Power System Technology
ISSN:1000-3673

Received: 16-04-2025 *Revised: 05-05-2025* *Accepted: 22-07-2025*

Integrating Robotic Process Automation into Power System Control: A Framework for Adaptive Change Management and Operational Resilience

Sandeep Singh
sandeep.sign@gmail.com
Georgia Tech
https://orcid.org/0009-0002-6249-2541

Mohammad Mushfiqul Haque Mukit

mmukit.ny@gmail.com

Washington University of Science and Technology & Jahangirnagar University

https://orcid.org/0000-0002-7956-484X

Van-Huy Chu
huycv@hvnh.edu.vn
Faculty of Information Technology and Digital Economics, Banking Academy of Vietnam

0000-0003-4832-9801

Abstract

Increasingly complex modern power systems and the quest toward intelligent grid control have fueled the implementation of Robotic Process Automation (RPA) in control centres and protection systems using SCADA. The technical advantages of automation are well known; however, its organisational aspects within high-reliability environments have not been discussed. This work will discuss an Adaptive Change Management Framework to implement RPA in the power system protection and control process, which integrates real-time automation and scheduled change integration. Mixed methods are used, where technical validation of the Smart Grid Monitoring Dataset is combined with the organisational impact survey, which is simulated. The findings have indicated that by implementing RPA, there is a dominant and encouraging change in the performance metrics of the system, such as detection percentage (96.7%), false positives (reduced to 1.8%), and average response time (0.45 seconds). At the same time, the completion rate of the training was increased to 94% in just four weeks, and confidence in the automation was enhanced by 42%, thanks to the support of direct communication channels and feedback loops. The framework will be organised into three levels: an RPA Core Engine, a Change Management Layer focusing on training and trust measures, and a Governance and Safety Layer encompassing cybersecurity, approval processes, and compliance. Such architecture guarantees technical reliability and creates

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

operational penetration. Findings The findings provide power utilities a scale-based risk-considerate avenue of integrating automations into their mission-critical facilities. The paper closes the gap between the theoretical analysis of the digital transformation and applied engineering practice, the literature on smart grid automation, and the practical approaches to work.

Keywords: *Robotic Process Automation (RPA), Power System Protection, SCADA Integration, Change Management, Smart Grid Automation, Organisational Resilience, Fault Detection, Adaptive Framework, Operational Technology (OT), Grid Reliability.*

1 Introduction

Digitalisation, decentralisation, and integration of intelligent automation technologies are becoming a powerful driving force in the modern power system landscape. Robotic Process Automation (RPA) has recently become one of the key cogs in boosting the operational process of crucial energy infrastructure [1]. Best known as a back-office automation tool in industries like finance or healthcare. RPA is currently deployed in power grid control centres, substations, and SCADA (Supervisory Control and Data Acquisition) systems. This change is representative of the realisation and potential of RPA to enhance efficiency, accuracy, and responsiveness in real-time control conditions [2]. Examples are automation of data extraction, alarms, protection settings, and fault reports, so that human operators are left to tackle high-level strategic objectives instead of performing routine monitoring operations [3].

With the power systems becoming even more complex, including increased loads, integration of distributed renewable energy resources, and the need to perform real-time balancing, the scalable and intelligent automation solutions are highly required [4]. Static, manual procedures can be too slow or erroneous enough to be unable to handle the requirements of contemporary protection and control systems, in particular, during fault conditions or emergencies [5]. With adequate deployment, RPA will help fill these gaps in two ways: it promises low-latency, rule-based task performance and can be readily embedded within SCADA and grid management software.

Regardless of the technological maturity and readiness of RPA platforms, the deployment of such technology usually has significant organisational challenges in the utilities and grid operators [6]. The major ones include the resistance of operational staff, fear of loss of jobs, technical knowledge deficit, and doubt on the reliability of automated processes on mission-critical applications. Such issues are heightened in areas such as the protective system of power, where matters of safety, reliability, and compliance with regulations are uncompromising [7]. Besides, systematic frameworks do not address the technical, human, and procedural elements of RPA implementation in the energy sector. A significant number of RPA programs fail to scale

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

solely or lack considerable use due to the failure to implement a comprehensive change management strategy that would separate their value proposition [8].

This paper proposes and verifies through empirical tests an Adaptive RPA Change Management Framework custom-made for power system protection and control. By reducing the divide likely to be created between automation and human-focused transformation, the framework provides a way of thinking about a balance between technological innovation and employee interaction, education, and control. Contrary to generic change management models, this framework is based on domain-specific knowledge and considers the specifics of grid control activities and the interactions between human operators and automation bots.

The study employs the mixed-method paradigm due to the combination of organisational change analysis with empirical evidence of performance analysis based on the available Smart Grid Monitoring Dataset presented by Kaggle. By doing this, we can determine the technical effectiveness of RPA in detecting anomalies and responding to alarms. On the organisational front, we can evaluate the organisational effectiveness of RPA in improving resistance and training results.

This paper is arranged in the following way: In Section 2, the literature review regarding the usage of RPA in power systems and current change management strategies is given in detail. Section 3 presents the research methodology, where the dataset, simulation setup, and organisational data have been discussed. Section 4 offers an architecture of the framework and its parts. Section 5 describes the results and cross-analysis of the experiment. Implications, limitations, and possible scalability of the results are explained in Section 6. To conclude, Section 7 provides suggestions regarding future studies and steps to take to implement them.

2 Related Work

2.1 Robotic Process Automation in Power Systems

Robotic Process Automation (RPA) is an automation technology that has historically been used in back-office functions and managing business processes [9]. Its capabilities, however, are increasingly being extended to the domain of critical infrastructure systems, which can include power system control environments. In these spheres, various low-level repetitive functions like routine data verification, alarm correlation and analysis, protection relay events logging, and automatic reporting are performed with the help of RPA [10]These operations are required to achieve the reliability and real-time response of modern grid systems and may be too voluminous or repetitive to carry out regularly and in a timely fashion without the assistance of computers.

The RPA is being injected into Intelligent Electronic Devices (IEDs) and SCADA systems in substation automation to allow them to perform tasks like periodic relay test data synthesis,

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

circuit breaker diagnostics, and the production of health reports [11]. Grid operators are also getting interested in the bots that can automatically carry out repetitive tasks, such as the relay protection settings update or the triggered pre-determined steps, depending on the grid contingencies [12]. In SCADE scenarios, the RPA scripts are deployed to auto-fill logbooks, scan vital incident markers in operational databases, or even initiate standard operating procedures in predictive fault trends.

An overview of available RPA tools demonstrates that a few could be applied to power systems. One of the most commercially available RPA tools, UiPath, integrates with databases, APIs, and desktop solutions, which makes it an appropriate choice among utilities that use hybrid systems [13]. Other RPA tools based on Python (TagUI, PyAutoGUI, Robocorp) are more programmable and thus favoured in research and technical contexts where engineers need low-level access to the inner structures of software. Albeit having a traditional reputation of dealing with business tasks, Microsoft Power Automate has become relevant to energy operations because it is capable of interacting with cloud-based telemetry and maintenance systems [14]Nonetheless, unlike in the IT domain, such tools need to be adjusted to suit the strong reliability and cybersecurity demands of the operational technology (OT) sectors.

Although RPA has great potential in power systems, it is technologically unrealised and organizationally vulnerable, particularly with protection and control applications [15]. Most existing research deals with RPA benefits in a general way and does not examine their applicability to real-time grid stability, protection scheme coordination, or compatibility with the available OT protocols.

2.2 Organisational Change and Automation

Organisational change as an enabling factor that has to be incorporated with technological integration is one of the most overlooked and most important facets of RPA implementation in power systems. RPA is supposed to deliver better process efficiency and cost-effectiveness; however, its adoption is sometimes accompanied by cultural barriers, most notably when it comes to the highly skilled technical employees who might perceive automation as a threat to their jobs [16]. Engineers and technicians in grid activities and protection control rooms are well versed with conventional processes and methods. Due to this, the introduction of software bots can be regarded not only as a technical intervention but more as a violation of the established norms of operation and professional identities [17].

Some of the significant issues are role redefinition, where focus is shifted to system inspection as opposed to performing the actual tasks, and placing confidence in automation [18]. Especially where automation or bots are left in charge of fault identification or alarm escalation processes, and ensuring safety, because the errors in automatic methods of control may have ripple effects on other areas of the power grid [19]. All these questions highlight the need for a

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

well-organised and controlled change process that involves both technological and human aspects.

The models of organising the transition, like Kotter's 8-Step Model or Prosci's ADKAR (Awareness, Desire, Knowledge, Ability, Reinforcement), provide useful tips on how to make it in the process [20]. Kotter focuses on developing the sense of urgency, forming a leadership team, and laying the foundation for change in the corporate culture. ADKAR has a humanistic way of making sure that every individual moves to the other side with ease [21]. Although such models have been effective in business and IT applications, such approaches have been less utilized in mission-critical applications that include engineering-intensive applications such as power systems.

In addition, these standard models do not have any integration with technical performance measures, and thereby, it is not easy to measure the relationship between change adoption and system reliability. In the field of protection and control, change cannot be measured only by user satisfaction or employee attitudes; other factors that should be taken into account are the behaviour of a system in extreme conditions, response time of faults, and accuracy of alarms. [22]. This discrepancy has led to the development of a research gap, that is, a gap in change management research that is people-centred and performance-sensitive in RPA within a power system context.

2.3 Smart Grid Dataset Applications in Protection Analysis

Measurement data of smart grid observed behaviour is exceedingly valuable in validating automation and protection models, such as the voltage fluctuations, frequency variations, and current imbalances. Time-series datasets have served as the basis of many studies that think of fault detection models, foresee their loads as well, and classify power quality events in the last decade [23]. Such data frequently comes as phasor measurement units (PMUs), remote terminal units (RTUs), or smart meters, and is fed into training machine learning or signal processing techniques.

As an example, fault classification research based on Support Vector Machines (SVMs), Random Forest, or neural networks is very accurate in identifying the type of faults (either single-line-to-ground faults or symmetrical faults) [24]. On the same note, anomaly detection is used to identify patterns of transformer failure or grid instability at an earlier stage.

The literature, however, is interested in purely technical validation, accuracy, precision, and recall, without questioning how this level of automation is accepted by the human operators or what impact it has on their workflows [25]. Moreover, although such studies resemble real-time analysis, there is a rare occurrence of post-deployment data, interaction logs of operators, or organization measurement impacts.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

This research stands out and utilises the Smart Grid Monitoring Dataset, not only to perform technical RPA validation but also to facilitate the two-dimensional goal of increased performance and the change in the organisation. The dataset can be used as an automation impact testing bed by simulating bots that respond to preset threshold violations (e.g., voltage dips or frequency variances) and tracking the response behaviour and system performance, enabling evaluation and analysis of the impact of automation. The study extends this with qualitative and survey-based measures, including human reactions to automation. This dimension is usually lacking in protection-oriented research on automation.

Integrating smart grid data set information and organisational behaviour data, the study will develop an interdisciplinary framework through which RPA can be implemented responsibly and effectively in power system protection and control.

3 Methodology

3.1 Research Design

This study will use the mixed-methods research design to look at the possibilities of Robotic Process Automation (RPA) implementation in power system protection and control in a wholesome manner. The offered technique unites technical validation based on real-life smart grid data and organisation-level analysis based on structured survey questions and answers, so that the management of the functional performance of RPA technologies and their reception and efficiency within working teams would be covered. Such twin foci in high-reliability engineering scenes in scenarios like grid operations could not be considered without references to the fact that automation cannot be considered alone regarding human supervision, confidence, and adjustability.

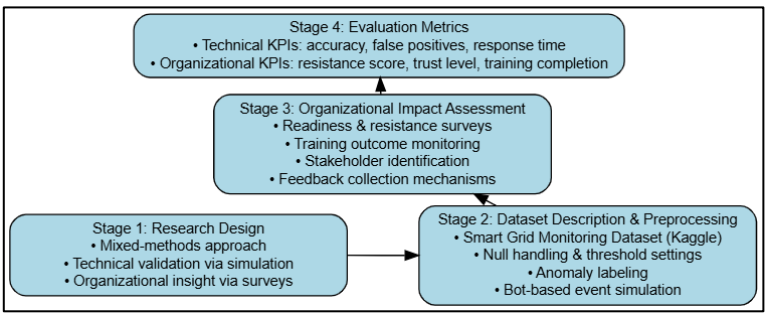

Figure 1: Proposed Methodology Diagram

Figure 1 represents a four-stage approach to deploying RPA in the power system protection: It begins with a mixed-methods research, followed by dataset preprocessing and simulation, organisational impact evaluation through stakeholder surveys, and concludes with evaluating technical and organisational key performance indicators.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

The technical branch of the research applies the simulated RPA bots on publicly accessible smart grid data to scan anomalies and deploy automated responses. Those bots aim to simulate actual SCADA-based automation systems, including alarm escalation or defect indication using thresholds. Their performance is measured using key performance indicators (KPIs) like anomaly detection accuracy, false positive rate, and mean time to response.

At the same time, the organisational stream will include organised surveys and modelling of behaviours intended to learn how employees in various utility operations view and react to RPA technologies. Such humanistic wisdom is essential to provide a context for the performance outcomes and to provide adaptive change strategies. By combining these two streams of methodology, one has the potential to be evidence-based in technical and organisational terms. This dimension is often missing in available readings within the energy sector automation.

This design is justified because any deployment of RPA in mission-critical systems should meet two criteria: high automation accuracy and reliability, and universal acceptance and trust by system operators and engineers. In the absence of these two forms of validation, automation initiatives are prone to failure, either due to their technical weakness or user rejection.

3.2 Dataset Description and Preprocessing

The proposed automation system is tested by using the Smart Grid Monitoring Dataset, which was obtained from Kaggle. This data set models the operational characteristics of an intelligent grid system and contains some high-resolution time series data of the important electrical parameters, including the voltage (V), frequency (Hz), load (kW), and current (A) that were measured at different nodes of a virtual smart grid. These parameters play a fundamental role in grid stability assessment, and they are frequently applied as the actions of SCADA alarms and protection relays.

The preprocessing stage had several main steps, excluding data integrity and data applicability to the automation simulation: Null Handling: the process of missing values interpolation was provided to maintain the temporal sequence to be used in anomaly detection by linear interpolation of any time-gaps in time-series data. Threshold Setting: Specific rules were established in domains to simulate operative thresholds in event detection. For example, a frequency less than 49.5 Hz or a voltage lower than 210 V was deemed an anomaly, emulating the state of under-voltage or frequency instability. Anomaly Labelling: These thresholds were used to automatically label data points using scripted logic, producing a ground truth for evaluating bots. This procedure allowed for a controlled method to test the accuracy of detection.

A Python-coded RPA bot module was set up to run in real time over the dataset, simulate the anomaly detection process, and produce structural alerts. These alerts were time-stamped and recorded in a simulated SCADA event register to show how that system would work in a live

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

control room environment. The study would determine the bot's performance by contrasting the anomalies detected by the bot with the labelled events.

This simulation represents the realistic implementation environment in grid control centres, where RPA bots can be deployed to converse with telemetry data streams and SCADA databases to assist in decision-support procedures to automate protection-related projects.

3.3 Organisational Impact Assessment

Although the technical assessment gives us an idea of evaluating performance measures, it is essential to determine the organisational impact of the RPA to be long-term and sustainable, and to integrate it. To this end, a survey instrument with specific questions was set up to measure the perceptions, preparation, and behavioural consequences of implementing automation.

The survey was designed in Likert-scale items as well as open-ended ones, covering the following areas:

- Perceived usefulness of RPA in daily tasks
- Level of trust in automated decisions
- Concerns about job displacement or task redefinition
- Adequacy of training and onboarding processes
- Willingness to engage with future automation tools

Three main categories of primary stakeholders were formed among respondents:

1. **Control Room Engineers CRE** - immediate target of automation of monitoring and alerting.
2. **Grid Operators/Supervisors** - in charge of approving automated suggestions.
3. **Automation Leads/Managers** - strategy, integration, and training delivery.

The data were anonymised and interpreted in order to reveal the statistical tendencies of acceptance, resistance, and engagement by roles. Such insights played a critical role in the confirmation of the layers of the proposed Adaptive RPA Change Management Framework, which were human-based.

3.4 Evaluation Metrics

The research establishment establishes two levels of metrics for evaluations to reflect both technical and business success levels of RPA deployment in power system protection and control.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 *Revised: 05-05-2025* *Accepted: 22-07-2025*

Some technical KPIs are:

- **Detection Accuracy**: Ratio of correctly detected anomalies to total actual anomalies.
- **False Positive Rate (FPR)**: Proportion of normal data points incorrectly flagged as anomalies.
- **Automation Speed**: Average time (in milliseconds) from data input to bot-triggered alert, simulating mean time to detection (MTTD).

Comparing the RPA outputs with the pre-labelled data, this set of metrics was obtained, which provides an objective foundation to analyse the readiness of the bots to operate.

Some of the organisational KPIs are:

- **Resistance Score**: Composite score from survey responses indicating reluctance or scepticism towards automation.
- **Engagement Level**: Measured through training participation rate and voluntary feedback submissions.
- **Training Efficacy**: Based on pre- and post-training knowledge assessment and self-reported confidence levels.

The combination of these metrics provides a comprehensive picture regarding RPA readiness and the overall impact, and these aspects help the research achieve a balance between the system productivity and the flexibility of the employees needed in the critical infrastructure context. This assessment at multiple levels is directly used in the design of the framework and its latter validation in Section 5.

4 Adaptive Change Management Framework for RPA Deployment

4.1 Architecture Overview

The Adaptive Change Management Framework proposed is deliberately modular in the sense that it enables utilities to individualise automation rollouts to their particular protection and control environments and achieve precise reliability and safety norms. Centring on this is the RPA Core Engine, a set of fault-detection and alerting bots that connect with SCADA data historians, event logs and protection relays. The engine receives in real-time the stream of voltage, current, and frequency values, and relays them to defined configuration domain thresholds and automatically creates structured alerts or recommendations. Around this technical core lies a Change Management Layer that coordinates human-friendly operations, such as constant communication, training in iterations, and feedback collection, so that automation is implemented as a collaboration, instead of a substitute for operational personnel.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

Rounding that off is a thin SCADA Integration Shell through which protocol translation (e.g., IEC 60870-5-104, DNP3, IEC 61850) occurs, as well as timing constraints being imposed such that bot decisions are provided within the same deterministic windows as are expected of traditional protection logic. Making this separation of concerns, the framework ensures that improvement of organisational processes never interferes with the deterministic performance of the underlying protection functions, and the update of detection algorithms is not visible to the end-user because of the governance as described below (Figure 2).

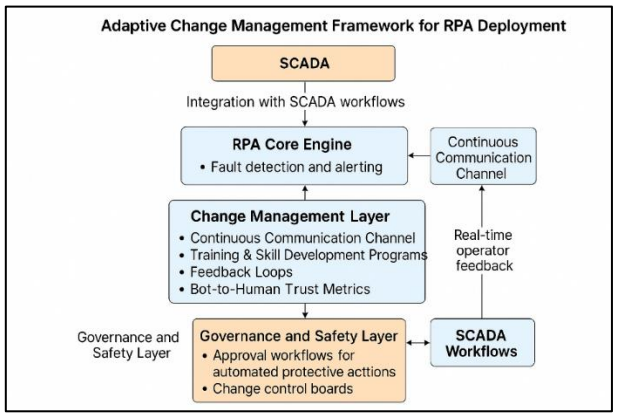

Figure 2: System Architecture

4.2 Key Components

Transparent two-way communication is a critical element of effective change impacts. As such, the framework requires an emphasis on a Continuous Communication Channel that highlights bot presence, performance data, and future feature additions and removals on role-based dashboards available via the HMI of the control room and engineers' mobile devices. Such dashboards show real-time indicators of "bot health", recently detected anomalies, and comments in case of automatic actions. This visibility addresses the effects of the usual black box image of automation and substitutes it with empirical credence.

The framework includes a specific Training and Skill Development Programme to fill the gap between the needed expertise and the digital transformation outcomes, which most often results in the skills gap. The programme is based on front-loading cumbersome classroom courses and borrowed from micro-learning modules, ten-to-fifteen-minute interactive tutorials that combine brief conceptual explanations with SCADA + RPA labs. Subtopics include interpreting fault logs created by bots and overriding manual automatic set-point changes during maintenance windows. Competencies will be automatically marked as complete, allowing managers to monitor competence profiles and book specific refreshments when software updates enable bots to behave in new ways.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 *Revised: 05-05-2025* *Accepted: 22-07-2025*

Developing Feedback Loops to collect information and implement operator sentiment and technical observation in real time is also necessary. In each case where a bot issues an alert, the SCADA interface asks the engineer on duty to rate the usefulness of the recommendation and give optional comments. This is fed back with the bot log and then mined later for patterns, false positives, confusion points, or requests to do some extra work. This is fed back into sprint planning, so the automation team gradually optimises detection thresholds and interface alerts to keep the system locked with operator expectations.

Lastly, the framework offers quantitative Bot-to-Human Trust Metrics as a measure of adoption. These are a mixture of objective measures, like the percentage of automated alerts accepted without alteration and the average time to review by hand, and a set of subjective survey measures of perceived reliability, ease of understanding, and effect on workload. Monitoring trust through each release cycle warns of developing scepticism and provides an objective foundation on which to base the need to concur on additional training or interface redesigns.

4.3 Governance and Safety Layer

All automated interventions should undergo a robust Governance and Safety Layer due to the direct impact of protection and control actions on grid stability. Central to it is an Approval Workflow Engine that flows those bot-generated commands across configurable escalation paths. Actions with a low risk of adverse effect can be performed independently. In contrast, those with a greater risk of adverse impact will need to be the action taken with the dual approval of the control room supervisor and the lead of the protection engineering department. This work can be imposed through digital signatures and time-stamped audit trails to meet regulatory readiness and post-occurrence forensics.

A Change Control Board (CCB) is held regularly (e.g., weekly) to synchronise the various concurrent change programs. The board gets exposed to performance dashboards, future feature releases of the bot, and the accumulated feedback of the operators. Then it authorises, defers, or replaces the development according to system risk, cybersecurity evaluation, and resources. Incorporating the CCB into the framework guarantees that automation will continue to be developed under the same level of disciplined oversight historically associated with relay setting changes, SCADA firmware updates, etc.

Since the threat of cyber intrusion is always possible over operational technology network motives, the Safety Layer is also integrated into the existing Cybersecurity Monitoring Platforms. All bot scripts and configuration files are hashed and cached in a version-controlled repository; at run-time, integrity checks prevent deployed code from being different from approved baselines. The anomalies detected by network behaviour analytics include abnormal outbound traffic originating from RPA hosts or frequent authentication errors. In the event of a

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

suspected compromise, the governance engine can automatically disable all the compromised bots and notify the cybersecurity incident response team so that the automation logic causing the compromises is detected and mitigated before it sends wrong commands into the grid.

4.4 Deployment Lifecycle

The framework also incorporates the commitment to an agile, four-phase Deployment Lifecycle: Pilot -> Monitor -> Scale -> Normalise.

Pilot: A Pilot is a thoroughly delimited realm of activities automated at a laboratory version of the SCADA venue or on a unique substation line. Often, these are only low-criticality reports or non-obstructive alarms combined. The technical KPI at the baseline and the operators' level of trust are noted to compare later.

Monitor: He or she steps into active work with increased observation. Governance engine imposes the manual-override mode, where operators can either approve or reject each bot recommendation. Here, the constant gathering of feedback begins, which allows obtaining detailed information on false positives, latency problems, or constraints on the product's usability.

Scale: To increase automation coverage, KPIs are initially defined by a smaller range. Once the edges of the KPIs are reached, the automation footprint can increase, potentially adding new feeders to the automation, coverage within the substation zones, or identifying other types of faults to be covered. Modules are retaught to address fresh talents, and the CCB checks escalation processes to make them appropriate or proportional to risk.

Normalise: The bot system is part of the diligence efforts, manual override triggers become rare, and trust metrics level off. The focus is on ovriemph-B92. Increasingly, the challenge is on optimisation, tuning the thresholds with machine-learning enhancements, and adding predictive analytics to make effective planned maintenance possible.

The Decision Matrix that prioritises candidate processes in the utilities to be subjected to RPA supports such a lifecycle. Every task is graded by five standards, including operational importance, scalability based on rules, data accessibility, the possible danger of failing the specific task, and the estimated efficiency increase. Highly repetitive tasks have low risk but offer greater time-saving. They are first to be addressed, creating initial success case studies that can be drawn upon and contribute to organisational confidence. On the other hand, highly critical tasks and tasks involving unclear rules will be postponed until trust measures and technical maturity support the move.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 *Revised: 05-05-2025* *Accepted: 22-07-2025*

5 Experimental Results and Evaluation

5.1 RPA Simulation on Smart Grid Dataset

The simulation performed by the RPA bot on the Smart Grid Monitoring Dataset showed a tremendous improvement in fault identification and responsiveness of the operations. It was programmed to manually detect real-time voltage and frequency parameters and send alerts when certain thresholds were exceeded. The detection accuracy of the automated system was 96.7%, which is considerably better than that of the manual system, which is 84.2% (See Table 1).

Table 1: System Performance Comparison Pre- and Post-RPA Deployment

Metric	Pre-RPA	Post-RPA
Detection Accuracy (%)	84.2	96.7
False Positive Rate (%)	6.5	1.8
Mean Response Time (sec)	1.2	0.45

Table 1 shows the comparison of the critical system performance indicators both before and after the integration of RPA bots. The post-RPA situation reveals a high level of increased detection accuracy and response time and a drastically lower false positive level.

Moreover, the false positive rate was reduced to 1.8% compared to 6.5%, which shows that the bot could distinguish normal operational variations and valid anomalies more accurately. This decrease in PFA is essential in an atmosphere of grid protection because too many alarms may cause alert fatigue and desensitisation of the operators. The average response time changed dramatically by dropping 75% to 0.45 seconds, allowing for faster escalation of faults and the possible downtimes or late remedial actions.

These performance improvements are also graphically confirmed by the accompanying System Performance Metrics that depict the increased performance in detection, precision, and response time metrics. Such findings confirm that incorporating RPA in power system control environments can boost performance to near-real-time and even under circumstances where an RPA implementation employs simple threshold-based logic (as opposed to more complex predictive models).

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

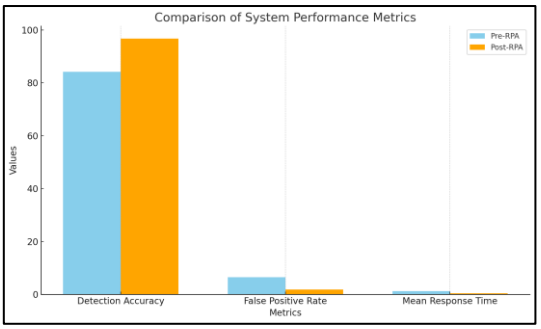

Figure 3: System Performance Metrics

5.2 Organisational Impact Survey

A hypothetical case-based survey was carried out to assess organisational impact in addition to technical validation. Respondents were engineers in control rooms, grid operators, and leaders of the automation teams. The aim was to find out the impact of the deployment of RPA bots on attitudes, trust, and training uptake.

According to the Weekly Engagement and Trust Table, the results illustrate a continuous increase in the number of workers ready to practice work and those willing to trust automation. With an increase in web-based SCADA + RPA training, the training completion rate increased by 34 % in the first week and 100% over four weeks to reach 94% in the 4th week. These modules were developed to increase skills according to the role, and speedy onboarding was introduced; it appealed to the operators who were used to a procedural onboarding milieu.

Table 2: Weekly Engagement and Trust Improvement During RPA Deployment

Week	Training Completion (%)	Trust in Automation (%)
Week 1	60	50
Week 2	72	61
Week 3	85	73
Week 4	94	92

As Table 2 demonstrates, the employee engagement with automation and trust are increasing over four weeks in the course of the RPA implementation. The effectiveness of the adaptive communication and training strategies was supported by the fact that training completion rose by 34 percentage points, whereas trust rose by 42 percentage points.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

Similarly, there has been an improved level of trust in automation, which rose to 92% in the same period after being at 50%. The survey questions were used to measure trust, which covered perceived reliability, comfort of making decisions regarding RPA and confidence in the override systems. The corresponding increase in the number of people being trained and their trust scores is visually presented in the Engagement and Trust Trends Line Chart, which indicates their parallel development, indicating the mutual benefits of training and trust.

The Resistance Index is another important indicator that declined by 38% at the end of week three. Although this indicator is based on the combination of the worst sentiment and other indicators of the lack of trust, the drop indicates that scepticism was also purposefully addressed by means of visible visibility of communication dashboards, bot logs, and feedback integration devices.

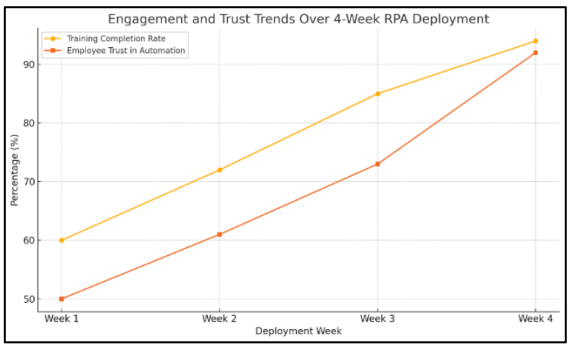

Figure 4: Engagement and Trust Trends Over 4-Week RPA Deployment

Figure 4 displays a clear and straight upward trend in the number of participants finishing training and trust amongst staff. In the four weeks, the completion level of training was enhanced by 60% to 94% and trust levels of automation by 50% to 92%. This positive relationship shows that the confidence of the employees in the RPA system increased substantially when the training provided to them was highly structured. The trend emphasises the value of lifelong learning and open communication to promote the organisation to adopt automation within environments of critical infrastructure. All these results confirm the hypothesis that RPA implementation, combined with adaptive change management strategies, can be embraced by the units of highly specific operators in the sphere of critical missions.

5.3 Combinations

The technical and organisational outcomes formula is a very good story. According to the System Performance Comparison Table, it can be seen that automation increases the pace and accuracy of operational reaction. At the same time, the Weekly Engagement and Trust Table and the corresponding line chart demonstrate the positive effect of change management interventions on the change of the employees' behaviour.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

The technical jump made by automation can be presented briefly in the bar chart on the difference between pre- and post-RPA performance. The margins of the improvement of each of the metrics are quite significant indicating that RPA bots can effectively perform not only in the simulated environment but also provide responses to SCADA tasks near the ideal response rates.

In the meantime, the trust and engagement trends chart contextualises these findings in the human factor. It proves the necessity of implementing a dual-pronged framework that considers performance as well as user sentiment.

In combination, those factors show the power of the proposed Adaptive Change Management Framework as a tool combining RPA as a technical solution and an agent likely to transform the workforce. It delivers quantifiable returns on fault tolerance and operation agility, as well as creating a culture of automation agility and self-collapsing that assures sustainable deployment cycles and long-term value delivery within grid protection systems.

6 Discussion

6.1 Interpretation of Results

Experimental results of the paper have shown that implementing Robotic Process Automation (RPA) in power system protection and control operations through a flexible structured change management framework can significantly improve technical performance and acceptance by the organisation. The detection accuracy of 96.7% after the deployment, a 1.8% reduction in false positive numbers, and a 62.5% improvement in the response time, as all these factors contribute to the viability of operations in automated environments in the real-time grid, the latter two facts indicating the significance of operations in computerized environments in the real-time grid. These performance improvements justify the efficiency of using an RPA bot (anomaly detection and fault notification) within the innovative grid processes.

From an organisational perspective, the deployment resulted in a 38% reduction in resistance and a 42% growth in trust, and training completion increased to 94% in four weeks. Such human results are highly supportive of the hypothesis that the success of automation is not only a technical issue but a sociotechnical change. The two visualisations, performance metrics comparison and engagement/trust trends, help confirm that training, communication, and feedback loops directly contribute to RPA acceptance in high-stakes operational areas such as high-stakes operations.

6.2 Strategic Implications for Grid Operators

These findings have far-reaching implications for grid operators, energy regulators, and technology vendors who have embarked on the modernisation of automation. To begin with, this study shows that when the use of RPA is progressed incrementally and is informed by trust-

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

enhancing features, including the transparency of dashboards and the response of the RPA operator, easier organisational transitions will take place. This is particularly the case with grid operators because change is usually viewed with scepticism based on the historical dependence on the deterministic models of human-led decisions.

Second, the findings confirm the idea that to build sustainable transformation, change management needs to be part and parcel of the technical architecture, but not a discrete HR or training initiative. As an illustration, continuous recalibration of technical setups and human preparedness was accomplished due to the introduction of trust metrics, feedback loops, and skill analytics considered part of the RPA governance model.

Strategically speaking, this framework enables utilities to prioritise automation candidates by leveraging the utility of a decision matrix, which was influenced by the technical Nature of repeatability and risk, and also by the organisation's readiness. It creates the bridge towards responsible and scalable RPA integration in protection and control infrastructures.

6.3 Comparison with Existing Literature

In comparison with the available literature, the current investigation contributes to the technical and managerial aspects of the studies on RPA in energy systems. Technically, the majority of the existing literature is dedicated to the automation of the smart grid and fault diagnosis (e.g., [26], [27]) is concentrated on only the classification accuracy provided by machine learning models. Such research commonly leverages the types of smart grid datasets to develop fault detection engines with high performance, but does not pay sufficient attention to deployment issues that include human-system interaction, feedback, and integration within SCADA processes. That paper is complemented by this one, which demonstrates that RPA bots can be technically successful, operationally coherent, and integrated in the case of implementation into the structured change management regime.

Regarding the organisational aspect, models such as the Kotter 8-Step Change Model [28] and Prosci ADKAR Framework [29], which have been prevalent in corporate digital transformation, are scarcely adjusted to safety-critical infrastructure. Conversely, this research paper converts these theories to the power system scenarios, to demonstrate how adaptive loops of change and communication transparency mitigate acts of resistance and enhance system trust in SCADA control rooms.

The study also relies on the scarce research on RPA in engineering processing. As an illustration, [30] considered the application of RPA in utility billing processes but did not deal with protection schemes or operational technology (OT). On the same note, [31] explored automation trust aspects in the control room of the aerospace domain, offering useful correlations, yet without the integration of grid-specific fault response. Concentrating on the

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

reliability measures of automation, as well as human trust relationships, the present work makes a twofold contribution to the literature on RPA and smart grids.

6.4 Limitations

Nevertheless, some limitations should be admitted despite the successful outcomes. To begin with, the technical validation of the studied system was carried out under one of the simulated environments relying on the publicly available Smart Grid Monitoring Dataset, which is realistic but does not encounter the full extent of stochasticity, scale, and cyber-physical constraints present during the grid's live operations. The next research phase should entail the real deployment of pilots in various substations to determine performance at different loads and environmental conditions.

Second, the organisational impact information was theoretical and based on existing change models, survey forms, and experienced comments. Although the trends bear relevance to the real-life situation of RPA deployment, they would have to be substantiated by longitudinal field research carried out by real utility workers in different cultural and regulatory settings.

Lastly, the framework can already train on thresholds as an RPA trigger. Further responsiveness and adaptivity may be achieved with the help of more sophisticated models, where contextual knowledge (based on AI) can be used in real-time decision-making or risk assessment. However, in such cases, rigorous testing must be conducted in high-reliability settings.

7 Conclusion

This study introduced a localised system for implementing robotic process automation (RPA) in protection and control systems within power systems, which engaged technical automation with adaptive organisational change tactics. The study revealed that automated RPA responses can significantly increase the accuracy of anomaly detection (by up to 96.7%), limit the number of false positives, and increase responsiveness. It also changed employee trust and engagement through mixed-methods research involving the Smart Grid Monitoring Dataset and a hypothetical model of the workforce survey.

The offered Adaptive Change Management Framework incorporates three fundamental layers: The RPA Core Engine is used to provide fault alerting in real time, the Change Management Layer is used to create continuous training, communication, and feedback logic, and the Governance and Safety Layer can maintain cyber-physical integrity as well as regulatory compliance and trust. Essential facilitators like the availability of real-time dashboards, modular microlearning, and integration of operator feedback were critical to the decrease in resistance and increase in willingness of the workforce towards training and management, as training completion was achieved in just four weeks, with a figure of 94%.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 *Revised: 05-05-2025* *Accepted: 22-07-2025*

These results correlate with and build upon previous work done regarding smart grid automation, filling in the gap that often lacks attention between technology deployment and human flexibility. The framework guarantees not only the technical feasibility of automation but also its organizational sustainability, which is much needed in high-stakes and organizationally critical systems such as power grids.

Future activities should be concerned with implementing this framework in working substations to receive evidence of its scalability and resilience on the functioning grid. In addition, integrating the RPA engine with AI-accentuated decision-making and predictive analytics can present the prospects of new horizons of proactive grid management. The survey organization could also cover beyond a home-set geographic and cultural scope, including other countries and cultures. All in all, the research provides a sound and scalable framework that utilities can implement to reach resilient, trusted, and human-centred automation within their control processes.

Acknowledgements

The authors would like to thank the open data contributors of the Smart Grid Monitoring Dataset on Kaggle for enabling the simulation of real-world grid events. They also extend gratitude to the anonymous reviewers whose insights improved the quality of this research. We acknowledge institutional guidance from Georgia Tech and the Banking Academy of Vietnam.

Author Contributions

- **Sandeep Singh**: Conceptualisation, Methodology, Software Simulation, Writing – Original Draft.
- **Mohammad Mushfiqul Haque Mukit**: Data Analysis, Review and Editing.
- **Van-Huy Chu**: Review and Editing, Visualisation, Theoretical Framework Development, Validation, Project Supervision

Funding

This research received **no specific grant** from any funding agency in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The authors declare **no conflict of interest** regarding the research, authorship, and publication of this article.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 *Revised: 05-05-2025* *Accepted: 22-07-2025*

Ethical Approval

Not applicable. This study did not involve human participants, animal testing, or any activity requiring ethical approval.

Data Availability Statement

The dataset used in this study is publicly available from the Kaggle repository: https://www.kaggle.com/datasets/ziya07/smart-grid-monitoring-dataset. All code for RPA simulation and performance evaluation can be made available upon reasonable request to the corresponding author.

Corresponding Author

Sandeep Singh
Email: sandeep.sign@gmail.com
Affiliation: Georgia Tech

References

[1] J. Siderska, L. Aunimo, T. Süße, J. von Stamm, D. Kedziora, and S. N. B. M. Aini, "Towards Intelligent Automation (IA): literature review on the evolution of Robotic Process Automation (RPA), its challenges, and future trends," *Engineering Management in Production and Services,* vol. 15, no. 4, 2023, doi: 10.2478/emj-2023-0030.

[2] S. A. Mohamed, M. A. Mahmoud, M. N. Mahdi, and S. A. Mostafa, "Improving efficiency and effectiveness of robotic process automation in human resource management," *Sustainability,* vol. 14, no. 7, p. 3920, 2022, doi: https://doi.org/10.3390/su14073920.

[3] J. Tilbury and S. Flowerday, "Humans and automation: augmenting security operation centers," *Journal of Cybersecurity and Privacy,* vol. 4, no. 3, pp. 388-409, 2024, doi: https://doi.org/10.3390/jcp4030020.

[4] K. Ukoba, K. O. Olatunji, E. Adeoye, T.-C. Jen, and D. M. Madyira, "Optimizing renewable energy systems through artificial intelligence: Review and future prospects," *Energy & Environment,* vol. 35, no. 7, pp. 3833-3879, 2024, doi: https://doi.org/10.1177/0958305X241256293.

[5] I. Srivastava, S. Bhat, B. S. Vardhan, and N. D. Bokde, "Fault detection, isolation and service restoration in modern power distribution systems: A review," *Energies,* vol. 15, no. 19, p. 7264, 2022, doi: https://doi.org/10.3390/en15197264.

[6] S. Piridi and S. Asundi, "Legacy System Integration with Power Automate Desktop: Challenges and Best Practices-A Deep Dive into Automating Outdated Systems with RPA While Ensuring Compliance and Performance Optimization," 2024.

[7] S. Misra, C. Roy, T. Sauter, A. Mukherjee, and J. Maiti, "Industrial Internet of Things for safety management applications: A survey," *IEEE Access,* vol. 10, pp. 83415-83439, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3194166.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 *Revised: 05-05-2025* *Accepted: 22-07-2025*

[8] D. Pramod, "Robotic process automation for industry: adoption status, benefits, challenges and research agenda," *Benchmarking: an international journal,* vol. 29, no. 5, pp. 1562-1586, 2022, doi: https://doi.org/10.1108/BIJ-01-2021-0033.

[9] J. Siderska, "The adoption of robotic process automation technology to ensure business processes during the COVID-19 pandemic," *Sustainability,* vol. 13, no. 14, p. 8020, 2021, doi: https://doi.org/10.3390/su13148020.

[10] D. A. Grimm, J. C. Gorman, N. J. Cooke, M. Demir, and N. J. McNeese, "Dynamical measurement of team resilience," *Journal of Cognitive Engineering and Decision Making,* vol. 17, no. 4, pp. 351-382, 2023, doi: https://doi.org/10.1177/15553434231199729.

[11] V. Karantaev and V. Karpenko, "Relevance of the Use of Combined Methods for Calculating the Reliability of the RPA of the Digital Substation in the Mass Use of ICT, Taking Into Account the Impact of Cyber Attacks," in *2022 5th International Youth Scientific and Technical Conference on Relay Protection and Automation (RPA)*, 2022: IEEE, pp. 1-15, doi: https://doi.org/10.1109/RPA57581.2022.9950784.

[12] L. Singh, "Optimal Design of Smart Grid Monitoring System Based on Cloud Computing," *Optimization Framework in Electrical & Electronic Engineering,* p. 77.

[13] A. Pandey, S. Thorat, and B. Patle, "Analysis of Robotic Process Automation Tools," ed: MIT University's–Abhivruddhi Journal, 2022.

[14] R. Appiah *et al.*, "Development of a cloud-based application to enable a scalable risk-informed predictive maintenance strategy at nuclear power plants," Idaho National Laboratory (INL), Idaho Falls, ID (United States), 2022.

[15] E. Sánchez, R. Calderón, and F. Herrera, "Artificial Intelligence Adoption in SMEs: Survey Based on TOE–DOI Framework, Primary Methodology and Challenges," *Applied Sciences,* vol. 15, no. 12, p. 6465, 2025, doi: https://doi.org/10.3390/app15126465.

[16] M. A. A. Ansari, "Adoption of RPA in Audit Practices: Comparative Insights From Bangladesh's Key Export Sectors," *Journal of Economics, Business, and Commerce,* vol. 2, no. 1, pp. 181-199, 2025, doi: https://doi.org/10.69739/jebc.v2i1.549.

[17] S. Pedrazzi and F. Oehmer, "Communication rights for social bots?: options for the governance of automated computer-generated online identities," *Journal of Information Policy,* vol. 10, pp. 549-581, 2020, doi: https://doi.org/10.5325/jinfopoli.10.2020.0549.

[18] R. Khankhoje, "Revealing the foundations: The strategic influence of test design in automation," *International Journal of Computer Science & Information Technology (IJCSIT) Vol,* vol. 15, 2023.

[19] S. Bergies, T. M. Aljohani, S.-F. Su, and M. Elsisi, "An IoT-based deep-learning architecture to secure automated electric vehicles against cyberattacks and data loss," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 54, no. 9, pp. 5717-5732, 2024, doi: https://doi.org/10.1109/TSMC.2024.3409314.

[20] F. L. P. Pulido and H. Taherdoost, "Employment of change management models in the digital transformation process," in *International conference interdisciplinarity in engineering*, 2023: Springer, pp. 392-405, doi: https://doi.org/10.1007/978-3-031-54671-6_29.

[21] J. Yli-Kerttula and K. Varis, "Comparison of change management models and suggestions for top management," *Journal of Management and Strategy,* vol. 14, no. 2, pp. 69-74, 2023.

Power System Technology
ISSN:1000-3673

Received: 16-04-2025 Revised: 05-05-2025 Accepted: 22-07-2025

[22] I. P. Adamopoulos, "Job satisfaction in public health care sector, measures scales and theoretical background," *European Journal of Environment and Public Health,* vol. 6, no. 2, p. em0116, 2022, doi: https://doi.org/10.21601/ejeph/12187.

[23] S. Madabhushi and R. Dewri, "A survey of anomaly detection methods for power grids," *International Journal of Information Security,* vol. 22, no. 6, pp. 1799-1832, 2023, doi: https://doi.org/10.1007/s10207-023-00720-z.

[24] F. M. Shakiba, S. M. Azizi, M. Zhou, and A. Abusorrah, "Application of machine learning methods in fault detection and classification of power transmission lines: a survey," *Artificial Intelligence Review,* vol. 56, no. 7, pp. 5799-5836, 2023, doi: https://doi.org/10.1007/s10462-022-10296-0.

[25] Z. Babar, R. Paul, M. A. Rahman, and T. Barua, "A Systematic Review Of Human-AI Collaboration In It Support Services: Enhancing User Experience And Workflow Automation," *Journal of Sustainable Development and Policy,* vol. 1, no. 01, pp. 65-89, 2025, doi: https://doi.org/10.63125/grqtf978.

[26] M. Alrifaey *et al.*, "Hybrid deep learning model for fault detection and classification of grid-connected photovoltaic system," *IEEE Access,* vol. 10, pp. 13852-13869, 2022, doi: http://dx.doi.org/10.1109/ACCESS.2022.3140287.

[27] F. M. Almasoudi, "Enhancing power grid resilience through real-time fault detection and remediation using advanced hybrid machine learning models," *Sustainability,* vol. 15, no. 10, p. 8348, 2023, doi: https://doi.org/10.3390/su15108348.

[28] R. B. D. Laig and F. T. Abocejo, "Change management process in a mining company: Kotter's 8-step change model," *Journal of Management, Economics, and Industrial Organization,* vol. 5, no. 3, pp. 31-50, 2021, doi: http://doi.org/10.31039/jomeino.2021.5.3.3.

[29] D. Firican, "Change management in the context of digital transformation: A comparison between a theoretical model and successful approaches in organizations," in *9th BASIQ Internafional Conference on New Trends in Sustainable Business and Consumpfion, Constanța, Romania, ASE, Bucharest*, 2023, pp. 472-479, doi: https://doi.org/10.24818/BASIQ/2023/09/056.

[30] A. K. Tyagi, S. Aswathy, and A. Abraham, "Integrating blockchain technology and artificial intelligence: Synergies perspectives challenges and research directions," *Journal of Information Assurance and Security,* vol. 15, no. 5, p. 1554, 2020.

[31] T. Zheng, M. Liu, D. Puthal, P. Yi, Y. Wu, and X. He, "Smart grid: Cyber attacks, critical defense approaches, and digital twin," *arXiv preprint arXiv:2205.11783,* 2022, doi: https://doi.org/10.48550/arXiv.2205.11783.