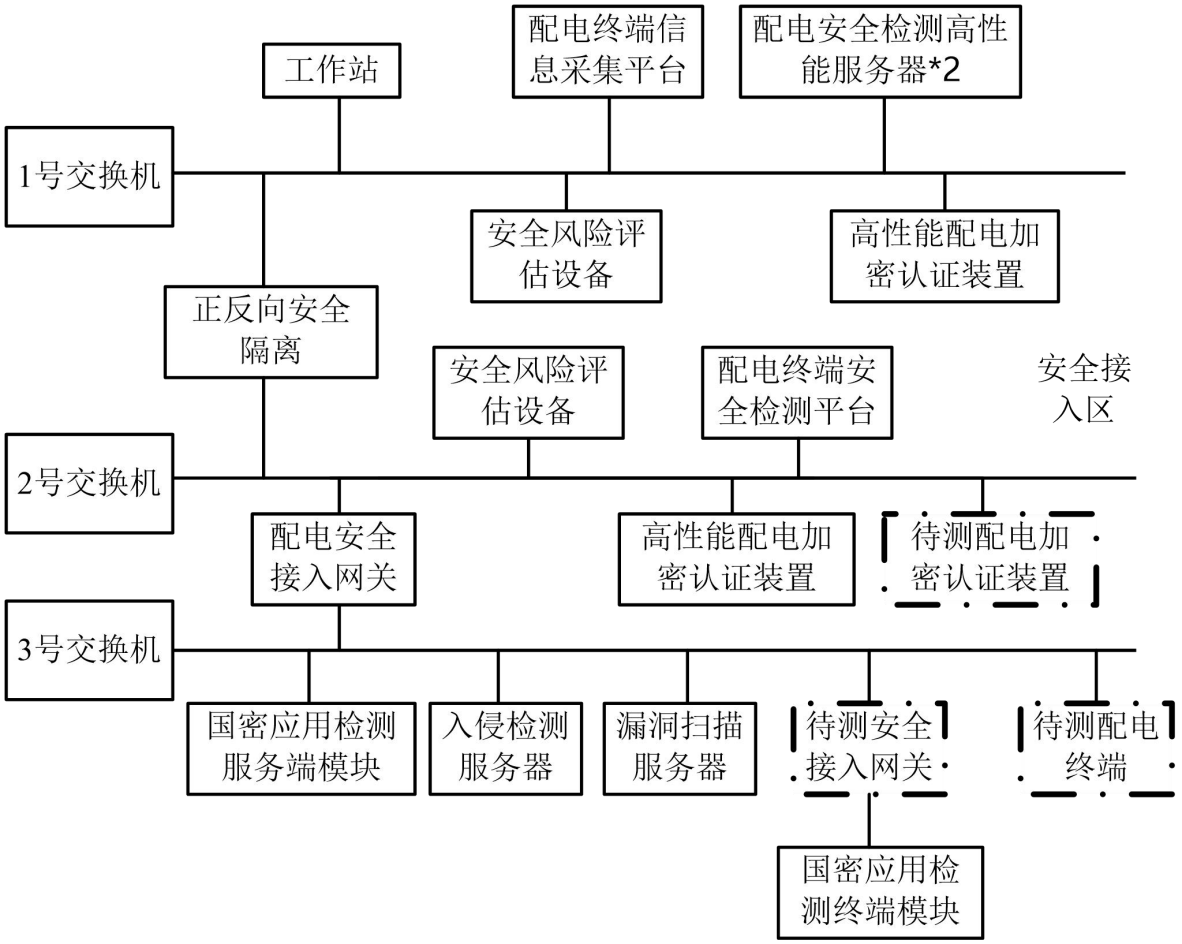
摘　要

本发明公开了一种基于流水线自动运转的配电终端安全检测系统及方法，包括配电终端流水线、安全检测平台以及安全检测综合管控平台，在配电终端进行安全检测时，由机器人和流水线实现被测终端的上下线和插拔线过程，由安全检测平台实现安全能力检测，由综合管控系统实现检测过程的信息交互，从而实现配电终端的全自动安全检测。通过本发明的研究，针对配电终端的信息安全提供了一套完整、高效、可靠的全自动检测系统及方法，为国家电网公司新一代配电网建设安全防护措施的完善提供了支持，使信息安全保障活动更好的遵循 PDCA 循环科学建设理念。

摘　要　附　图


工作站
配电终端信息采集平台
配电安全检测高性能服务器*2
1号交换机
安全风险评估设备
高性能配电加密认证装置
正反向安全隔离
安全风险评估设备
配电终端安全检测平台
安全接入区
2号交换机
配电安全接入网关
高性能配电加密认证装置
待测配电加密认证装置
3号交换机
国密应用检测服务端模块
入侵检测服务器
漏洞扫描服务器
待测安全接入网关
待测配电终端
国密应用检测终端模块

权　利　要　求　书

1. 一种基于流水线自动运转的配电终端安全检测系统，包括：配电终端检测流水线、配电终端安全检测平台，以及连通两者进行信息交互的综合管控系统；其特征在于，所述配电终端检测流水线用于配电终端的接入和运出，所述配电终端安全检测平台用于对所述安全检测系统自身以及配电终端进行安全检测，其包括高性能配电加密认证装置、安全风险评估设备、入侵检测服务器、安全设备检测装置及漏洞扫描服务器；所述安全风险评估设备采用矩阵法或相乘法计算威胁出现的频率、评估脆弱性的严重程度以及信息资产的重要程度，确定由于威胁或利用脆弱性导致安全事件发生的可能性、综合安全事件所作用的资产价值及脆弱性的严重程度判断安全事件造成的损失。

2. 如权利要求1所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述配电终端安全检测平台包括：1、2号交换机通过正、反向安全隔离分开，形成两个网络安全区，2、3交换机通过配电安全接入网关隔离，形成第3网络安全区；两台配电加密认证装置分别接在1、2号交换机上；两台安全风险评估设备分别接在1、2号交换机上；两台配电安全检测服务器接入1号交换机上；入侵检测服务器和漏洞扫描服务器连接到3号交换机上；国密应用检测终端模块通过被测安全网关接入3号交换机；国密应用检测服务端模块连接到3号交换机上；待测配电终端接入3号交换机；待测配电加密认证装置连接到2号交换机。

3. 如权利要求 1 所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述配电终端安全检测系统配置有配电自动化国产密码应用检测平台，所述配电自动化国产密码应用检测平台基于配电终端安全检测平台，由配电终端接入设备安全检测、配电终端采集平台安全检测、配电加密认证装置检测、以及配电安全接入网关检测四部分组成。

~~4. 如权利要求 1 所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述安全风险评估设备采用矩阵法或相乘法计算威胁出现的频率、评估脆弱性的严重程度以及信息资产的重要程度，确定由于威胁或利用脆弱性导致安全事件发生的可能性、综合安全事件所作用的资产价值及脆弱性的严重程度判断安全事件造成的损失。~~

~~5~~4. 如权利要求 1 所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述配电终端安全检测平台基于入侵检测服务器进行敏感数据外发检测和客户端攻击检测。

~~6~~5. 如权利要求 ~~5~~4 所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述入侵检测采用被动检测的方式对安全检测平台和配电终端进行网络攻击和入侵检测，通过采集数据包，从数据流量中检测异常流量变化，以发现网络异常。

~~7~~6. 如权利要求 1 所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述配电终端安全检测平台基于漏洞扫描服务器按照发现漏洞、复现漏洞、模拟漏洞攻击、评估

及验证影响的顺序进行漏洞安全评估。

~~8~~7. 如权利要求 ~~7~~6 所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述漏洞扫描服务器应用开放式扫描、隐蔽式扫描、半开放式扫描中的任一种进行扫描。

~~9~~8. 如权利要求 1 所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述配电终端检测流水线包括装载机器人、卸载机器人、插拔线机器人、流水线体和检测工位。

~~10~~9. 如权利要求 ~~9~~8 所述基于流水线自动运转的配电终端安全检测系统，其特征在于，所述装载机器人用于将被测配电终端自动运送到检修工位；所述插拔线机器人对被测配电终端进行插拔线操作，使其接入安全检测平台；所述卸载机器人根据所述配电终端安全检测平台的检测结果对被测终端进行区分，按照合格与否进行分类筛检，不合格设备卸载到不合格产品区。

~~11~~10. 一种包含权利要求 1-~~10~~9 任一项所述基于流水线自动运转的配电终端安全检测系统的搭建方法，包括以下步骤：

步骤 1）：搭建配电终端全自动流水线；

步骤 2）：搭建配电终端安全检测平台；

步骤 3）：搭建综合管控系统，分别与全自动流水线和安全检测平台进行接口交互。

~~12~~11. 一种利用权利要求 1-~~10~~9 任一项所述基于流水线自动运转的配电终端安全检测系统对配电终端进行检测的方法，包括以下步骤：

步骤 1）：装载机器人在综合管控系统的控制下将被测配电终端自动运送到检修工位，插拔线机器人对待检测配电终端进行插线操作，使其接入安全检测平台；并传送信号给综合管控系统；

步骤 2）：配电终端安全检测平台按照综合管控系统给出的指令对配电终端进行安全检测，并将检测结果发送给综合管控系统；

步骤 3）：综合管控系统在接收到检测结果后，根据检测结果发送指令给检测流水线，卸载机器人根据所述指令进行下一步操作。

~~13~~12. 如权利要求 ~~12~~11 所述对配电终端进行检测的方法，其特征在于：

所述步骤 3）所述卸载机器人根据指令进行的下一步操作包括对被测终端进行区分，按照合格与否进行分类筛检，不合格设备卸载到不合格产品区。

一种基于流水线自动运转的配电终端安全检测系统及方法

技术领域

本发明涉及配电自动化终端检测领域，具体涉及一种基于流水线自动运转的配电终端安全检测系统及方法。

背景技术

国家电网公司正在全面建设以特高压电网为骨干网架、各级电网协调发展的坚强电网，以信息化、自动化、互动化为特征的自主创新、国际领先的智能电网。配电网处于电网的中间环节，是直接面向社会和客户的重要能源载体，是分布式电源和电动汽车的变革支持，因此也是坚强、智能电网的重要基础和组成部分。基于配电终端的配电自动化是实现智能配电网的重要手段，为配电网的监测和控制提供坚实基础，是提高城网供电可靠性的必然需要，是建设智能配电网的基石。因而配电终端信息采集系统的安全性及稳定性将直接影响调控人员对配电网的调控水平。

随着计算机和网络技术的发展以及信息化与电力监控系统的深度融合，配电终端信息采集系统，特别是各配电终端面临的信息安全问题日益严峻。2010 年的“震网”病毒、2012 年的“火焰”超级病毒、2014 年的“Havex”病毒、2015 年的“Black Energy”病毒等专门针对电力系统的病毒爆发给电力企业、社会经济带来了巨大损失，直接或间接地威胁到了国家安全。2015 年，因为黑客攻击造成乌克兰电网大停电，给我国电网的安全防护带来了很高的警示性。虽然国网系统采用高安全级别的安全防护，但是随着配电自动化终端采用无线移动网络进行采集信息的传输，为电网的安全防护带来更高的挑战。因此，提高基于大量配电终端的配电终端信息采集系统的信息安全性、运行稳定性，避免出现网络信息安全问题刻不容缓。

国网运检部在 2017 年初发布运检三〔2017〕6 号文，《国网运检部关于做好“十三五”配电自动化建设应用工作的通知》中在第五部分“加强专业协同”第 3 条“加强设备质量管控”的工作安排中明确要求如下：“各单位运检部门要会同物资部门，强化设备入网检测、到货检测、运行分析评价三级质量管控措施，严把设备质量关。配电终端、线路故障指示器、智能配变终端、一二次成套开关等设备的采购，所采购设备必须通过中国电科院组织的专项检测；各单位对配电终端、线路故障指示器、智能配变终端采取到货全检”。

国网山东省电力公司电力科学研究院作为山东省配电网的技术支撑和电网安全运行分析单位，对配电终端及其相关系统的安全检测十分必要。之前针对安全方面的检测，没有成熟的手段和有效的支撑，同时配电终端航空插头的插拔线工作也异常繁琐，导致信息安全的检测难以实现。同时需要进行到货全检后，配电自动化终端检测中心每年将检测的终端数量是十分庞大的，单纯依靠人工进行逐台设备的检测，进行到货全检将会面临检测能力欠缺，检测人员不足，检测信息无法统一管理的困境。因此，依靠先进的全自动检测技术，实现低人工情况下的高效能全自动安全检测，满足国网运检部对配电终端安全检测和检测能力的全面要求，仍是待解决的技术问题。

发明内容

本发明专利针对上述技术问题提供了一种基于流水线自动运转的配电终端安全检测系统及检测方法，其目的在于通过流水线自动上、下料的方式，对配电终端自动进行安全检测。

一种基于流水线自动运转的配电终端安全检测系统，包括：配电终端检测流水线、配电终端安全检测平台，以及连通两者进行信息交互的综合管控系统；其特征在于，所述配电终端检测流水线用于配电终端的接入和运出，所述配电终端安全检测平台用于对所属安全检测系统自身以及配电终端进行安全检测，其包括高性能配电加密认证装置、安全风险评估设备、入侵检测服务器、安全设备检测装置及漏洞扫描服务器。

其中，所述配电终端安全检测平台的具体结构为，1、2 号交换机通过正、反向安全隔离分开，形成两个网络安全区，2、3 交换机通过配电安全接入网关隔离，形成第 3 网络安全区；两台高性能配电加密认证装置分别接在 1、2 号交换机上；两台安全风险评估设备分别接在 1、2 号交换机上；两台配电安全检测高性能服务器接入 1 号交换机上；入侵检测服务器和漏洞扫描服务器连接到 3 号交换机上；国密应用检测终端模块通过被测安全网关接入 3 号交换机；国密应用检测服务端模块连接到 3 号交换机上；待测配电终端接入 3 号交换机；待测配电加密认证装置连接到 2 号交换机。

其中，所述配电终端安全检测系统配置有配电自动化国产密码应用检测平台，所述配电自动化国产密码应用检测平台基于配电终端安全检测平台，由配电终端接入设备安全检测、配电终端采集平台安全检测、配电加密认证装置检测、以及配电安全接入网关检测四部分组成。

其中，所述安全风险评估设备主要从威胁评估、脆弱性评估和信息资产评估三方面进行评估，计算威胁出现的频率、评估脆弱性的严重程度以及信息资产的重要程度，采用矩阵法或相乘法计算确定由于威胁或利用脆弱性导致安全事件发生的可能性、综合安全事件所作用

的资产价值及脆弱性的严重程度判断安全事件造成的损失。

其中，所述配电终端安全检测平台基于入侵检测服务器进行敏感数据外发检测和客户端攻击检测。所述入侵检测采用被动检测的方式对安全检测平台和配电终端进行网络攻击和入侵检测，通过采集数据包，从数据流量中检测异常流量变化，以发现网络异常。

其中，所述配电终端安全检测平台基于漏洞扫描服务器按照发现漏洞、复现漏洞、模拟漏洞攻击、评估及验证影响的顺序进行漏洞安全评估。所述漏洞扫描服务器应用开放式扫描、隐蔽式扫描、半开放式扫描中的任一种进行扫描。

其中，所述配电终端检测流水线包括装载机器人、卸载机器人、插拔线机器人、流水线体和检测工位。所述装载机器人用于将被测配电终端自动运送到检修工位；所述插拔线机器人对待检测配电终端进行插拔线操作，使其接入安全检测平台；所述卸载机器人根据所述配电终端安全检测平台的检测结果对被测终端进行区分，按照合格与否进行分类筛检，不合格设备卸载到不合格产品区。

本发明还提供一种基于流水线自动运转的配电终端安全检测系统的搭建方法，包括以下步骤：

步骤 1)：搭建配电终端全自动流水线；

步骤 2)：搭建配电终端安全检测平台；

步骤 3)：搭建综合管控系统，分别与全自动流水线和安全检测平台进行接口交互。

本发明进一步提供一种基于基于流水线自动运转的配电终端安全检测系统对配电终端进行检测的方法，包括以下步骤：

步骤 1)：装载机器人在综合管控系统的控制下将被测配电终端自动运送到检修工位，插拔线机器人对待检测配电终端进行插线操作，使其接入安全检测平台；并传送信号给综合管控系统；

步骤 2)：配电终端安全检测平台按照综合管控系统给出的指令对配电终端进行安全检测，并将检测结果发送给综合管控系统；

步骤 3)：综合管控系统在接收到检测结果后，根据检测结果发送指令给检测流水线，卸载机器人根据所述指令进行下一步操作。

其中，所述步骤 3）中所述卸载机器人根据指令进行的下一步操作包括对被测终端进行区分，按照合格与否进行分类筛检，不合格设备卸载到不合格产品区。

本发明具有的有益效果

1. 本发明提供的基于流水线自动运转的安全检测系统及方法，实现了配电终端安全检测

的自动化，节约了人力物力，提高了检测效率。

2. 本发明提出的基于流水线自动运转的安全检测系统及方法，是配电终端的安全防护措施的合理补充，可有效提高配电终端信息采集系统的安全性，对于保证配电终端信息采集系统安全稳定的运行具有重要意义。

3. 本发明有效验证山东电力部署的配电终端信息采集系统的安全防护措施的整体有效性和健壮性，实现对配电系统安全防护措施的有效性和健壮性的常态化检测，提高系统安全防护能力。

附图说明

构成本发明的一部分的说明书附图用来提供对本发明的进一步理解，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。

图 1 为本发明的基于流水线自动运转的安全检测系统基础框架；

图 2 为本发明中配网终端安全风险检测平台系统结构图；

图 3 为基于本发明配电终端安全风险检测平台的国产密码检测平台逻辑框图；

图 4 为本发明信息安全风险分析原理图；

图 5 为本发明安全漏洞扫描检测流程图。

具体实施方式

应该指出，以下详细说明都是例示性的，旨在对本申请提供进一步的说明。除非另有指明，本文使用的所有技术和科学术语具有与本申请所属技术领域的普通技术人员通常理解的相同含义。

需要注意的是，这里所使用的术语仅是为了描述具体实施方式，而非意图限制根据本申请的示例性实施方式。如在这里所使用的，除非上下文另外明确指出，否则单数形式也意图包括复数形式，此外，还应当理解的是，当在本说明书中使用术语“包含”和/或“包括”时，其指明存在特征、步骤、操作、器件、组件和/或它们的组合。

下面结合附图与实施例对本发明作进一步说明。

如图 1 所示，本发明提出的一种基于流水线自动运转的配电终端安全检测系统，包括配电终端检测流水线、配电终端安全风险检测平台，以及连通两者进行信息交互的综合管控系统。

其中，配电终端检测流水线包括装载机器人、卸载机器人、插拔线机器人、流水线体和检测工位等，用于将配电终端运入和运出，实现配电终端与安全风险检测平台的全自动接入和断开。

配电终端安全风险检测平台是一套相对独立的系统，在对平台自身安全性能检测的基础上，完成对配电终端国产密码的应用及验证检测，平台自身安全性能检测包括安全风险评估、安全设备检测、入侵检测、以及安全漏洞分析等，通过对平台自身以及配电终端从多个方面进行安全性检测，生成检测结果及检测报告进行反馈。

综合管控系统将配电终端流水线与安全风险检测平台进行连通，控制、操作配电终端检测流水线的进度，向配电终端安全风险检测平台发送包括厂家、版本、IP 地址等检测信息，以及发送启动、停止等检测控制信号；将检测结果、检测报告、检测原始数据、以及交互命令等信息在配电终端流水线与安全风险检测平台之间共享与交互，综合管理整个安全检测过程。

如图 2 所示，配电终端安全检测平台主要包括高性能配电加密认证装置、国密应用检测终端模块、安全风险评估设备、正反向安全隔离设备、配电安全接入网关、入侵检测服务器、漏洞扫描服务器、交换机、配电安全检测高性能服务器等。该平台具备自身安全性检测功能，能完成对自身的安全性能的检测；在此基础上，对被检测配电终端的密码安全性进行检测。

由图 2 可见，1、2 号交换机通过正、反向安全隔离分开，形成两个网络安全区，2、3 交换机通过配电安全接入网关隔离，形成第 3 网络安全区；两台高性能配电加密认证装置分别接在 1、2 号交换机上；两台安全风险评估设备分别接在 1、2 号交换机上；入侵检测服务器和漏洞扫描服务器连接到 3 号交换机上；国密应用检测终端模块通过被测安全网关接入 3 号交换机；国密应用检测服务端模块连接到 3 号交换机上；待测配电终端接入 3 号交换机；待测配电加密认证装置连接到 2 号交换机。

安全检测平台自身安全性能检测包括安全设备检测、入侵检测、漏洞扫描检测以及安全风险评估。

对本发明提供的安全检测平台进行的安全设备检测主要是针对平台中正、反向安全隔离设备、防火墙、安全接入网关、配电加密装置进行安全检测，通过应用双向身份认证、加密/解密、网络风暴测试、漏洞扫描、渗透攻击等技术手段测试平台的安全防护水平。

配电终端应对网络攻击和黑客入侵的能力直接影响配电终端信息采集系统的稳定性，本发明提供的配电终端安全检测平台配置入侵检测服务器（如图 2 所示），采用被动检测的方式对配电终端进行网络攻击和入侵检测，包括从配电终端信息采集系统网络中采集数据包，对 IEC 60807-5-104 报文进行深度解析，生成可供参考的网络交互信息列表，利用配电终端信息采集系统自身针对各类 SCADA/HMI（实时监控采集界面）以及 DCS/PLC（可编程逻辑控制器）等工业控制系统漏洞攻击规则对流量中存在的入侵行为进行检测、告警，同时基于 IP 地

址、上行流量、下行流量、总流量、会话数和应用类型等维度进行流量分析、展示，并对 SYN Flood（一种利用 TCP 协议缺陷，发送大量伪造的 TCP 连接请求，从而使得被攻击方资源耗尽（CPU 满负荷或内存不足）的攻击方式）、scan（扫描攻击）、arp spoof（IP 地址欺骗攻击）、Dos（拒绝服务攻击）流量等进行检测，从流量角度，比如当网络内短时间出现大量数据包，导致配电终端与配电终端信息采集系统正常交互异常时，发现网络中的异常。另外，网络中重要的服务器可以通过自学习和人工确认的方式从外联地址、端口和协议等维度建立连接白名单，以防止黑客的恶意入侵行为。

针对本发明配电终端安全检测平台进行的网络端口及安全漏洞扫描检测包括开放式扫描、隐蔽式扫描、半开放式扫描三种。

其中，在开放式扫描过程中，对于产生的大量的审计数据，使用 TCP 反向 Ident 扫描技术进行测试，若被测试系统用户使用 TCP 服务器进行连接，即可发现用户的用户名。该扫描方式可靠性高。

隐蔽式扫描技术主要包括 TCP-FIN 扫描，TCP-FTP 返回式扫描和分段扫描等，能够发现并检测出被测系统被入侵，有效避免漏洞入侵计算机的检测系统和防火墙。

半开放式扫描技术包括 TCP 间接扫描方式和 TCP SYN 扫描方式，测试时也可以发现并检测出被测系统是否被入侵。

本发明综合应用上述三种扫描方式，按照图 5 所示安全漏洞扫描流程图，进行发现漏洞、复现漏洞、模拟漏洞攻击、评估及验证影响，进而提出解决方案、对解决方案进行验收、最终实施方案，由此评估配电终端安全检测平台自身策略的防护能力及存在的漏洞及影响。

在对配电终端安全检测平台进行安全设备检测、入侵检测、漏洞扫描检测的基础上，进行安全风险评估。如图 4 所示，安全风险评估设备从信息资产、威胁、脆弱性三个方面对进行评估，计算威胁出现的频率、评估脆弱性的严重程度以及信息资产的重要程度，采用相应的风险计算方法确定由于威胁或利用脆弱性导致安全事件发生的可能性、综合安全事件所作用的资产价值及脆弱性的严重程度判断安全事件造成的损失，从而完成安全检测平台的安全风险评估。

目前，常用的风险评估算法是矩阵法和相乘法。

1) 矩阵安全风险评估

矩阵法主要适用于由两个要素值 x，y 确定一个要素值 z 的情形，在风险值计算中，由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值可以应用矩阵法。首先需要确定二维计算矩阵，矩阵内各个要素的值根据具体情况和函数递增情况采用

数学方法确定，然后将两个元素的值在矩阵中进行比对，行列交叉处即为所确定的计算结果。

即 $z = f(x,y)$，函数 f 可以采用矩阵法。

矩阵法的原理是：

$x = \{x_1, x_2, \cdots, x_i, \cdots, x_m\}, 1 \le i \le m$，$x_i$ 为正整数，

$y = \{y_1, y_2, \cdots, y_j, \cdots, y_n\}, 1 \le y \le n$，$y_j$ 为正整数，

以要素 x，比如对系统的威胁和要素 y，比如系统脆弱性的取值构建一个二维矩阵，如表 A.1 所示。矩阵行值为要素 y 的所有取值，矩阵列值为要素 x 的所有取值。矩阵内 $m \times n$ 个值即为要素 z 的取值，$z = \{z_{11}, z_{12}, \cdots, z_{ij}, \cdots, z_{mn}\}, 1 \le i \le m, 1 \le j \le n$，$z_{ij}$ 为正整数。

表 1 矩阵构造

	y	y_1	y_2	…	y_j	…	y_n
x	x_1	z_{11}	z_{12}	…	z_{1j}	…	z_{1n}
	x_2	z_{21}	z_{22}	…	z_{2j}	…	z_{2n}
	…	…	…	…	…	…	…
	x_i	z_{i1}	z_{i2}	…	z_{ij}	…	z_{in}
	…	…	…	…	…	…	…
	x_m	z_{m1}	z_{m2}	…	z_{mj}	…	z_{mn}

对于 z_{ij} 的计算，可以采取以下计算公式，

$z_{ij} = x_i + y_j$，

或 $z_{ij} = x_i \times y_j$，

或 $z_{ij} = \alpha \times x_i + \beta \times y_j$，其中 α 和 β 为正常数。

z_{ij} 的计算需要根据实际情况确定，矩阵内 z_{ij} 值的计算不一定遵循统一的计算公式，但必须具有统一的增减趋势，即如果 f 是递增函数，z_{ij} 值应随着 x_i 与 y_j 的值递增，反之亦然。

矩阵法的特点在于通过构造两两要素计算矩阵，可以清晰罗列要素的变化趋势，具备良好灵活性。

在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，例如由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值等，同时需要整体掌握风险值的确定，因此矩阵法在风险分析中得到广泛采用。

2) 相乘法安全风险评估

相乘法主要用于两个或多个要素值 x，y 确定一个要素值 z 的情形,即 $z=f(x,y)$，在风险值计算中，由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值可以应用，函数 f 可以采用相乘法。

相乘法的原理是：

$z=f(x,y)=x\otimes y$ 。

当 f 为增量函数时，$\otimes$ 可以为直接相乘，也可以为相乘后取模等，例如：

$z=f(x,y)=x\times y$,

或 $z=f(x,y)=\sqrt{x\times y}$,

或 $z=f(x,y)=\left[\sqrt{x\times y}\right]$,

或 $z=f(x,y)=\left[\dfrac{\sqrt{x\times y}}{x+y}\right]$ 等。

相乘法提供一种定量的计算方法，直接使用两个要素值进行相乘得到另一个要素的值。相乘法的特点是简单明确，直接按照统一公式计算，即可得到所需结果。

在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，例如由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值，因此相乘法在风险分析中得到广泛采用。

在完成了信息资产、威胁、脆弱性评估后，以及已有安全措施评估后，采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。风险分析的主要内容为：

1) 对信息资产进行评估，并对资产的价值进行赋值；

2) 对威胁进行评估，描述威胁的属性，并对威胁出现的频率赋值；

3) 对脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值；

4) 根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性；

5) 根据脆弱性的严重程度及安全事件所作用的资产的价值计算安全事件造成的损失；

6) 根据安全事件发生的可能性以及安全事件出现后的损失，计算安全事件一旦发生对组织的影响，即风险值。

按照信息安全风险计算原理，以下面的范式形式化加以说明：

风险值=R（A，T，V）= R(L(T，V)，F(Ia，Va))。

其中，R 表示安全风险计算函数；A 表示资产；T 表示威胁；V 表示脆弱性； Ia 表示安全事件所作用的资产价值；Va 表示脆弱性严重程度；L 表示威胁利用资产的脆弱性导致安全事件的可能性；F 表示安全事件发生后造成的损失。具体包括以下三个关键计算环节：

1) 计算安全事件发生的可能性

根据威胁出现频率及脆弱性的状况，计算威胁利用脆弱性导致安全事件发生的可能性，即：

安全事件的可能性=L(威胁出现频率，脆弱性)＝L(T，V)。

在具体评估中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识公开程度等）、资产吸引力等因素来判断安全事件发生的可能性。

2) 计算安全事件发生后造成的损失

根据资产价值及脆弱性严重程度，计算安全事件一旦发生后造成的损失，即：

安全事件造成的损失=F(资产价值，脆弱性严重程度)＝F(Ia，Va)。

部分安全事件的发生造成的损失不仅仅是针对该资产本身，还可能影响业务的连续性；不同安全事件的发生对组织的影响也是不一样的。在计算某个安全事件的损失时，应将对组织的影响也考虑在内。

部分安全事件造成的损失的判断还应参照安全事件发生可能性的结果，对发生可能性极小的安全事件，如处于非地震带的地震威胁、在采取完备供电措施状况下的电力故障威胁等，可以不计算其损失。

3) 计算风险值

根据计算出的安全事件的可能性以及安全事件造成的损失，计算风险值，即：

风险值=R(安全事件的可能性，安全事件造成的损失)＝R(L(T，V)，F(Ia，Va))。

评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。矩阵法通过构造一个二维矩阵，形成安全事件的可能性与安全事件造成的损失之间的二维关系；相乘法通过构造经验函数，将安全事件的可能性与安全事件造成的损失进行运算得到风险值。

返回图 2，利用安全检测平台对对配电终端进行检测时，首先将被检测配电终端接入本平台，设置被测配电终端的地址信息，平台针对配电终端进行国产密码应用检测。

国产密码的应用是保证配电自动化业务安全的核心支撑和重要保障措施，对国产密码的应用进行检测是安全检测的重要环节。如图 3 所示，配电终端安全风险检测平台对配电终端进行国产密码应用的检测是基于图 2 所示的配电自动化国产密码检测平台进行的，该配电自动化国产密码检测平台由配电终端设备安全检测 1、配电终端采集平台安全检测 2、配电加密认证装置检测 3、以及配电安全接入网关检测 4 四部分组成。具体地，配电自动化国产密码检测平台基于前述安全检测平台，主要包括 2 台两台配电安全检测高性能服务器、正向及反向物理安全隔离设备、3 台网络交换机（交换机 1、2、3 号）、高性能配电加密认证装置、配电安全接入网关、以及国密应用检测终端模块、国密应用检测服务端模块、加密装置接口服务程序、入侵检测服务器以及安全风险评估设备。

配电终端接入设备安全检测还包括信息安全通用功能检验和专用规约安全功能检验两部分，配电终端通过网络安全网关对通信报文进行加密后传到安全风险评估设备，安全风险评估设备通过高性能配电加密认证装置进行报文的解密和解析，验收配电终端上送报文加密的正确性，同时验收规约上送信息的准确性。

信息安全通用功能检验通过正向通信符合性检验和反向异常通信报文检验两个子模块实现。正向通信符合性检验可以实现主站、网关、现场运维工具与终端认证的功能检验，远程密钥更新、远程证书管理功能检验，现场密钥更新、导出公钥功能检验，导入证书功能检验，现场获取终端密钥版本的功能检验。正向通信符合性检验由用国产高性能加密认证装置和正向通信符合性检验功能模块组成，通过两者之间的密钥/公钥的管理交互，实现与配电终端通信过程相关功能的验证。反向异常通信报文检验可以通过签名错误、不要签名、校验和错误、未通过安全认证的越权访问、更新终端签名错误、不带签名检验，更新证书不带签名、签名错误检验，MAC 错误检验等多种方法，检测设备是否严格的遵守了国产密码应用的相关规定。反向异常通信报文检验由国产高性能加密认证装置和反向异常通信报文检验功能模块组成，通过两者的信息交互，模拟配电终端通信的各种异常情况，实现配电终端对异常通信过程符合性的验收。

专用规约安全功能检验也是通过正向通信符合性检验和反向异常通信报文检验两个子模块来实现。正向通信符合性检验包括：遥控功能检验、远程参数更新功能检验、远程程序升级功能检验、总召唤功能检验、执行时间检验。正向通信符合性检验由用国产高性能加密认证装置和正向通信符合性检验功能模块组成，正向通信符合性检验功能模块通过国科高性能

加密认证装置进行通信报文加密，然后与配电终端进行通讯，验证配电终端通信过程正常功能的符合性。反向异常通信报文检验包括：重放报文检验、错误报文检验、不带签名的报文检验、不带时间的报文检验、不带随机数的遥控执行报文检验、明文报文检验。反向异常通信报文检验由国产高性能加密认证装置和反向异常通信报文检验功能模块组成，反向异常通信报文检验模块通过国科高性能加密认证装置进行通信报文加密，模拟配电终端通信的各种异常情况，实现配电终端对异常通信过程符合性的验收。

通过这些检测可以检测配电终端设备是否在通信过程中严格的遵守了国产密码应用的相关规定。

综合管控系统采用 TCP/IP 方式，分别与配电终端检测流水线和配电终端安全检测平台进行互连，实现整个检测过程的统一管控。

本发明还提供一种基于流水线自动运转的配电终端安全检测方法，包括：

搭建配电终端全自动流水线，包括装载机器人、卸载机器人、插拔线机器人、流水线体和检测工位，配电终端通过该全自动流水线实现自动上线、下线。具体地，当对配电终端进行安全检测时，装载机器人将被测配电终端自动运送到检修工位；插拔线机器人对待检测配电终端进行插拔线操作，使其接入安全检测平台；所述卸载机器人根据检测结果对被测终端进行区分，按照合格与否进行分类筛检，不合格设备卸载到不合格产品区。

搭建配电终端安全检测平台，包括配电加密认证装置、安全风险评估设备、入侵检测设备、安全设备检测装置及漏扫设备等多种设备，共同实现对配网终端多方面的安全检测。该配电终端安全检测平台是一套相对独立的系统，可实现完善的系统国产密码应用及验证技术、安全设备检测技术、入侵检测技术、终端设备信息传输安全监测技术、网络端口扫描技术、三区 web 安全漏洞分析等。

搭建综合管控系统，分别与全自动流水线和安全检测平台进行接口交互。综合管控系统可在装载机器人将待检测配电终端送到检测工位后，传送信号给安全检测平台；安全检测平台检测结束后，将检测结果返回到综合管控系统，并发送指令给检测流水线，卸载机器人根据指令进行下一步操作。

上述虽然结合附图对本发明的具体实施方式进行了描述，但并非对本发明保护范围的限制，所属领域技术人员应该明白，在本发明的技术方案的基础上，本领域技术人员不需要付出创造性劳动即可做出的各种修改或变形仍在本发明的保护范围以内。

说　明　书　附　图

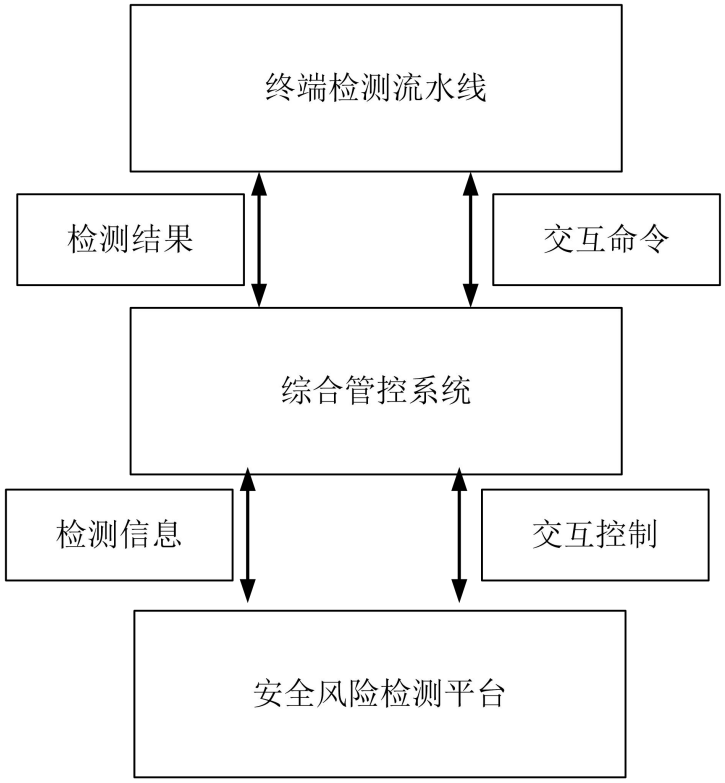


图 1

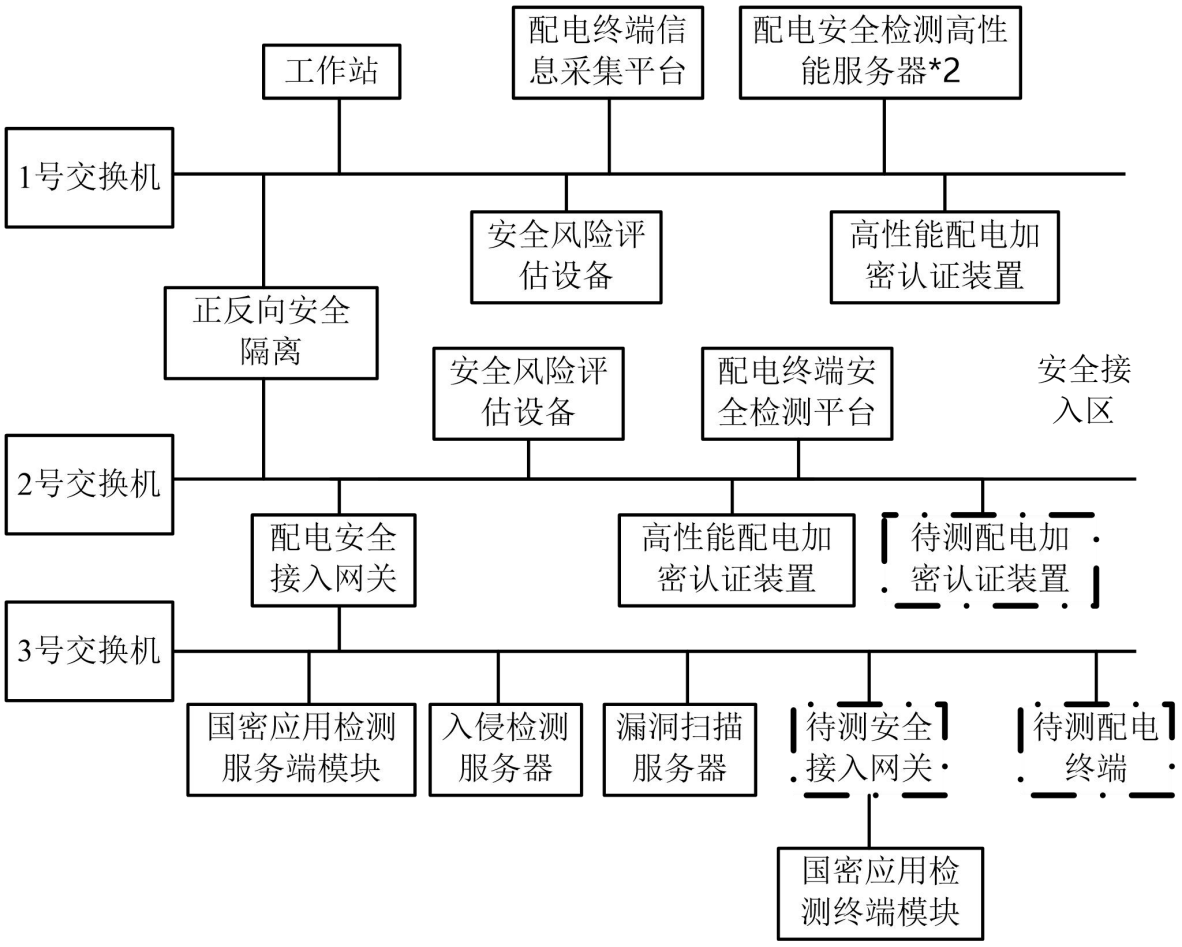

工作站
配电终端信息采集平台
配电安全检测高性能服务器*2
1号交换机
安全风险评估设备
高性能配电加密认证装置
正反向安全隔离
安全风险评估设备
配电终端安全检测平台
安全接入区
2号交换机
配电安全接入网关
高性能配电加密认证装置
待测配电加密认证装置
3号交换机
国密应用检测服务端模块
入侵检测服务器
漏洞扫描服务器
待测安全接入网关
待测配电终端
国密应用检测终端模块

图 2

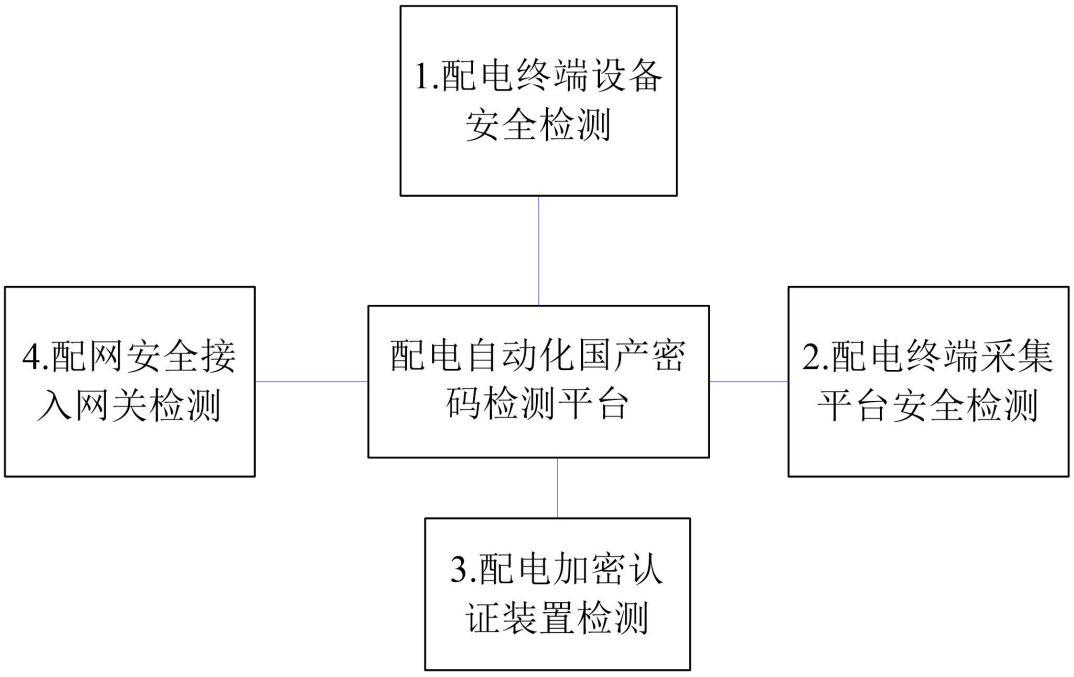

1.配电终端设备安全检测
4.配网安全接入网关检测
配电自动化国产密码检测平台
2.配电终端采集平台安全检测
3.配电加密认证装置检测

图 3

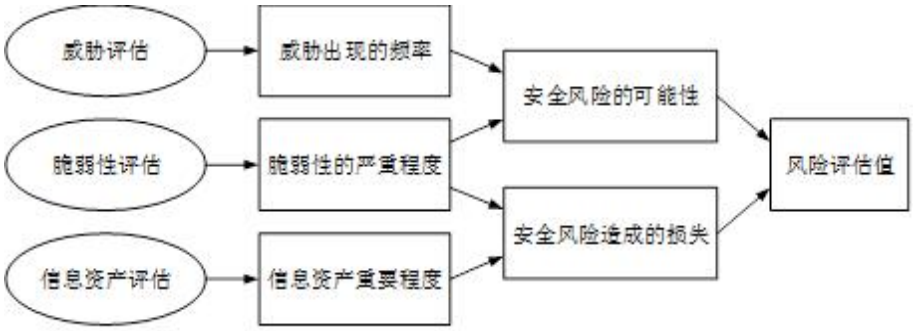

威胁评估
威胁出现的频率
脆弱性评估
脆弱性的严重程度
信息资产评估
信息资产重要程度
安全风险的可能性
安全风险造成的损失
风险评估值

图 4

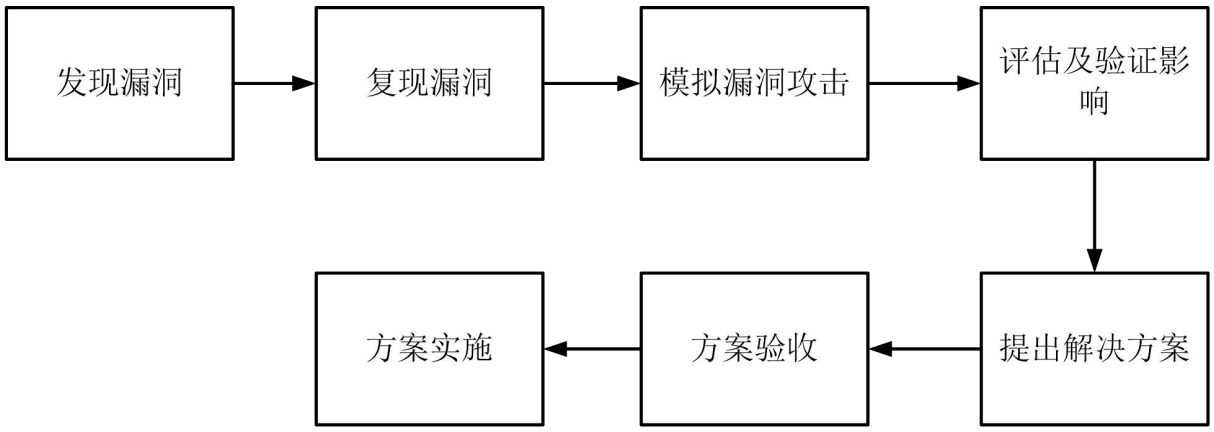

发现漏洞
复现漏洞
模拟漏洞攻击
评估及验证影响
提出解决方案
方案验收
方案实施

图 5