Les cyberattaques dans les réseaux électriques intelligents : une revue des attaques et des contre-mesures

Culture Sciences de l'Ingénieur

La Revue 3E.I

Édité le 09/07/2026

école normale supérieure paris-saclay

Mariem BOUSLIMANI[1,2], Fatima BENBOUZID-SI TAYEB[1], Yassine AMIRAT[2], Mohamed BENBOUZID[3]

[1] *École nationale Supérieure d'Informatique (ESI)*
Laboratoire des Méthodes de Conception de Systèmes, Alger, Algérie

[2]*ISEN Yncréa Ouest, LabISEN, Brest, France*

[3]*Université de Brest, UMR CNRS 6027 IRDL, Brest, France*

Cette ressource fait partie du N°120 de La Revue 3EI du 3ème trimestre 2025.

Les réseaux électriques intelligents (Smart Grids) se sont développés en tant que structures complexes intégrant des réseaux de communication, des ressources énergétiques distribuées et des dispositifs intelligents. Cependant, cette intégration a généré diverses vulnérabilités, soulevant des préoccupations et des défis majeurs en matière de sécurité. Les Smart Grids actuels sont vulnérables à diverses cyberattaques, ce qui a conduit les chercheurs à développer des techniques de détection, d'atténuation et de prévention de ces attaques. Cet article se concentre spécifiquement sur les attaques par replay dans les Smart Grids, en reconnaissant la nécessité critique de traiter cette menace particulière. À travers une revue complète de la littérature existante concernant la détection, l'atténuation et la prévention des attaques par replay dans les Smart Grids, les micro-réseaux et les systèmes cyber-physiques (CPS), nous visons à fournir des perspectives sur des stratégies de défense efficaces applicables aux diverses infrastructures énergétiques interconnectées.

Mots-clés - Réseau électrique intelligent, micro-réseau, cybersécurité, cyberattaque, attaque par replay, détection d'attaque.

1 - Introduction

L'intégration des réseaux de communication et des dispositifs intelligents dans le réseau électrique traditionnel, ainsi que l'émergence de la production décentralisée (DG) au sein des micro-réseaux (MG), ont facilité le déploiement des réseaux électriques intelligents (Smart Grids - SG). Cette évolution est portée par l'essor des ressources énergétiques distribuées (DER) et des systèmes de stockage d'énergie (ESS).

À l'instar des systèmes électriques conventionnels, le SG englobe la production, le transport et la distribution de l'électricité. Celle-ci est générée dans des centrales utilisant des combustibles fossiles (charbon, gaz) ou des sources d'énergie renouvelable (SER), telles que le solaire, l'éolien et l'énergie marémotrice. L'énergie est ensuite acheminée via des lignes à haute tension avant d'être distribuée aux utilisateurs finaux.

Face aux préoccupations environnementales croissantes, l'intégration des DER au niveau de la distribution permet désormais aux consommateurs de réinjecter leur propre production dans le

réseau. Ce changement de paradigme transforme le flux d'énergie, autrefois unidirectionnel, en un flux bidirectionnel.

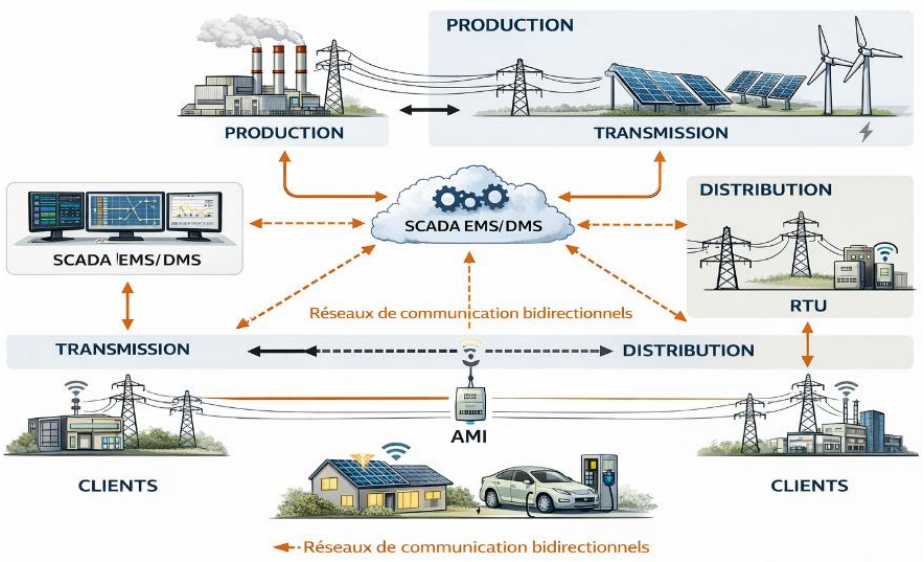

Figure 1: Modélisation d'un réseau électrique intelligent (SG)

Les réseaux électriques intelligents (**Smart Grids**) se caractérisent par l'intégration de réseaux de communication reliant divers dispositifs, tels que des onduleurs intelligents, des contrôleurs, des compteurs communicants, des unités terminales distantes (RTU) et des unités de mesure de phaseurs (PMU). L'information circule de manière bidirectionnelle entre les centres de contrôle et les clients. Les systèmes **SCADA** supervisent et contrôlent les conditions opérationnelles du réseau en collectant des mesures et en transmettant des commandes. Ils interagissent étroitement avec les systèmes de gestion de l'énergie (EMS) et de distribution (DMS). Par ailleurs, les PMU améliorent l'observabilité du système grâce à la synchronisation GPS pour l'horodatage des mesures. La figure 1 illustre l'architecture d'un SG.

Côté client, l'infrastructure de comptage avancée (**AMI**) regroupe les compteurs intelligents, les concentrateurs de données et le système de gestion des données de comptage (MDMS), permettant ainsi la tarification en temps réel et une gestion optimisée des flux d'énergie.

Cependant, l'omniprésence de ces technologies soulève des défis de sécurité majeurs. Les dispositifs intelligents sont vulnérables à diverses cyberattaques (figure 2) :

- L'**Injection de fausses données (FDI)** consiste à altérer les mesures issues des capteurs ou des compteurs intelligents avant de les réinjecter dans le réseau. L'objectif est de tromper les algorithmes de contrôle pour provoquer des décisions opérationnelles erronées.
- Le **Déni de service (DoS)** vise à saturer un serveur ou un nœud de communication par un flux massif de requêtes, le rendant incapable de traiter les messages légitimes et paralysant ainsi la surveillance du réseau.
- L'**attaque par rejeu (Replay) ou attaque par répétition**, cette attaque consiste à intercepter des données ou des commandes valides pour les renvoyer ultérieurement. Cela permet de simuler un état normal du système alors qu'une anomalie est en cours, ou de répéter une commande de commutation malveillante.
- L'**homme du milieu (MitM) ou attaque par interception,** permet à un attaquant de s'insérer dans le flux de communication entre deux dispositifs pour intercepter, lire ou modifier les échanges en usurpant l'identité de l'un des correspondants, voire des deux.

- L’**attaque par délai (Delay)** consiste à introduire délibérément une latence dans la transmission des données. Dans un réseau électrique, un retard de quelques millisecondes sur un message critique peut empêcher de réagir à temps.
- **Aurora** consiste à manipuler les disjoncteurs d'un générateur électrique ou un alternateur pour le déconnecter puis le reconnecter au réseau alors qu'il est désynchronisé. Le choc mécanique résultant peut causer des dommages et dégâts physiques catastrophiques au niveau de l’alternateur.

Bien que les pannes causées par une cyberattaque sur le réseau électrique ressemblent à celles provoquées par des aléas climatiques, un scénario pour lequel les opérateurs disposent déjà de plans de reprise d'activité, la menace informatique est unique. Sa dangerosité réside dans sa capacité à frapper plusieurs nœuds stratégiques en même temps. Cette simultanéité rendrait la crise particulièrement difficile à endiguer et entraverait fortement le déploiement sur le terrain des équipes de maintenance.

Si la littérature scientifique recense largement ces menaces de manière générale, peu de travaux ciblent spécifiquement les attaques par rejeu (replay attacks). Cet article se propose donc d'étudier cette vulnérabilité particulière, en passant en revue les méthodes actuelles de détection, d'atténuation et de prévention au sein des réseaux électriques intelligents (SG pour Smart Grids) et des systèmes cyber-physiques (CPS).

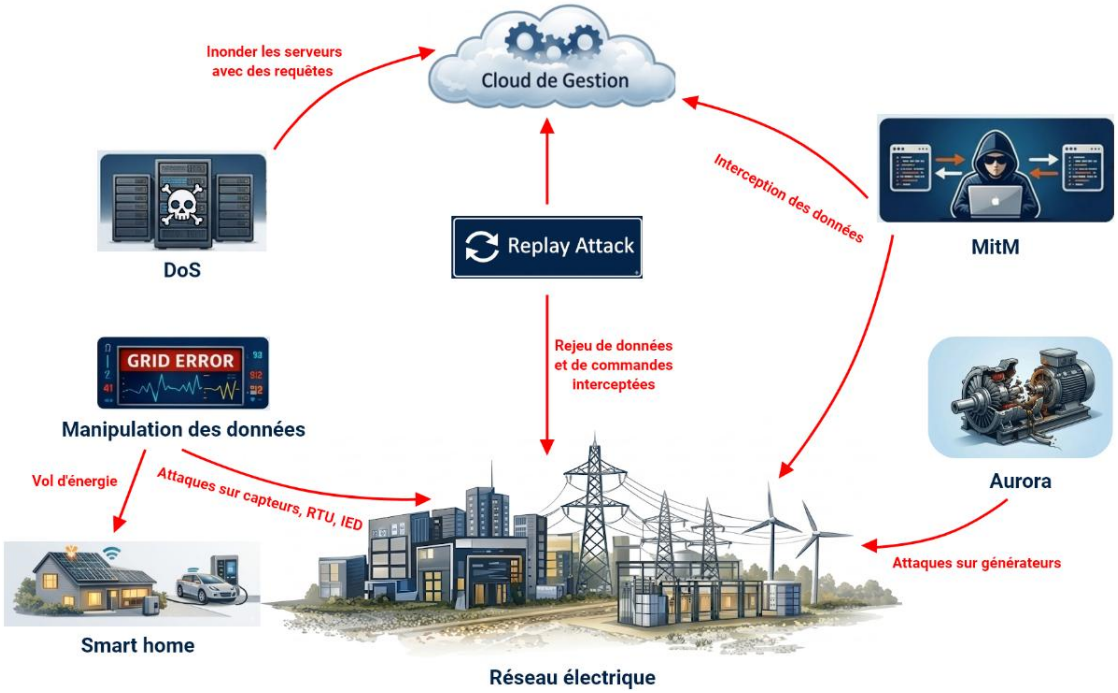

Figure 2 : Cyberattaques sur les SG

2 - Attaques par Replay : vecteurs, impact et contre-mesures

Une attaque par replay consiste à intercepter une communication, enregistrer des messages (mesures de capteurs, commandes) puis à les rejouer. Si le système est en régime permanent, l’attaque est efficace car elle donne l'illusion d'une activité normale. Ces attaques sont faciles à mettre en œuvre et difficiles à détecter par des détecteurs statistiques, car elles ne modifient pas la distribution des données.

Les attaques par replay peuvent viser divers éléments des SG : capteurs compromis, compteurs intelligents, interception des communications via des attaques MitM (Man in the Middel), ou encore

attaques sur les réseaux sans fil. Plusieurs scénarios illustrent leur impact, comme l'altération des commandes de régulation de tension ou la relecture de messages de tripping, causant des dégâts matériels ou des interruptions de service. La figure 3 illustre ce type d'attaque

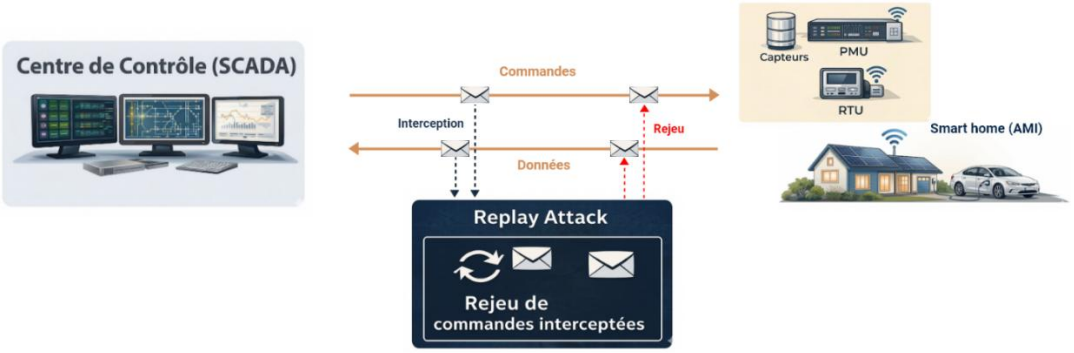

Figure 3: Illustration de l'attaque par replay dans un SG

Les conséquences vont des pertes économiques aux dommages physiques du réseau, en passant par le masquage de défaillances critiques.

La littérature scientifique propose plusieurs stratégies pour contrer ces menaces, classées selon leur approche technique, en techniques de Validation des Donnée, techniques de Sécurité Informatique et IA, et les techniques systémiques.

- ## Watermarking

Le watermarking (figure 4) ajoute des signaux de contrôle aux mesures pour détecter les attaques. Plusieurs variantes existent : watermarking multiplicatif, périodique, événementiel, ou basé sur des observateurs. Les stratégies incluent aussi des tests CUSUM, des techniques de lissage, ou l'injection de signaux d'authentification aléatoires.

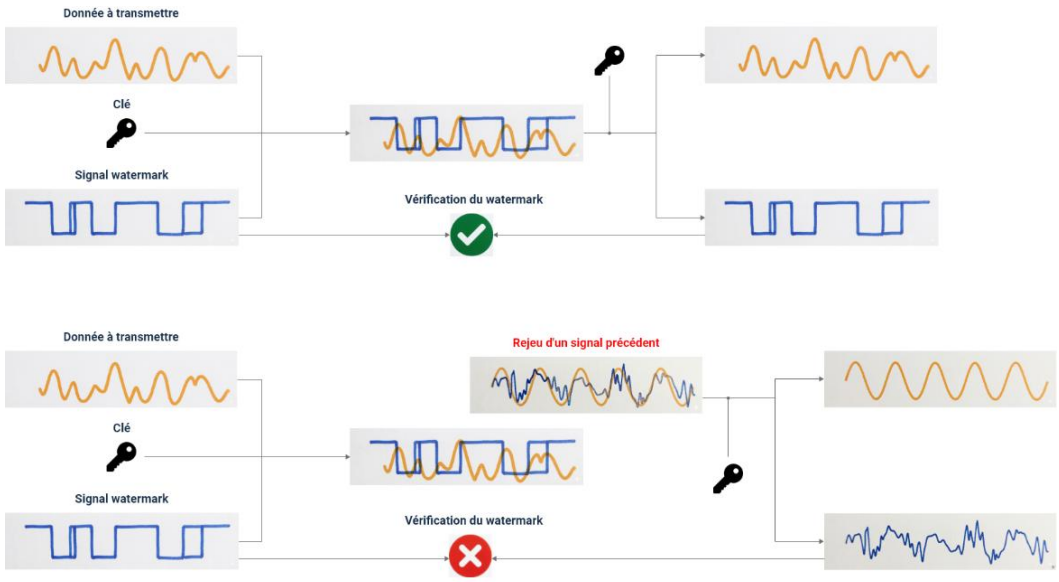

Figure 4: Protection des données contre l'attaque par replay en utilisant la technique du Watermarking

- ## Cryptographie

Les méthodes cryptographiques incluent la gestion des clés, l'authentification RSA, la signature numérique, l'usage du Blockchain ou de Merkle Tree pour réduire les coûts de communication et améliorer la sécurité.

- **Apprentissage automatique**

Les techniques d'apprentissage automatique, telles que le renforcement, les autoencodeurs LSTM ou les classificateurs basés sur l'entropie de permutation, permettent de détecter les attaques par replay, même en présence de bruit.

- **Estimation d'état**

L'estimation d'état basée sur le filtre de Kalman distribué permet de détecter les anomalies dues aux attaques. Ces techniques sont adaptées aux micro-réseaux et aux systèmes à bande passante limitée.

- **Traitement du signal**

L'injection de signaux de test dans les actionneurs ou le contrôle des intervalles d'excitation permettent de détecter l'absence de réponse attendue, signe d'une attaque.

- **Schémas de codage**

L'utilisation de codage d'état, de codage de sortie ou de codage stochastique peut amplifier les résidus de mesure en cas d'attaque, facilitant ainsi la détection.

- **Théorie des jeux**

L'approche basée sur la théorie des jeux permet de concevoir des stratégies d'injection de bruit optimales ou des politiques de contrôle adaptatives.

- **Autres techniques**

D'autres méthodes incluent l'estimation adaptative déclenchée par événements, les observateurs dédiés pour isoler les attaques des fautes de capteurs, ou la modification des lois de commande pour augmenter la probabilité de détection.

3 - Discussion

La conception de contre-mesures efficaces doit équilibrer coût computationnel, performance du système et efficacité de détection. Les méthodes événementielles, la réduction de la charge cryptographique, ou l'intégration d'algorithmes légers d'IA sont des pistes prometteuses. La distinction entre attaques et fautes est également cruciale pour éviter des réactions inappropriées.

L'apprentissage automatique offre des perspectives intéressantes, mais l'obtention de jeux de données d'entraînement à jour reste un défi.

4 - Exemples de l'impact de la cyberattaque sur les parcs éoliens

- **Attaques sur le STATCOM**

Les parcs éoliens conventionnels exploitent des génératrices asynchrones à cage d'écureuil. Le stator de ces machines étant directement raccordé au réseau, elles nécessitent d'imposantes batteries de condensateurs pour compenser la puissance réactive absorbée. Pour pallier ce problème et soutenir la tension au point de couplage commun (PCC), on y associe généralement des compensateurs statiques (STATCOM). Dans le scénario analysé, une attaque par injection de

fausses données est initiée à t = 4,5 s sur le capteur de tension CA. Les simulations révèlent une augmentation anormale de la puissance réactive dès l'injection du signal corrompu, forçant le STATCOM à absorber cette puissance de manière critique. La figure 5 illustre les variations des puissances actives et réactives à la sortie de la génératrice lors d'une attaque du capteur de tension.

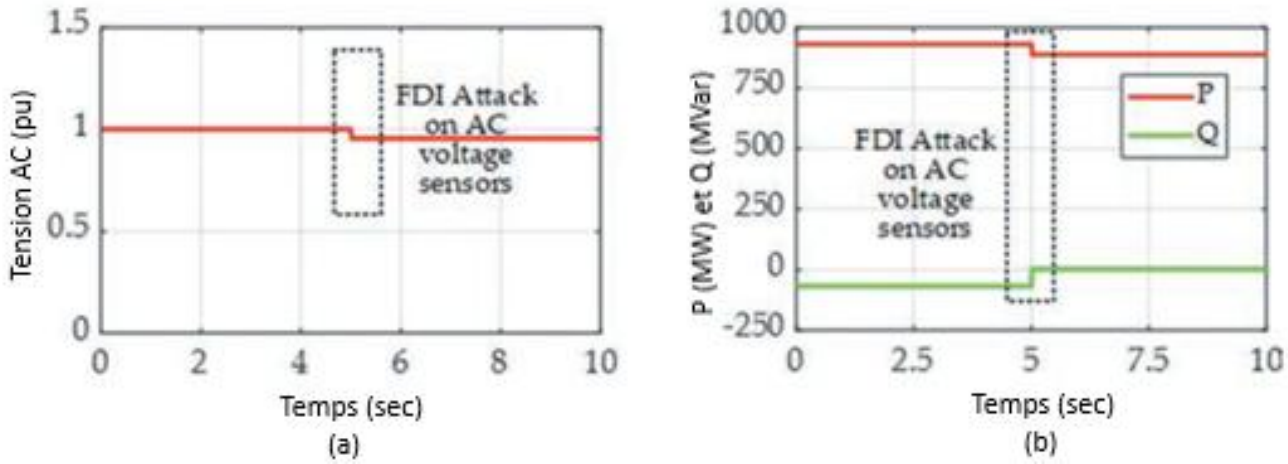

Figure 5 : Attaque du STATCOM : (a) Tension du réseau AC, (b) Puissance active et réactive FDIA (Fault Data Injection Attack) qui génère une dérive

- **Attaques ciblant les génératrices asynchrones doublement alimentées (DFIG)**

Très répandue dans l'éolien, la technologie DFIG offre un contrôle de couple haute performance tout en limitant le coût et le dimensionnement de l'interface électronique de puissance. Elle repose sur une machine à induction à rotor bobiné associée à un convertisseur statique côté rotor. Afin de mettre en évidence la vulnérabilité de cette architecture, une attaque FDIA (Fauls Data injection Attack) a été injectée dans le capteur de tension CA (Figure 6). L'anomalie franchit immédiatement le seuil de sécurité, ce qui active les protections contre les surtensions. La DFIG se montre ainsi particulièrement sensible aux cyberattaques, dont l'issue directe peut être le déclenchement intempestif ou la mise hors service complète d'une unité de production renouvelable majeure.

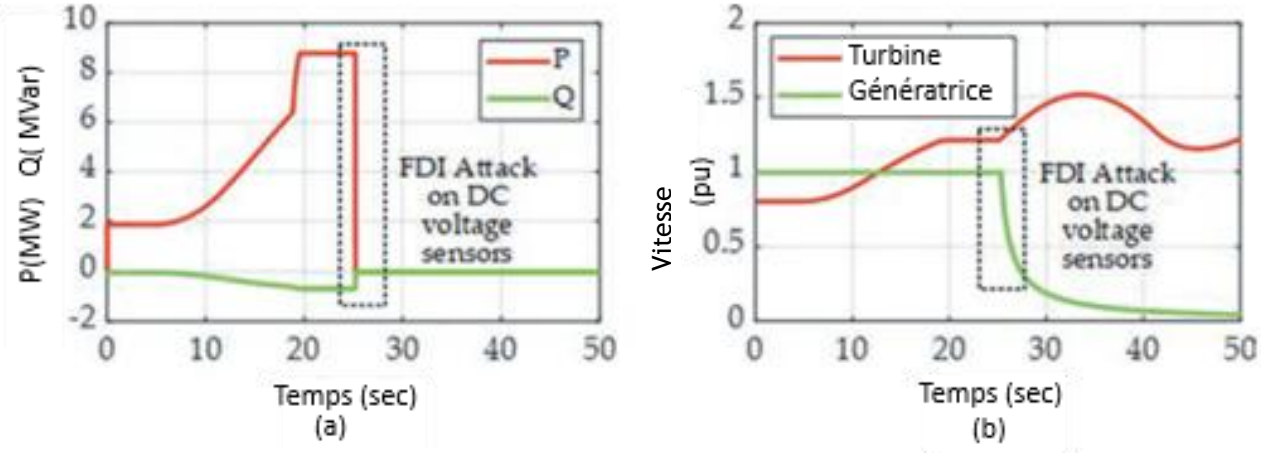

Figure 6 : Impact d'une FDIA sur le capteur de la tension du bus continu dans une application éolienne avec une génératrice asynchrone à double alimentation :(a) Puissance active et réactive, (b) vitesses de la génératrice et de la turbine – conséquence Arrêt ou déclenchement

5 - Conclusion

L'intégration de technologies intelligentes rend les SG vulnérables aux cyberattaques. Les attaques par replay, simples à mettre en œuvre, peuvent avoir des conséquences graves. Cet article a

présenté une revue des méthodes de détection et d'atténuation, avec un accent particulier sur la réduction des coûts computationnels et la distinction entre attaques et fautes. Plusieurs techniques - watermarking, cryptographie, apprentissage automatique - ont été explorées, soulignant la nécessité de recherches continues pour assurer la sécurité des SG.

6 - Références bibliographiques

M. Bouslimani, F. Benbouzid-Si Tayeb, Y. Amirat and M. Benbouzid, "Cyber-Physical Security in Smart Grids: A Comprehensive Guide to Key Research Areas, Threats, and Countermeasures," *Appl. Sci.* **2025**, *15*, 12367. https://doi.org/10.3390/app152312367

G. Desarnaud, « Cyberattaques et systèmes énergétiques. Faire face au risque », Études de l'Ifri, janvier 2017

T. Berghout, W. H. Lim, Y. Amirat, F. Benbouzid-Si Tayeb and M. Benbouzid, "Exploratory Data Analysis and Recurrent Expansion for Power Systems Cybersecurity Forensics," *IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society*, Chicago, IL, USA, 2024, pp. 1-6, https://doi.org/10.1109/IECON55916.2024.10905101

S. Sahoo, F. Blaabjerg and T. Dragicevic, "Cyber Security for Microgrids", The Institution of Engineering and Technology 2022, ISBN 978-1-83953-332-7.