



Cyber Security Issues in High Renewable Penetration Grid from a Voltage Stability Perspective

K. Poli Naidu^{1*}, S. Sushma¹, P. Karthik¹

¹Department of Electrical and Electronics Engineering, GMR Institute of Technology Deemed to be University, Rajam, India

*Email: 23341a0270@gmr.it.edu.in

DOI : <https://doi.org/10.55248/gengpi.07.0926.3113>

ABSTRACT—

The increasing penetration of solar photovoltaic (PV), wind generation, and other inverter-based resources is changing the operating characteristics of modern power grids. At the same time, monitoring, protection, voltage-control, and energy-management functions are becoming increasingly dependent on digital communication and control infrastructure. This integration creates a cyber-physical environment in which a cyberattack can propagate into the physical power system and potentially influence its stability [7], [10]. False data injection attacks (FDIAs) are particularly important because manipulated measurements can influence state estimation and control decisions while remaining difficult to detect using conventional residual-based methods [1], [4]. Other threats, including denial-of-service, replay, man-in-the-middle, and malicious command attacks, can also interfere with measurements, communication, or control functions [8], [10]. This paper reviews cybersecurity issues in high-renewable-penetration grids from a voltage-stability perspective. Existing statistical, machine-learning, deep-learning, graph-based, and localization-oriented detection methods are examined [3], [5], [7], [9]. The review emphasizes the increasing need for topology-aware and stability-oriented detection methods, while also highlighting several limitations, including reliance on benchmark systems, simplified cyber-network models, limited validation using real-world data, challenges posed by adaptive attacks, and the impact of converter-driven stability issues [10]. Finally, a conceptual framework integrating cyberattack detection, localization, voltage-stability assessment, and risk-aware mitigation is proposed.

Index Terms— Cybersecurity, false data injection attack, voltage stability, renewable energy, inverter-based resources, smart grid, cyber-physical power system, machine learning, graph-based detection.

I. INTRODUCTION

The transition toward renewable-energy-based electricity generation has significantly changed the structure and operating environment of modern power systems. Solar photovoltaic (PV), wind generation, energy storage, and other inverter-based resources are increasingly integrated into electrical networks. Unlike conventional synchronous generators, many renewable resources are connected through power-electronic interfaces, creating additional interactions between converter controls, network conditions, and other power-system components [10].

The increasing digitalization of the grid has occurred alongside this transition. Supervisory Control and Data Acquisition (SCADA), Phasor Measurement Units (PMUs), Energy Management Systems (EMS), communication networks, intelligent controllers, and wide-area monitoring systems enable operators to obtain more detailed and timely information about the operating condition of the power grid [10]. Voltage-regulating equipment such as capacitor banks, voltage regulators, on-load tap changers (OLTCs), SVC/VAR compensators, and smart inverters are also increasingly connected to communication networks [7].

This connectivity improves monitoring and control, but it also expands the potential cyberattack surface. A modern power system therefore cannot be considered purely as an electrical network; it is a cyber-physical system in which cyber events can produce physical disturbances [10].

False data injection attacks represent one of the major cybersecurity concerns in this environment. An FDIA modifies power-system measurements so that the control center receives incorrect information [1]. Such manipulation can affect state estimation, observability, topology processing, contingency analysis, optimal power flow, automatic generation control, and other power-system functions [1].

The problem becomes more serious when an attacker deliberately designs an attack to influence a physical stability condition. Liang et al. showed that a suitably constructed FDIA can alter the estimated system state while remaining difficult to identify using conventional bad-data detection methods [4]. Jafari et al. Further studies have examined FDIAs that are specifically designed to influence small-signal stability [2]. In recent years, research has increasingly shifted toward data-driven and topology-aware detection methods. Statistical techniques have been evaluated using real PMU data [3], while machine-learning methods have been extensively surveyed for FDIA detection [5]. More recent work has combined graph-based learning and

temporal modeling to detect FDIAs targeting voltage stability [7]. Other research has investigated localization of compromised buses and measurements [9].

However, important challenges remain. Existing studies often rely on simulated attacks, conventional benchmark systems, and simplified representations of the cyber layer [10]. In addition, cybersecurity research specifically addressing converter-driven stability remains comparatively limited [10].

Accordingly, this review examines cybersecurity threats from the perspective of voltage stability in high-renewable-penetration grids. The principal objectives of this study are:

1. To identify the major cybersecurity threats that can affect voltage stability in high-renewable-penetration power systems.
2. To review existing approaches for the detection and localization of False Data Injection Attacks (FDIAs) in power systems.
3. To examine the application of machine learning and graph-based techniques for improving the detection and analysis of cyber threats affecting voltage stability.
4. To identify research gaps associated with renewable-rich and converter-dominated systems.
5. To propose a conceptual cybersecurity–voltage-stability framework.

II. HIGH-RENEWABLE-PENETRATION POWER GRIDS AND VOLTAGE STABILITY

A. Increasing Renewable Penetration

High renewable penetration introduces a greater proportion of inverter-based resources into the power system. Solar PV and wind generation commonly depend on power-electronic converters, making their behavior closely associated with converter controls and grid conditions [10].

The digital control of voltage-regulating equipment further increases the interaction between the physical and cyber layers. Capacitor banks, voltage regulators, OLTCs, SVC/VAR compensators, and smart inverters can be connected to communication infrastructure and remotely controlled [7].

Consequently, the reliability of the physical power system increasingly depends on the availability and integrity of cyber information. This creates a requirement for cybersecurity mechanisms that consider not only information security but also the possible physical consequences of compromised measurements or controls.

B. Inverter-Based Resources and Converter-Driven Stability

The behavior of renewable-rich grids differs from that of traditional generator-dominated systems because of the increasing presence of power-electronic interfaces. Solar PV, wind generation, HVDC systems, and other converters introduce additional dynamic interactions [10].

The reviewed stability literature identifies converter-driven stability as a comparatively new research area. Although the penetration of converter-based resources is increasing, research specifically investigating cyberattacks against converter-driven stability remains limited [10].

This gap is important because a cyberattack affecting converter measurements or control signals may produce physical behavior that cannot be adequately represented using conventional synchronous-machine-based assumptions.

C. Voltage Stability

Voltage stability is the ability of a power system to maintain acceptable bus-voltage conditions following a disturbance [10]. Voltage instability may result in voltage fluctuations, under-voltage or over-voltage conditions, line tripping, loss of load, cascading failures, and voltage collapse [10].

Voltage stability can be influenced by physical conditions such as system overloading, reactive-power limitations, and equipment failures [7]. In a cyber-physical grid, however, the information used by monitoring and control systems is also important.

FDI attacks can target voltage measurements, PMU measurements, load measurements, state-estimation inputs, and voltage-control systems [10]. An attacker can therefore attempt to influence the information used by operators or controllers rather than directly manipulating physical equipment

D. Cyber-Physical Architecture

A modern power grid contains two strongly interconnected layers. The physical layer includes generators, loads, transmission lines, transformers, power-electronic interfaces, and meters. The cyber layer includes sensors, communication networks, monitoring and control systems, EMS, SCADA, and WAMPAC infrastructure [10].

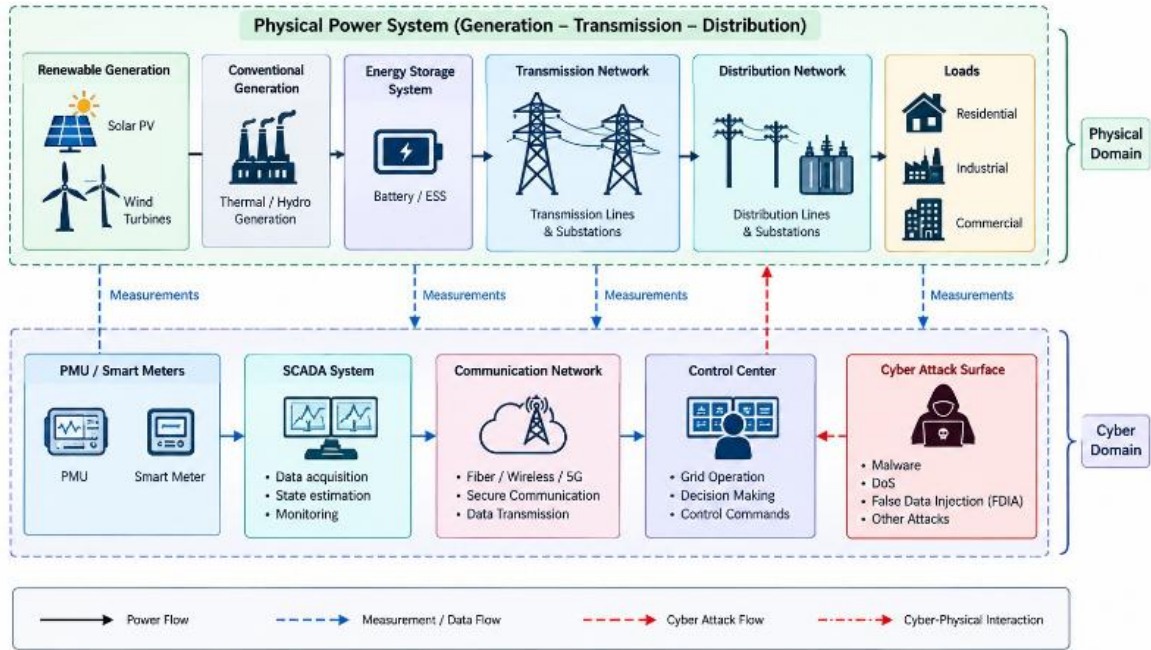


Fig. 1. Cyber-physical architecture of a high-renewable-penetration power grid.

The interaction between these layers means that measurement manipulation, communication delays, and malicious control commands can produce cyber-physical disturbances [10].

III. CYBERSECURITY THREATS AND VOLTAGE-STABILITY IMPACT

A. Major Cybersecurity Threats

The reviewed literature identifies several types of cyberattacks that can affect the operation and stability of power systems. These include false data injection attacks, denial-of-service attacks, replay attacks, man-in-the-middle attacks, and malicious command attacks [1], [8], [10].

MAJOR CYBERATTACKS AND THEIR POSSIBLE VOLTAGE-STABILITY IMPACT

Attack	Target	Main Cyber Effect	Voltage-Stability Relevance
FDIA	Measurements/state estimation	False information	Incorrect state/control decisions [1], [4]
DoS	Communication infrastructure	Loss/delay of information	Reduced monitoring/control capability [10]
Replay	Measurement streams	Reuse of previous data	Incorrect representation of operating conditions [8]
MitM	Communication links	Interception/modification	Manipulated information exchange [10]
Malicious command	Controllers/field devices	Unauthorized operation	Undesired physical response [10]

B. False Data Injection Attacks

The measurement model used in state estimation can be expressed as

$$z = Hx + e \quad (1)$$

where z represents the measurement vector, H is the measurement matrix, x is the system state, and e represents measurement noise [4].

An attacker can modify the measurements according to

$$z_a = z + a \quad (2)$$

where a is the attack vector [4].

For a linearized system, a stealthy FDIA can be constructed in the form

$$a = Hc \quad (3)$$

where c is a nonzero vector [4]. Under this condition, the estimated system state can be altered without necessarily causing the residual to exceed the conventional bad-data detection threshold [4].

This characteristic makes FDIA particularly significant for cyber-physical stability analysis. A successful attack may remain hidden while the manipulated information is used by subsequent monitoring or control functions [1], [4].

C. Denial-of-Service Attacks

A denial-of-service attack attempts to disrupt the availability of a communication or computing resource. In a power-system environment, loss or delay of information can affect monitoring and control functions [10].

The physical consequence of a DoS attack depends on the affected system and the duration of the disruption. The reviewed literature also indicates that DoS attacks may have greater physical consequences when combined with other attack types [10].

D. Replay Attacks

Replay attacks use previously recorded information in place of current system measurements. In a changing power-system operating condition, old information may no longer accurately represent the actual system state [8].

Replay attacks are therefore relevant to systems that depend on continuously updated measurements for state estimation and control.

E. Man-in-the-Middle and Malicious Command Attacks

Man-in-the-middle attacks can compromise communication between system components by intercepting or modifying information [10]. Malicious command attacks can directly affect control functions or field devices.

The reviewed literature groups measurement manipulation, communication delays, and malicious commands among the important mechanisms through which cyberattacks can produce physical disturbances [10].

F. Cyber-to-Physical Propagation

The cybersecurity problem becomes a stability problem when a cyberattack changes the physical operating state of the grid.

The general sequence is:

Cyber vulnerability → **Cyberattack** → **Measurement/communication/control manipulation** → **Incorrect state estimation or control** → **Physical-system response** → **Voltage-stability impact** [10].

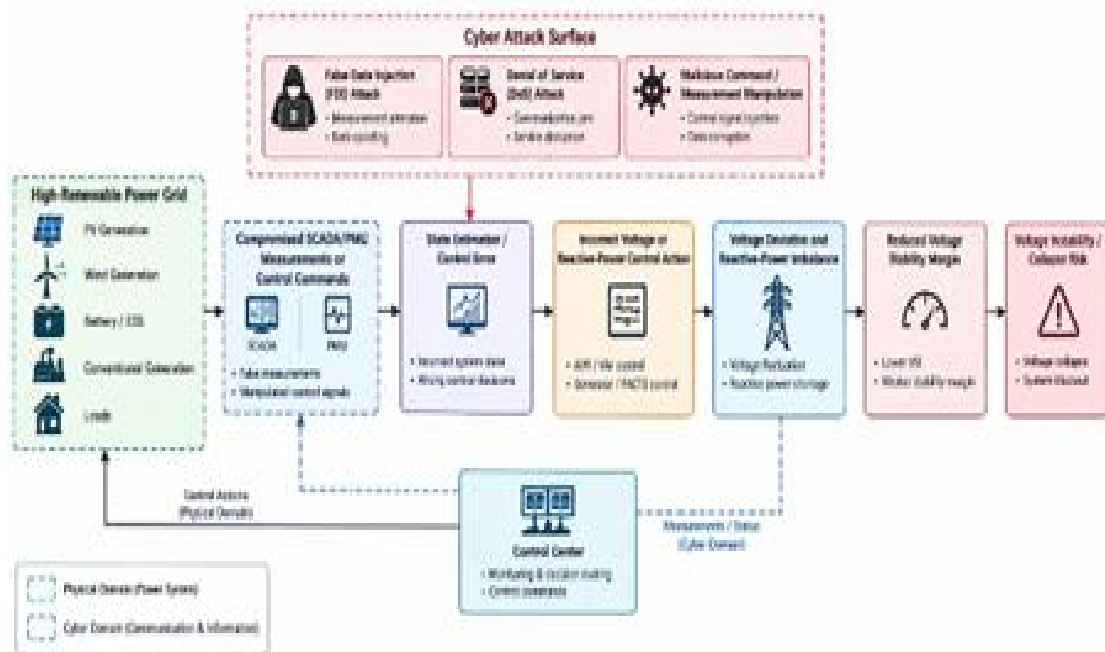


Fig. 2. Cyber-to-physical propagation mechanism from cyberattack to voltage-stability degradation [10].

For voltage stability, FDI attacks can target load measurements, PMU measurements, voltage measurements, state-estimation inputs, and voltage-control systems [10]. The reviewed studies also indicate that denial-of-service (DoS) attacks and malicious breaker operations can contribute to voltage instability in power systems [10].

IV. EXISTING DETECTION AND MITIGATION APPROACHES

A. Conventional Model-Based Detection

Traditional FDIA detection relies heavily on state-estimation residuals and bad-data detection. These methods use the mathematical model of the power system to identify measurements that deviate significantly from expected values [1], [4].

Their main limitation is that carefully designed stealthy attacks can satisfy the mathematical conditions required to avoid conventional residual-based detection [4].

This limitation has motivated research into statistical and data-driven detection techniques.

B. Statistical Detection

Paudel evaluated several FDIA detection methods using real PMU measurements [3]. The study considered Bad Data Detection (BDD), Median Absolute Deviation (MAD), Kullback–Leibler Divergence (KLD), CUSUM, and Weighted Voting (WV) [3].

Four FDIA patterns were investigated. The study found that no single detection method was able to detect every attack effectively. Combining different detectors through weighted voting improved overall detection capability [3].

This result suggests that hybrid detection may be more suitable than relying on a single statistical indicator.

C. Stability-Oriented FDIA

Jafari et al. investigated FDIAs designed to influence power-system small-signal stability [2]. The approach combined AC power-flow analysis, optimization, and small-signal stability constraints.

The significance of this work is that the attacker is not simply assumed to introduce arbitrary measurement errors. Instead, the attack can be formulated with a specific physical objective [2].

A similar stability-oriented perspective is particularly important for voltage-stability studies in renewable-rich grids.

D. Machine-Learning-Based Detection

Machine learning has been widely studied as an alternative to conventional model-based detection. Sayghe et al. reviewed supervised, semi-supervised, unsupervised, and deep-learning approaches for FDIA detection [5].

The reviewed algorithms include SVM, KNN, fuzzy C-means, Local Outlier Factor, Isolation Forest, MLP, RNN, DBN, and autoencoders [5].

ML-based approaches can identify complex patterns in measurements that may not be easily represented using fixed residual thresholds. Nevertheless, their performance depends on training data, attack representation, computational requirements, and generalization to operating conditions not represented in the training dataset [5].

E. Graph-Based and Spatio-Temporal Detection

A power grid is naturally represented as a graph because buses are connected through transmission lines. Therefore, measurements associated with neighboring buses are not independent.

Fahim et al. proposed an unsupervised Graph Autoencoder (GAE) approach specifically for FDIA targeting voltage stability [7]. In the proposed representation, buses are modeled as nodes and transmission lines as edges [7].

Chebyshev graph convolution is used to capture spatial relationships, while LSTM captures temporal behavior in the measurements [7]. The GAE reconstructs the input data, and reconstruction error is used to identify abnormal measurements [7].

The method was evaluated on a 486-bus Iberian power-system topology [7].

The methodology can be summarized as:

Power system → normal data generation → FDIA injection → bi-level optimization → graph construction → active/reactive measurements → Chebyshev graph convolution → LSTM → latent representation → graph autoencoder → reconstruction error → attack detection [7].

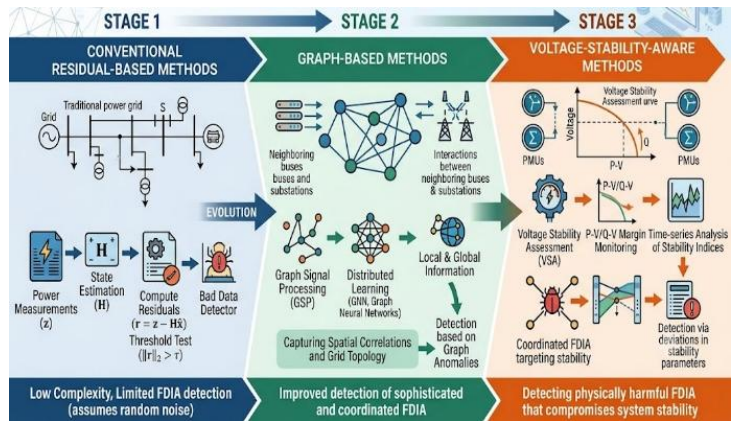


Fig. 3. Evolution of FDIA detection approaches from conventional residual-based methods to graph-based and voltage-stability-aware methods [3], [5], [7].

The study reported average values of 98.11% accuracy, 98.76% detection rate, and 8.13% false alarm rate for its evaluated scenarios [7]. These values should be interpreted within the experimental conditions of that study and should not be generalized directly to operational grids.

F. FDIA Localization

Detection determines whether abnormal behavior exists, but localization attempts to determine where the attack has occurred.

Xi et al. proposed an intuitionistic fuzzy set-based multilayer random vector functional link network for FDIA detection and localization [9]. The study used measurements from SCADA and PMUs and evaluated the proposed approach on the IEEE 14-bus, 57-bus, and 118-bus systems [9]. The reported localization accuracies were 97.76%, 96.10%, and 99.50% for the IEEE 14-bus, 57-bus, and 118-bus systems, respectively [9].

Although these results demonstrate the potential of intelligent localization, further validation using realistic renewable-rich cyber-physical systems is required.

SUMMARY OF THE REVIEWED RESEARCH

Ref.	Main Focus	Method	Main Limitation
[1]	FDIA attacks/countermeasures	Survey	Real-time and scalability challenges
[2]	FDIA and stability	Optimization + stability constraints	Benchmark-system evaluation
[3]	FDIA detection	BDD, MAD, KLD, CUSUM, WV	Limited measurement environment
[4]	FDIA theory	State-estimation/model-based	Classical system assumptions
[5]	ML-based detection	ML/DL methods	Data/generalization challenges
[6]	DDoS detection	Clustering + ML	Not voltage-stability focused
[7]	Voltage-stability FDIA	GAE + GCN + LSTM	Simulation-focused evaluation
[8]	Replay + FDIA	RMT + SVD-CNN	Attack differentiation/localization
[9]	FDIA localization	IF-RVFLNML	Benchmark-system evaluation
[10]	Cyberattack/stability mapping	CPPS stability review	Need for realistic validation

V. CYBERSECURITY CHALLENGES IN HIGH-RENEWABLE-PENETRATION GRIDS

A. Expanding Cyberattack Surface

The increasing number of digitally connected devices creates additional cyber interfaces. Smart inverters, PMUs, SCADA systems, communication networks, and remotely controlled voltage-regulation equipment increase the interdependence between the cyber and physical layers [7], [10].

Therefore, cybersecurity should be considered across the entire measurement–communication–estimation–control chain rather than only at the control-center level.

B. Limitations of Existing Detection Methods

Stealthy FDIAs can bypass conventional residual-based detection [4]. ML-based approaches provide additional detection capabilities but can depend strongly on representative training data [5].

This creates an important problem for renewable-rich systems because operating conditions may vary significantly. A detector trained under a limited set of operating conditions may not necessarily perform similarly under different generation and loading conditions.

C. Realistic Cyber-Physical Modeling

The electrical system and cyber system operate according to different physical and computational characteristics. Power-system models represent electrical dynamics, whereas communication networks involve latency, packet behavior, routing, computing, and discrete events [10].

The reviewed literature identifies the lack of realistic cyber-physical power-system models as an important research challenge [10].

D. Dependence on Benchmark Systems

Standard IEEE test systems are widely used for evaluating cybersecurity approaches [10]. They provide reproducible experimental conditions, but they cannot represent every characteristic of modern renewable-rich systems.

The reviewed literature points out that relying heavily on older benchmark systems and simplified representations of cyber networks remains a limitation [10].

E. Converter-Driven Stability

The increasing use of solar PV, wind, HVDC, and power converters creates new cyber-physical interactions [10].

However, cybersecurity research specifically addressing converter-driven stability remains limited [10]. This is particularly important for future high-renewable grids.

VI. RESEARCH GAPS AND FUTURE DIRECTIONS

The reviewed papers reveal several directions in which cybersecurity and voltage-stability research can be extended.

A. Realistic Cyber-Physical Testbeds

Future studies should combine realistic power-system models with communication-network models. The development of benchmark cyber-physical power-system models would allow more meaningful comparison between detection approaches [10].

B. Renewable-Specific Analysis

Future FDIA studies should explicitly evaluate different renewable penetration levels. This would help determine how cyberattack consequences vary with changing inverter-based generation.

C. Converter-Driven Stability

Cybersecurity analysis should be extended to converter-driven stability because this area remains comparatively underdeveloped [10].

D. Coordinated Attacks

The literature identifies coordinated cyberattacks as an important research direction. A combination such as DoS + FDIA can simultaneously disrupt communication and introduce false measurements, potentially increasing physical impact [10].

E. Online Detection

Many ML/DL methods depend on offline training and representative datasets [5]. Future detectors should operate efficiently under changing grid conditions and detect previously unseen attack patterns.

F. Detection and Localization

A practical cybersecurity system should ideally detect an attack and identify the compromised measurement or system area. Recent localization work demonstrates the potential of this approach [9].

G. Cybersecurity-Aware Voltage Stability

The conventional stability problem asks how the physical system responds to disturbances. A cyber-physical perspective additionally asks whether the information used to make operational decisions can be trusted [10].

H. Adaptive Attacks

Future research should investigate attackers capable of adapting their attack vectors to system operating conditions. Such attacks are more representative of a stability-oriented threat than fixed abnormal-data scenarios.

VII. PROPOSED CYBERSECURITY–VOLTAGE-STABILITY FRAMEWORK

Based on the reviewed research, a conceptual framework is proposed for evaluating cyber threats from a voltage-stability perspective.

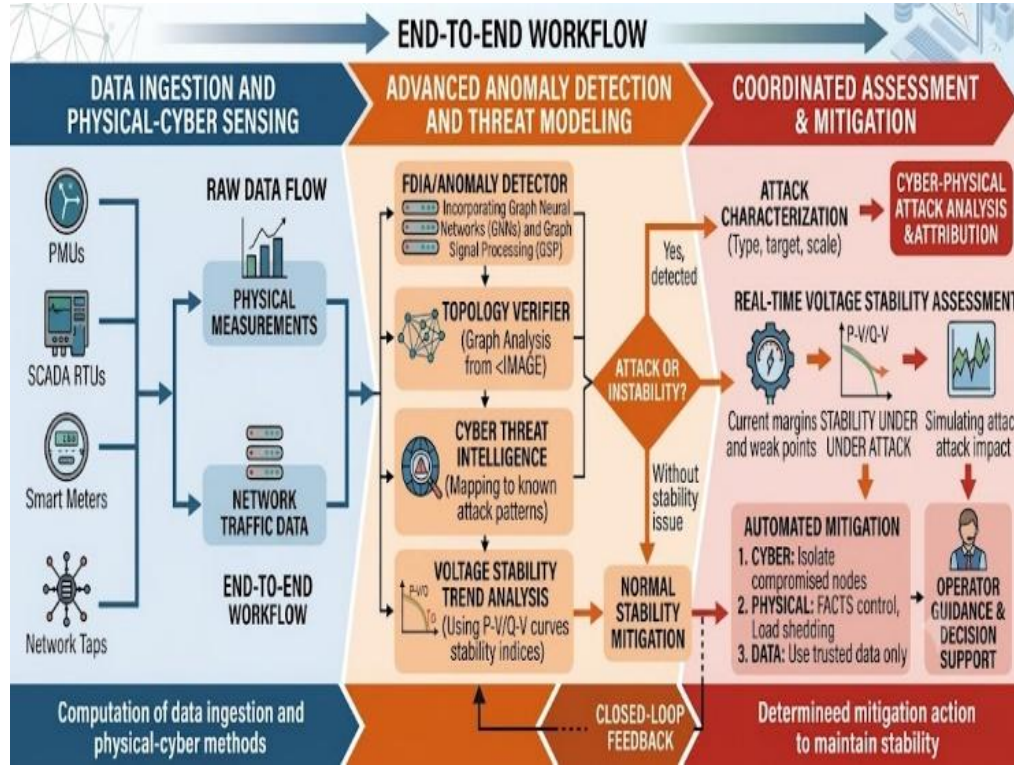


Fig. 4. Proposed cybersecurity–voltage-stability assessment and mitigation framework.

The framework contains the following stages.

A. High-Renewable Grid Representation

The system model should represent renewable generation, inverter-based resources, conventional generators, transmission networks, loads, and voltage-control devices [7], [10].

B. Cyber Threat Modeling

Potential attack scenarios include FDIA, replay, DoS, man-in-the-middle, and malicious commands [8], [10].

C. Data Acquisition

SCADA and PMU measurements provide the primary information for monitoring [3], [9]. Both temporal behavior and spatial relationships should be considered.

D. Attack Detection

Multiple detection layers can be employed. Statistical detection methods provide an initial indication of abnormal behavior, whereas machine learning, deep learning, and graph-based methods are better suited to identifying more complex patterns in the data [3], [5], [7].

E. Attack Localization

Once an anomaly is detected, localization techniques can identify potentially compromised buses or measurements [9].

F. Voltage-Stability Assessment

The detected attack should then be evaluated according to its possible physical impact. This step distinguishes a cyber anomaly from a cyber event that poses a significant voltage-stability risk.

G. Risk-Aware Mitigation

The final stage combines cyberattack information with physical-system impact. The resulting risk assessment can support appropriate mitigation and resilient operation.

The proposed process is therefore:

Detection → Localization → Voltage-stability assessment → Risk evaluation → Mitigation.

This extends the cybersecurity problem from just intrusion detection towards voltage-stability and risk assessment. In other words, from intrusion detection we move towards cyber-physical stability management.

VIII. DISCUSSION

From the literature reviewed, it is evident that cybersecurity and power-system stability is becoming highly intertwined. The cyber-physical stability framework shows that measurement manipulation, communication delays, and malicious commands can be mechanisms through which cyber events can have physical disturbances [10].

FDIA is the most prominent example in that an attacker can modify measurements without interacting directly with the physical components [1]. If the modified information affects any state estimation or control decision, the physical response could potentially affect voltage stability [7], [10].

While statistical methods provide useful anomaly indicators, individual detectors may not perform consistently on all attack patterns [3]. While ML methods offer more flexibility, they do introduce dependencies on training data and generalizations [5].

Graph-based methods provide an alternative, important development. Since buses and transmission lines constitute a physical network, explicitly modeling the topology can provide information that conventional feature-based methods would miss [7].

The localization work of [9] further suggests that locating the attacked system area can also complement detection. However, the reviewed studies demonstrate that high reported performance figures are generally associated with specific datasets, attack models, and benchmark systems.

Performance figures should therefore not be interpreted as universal benchmarks for operational-grid performance. Real systems have measurement uncertainty, varying operating conditions, communication limitations, heterogeneous equipment that is difficult to completely reproduce in-simulation [10].

A future cybersecurity system should therefore combine three perspectives:

1. **Cyber perspective:** is the information or communication channel compromised?
2. **Electrical perspective:** is what physical condition being affected?
3. **Stability perspective:** could the cyber event significantly degrade system stability?

Integrating all three perspectives offers a more complete basis for cybersecurity assessment for renewable-rich grids.

IX. CONCLUSION

The rising penetration of renewables and inverter-based resources is being accompanied by the increasing degree of digital monitoring, communication, and control. This has resulted in a highly interconnected cyber-physical power-system environment [7], [10].

Among the cybersecurity threats reviewed, FDIA is of particular concern since manipulated measurements can affect state estimation and operational decisions while remaining undetected by current residual-based methods [1], [4]. DoS, replay, man-in-the-middle, and malicious command attacks offer additional avenues through which cyber events can influence physical-system operation [8], [10].

The reviewed research demonstrates a progression from conventional model-based detection towards statistical, machine-learning, deep-learning, graph-based, and localization-oriented approaches [3], [5], [7], [9]. The graph-based spatio-temporal methods are particularly pertinent as they can incorporate both electrical topology and measurement dynamics [7].

Nevertheless, there is still much research to be done. Most studies tend to rely on benchmark systems, simulated attacks, simplified cyber networks, and limited operating conditions [10]. Converter-driven stability, realistic attacker behavior, coordinated attacks, online detection, and integrated cyber-physical testbeds would need further investigating.

Voltage-stability-wise, cybersecurity should not simply just detect an abnormal measurement. Instead, a more useful approach would be to locate the attack, assess its potential physical consequence, evaluate its voltage-stability significance, and risk-aware mitigation.

The framework proposed in this review follows this integrated principle:

Cyber Threat → Detection → Localization → Voltage-Stability Assessment → Risk Evaluation → Mitigation.

Such an approach can provide a foundation for future research into resilient high-renewable-penetration power systems.

REFERENCES

- [1] S. Aoufi, A. Derhab, and M. Guerroumi, "Survey of false data injection in smart power grid: Attacks, countermeasures and challenges," *Journal of Information Security and Applications*, vol. 54, Art. no. 102518, 2020, doi: 10.1016/j.jisa.2020.102518.
- [2] M. Jafari, M. A. Rahman, and S. Paudyal, "False Data Injection Attack Against Power System Small-Signal Stability," 2021.
- [3] S. Paudel, "An evaluation of methods for detecting false data injection attacks in the smart grid," *Frontiers in Computer Science*, vol. 6, Art. no. 1504548, 2024, doi: 10.3389/fcomp.2024.1504548.
- [4] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, 2015, doi: 10.1109/TSG.2015.2495133.
- [5] A. Sayghe *et al.*, "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, 2020, doi: 10.1049/iet-stg.2020.0015.
- [6] F. R. Hamade, M. Habiban, and A. A. H. Alrammahi, "DDoS attack detection using machine learning and improved clustering algorithm," *International Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 14, no. 2, pp. 82–87, 2025, doi: 10.18178/ijeetc.14.2.82-87.
- [7] S. R. Fahim, R. Atat, A. Takiddin, M. Ismail, K. R. Davis, and E. Serpedin, "An unsupervised approach to enhance cyber resiliency of power systems against false data injection attacks on voltage stability," *International Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 14, no. 2, pp. 88–93, 2025, doi: 10.18178/ijeetc.14.2.88-93.
- [8] "Replay attacks and false data injection attacks in cyber-physical power systems," *Scientific Reports*, vol. 14, Art. no. 2758, 2024, doi: 10.1038/s41598-024-52954-z.
- [9] L. Xi, Z. Li, Z. Li, H. Chen, F. Bai, and Y. Wang, "FDIA localization detection based on intuitionistic fuzzy set-multiple hidden layer random vector functional link network," *CSEE Journal of Power and Energy Systems*, vol. 12, no. 2, 2026, doi: 10.17775/CSEEJPES.2024.06550.
- [10] I. Semertzis, A. Ștefanov, A. Presekal, B. Kruimer, J. L. Rueda Torres, and P. Palensky, "Power system stability analysis from cyber attacks perspective," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3443061.