Enhancing Cyber-Resiliency of DER-Based Smart Grid : A Survey
Authors: Mengxiang Liu, Zhenyong Zhang, Pudong Ge, Ruilong Deng, Mingyang Sun, Peng Cheng, Jiming Chen, and Fei Teng
Submitted to: IEEE Transactions on Smart Grid
Reference number: TSG-00644-2023

Responses to Associate Editors' Comments

The authors would like to thank gratefully the Associate Editors, for the valuable comments that help improve the manuscript significantly. In the revised manuscript, we have made the following changes in response to the comments.

Editor's comments

Comments: *This paper presents an interesting survey on DER-based smart grid cyber security. Four experts have carefully reviewed this work. As you can see, they have raised concerns about the contributions of this work. The literature review also needs significant improvement and more solid justifications of how unique this work is as compared to others are needed. Some important discussions on detection and mitigation algorithms, blockchain, etc. I would recommend a resubmission of this work after the authors comprehensively address the concerns. The current version goes beyond a standard revision. We look forward to the new version of the paper.*

Response: We thank the Editor for the nice summary and constructive comments. We have revised this manuscript accordingly and mainly made the following modifications:

- Systematical comparisons with existing surveys have been conducted to highlight this paper's uniqueness and contributions.
- The implementation and guidance details of threat modeling and prevention technologies have been shed more light.
- The features of and lessons learned from detection and mitigation strategies have been comprehensively summarized in tables to better demonstrative the findings of this manuscript.
- The cyber-recovery process has been carefully explained and extensively compared with existing black-start and physical-recovery services to highlight its necessity.

The comments of all reviewers have been addressed, and the details can be found in the following responses and the revised manuscript, where the corresponding revision parts have been marked in blue. To adhere to the page requirement of the initial submission, certain sections of the manuscript have been streamlined. For a more comprehensive understanding, the full-version revised manuscript can be accessed for additional reading.

Best Regards,
Authors

Responses to Reviewers' Comments

The authors would like to express sincere gratitude to the anonymous reviewers for their valuable comments that help improve the manuscript significantly. All comments have been carefully addressed as illustrated in the following response and the revised manuscript, where the related modifications have been marked in blue. To adhere to the page requirement of the initial submission, certain sections of the manuscript have been streamlined. For a more comprehensive understanding, the full-version revised manuscript can be accessed for additional reading.

Reviewer 1's Comments

Summary: *The paper provides an insightful discussion on the pressing need for cyber-resiliency in Distributed Energy Resources (DER)-based smart grids, given the extensive exposure of geographically dispersed DERs to potential cyber threats. It thoroughly reviews strategies to enhance cyber-resiliency and introduces a framework embedding key resiliency enablers. The paper's limitation, however, lies in its high-level examination of cyber-attacks from a reliability and risk perspective, which detaches it from practical application to smart grids and the journal's scope.*

Despite offering abundant information on cyber threats and defense mechanisms, the paper needs to conclude on specific techniques or present applied work that directly tackles the mitigation and defense against cyber-attacks. High-level studies undoubtedly open up avenues for research, though they might appear generic and need sufficient information for the authors to build their claims.

Response: We thank the Reviewer for the nice summary and constructive comments. We have revised the manuscript accordingly to provide practical and comprehensive guidelines regarding current resilience enhancement methods and insightful recommendations of further research opportunities. The main modifications are

- Extensive comparisons between this survey and existing ones have been conducted to clarify the motivation and contributions (Response to comment 1).
- The purposes of presenting a fresh hierarchical framework for the DER-based smart grid have been illustrated, and its differences from existing framework have been also identified (Response to comment 2).
- Attack techniques, risk assessment, and prevention technologies have been enriched with extensive technical details and practical implementation guidelines (Responses to comments 3-5).
- Tabulated presentations summarizing the pros and cons of each type of detection/mitigation method and the lessons learned have been appended. Moreover, the refined future research directions have been demonstrated in the conceptual resilience enhancement framework (Responses to comments 6-8).
- Besides, comprehensive proofread, reference standardization, and figure and table revisions have been accomplished to increase this manuscript's readability (Responses to minor comments).

To adhere to the page requirement of the initial submission, certain sections of the manuscript have been streamlined. For a more comprehensive understanding, the full-version revised manuscript can be accessed for additional reading.

Major Comments

Comment 1: *Regarding related works, the authors cite references that exclude intrusion detection systems or prevention techniques. However, there are notable papers proposing ideas on these topics. For example, Adhikari, Morris, and Pan proposed a cyber-physical power system test bed for intrusion detection systems. Additionally,*

TABLE I: Comparison between our survey and existing surveys

Resilience Enhancement Phases		[28]	[29]	[30]	[10]	[31]	[32]	[33]	This Paper
Threat Identification	Adversary Model	F	N	N	N	N	N	N	F
	Vulnerability Coverage	M	P	P	M	M	M	F	F
	Risk Assessment	P	F	P	F	F	P	P	F
Defense-in-Depth Strategies	Prevention	M	N	M	N	M	P	N	F
	Detection	P	N	N	M	M	M	M	F
	Mitigation	P	P	P	P	P	M	P	F
	Recovery	N	N	N	N	N	N	N	F

F: Fully Covered, M: Mostly Covered, P: Partially Covered, N: Not Covered

prevention techniques are quite broad, requiring further clarification on how they are expected to counter cyber threats. The gaps identified need detailed emphasis and highlighting.

[131] U. Adhikari, T. H. Morris and S. Pan, "A cyber-physical power system test bed for intrusion detection systems," *2014 IEEE PES General Meeting — Conference & Exposition*, National Harbor, MD, USA, 2014, pp. 1-5, doi: 10.1109/PESGM.2014.6939262.

[132] S. Pan, T. Morris and U. Adhikari, "Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems," in *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3104-3113, Nov. 2015, doi: 10.1109/TSG.2015.2409775.

[102] Mohammad Saber, A. Youssef, D. Svetinovic, H. H. Zeineldin and E. F. El-Saadany, "Anomaly-Based Detection of Cyberattacks on Line Current Differential Relays," in *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4787-4800, Nov. 2022, doi: 10.1109/TSG.2022.3185764.

Response: We thank the Reviewer for the constructive comment. The section discussing the related *surveys* mainly compare this survey with existing ones to highlight its necessity and comprehensiveness. The results are summarized in TABLE I, indicating this paper's extensive coverage on both threat identification and defense-in-depth strategies. To address the contributions made by Adhikari, Morris, and Pan in attack detection using multiple features from network and physical domains based on data mining methods, the related papers have been marked as a pioneering work in developing host, network, and physical intersecting intrusion detection systems, aiming to attract more attention to this imperative direction. Moreover, the effort made by Saber *et al.* to detect false-tripping attacks against line current differential relays using local current information has also been well highlighted. The modifications in the revised manuscript are as follows:

(Page 13, left column, and in the middle) Pan *et al.* has made their attempts towards this direction and successfully applied a data mining technique called common path mining to automatically and accurately learn patterns for scenarios, which are used to identify attacks from normal control operations and external disturbances, from a fusion of synchrophasor measurement data, and information from relay, network security logs, and EMS logs [131], [132].

(Page 9, left column, and in the top) By employing the Isolation Forest algorithm, which is trained on features determined from local current measurements, Saber *et al.* proposed an anomaly-based scheme for detecting false-tripping attacks against line current differential relays, in the form of relay attacks, replay attacks, general false-data-injection attacks, and time-synchronization attacks [102].

Moreover, the manuscript has also summarized and classified the current prevention technologies as shown in Fig. 1. In particular, these technologies are divided into cyber- and physics-based according to their application scenarios. Cyber-based technologies are collected from the IT domain like encryption and authentication, and they can be deployed at host, protocol, system, and network levels to *prevent the adversary from intruding into the system network*. Implementation guidance and recommendations on four basic aspects including network architecture, access control, communication protocol, and software update are specified, and further improvements benefited from advanced technologies like blockchain and moving target defense are also discussed. Physics-based methods aim to exploit the robustness of control and operation algorithms or deploy extra protection and virtualized devices

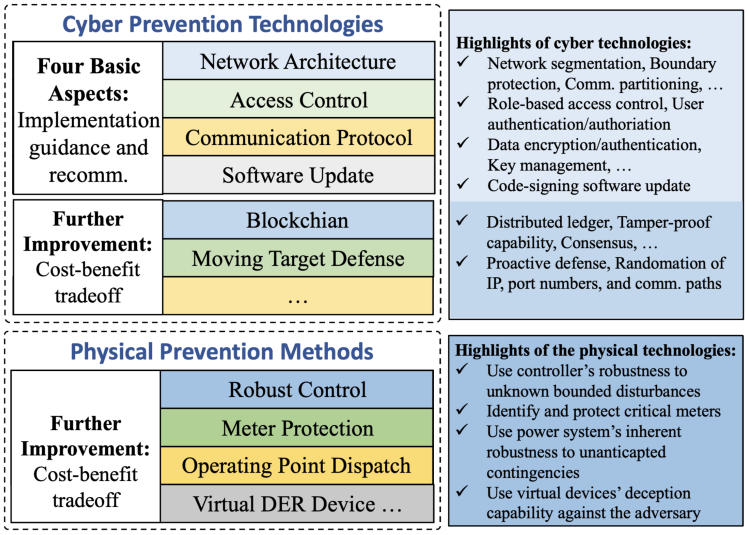

Fig. 1: Summary of Prevention Technologies and Methods

in the OT environment to *prevent the attack from inducing hazardous consequences on the system operation*. For example, by modeling the attack as an unknown and bounded disturbance, the famous robust control tool can be adopted to ensure the proper functionality of the controller [85]. Besides, meter protection, operating point dispatch, and virtual DER devices are other useful prevention technologies in the physical domain. The details of these prevention technologies can refer to the response to Comment 5 of this Reviewer.

One critical perception is that there is no combination of cyber and physical prevention technologies/methods that can ensure 100% security, i.e., all potential adversaries are prevented. The core challenge and gap of adopting these prevention technologies is to balance the cost-benefit tradeoff, and several directions like cost-efficient MTD and lightweight blockchain are highlighted in Section VIII in the revised manuscript.

[10] J. Ye *et al.*, "A review of cyber–physical security for photovoltaic systems," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 4, pp. 4879–4901, 2022.

[28] I. Zografopoulos *et al.*, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *arXiv preprint arXiv*:2205.11171, 2022.

[29] S. Sahoo *et al.*, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5326–5340, 2019.

[30] A. Vosughi *et al.*, "Cyber-physical vulnerability and resiliency analysis for der integration: A review, challenges and research needs," *Renewable & Sustainable Energy Reviews*, vol. 168, p. 112794, 2022.

[31] J. Qi *et al.*, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 28–39, 2016.

[32] Y. Li *et al.*, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, 2022.

[33] N. D. Tuyen *et al.*, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, vol. 10, pp. 35 846–35 875, 2022.

[85] K. Zhou *et al.*, Essentials of robust control. Prentice hall Upper Saddle River, NJ, 1998, vol. 104.

Comment 2: *For the Hierarchical Framework of the DER-based Smart Grid, the paper's objective and message need to be clearer. More information on the relationship or comparison with existing systems is also necessary. It is not clear here the take home message form this point and if you made a comparison with the current existing systems.*

Response: We thank the Reviewer for the constructive Comment. According to the actors and corresponding functionalities involved in the DER-based smart grid, they are divided into four levels comprising DER device,

DER aggregator, distribution utility, and transmission operation as shown in Fig. 2, where the utilized communication protocols are specified clearly. The presentation of this framework is to 1) clarify the way to control, manage, and operate numerous graphically dispersed DERs while meeting the objectives within multiple time scales and then 2) fully understand the potential vulnerabilities exploitable by the adversary and possibly induced consequences.

Two basic messages can be observed from the presented framework: i) The hardware vulnerability is mainly from DERs and field controllers, and the personnel vulnerability is among the operation and management staff in upper levels. Moreover, software and communication vulnerabilities spread throughout all the levels. ii) The possible consequences induced by exploiting these vulnerabilities include consumer privacy leakage, distribution-scale power quality degradation and violate violation, and transmission-scale frequency instability and blackout. Both messages i) and ii) have been illustrated clearly in subsection III-B in the revised manuscript.

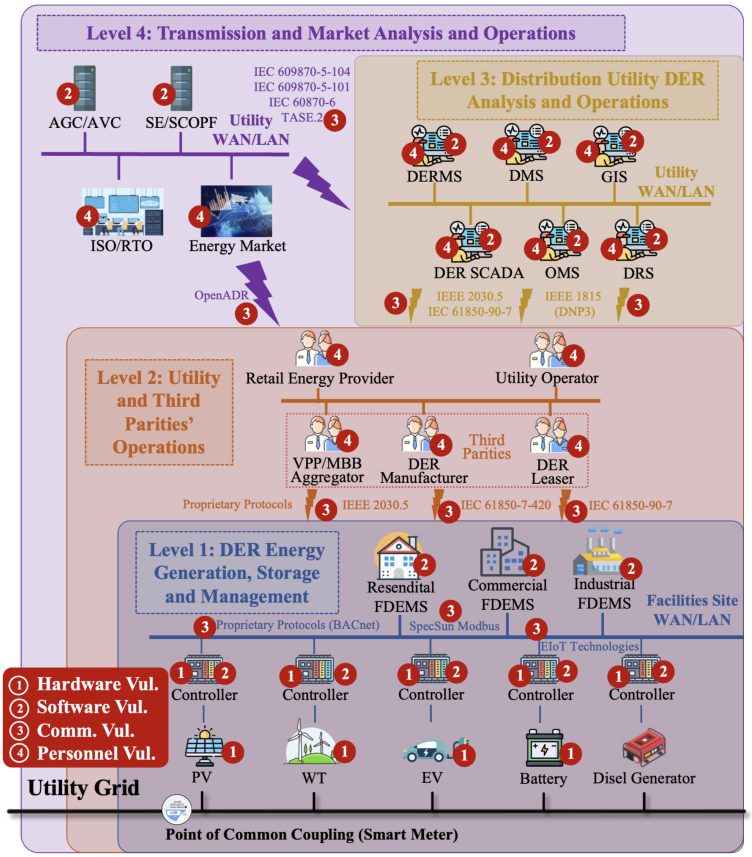

Fig. 2: Hierarchical framework of DER-based smart grid and and the associated vulnerabilities.

Moreover, we have compared the proposed framework with two most-related existing ones to highlight its uniqueness. The corresponding modification in the revised manuscript is as follows:

(Page 5, left column, and in the middle) Compared with the existing DER System architectures [13], [31], the uniqueness of the proposed hierarchical framework is reflected through the following aspects: i) The four-level framework comprising the DER device, DER aggregator, distribution utility, and transmission operation is proposed for the first time. ii) Actors, functionalities, and communication protocols in each layer are specified to clarify potential vulnerabilities and possible consequences; iii) Newly emerging DER-related entities like VPP and MBB aggregators and the P2P energy trading mode are incorporated.

[13] C. Frances *et al.*, "Cyber security for der systems," *Electric Power Research Institute*, Tech. Rep., 2013.

[31] J. Qi *et al.*, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory & Applications*,

vol. 1, no. 1, pp. 28–39, 2016.

Comment 3: *Table I of Attack Techniques Summary and Classification could be improved with a graphical representation, such as a pie chart that quantifies the risk and occurrence of each attack technique. Including more attack techniques, like FDIA and replay attacks, and their direct implications on smart grid applications would add more value to the discussion and table summary inclusion.*

Response: We thank the Reviewer for the constructive Comment. We have added a 3-dimension pie chart that summarizes the attack techniques adopted by the cyberattack events against industrial control systems (ICSs) with data source from HACKMAGEDDON[1] as shown in Fig. 3, providing a high-level understanding of different attack techniques' risks and occurrence. In particular, the malware from supply-chain compromise, malicious firmware installation, and Trojan attacks is the most commonly adopted attack technique, followed by known/zero-day vulnerabilities, targeted attacks, and account takeover attacks. One take home message from these attack statistics is that the observed cyberattack events are becoming more and more mature, indicating the adversary's increasing intelligence. Moreover, the human-involved threats like insiders and social engineering attacks are gaining increasing attentions. In addition, FDI and replay attacks are included in TABLE I, and attack techniques' direct implications on smart grid applications are specified. In the full-version revised manuscript, the corresponding modification is as follows:

(Page 4, right column, and in the bottom) *Attack Model:* The attack model specifies the attack techniques by exploiting those vulnerabilities and potential attack impacts in the context of DER-based smart grid. Inspired by the MITRE ATT&CK Matrix for ICS, the attack techniques are divided into initial access acquisition, information discovery, and execution and implication according to the adversary's intrusion and execution phases [66]. As shown in TABLE I, specific description and impacts of attack techniques are provided. According to the statistical data published on HACKMAGEDDON[1], the top attack techniques adopted by the cyber attack events against ICSs during 2022 are depicted in Fig. 3 to provide a high-level understanding of different attack techniques' risks and occurrence. In particular, the malware from supply-chain compromise, malicious firmware installation, and Trojan attacks is the most commonly adopted attack technique, followed by known/zero-day vulnerabilities, targeted attacks, and account takeover attacks. One take home message from these attack statistics is that the observed cyberattack events are becoming more and more mature, indicating the adversary's increasing intelligence. Moreover, the human-involved threats like insiders and social engineering attacks are gaining increasing attentions. Note that TABLE I merely lists the attack techniques against smart grid, and it does not include all attack techniques highlighted in Fig. 3.

[66] M. J. Assante *et al.*, "The industrial control system cyber kill chain," *SANS Institute InfoSec Reading Room*, vol. 1, p. 24, 2015.

Comment 4: *The risk assessment segment in Fig. 5 must provide the rationale behind the presented percentages and quantification for attack impact and likelihood of success. Also, touted as a significant contribution, the risk matrix is given only a brief explanation.*

Response: We thank the Reviewer for the constructive Comment. We have detailed the generation of the risk assessment matrix for DER-based smart grid, which basically takes the inputs of attack implementation likelihoods and attack consequences as illustrated in Fig. 4. In summary, the risk levels will be qualitatively classified as Extreme, High, Medium, and Low based on the qualitatively classified attack implementation likelihood and attack consequence as indicated by Fig. 5.

[1] https://www.hackmageddon.com/

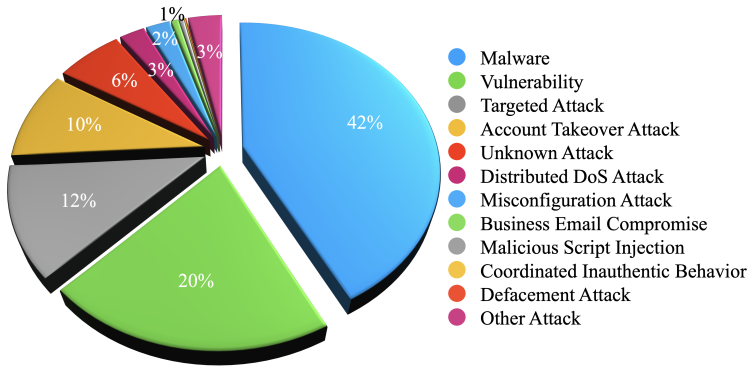

Fig. 3: Statistics of attack techniques adopted by the cyberattack events against ICSs during 2022.

TABLE I: Attack Techniques Summary and Classification

Types	Attack Techniques	Description and Direct Impacts
Initial access acquisition	Network service exploitation	Use directory traversal, cross-site scripting, SQL injection to illegally access DER network.
	Wireless compromise	Exploit wireless protocol vulnerability to obtain illegal remote access to DER network.
	Supply-chain compromise	Gain control systems' access by manipulation of products before receipt by end consumers.
	Zero-day attack	Exploit zero-day vulnerability to get illegal access to the DER system.
	Social engineering attack	Use personal information or subterfuge to learn a legal user's password.
Information discovery	Insider attack	Employ persons within the organization that have access to critical information.
	Side-channel attack	Analyze time/power/electromagnetic information to infer critical information.
	Eavesdropping attack	Take screenshot of HMI and workstation or listen to communicated confidential.
Execution and Implication	Malicious firmware installation	Install malicious firmware into inverter/converter to execute illegal actions.
	Trojan attack	A malware disguising itself as legitimate code or software and gain legitimate users' privileges.
	Hall spoofing attack	Mislead hall sensor's measurement by placing a camouflaged attack tool near the inverter.
	PLL attack	Inject false pulse voltage signal to mislead PLL reading to DER controller.
	Control logic modification	Modify control logic of DER controller to manipulate outputs or trigger overflow bug.
	Brute force attack	Repetitively change I/O point values to impact the process function associated with that point.
	Denial-of-service/control attack	Deliberately overload a DER stakeholder and prevent it from performing normal functions.
	Adversary-in-the-middle/FDI attack	Modify and inject data streams exchanged in the DER network.
	Replay attack	Replace current transmission data with previously recorded data in the DER network.
	IoT Botnet attack	Manipulate a large volume of high-watt IoT loads to induce frequency instability.
	P2P energy market attack	Submission of fake contract, modification of transaction, etc. to gain illegal profits.
	AI/ML adversarial attack	Create adversarial examples with imperceptible perturbation to mislead AI/ML outputs.

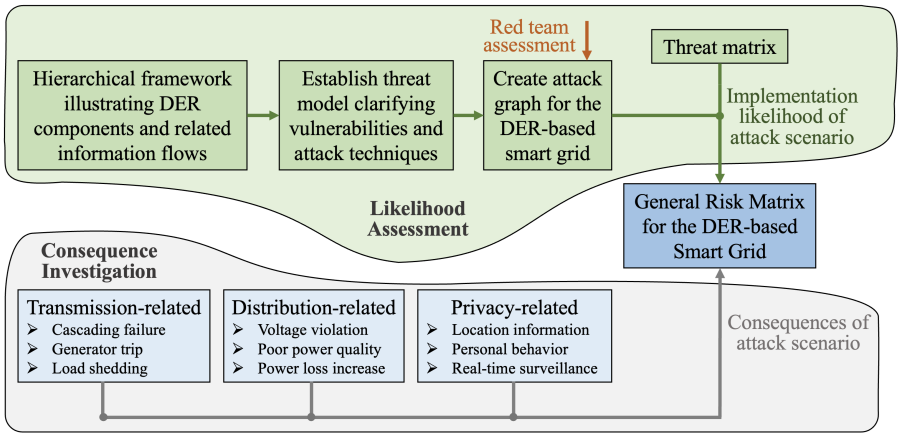

Fig. 4: Generation scheme of the risk materix for the DER-based smart grid.

Attack Implementation Likelihoods	Attack Consequences					
		Insignificant No Observable Impact like Privacy Leak	**Minor** Small Distribution Impact like Poor Power Quality	**Moderate** Large Distribution Impact like Feeder Voltage Voliation	**Major** Small Transmission Impact like Energy Price Manipulation	**Severe** Large Transmission Impact like Cascading Failure and Blackout
	Almost Certain Attacker: Script Kiddie Funding: No Time: Days	**Medium**	**High**	**High**	**Extreme**	**Extreme**
	Likely Attacker: Skilled Actor Funding: Little Time: Weeks	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
	Possible Attacker: Moderately-Skilled Team Funding: Some Time: Months	**Low**	**Medium**	**Medium**	**High**	**Extreme**
	Unlikely Attacker: Skilled Team Funding: Substantial Time: Years	**Low**	**Low**	**Medium**	**High**	**High**
	Rare Attacker: Nation State Funding: Substantial Time: Years	**Low**	**Low**	**Low**	**Medium**	**High**

Fig. 5: Risk matrix reference for the DER-based smart grid.

In the likelihood assessment phase, based on the previously established threat model, the red team will first conduct multiple assessment activities comprising visits to manufacturing facilities, development and testing labs, and assessments of fielded DER systems. The team mainly assesses the cybersecurity posture of state-of-the-art DER equipment using authorized, adversary-based assessment techniques, often in close collaboration with the vendors. Then, attack graphs will be created to show the steps an adversary must take to move from a system/network access point to a consequence or objective. A demonstrative example that illustrates the deployment of malicious firmware against EVs [71] is shown in Fig. 6. The first step in this attack graph is to craft the payload that will be delivered to the deployed EV supply equipment. Afterwards, the adversary will gain access to the business network using either a malicious insider or using remote attack techniques, followed by pivoting through the business network until getting access to the firmware repository. Different methods will be chosen to insert malicious firmware depending on if the update requires code signing. Finally, by triggering shutdown signals following specific strategics, expected consequences can be induced.

The attack graphs will be utilized to estimate the skill and time it would take adversaries to execute different attack scenarios. Combined with the general threat matrix, which enables government entities and intelligence organizations to categorize threat into a common vocabulary, the attack implementation likelihoods are qualitatively classified as Almost Certain, Likely, Possible, Unlikely, and Rare according to the adversary's knowledge, funding, and time. Note that other threat attributes like intents and targets and more granular classification levels can be incorporated into the risk matrix, and here the simplified version is shown only for demonstrative purpose.

In the consequence investigation phase, the consequences of attack scenarios on smart grid are observed from the experimental results obtained using high-fidelity smart grid simulator like OPAL-RT and Typhoon HIL and privacy inference simulation results. According to the impact scale and severity on smart grid, the attack consequences are qualitatively classified as Severe, Major, Moderate, Minor, and Insignificant. For example, the privacy leak normally not affects the power system operation and thus is deemed as insignificant, while the large-scale transmission level cascading failure and blackout will severely affect the power supply and hence is assumed as severe. Finally, the generated risk matrix is presented in Fig. 5 with the columns being the consequence levels and rows being the likelihood levels. As indicated by the colors of entries, the qualitatively classified risk levels include Extreme, High, Medium, and Low, and play a vital role in determining what kinds of defense technologies and methods should

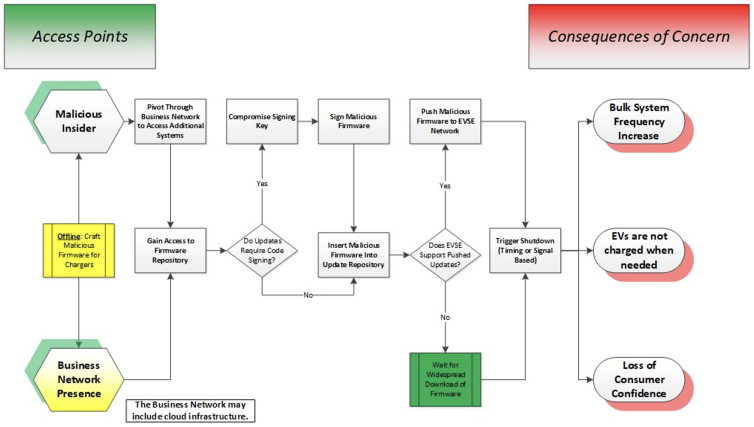

Fig. 6: Attack graph illustrating the malicious firmware deployment against EVs [21].

be adopted. A thorough risk assessment process against EV supply equipment has been conducted coordinately by multiple National Laboratories of USA and is detailed in [71]. Some insights are synthesised from this practice:

- The attack with almost certain probability cannot currently be achieved as no public scripts and tools that can indeed impact the power system exist.
- The skilled actor/team or nation state can cause insignificant and minor impact on the DER-based smart grid. For example, the personal behavior pattern may be inferred after eavesdropping the energy usage and DER generation data from smart meters/PMUs and data servers, and frequency/voltage deviations can appear in islanded microgrids when multiple primary/secondary controllers are compromised by a skilled team.
- Since the DER penetration is not high, moderate, major, and severe attack impact cannot be caused by purely manipulate the DER actions. It has been pointed out that approximately 30% of DER deployment relative to peak load begins to show infrequent but potential grid-level consequences. Hence, attention should be paid this threat that is currently impossible, but is likely to be possible under the global trend towards the low-carbon power system.

[71] J. Johnson *et al.*, "Cybersecurity for electric vehicle charging infrastructure." Sandia National Lab, Tech. Rep., 2022.

In the revised manuscript, the corresponding modification is in Subsection III-C, Page 5, left column, and in the bottom. For further reading, a more comprehensive description can be found in the full-version revised manuscript.

Comment 5: *As for the prevention techniques mentioned, their applicability to smart grids and their implementation status should be clearly established in the current industrial systems.*

Response: We thank the Reviewer for the constructive comment. We have rewritten the prevention section and emphasises are put on the implementation recommendations of the four basic cyber prevention technologies including network architectures guidelines, access control requirements, communication requirements, and patching requirements.

Network Architecture Guidelines: A practical set of cybersecurity requirements pertaining to the network components supporting DER communications has been provided to minimize the likelihood, duration, or impact of a successful cyberattack [110]. This set of requirements does not make any assumption to the communication protocols, particular functional standards, or certain ownership/business models in terms of their effectiveness in cybersecurity. Rather, it aims to provide a holistic view of the interconnected DER-based smart grid, and it suggests how they can be protected from cyberattacks. Four aspects of requirements and their implementation guidelines are detailed.

- (*Resource Criticality Level*) Each DER or supporting system participating in DER communications must be categorized into one of three distinct criticality levels—high impact, medium impact, or low impact as shown in Fig. 7. The resource's criticality level is determined by the impact of any misuse of that resource to grid reliability, public safety, finances, and privacy. Different headends are allocated to different critical groups to accomplish separate control paths.
- (*Network Segmentation*) Resources with different criticality levels must be located in different security zones. As shown in Fig. 7, the central management systems will typically consist of multiple zones containing headends of various criticality levels and a zone containing the core managing system, which will have the highest criticality of all the zones. Moreover, communications between two different security zones must be routed through the security gateways with access controls like a firewall. In particular, communications between a system/resource in the high-impact zone and a system/resources in the low-impact zone must be routed through a DMZ[2] like the managing system in Fig. 7 communicating with low-impact residential DERs).
- (*Boundary Protection*) Access controls in security gateways should be configured to deny a connection request from a lower-security zone to a higher security zone by default. In Fig. 7, traffic should be blocked from the Internet to the DMZs and from the DMZs to the managing system, and should only be allowed in the opposite direction. Security gateways at the boundary of high-impact zones and interfacing with external networks must be monitored on a 24/7 basis to detect security events negatively impacting the operation of systems or resources in the security zone.
- (*Communications Partitioning*) DER communications to/from must be physically or logically partitioned from other types of communication. In Fig. 7, a shared switch uses VLANs to segregate the corporate VLAN from the DB VLAN. Communications required for the administration of network infrastructure must be physically or logically partitioned from other types of communication. The reference architecture in Fig. 7 shows a management VLAN for several switches and firewalls.

It is noted that the network security architecture addresses only a portion of the cybersecurity risks associated with DER integration. To protect DER and the connected grid adequately, a more comprehensive cybersecurity standard including communication security, access control, patch management, etc, as introduced in the following subsections must be developed and implemented.

Role-based Access Control: With multiple entities needing differing levels of access to DER data and control modes, there is a need to establish robust access control security policies and technologies. Access control restricts access to resource functionality unless the user is authorized, preventing unauthorized users from changing power system control settings. Role-based access control (RBAC) is a natural choice for DER communication environments because there are clear roles for subjects based their company of employment, job position, and responsibilities [25]. Establishing an RBAC mechanism for the DER-based smart grid requires detailed information on the hardware and software. Based on the IEC 62351-8 RBAC implementation, these requirements are covered below.

- (*User Authentication*) Users must provide one or more proofs of identity to ensure they are who they claim to be. Some options for user authentication includes Challenge-Response, Kerberos [111], and Digital Signatures.
- (*User Authorization*) Users are permitted to access data, services, resources, or objects granted by the security policy. Two types of authorization mechanisms are structured query language [112] and lightweight directory access protection (LDAP) [113].

When selecting these mechanisms for the DER AC implementation, the administrative overhead and ease of

[2]The DMZ is a separate network zone where traffic entering and exiting the DMZ is controlled by the relevant security gateways, but an additional level of control/ traffic filtering is exerted by the devices inside the DMZ.

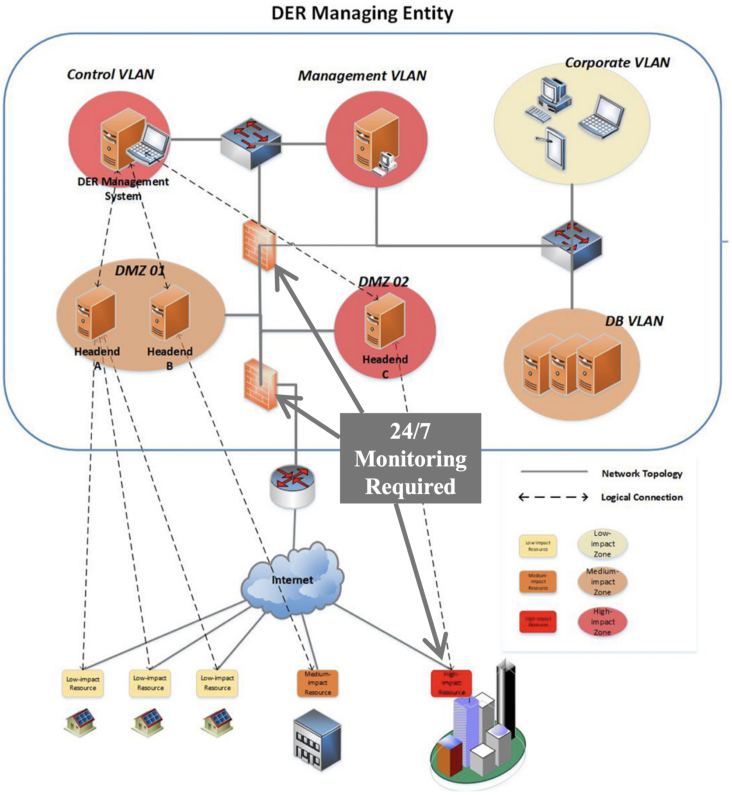

Fig. 7: Reference network segmentation for DER-based smart grid.

implementing administration delegation are important. For instance, it is common to use Kerberos for authentication and LDAP for authorization. The implementation of RBAC can be achieved through push and pull models. The push model requires the subject to fetch the token from the identity provider before sending it to the object. Whereas the pull model requires the object to fetch the token from the identity provider. Depending on the type of operational environment and object, the use of either the push or pull models may be appropriate. Access tokens are used to transport roles, whose distribution is provided by an LDAP-enabled repository/server/device. When communicating with the repository, LDAP v3 with SSL/TLS should be used with unique user identifier, authentication information, and access token entries.

It would be absolutely preferred to establish protocol-agnostic AC requirements. However, due to the unique characteristics of each of the IEEE 1547-2018 protocols, there are specific considerations needed when building an AC system for each of these protocols. This is primarily because IEEE 2030.5 client/server implementations naturally make the IEEE 2030.5 server the AC object; while DNP3 and Modbus implementations work best with the DER acting as the object. Interested readers can refer to [25] to see potential DER RBAC implementation cases for IEEE 2030.5, IEEE 1815, and SunSpec Modbus.

Communication Requirements: In IEEE 1547-2018 interconnection and interoperability standard [4], standardized information exchange interfaces between associated DER entities like IEEE 2030.5, IEEE 1815, SunSpec Modbus, and IEC 61850-7-420 have been identified to improve the interoperability. To ensure the security of information that flows over public or private networks, DER communications and their corresponding security measures must be standardized, to prevent malicious control or misuse of DERs. For instance, some protocols lack authentication and authorization, allowing unauthorized control of DER equipment by individuals with network access and knowledge of the DER's address. Moreover, implementing cryptographic methods in protocols lacking inherent security features

may require a bump-in-the-wire approach, which does not provide application layer security and can introduce latency. Therefore, to ensure the security of data-in-transit for DER equipment, it is crucial to address the security requirements to: i) assure the data authenticity flowing over the network, 2) verify the device identity, 3) confirm that encryption keys are securely managed, and 4) provide access control.

Based on a thorough analysis of the security strengths and weakness of communication technologies, a unified set of security recommendations for DER application protocols has been proposed [24]:

- (*Data Encryption and Data Authentication for Bulk Traffic*) Adopt TLS v1.3 with authenticated encryption using additional data such as AES Galois Counter Mode [114].
- (*Device Authentication*) Use X.509v3 digital certificates with mutual client/server authentication [115].
- (*Key Management*) Align with TLS v1.3, adopt Elliptic Curve for ephemeral symmetric key exchange and RSA generated node authentication signatures [116].

Conflicts still exist between these security requirements and the processing limitations of DER equipment. For example, DER equipment without cryptographic hardware relies heavily on standard software libraries to support encryption, authentication, and hashing operations executed on the CPU, which may induce unacceptable latency for communication-based control of devices supplying grid-support functions. Nevertheless, some preliminary case studies indicate that the proper implementation of these security features will not impact DER-based grid control systems (well below the IEEE 1547-2018 limits for DER latency) but improved the security posture of the devices and networked system [117]. The change in roundtrip time due to addition of encryption is on the order of *milliseconds*. In order to meet the stringent latency and messaging throughput requirements while retaining the benefits of public key cryptography, less-online/more-offline signatures model was proposed to allow the verification to be divided into online/offline phases such that online verification does not perform any expensive operations [118]. It is promising to further alleviate the computation burden when integrated with the rapidly developing quantum computation technologies.

Code-Signing Software Patching: Since the DER equipment is expected to operate in the field for 25 or more years, there will undoubtedly be newly discovered vulnerabilities in software packages or custom code that is running on the equipment during this period. In those situations, it is necessary to improve the security level of software supply chain using code-signing or equivalent mechanisms, which identify the source of the patch and confirm the integrity of the data.

Based on many standards and guides for patch management in the literature and an active community researching solutions for Industrial Control Systems [119] (ICS) and Internet of Things (IoT) firmware updates, the application of these requirements and recommendations within DER environments has been fully investigated. The primary technology used for secure patching in the DER environment is the code-signing scheme [26], which uses a digital signature mechanism to verify the identity of the data source and a checksum/hash to verify the data has not been altered in transit. Basically, three main actors are included in the code-signing scheme:

- The *developer* of the code or data who submits the code to the signer.
- The *signer* entity that is responsible for managing the signing keys. The signer securely generates the private/public key pair and then provides the public key to a certification authority (CA) through a certificate signing request (CSR) to tie their identity to the public key.
- The *verifier* that is responsible for validating the signed code signature.

In particular, PKI code signing with digital signatures is recommended in that it has better security features in terms of integrity, authentication, and non-repudiation compared to other cryptographic primitives like hashes, message authentication code (MAC), and hash-based message authentication code (HMAC). A reference implementation of

the PKI-based coding signing for the DER environments is provided in [26]. Nevertheless, there are still multiple threats to the code-signed firmware. For example, it is possible that software developed by an organization has malicious firmware embedded in the signed version. This could be perpetrated by an *insider* or through compromise of the firmware development environment, as was the case in the well-known SolarWinds attack. Awareness of this type of risk and application of appropriate mitigation methods are critical for all DER vendors. A list of suggested firmware update requirements for DER equipment, product suppliers, integrators, aggregators, and owners is also provided to adress this issue [26].

In the revised manuscript, a reduced description about these prevention technologies can be found in Page 6, left column, and in the bottom. The more comprehensive description can be accessed referring to the full-version revised manuscript. Please note that here all the reference indexes are the same as those in the full-version revised manuscript.

[4] "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std 1547-2018*, pp. 1–138, 2018.

[24] I. Onunkwo, "Recommendations for data-in-transit requirements for securing der communications." Sandia National Lab, Tech. Rep., 2020.

[25] J. Johnson, "Recommendations for distributed energy resource access control," Sandia National Lab, Tech. Rep., 2021.

[26] J. Johnson *et al.*, "Recommendations for distributed energy resource patching," Sandia National Lab, Tech. Rep., 2021.

[110] EPRI, "Epri security architecture for the distributed energy resources integration network," Accessed: 2023 [Online].

[111] B. C. Neuman and others, "Kerberos: An authentication service for computer networks," *IEEE Communications magazine*, vol. 32, no. 9, pp. 33–38, 1994.

[112] H.-P. Halvorsen, Structured query language. University College of Southeast Norway, 2016.

[113] W. Yeong *et al.*, "Lightweight directory access protocol," Tech. Rep., 1995.

[114] P. Rogaway, "Authenticated-encryption with associated-data," in Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 98–107.

[115] I. T. U. (ITU), "X.509 : Information technology," Accessed: 2023, [Online]. Available: https://www.itu.int/rec/T-REC-X.509.

[116] D. Hankerson *et al.*, Guide to elliptic curve cryptography. *Springer Science & Business Media*, 2006.

[117] I. Onunkwo *et al.*, "Cybersecurity assessments on emulated der communication networks," Sandia National Lab, Tech. Rep., 2019.

[118] E. Esiner *et al.*, "Lomos: Less-online/more-offline signatures for extremely time-critical systems," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3214–3226, 2022.

[119] "Ieee recommended practice for microprocessor-based protection equipment firmware control," *IEEE Std C37.231-2006*, pp. 1–25, 2007.

Comment 6: *In terms of the lessons learned from each IDS, a tabulated or graphical presentation would provide a clearer picture of the strengths and weaknesses of each technology and the identified gaps. More statistical data about the accuracy and precision of these methods and their reliability for the system would be beneficial.*

Response: We thank the Reviewer for the constructive comment. We have added TABLEs II and III to summarize the scenarios, adopted tools and methods, and statistical performance metrics of reviewed intrusion detection systems (IDSs). The cons and pros of each type of IDS as well as research trends and gaps are highlighted in learned lessons. Moreover, from a high-level perspective, a set of evaluation metrics regarding the IDS is refined from the summary: 1) Performance-related metrics: detected attack types, detection accuracy, and detection latency; 2) Cost-related metrics: memory and computation overhead, hardware investment, and control and operation performance sacrifice. The design of IDS should at least consider one type of performance- and cost-related metrics and address the tradeoff issue between them. However, it is indeed difficult to give a comparative study regarding all IDS methods in the literature due to the lack of a set of benchmark testbeds or datasets. On one hand, it is unrealistic to establish a high-fidelity smart grid testbed without considering space and budget limitation. On the other hand, the sensitivity information contained in the real-world power system data hinders its disclosure for research purpose. Many efforts are still required from academic and industry as well as governments to address this critical issue and pave the way towards the cyber-resilient smart grid under highly penetrated DERs.

TABLE II: Summary of IDSs

Type	Lit.	Scenario	Tools/Methods	Evaluation Metrics	Lessons Learned
Host-based IDSs					
Signature-	[28]	Upper hosts	Tripwire, Tanium, OSSEC, etc.	Attack: Known attacks; Detection latency: Timely	1) Current research status regarding HIDSs mainly focuses on the upper hosts and smart meters. 2) As the most basic components that interfaces renewable sources with power grid, the energy conversion devices like converters have not obtained enough attention. 3) It is challenging to attain comparable performance using strictly limited resources on inverters.
Anomaly-	[130]	Smart meter	Abstract model based verification of core system calls	Attack: Known and unknown; Coverage: 100% known and 69.9% unknown; Latency: 10s; Memory overhead: 4.15%	
	[132], [133]	Inverter controller	Custom-built HPCs and time series analysis	Attack: Firmware modification; Accuracy: 97.22%	
Hybrid	[131]	Smart meter	Collaborative signature and anomaly combined detection	Attack: Known and unknown; Accuracy: >80%; Memory overhead: 0.8%	
Network-based IDSs					
Signature-	[29]	DER comm. network	Snort with default rules	Attack: 5 scenarios; Detection coverage: 60%; Memory overhead: 31.25%	1) Extra communication components like switches and network taps are usually required to ensure that NIDSs can access required network traffic for monitoring, and thus achieve expected detection performance. Therefore, the deployment cost of NIDSs has to be concerned in the planning phase with numerous geographically dispersed terminal devices in the DER-based smart grid. 2) The signature-based NIDS can generate a highly reliable result regarding known attacks, but is not capable of addressing unknown attacks even if they are very similar to known attacks. On the contrary, the anomaly-based NIDS can handle unknown attacks such as zero-day attacks, while its rate of false positive alarms is higher than that of the signature-based NIDS. The combination of the basic principles of signature- and anomaly-based methods to enhance NIDS's detection performance is still not clear. 3) The NIDS based on general network features can be easily applied to various scenarios regardless of the communication protocol and communication architecture, while the NIDS using specific protocol-specific features can lead to better detection performance in terms of accuracy and response time. To meet the increasing applicability and performance requirements, more efforts should be devoted to the design of NIDSs incorporating both general network and protocol-specific features.
	[136]	DER comm. network	Cross-level Snort-based detection with tailored rules	Attack: DoS attack; Accuracy: 100%; Latency: ≤500ms	
	[137]	DER comm. network	Suricate with stateful rules	Attack: FDI attack; Accuracy: 100%; Latency: N.A.	
	[137]	DER comm. network	Attack table, Temporal failure propagation graph	Attack: DoS and FDI attacks; Accuracy: 100%; Latency: N.A.	
Anomaly-	[29], [139]	DER comm. network	Adaptive resonance theory artificial NN	Attack: 5 scenarios; Detection coverage: 80%; Memory overhead: 45%; Train/test latency: 33ms/14ms	
	[140], [141]	AMI	Support vector machine, Artificial immune systems, State machines	Attack: FDI, DoS, and eavesdropping attacks; Accuracy: 99.33%; Latency: N.A.	
	[142]	GOOSE and SV network	Collaborative and distributed intrusion detection with normal behaviour model	Attack: FDI attack; Accuracy: N.A.; Latency: 2ms; Memory overhead: 2%	
	[143]	GOOSE network	A finite state machine model	Attack: FDI attack; Accuracy: 95%; Latency: 0.06ms;	
	[144]	IEC 61850 network	Access control, Protocol whitelisting, Multiparameter-based detection	Attack: DoS and FDI attacks; Accuracy: 100%; Latency: <0.3ms	
	[145]	ZigBee network	Normal behaviour model established referring to SEP 2.0 and IEEE 802.15.4 standards	Attack: FDI, replay, and DoS attacks; Accuracy: ≥92.5%; Latency: N.A.	
	[146]	GOOSE and MMS network	Statistical traffic features and specification-based metrics	Attack: 27 scenarios; Accuracy: 98.89%; Latency: N.A.	
	[147]	SCADA network	Traffic data characteristics of transport, operation, and content levels	Attack: 12 scenarios; Accuracy: 100%; Latency: 423ms	
Physics-based IDSs					
Data-	[148]	EMS	Kernel SVR	Attack: FDI attack; Accuracy: 100%; Latency: 2 hours	1) Generally speaking, the HIDS and NIDS can perceive the anomalous traces on host and network related features resulted from malicious intruders, with a quicker rate, than the PIDS as the adversary will not disrupt the physical functionalities immediately after intruding the DER communication network. But the PIDS works as the last detection layer by observing the induced physical impacts when the HIDS and PIDS are both invalidated. 2) The data-driven and model-based PIDSs have their own cons and pros. The data-driven PIDS can achieve satisfactory detection performance against a wide varieties of cyberattacks without requiring any model knowledge. But it relies heavily on the diversity of training data and requires powerful computation resource, and the inexplicable detection results also limits its widespread application. The model-based PIDS is capable to detect known types of cyberattacks in a timely and reliable manner with explainable detection results and acceptable computation burden. However, the detection performance can degrade significantly when the system parameters vary and it only works under limited types of cyberattacks.
	[150]	Microgrid	Auto-regressive exogenous model NN	Attack: FDI attack; Accuracy: 100%; Latency: N.A.	
	[151], [152]	EV and PV farm	LSTM and CNN classifiers, Physics-guided features	Attack: Replay and FDI attacks; Accuracy: ≥98.44%; Latency: N.A.	
	[153]-[155]	PV farm	LSTM and CNN classifiers, Transfer learning	Attack: FDI attack; Accuracy: ≥95.23%; Latency: N.A.	
	[156]	Microgrid	STL requirements based specifications	Attack: DoS and FDI attacks; Accuracy: 100%; Latency: <1s	
Model-	[157], [158]	Substation	On-the-fly power system dynamics simulation	Attack: FDI attack; Accuracy: 83%; Latency: 859ms	
	[159]	Microgrid	Consensus-oriented metric CVF	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[160]	Microgrid	Dual variable-related detection metrics	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[161], [162]	Microgrid	Luenberger observer, UIO	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[163]	Microgrid	Candidate invariant	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[164]	Microgrid	Stable kernel representation	Attack: FDI attack; Accuracy: 100%; Latency: <1s	
	[166], [167]	Microgrid	Watermarking, Primary control gain perturbation	Attack: FDI and replay attacks; Accuracy: 100%; Latency: <1s; Proactive cost: Neglectable	

TABLE III: Summary of IDSs (Continue of TABLE II)

#	Lit.	Scenarios	Tools/Methods	Evaluation Metrics	Lessons Learned
Physics-based IDSs					
Data and model blended	[168]	State estimation	LSTM, Event-triggered MTD	Attack: FDI attack; Accuracy: 98.16%; Operation cost: 0.5%	3) The data and physics blended PIDS has became a prevailing topics as it is particularly suitable for the DER-based smart grid with massive measurement data and well-known physical dynamics. 4) The proactive detection strategy by perturbing system parameters can enhance the detection capability against powerful adversaries with acceptable sacrifice on either control or operation performance.
	[169]	AGC	CNN, LSTM, DNN, knowledge of physics	Attack: FDI atatck; Accuracy: 93.2%; Latency: N.A.	
	[170]	Energy theft	Linear regression, Power flow dynamics	Attack: FDI attack; Accuracy: 94%; Latency: N.A.	
	[171]	Grid-tied converter	Spline learning, Power electronics dynamics	Attack: FDI attack; Accuracy: 98.23%; Latency: 25ms	
	[?]	State estimation	Graph convolutional network	Attack: FDI attack; Accuracy: 99.25%; Latency: N.A.	

The related modifications can be only found in the full-version revised manuscript (Page 13, right column, and in the bottom).

Comment 7: *The mitigation section could be enriched by including specific model-based or model-free techniques*

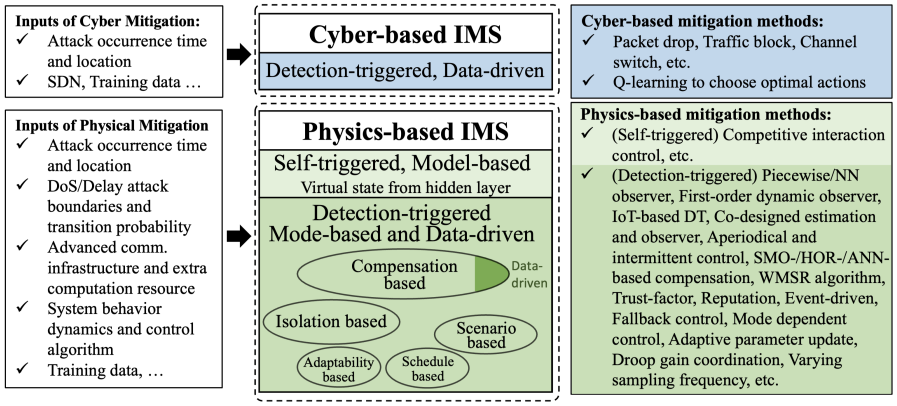

Fig. 8: Summary and classification of IMSs.

commonly employed in defense and mitigation. For the recovery techniques, contrasting the impact of cyber threats on restoration and black start methods with extreme events would be worthwhile, and how the recovery algorithm using restoration will be recovering the system from the cyber events.

Response: We thank the Reviewer for the constructive comment. We have added a classification dimension for the reviewed impact mitigation systems (IMSs) as model-based or data-driven as shown in Fig. 8. The cyber-based IMSs are all data-driven, and most physics-based IMSs are model-based with only a few being data-driven. This phenomenon is caused by the inherent difficulty of recovering control-acceptable healthy data from compromised data using purely data-driven methods, since it is difficult to train the model covering all possible attack forms.

According to NIST's guide for cybersecurity event recovery [126], the recovery schedule comprises Phase I: Prepare personnel and communication, Phase II: Learn attack and mitigation situations, and Phase III: Determine recovery the order as shown in Fig. 9. Phases I and II are more like preparation steps based on the information from the previous detection and mitigation steps, and Phase III is the core part that determines the recovery order of blackout areas, compromised cyber components, and damaged physical equipment to achieve the restoration of power supply and infrastructure functionalities.

Moreover, TABLE IV is given to clarify the differences between the focused cyber-recovery and conventional black-start and physical-recovery. In particular, the black-start service aims to energize power grid without requiring external power supplies in the event of partial or total shutdown, and the generator providing this service is called as black-start capable generator like diesel generators. The feasibility of using DERs to provide a "bottom-up" black start approach has been investigated [127], which has potential advantages of reduced restoration time and more flexible recovery procedure compared with the conventional large thermal plants. These black-start capable DER units can also provide ancillary services like reactive power support to assist the voltage control during synchronization and grid reconnection [128].

The black-start capable units are adopted in both the physical- and cyber-recovery processes to restore the power supply service in the physical side. Besides that, the reestablish of communication network is also involved when the extreme event damages/compromises cyber components and induces network disconnection. The difference between physical- and cyber-recovery processes in restoring the power supply service lies in their focuses. The physical-recovery *mainly* focuses on the power grid energization in the *physical* side since natural disasters usually first damage physical power lines and generators [21]. While the cyber-recovery needs to concern both the physical side's grid energization and cyber side's communication network reestablishment as cyberattacks will first invalidate cyber components and then affect the power supply service. In restoring the infrastructure functionality, the cyber-

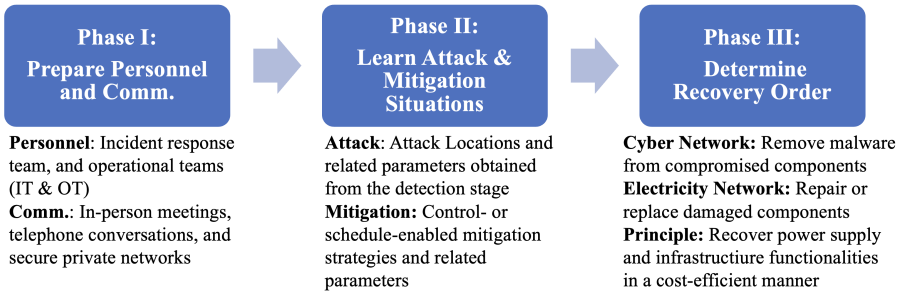

Fig. 9: Phases included in the general recovery plan under cyberattacks.

TABLE IV: Comparsions between black-start, physical-recovery, and cyber-recovery.

Tasks	Black-Start	Phyical-Recovery under Natural Disasters	Cyber-Recovery under Attacks
Power Supply Service	*Physical*: Energize power grid without requiring external power supplies in the event of partial or total shutdown	*Cyber*: Reestablish comm. network utilizing mobile comm. vehicles or other resources (*Occasional*) *Physical*: Energize power grid utilizing mobile generation vehicles and black-start generators (*Main*)	*Cyber*: Reestablish comm. network utilizing mobile comm. vehicles or other resources (*Main*) *Physical*: Energize power grid utilizing mobile generation vehicles or black-start generators (*Main*)
Infrastructure Function	N.A.	*Cyber and Physical*: Repair or replace damaged components	*Cyber*: Remove cyber malware *Physical*: Repair or replace damaged components

recovery needs to additionally schedule recovery crews to remove the cyber malware compared with the physical-recovery. Two key challenges of cyber-recovery are thereby identified: i) Particular attention should be paid to the cyber-side modeling and the resultant strong cyber-physical coupling may complicate the recovery schedule problem; ii) Additional attack movements may occur when the adversary perceives the recovery actions. The incorporation of this kind of attack movement usually requires to solve multiple-level optimization problems, posing nontrivial challenges for the solving process.

In the revised manuscript, the modification is in Section VII, page 11, right column, and in the bottom.

[21] C. Wang *et al.*, "Cyber-physical interdependent restoration scheduling for active distribution network via ad hoc wireless communication," *IEEE Transactions on Smart Grid*, 2023

[126] M. Bartock, *et al.*, "Guide for cybersecurity event recovery," 2016.

[127] W. Yan *et al.*, "Feasibility studies on black start capability of distributed energy resources," 2021.

[128] K. B. Ganesh *et al.*, "Ancillary services from ders for transmission and distribution system operators," in 2022 22nd National Power Systems Conference (NPSC). IEEE, 2022, pp. 482–487.

Comment 8: *Lastly, for the challenges and future directions, utilizing tabular forms and conceptual diagrams with observable metrics would greatly help summarize the survey's outcomes and support the proposed methods.*

Response: We thank the Reviewer for the constructive comment. In the full-version revised manuscript, we have added a diagram to clearly indicate the challenges and future directions following the holistic resilience enhancement framework as shown in Fig. 10, where the five aspects encompassing identification, prevention, detection, mitigation, and recovery are included.

Minor Comments

Comment 1: *Some references need to be properly formatted or included.*

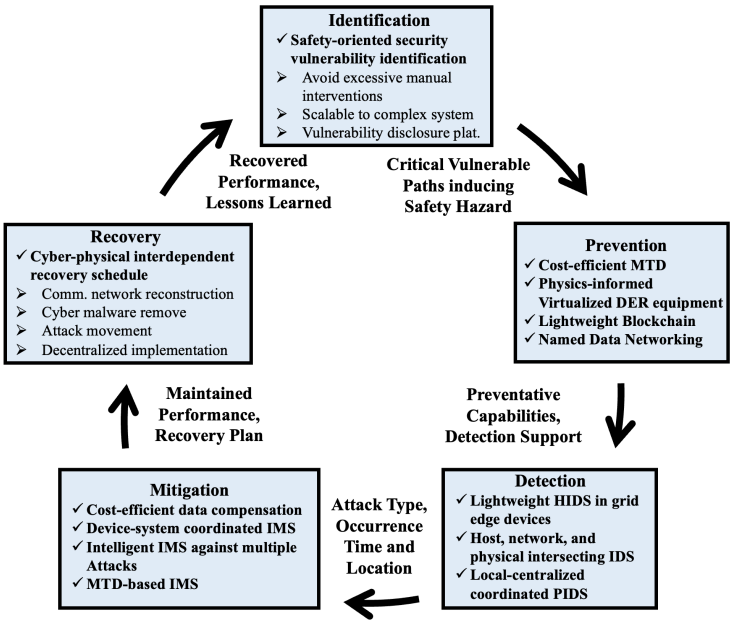

Fig. 10: Future directions that can further enhance grid resilience.

Response: We thank the Reviewer for the constructive comment. We have standardized the reference format and included some critical references as required.

Comment 2: *Fig. 5 has a box obscuring the text, making it unreadable; it needs adjustment.*

Response: We thank the Reviewer for the constructive comment. We have removed the box from Fig. 5.

Comment 3: *A proofreading round is necessary to enhance sentence structure and readability.*

Response: We thank the Reviewer for the constructive comment. We have proofread the manuscript thoroughly to enhance its logic and readability.

Comment 4: *Table I could be condensed or introduce simple metrics to improve understanding.*

Response: We thank the Reviewer for the constructive comment. We have classified the attack techniques in TABLE I as initial access acquisition, information discovery, and execution and implication according to the adversary's intrusion and execution phases.

TABLE V: Comparison between our survey and existing surveys

Resilience Enhancement Phases		[40]	[20]	[17]	[10]	[41]	[42]	[43]	This Paper
Threat Identification	Adversary Model	F	N	N	N	N	N	N	F
	Vulnerability Coverage	M	P	P	M	M	M	F	F
	Risk Assessment	P	F	P	F	F	P	P	F
Defense-in-Depth Strategies	Prevention	M	N	M	N	M	P	N	F
	Detection	P	N	N	M	M	M	M	F
	Mitigation	P	P	P	P	P	M	P	F
	Recovery	N	N	N	N	N	N	N	F

F: Fully Covered, M: Mostly Covered, P: Partially Covered, N: Not Covered

Reviewer 2's Comments

Summary: *The authors have provided a comprehensive overview of the cybersecurity of DER-based smart grids. The authors have effectively organized the research papers into several topics, including threat modeling, risk assessment, intrusion prevention systems, intrusion detection systems, and mitigation methodologies.*

Response: We thank the Reviewer for the nice summary. According to the comments, we have systematically compared this survey with existing surveys, proofread all writing typos, and added an acronym table in the revised manuscript.

To adhere to the page requirement of the initial submission, certain sections of the manuscript have been streamlined. For a more comprehensive understanding, the full-version revised manuscript can be accessed for additional reading.

Comment 1: *There are several high-quality review papers on the cybersecurity of DERs, including one published in IEEE ACCESS. However, this published paper is not listed in the reference list, and it appears to have some overlaps with the content of this manuscript. The authors need to justify the uniqueness by comparing it to the published paper listed below.*

[33] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy," in *IEEE Access*, vol. 10, pp. 35846-35875, 2022.

Response: We thank the Reviewer for the constructive Comment. We have addressed the critical contributions made by reference [33], which discussed the vulnerabilities of typical inverter-based power system with DER integration, nature of several types of cyberattacks, state-of-the-art defense strategies including detection and mitigation techniques. Compared with [33], our survey provides a more comprehensive threat identification model including adversary model and risk assessment, and more extensive coverage of defense-in-depth strategies especially on prevention, mitigation, and recovery. To highlight the completeness of this survey, the comparative results in terms of threat identification and defense-in-depth strategies have been summarized in TABLE V.

In the revised manuscript, the related modification is in Page 2, right column, and in the bottom.

Comment 2: *In Section V-A, the term "advanced AMI" is confusing because AMI already stands for advanced metering infrastructure. Does it refer to a new generation or an upgrade of AMI?*

Response: We thank the Reviewer for the constructive comment. We have revised this typo and proofread the whole paper thoroughly to avoid similar errors.

Comment 3: *It is suggested to list all acronyms in a table to enhance the accessibility of the manuscript and aid readers in understanding the content more easily.*

Response: We thank the Reviewer for the constructive Comment. In the full-version revised manuscript, we have

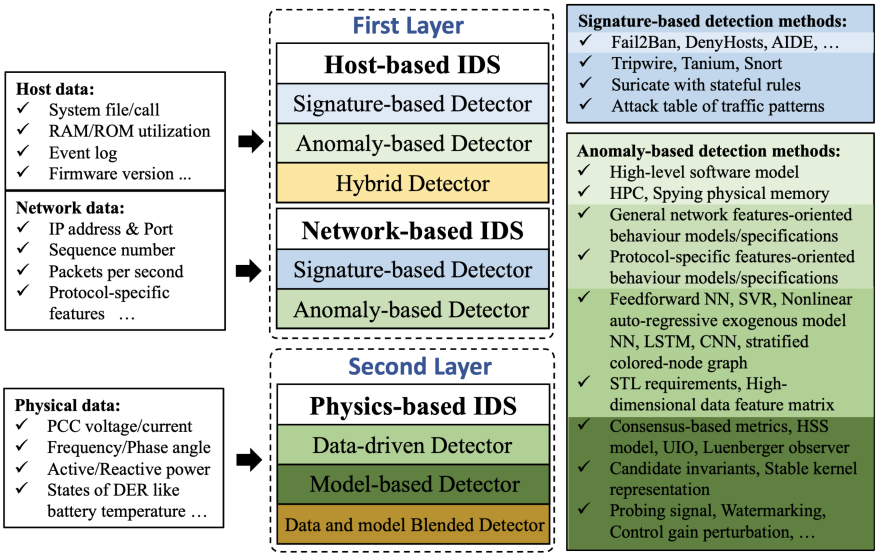

Fig. 11: Summary and classification of IDSs.

added a table of acronyms in the beginning of the revised manuscript (after the abstract) to improve its readability.

Reviewer 3's Comments

Summary: *This paper presents a survey on cyber-physical security in DER-enabled power systems. Here are the detailed comments.*

Response: We thank the Reviewer for the nice summary. According to the comments, we have made the following modifications in the revised manuscript:

- The data and model blended detection methods have been reviewed (Response to comment 1).
- The cons and pros of detection and mitigation methods have been summarized in tables (Response to comment 2).
- The evaluation metrics of detection and mitigation methods have also been discussed (Response to comment 3).
- The generation of risk assessment matrix that informs the system operator about the attack scenarios' severity has been elaborated (Response to comment 4).
- The differences among black-start, physical-recovery under natural disasters, and cyber-recovery under attacks have been extensively illustrated (Response to comment 5).

To adhere to the page requirement of the initial submission, certain sections of the manuscript have been streamlined. For a more comprehensive understanding, the full-version revised manuscript can be accessed for additional reading.

Comment 1: *In Section V-C, it is important to include hybrid approaches (i.e., physics-enhanced data-driven methods), which are not currently discussed in this paper.*

Response: We thank the Reviewer for the constructive comment. We have discussed the data and model blended detectors in the physics-based intrusion detection systems (IDS) as shown in Fig. 11. The particular discussion in the revised manuscript is as follows:

(Page 9, right column, and in the top) The data and model blended PIDS has also attracted increasing attention recently due to its benefits in performance enhancement and data requirement reduction. By incorporating physical dynamics into the data recovery algorithm, Xu *et al.* proposed a blending data-driven and physics-based approach to improve the detection accuracy while reduce the operational cost resulted from MTD [113]. Based on the combination of prior knowledge of physics and system metrics, a physics-informed context-based anomaly detection method was proposed to counter the stealthy attacks against agc [114]. To achieve timely and accurate attack localization and also output explainable detection results, Peng *et al.* incorporated the nodal admittance matrix and physical property of power grid into the graph convolutional network [115].

[113] W. Xu *et al.*, "Blending data and physics against false data injection attack: An event-triggered moving target defence approach," *IEEE Transactions on Smart Grid*, vol. 14, no. 4, pp. 3176–3188, 2023.

[114] M. N. Nafees *et al.*, "On the efficacy of physics-informed context-based anomaly detection for power systems," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2022, pp. 374–379.

[115] S. Peng *et al.*, "Localizing false data injection attacks in smart grid: A spectrum-based neural network approach," *IEEE Transactions on Smart Grid*, pp. 1–1, 2023.

In summary, this kind of data and model blended IDS is of great practical importance as it incorporates the pros of advanced data-driven methods and the well-recognized model knowledge of smart grid. More attentions are still needed to illustrate the integration scheme of historical data and model knowledge and prove its potential for detection performance improvement.

Comment 2: *What are the advantages and disadvantages of the mitigation methods (compensation-based, isolation-based, scenario-based, adaptability-based, and schedule-based) in physical-based detection-triggered IMS? It would be beneficial to provide a comprehensive table outlining all of the advantages and disadvantages.*

Response: We thank the Reviewer for the constructive comment. We have provided TABLE VI in Page 18 of the full-version revised manuscript to summarize the reviewed mitigation methods with particular attentions on applied scenarios, adopted tools/methods, and evaluation metrics. Moreover, the cons and pros of each type of IMS as well as research trends and gaps are highlighted in learned lessons. For the five mitigation strategies of physics-based detection-triggered IMSs, their features including pros and cons are summarized as follows:

- The most common compensation-based strategy can work for both FDI and DoS attacks, and usually needs to integrate robust control, adaptive control, and NN methods to estimate the injected bias/healthy data.
- The isolation-based IMS can be regarded as the simplest strategy, but it only works under FDI attacks and is subject to the number of attacks.
- The scenario- and adaptability-based IMSs are usually used to counter DoS attacks, where the former is customized for attack scenarios (less conservativeness, limited attack scenarios) and the latter adapts automatically without requiring specific attack information (more conservativeness, unlimited attack scenarios).
- The schedule-based IMS can mitigate both FDI and DoS attacks but needs to utilize extra flexible resources.

In the revised manuscript, the related modifications are in Page 11, left column, and in the bottom.

Comment 3: *Could the authors summarize the evaluation matrix for the performance of the detection and mitigation algorithms for the DER-enabled power system? This would help readers understand the criteria used to evaluate the effectiveness of these algorithms.*

Response: We thank the Reviewer for the constructive comment. In the full-version revised manuscript, we have summarized the evaluation metrics from the aspects of performance and cost that have been adopted by detection and mitigation methods as follows:

TABLE VI: Summary of IMSs

Types	Lit.	Scenarios	Methods/Ideas	Evaluation Metrics	Lessons Learned
Cyber-based IMSs					
Detection-triggered, Data-driven	[31], [141]	DER comm.	Block network traffic	Attack: DoS and FDI attacks; Effect: Isolation; Extra cost: No	1) Cyber-side aggressive actions may affect physical functionalities. 2) Knowledge from the physical side can be integrated to improve the performance.
	[171]	Microgrid comm.	SDN enabled traffic block	Attack: FDI and replay attacks; Effect: Isolation; Extra cost: SDN	
	[144]	ZigBee HAN	Q-learning	Attack: FDI and replay attacks; Accuracy: 93.46%; Latency: Neglectable	
Physics-based IMSs					
Detection-triggered, Compensation-based	[172]	LFC	Piecewise observer based robust control	Attack: Resources constrained FDI and DoS attacks; Effect: H_∞ performance guarantee; Extra cost: No	**Comparisons between Detection- and Self-triggered IMSs:** 1) Majority of physics-based IMSs are detection-triggered, and only a small portion are self-triggered. 2) Although the self-triggered does not require the inputs from IDSs, which can avoid potential false positive alarms, two limitations also come along with this cons: i) A hidden secure network layer independent from the original control layer should run all the time, inducing extra computation and communication overheads; ii) The introduction of hidden layer can expose larger attack surfaces if not equipped with appropriate security strategies. The two limitations hinder the further investigation of self-triggered IMSs. **Comparisons of different Detection-triggered IMSs:** 3) After incorporating the inputs of IDSs, much more mitigation strategies like isolation- and scenario-base for the detection-triggered IMSs. The most common compensation-based strategy can work for both FDI and DoS attacks, and usually needs to integrate robust control, adaptive control, and NN methods to estimate the injected bias/healthy data. The isolation-based IMS can be regarded as the simplest strategy, but it only works under FDI attacks and is subject to the number of attacks. The scenario- and adaptability-based IMSs are usually used to counter DoS attacks, where the former is customized for attack scenarios and the latter adapts automatically without requiring specific attack information. The schedule-based IMS can mitigate both FDI and DoS attacks by utilizing flexible resources. 4) It is not hard to observe that the performance of each IMS can be guaranteed only when the adversary's capability is restricted like bounded FDI attacks. In particular, the compensation-/isolation-/scenario-/adaptability-based IMSs try to enhance the tolerance of control algorithms against cyberattacks and can work immediately once perceiving anomaly. When the adversary's capability exceeds control algorithms' tolerance, the schedule-based IMS is expected to alleviate the severe consequence by adopting available flexible resources. Hence, the cooperative design of control-enabled and schedule-driven mitigation strategies can defend against a wider range of attacks. 5) The investigation of data-driven physics-based IMSs is rare, and most of them are model-based. This phenomenon is caused by the inherent difficulty of recovering control-acceptable healthy data from compromised data using purely data-driven methods, since it is difficult to train the model covering all possible attack forms.
	[173]	Variable-speed WT	NN observer, Dual-triggered control	Attack: Resources constrained DoS attack; Effect: Exponential convergence guarantee; Extra cost: No	
	[174]	Microgrid control	First-order dynamic observer	Attack: Resource constrained DoS attack; Effect: Exponential convergence; Extra cost: No	
	[175]	Microgrid control	IoT-based DT, Luenberger observer	Attack: DoS and FDI attacks; Latency: Timely; Extra cost: DT, Cloud service	
	[176]	Microgrid control	SMO and HOD	Attack: Bounded FDI attack; Effect: Lyapunov stable; Extra cost: No	
	[177]	Microgrid control	Robust output feedback control	Attack: Bounded FDI attacks; Effect: L_2-gain boundedness; Extra cost: No	
	[178]	Microgrid control	Adaptive observer	Attack: Bounded (unbounded) FDI attacks; Effect: UUB (Asymptotic) stability; Extra cost: No	
	[179]	Microgrid control	ANN, PI-based controller	Attack: FDI attack; Effect: Compensation error $\leq 0.02\%$; Latency: $<$0.15s; Extra cost: No	
	[180]	Microgrid control	Nonlinear adaptive observer	Attack: FDI attack; Effect: Input-to-state stability; Extra cost: No	
	[181]	Microgrid control	Impact-oriented compensation	Attack: Constant FDI attack; Latency: 2s; Extra cost: No	
	[182]	Variable-speed WT	Adaptive resilient control	Attack: Bounded FDI attack; Effect: UUB stability; Extra cost: No	
Detection-triggered, Isolation-based	[183]	Microgrid control	Aperiodically intermittent control	Attack: Quantitatively limited FDI attack; Effect: Asymptotically stability; Extra cost: No	
	[184], [185]	ED and Microgrid	WMSR algorithm	Attack: Quantitatively limited FDI attack; Effect: Optimal dispatch, Asymptotically stability; Extra cost: No	
	[186]-[188]	Microgrid control	Trust-factor based control	Attack: Quantitatively limited FDI attack; Effect: Asymptotically stability; Extra cost: No	
	[189], [190]	ED	Reputation-driven bad data replacement	Attack: Quantitatively limited FDI attack; Effect: Optimal dispatch; Extra cost: Multiple-hop communications	
	[191], [192]	Microgrid control	Event-driven bad data replacement	Attack: Quantitatively limited FDI attack; Effect: Successful mitigation: Extra cost: No	
Detection-triggered, Scenario-based	[193]	ESS management	Rule-based fallback control	Attack: DoS attack; Effect: Maintain ESSs' SOC within allowable limits; Extra cost: No	
	[194]	Microgrid control	Adaptive control, network reconfiguration	Attack: Resource constrained DoS attack; Effect: Stochastic stability; Extra cost: network configuration	
	[195]	Microgrid control	Mode dependent control	Attack: Resource constrained Markovian DoS attack; Effect: Stochastic stability; Extra cost: No	
Detection-triggered, Adaptability-based	[33]	Microgrid control	Adaptive control	Attack: Resource constrained DoS attack; Effect: Secure consensus; Extra cost: No	
	[196]	Microgrid control	Adaptive event-triggered control	Attack: Resource constrained DoS attack; Effect: Global asymptotically stability; Extra cost: No	
Detection-triggered, Schedule-based	[197]	LFC	DER droop schedule	Attack: IoT Botnet attack; Effect: Exponentially stability; Extra cost: Operational cost	
	[198], [199]	Microgrid control	Sampling frequency adjustment	Attack: Resource constrained DoS attack; Effect: Asymptotically stability; Extra cost: More communication	
Self-triggered, Compensation-based	[32], [200], [201]	Microgrid control	Competitive interaction control	Attack: Bouded and unbounded FDI attacks; Effect: Input-to-state and UUB stability; Extra cost: SDN based secure hidden communication layer	

- (Page 13, right column, and in the bottom) 1) Performance-related intrusion detection system (IDS) metrics: detected attack types, detection accuracy, and detection latency; 2) Cost-related IDS metrics: memory and computation overhead, hardware investment, and control and operation performance sacrifice. The design of IDS should at least consider one type of performance- and cost-related metrics and address the tradeoff issue between them.
- (Page 17, left column, and in the middle) 1) Performance-related impact mitigation system (IMS) metrics: mitigated attack types and mitigation effects; 2) Cost-related IMS metrics: computation and communication overhead and hardware investment. It is recommended to appropriately balance the tradeoff between these metrics when designing IMSs.

The above summary only explains a very high-level evaluation metrics, while more specific descriptions can refer to TABLEs II, III (Responses to reviewer 1), and VI. Nonetheless, it is indeed difficult to give a comparative study regarding all detection/mitigation methods in the literature due to the lack of a set of benchmark testbeds or datasets. On one hand, it is unrealistic to establish a high-fidelity smart grid testbed without considering space and budget

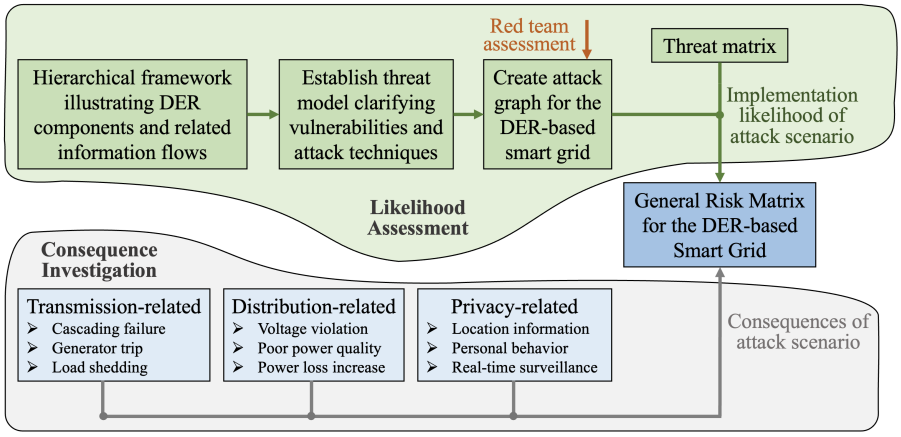

Fig. 12: Generation scheme of the risk matrix for the DER-based smart grid.

limitation. On the other hand, the sensitivity information contained in the real-world power system data hinders its disclosure for research purpose. Many efforts are still required from academic and industry as well as governments to address this critical issue and pave the way towards the cyber-resilient smart grid under highly penetrated DERs.

Comment 4: *Can the authors elaborate on the attack impact assessment? It would be better to summarize or propose an evaluation matrix for cyber-attacks in DERs.*

Response: We thank the Reviewer for the constructive comment. We have proposed a general risk assessment matrix to assess the risk of attack scenarios, which takes inputs of attack implementation likelihoods and attack consequences as indicated by Fig. 12. Please refer to the response to comment 4 of Reviewer 1 for more details.

Comment 5: *When implementing the black start of DER, some issues such as ancillary services and infrastructure systems are also considered. In the Section on recovery strategy, could the authors clarify the difference between the proposed recovery and the black start of DERs in the power system?*

Response: We thank the Reviewer for the constructive Comment. We have systematically compared the proposed cyber-recovery with two existing similar but essentially different services, i.e., black-start and physical-recovery, and TABLE VII is provided to demonstrate these differences.

In particular, the black-start service aims to energize power grid without requiring external power supplies in the event of partial or total shutdown, and the generator providing this service is called as black-start capable generator like diesel generators. The feasibility of using DERs to provide a “bottom-up” black start approach has been investigated [127], which has potential advantages of reduced restoration time and more flexible recovery procedure compared with the conventional large thermal plants. These black-start capable DER units can also provide ancillary services like reactive power support to assist the voltage control during synchronization and grid reconnection [128].

The black-start capable units are adopted in both the physical- and cyber-recovery processes to restore the power supply service in the physical side. Besides that, the reestablish of communication network is also involved when the extreme event damages/compromises cyber components and induces network disconnection. The difference between physical- and cyber-recovery processes in restoring the power supply service lies in their focuses. The physical-recovery *mainly* focuses on the power grid energization in the *physical* side since natural disasters usually first damage physical power lines and generators [21]. While the cyber-recovery needs to concern both the physical

TABLE VII: Comparsions between black-start, physical-recovery, and cyber-recovery.

Tasks	**Black-Start**	**Phyical-Recovery under Natural Disasters**	**Cyber-Recovery under Attacks**
Power Supply Service	*Physical*: Energize power grid without requiring external power supplies in the event of partial or total shutdown	*Cyber*: Reestablish comm. network utilizing mobile comm. vehicles or other resources (*Occasional*) *Physical*: Energize power grid utilizing mobile generation vehicles and black-start generators (*Main*)	*Cyber*: Reestablish comm. network utilizing mobile comm. vehicles or other resources (*Main*) *Physical*: Energize power grid utilizing mobile generation vehicles or black-start generators (*Main*)
Infrastructure Function	N.A.	*Cyber and Physical*: Repair or replace damaged components	*Cyber*: Remove cyber malware *Physical*: Repair or replace damaged components

side's grid energization and cyber side's communication network reestablishment as cyberattacks will first invalidate cyber components and then affect the power supply service.

In restoring the infrastructure functionality, the cyber-recovery needs to additionally schedule recovery crews to remove the cyber malware compared with the physical-recovery. Two key challenges of cyber-recovery are thereby identified: i) Particular attention should be paid to the cyber-side modeling and the resultant strong cyber-physical coupling may complicate the recovery schedule problem; ii) Additional attack movements may occur when the adversary perceives the recovery actions. The incorporation of this kind of attack movement usually requires to solve multiple-level optimization problems, posing nontrivial challenges for the solving process.

In the revised manuscript, the modifications are in Section VII, page 12, left column, in the middle.

[21] C. Wang *et al.*, "Cyber-physical interdependent restoration scheduling for active distribution network via ad hoc wireless communication," *IEEE Transactions on Smart Grid*, 2023.

[127] W. Yan *et al.*, "Feasibility studies on black start capability of distributed energy resources," 2021.

[128] K. B. Ganesh *et al.*, "Ancillary services from ders for transmission and distribution system operators," in *2022 22nd National Power Systems Conference (NPSC)*. IEEE, 2022, pp. 482– 487.

Reviewer 4's Comments

Summary: *This manuscript is basically a survey paper that summarizes issues around resiliency of DER (distributed energy resources) systems. The manucript covers threat modelling, risk analysis, defence strategies (prevetion, detection, impact mitigation, and recovery). The topic is of practical importance and summary of this sort would be helpful for researchers that are new to the area (however i am not sure it is suitable for this specific journal). Authors well summarizes the threat models and attack surface.*

Response: We thank the Reviewer for the nice summary. According to the comments, we have highlighted and reformulated the novelty and motivation of this survey, elaborated the implementation, recommendations, and compatibility of security technologies, and added the discussions of some critical literature as required in the revised manuscript.

To adhere to the page requirement of the initial submission, certain sections of the manuscript have been streamlined. For a more comprehensive understanding, the full-version revised manuscript can be accessed for additional reading.

Comment 1: *Because its nature is summarizing literature, I didn't find much new insight from this paper. On the other hand as a survey paper the coverage is not enough in some parts. also overall the discussion is shallow and high-level. Moreover, in the intro authors claim that "holistic framework is proposed", authors only enumerate discussion points and didn't discuss the concrete system design or implementation at all. If it is claimed as a contribution, I strongly suggest to add (at least) discussion on actual system design (e.g., which security technologies are used in each part of the system).*

Response: We thank the Reviewer for the constructive Comment. The main novelty of this survey is to provide a systematical review on existing identification, prevention, detection, mitigation, and recovery standards/methods/literature standing on the perspective of cyber-resilience-enhancement (CRE) of DER-based smart grid. To the best of the authors' knowledge, it is the first time to conduct such extensive review and systematical summary of CRE works in the area of DER-based smart grid. To better clarify this paper's motivation and contributions, we have compared it with several state-of-art survey papers mainly discussing the cybersecurity issue of smart grid and listed the results in TABLE V (Response to comment 1 of Reviewer 2).

Besides, we have specified implementation guidance, recommendations, benefits, and limitations of these CRE strategies in the revised manuscript:

- (Page 5, left column, and in the bottom) For threat identification, the steps of generating risk assessment matrix has been illustrated with demonstrative application to EVs.
- (Page 5, right column, and in the bottom) For prevention technologies, implementation guidance and recommendations on network architecture, access control, communication protocol, and software update have been provided.
- (Section V and section VI) For detection and mitigation methods, systematical classification and insightful summary of cons, pros, and involved evaluation metrics have been included to guide the further improvement.
- (Page 11, right column, and in the bottom) For cyber-recovery schedule, its differences from existing black-start and physical-recovery and its key challenges have been highlighted to appeal further investigation.

Comment 2: *Besides, some citation and/or discussion could be added for the sake of comprehensiveness. Below are some suggestions. - When authors discuss defence in depth, it is also important to consider compatibility among different kinds of cybersecurity solutions. Such tabilation in different context is found in the paper below.*

TABLE VIII: Pairwise Comparisons of the Capability between Defense-in-Depth Strategies

Defense-in-Depth Strategies		(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Prevention	Network Segmentation (1)		N	N	N	N	N	N	N	N	N
	Access Control (2)	D		N	N	N	N	N	N	N	N
	Secure Comm. Protocol (3)	D	D		N	N	C	C	C	C	C
	Software Upd. Verification (4)	D	D	D		N	N	N	N	N	N
Detection	Host-based IDS (5)	N	N	N	N		N	N	N	N	N
	Network-based IDS (6)	N	N	C	N	N		N	N	N	N
	Physics-based IDS (7)	N	N	C	N	N	N		N	N	N
Mitigation	Detection-triggered IMS (8)	N	N	C	N	D	D	D		N	N
	Self-triggered IMS (9)	N	N	C	N	N	N	N	N		N
Cyber-physical Interdependent Recovery (10)		N	N	C	N	D	D	D	D	D	

D: Dependency, N: Neural, C: Conflict

[215] Tan, Heng Chuan, *et al*. "Tabulating cybersecurity solutions for substations: Towards pragmatic design and planning." *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*. IEEE, 2019.

Response: We thank the Reviewer for the constructive comment. In the full-version revised manuscript (page 19, left column, and in the bottom), we have provided TABLE VIII to summarize pairwise comparisons of the capability between defense-in-depth strategies, i.e., how much each defense mechanism supports one another to achieve defense-in-depth protection [215].

Pairwise comparisons of the capability between defense-in-depth strategies are summarized in TABLE VIII, i.e., how much each defense mechanism supports one another to achieve defense-in-depth protection [215]. In particular, the network segmentation is the most basic cyber prevention technology, and it does not requires dependencies from other technologies. Based on a well-segmented network architecture, an appropriate access control mechanism is developed to grant participators' accesses to resources with different criticality. Then, secure communication protocols are designed to allow entities to transmit information in a secure manner. On top of these three prevention technologies, the code-signing software update scheme is established to guarantee the integrity of installed software. The conflict mainly comes from the computation burden resulted from encryption-enabled secure communication protocols, which may degrade the subsequent detection, mitigation, and recovery performance and even invalidate these functionalities. Moreover, the dependency relation also exists between IDSs and detection-triggered IMSs as well as recovery and IDSs/IMSs.

Comment 3: *Regarding cryptographic protection, such as message authentication, a recent TSG articls discusses a low-latency scheme for IEC 61850 and GOOSE and SV commmuncation. Also I am sure much more schemes in this category. Since it is essential for securiing the DER system, authors should expand the discussion.*

[82] Esiner, Ertem, *et al*. "LoMoS: Less-online/more-offline signatures for extremely time-critical systems." *IEEE Transactions on Smart Grid* 13.4 (2022): 3214-3226.

Response: We thank the Reviewer for the constructive comment. We have addressed the less-online/more-offline signatures model proposed by [82] and its advantages in meeting the stringent latency and messaging throughput requirements. In the revised manuscript, the modification is as follows:

> (Page 7, left column, and in the top) In order to meet the stringent latency and messaging throughput requirements while retaining the benefits of public key cryptography, less-online/more-offline signatures model was proposed to allow the verification to be divided into online/offline phases such that online verification does not perform any expensive operations [82].

Comment 4: *Regarding virtualized DER equipments, the concept is closely related to in-network deception technologies. Such a scheme for IEC 61850 based system was discussed in the paper below, for instance. Also more papers in honeypot technologies for smart grid can be found.*

[133] Yang, Dianshi *et al.* "DecIED: Scalable k-anonymous deception for iec61850-compliant smart grid systems." *Proceedings of the 6th ACM on Cyber-Physical System Security Workshop*. 2020.

Response: We thank the Reviewer for the constructive comment. We have discussed the creation of virtual IEDs that imitates the device characteristics and communication models of IEC 61850-compliant IEDs, which can realize k-anonymous smokescreen by virtually showing $k-1$ indistinguishable decoy devices [133]. In the full-version revised manuscript, the modification is as follows:

(Page 11, left column, and in the middle) Besides virtual DER devices, the methodology of creating virtual IEDs named as DecIED that imitates the device characteristics and communication models of IEC 61850-compliant IEDs was proposed, which can realize k-anonymous smokescreen by virtually showing $k-1$ indistinguishable decoy devices [133].

Comment 5: *Regarding the paragraph about blockchain in Section IV, it is not very clear to me. when it is used between 2 stakeholders. not much trust is attained. It basically just a log append only log, where the validity is not evaluated by third party. Please elaborate if i misunderstand the point.*

Response: We thank the Reviewer for the constructive comment. In the full-version revised manuscript (page 10, left column, and in the bottom), we have revised the confusing description of blockchain. Actually, Blockchain is a digital data structure comprised of a shared, decentralised, and distributed database or ledger with a continuous log of chronological transactions. Each block contains transaction data, a timestamp, and a hash point which is linked to the previous block. The hash values are crucial to its tamper-proof capability as the compromise of the block content requires to alter all subsequent blocks, which is practically impossible. Additionally, blockchain provides a consensus mechanism to prevent one node from continuously adding blocks, making it more difficult to alter blocks with a sufficient rapid rate. Hence, the blockchain technology can be introduced to establish a trustworthy network for *multiple* stakeholders comprising DER owners, DER aggregators, and utility operator without requiring a trusted third party. The pros of blockchain on security enhancement will become more salient as the increase of distributed entities' number.

Comment 6: *In the summary part of Section IV, i think it is good if authors discuss A-I-C (availability first in ICS) instead of C-I-A, in smart grid system. This would support the argument there.*

Response: We thank the Reviewer for the constructive Comment. We have revised the manuscript accordingly. In the revised manuscript, the modification is as follows:

(Page 5, left column, and in the middle) Following the perspective of AIC, the potential attack impacts on the DER-based smart grid are divided into security- and privacy-related. The security-related impact focuses on how can the cyber-physical attacks impact/disrupt the data availability and integrity, and thus affecting the device-level functionalities and grid-level process and operation. In the distribution level, the security-related impact includes 1) Consumer expense increase in residential units, 2) Frequency/voltage deviation and power sharing failure in microgrids, 3) Poor power quality, 4) Intentional islanding failure, 5) Increased power loss, 6) Aggravated equipment wear, and 7) Voltage violation. In the transmission level, the security-related impact consists 1) Energy price/load manipulation, 2) Generator trip and load shedding, and 3) Cascading failure and large-scale blackout. It is intuitive that the impact scale is up to the scale of DER systems (Residential, Commercial, or Utility) that

is compromised by the adversary. The privacy-related impact concerns the customer information leak caused by data confidentiality violation, including location information, personal behavior patterns and activities inside home, and real-time surveillance information.

Comment 7: *Regarding IDS that uses protocol spec, the following papers discuss such a scheme for IEC 61850 GOOSE. Please add to the discussion.*

[99] Bohara, Atul, *et al.* "Ed4gap: Efficient detection for goose-based poisoning attacks on iec 61850 substations." *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2020.

Response: We thank the Reviewer for the constructive comment. We have discussed this critical network-based IDS and the modification in the revised manuscript is as follows:

(Page 8, right column, and in the middle) A finite state machine model for network communication was defined to detect the GOOSE-based poisoning attacks [99].

Comment 8: *Regarding IDS that utilize both general network info and protocol specific features, I think thre are some attempts alrady. The following emsemble approaches should be refered to.*

[101] Ren, Wenyu *et al.* "Edmand: Edge-based multi-level anomaly detection for scada networks." *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018.

Response: We thank the Reviewer for the constructive comment. We have discussed this innovative network-based IDS incorporating both general network and protocol specific features and the modification in the revised manuscript is as follows:

(Page 8, right column, and in the middle) By monitoring the traffic data characteristics of transport, operation, and content levels in SCADA network, Ren *et al.* developed a edge-based multi-level anomaly detection framework [101].

Comment 9: *Regarding physics based IDS, there is a line of work named command authentication. Such schemes also utilizes power system physics (namely power flow simulator) to evaluate the validity of SCDA control commands. So it will fir the discussion here.*

[164] Mashima, Daisuke *et al.* "Securing substations through command authentication using on-the-fly simulation of power system dynamics." *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018.

[165]Meliopoulos, Sakis *et al.* "Command authentication via faster than real time simulation." *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016.

Response: We thank the Reviewer for the constructive comment. We have discussed this series of command authentication works using on-the-fly power system dynamics. In the full-version revised manuscript, the modification is as follows:

(Page 13, left column, and in the top) Based on on-the-fly power system dynamics simulation results, command authentication schemes were proposed to evaluate the legitimacy and validity of remote control commands near the edge of smart grid infrastructure (e.g., in substations), which can enhance the attack detection capability compared to the traditional schemes solely using steady-state information [164], [165].

Comment 10: *In Section VIII, I don't think supply chain attack can be countered only with signatures. Even if it is singed, situlation like SolarWinds could happen. Besides, another future direction that may needs to be discussed is security/vulnerability sharing framework among smart grid operators or vendors that does not conflict with each*

operator's confidentiality/privacy requirement.

Response: We thank the Reviewer for the constructive comment. We have addressed the threat of solarwind-like attacks against code-signing software update, where the modification in the revised manuscript is as follows:

> (Page 7, left column, and in the middle) Nevertheless, there are still multiple threats to the code-signed firmware. For example, it is possible that software developed by an organization has malicious firmware embedded in the signed version. This could be perpetrated by an *insider* or through compromise of the firmware development environment, as was the case in the well-known SolarWinds attack. Awareness of this type of risk and application of appropriate mitigation methods are critical for all DER vendors.

Besides, the future direction in disclosing security issues and cyber vulnerabilities while preserving the privacy of customers, operators, and stakeholders, which is reflected in the revised manuscript as follows:

> (Page 12, right column, and in the middle) Besides, it is of great importance to establish a sharing platform of security issues and cyber vulnerabilities where the participators' privacy will not be leaked by the disclosure of these critical information.

Comment 11: *Last but not the reast, some acronyms are not defined in the paper (at its first appearance), such as NN, LFC, etc. Also I saw a number of English errors to be corrected via proofreading.*

Response: We thank the Reviewer for the constructive comment. We have added a table of acronyms before the Introduction in the full-version revised manuscript and proofread the whole manuscript thoroughly to correct potential errors.