International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Robust Optimal Power Flow under Industrial Cyberattacks and Renewable Uncertainty

Vasil Metodiev[1], Iliyan Vasilev[2]
[1,2] University of Chemical Technology and Metallurgy, Sofia, Bulgaria

ABSTRACT: The digitalization of electric-power operation couples optimal power flow (OPF) with measurement systems, communication networks and increasingly variable renewable generation. Power system operators may have to make dispatch decisions using load measurements that have been altered by false-data injection attacks. At the same time, actual renewable power generation may differ from what was forecast. When these two problems occur together, the system may need more balancing capacity than would be expected if each uncertainty were considered separately. This paper examines both effects through a scenario-based robust direct-current optimal power flow (DC-OPF) approach. The proposed model determines generator schedules and upward and downward reserves with ensuring that the system can respond to bounded combinations of corrupted load measurements and renewable forecast errors. The approach focuses on reducing their operational consequences. It assumes that the operator does not know the exact amount of corruption measurement but can define reasonable limits for measurement errors and renewable uncertainty. The study uses the publicly available PGLib-OPF v23.07 IEEE 14-bus and IEEE 30-bus networks, with additional renewable generation and cyberattack scenarios introduced for testing. The results show that the robust approach increases preventive operating costs by 0.98% for the 14-bus system and 1.97% for the 30-bus system compared with a deterministic OPF using a standard 10% balancing-reserve rule. In 3,000 out-of-sample scenarios for each network, the robust schedule avoided emergency load shedding within the defined uncertainty limits. By comparison, the deterministic approach required load shedding in 62.77% of the IEEE 30-bus scenarios, with an average of 2.56 MW and a maximum of 18.93 MW of unserved power. These results suggest that the benefit of robust OPF is not simply a change in how generation is scheduled. More importantly, it helps place reserve capacity where it can be used effectively, reducing the risk that corrupt measurements and unexpected renewable fluctuations will prevent the power system from operating within its physical limits.

KEYWORDS: cyber-resilient optimal power flow, false data injection, renewable uncertainty, robust optimization, reserve co-optimization, smart grid, cyber-physical power systems.

INTRODUCTION

Electric-power systems are becoming cyber-physical infrastructures in which economic scheduling, state estimation, protection, communication and control are inseparable. Optimal power flow (OPF) plays an important role in power system operation. It uses network measurements and generation forecasts to determine how much power each generator must produce keeping the system within transmission and generator limits. The increasing use of digital communication and monitoring also creates opportunities for cyberattacks. If an attacker changes the measurements used by the OPF, the resulting dispatch decisions may be based on incorrect information. False-data injection attacks are a particular concern because they can alter state estimates or other inputs used by the operator without producing changes that are easily recognized as suspicious (Liu et al., 2009; Pasqualetti et al., 2013). Renewable energy creates another challenge. The more wind and solar power is connected to the grid, more differences between forecast and actual generation become harder to avoid. These variations adds additional balancing reserves and can change power flows across transmission lines, even when no cyberattack is taking place.

The integration of renewable energy sources into smart-city infrastructure has also been reviewed by Nikolov (2024), who highlights their role in sustainable energy systems and the supporting monitoring infrastructure.

These two sources of uncertainty are usually studied in different research streams. The cyber-security literature examines whether an adversary can modify measurements, shared optimization variables or state estimates and how such manipulation can be detected or isolated. The uncertainty-aware OPF literature focuses on stochastic, chance-constrained, robust or distributionally robust methods for renewable generation and load variability. Both streams are mature, but their separation is operationally artificial. A

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

control room acts on one set of information. If the load vector is corrupted while renewable output simultaneously deviates from forecast, the system must remain feasible under the combined net-injection error rather than under either error separately.

In practice, power system operators cannot always rely on cyberattacks being detected before dispatch decisions are made. Attack detection and identification are important, but they take time and depend on the methods and thresholds being used. Another way to reduce the risk is to design the dispatch so that the system can still operate safely when measurements contain errors within known limits. This require keeping more reserve capacity available, which increases operating costs but gives the system more flexibility when unexpected conditions occur. The trade-off is related to the price of robustness discussed by Bertsimas and Sim (2004). In this study, however, the uncertainty comes from two different sources: deliberate changes to load measurements caused by cyberattacks and ordinary differences between forecast and actual renewable generation. Previous research examines these problems from several perspectives. Khanna et al. (2017) showed that manipulating load measurements can affect the decisions made by security-constrained OPF. Duan et al. (2018) and Cheng and Chow (2022) studied ways to make distributed OPF more reliable when information exchanged between agents is corrupted. Other researchers have focused on renewable energy uncertainty. For example, Zhang et al. (2017), Roald et al. (2017) and Roald and Andersson (2018) examined how generation and reserve requirements can be determined using chance-constrained and distributionally robust OPF methods. Recent studies study how uncertainty sets can better represent variations in renewable generation and the relationships between uncertain variables (Esteban-Pérez & Morales, 2023; Huang et al., 2025; Ou et al., 2026). Load-measurement attacks and renewable forecast errors are often considered separately. This paper examines them together using a benchmark model in which both types of uncertainty are included in the same uncertainty set. The aim is to determine how much reserve capacity is needed, where it should be allocated and whether corrective changes in generation can keep the network within its operating limits.

The contribution of this study is fourfold. First, it formulates corrupted demand measurements and renewable forecast errors as a common net-injection uncertainty acting on a DC-OPF model. Second, it co-optimizes the nominal dispatch with upward and downward reserve and requires feasible corrective redispatch for all corner scenarios of the bounded uncertainty set. Third, it evaluates the approach on openly available PGLib-OPF benchmark networks so that network parameters, thermal limits and generator data are reproducible. Fourth, it evaluates resilience using physical consequences - probability and magnitude of load shedding, renewable curtailment and emergency operating cost - instead of treating the optimization objective alone as evidence of security.

This paper treats attack detection and maintaining system operation during an attack as two separate problems. The proposed model is not designed to identify attackers, determine their intentions or replace existing security methods used in state estimation. Instead, it focuses on preparing the power system for situations where the measurements used for dispatch may not be reliable. Allocating sufficient reserves in advance, the system has a better chance of remaining within its operating limits even when some of the input data have been corrupted. This does not mean that every cyberattack can be detected or that all possible attacks can be represented as measurement errors within fixed bounds. The approach is intended to reduce the operational effects of certain types of attacks, rather than provide complete protection against every cyber threat.

From Deterministic OPF to Cyber-Resilient Dispatch

For a transmission network represented by buses N, branches L and controllable generators G, the conventional DC-OPF computes active-power generation p_g and bus voltage angles θ_i to minimize generation cost. For branch $\ell=(i,j)$, the linearized active-power flow is proportional to the angle difference. Transformer tap ratios from the benchmark are retained through an effective branch susceptance. The model is intentionally DC rather than AC so that the interaction between information corruption, reserve and network feasibility remains transparent and can be formulated as a linear program.

Let d_i denote the active-power demand that the operator believes to be present at bus i and let $\hat{w}_i$ denote the scheduled renewable injection. The nominal nodal balance requires conventional generation plus renewable power to equal demand plus net export. Thermal ratings and phase-angle-difference bounds limit the feasible network region.

$$f_{ij} = \frac{B_{ij}}{\tau_{ij}}(\theta_i - \theta_j), \qquad |f_{ij}| \le F_{ij}^{\max}$$

$$\sum_{g \in G_i} p_g^0 + \hat{w}_i - \tilde{d}_i = \sum_{j:(i,j)\in L} f_{ij}^0$$

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

The superscript 0 denotes the preventive or nominal operating point. The key cyber-physical question is what happens when the quantities used in this balance are not the quantities realized by the physical system. A deterministic OPF treats the reported demand and renewable forecast as exact. A cyber-resilient OPF instead treats them as the center of an uncertainty region and explicitly plans corrective capability around that center.

Corrupted Measurement and Renewable-Uncertainty Model

A false-data injection affecting load information can be represented as an additive or multiplicative error between the reported and true demand. In the present study, the PGLib load vector is interpreted as the operator's nominal measurement vector $\tilde{d}$. The unknown physical demand d differs from this vector by a bounded corruption term a. Positive a means that the true demand is larger than the value trusted by the OPF, a particularly critical condition because insufficient conventional generation may then be scheduled.

Renewable generation is modeled by a forecast $\hat{w}$ and a forecast error ε. The two errors have different physical origins - one is adversarial and one is stochastic - but both enter the nodal power balance through net injection. For operational feasibility, the distinction matters mainly through the admissible uncertainty set and the spatial buses at which the errors occur.

$$d_i = \tilde{d}_i + a_i, \qquad w_i = \hat{w}_i + \varepsilon_i$$
$$|\, a_i \,| \leq \kappa_i \tilde{d}_i, \qquad |\, \varepsilon_i \,| \leq \rho_i \hat{w}_i$$

For the main experiment, uncertainty is represented using a box-shaped set that defines the possible range of errors at selected demand and renewable generation buses. This approach was chosen because it is relatively simple to apply and makes the assumptions easy to check. It does not assume that real attackers always act independently or that renewable forecast errors always remain within fixed limits. Instead, the defined ranges provide a clear set of conditions under which the dispatch must remain feasible. More advanced approaches could also be used, such as uncertainty sets that limit the number of affected buses, ellipsoidal sets, Wasserstein ambiguity sets or models that account for relationships between uncertain variables. These alternatives would change how uncertainty is represented, but the main purpose of the framework would remain the same: to keep the power system operating within its limits despite possible measurement corruption and renewable generation errors.

$$\mathcal{U} = \{(a, \varepsilon):\ -\kappa_i \tilde{d}_i \leq a_i \leq \kappa_i \tilde{d}_i,$$
$$-\rho_i \hat{w}_i \leq \varepsilon_i \leq \rho_i \hat{w}_i\}$$

For the linear DC network with continuous corrective redispatch, the vertices of this bounded polytope provide a finite representation of the stress cases. If a fixed preventive decision admits feasible recourse at all vertices, any interior uncertainty realization can be represented as a convex combination of those vertices and corresponding recourse actions. The empirical design therefore enforces 16 corner scenarios for the IEEE 14-bus case and 64 for the IEEE 30-bus case. The proposed cyber resilient OPF is explicitly presented in a diagram in Figure 1.

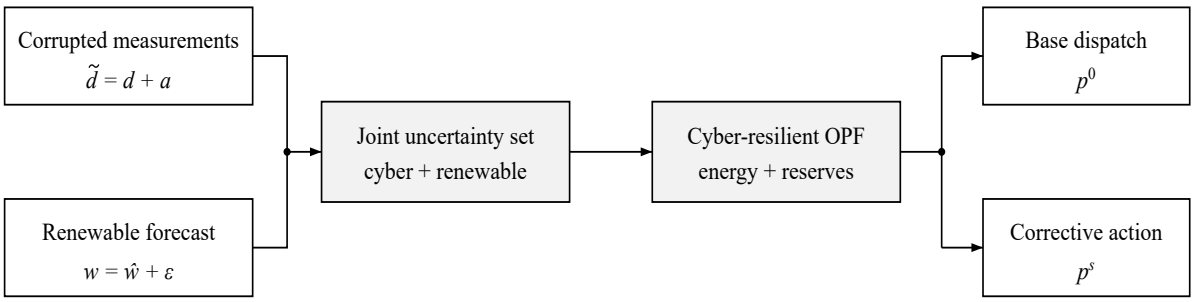

Figure 1. Integrated logic of the proposed cyber-resilient OPF: uncertain data are converted into a joint uncertainty set, which determines reserve and scenario-feasible corrective actions.

Robust Reserve Co-Optimization Formulation

The model first determines the planned generation output p^0 and the amount of upward and downward reserve capacity, represented by r^+ and r^-. Its objective is to minimize the cost of scheduled generation while also accounting for the cost of keeping reserves available. In the numerical experiments, reserve costs are estimated as a proportion of each generator's marginal energy cost. These are assumed values used for testing and do not represent actual prices from a specific reserve market. For each uncertainty scenario

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

s, the model calculates an adjusted generation schedule p^s and the corresponding bus voltage anglesθ^s. Any adjustment must stay within the available reserves and the operating limits of the generators. The model also checks that power supply and demand remain balanced at each bus, transmission lines are not overloaded and voltage-angle differences stay within their permitted limits. This means that having enough reserve capacity across the whole system is not sufficient on its own. The reserves must also be located at generators that can respond to changes in demand or renewable generation without violating network constraints. The approach therefore considers not only how much reserve is available, but also where it can be used effectively.

$$\min \sum_{g\in G} c_g\, p_g^0 + \sum_{g\in G} q_g^+ r_g^+ + \sum_{g\in G} q_g^- r_g^-$$
$$P_g^{\min} \le p_g^0 \le P_g^{\max}, \qquad 0 \le r_g^+,\ r_g^-,$$
$$p_g^0 + r_g^+ \le P_g^{\max}, \qquad p_g^0 - r_g^- \ge P_g^{\min}$$
$$-r_g^- \le p_g^s - p_g^0 \le r_g^+ \qquad \text{for all scenarios } s$$
$$\sum_{g\in G_i} p_g^s + (\hat{w}_i + \varepsilon_i^s) - (\tilde{d}_i + a_i^s) = \sum_j f_{ij}^s$$
$$|\, f_{ij}^s \,| \le F_{ij}^{\max}, \qquad |\, \theta_i^s - \theta_j^s \,| \le \Delta\theta_{ij}^{\max}$$

The difference between the proposed robust approach and a conventional reserve rule is important. A fixed reserve percentage may provide enough capacity to cover the overall power imbalance, but it does not necessarily place that capacity where it is needed. The robust model accounts for these network restrictions when deciding where reserves should be allocated. This can be seen in the IEEE 30-bus experiment, where a substantial share of the upward reserve is assigned to generator 2 rather than simply increasing the reserve of the cheapest generator. The decision is influenced by the ability of the network to support corrective changes in generation, not just by the total reserve capacity.

Interpretative Logic of Cyber-Resilient OPF

The model brings together three issues that affect how a power system responds to unexpected conditions. One is the reliability of the information used by the operator. Reported demand and forecast renewable generation may not match what is actually happening in the network, so these differences need to be considered when planning generation. Another issue is the amount of reserve available. Generators need enough flexibility to increase or decrease their output when demand or renewable production changes. The third issue is the transmission network itself. Having enough generation available does not always solve the problem, particularly when transmission lines are already operating close to their limits. For this reason, the model considers where generation and reserves are located, as well as how much capacity is available. False-data injection attacks can create problems by changing the load values used in dispatch calculations. For instance, if the reported demand is lower than the real demand, the OPF may schedule less generation than the system actually needs. Although this schedule may satisfy the calculations, it may not be suitable for the real operating conditions. The opposite can also happen. If an attacker increases the reported demand, the operator may schedule unnecessary generation, potentially increasing congestion on certain transmission lines. Both cases are included in the proposed model because the effect of an attack depends partly on whether the measurements are increased or decreased.

Errors in renewable generation forecasts can make these situations worse. If wind or solar production is lower than expected, conventional generators must supply the missing power. If production is higher than forecast, some generators may need to reduce their output. When these changes occur alongside a cyberattack, the combined effect can be greater than either problem considered separately. For example, a reduced load measurement and an overestimated renewable forecast could both lead to insufficient scheduled generation. The location of the affected buses also matters. A disturbance does not need to be particularly large to create difficulties if it causes additional power to flow through an already heavily loaded transmission line. To assess how well the proposed dispatch handles these situations, the study looks at the emergency actions required once actual conditions are known. Load shedding is assigned a high penalty because it means that part of the electricity demand cannot be supplied. The model also allows renewable generation to be curtailed, although this carries a smaller penalty. When no load shedding is needed across the tested scenarios, the result suggests that the scheduled generation and reserves are sufficient to handle the disturbances considered. This finding should

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

still be interpreted within the limits of the experiment. It shows that the approach can maintain feasible operation for the specified measurement and forecast errors, but it does not establish protection against cyberattacks outside those assumptions.

$$R_{\text{shed}} = 1 - \mathbb{P}(L_{\text{shed}} > 0), \qquad \text{EENS} = \mathbb{E}[L_{\text{shed}}] \times \Delta t$$

$$\text{Price}_{\text{of resilience}} = \frac{C^{\text{robust}}_{\text{preventive}} - C^{\text{det}}_{\text{preventive}}}{C^{\text{det}}_{\text{preventive}}}$$

Open Benchmark Data and Empirical Design

The empirical analysis uses the open PGLib-OPF benchmark library maintained by the IEEE PES Task Force on Benchmarks for Validation of Emerging Power System Algorithms. PGLib provides curated MATPOWER-format network, load, generation, branch-rating and cost data under a Creative Commons Attribution license (Babaeinejadsarookolaee et al., 2019). The reported computations use the v23.07 IEEE 14-bus and IEEE 30-bus cases. The benchmark files contain synchronous condensers with zero active-power capability; these units are retained in the network data conceptually but excluded from active-power dispatch because their Pmax is zero in the selected PGLib cases. Table 1 shows open benchmark system.

Table 1. Open benchmark systems and study modifications

Benchmark	Buses	Branches	Active P generators	Base load (MW)	Renewable forecast (MW)	Robust corner scenarios
IEEE 14-bus	14	20	2	259.0	46.62	16
IEEE 30-bus	30	41	2	283.4	51.012	64

Renewable generators are added as transparent study modifications rather than presented as original PGLib assets. Installed renewable capacity is set to 30% of system load and the nominal forecast is 60% of that capacity, giving forecast injections of 46.62 MW in the 14-bus system and 51.012 MW in the 30-bus system. In the 14-bus case renewable injections are placed at buses 9 and 14. In the 30-bus case they are placed at buses 7, 21 and 30. These locations create distributed injections without altering the original branch parameters. The cyber stress set targets high-demand buses because load corruption at these locations has a clear physical interpretation and produces nontrivial redispatch. Buses 3 and 4 are attackable in the 14-bus case. Buses 5, 8 and 7 are attackable in the 30-bus case. The main experiment bounds each attacked load measurement by plus or minus 15% and each renewable site by plus or minus 30% of its forecast. These are engineering stress-test ranges introduced by this study, not estimated historical attack distributions.

The deterministic model is used as a reference for comparison. It first calculates the generation schedule by the standard DC-OPF method. It then sets aside upward and downward reserves, each equal to 10% of the expected net demand. The problem with this approach is that reserves are allocated according to a general rule, without accounting for where measurement attacks or renewable forecast errors may occur in the network. The robust model takes a different approach by determining the reserve requirements from the combined uncertainty scenarios and the associated network constraints. To evaluate how both methods perform with actual disturbances, a separate linear optimization problem is solved with fixing the initial generation schedule and available reserves. This second problem minimizes generation costs while applying a penalty of 5,000 USD/MWh for involuntary load shedding and 5 USD/MWh for renewable curtailment.

The two approaches are tested using 3,000 out-of-sample scenarios for each network. In each scenario, every bus that can be attacked has an independent 55% probability of being affected, and at least one bus is required to be compromised. The amount of measurement corruption is selected from a triangular distribution within the specified attack limits. Its most likely value is slightly positive, making cases where actual demand is higher than reported demand somewhat more common. Renewable forecast errors are generated separately using a normal distribution with a mean of zero. The standard deviation is set to half of the specified uncertainty bound, and values outside that bound are excluded. These settings allow the two dispatch methods to be compared under a range of combined measurement attacks and renewable generation errors that were not used to determine the original schedules. The robust optimization itself does not use these distributions; it uses only the bounds. The random sampling is used solely to compare the frequency and magnitude of emergency actions after the schedules are fixed. The main empirical parameters are summarized in Table 2.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

Table 2. Main empirical parameters

Parameter	Value	Role
Cyber load-error bound	±15% on attackable bus demand	Stress-test parameter; robust set
Renewable-error bound	±30% of renewable forecast	Stress-test parameter; robust set
Deterministic reserve rule	10% of nominal net demand, up and down	Comparator, not a market standard
Robust reserve price	10% of marginal energy cost (up); 5% (down)	Prevention-cost weighting
Value of lost load	5,000 USD/MWh	Emergency feasibility penalty
Renewable curtailment penalty	5 USD/MWh	Emergency feasibility penalty
Monte Carlo scenarios	3,000 per benchmark	Out-of-sample evaluation

Empirical Results

The robust model produces almost the same initial generation schedule as the deterministic model. The main difference is the amount of reserve kept available to deal with unexpected changes. In the IEEE 14-bus system, both approaches schedule 212.38 MW from generator 1, while generator 2 produces no active power after the renewable forecast is taken into account. The reserve requirements are different. The deterministic approach uses the 10% rule and allocates 21.238 MW of reserve in each direction. The robust model requires 35.286 MW of upward and downward reserve. Even this increase, the total preventive cost is only 0.98% higher, mainly because reserve capacity is priced at a fraction of the generation cost.

The IEEE 30-bus case shows a clearer difference in how the two models allocate reserves. Both models use the same initial generation schedule, with 205.094 MW from generator 1 and 27.294 MW from generator 2. However, the deterministic model places all upward reserve at generator 1 and all downward reserve at generator 2. The robust model distributes these reserves differently. Generator 1 provides 6.356 MW of upward reserve, while generator 2 provides 30.997 MW. The full 37.354 MW of downward reserve is assigned to generator 1. Although the total upward reserve reaches 37.354 MW, the important difference is where that reserve is located. The results show that choosing generators based only on cost or total available capacity may not be sufficient when transmission constraints are present, also considering network limits, the robust model places reserves where they can support corrective changes in generation during disturbances. This is an important finding of the study, as it shows that improving system resilience depends not only on having more reserve capacity, but also on making sure that capacity can be used where it is needed. Table 3 as well as Figure 2 shows the 2 cases and some of the reserved results.

Table 3. Preventive dispatch and reserve results

Case	Det. preventive cost	Robust preventive cost	Premium	Det. up reserve	Robust up reserve	Det. down reserve	Robust down reserve
IEEE 14-bus	1707.49	1724.18	0.98%	21.238	35.286	21.238	35.286
IEEE 30-bus	5305.84	5410.27	1.97%	23.239	37.354	23.239	37.354

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

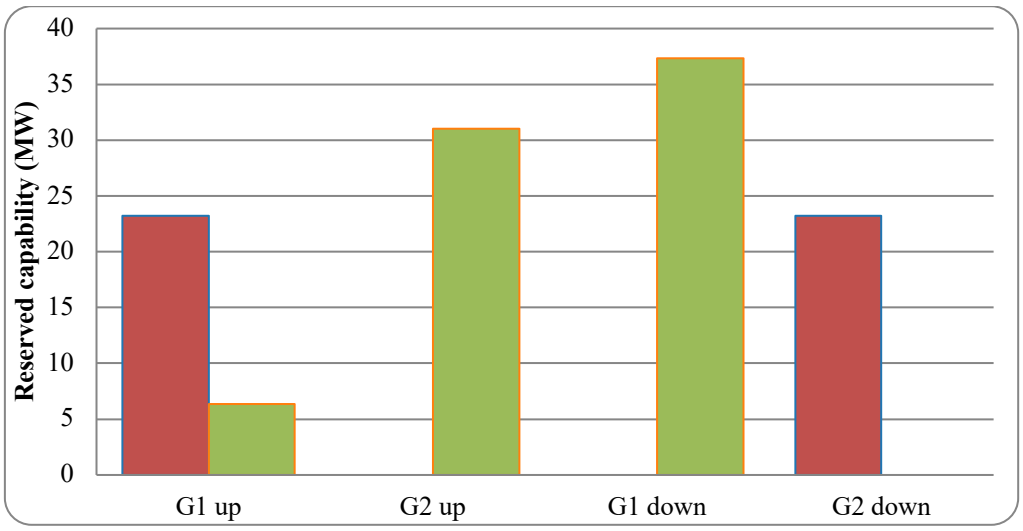

Figure 2. IEEE 30-bus reserve allocation. The robust solution redistributes upward corrective capability toward generator 2 instead of relying only on the cheapest generator.

The out-of-sample tests examine whether each model has enough reserve capacity to adjust generation when unexpected disturbances occur. In the IEEE 14-bus system, the deterministic approach handles most of the 3,000 test scenarios without difficulty, mainly because transmission congestion is relatively low under the modified operating conditions. However, load shedding is still needed in 10 scenarios, representing 0.33% of the total, with a maximum of 4.62 MW of unsupplied power. The robust model performs better in this comparison, as none of the 3,000 scenarios requires load shedding.

The contrast is much larger in the 30-bus system. Under the deterministic schedule, 62.77% of the 3,000 joint cyber-renewable samples require positive load shedding. Mean unserved power is 2.563 MW and the maximum reaches 18.931 MW. The deterministic schedule also curtails an average of 1.597 MW of renewable generation because the fixed reserve pattern cannot always absorb both positive and negative deviations while satisfying network constraints. In the robust solution, no load shedding or renewable curtailment is required in the sampled scenarios within the design bounds. Table 4 gifts the four bus cases and some of its parameterization.

Table 4. Out-of-sample physical resilience over 3,000 scenarios per case

Case	Schedule	P(load shed)	Mean shed (MW)	Max shed (MW)	Mean curtail. (MW)	Mean emergency objective
IEEE 14-bus	Deterministic	0.33%	0.006	4.620	-	1716.59
IEEE 14-bus	Robust	0.00%	0.000	0.000	-	1688.08
IEEE 30-bus	Deterministic	62.77%	2.563	18.931	1.597	17994.95
IEEE 30-bus	Robust	0.00%	0.000	0.000	0.000	5298.87

The emergency cost reported in Table 4 is mainly influenced by the high penalty assigned to load shedding. This means it should not be treated as an actual market cost or as the expected cost of producing electricity. Instead, it provides a way to compare how seriously each approach is affected when the system cannot meet demand within its operating limits. In the IEEE 30-bus case, the large difference between the two models comes from the deterministic approach having insufficient reserve capacity in the locations where it is needed. The results therefore show an improvement in the system's ability to handle disturbances, rather than a reduction in day-ahead electricity prices. Figure 3 presents the empirical cumulative distribution of load shedding of the IEEE 30 bus.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

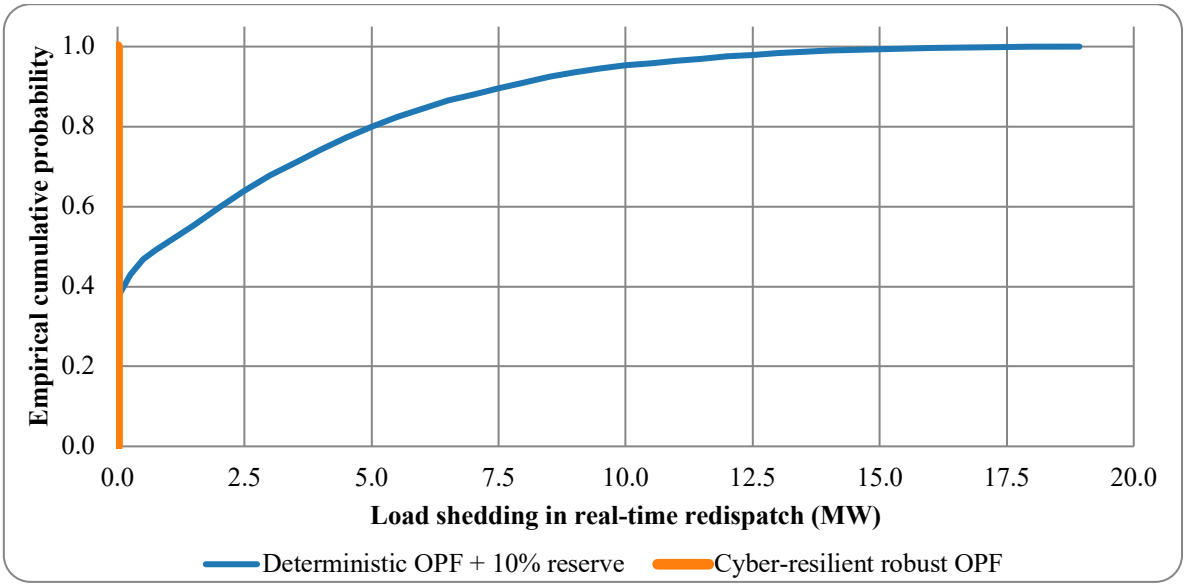

Figure 3. Empirical cumulative distribution of load shedding in the IEEE 30-bus out-of-sample experiment.

Sensitivity to Attack and Renewable Uncertainty

A sensitivity analysis was carried out on the IEEE 30-bus system using nine combinations of uncertainty limits. The measurement-corruption bound is varied between 5% and 15%, and the renewable forecast-error bound ranged from 10% to 30%. For each combination, the robust model is recalculated again and tested against all 64 corner scenarios. The deterministic model continued to use the same 10% reserve rule throughout the analysis. The results reveal a clear difference between the two approaches. With the deterministic model, the maximum amount of load shedding increases as either measurement corruption or renewable uncertainty becomes larger. When both uncertainties reach their highest levels, load shedding rises to 32.15 MW. The robust model, on the other hand, remains feasible in all tested corner scenarios because its reserve requirements are calculated using the selected uncertainty limits. As these limits increase, the amount of upward reserve also grows, from 12.45 MW with the lowest uncertainty levels to 37.35 MW under the conditions used in the main experiment.

The results also show that the robust approach is not always more expensive. When the level of uncertainty is low, it may cost slightly less than the deterministic model, as it requires less reserve than the fixed 10% rule. As measurement errors and renewable forecast uncertainty increase, the system needs more reserve to handle possible disturbances, which raises the cost. At the highest tested levels, with 15% measurement corruption and 30% renewable forecast error, the robust model costs 1.97% more than the deterministic approach. This shows that robust optimization is not simply about increasing reserve capacity. The model determines how much reserve is needed and where it should be placed, taking into account both the uncertainty and the limits of the transmission network. Table 5 gives the IEEE 30-bus sensitivity to joint uncertainty bounds. Figure 4 shows the worst case deterministic load shedding across the joint uncertainty grid.

Table 5. IEEE 30-bus sensitivity to joint uncertainty bounds

Cyber bound	Renewable bound	Det. corner cases with shedding	Det. worst-case shed (MW)	Robust upward reserve (MW)	Robust cost vs fixed-10% benchmark
5%	10%	54.7%	10.33	.12.45	-0.64%
5%	20%	62.5%	14.37	17.55	-0.12%
5%	30%	65.6%	18.40	22.65	0.40%
10%	10%	50.0%	16.63	19.80	0.14%
10%	20%	54.7%	20.66	24.90	0.66%
10%	30%	56.2%	25.07	30.00	1.18%

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

15%	10%	50.0%	23.08	27.15	0.92%
15%	20%	51.6%	27.62	32.25	1.45%
15%	30%	54.7%	32.15	37.35	1.97%

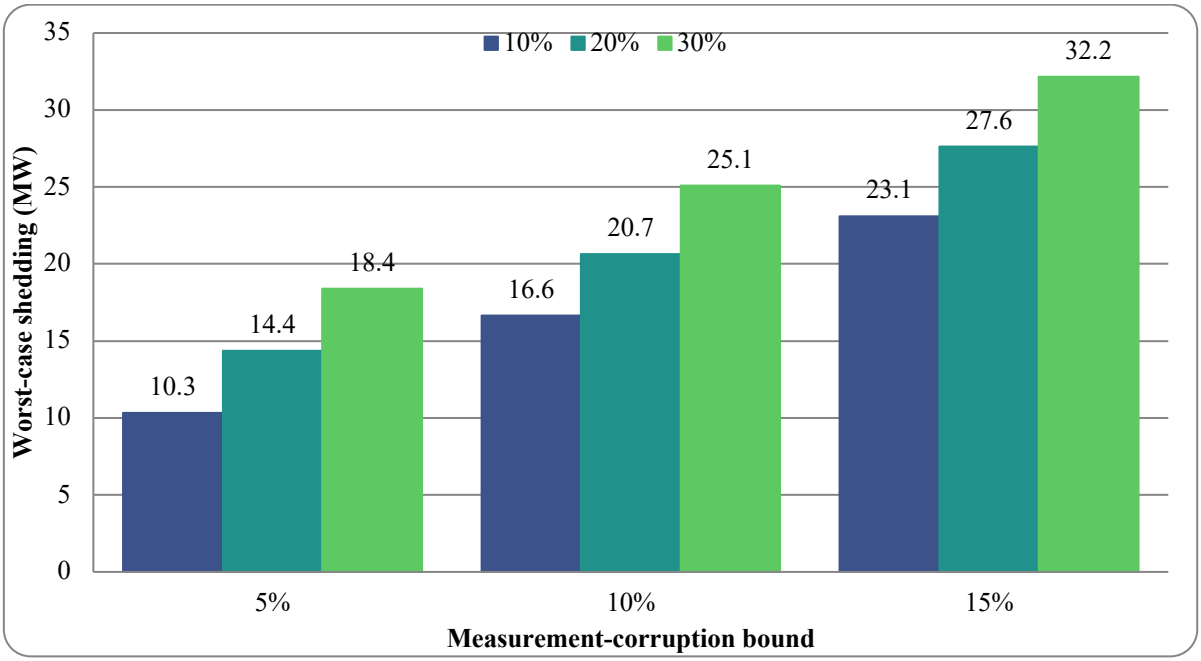

Figure 4. Worst-case deterministic load shedding across the joint uncertainty grid. The corresponding robust solutions have zero shedding at the design corners by construction.

Security and Control Interpretation

The results show why cybersecurity in power systems needs to consider more than whether an attack has been detected. Incorrect measurements become a problem when they influence decisions about how the physical network is operated. In OPF, for example, changes to reported demand can affect generator schedules, available reserves and power flows through transmission lines. Detecting suspicious measurements is important, but detection alone does not ensure that the system has enough reserve capacity to respond while the attack is still identified.

The idea behind the proposed model is to account for possible errors in the measurements before deciding how much power each generator should produce. If the measurement errors remain within the limits considered in the model, the generators should have enough reserve to adjust their output without cutting electricity supply. This applies to the simplified DC network used in the study. If an attack causes larger errors than expected, the model can no longer guarantee that load shedding will be avoided. However, the reserves may still help the system deal with the disturbance. The operator therefore needs to decide how much uncertainty to account for. Allowing for larger attacks usually means keeping more reserve available, which also increases operating costs.

The IEEE 30-bus experiment shows that the location of reserves matters as much as the amount available. Even if the generators have enough spare capacity in total, that power may not reach the buses where it is needed because some transmission lines are already close to their limits. The usual method of assigning a fixed percentage of reserve does not fully consider this issue. In the robust model, reserve allocation takes account of the network layout and transmission limits. This helps ensure that generators can adjust their output without overloading other parts of the network. The same problem can arise in larger power systems that use battery storage, controllable loads, phase-shifting transformers, HVDC connections or network switching. In all these cases, having spare capacity is only useful if the network can support the changes needed to manage a disturbance. Robust dispatch and attack detection can also work together. They address different parts of the same problem. Detection methods help identify measurements that may have been manipulated, while robust OPF helps the system operate when the available information is uncertain. One possible improvement would be to adjust the uncertainty limits according to how reliable each measurement appears to be. For

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

example, a sensor with a high confidence score could be assigned a smaller uncertainty range, while a less reliable measurement would receive a wider range. The OPF could then allocate additional reserves or adopt a more conservative operating schedule in parts of the network where the information is less trustworthy. In this case, the uncertainty bound would change with the confidence assigned to each measurement rather than remaining fixed.

Another limitation of the current model is that it considers only one operating period. In practice, cyberattacks and renewable generation changes can continue over several periods. Generators cannot always change their output immediately, and batteries must operate within their available state of charge. A small measurement error that continues over time could also influence several consecutive dispatch decisions without appearing particularly serious in any single period. Future work could therefore extend the model to multiple time steps, including generator ramp limits, battery energy constraints and changes in reserve availability over time. A rolling robust or distributionally robust model predictive control (MPC) approach would be worth investigating, as it could update the dispatch and uncertainty limits whenever new measurements become available.

Reproducibility, Scope and Limitations

The reported network data are traceable to PGLib-OPF v23.07. The empirical modifications - renewable placement, renewable penetration, cyberattack bounds, reserve-price weights and emergency penalties - are stated explicitly in Tables 1 and 2. The scenario generator and the optimization model are linear and can be reproduced in MATLAB, Julia, Python or another environment that supports linear programming. The PGLib cases are in MATPOWER format, which also permits direct validation against established power-system tools (Zimmerman et al., 2011).

The study has several limitations that should be considered when interpreting the results. First, it uses a DC power-flow model, which does not account for reactive power, voltage variations, losses or nonlinear AC behaviour. A schedule that satisfies DC constraints may therefore still violate some AC operating limits. Second, the attack model considers bounded measurement changes at selected load buses. It does not cover other threats, such as changes to network topology, breaker manipulation, GPS spoofing, communication failures or coordinated attacks designed to avoid detection. Third, renewable uncertainty is represented using predefined limits rather than actual forecast-error records. The results should therefore be viewed as a controlled stress test, not as an estimate of the risks faced by a real power system over a year.

The deterministic model is a fairly simple benchmark. It uses a fixed 10% reserve rule, which was chosen for this study rather than taken from the practice of a particular grid operator. The comparison helps show why the amount of reserve alone is not enough and why its location in the network also matters. The random distributions used to generate the test scenarios are also assumptions made for the experiment. The robust model does not rely on these distributions, provided the errors remain within the specified limits. Using different distributions might change how often load shedding occurs in the simulations, but the model would still remain feasible at the tested corner points. Future work may address these limitations extending the approach to AC optimal power flow, including N-1 security requirements and considering more complex cyberattack patterns. Renewable uncertainty could also be represented using historical forecast data and methods such as Wasserstein or moment-based ambiguity sets. Another possibility is to use confidence scores from attack-detection systems to adjust the uncertainty limits. These extensions would allow the model to better reflect real operating conditions and strengthen the connection between cybersecurity and power system control.

DISCUSSION

The main finding of this study is that cyber-resilient OPF helps maintain reliable power system operation when the available measurements may be incorrect. In both test networks, the initial generation schedules change very little. Therefore, comparing only generation costs would not show the main benefit of the robust approach. The difference is in the available reserves and where they are allocated. Under more demanding conditions, the robust model provides additional reserve capacity at generators that can respond without violating network limits.

The results also show that improving reliability comes at a cost. In the IEEE 30-bus experiment, the robust model increases preventive costs by 1.97% but avoids load shedding across the defined uncertainty set and all 3,000 sampled scenarios. This percentage depends on the network characteristics, generation costs, reserve prices and assumed uncertainty limits, so it should not be applied directly to other systems. However, the comparison shows how the additional cost of reserve capacity can be measured against the risk of insufficient power supply during disturbances.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

The large deterministic shedding frequency in the 30-bus experiment should also be interpreted carefully. It is not evidence that conventional OPF in real systems would shed load with similar frequency. Real operators use multiple reserve products, security constraints, state estimation, operator intervention and protection schemes. The experiment isolates one mechanism by comparing a generic aggregate reserve rule against a topology-aware robust design under deliberately simultaneous cyber and renewable disturbances. The high event frequency reveals the weakness of that simplified comparator under the chosen stress set, not a measured frequency of real blackouts.

CONCLUSION

This paper developed a robust optimal power flow approach that determines generation schedules and reserves while considering both corrupted load measurements and renewable generation uncertainty. The model accounts for possible measurement errors within defined limits and checks whether generation can be adjusted without violating network constraints under the extreme combinations of these uncertainties. Using open PGLib-OPF IEEE 14-bus and IEEE 30-bus benchmarks, the empirical study showed that the main operational benefit is not a radically different nominal dispatch but a different amount and spatial allocation of reserve. At the principal uncertainty bounds, robust preventive cost is 0.98% above the deterministic-reserve benchmark for the IEEE 14-bus case and 1.97% above it for the IEEE 30-bus case. In the 3,000 out-of-sample test scenarios, the robust model avoided load shedding as long as the disturbances remained within the defined limits. In comparison, the deterministic model required load shedding in 62.77% of the IEEE 30-bus scenarios, with a maximum of 18.93 MW. These results show why corrupted load measurements and renewable forecast errors should be considered together when planning power system operation. The performance of a cyber-resilient OPF should not be judged only by operating cost or the ability to detect attacks. It is also important to examine whether the system can adjust generation and continue operating within its physical limits when the available information is unreliable. Future work should consider AC power-flow constraints, attacks affecting a limited number of buses and uncertainty models based on actual renewable forecast data. The main aim remains to ensure that errors in the information used by the operator do not lead to serious problems in the physical power network.

REFERENCES

1. Babaeinejadsarookolaee, S., Birchfield, A., Christie, R. D., Coffrin, C., DeMarco, C., Diao, R., et al. (2019). The Power Grid Library for Benchmarking AC Optimal Power Flow Algorithms. arXiv:1908.02788. PGLib-OPF benchmark repository, version 23.07 used in this study.
2. Bertsimas, D., & Sim, M. (2004). The price of robustness. Operations Research, 52(1), 35-53. doi:10.1287/opre.1030.0065.
3. Calafiore, G. C., & El Ghaoui, L. (2006). On distributionally robust chance-constrained linear programs. Journal of Optimization Theory and Applications, 130(1), 1-22. doi:10.1007/s10957-006-9084-x.
4. Cheng, Z., & Chow, M.-Y. (2022). Resilient collaborative distributed AC optimal power flow against false data injection attacks: A theoretical framework. IEEE Transactions on Smart Grid, 13(1), 795-806. doi:10.1109/TSG.2021.3113287.
5. Dai, L., Xiao, H., & Yang, P. (2024). Robust optimal power flow considering uncertainty in wind power probability distribution. Frontiers in Energy Research, 12, 1402155. doi:10.3389/fenrg.2024.1402155.
6. Duan, J., Zeng, W., & Chow, M.-Y. (2018). Resilient distributed DC optimal power flow against data integrity attack. IEEE Transactions on Smart Grid, 9(4), 3543-3552. doi:10.1109/TSG.2016.2633943.
7. Esteban-Perez, A., & Morales, J. M. (2023). Distributionally robust optimal power flow with contextual information. European Journal of Operational Research, 306(3), 1047-1058. doi:10.1016/j.ejor.2022.10.024.
8. Hemmati, R., & Saboori, H. (2026). Distinguishing noise from low-amplitude false data in cyber-resilient rolling energy management of smart distribution networks. Energy Conversion and Management: X, 30, 101615. doi:10.1016/j.ecmx.2026.101615.
9. Huang, W., Qian, T., Tang, W., & Wu, J. (2025). A distributionally robust chance constrained optimization approach for security-constrained optimal power flow problems considering dependent uncertainty of wind power. Applied Energy, 383, 125264. doi:10.1016/j.apenergy.2024.125264.
10. Khanna, K., Panigrahi, B. K., & Joshi, A. (2017). Bi-level modelling of false data injection attacks on security constrained optimal power flow. IET Generation, Transmission & Distribution, 11(14), 3586-3593. doi:10.1049/iet-gtd.2017.0226.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 09 Issue 11 November 2026
DOI: 10.47191/ijcsrr/V9-i11-05, Impact Factor: 8.048
IJCSRR @ 2026
www.ijcsrr.org

11. Li, X., Yang, J., Du, D., Zhou, Z., Li, K., & Wu, L. (2025). Resilient distributed economic dispatch for cyber-physical power systems considering carbon emissions trading and false data injection attacks. Energy, 332, 136881. doi:10.1016/j.energy.2025.136881.
12. Liu, Y., Ning, P., & Reiter, M. K. (2009). False data injection attacks against state estimation in electric power grids. Proceedings of the 16th ACM Conference on Computer and Communications Security, 21-32. doi:10.1145/1653662.1653666.
13. Ou, W., Li, P., Weng, Z., Xiao, J., & Bai, X. (2026). Sinkhorn distributionally robust chance-constrained optimal power flow under renewable energy uncertainty. Electric Power Systems Research, 250, 112179. doi:10.1016/j.epsr.2025.112179.
14. Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. IEEE Transactions on Automatic Control, 58(11), 2715-2729. doi:10.1109/TAC.2013.2266831.
15. Roald, L., Misra, S., Krause, T., & Andersson, G. (2017). Corrective control to handle forecast uncertainty: A chance constrained optimal power flow. IEEE Transactions on Power Systems, 32(2), 1626-1637. doi:10.1109/TPWRS.2016.2602805.
16. Roald, L., & Andersson, G. (2018). Chance-constrained AC optimal power flow: Reformulations and efficient algorithms. IEEE Transactions on Power Systems, 33(3), 2906-2918. doi:10.1109/TPWRS.2017.2745410.
17. Zhang, Y., Shen, S., & Mathieu, J. L. (2017). Distributionally robust chance-constrained optimal power flow with uncertain renewables and uncertain reserves provided by loads. IEEE Transactions on Power Systems, 32(2), 1378-1388. doi:10.1109/TPWRS.2016.2572104.
18. Zimmerman, R. D., Murillo-Sanchez, C. E., & Thomas, R. J. (2011). MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. IEEE Transactions on Power Systems, 26(1), 12-19. doi:10.1109/TPWRS.2010.2051168.
19. Open Power System Data. (2020). Data Package Time Series, version 2020-10-06: load, wind and solar power generation and prices in hourly resolution. doi:10.25832/time_series/2020-10-06. (Relevant open source for future historical calibration; not used to produce the numerical values reported in the present PGLib stress test.)
20. Nikolov, N. (2024). Integration of renewable energy systems in the infrastructure of smart cities. Annual of Natural Sciences Department, 9, 44–52. doi:10.33919/ansd.24.9.5.

Data and reproducibility note: PGLib-OPF is available at https://github.com/power-grid-lib/pglib-opf. The empirical uncertainty distributions and all study-specific parameter values are defined explicitly in this article; renewable and cyber scenarios are reproducible stress-test modifications and are not claimed to be historical observations.

Cite this Article: Metodiev, V., Vasilev, I. (2026). Robust Optimal Power Flow under Industrial Cyberattacks and Renewable Uncertainty. International Journal of Current Science Research and Review, 9(11), pp. 5556-5567. DOI: https://doi.org/10.47191/ijcsrr/V9-i11-05