块、数据库、数据校验模块、风险评估分析模块、身份鉴别模块、指标展示模块构成。针对电力监控系统网络安全管理业务需求,提出数据建模、账户权限分配、指标分析、数据有效性校验相关方法,以网页访问形式向各单位发布电力监控系统网络安全风险监测预警信息,对电力监控系统网络安全风险数据进行有效的管理和展示,提升电力监控系统网络安全管理信息化水平。



1. 一种电力监控系统网络安全管理信息发布方法,其特征在于,包括以下步骤:

建立基础数据库,并收集各管理对象网络资产台账、网络拓扑图、风险评估报告、等级保护测评报告等结构化数据与各管理对象网络安全等级保护测评报告、策略配置清单、日常巡检记录等非结构化数据,将所得数据存储于所述的基础数据库内;

建立实时数据库,并实时采集电网电力监控系统网络安全预警信息、各管理对象的网络安全问题清单、待办事项及完成进度清单等数据,将所得的实时数据动态储存至所述实时数据库;

对所收集到的数据进行有效性校验,实现实时数据库与基础数据库之间的关联;

建立网络安全风险评估分析模型,计算各管理对象网络安全风险指标;

建立结果数据库,将网络安全风险评估分析模型计算所得的网络安全风险指标结果存入结果数据库;

对各管理对象的风险指标进行分类、对比,实现网络安全态势的不同管理对象之间及同一管理对象不同管理阶段之间的指标对比;

对客户端登陆用户的身份进行识别,并根据用户身份权限管理矩阵对当前登陆用户的操作和访问权限进行描述和限制,对获得访问权限的用户展示风险指标对比结果。

2. 根据权利要求1所述的一种电力监控系统网络安全管理信息发布方法,其特征在于,所述对所收集到的数据进行有效性校验时,校验逻辑采用JS脚本方式描述和实现,校验内容包括录入信息的数据类型、字符长度、文件类型、语义、数值范围,将录入错误信息剔除并采用气泡信息方式在页面上给出相应提示,将正确信息进行储存。

3. 根据权利要求1所述的一种电力监控系统网络安全管理信息发布方法,其特征在于,所述对获得访问权限的用户展示风险指标对比结果,根据用户指定的查询信息,以动态报表生成及导出、文档查询及下载等方式对查询结果进行网页展示。

4. 根据权利要求1所述的一种电力监控系统网络安全管理信息发布方法,其特征在于,所述非结构化数据包括标准文档、工作记录与测评报告,收集到所述非结构化数据后,进行文档版本管理,将管理后的文档分类储存,再将储存后的分类文档转换成磁盘文件进行保存;所述结构化数据包括在线填报数据与报表导入数据,将收集到的结构化数据进行数据库建模、填报页面设计、填报数据校验处理后储存至结构化数据库。

5. 一种电力监控系统网络安全管理信息发布系统,其特征在于,所述系统由应用服务器、多个网页客户端、信息录入模块、数据库、数据校验模块、风险评估分析模块、身份鉴别模块、指标展示模块构成;其中所述应用服务器用于为该平台的数据库、功能模块提供运行环境支撑,通过电力综合数据网向多个客户端提供远程访问和信息调阅应用服务;所述信息录入模块用于提供信息录入功能,支持离线报表导入或在线填报方式将所述信息存储到数据库服务器中;

所述数据校验模块用于对录入信息的正确性进行判断,校验内容包括录入信息的数据类型、字符长度、文件类型、语义、数值范围,校验逻辑采用JS脚本方式描述和实现,剔除录入错误信息并采用气泡信息方式在页面上给出相应提示,储存录入正确信息;

所述数据库由基础数据库、实时数据库和结果数据库三部分构成,其中:基础数据库包括各管理对象的设备资产台账、网络拓扑图,风险评估报告、等级保护测评报告信息;实时数据库用于动态存储电网电力监控系统网络安全预警信息、各管理对象的网络安全问题清

单、待办事项及完成进度清单；结果数据库用于存储各管理对象的网络安全风险评估指标，包括各供电局、发电厂、变电站的电力监控系统网络资产构成、总体网络安全风险值和工作完成情况进度指标；

风险评估分析模块用于根据网络安全风险评估分析算法自动计算相关单位、相关类型系统的网络安全风险评估值；

身份鉴别模块根据用户身份权限管理矩阵对当前登陆用户的操作和访问权限进行描述和限制；

指标展示模块用于根据用户指定的查询信息，以动态报表生成及导出、文档查询及下载等方式对查询结果进行网页展示。

6. 根据权利要求5所述的一种电力监控系统网络安全管理信息发布系统，其特征在于，所述身份鉴别模块采用数字证书加登陆口令方式对客户端登陆用户的身份进行识别。

一种电力监控系统网络安全管理信息发布方法及系统

技术领域

[0001] 本发明涉及电力网络安全领域,特别涉及一种电力监控系统网络安全管理信息发布方法及系统。

背景技术

[0002] 电力行业的网络安全管理理论和方法是目前国内外相关企业、研究机构研究的热点,包括网络资产管理、风险评估分析方法、网络事件监测分析等,但相关研究均尚未系统化的开展,尚未形成满足电网和发电企业日常网络安全管理需求的信息管理系统。众所周知,传统的电力监控系统网络安全信息发布方式较为单一,信息发布的内容多以风险分析报告、数据报表形式为主,信息发布的实时性低、可读性差;而随着电力监控系统网络安全管理和防护体系逐步建立完善,网络安全信息的类型和数量越来越多,各单位对网络安全信息的可视化需求也越来越高,如何有效跟进风险处置过程,如何多维度分析电网网络安全态势,如何为各管理者直观展示分析结果,是电网网络安全管理体系建设过程中迫切需要解决的问题。其中缺乏有效的信息采集技术手段,相关信息汇总工作量大、人工汇总效率低下、重要报表统计和上报不及时;缺乏有效的信息管理技术手段,各单位网络安全管理人员难以及时掌握本单位设备资产信息,上报数据质量不满足管理要求;缺乏有效的工作闭环管控技术手段,各单位网络安全管理人员难以及时掌握相关工作任务完成情况,无法及时对相关工作遗留问题进行闭环管控,主管部门难以及时准确分析和掌握全网安全态势的问题,无法满足各单位电力监控系统安全防护的设备资产管理、信息自动统计分析和工作闭环管控需求,是电力行业的网络安全管理领域中首当其冲的问题。

发明内容

[0003] 针对现有技术所存在的问题,本发明提供了一种电力监控系统网络安全管理信息发布方法及系统,用于收集、汇总、分析和展示各供电单位和发电企业电网电力监控系统网络安全态势信息,并以网页访问形式为各单位发布电力监控系统网络安全风险监测预警信息。解决缺乏有效的信息采集技术手段,相关信息汇总工作量大、人工汇总效率低下、重要报表统计和上报不及时;缺乏有效的信息管理技术手段,各单位网络安全管理人员难以及时掌握本单位设备资产信息,上报数据质量不满足管理要求;缺乏有效的工作闭环管控技术手段,各单位网络安全管理人员难以及时掌握相关工作任务完成情况,无法及时对相关工作遗留问题进行闭环管控,主管部门难以及时准确分析和掌握全网安全态势的问题,满足各单位电力监控系统安全防护的设备资产管理、信息自动统计分析和工作闭环管控需求,提升了我省电力监控系统网络安全管理信息化水平,为电力监控系统网络安全体系建设顶层设计提供辅助参考。

[0004] 一种电力监控系统网络安全管理信息发布方法,包括以下步骤:

[0005] 建立基础数据库,并收集各管理对象网络资产台账、网络拓扑图、风险评估报告、等级保护测评报告等结构化数据与各管理对象网络安全等级保护评测报告、策略配置清

单、日常巡检记录等非结构化数据,将所得数据存储于所述的基础数据库内;

[0006] 建立实时数据库,并实时采集电网电力监控系统网络安全预警信息、各管理对象的网络安全问题清单、待办事项及完成进度清单等数据,将所得的实时数据动态储存至所述实时数据库;

[0007] 对所收集到的数据进行有效性校检,实现实时数据库与基础数据库之间的关联;

[0008] 建立网络安全风险评估分析模型,计算各管理对象网络安全风险指标;

[0009] 建立结果数据库,将网络安全风险评估分析模型计算所得的网络安全风险指标结果存入结果数据库;

[0010] 对各管理对象的风险指标进行分类、对比,实现网络安全态势的不同管理对象之间及同一管理对象不同管理阶段之间的指标对比;

[0011] 对客户端登陆用户的身份进行识别,并根据用户身份权限管理矩阵对当前登陆用户的操作和访问权限进行描述和限制,对获得访问权限的用户展示风险指标对比结果。

[0012] 所述对所收集到的数据进行有效性校检时,校验逻辑采用JS脚本方式描述和实现,校验内容包括录入信息的数据类型、字符长度、文件类型、语义、数值范围,将录入错误信息剔除并采用气泡信息方式在页面上给出相应提示,将正确信息进行储存。

[0013] 所述对获得访问权限的用户展示风险指标对比结果,根据用户指定的查询信息,以动态报表生成及导出、文档查询及下载等方式对查询结果进行网页展示。

[0014] 所述非结构化数据包括标准文档、工作记录与测评报告,收集到所述非结构化数据后,进行文档版本管理,将管理后的文档分类储存,再将储存后的分类文档转换成磁盘文件进行保存;所述结构化数据包括在线填报数据与报表导入数据,将收集到的结构化数据进行数据库建模、填报页面设计、填报数据校验处理后储存至结构化数据库。

[0015] 一种电力监控系统网络安全管理信息发布系统,由应用服务器、多个网页客户端、信息录入模块、数据库、数据校验模块、风险评估分析模块、身份鉴别模块、指标展示模块构成;其中所述应用服务器用于为该平台的数据库、功能模块提供运行环境支撑,通过电力综合数据网向多个客户端提供远程访问和信息调阅应用服务;所述信息录入模块用于提供信息录入功能,支持离线报表导入或在线填报方式将所述信息存储到数据库服务器中;

[0016] 所述数据校验模块用于对录入信息的正确性进行判断,校验内容包括录入信息的数据类型、字符长度、文件类型、语义、数值范围,校验逻辑采用JS脚本方式描述和实现,剔除录入错误信息并采用气泡信息方式在页面上给出相应提示,储存录入正确信息;

[0017] 所述数据库由基础数据库、实时数据库和结果数据库三部分构成,其中:基础数据库包括各管理对象的设备资产台账、网络拓扑图,风险评估报告、等级保护测评报告信息;实时数据库用于动态存储电网电力监控系统网络安全预警信息、各管理对象的网络安全问题清单、待办事项及完成进度清单;结果数据库用于存储各管理对象的网络安全风险评估指标,包括各供电局、发电厂、变电站的电力监控系统网络资产构成、总体网络安全风险值和工作完成情况进度指标;

[0018] 风险评估分析模块用于根据网络安全风险评估分析算法自动计算相关单位、相关类型系统的网络安全风险评估值;

[0019] 身份鉴别模块根据用户身份权限管理矩阵对当前登陆用户的操作和访问权限进行描述和限制;指标展示模块用于根据用户指定的查询信息,以动态报表生成及导出、文档

查询及下载等方式对查询结果进行网页展示。所述身份鉴别模块采用数字证书加登陆口令方式对客户端登陆用户的身份进行识别。

[0020] 本申请的有益效果：本发明所提的分层分级控制框架通过集合灵活资源模型，相较传统的单层集中式协调控制策略，能够有效降低不同层级控制中心之间的数据传输容量，并提高每个层级优化计算的效率。同时多时间尺度分级控制能够充分考虑可再生能源出力的波动性与随机性，有效消除其预测误差对运行优化的影响。

[0021] 本发明提供了一种电力监控系统网络安全管理信息发布方法及系统，用于收集、汇总、分析和展示各供电单位和发电企业电网电力监控系统网络安全态势信息，针对电力监控系统网络安全管理业务需求，提出数据建模、账户权限分配、指标分析、数据有效性校验相关方法，具备电力监控系统安全防护的设备资产管理、信息自动统计分析和工作闭环管控的应用功能，以网页访问形式向各单位发布电力监控系统网络安全风险监测预警信息，能够以图型、报表、文档形式对电力监控系统网络安全风险数据进行有效的管理和展示，提升电力监控系统网络安全管理信息化水平，为电力监控系统网络安全体系建设顶层设计提供辅助参考。

附图说明

[0022] 为了更清楚地说明本申请的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，对于本领域普通技术人员而言，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0023] 图1为本申请一种电力监控系统网络安全管理信息发布方法流程图；

[0024] 图2为本申请对结构化数据与非结构化数据的处理流程图。

具体实施方式

[0025] 一种电力监控系统网络安全管理信息发布方法，如图1所示，包括以下步骤：

[0026] 建立基础数据库，并收集各管理对象网络资产台账、网络拓扑图、风险评估报告、等级保护测评报告等结构化数据与各管理对象网络安全等级保护评测报告、策略配置清单、日常巡检记录等非结构化数据，将所得数据存储于所述的基础数据库内；

[0027] 建立实时数据库，并实时采集电网电力监控系统网络安全预警信息、各管理对象的网络安全问题清单、待办事项及完成进度清单等数据，将所得的实时数据动态储存至所述实时数据库；

[0028] 对所收集到的数据进行有效性校检，实现实时数据库与基础数据库之间的关联；

[0029] 建立网络安全风险评估分析模型，计算各管理对象网络安全风险指标；

[0030] 建立结果数据库，将网络安全风险评估分析模型计算所得的网络安全风险指标结果存入结果数据库；

[0031] 对各管理对象的风险指标进行分类、对比，实现网络安全态势的不同管理对象之间及同一管理对象不同管理阶段之间的指标对比；

[0032] 对客户端登陆用户的身份进行识别，并根据用户身份权限管理矩阵对当前登陆用户的操作和访问权限进行描述和限制，对获得访问权限的用户展示风险指标对比结果。

[0033] 所述对所收集到的数据进行有效性校检时，校验逻辑采用JS脚本方式描述和实

现,校验内容包括录入信息的数据类型、字符长度、文件类型、语义、数值范围,将录入错误信息剔除并采用气泡信息方式在页面上给出相应提示,将正确信息进行储存。

[0034] 所述对获得访问权限的用户展示风险指标对比结果,根据用户指定的查询信息,以动态报表生成及导出、文档查询及下载等方式对查询结果进行网页展示。

[0035] 所述非结构化数据包括标准文档、工作记录与测评报告,如图2所示,收集到所述非结构化数据后,进行文档版本管理,将管理后的文档分类储存,再将储存后的分类文档转换成磁盘文件进行保存;所述结构化数据包括在线填报数据与报表导入数据,将收集到的结构化数据进行数据库建模、填报页面设计、填报数据校验处理后储存至结构化数据库。

[0036] 一种电力监控系统网络安全管理信息发布系统,由应用服务器、多个网页客户端、信息录入模块、数据库、数据校验模块、风险评估分析模块、身份鉴别模块、指标展示模块构成;其中所述应用服务器用于为该平台的数据库、功能模块提供运行环境支撑,通过电力综合数据网向多个客户端提供远程访问和信息调阅应用服务;所述信息录入模块用于提供信息录入功能,支持离线报表导入或在线填报方式将所述信息存储到数据库服务器中;

[0037] 所述数据校验模块用于对录入信息的正确性进行判断,校验内容包括录入信息的数据类型、字符长度、文件类型、语义、数值范围,校验逻辑采用JS脚本方式描述和实现,剔除录入错误信息并采用气泡信息方式在页面上给出相应提示,储存录入正确信息;

[0038] 所述数据库由基础数据库、实时数据库和结果数据库三部分构成,其中:基础数据库包括各管理对象的设备资产台账、网络拓扑图,风险评估报告、等级保护测评报告信息;实时数据库用于动态存储电网电力监控系统网络安全预警信息、各管理对象的网络安全问题清单、待办事项及完成进度清单;结果数据库用于存储各管理对象的网络安全风险评估指标,包括各供电局、发电厂、变电站的电力监控系统网络资产构成、总体网络安全风险值和工作完成情况进度指标;

[0039] 风险评估分析模块用于根据网络安全风险评估分析算法自动计算相关单位、相关类型系统的网络安全风险评估值;

[0040] 身份鉴别模块根据用户身份权限管理矩阵对当前登陆用户的操作和访问权限进行描述和限制;指标展示模块用于根据用户指定的查询信息,以动态报表生成及导出、文档查询及下载等方式对查询结果进行网页展示。所述身份鉴别模块采用数字证书加登陆口令方式对客户端登陆用户的身份进行识别。

[0041] 本发明所提的分层分级控制框架通过集合灵活资源模型,相较传统的单层集中式协调控制策略,能够有效降低不同层级控制中心之间的数据传输容量,并提高每个层级优化计算的效率。同时多时间尺度分级控制能够充分考虑可再生能源出力的波动性与随机性,有效消除其预测误差对运行优化的影响。

[0042] 本发明提供了一种电力监控系统网络安全管理信息发布方法及系统,用于收集、汇总、分析和展示各供电单位和发电企业电网电力监控系统网络安全态势信息,针对电力监控系统网络安全管理业务需求,提出数据建模、账户权限分配、指标分析、数据有效性校验相关方法,具备电力监控系统安全防护的设备资产管理、信息自动统计分析和工作闭环管控的应用功能,以网页访问形式向各单位发布电力监控系统网络安全风险监测预警信息,能够以图型、报表、文档形式对电力监控系统网络安全风险数据进行有效的管理和展示,提升电力监控系统网络安全管理信息化水平,为电力监控系统网络安全体系建设顶层

设计提供辅助参考。

[0043] 应当理解的是,本发明并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本发明的范围仅由所附的权利要求来限制。

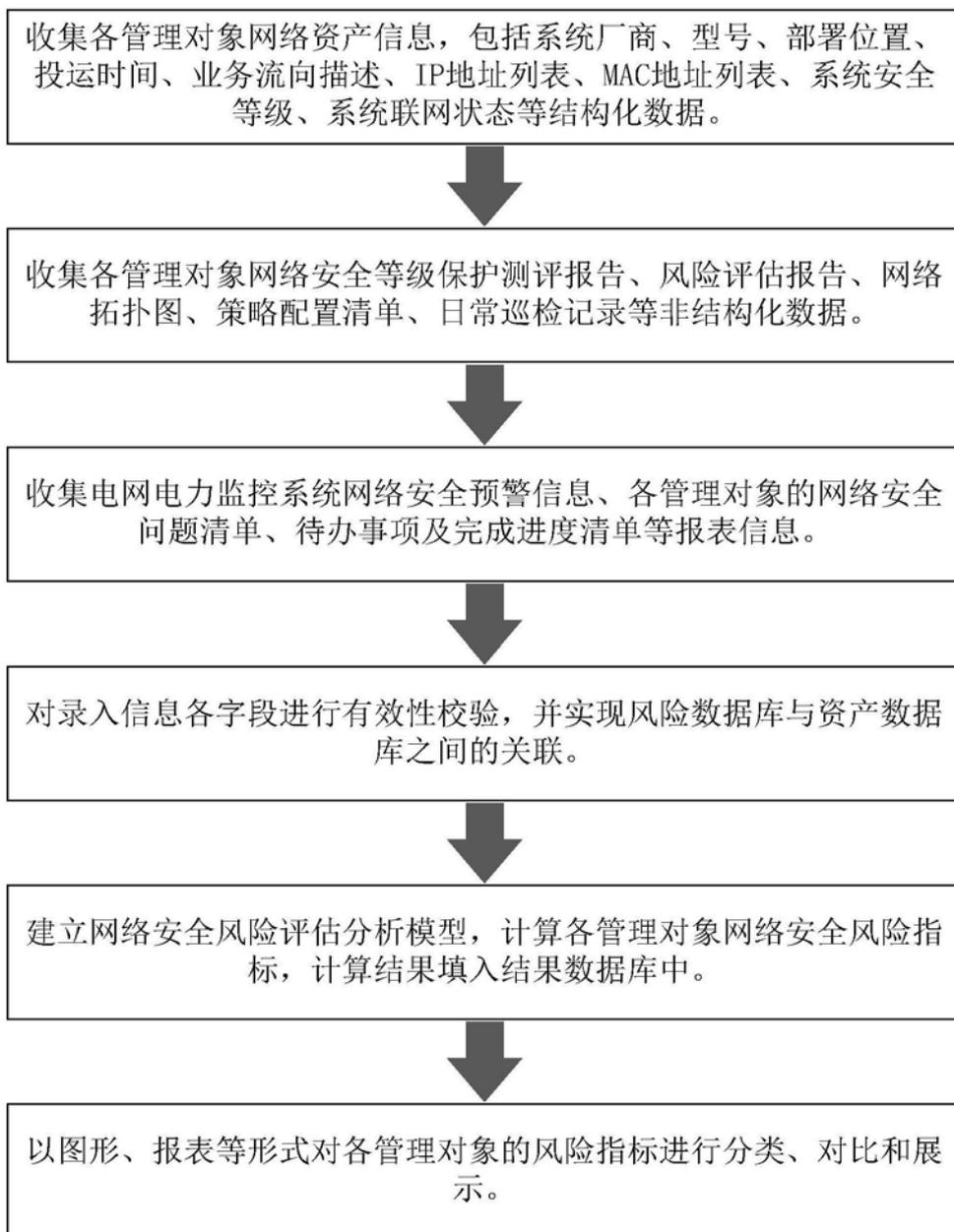


图1

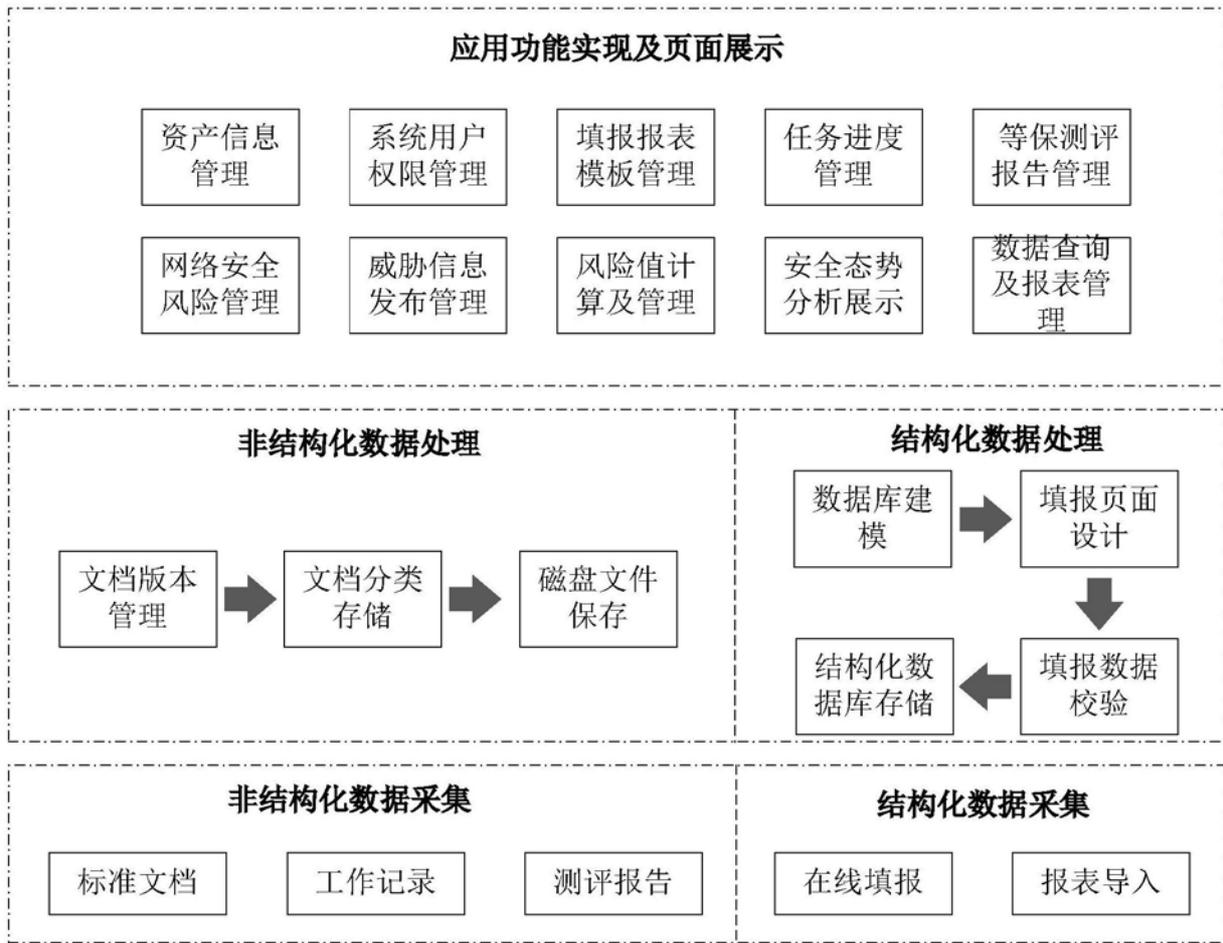


图2