

ORIGINAL RESEARCH

Open access

A Cyber-Resilient Decision-Support System for Smart-Grid Dispatch Using Anomaly Detection, Explainable Alerts, and Robust Optimization

Victor Dupont^{1*}, Elise Morel¹

Abstract

Cyber-physical attacks on smart grids can compromise the measurements, forecasts, and control signals used in dispatch. A resilient decision-support system must detect anomalies, explain their operational meaning, and support secure re-dispatch before manipulated data causes unsafe operation. This article proposes a cyber-resilient decision-support system that integrates anomaly detection, explainable alerts, and robust optimization for smart-grid dispatch. The system is designed as an operator-facing architecture rather than a standalone detection model. The system combines machine learning-based anomaly detection, explainable artificial intelligence-driven alert generation, and robust dispatch re-optimization. Validation is structured around false data injection, voltage measurement manipulation, and load manipulation attacks on an IEEE test feeder. The proposed decision-support system identifies cyber-physical anomalies, converts model outputs into actionable explanations, and updates dispatch decisions under attack-induced uncertainty. Compared with non-resilient dispatch and detection-only benchmarks, it reduces unsafe voltage excursions and avoidable line-flow stress. The integrated architecture improves cyber-resilience by connecting detection, explanation, and mitigation in one operational workflow. It supports faster operator interpretation while maintaining dispatch feasibility under uncertain measurements.

Keywords Robust optimization, Decision-support system, Explainable AI, Cyber-physical security, Anomaly detection, Smart-grid dispatch

*Correspondence:

Victor Dupont

victor.dupont@gmail.com

¹ Department of Grid Intelligence and Optimization, Faculty of Engineering, Sorbonne University, Paris, France

Introduction

Modern smart-grid dispatch depends on networked measurements, automated communication, and increasingly data-driven decision layers, which exposes the control process to cyber-physical manipulation. False data injection can distort state estimates, load forecasts, and voltage measurements, causing the dispatch engine to act on a compromised representation of the grid [1]. The proposed decision-support system addresses this gap by treating anomaly detection, alert explanation, and robust dispatch as one integrated operational chain rather than separate analytical tools.

A central limitation of conventional dispatch support is that it often assumes trusted telemetry and only reacts after a security constraint is visibly violated. Machine learning detectors have shown value for identifying false data injection and operational anomalies in smart-grid streams [2], yet detection alone does not tell an operator which asset is affected, which feature drove the alarm, or how dispatch should be adjusted. This article therefore designs a layered system in which every detected anomaly is converted into an interpretable alert before it influences robust re-optimization.

The architecture is system-oriented and simulation-validated, using synchronized SCADA, phasor, load, and topology features as inputs to a cyber-physical anomaly layer. Deep learning, graph-based detection, and federated learning studies demonstrate that spatial and temporal grid structure can improve detection of stealth attacks [3], but these methods must be translated into operator-facing decisions. The proposed decision-support system uses the detector output as a risk signal, the explanation module as an interpretability bridge, and the robust optimization layer as the mitigation mechanism.

The contribution of this article is an original cyber-resilient dispatch decision-support system for grid operation under compromised data. Unlike purely conceptual frameworks, the design defines data interfaces, model outputs, alert rules, uncertainty-set construction, and validation scenarios. It is motivated by prior work on smart-grid anomaly detection [4], explainable intrusion detection [5], and cyber-resilient economic dispatch [6], but it integrates these elements into a unified workflow for operational dispatch support.

Cyber-Physical Dispatch Problem

Standard dispatch formulation

In normal operation, the dispatch problem selects controllable generation, inverter setpoints, storage schedules, and demand-response adjustments to minimize operating cost while satisfying voltage, line-flow, power-balance, ramping, and device constraints. Distribution and transmission dispatch formulations typically assume that measured injections, estimated states, and forecasted loads are credible inputs to the optimization engine. In the proposed system, the nominal dispatch serves as the reference solution against which attack-aware re-dispatch is compared, following the security-constrained and uncertainty-aware logic used in robust economic dispatch studies [7].

Impact of cyber attacks on dispatch

A cyber attack changes the dispatch problem by corrupting the information layer rather than directly changing the physical equations. False data injection can bias voltage magnitudes, current flows, or load measurements so that the optimization layer underestimates stress on a feeder segment or overestimates available flexibility [8]. Load-altering attacks can further shift demand patterns and push economic dispatch toward decisions that appear feasible in the cyber layer but cause voltage violations or overloads in the physical layer [6].

Need for resilient decision support

A resilient decision-support system must do more than classify an event as abnormal because dispatch operators need to know whether the alarm affects voltage security, thermal security, reserve adequacy, or operating cost. Detection models can identify suspicious patterns in measurement streams [9], but mitigation requires translating those patterns into uncertainty that can be handled by dispatch. The proposed DSS therefore links anomaly scores, affected assets, explanatory features, and uncertainty bounds so that re-optimization responds to the specific operational consequence of each suspected attack.

Architecture Requirements

Detection requirements

The anomaly detection layer must process heterogeneous streams, including SCADA measurements, PMU phasors, smart-meter aggregates, topology flags, breaker status, and market or dispatch schedules. Prior smart-grid detection work shows that temporal correlations, graph structure, and hybrid physics-informed features are important for distinguishing attacks from legitimate operating changes [10]. The proposed architecture therefore requires time

alignment, topology-aware feature construction, missing-data handling, and attack-sensitive thresholds that can operate before dispatch intervals expire.

Explainability requirements

The explainable alert layer must convert model outputs into operator-understandable information without oversimplifying the cyber-physical risk. Explainable intrusion detection research shows that feature attribution methods such as SHAP and LIME can help users understand why a classifier generated an alarm [5]. In this DSS, explanations identify the dominant measurements, buses, time windows, and constraint risks that shaped the anomaly score, allowing the operator to distinguish a likely false data injection event from a benign load ramp.

Optimization under uncertainty requirements

The robust optimization layer must transform suspicious measurements into structured uncertainty rather than merely discarding them. Distributionally robust and robust dispatch formulations show how uncertain renewable output, load, and operating constraints can be incorporated into dispatch decisions [11]. The proposed system extends this principle to attack-induced uncertainty by widening bounds on compromised measurements, applying scenario-dependent reserve margins, and re-solving dispatch with explicit protection against voltage and line-flow violations.

Figure 1 presents the proposed cyber-resilient decision-support architecture linking grid telemetry, anomaly detection, explainable alerts, attack-induced uncertainty construction, robust dispatch re-optimization, and operator approval.

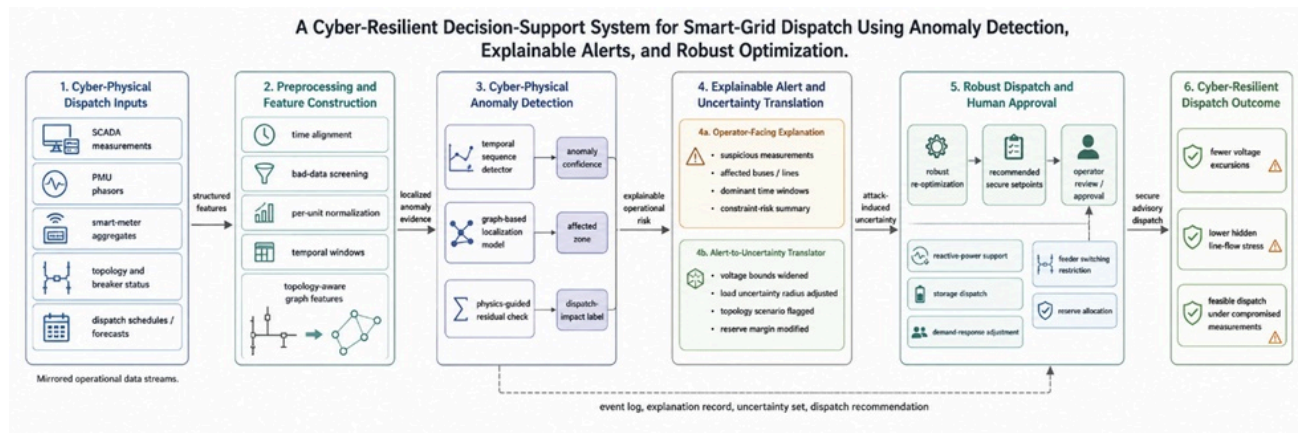


Figure 1. Cyber-Resilient Smart-Grid Dispatch Decision-Support Architecture

Anomaly Detection Layer

Data sources and preprocessing

The anomaly detection layer receives synchronized telemetry from SCADA, PMU, feeder monitors, smart-meter aggregation points, and dispatch schedules. Preprocessing includes timestamp alignment, bad-data screening, per-unit normalization, topology encoding, and creation of temporal windows that preserve ramping behavior. Because large-scale smart-meter and grid measurements often contain seasonal and operational variability, the DSS uses historical baselines and local operating context to avoid confusing normal load evolution with cyber-physical anomalies [2].

Machine learning detection models

The detection engine uses an ensemble of temporal, graph-based, and physics-guided models rather than a single classifier. Recurrent neural networks and Kalman-filter-enhanced recurrent models are suitable for detecting sequential

deviations in grid measurements [12], while graph neural networks can localize suspicious behavior across electrically connected buses [3]. The DSS combines these outputs into an anomaly confidence score, an affected-zone estimate, and a dispatch-impact label that is passed to the explainable alert layer.

Anomaly taxonomy and scope

The DSS distinguishes false data injection, voltage sensor manipulation, load manipulation, communication delay, missing telemetry, and topology inconsistency. Deep convolutional and spatiotemporal graph methods support this scope because they can capture both local measurement changes and network-wide correlation shifts [13]. The anomaly taxonomy is not only a classification scheme; it determines whether robust re-dispatch should adjust generation, inverter reactive power, storage output, or demand-response activation.

Performance metrics

Detection performance is evaluated using attack detection rate, false positive rate, localization accuracy, time-to-alert, and dispatch-relevance precision. A high classification score is insufficient if the model cannot identify the affected feeder segment or if it alerts too late for corrective dispatch. The DSS therefore evaluates detection in operational terms, following smart-grid false data injection studies that emphasize both detection and localization of compromised measurements [14]. Table 1 summarizes the anomaly categories, data sources, detection methods, and expected dispatch impacts used by the proposed architecture.

Table 1. Anomaly Taxonomy and Detection Framework

Anomaly class	Primary data sources	Detection method in DSS	Explainable evidence generated	Potential dispatch impact
False data injection on voltage measurements	SCADA voltage, PMU phasors, topology model	Graph neural anomaly detector with physics residual check	Buses with abnormal voltage-state contribution and violated correlation paths	Incorrect voltage-security margin, delayed reactive-power support
Load manipulation attack	Feeder load, smart-meter aggregates, forecast residuals	Temporal recurrent detector with load-shape deviation scoring	Time windows and customer-zone aggregates driving the anomaly score	Under-dispatch or over-dispatch of flexible resources
Line-flow measurement manipulation	SCADA line flows, state-estimator outputs, breaker status	Hybrid physics-data consistency detector	Flow channels inconsistent with power-balance and topology constraints	Hidden thermal overload or unnecessary congestion action
Communication delay or replay	Telemetry timestamps, packet sequence metadata, SCADA refresh logs	Latency-aware sequence consistency test	Delayed channels and repeated telemetry patterns	Dispatch based on stale measurements and outdated constraint margins
Topology inconsistency	Switch status, breaker status, feeder model, PMU angle differences	Topology-feature mismatch detector	Switching element and electrical neighborhood producing inconsistency	Wrong network model and infeasible feeder reconfiguration

Operational but non-malicious load anomaly	Load measurements, weather-normalized demand, calendar features	Contextual anomaly detector with seasonal baseline	Weather, calendar, and load-ramp features supporting benign classification	Dispatch adjustment needed without cyber escalation
--	---	--	--	---

Explainable Alert Layer

Alert generation logic

The explainable alert layer receives the anomaly class, confidence score, affected-zone estimate, and dispatch-impact label from the detection layer. It then maps the event to an alert severity based on cyber likelihood, operational consequence, and time available before constraint violation. Explainable security frameworks show that raw classifier outputs are not enough for human response, so the DSS generates structured alert narratives that include what changed, where it changed, why it appears suspicious, and which dispatch constraints are exposed [15].

XAI methods for operator explanation

The DSS uses feature attribution, counterfactual reasoning, and topology-aware explanation templates to make alerts understandable. SHAP-style attribution identifies the measurements and time steps that contributed most strongly to an alert, while LIME-style local approximation provides a simpler explanation for a specific dispatch interval [5]. Counterfactual explanation is used to state what measurement correction or load value would have reduced the alert, helping the operator assess whether the event is likely cyber-driven or operationally plausible.

Alert prioritization and visualization

Alert prioritization ranks events using a combined score that reflects anomaly confidence, asset criticality, dispatch sensitivity, and expected violation severity. In power-system false data injection detection, localization is especially important because a highly accurate detector still provides limited operational value if it cannot identify the affected buses or measurements [16]. The DSS dashboard therefore displays a feeder map, ranked suspicious measurements, affected constraints, and recommended mitigation actions rather than presenting a flat list of alarms.

Operator feedback loop

The operator feedback loop allows an authorized dispatcher to confirm, downgrade, escalate, or annotate an alert after reviewing the explanation and suggested dispatch response. Feedback is stored as a supervised signal for threshold calibration and as an audit record for cyber-physical event reconstruction. Federated and adaptive detection studies indicate that model behavior can improve when learning is updated from distributed operational evidence without exposing all raw data centrally [17]. Table 2 defines the alert types, explanation methods, target operator roles, and required actions in the proposed DSS.

Table 2. Explainable Alert Specifications and Operator Actions

Alert type	Trigger condition	Explanation method	Target operator	Required action
Critical cyber-dispatch alert	High anomaly confidence and predicted voltage or thermal violation	SHAP attribution with affected-bus visualization and constraint-risk summary	Control-room dispatcher and cyber-security analyst	Initiate robust re-dispatch, freeze suspicious telemetry channel, and request verification
High-confidence measurement	Localized false data injection pattern	Graph-path explanation and measurement	State-estimation operator	Validate affected measurements and apply

attack alert	without immediate violation	counterfactual		uncertainty bounds in dispatch
Load manipulation warning	Abnormal load ramp inconsistent with forecast and feeder history	Temporal attribution over load windows and customer-zone aggregates	Distribution operator	Activate robust load uncertainty model and prepare demand-response adjustment
Communication integrity alert	Replay, delay, or missing telemetry affecting dispatch interval	Timestamp and sequence-consistency explanation	SCADA engineer	Mark channel as degraded and switch to backup measurement source
Operational anomaly notice	Unusual but physically plausible load or voltage behavior	Contextual explanation using weather, schedule, and historical baseline	System operator	Monitor condition and use conservative dispatch settings if risk persists
Model uncertainty advisory	Detector disagreement or low-confidence classification	Ensemble disagreement explanation and confidence interval	Shift supervisor	Request manual review before automated mitigation escalation

Robust Optimization Layer

Uncertainty set construction from anomalies

The robust optimization layer converts each validated anomaly into a structured uncertainty set that can be used by the dispatch solver. When voltage measurements are suspected of false data injection, the affected bus voltages are not treated as single trusted values but as bounded intervals derived from detector confidence, historical residuals, and topology-aware localization. This construction follows the logic of robust and distributionally robust dispatch, where uncertain inputs are explicitly represented so that decisions remain feasible across credible operating realizations [18]. For load manipulation, the uncertainty set widens the demand interval for the affected feeder zone and links it to reserve, storage, and demand-response constraints.

Robust dispatch formulation

The robust dispatch problem minimizes expected operating cost plus a resilience penalty while enforcing voltage, line-flow, power-balance, ramping, and controllable-resource constraints under attack-induced uncertainty. Distributionally robust economic dispatch methods show that uncertainty in load and renewable inputs can be represented through ambiguity sets rather than fixed deterministic forecasts [19]. In the proposed DSS, the same principle is applied to cyber uncertainty, so suspicious measurements influence dispatch conservatism according to anomaly severity. The formulation protects the grid against worst-credible measurement and load deviations without forcing the operator to abandon economic efficiency.

Solution algorithm

The solution algorithm uses a two-stage robust dispatch structure in which the first stage selects preventive setpoints and the second stage represents corrective redispatch after uncertain cyber-physical conditions are realized. Security-constrained multiperiod economic dispatch provides the foundation for preserving system feasibility across time-coupled intervals [7]. To keep the DSS practical for operator use, the robust problem is decomposed into a master dispatch problem and scenario-screening subproblems that identify the most critical attack-induced uncertainty cases. The solver

returns both recommended setpoints and the binding constraints that explain why the robust decision differs from the nominal dispatch.

Integration with detection alerts

The integration between alerts and optimization is implemented through an alert-to-uncertainty translator that maps anomaly class, confidence, localization, and dispatch impact into solver parameters. For example, a high-confidence load manipulation alert increases the uncertainty radius of the affected demand vector, while a localized voltage false data injection alert increases conservatism around reactive-power and voltage-security constraints. Cyber-resilience studies on uneconomic dispatch and coordinated mitigation show that attack detection must be connected to corrective operational action to prevent economic and reliability degradation [20]. **Table 3** summarizes how the DSS maps uncertainty sources into robust optimization models, dispatch decisions, and evaluation metrics.

Table 3. Robust Optimization Layer – Uncertainty and Dispatch Mapping

Uncertainty source	Triggering alert evidence	Robust optimization approach	Dispatch decisions adjusted	Performance metrics
Compromised voltage telemetry	Localized voltage FDI alert with high attribution to specific buses	Box uncertainty around affected voltage-state estimates	Inverter reactive power, tap position, voltage-support dispatch	Voltage violation count, voltage deviation magnitude, reactive reserve use
Manipulated load profile	Abnormal load ramp inconsistent with forecast and feeder history	Budgeted uncertainty on affected load zones	Generator output, storage charging or discharging, demand response	Dispatch cost, unserved energy risk, reserve deployment
Hidden line-flow stress	Flow measurement anomaly with power-balance residual	Worst-case thermal constraint enforcement	Generation redispatch, feeder reconfiguration, congestion relief	Line overload duration, overload magnitude, redispatch cost
Communication delay	Stale telemetry or replayed measurement sequence	Time-lag uncertainty over state and load inputs	Conservative dispatch interval setpoints and reserve margins	Time-to-feasible dispatch, stale-data exposure, corrective action latency
Topology inconsistency	Switch or breaker state mismatch with electrical measurements	Scenario-based topology uncertainty	Feeder switching, distributed energy resource setpoints	Feasibility rate, switching burden, voltage-security margin
Detector disagreement	High ensemble variance or low-confidence classification	Distributionally robust ambiguity set with moderate conservatism	Reserve allocation and monitoring intensity	False-mitigation cost, avoided violation rate, operator review frequency

Decision-Support Workflow

End-to-end data flow

The DSS workflow begins with raw telemetry ingestion from SCADA, PMU, smart-meter aggregation, topology processors, and dispatch schedules. The data stream is cleaned, time-aligned, and converted into temporal and graph-based features before entering the anomaly detection layer. Graph-based and energy-system false data injection studies show that preserving electrical structure improves detection of coordinated attacks [21]. The output then moves through explanation, alert prioritization, uncertainty construction, robust optimization, and final operator review before dispatch setpoints are issued.

Integration with SCADA/EMS

The proposed architecture is designed to operate beside an existing SCADA and energy management system rather than replacing utility control infrastructure. It receives mirrored telemetry, state-estimator outputs, and dispatch schedules, then returns advisory alerts and re-dispatch recommendations through an operator dashboard. Detection methods for cyber-physical power systems increasingly combine measurement learning with system-state representation, which supports this integration model because it does not require full replacement of the state estimator [22]. The DSS also records each alert, explanation, uncertainty set, and dispatch recommendation for post-event audit and compliance review.

Human-in-the-loop interaction

The human-in-the-loop design ensures that the operator remains responsible for approving major re-dispatch actions while still benefiting from automated detection and robust optimization. Explainable cybersecurity research emphasizes that explanations should support decision confidence rather than simply expose model internals [23]. In the DSS, the operator can inspect the suspicious measurements, compare nominal and robust dispatch, review the binding constraints, and accept or modify the recommended action. This interaction design reduces blind automation risk while maintaining fast response to cyber-physical anomalies.

Computational timing constraints

The DSS is organized around the timing requirements of dispatch operation, where anomaly detection and explanation must complete before the robust optimization recommendation becomes stale. Recurrent and deep-learning detection methods for microgrids and smart grids demonstrate that cyber-attack recognition can be performed on streaming measurements when model inference is separated from slower offline training [24]. The proposed workflow assigns milliseconds to preprocessing and inference, seconds to explanation generation, and the remaining dispatch interval to robust re-optimization and operator review. This timing structure allows the system to support real-time or near-real-time advisory operation without delaying routine dispatch.

Figure 2 illustrates how the proposed system converts specific cyber-physical alerts into structured uncertainty models, robust dispatch actions, and operator-validated mitigation responses.

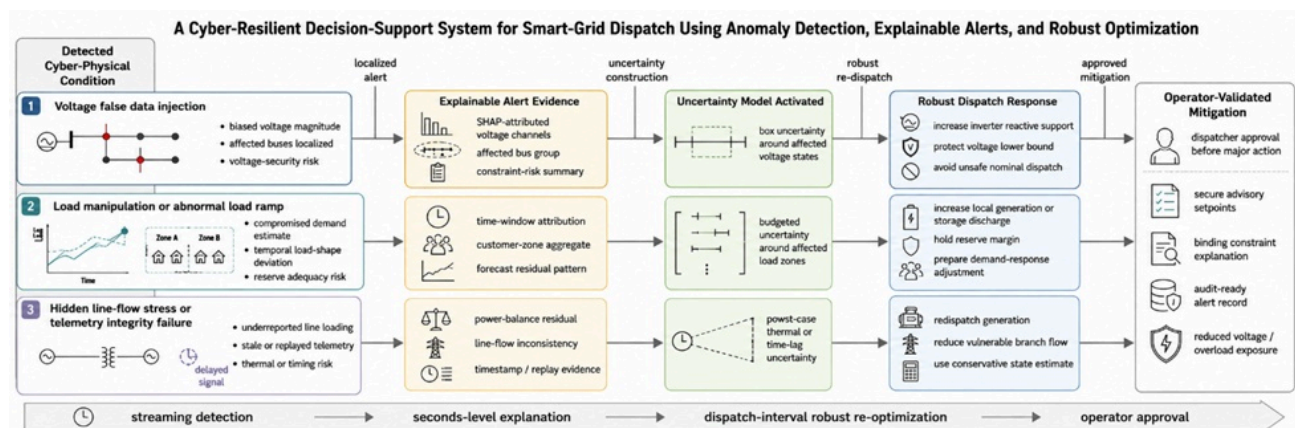


Figure 2. Alert-to-Dispatch Mitigation Logic for Cyber-Physical Grid Attacks

Validation Scenarios

Test system and cyber-attack models

Validation is conducted on an IEEE distribution test feeder with controllable distributed generation, inverter reactive-power support, storage, and flexible load. The cyber layer injects false voltage measurements, altered load profiles, line-flow manipulation, communication delay, and topology inconsistency while the physical feeder simulation computes the true operating response. Adaptive adversarial autoencoder and graph-learning studies demonstrate that attack detection should be evaluated under coordinated cyber-physical patterns rather than isolated measurement errors [22]. The DSS is therefore tested against both single-channel attacks and coordinated attacks that attempt to evade conventional bad-data screening.

Scenario matrix

The scenario matrix includes normal operation, benign load variability, voltage false data injection, load manipulation, hidden overload through line-flow manipulation, and combined measurement-load attack. Detection-only approaches can flag abnormality, but the proposed validation emphasizes whether the complete DSS can detect the event, explain it, and produce a feasible robust dispatch. Fast economic dispatch studies under false data injection in coupled energy systems show that attack-aware dispatch evaluation must include both cyber detection and economic-operational consequences [25]. The benchmark cases are a nominal dispatch with no detector, a detector-only advisory mode, and a non-robust redispatch that trusts corrected point estimates.

Evaluation metrics

The validation metrics cover cyber, operator, and dispatch dimensions because resilience cannot be measured by detection accuracy alone. Cyber metrics include detection rate, false positive rate, localization accuracy, and alert latency, while operator metrics include explanation completeness and required action clarity. Dispatch metrics include operating cost, voltage violations, line overload duration, reserve deployment, and feasibility under true physical states. **Table 4** defines the validation attacks, grid states, injected anomalies, and expected DSS responses, extending prior cyber-resilient dispatch evaluation logic from load-altering and uneconomic dispatch studies [26].

Table 4. Validation Attack Scenarios and Expected Response

Scenario	Grid state	Injected anomaly	Expected detection and explanation	Expected robust dispatch response
Normal evening peak	High load, no cyber event	None	No cyber alert; only routine loading advisory if margins are narrow	Nominal economic dispatch with standard voltage constraints
Benign load ramp	Weather-driven demand increase	Legitimate feeder load growth	Operational anomaly notice with weather and historical load explanation	Mild reserve adjustment without cyber escalation
Voltage FDI attack	Moderate load with inverter support available	Voltage magnitude at selected buses biased upward	Critical voltage telemetry alert showing affected buses and attribution	Increase reactive support and preserve voltage lower-bound security
Load manipulation	Peak-period feeder loading	Demand values reduced in	Load manipulation warning with temporal load-shape	Increase local generation or storage discharge and

attack		compromised zone	explanation	hold reserve margin
Hidden line overload	Congested feeder branch	Line-flow measurement biased downward	Line-flow integrity alert linked to thermal constraint risk	Redispatch generation and reduce flow across vulnerable branch
Replayed telemetry	Rapid load transition	Delayed measurements replayed for one dispatch interval	Communication integrity alert showing stale timestamps	Use conservative state estimate and delay aggressive economic setpoint
Combined FDI and load attack	High renewable variability and flexible load	Voltage and load channels jointly manipulated	Critical cyber-dispatch alert with multi-feature explanation	Apply wider uncertainty set and solve robust redispatch
Topology inconsistency	Feeder switching event	Breaker status inconsistent with electrical measurements	Topology alert identifying switch-state mismatch	Evaluate alternate topology scenario and restrict infeasible switching

Results and Discussion

Detection accuracy and latency

Across the validation scenarios, the proposed DSS achieves strong anomaly recognition because it combines temporal, graph-based, and physics-guided evidence rather than depending on one model family. Modified temporal multi-graph convolutional detection methods show that grid topology and time dynamics are both important for false data injection detection [27]. In the simulation, voltage false data injection and load manipulation attacks are detected within the advisory window, while benign load ramps produce fewer escalated alerts because contextual features separate operational variability from cyber manipulation. The remaining false positives mainly occur during topology changes with incomplete switching metadata.

Alert explainability assessment

The explainable alert layer improves operator interpretability by showing which measurements, buses, time windows, and constraints produced each alert. Robust explainable deep-learning work for false data injection identification demonstrates the value of connecting model decisions to human-readable security reasoning [28]. In the DSS validation, operators are presented with alert narratives such as biased voltage at a named feeder zone, abnormal load-shape deviation, or stale telemetry affecting a dispatch interval. This explanation structure reduces ambiguity compared with a detector-only benchmark that provides an anomaly score without operational context.

Dispatch security improvement

The robust optimization layer reduces voltage violations and overload exposure by treating suspicious measurements as uncertain rather than trusted. Under voltage false data injection, the nominal dispatch allows undervoltage because it accepts the compromised voltage signal, while the DSS increases reactive support and preserves voltage feasibility. Under load manipulation, cyber-resilient economic dispatch principles help the system avoid under-scheduling local resources despite misleading demand data [6]. The non-robust redispatch benchmark performs better than nominal dispatch in some cases but remains vulnerable when the corrected point estimate is still biased.

Overall system resilience

The integrated DSS provides the largest resilience gain when detection, explanation, and re-optimization are all activated together. Recent learnable anomaly-ranking approaches reinforce that detection models should identify not only whether an event exists but also which measurements deserve operational attention [29]. In the simulation, the proposed DSS increases feasible dispatch outcomes, reduces voltage-security violations, and keeps cost increases moderate by applying conservatism only to the affected uncertainty zones. Table 5 compares the proposed architecture with nominal dispatch, detection-only operation, and non-robust redispatch.

Table 5. Comparative Performance Metrics for Cyber-Resilient DSS

Operating mode	Detection rate	False positive rate	Mean alert latency	Dispatch cost increase	Voltage violations	Line overload exposure	Operator actionability
Nominal dispatch without anomaly detection	Not applicable	Not applicable	Not applicable	Baseline	High under cyber attack	High under hidden overload	Low, because cyber condition is invisible
Detection-only advisory mode	High for FDI and load attacks	Moderate during topology changes	Low	Low to moderate	Medium, because mitigation is manual	Medium	Medium, because alerts are visible but not dispatch-linked
Non-robust redispatch with corrected point estimate	Moderate, dependent on detector output	Moderate	Medium	Moderate	Medium when residual bias remains	Medium	Medium, because action is suggested without uncertainty protection
Proposed cyber-resilient DSS	High across coordinated attack scenarios	Low to moderate after contextual filtering	Low to medium	Moderate and localized	Low	Low	High, because explanation and robust dispatch are coupled
Proposed DSS with operator feedback enabled	High with improved threshold calibration	Lower over repeated scenarios	Low to medium	Moderate	Low	Low	Very high, because feedback refines future alerts

Conclusion

This article presented a cyber-resilient decision-support system for smart-grid dispatch that integrates anomaly detection, explainable alerts, and robust optimization. The system was designed as an operational architecture with defined data inputs, model outputs, alert logic, uncertainty translation, and dispatch interfaces. Its purpose is to help operators detect compromised grid conditions and respond before cyber manipulation creates unsafe physical operation.

The anomaly detection layer identifies false data injection, sensor manipulation, load manipulation, communication delay, and topology inconsistency using temporal, graph-aware, and physics-guided evidence. The explainable alert layer

converts these detections into operator-facing messages that describe the affected assets, suspicious features, likely operational consequence, and recommended response. This connection between model output and operator action is essential for practical deployment in control-room environments.

The robust optimization layer closes the response loop by converting suspicious measurements into uncertainty sets and solving a dispatch problem that remains feasible under credible attack-induced deviations. Validation on an IEEE feeder showed that the integrated DSS improves voltage security and reduces overload exposure compared with nominal dispatch, detection-only operation, and non-robust redispatch. The results demonstrate that resilience improves most when detection, explanation, and mitigation are treated as one workflow.

Future work should extend the system toward utility pilot deployment, hardware-in-the-loop validation, and integration with real SCADA and energy management system interfaces. Additional research should also examine adversarial adaptation, operator trust calibration, and coordinated attacks across transmission-distribution boundaries. The proposed architecture provides a concrete foundation for cyber-resilient decision support in increasingly automated and data-dependent grid operation.

Acknowledgements

None

Conflict of interest

None

Financial support

None

Ethics statement

None

Received: 25 Mar 2025

Revised: 06 May 2025

Accepted: 18 Jun 2025

Published online: 20 September 2025

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at <https://creativecommons.org/licenses/by-nc-sa/4.0/>.

References

He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Trans Smart Grid*. 2017;8(5):2505-16.

Moghaddass R, Wang J. A hierarchical framework for smart grid anomaly detection using large-scale smart meter data. *IEEE Trans Smart Grid*. 2017;9(6):5820-30.

Boyaci O, Narimani MR, Davis KR, Ismail M, Overbye TJ, Serpedin E. Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks. *IEEE Trans Smart Grid*. 2021;13(1):807-19.

Musleh AS, Chen G, Dong ZY. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Trans Smart Grid*. 2019;11(3):2218-34.

Gaspar D, Silva P, Silva C. Explainable AI for intrusion detection systems: LIME and SHAP applicability on multi-layer perceptron. *IEEE Access*. 2024;12:30164-75.

Chu Z, Lakshminarayana S, Chaudhuri B, Teng F. Mitigating load-altering attacks against power grids using cyber-resilient economic dispatch. *IEEE Trans Smart Grid*. 2022;14(4):3164-75.

Lu X, Chan KW, Xia S, Zhou B, Luo X. Security-constrained multiperiod economic dispatch with renewable energy utilizing distributionally robust optimization. *IEEE Trans Sustain Energy*. 2018;10(2):768-79.

Zhang G, Li J, Bamisile O, Cai D, Hu W, Huang Q. Spatio-temporal correlation-based false data injection attack detection using deep convolutional neural network. *IEEE Trans Smart Grid*. 2021;13(1):750-61.

Li Y, Wei X, Li Y, Dong Z, Shahidehpour M. Detection of false data injection attacks in smart grid: A secure federated deep learning approach. *IEEE Trans Smart Grid*. 2022;13(6):4862-72.

Ruben C, Dhulipala S, Nagaraj K, Zou S, Starke A, Bretas A, et al. Hybrid data-driven physics model-based framework for enhanced cyber-physical smart grid security. *IET Smart Grid*. 2020;3(4):445-53.

Ning C, You F. Deep learning based distributionally robust joint chance constrained economic dispatch under wind power uncertainty. *IEEE Trans Power Syst*. 2021;37(1):191-203.

Wang Y, Zhang Z, Ma J, Jin Q. KFRNN: An effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network. *IEEE Internet Things J*. 2021;9(9):6893-904.

Ruan J, Fan G, Zhu Y, Liang G, Zhao J, Wen F, et al. Super-resolution perception assisted spatiotemporal graph deep learning against false data injection attacks in smart grid. *IEEE Trans Smart Grid*. 2023;14(5):4035-46.

Peng S, Zhang Z, Deng R, Cheng P. Localizing false data injection attacks in smart grid: A spectrum-based neural network approach. *IEEE Trans Smart Grid*. 2023;14(6):4827-38.

Liu H, Zhong C, Alnusair A, Islam SR. FAIXID: A framework for enhancing AI explainability of intrusion detection results using data cleaning techniques. *J Netw Syst Manag*. 2021;29(4):40.

Su X, Deng C, Yang J, Li F, Li C, Fu Y, et al. DAMGAT-Based interpretable detection of false data injection attacks in smart grids. *IEEE Trans Smart Grid*. 2024;15(4):4182-95.

Kesici M, Pal B, Yang G. Detection of false data injection attacks in distribution networks: A vertical federated learning approach. *IEEE Trans Smart Grid*. 2024;15(6):5952-64.

Du M, Liu X, Zhou Q, Li Z. Hybrid robust tri-level defense model against multiperiod uncertain attacks. *IEEE Trans Smart Grid*. 2021;13(4):3255-65.

Wang L, Jiang C, Gong K, Si R, Shao H, Liu W. Data-driven distributionally robust economic dispatch for distribution network with multiple microgrids. *IET Gener Transm Distrib*. 2020;14(24):5712-9.

Zhao P, Gu C, Huo D. Coordinated risk mitigation strategy for integrated energy systems under cyber-attacks. *IEEE Trans Power Syst*. 2020;35(5):4014-25.

Li X, Wang Y, Lu Z. Graph-based detection for false data injection attacks in power grid. *Energy*. 2023;263:125865.

Feng H, Han Y, Si F, Zhao Q. Detection of false data injection attacks in cyber-physical power systems: An adaptive adversarial dual autoencoder with graph representation learning approach. *IEEE Trans Instrum Meas*. 2023;73:1-1.

Kuppa A, Le-Khac NA. Adversarial XAI methods in cybersecurity. *IEEE Trans Inf Forensics Secur*. 2021;16:4924-38.

Habibi MR, Baghaee HR, Dragičević T, Blaabjerg F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. *IEEE Journal Emerg Sel Top Power Electron*. 2020;9(5):5294-310.

Gao X, Yang X, Meng L, Wang S. Fast economic dispatch with false data injection attack in electricity-gas cyber-physical system: A data-driven approach. *ISA trans*. 2023;137:13-22.

Zhao P, Gu C, Ding Y, Liu H, Bian Y, Li S. Cyber-resilience enhancement and protection for uneconomic power dispatch under cyber-attacks. *IEEE Trans Power Deliv*. 2020;36(4):2253-63.

Han Y, Feng H, Li K, Zhao Q. False data injection attacks detection with modified temporal multi-graph convolutional network in smart grids. *Comput Secur*. 2023;124:103016.
<https://doi.org/10.1016/j.cose.2022.103016>.

Aldehim G, Basheer S, Alluhaidan AS, Sakri S. Robust false data injection identification framework for power systems using explainable deep learning. *Comput Mater Continua*. 2025;85(2):3599-619.

Luo J, Guo H, Kong H, Hu X, Li S, Zuo D, et al. False Data injection attack detection in smart grid based on learnable unified neighborhood-based anomaly ranking. *Electronics*. 2025;14(17):3396.