

基于 RPA 技术的电力系统主机加固

董贤 陈钊 张龙浩 高泽勇

(南方电网储能股份有限公司西部检修试验分公司, 贵州黔西南州兴义市 562400)

摘要: 电力系统中主机加固操作十分广泛, 但该工作依赖于人工操作且存在 Windows 和 Linux 操作系统两个版本, 电力系统中的主机加固工作涵盖范围广泛, 包括安全策略检查、补丁安装和系统恢复等关键操作。然而, 由于此类工作依赖于人工操作, 且涉及到 Windows 和 Linux 操作系统两个版本的主机环境, 工作难度相对较高, 专业性要求高, 且重复性操作较多, 导致人工误操作频发。本文提出一种将 RPA 机器人技术与电力系统主机加固工作相结合的解决方案, 以提高工作效率和安全性。

关键词: RPA; 主机加固; 电力系统

一、概述

目前国内外网络安全形势日益严重, 黑客、病毒以及恶意代码等各种形式的恶意攻击日益增多。能源、电力、通信、交通等领域的关键信息基础设施是网络安全的重中之重, 物理隔离防线可被跨网入侵, 电力调配指令可被恶意篡改, 这些都是重中之重。高普及率和市场占有率的 Windows 系统存在黑客攻击等诸多安全问题。近几年, 电力系统为了避免该类问题, 在各类改造中将 Windows 系统更换为 Linux 系统, 但电力系统内部依然存在大量 windows 系统。为确保电力系统网络安全, 主机加固成为了必要。目前该块任务一直依赖于人工加固, 涉及不同版本 Windows 和 Linux 系统, 相关重复性操作多, 且主机拥有者可能无法自己实现加固导致业务人员工作量大, 维护成本变高。

为了解决上述问题, 本文提出一种基于 RPA 机器人的电力系统主机加固方法。通过 RPA 机器人模拟软件加固业务人员快速实现当前计算机主机加固, 同时根据完成项目实现相关登记表作为反馈, 从而实现更高效、快捷、精准的操作。

二、机器人流程自动化 (RPA)

(一) RPA 现状

RPA, 即机器人流程自动化 (Robotic Process Automation), 是一种基于软件的自动化技术, 旨在模拟用户在操作系统中的交互行为, 自动执行基于规则、重复的业务流程。

RPA 在全球范围内拥有广泛的应用场景, 尤其是在金融、保险、零售、医疗等多个领域。它可以帮助企业在面对复杂且重复性高的工作时, 实现流程自动化, 从而提高生产力和降低成本。同样地, 电力系统在全面实行数字化转型, RPA 技术也逐步渗透于在电力行业中的相关项目中, 不仅极大地缓解了电力系统内部工作压力并提高效率, 而且减少了人为误操作带来的后果。

(二) RPA 工作机理

RPA 是一种可以模拟人工操作的脚本开发工具, 通过模仿用户的按键和点击动作实现操作流程的自动化。传统的自动化技术是由编程人员编写专用的脚本语言, 借助系统间的接口完成自动化交互工作。而 RPA 机器人流程自动化是通过直接用户图形界面 (GUI) 自动化技术来模仿用户操作, 通过屏幕抓取技术来识别和解析屏幕视觉信息, 然后根据这些信息执行预定的自动化脚本。

RPA 能够处理错误和异常情况, 例如通过重试机制、警报通知或将任务转交给人工干预; 可以利用后台监控工具跟踪机器人的活动、性能和状态。所有操作都会被记录在日志中, 以便于审计和故障排除; 可以集成人工智能 (AI) 和机器学习 (ML) 技术, 以提高决策能力、预测分析和处理更复杂的任务。RPA 软件通常设计为跨多个系统和平台运行, 包括不同的操作系统、应用程序

和数据库。RPA 解决方案可以轻松扩展, 以适应不断变化的业务需求。通过添加更多的机器人或调整现有的自动化流程, 可以快速响应业务变化。

三、RPA 技术应用于电力系统中的应用优势

(一) 提高电力系统运维效率

RPA 技术具有自动收集、整合、分析电力系统运行产生的如电压、电流、温度等海量监测数据, 以及常规的故障报修记录和维修台账等数据, 这些数据是评估系统运行状态, 预测潜在故障与优化系统运维策略的重要依据。通过将 RPA 技术应用于电力系统, 能够帮助工作人员更加快速、准确地获取到设备和系统的状态信息, 从而及时发现潜在故障并进行相应维修措施, 以提高设备和系统的可靠性和稳定性。同时, RPA 技术还可以模拟工作人员在计算机上的机械性运维操作, 比如自动巡检、巡检报告生成和潜在故障报修等。这不仅能够实现 24 小时不间断开展运维工作, 还能够自动完成一些机械性运维工作。

(二) 减少工作中人为错误

RPA 技术能够按照预设好的程序和标准, 自动执行相应的操作, 比如数据录入、信息核对、文件处理等。这些都是电力系统操作中重复性高且容易出现错误的。借助 RPA 自动执行可以避免传统人工操作中因注意力长时间集中而出现的一些疏漏。另外, 电力系统涉及大量数据整合和校验工作, 且十分烦琐, 人工完成这些工作不仅容易出现错误, 还浪费时间。运用 RPA 技术可以快速完成数据自动录入、整合和校验, 从而提高数据处理的效率和质量。此外, 在电力系统中, 许多操作需要遵守严格的法规和标准, RPA 技术能够实现自动化流程处理, 保障操作的合规性。

(三) 促进多部门数据共享

传统的电力系统工作由于业务的复杂性等诸多因素, 不同部门所使用的信息系统不尽相同, 形成了一个“信息孤岛”。RPA 技术应用能够帮助工作人员更加高效地完成一些跨平台、跨系统的工作任务, 促进多部门数据共享。与此同时, RPA 技术还能够按照设定好的流程和要求, 对不同部门的数据进行标准化处理, 从而消除因数据格式不一致而出现的数据共享障碍。在此过程中, 通过预先设定 RPA 也能自动对相应数据进行审查, 确保数据是能够共享的, 避免出现数据滥用或泄露的情况。在具体操作中, 需要对数据使用进行身份认证和访问权限控制, 确保只有授权工作人员才能完成跨部门数据使用。

四、基于 RPA 技术的电力系统主机加固

(一) 业务背景

目前国内外网络安全形势日益严重, 黑客、病毒以及恶意代码等各种形式的恶意攻击日益增多。2011 年, 美国利用“震网”

蠕虫病毒攻击伊朗的铀浓缩设备,已经造成伊朗核电站推迟发电,1/5的离心机报废,造成巨大国际影响;2015年12月23日,黑客对乌克兰境内三处变电站SCADA系统发起网络攻击,导致伊万诺—弗兰科夫地区发生大面积停电事件,140万人受到影响,整个停电事件持续6个小时之久,这是全世界第一次由于黑客攻击造成电网大规模停电的事件。

电力系统主机的安全加固对于电力系统网络安全至关重要。

(二)业务痛点

电力系统中现存的Windows系统,依旧可能是黑客攻击的目标并且存在诸多安全问题(除了系统漏洞MS17-010传播WannaCry蠕虫外,Windows系统本身还存在缓冲区溢出、IIS解析、IE浏览器、不受保护的Windows网络共享、office病毒等)也层出不穷。为确保电力系统安全稳定运行,主机系统安全加固成为了必要。

目前电力系统中涉及保信、行波测距等主站端系统及厂站端的保信子站、故障录波器继电保护专业,以及监控系统中各类通讯机、监控主机、历史服务器等运行涉及的系统和装置。但诸多设备和系统的软件加固一直依赖于人工操作;同时系统和设备涉及Windows和Linux操作系统,工作难度较高、工作较为复杂,专业性强;软件加固过程中相关重复性操作多、人工误操作难以避免;设备拥有者或系统维护人员可能无法自己实现加固导致业务人员加固工作量大,维护和培训成本变高。

(三)解决方案

本文提出了一种基于RPA机器人的基本功能模块、语句、识别和程序调用的功能与电力系统主机加固工作相结合,其目的在于解决人工加固电力系统主机存在的操作重复率高、操作效率低、各专业难度较大、业务工作量较大等问题,实现主机或系统用户高效快捷完成自动加固功能,专业加固人员实现操作和工作量减负以及系统安全、稳定、精确加固的目标。

通过前期研究可发现,针对Windows系统,主机加固主要是通过身份鉴别(密码策略设置符合复杂度要求、启用登录失败处理、应用软件账户权限设置等)、访问控制(禁用不必要服务、关闭Windows自动播放功能、禁止可远程访问的注册表路径和子路径、禁止匿名远程连接等)、资源控制(配置登录终端的操作超时锁定等)以及关闭高危端口等Windows系统操作功能。针对Linux系统,主机加固主要是针对账号识别(弱口令、无用账号检查、添加口令策略、Grub/lilo密码等)、服务限制(关闭不必要服务、检查SSH服务、检查TCP Wrapper等)、网络参数、文件系统管理(设置umask值、Bash历史命令)、日志检查(syslogd日志等)等Linux系统操作功能。



图1 主机加固流程图

如图1主机加固流程图所示,Windows与Linux属于不同操作

系统,操作界面即用户图形界面(GUI)不同,需要针对两种不同的操作系统分别配置不同的程序。然后,通过用户图形界面自动化技术来模仿主机加固人员鼠标动作,点击windows和linux系统相应软件或通过终端指令调出软件相应元素的方式,自动实现主机加固过程。同时,通过在子程序中增加表单填写功能,可实现完成一个子程序后自动调用表单并且在对应表单表格中填写完成情况,达到详细记录流程完成情况与加固情况的功能,最终反馈给用户侧。

(四)应用成效

目前,业务人员以人工操作为主实现电力系统主机加固,需要手动切换各种软件和操作窗口。完成一次主机加固操作需执行百余次界面操作约2h,同时还需要5min完成手动登记主机安全加固作业表单,总计约125min。人工操作效率低并且误操作概率较大。

专业加固业务人员或非专业业务人员执行本方案后,可自动实现主机加固功能,并且在完成一个子程序后可以快速填写表单,整个加固过程仅需要10min。也就意味着,同一个人连续执行主机加固,在同样的2h可完成至少12台,效率至少提高了1200%。由于程序执行可同时应用于多台主机系统,如此计算提升效率更是成倍上升。与此同时在专业人员配置上得到高效优化,在执行难度更是显著下降。

五、结语

在当前的电力系统管理中,我们通过引入RPA技术与主机加固系统相结合,取得了显著成效。“在电力系统中,我们创新性地地将RPA机器人技术与电力系统主机加固工作相结合,形成了自动化主机加固流程,加固效率在2h内对比人工提升了近12倍。因此,本方案极大提高加固效率,降低了时间成本与人员培训成本,减少了人工操作可能带来的误差,有助于延长系统稳定性”

展望未来,我们将继续探索将RPA技术与更先进的大语言模型相结合的可能性,在以下几个方面实现突破:首先,可以在预设的空白表中快速生成符合要求的加固表单,这不仅节省了大量的重复性工作,而且提高了数据处理的准确性;其次,利用人工智能生成详尽、可靠的图表及报告,并且对错误分析结果进行总结,实现主机加固过程的智能化和可视化。此外,这种创新组合预计能显著减少代码编写的数量,同时增强程序的可靠性和稳定性,为电力系统的智能化升级开辟新的道路。综上所述,RPA与主机加固技术的结合,无疑为电力系统管理领域带来了革命性的变革。随着技术的不断进步,我们有理由相信,这项创新将继续推动电力系统向着更加安全、高效、可靠的方向发展。

参考文献:

- [1] 陈美菱,常青云.基于RPA技术的电力业务系统自动化处理策略[J].电子元器件与信息技术,2022(10):109-112.
- [2] 陈薇,黄令忠.基于RPA技术的电力营销稽查全过程监控系统设计[J].电子技术(上海),2022(005):051.
- [3] 汤建华,严锋,刘飞,等.基于RPA技术进行电力系统数据智能化爬取与分析的系统:CN202011266827.9[P].CN112215727A[2024-11-04].
- [4] 孙春艳,徐康.基于RPA技术的电网数字化流程跟踪控制系统[J].微型电脑应用,2024,40(1):103-105.
- [5] 万雪枫.RPA技术在电力业扩报装流程管理中的应用[J].集成电路应用,2023(11):320-321.