International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 68 No. 2 Sep. 2023, pp. 317-327

http://www.ijisr.issr-journals.org/

Problématique des cyberattaques dans les réseaux électriques: Cas des entreprises d'énergie électrique au Togo

[The problem of cyberattacks on power grids: The case of electric power companies in Togo]

Abasse Kpegouni, Eyouléki Tchéyi Gnadi Palanga, and Adekunlé Akim Salami

Centre d'Excellence Régional pour la Maitrise de l'Electricité (CERME), Université de Lomé, 01 BP: 1515 Lomé, Togo

ABSTRACT: The evolution of information and communication technologies and their integration in almost all sectors of the economy (telecommunications, industry, transport, energy, trade, etc.) has made it possible to improve management and decision-making in real time in these sectors. In the industrial sector, and particularly in the electro-energy sector, information and communication technologies offer advantages in terms of speed, efficiency, cost-effectiveness, etc., as smart grids allow a large number of connected objects to interact, communicate and collaborate. On the other hand, these technological advances and the increase in Internet connectivity of electric power companies have led to an increase in the number of access points, making them more vulnerable to cyber-attacks. As a result, IT security for power grids is essential. The objective of this paper is to highlight, based on the extensive literature review and critical analyses, the cybersecurity issues in Smart Grids. The vulnerabilities of electrical infrastructures and the different solutions or systems implemented by researchers to address the problems of cyber-attacks have been presented. Machine learning and artificial intelligence techniques will be used in the following research to detect and block attacks on an electrical infrastructure in order to protect the electrical network from cyber-attacks.

KEYWORDS: problematic, cyber-attacks, electrical networks, enterprise, electrical energy.

RESUME: L'évolution des technologies de l'information et de la communication et leurs intégrations dans presque tous les secteurs de l'économie (télécommunications, industries, transports, énergie, commerce, etc.) a permis d'améliorer la gestion et la prise de décision en temps réel dans ces secteurs. Dans le secteur industriel et particulièrement celui de l'électroénergétique, les technologies de l'information et de la communication présentent des avantages en termes de rapidité, d'efficacité, de rentabilité, etc. car, les réseaux électriques intelligents permettent à un grand nombre d'objets connectés d'interagir, de communiquer et de collaborer. En revanche, ces avancées technologiques et l'accroissement de la connectivité à Internet des entreprises d'énergie électrique ont entrainé la multiplication des points d'accès qui les rendent plus vulnérables aux cyberattaques. Par conséquent, la sécurité informatique pour les réseaux électriques s'avère indispensable. L'objectif de cet article est de ressortir sur la base de la revue documentaire approfondie et des analyses critiques, les problèmes de cybersécurité dans les réseaux électriques intelligents (Smart Grid). Les points de vulnérabilités des infrastructures électriques et les différentes solutions ou systèmes mis en place par les chercheurs face aux problèmes des cyberattaques ont été présentés. Les techniques de machine Learning et de l'intelligence artificielle seront utilisées dans la suite de cette recherche pour détecter et bloquer les attaques sur une infrastructure électrique afin de protéger le réseau électrique des cyberattaques.

MOTS-CLEFS: problématique, cyberattaques, réseaux électriques, entreprise, énergie électrique.

Corresponding Author: Abasse Kpegouni

1 INTRODUCTION

L'évolution des technologies de l'information et de la communication (TIC), notamment avec le développement d'Internet, a fait que les réseaux et les systèmes d'information des entreprises jouent aujourd'hui un rôle crucial dans la société. Cette évolution des TIC et surtout des systèmes distribués a malheureusement contribué à faire évoluer de manière considérable les menaces informatiques. Les risques auxquels sont confrontées les entreprises et les organisations aujourd'hui, sont tels que la sécurité informatique prend une place prépondérante et vitale au sein des institutions privées et publiques [1]. Il ne s'agit plus de considérer la sécurité comme un luxe réservé aux grandes organisations ou entreprises car il n'est pas rare d'assister de nos jours à des prises d'otages de petits systèmes ou réseaux afin de s'en servir comme relais pour réaliser des attaques de grandes envergures sur de gros systèmes ou réseaux. Au même moment, le niveau de connaissance requis pour devenir pirate ne cesse de diminuer en raison de la prolifération d'outils et de logiciels malveillants (*malwares*) disponibles gratuitement sur Internet; ce qui favorise la fréquente présence des cyberattaques sur la toile. Plusieurs techniques se développement de jour en jour par les cyberattaquants pour mettre en péril les infrastructures des entreprises [2], [3], [4]. D'où la sécurité des infrastructures tend à s'améliorer quotidiennement.

Dans les systèmes industriels et particulièrement ceux de l'électricité, les TIC sont largement utilisées aujourd'hui. Grâce au système SCADA (*Supervisory Control And Data Acquisition*), l'exploitation du réseau électrique et la collecte des données de différents postes et équipement en temps réel à l'aide des RTU (*Remote Terminal Unit*) et PMU (*Phasor Measurement Unit*) deviennent de plus en plus facile. Ce qui constitue un avantage d'une part, puisqu'ils permettent aux gestionnaires du réseau électrique de pouvoir superviser et gérer le réseau en temps réel. D'autre part, ils entrainent une faille de sécurité pour le réseau électrique car les TIC utilisent les protocoles Ethernet et TCP/IP pour mener des communications entre les équipements et d'autres systèmes d'exploitation contrairement au réseau électrique conventionnel. Or, ces protocoles sont sensibles aux attaques IP tels que attaque de routage, usurpation d'adresse IP ou TCP SYN, etc [5].

Ces progrès technologiques et les avantages qu'elles offrent notamment la rapidité, l'efficacité, la rentabilité, etc., ont imposé de nouvelles normes et exigences de performance aux systèmes électriques. La conception et le développement des technologies avancées d'acquisition des données, de réseaux de capteurs et d'éléments d'exécution ont entrainé une complexité accrue des systèmes de mesure et des processus de gestion dans le système énergétique [6]. Les tendances économiques et technologiques ainsi que la croissance démographique ont montré que la demande en énergie électrique sur le plan mondial croit considérablement [7] et que les productions conventionnelles n'arrivent pas à combler, ce qui entraine le déficit en fourniture d'énergie électrique aux consommateurs [8]. Dans le souci de venir combler ce manque à gagner afin d'assurer la sécurité énergétique tout en réduisant l'énergie fossile et le réchauffement climatique, il fallait développer et déployer les énergies renouvelables dans le système électrique existant. Cela nécessite un changement d'infrastructure électrique en adoptant des stratégies technologiques avancées afin de mieux contrôler les activités du secteur électroénergétique et de rendre l'approvisionnement plus stable [9]. Ce changement de l'infrastructure doit nécessairement intégrer les TIC dans l'exploitation du réseau électrique afin d'assurer la gestion intelligente en fourniture de l'électricité aux consommateurs.

En effet, l'intégration des TIC dans les systèmes électroénergétiques, a permis la conception et le développement des réseaux électriques intelligents (*Smart Grid*) qui permettent à un grand nombre d'objets connectés d'interagir, de communiquer et de collaborer [10], [12]. Également, ces réseaux électriques intelligents permettent d'assurer la sécurité du réseau et de réduire le coût de consommation des clients en leurs permettant de suivre en temps réels leurs consommations grâce à une régulation intelligente de la charge électrique [13]. Ceci facilite la supervision, la gestion du réseau à distance et l'amélioration des services.

Ces avancées en TIC et l'accroissement de la connectivité Internet ont tellement exposé les réseaux électriques aux vulnérabilités [9], [12]. Ce qui accentue l'exposition éventuelle du réseau aux cybermenaces. Une cyberattaque réussie a le potentiel de perturber les activités ou de compromettre le fonctionnement de nature délicate. Par ailleurs, les conséquences indirectes d'une cyberattaque peuvent entraîner une perte de production et une perturbation des ventes, en plus de miner la confiance des consommateurs [25]. Des coûts économiques indirects tels que ceux-ci peuvent être tout aussi importants que les dommages à l'équipement et aux infrastructures et avoir de lourdes conséquences à long terme sur l'emploi, l'innovation et la croissance économique [25]. Or, dans de nombreux cas, il n'existe pas de politique de gestion de la sécurité informatique des infrastructures industrielles. Il n'existe pas non plus des mesures spécifiques concernant la gestion des sous-traitants et les intervenants sur les systèmes. C'est le cas par exemple des entreprises togolaises d'énergie électrique (CEB et CEET, etc.). Ces deux structures principalement ne disposent pas de stratégie de sécurité informatique. Également, il n'existe pas de politique de gestion des droits d'accès des utilisateurs définissant leurs actions sur les systèmes et interdisant les agents n'appartenant plus à l'entreprise d'intervenir sur le système. L'absence ou le manquement de tout ceci constitue une vulnérabilité pour

l'infrastructure. Quels sont les apports des chercheurs aux problèmes des cyberattaques des entreprises d'énergie électrique ?

La suite de l'article se présentera de la manière suivante: la section 2 présente les entreprises électroénergétiques togolaise, le système électrique et leurs environnements TIC; dans la section 3, la méthodologie utilisée est présentée; la section 4 présente les résultats et qui feront l'objet de discussions dans la section 5.

2 ENTREPRISES ÉLECTROÉNERGÉTIQUE, SYSTÈMES ÉLECTRIQUES ET ENVIRONNEMENT TIC

Cette section présente les entreprises électroénergétiques togolaises, leurs systèmes électriques et leurs environnements TIC.

2.1 ENTREPRISES ÉLECTROÉNERGÉTIQUES

2.1.1 LA CEB

La CEB (Communauté Electrique du Bénin), établissement public international institué par l'accord international portant Code Daho-Togolais de l'électricité du 27 juillet 1968, est un organisme international à caractère public. Elle a été créée pour jouer le rôle de monopole de production, du transport, de l'importation de l'énergie électrique et est l'acheteur unique pour le compte du Togo et du Bénin. Jusqu'en fin décembre de l'année 2018, la CEB était le principal fournisseur en énergie électrique du Togo et du Bénin en alimentant les sociétés de distribution nationales des deux pays au tarif de 58 FCFA/kWh en vigueur depuis 2014. Certains industriels sur le territoire du Togo et du Bénin sont alimentés en énergie électrique par la CEB au tarif de 65 FCFA/kWh. Mais, à compter du 1er janvier 2019, le sommet des Chefs d'État du Togo et du Bénin tenu à Lomé le 27 novembre 2018 confie désormais à la CEB la mission de gestionnaire du réseau de transport d'énergie sur le territoire de la communauté avec pour activité connexe la poursuite de l'exploitation des moyens de production du barrage de Nangbéto et des deux turbines à gaz installés dans les deux pays.

2.1.2 LA CEET

La CEET (Compagnie Energie Electrique du Togo), assure le service public national de distribution et de vente de l'énergie électrique. Elle dispose de ses propres moyens de production et s'approvisionne essentiellement en énergie électrique pour l'équilibre de la demande sur son réseau de distribution via le réseau de transport de la CEB auprès de l'opérateur Contour Global Togo SA et des fournisseurs d'électricité au Ghana (VRA) et au Nigéria (TCN). Depuis le 1er janvier 2011, les tarifs de vente de l'énergie électrique, en vigueur sur l'ensemble du territoire togolais sont ceux fixés par l'arrêté interministériel n°019/MME/MEF/MCDAT/MPR-PDAT/MCPSP du 26 novembre 2010 portant fixation des tarifs de vente de l'énergie électrique au Togo.

2.1.3 LA SOCIÉTÉ CGT

La société CGT (Contour Global Togo SA) dispose d'une centrale thermique d'une capacité de 100 MW composée de six (6) moteurs Wärtsilä 18V50DF d'une puissance unitaire d'environ 16,5 MW permettant d'utiliser comme combustibles de base le gaz naturel et le HFO (*Heavy Fuel-Oil*) ou mazout lourd et comme combustible de secours le LFO (*Light Fuel-Oil*). Cette centrale est mise en service industriel, le 13 octobre 2010. La société CGT est un producteur indépendant d'énergie électrique (IPP) disposant d'une convention de concession conclue en 2006 avec l'Etat togolais pour une durée de 25 ans d'exploitation. Conformément au contrat d'achat-vente d'énergie qu'elle a signé avec la CEET dans le cadre de cette concession, CGT assure la production de l'énergie électrique et la CEET est chargée de fournir les combustibles nécessaires à l'exploitation de la centrale. Au cours de l'année 2020, le coût de production de l'énergie électrique de cette centrale est de 47,72 FCFA/kWh hors Take or pay [7].

2.2 SYSTÈME ÉLECTRIQUE

Trois systèmes électriques différents permettent d'alimenter le Togo en énergie électrique. Il s'agit du:

Système électrique interconnecté de la Communauté Electrique du Bénin (CEB): à ce jour, il couvre quatre (4) régions sur les cinq (05) au Togo. Cette interconnexion s'étend de Lomé (au Sud) à Kantè (au Nord) et permet de desservir les grandes agglomérations et localités des régions Maritime, Plateaux, Centrale et Kara. Toutefois, les villes de Dapaong, de Cinkassé et de Mango dans la région des Savanes sont également alimentées par le réseau de la CEB à partir de la ville de Bawku au nord

du Ghana. Les principales composantes de ce système électrique interconnecté est composé des infrastructures de production, de transport et de la distribution;

Système électrique connecté au réseau frontalier (Ghana et Bénin): entre 2010 et 2014, le système d'Echange d'Energie Electrique de l'Afrique de l'Ouest (EEEOA/WAPP) a initié des projets d'électrification rurale transfrontalière dans le cadre de la mise en œuvre de la décision des Chefs d'Etat des pays membres de la Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO) relative à l'échange d'énergie transfrontalier [7], [14]. Ainsi, certaines localités frontalières à l'Est et à Ouest du Togo sont alimentées en énergie électrique à partir des réseaux électriques d'Electrical Company of Ghana (ECG) et de Gridco du Ghana et du réseau de la Société Béninoise d'Energie Electrique (SBEE). Le tableau 1 ci-dessous présente la situation des localités électrifiées.

Tableau 1. Localités électrifiées par la connexion au réseau transfrontalier

Régions	Localités électrifiées à partir du Ghana	Localités électrifiées à partir du Bénin	Total
Savanes	1	-	1
Kara	-	6	6
Centrale	-	2	2
Plateaux	31	1	32
Maritime	3	3	6
Total des localités électrifiées	35	12	47

Source: Statistique CEET, 2020

Système électrique isolé: certaines localités situées très loin du réseau de distribution sont alimentées par des centrales équipées de groupes diesel dans le cadre des projets d'électrification rurale initiés par l'Etat. La puissance installée de ces centrales varie de 36 kW (pour les petites localités) à 350 kW[1] (pour les plus grandes localités). Il faut noter que toutes ces localités concernées par le système électrique isolé ont un mini réseau de distribution en Basse Tension (BT) tiré à partir de la centrale isolée. En 2020, on compte dix-huit (18) localités qui sont alimentées par ce système électrique isolé et qui totalisent une puissance installée et disponible de près de 2,56 MW dont 0,6 MW pour les quatre localités alimentées par les mini-grids solaires photovoltaïques. Il faut noter qu'à partir de 2018, le réseau de distribution de la ville de Mango est raccordé au réseau interconnecté de distribution de la CEET et par conséquent ce réseau ne fait plus partie du système isolé.

2.3 ENVIRONNEMENT TIC

L'environnement TIC des entreprises électroénergétiques se présentent de la manière suivante.

2.3.1 INFRASTRUCTURE INFORMATIQUE DU RÉSEAU DE LA CEB

La CEB dispose d'un dispatching principal installé à Lomé (Togo) et d'un dispatching de secours qui se trouve à Calavi (Bénin) qui permettent aux gestionnaires du réseau électrique d'assurer sa conduite et son exploitation. Ces centres de dispatching reposent sur le réseau SCADA intégrant les outils numériques tels que les ordinateurs, les serveurs, les RTU/PMU, les systèmes d'exploitation, les logiciels métiers, les clé USB, les disques durs externe, la fibre optique, les câbles Ethernet, etc. pour assurer quotidiennement les activités de supervision, de contrôle et d'acquisition de données sur les consommations, les productions, l'importation de l'énergie électrique, etc. Ce réseau SCADA n'assure son fonctionnement normal que grâce au réseau privé de télécommunication qui interconnecte les différents postes de transformations électriques à travers la fibre optique et des différents équipements de télécommunications déployés (les autocommutateurs, les multiplexeurs optiques, les équipements CPL, etc.) dans le but d'assurer une communication entre les organes du réseau et de pouvoir conduire le réseau depuis le dispatching. Il existe donc une corrélation directe entre le réseau SCADA et le réseau télécom car il faut qu'un poste de

[1] En 2018, la centrale de Mango d'une puissance de 800 kW n'est plus en exploitation pour raison de raccordement du réseau isolé de la ville de Mango au réseau interconnecté de distribution de la CEET

transformation soit télé-signalé avant que ce dernier ne puisse être commandé depuis le dispatching. La figure 1 montre l'architecture de ce réseau SCADA.

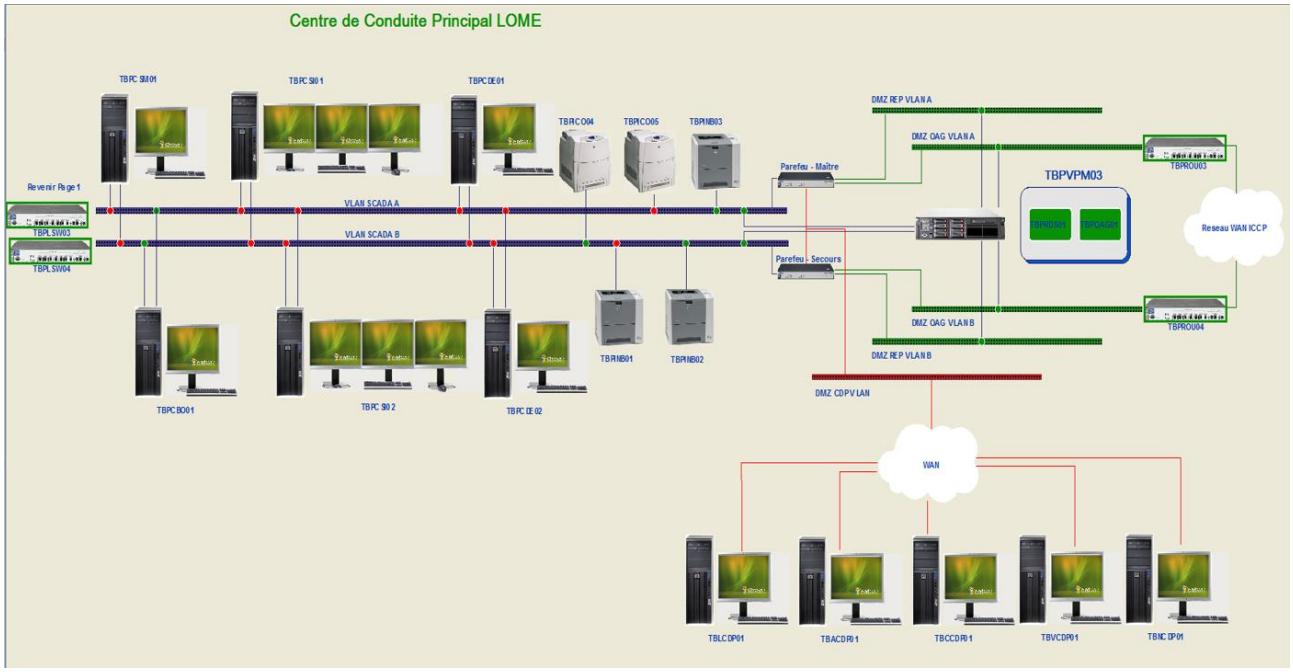

Fig. 1. Architecture du système SCADA pour le dispatching principal

Source: CEB, 2022

Cette architecture montre qu'il n'y a pas des dispositifs sécuritaires mis en place pour protéger le réseau contre les attaques. Pour les responsables, étant donné que le réseau SCADA n'est pas connecté au réseau Internet, ce dernier est déjà protégé. Or ils oublient que les attaques ne proviennent pas seulement du réseau Internet, ils peuvent provenir de l'intérieur, des sous-traitants, et d'autres sources.

2.3.2 INFRASTRUCTURE INFORMATIQUE DES AUTRES RÉSEAUX: CEET, CGT

La CEET et la société CGT ne disposent pas jusqu'à ce jour de réseau informatique pour la supervision et le contrôle des activités de distribution et de production de l'énergie électrique. Par conséquent, la stratégie sécuritaire du réseau contre les cyberattaques n'existe pas. Les activités de distribution de l'énergie électrique par la CEET se font de façon analogique et manuelle avec tous les problèmes et conséquences qui y vont avec, occasionnant de nombreuses pertes d'électricité qui sont estimées en 2020 à 16,04% [7].

3 MÉTHODOLOGIE

L'approche adoptée est qualitative. Elle est focalisée sur une étude approfondie sur la base de la revue documentaire et des analyses critiques, les problèmes de cybersécurité dans les réseaux électriques intelligents. Elle repose essentiellement sur la revue documentaire des écrits reposant sur la sécurité des installations électroénergétique en deux phases. La première phase a consisté à analyser les différentes vulnérabilités des systèmes industriels faces aux cyberattaques ainsi que leurs évolutions. La deuxième étape s'est attelée à l'identification des systèmes de sécurité mise en place par différents chercheurs, leurs efficacités et leurs spécificités. La recherche a été limitée aux études publiées entre 2010 et 2022. Afin d'évaluer la situation sur les problèmes de sécurité informatique pour les entreprises d'énergie électrique au Togo par rapport aux pays d'autres continents, un stage en entreprise de trois mois a été effectué à la CEB (Communauté Electrique du Bénin).

4 RÉSULTATS

4.1 POINTS DE VULNÉRABILITÉ ET LEURS ÉVOLUTIONS

La forte intégration des TIC dans les réseaux électriques intelligents conduit à une augmentation exponentielle des vulnérabilités et par ricochet à la multiplicité des attaques du système électrique qui pourrait entrainer des *« black-out »* [9], [12]. Ces vulnérabilités sont de diverses ordres. Selon les dernières évolutions et tendances faites sur le plan africain et mondial en 2021 et 2022 sur la cybersécurité [15], [16]:

- 85% de la violation de la cybersécurité des entreprises sont causées par une erreur humaine;
- 94% de tous les logiciels malveillants sont livrés par courriel;
- Les attaques de ransomware se produisent tous les 10 secondes;
- 71% de toutes les cyberattaques sont motivées financièrement, suivi par le vol de la propriété intellectuelle, puis l'espionnage;
- Le coût mondial annuel de la cybercriminalité est estimé à 10,5 billions de dollar d'ici 2025.

Ses chiffres sont révélateurs et alarmants. Ils doivent susciter la conscience des responsables des entreprises et prendre des dispositions idoines pour éradiquer l'impact négatif des cyberattaques sur les entreprises. Aussi, les analystes de Cybersecurity Ventures, prédisent que les coûts associés à la cybercriminalité vont croitre de 15 % par an pour les cinq prochaines années. En 2021, les prévisions financières des dommages causés par les cyberattaques sont évaluées à [15], [16]:

- 6 billions de dollars par an;
- 500 milliards de dollars par mois;
- 115,4 milliards de dollars par semaine;
- 16,4 milliards de dollars par jour;
- 684,9 millions de dollars par heure;
- 11,4 millions de dollars la minute;
- 190 mille de dollars la seconde.

La réussite d'une cyberattaque sur un système informatique passe par l'exploitation d'au moins une vulnérabilité, qui peut être technique, humaine ou organisationnelle. D'une façon générale les systèmes de contrôle commande (ICS) en particulier ceux du système électroénergétique sont plus vulnérables que les systèmes informatiques classiques [17]. Plusieurs raisons sont à la base de leurs vulnérabilités. Néanmoins, une liste non exhaustive des points de vulnérabilité des systèmes électriques sont présentés comme suit:

Longue durée des installations: la durée de vie des installations OT *(Operational Technology)* est souvent très longue, elles sont généralement renouvelées tous les 10 ou 15 ans ou plus. L'objectif essentiel étant de faire fonctionner en continue (24h/24) un système de production, et tout ce qui nécessite ou peut générer un arrêt est évité. Il y a donc des vulnérabilités dues à l'obsolescence des installations qui se révèlent alors comme autant de failles s'exposant à des cybermenaces;

Intégration des TIC et connectivité à Internet: au départ, les infrastructures des systèmes industriels avaient longtemps la particularité de rester autonome vis-à-vis des TIC et étaient donc peu exposés aux risques des cyberattaques car le fonctionnement de ses équipements n'intégrait pas des outils informatiques. Pour les attaquer, il fallait être capable de bien comprendre l'architecture du système dans ses détails sans quoi, il serait difficile de compromettre leur bon fonctionnement. Par la suite, trois facteurs selon [11] ont entrainé l'intégration progressive des TIC au sein des systèmes industriels: *« le besoin de rationnaliser la production avec des outils capables de récolter et de traiter d'importantes masses de données; le besoin d'échanger des données avec des acteurs extérieurs aux sites industriels (opérateurs, entités de gestion, etc.); la nécessité de faire des économies sur les logiciels employés et de faciliter la communication entre sites de gestion et sites industriels ».* Ainsi, cette intégration des TIC et les échanges de données et de connexions avec les entités extérieures se sont multipliés. Ce qui a rendu les infrastructures électroénergétique plus vulnérables. Il existe parfois des connexions directes à Internet, plus ou moins officielles et parfois temporaires pour des opérations de maintenance ou de configuration, et celles-ci représentent une réelle vulnérabilité.

Non protection des ports physiques (USB, RJ45): pour le commun des mortels, le fait de ne pas être connecté à Internet suffisait pour éviter tout risque de piratage informatique. Or, on constate que c'est plutôt le contraire, même si un système n'est pas connecté à Internet, il peut être victime d'une malveillance informatique. Stuxnet en est un exemple démonstratif. La source d'attaque était la clé USB contenant un ver informatique et qui avait été introduite sur une machine de l'entreprise. Cette clef a infecté toutes les machines du réseau informatique. Ce qui a causé des dommages physiques à l'enrichissement

nucléaire Iranien en 2010 [18]. Donc les ports USB et RJ45 constituent des sources de vulnérabilités des systèmes électroénergétique qu'il faudrait prendre soin de protéger;

Non mise à jour des logiciels: étant donné que les infrastructures électroénergétique fonctionne 24h sur 24, de ce fait, redémarrer une station de travail pour mettre à jour ses logiciels peut entraîner un arrêt coûteux, voire dangereux des opérations. Ce qui fait que les applications propriétaires et les systèmes d'exploitation installées deviennent de plus en plus obsolètes. Ces systèmes n'ayant pas été conçus pour recevoir des correctifs pour la plupart, s'exposent à des vulnérabilités;

Inexistence de politique de gestion de la sécurité: dans de nombreux cas, il n'existe pas de politique de gestion de la sécurité des infrastructures industrielles. Il n'existe pas non plus des mesures spécifiques concernant la gestion des sous-traitants et les intervenants sur les systèmes. C'est le cas par exemple des entreprises Togolaise d'énergie électrique (CEB et CEET, etc.). Ces deux structures principalement ne disposent pas de stratégie de sécurité informatique. Également, il n'existe pas de politique de gestion des droits d'accès des utilisateurs définissant leurs actions sur les systèmes et interdisant les agents n'appartenant plus à l'entreprise. L'absence ou le manquement de tout ceci constitue une vulnérabilité pour l'infrastructure.

4.2 CAS DU TOGO

Au Togo, les télécommunications sont utilisées aujourd'hui dans les réseaux électriques notamment celui du transport pour établir des communications entre différents équipements du réseau. Ce qui facilite en partie la supervision, le contrôle et l'acquisition des données du réseau grâce au système SCADA. Or, le SCADA utilise les technologies informatiques tels que les ordinateurs, les serveurs, les protocoles IP, les supports USB, etc. pour son fonctionnement. Aussi, un projet de partenariat est en cours de négociation entre opérateur télécom (Togocom) et l'entreprise chargée du transport de l'énergie électrique au Togo (CEB) en vue de pouvoir utiliser la fibre optique de ce dernier pour distribuer de la connexion Internet aux abonnés. De plus, le projet WAPP *(West African Power Pool)* veut interconnecter les réseaux électriques de 330 kV de l'Afrique de l'Ouest avec la construction d'un dispatching central à Calavi au Bénin pour tous les pays Ouest-Africains dans le but de mettre en place le marché régional de l'électricité [14]. Ce qui entrainera forcement la mise à jour des réseaux électriques actuels ou la refonte vers les *Smart Grids* afin de répondre efficacement aux standards et technologies qui seront utilisés dans ce vaste réseau (les PMU, etc.). Tout ceci constitue des atouts pour les réseaux électriques togolais. En revanche, ces atouts deviennent une source de vulnérabilités aux cyberattaques pour les réseaux électriques ouest africains, et les réseaux électriques togolais ne seront pas épargnés; d'où l'aspect sécuritaire des réseaux électriques contre les cyberattaques doit être pensé dès maintenant. Le présent article s'inscrit dans une approche anticipative afin de contribuer à renforcer la sécurité des réseaux électriques togolais.

4.3 IDENTIFICATION DES SYSTÈMES DE SÉCURITÉ OU SOLUTIONS MISE EN PLACE

Le tableau 2 montre les différentes solutions ou systèmes de sécurité proposés par les chercheurs face aux problèmes des cyberattaques dans le secteur industriel.

Tableau 2. Apports des chercheurs face aux problèmes des cyberattaques des systèmes industriels

Références	Titre de l'article / thèse / mémoire	Méthodes	Résultats
[5]	Cyber-power system security in a smart grid environment	Utilisation des techniques de cybersécurité et leurs applications aux réseaux électriques	Les auteurs ont proposé l'installation d'un IDS et les pare-feu d'accès à distance dans les sous stations électriques. Le test de cette solution a été réalisé en utilisant les données de test des attaques de l'Université Collège Dublin (UCD).
[19]	Cyberdéfense des systèmes de contrôle-commande industriels: une approche par filtres basée sur la distance aux états critiques pour la sécurisation face aux cyberattaques	Une approche hybride a été utilisée dans la lutte contre les cyberattaques des infrastructures. La première est celle par filtre basée sur la distance aux états critiques et la seconde est basée sur les IDS (*Intrusion Detection System*)	En plaçant le filtre compte-rendu proche des capteurs qui assurent la remontée des données, on peut détecter les attaques qui passeront sur le système. Cette approche hybride pourrait améliorer la protection des infrastructures industrielles contre les cyberattaques.
[20]	Cyberdéfense des infrastructures critiques	Développement d'un modèle (algorithme) de détection d'intrusion	Un outils IDS a été conçu à l'image de l'IDS générique selon la norme 61850 et a permis de détecter les attaques orientées processus.
[9]	A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection	Utilisation des réseaux de neurones artificiels (ANN) basés sur l'algorithme d'optimisation des baleines (WOA-ANN)	Ce modèle a permis de classer d'un côté les cyberattaques et les incidents du système électrique habituel de l'autre. Ceci permet de détecter facilement les attaques sur le réseau électrique par analogie de ce que les baleine font pour capturer une proie. Selon les auteurs, il existe trois types d'attaques par intrusion à savoir attaque par injonction de fausses données (FDI), attaque par redistribution de la charge (LR) et attaque par dénis de service (DoS).
[13]	Architecture and Key Technology of Intelligent Energy Service System Based on Industrial Internet	Revue documentaire sur les outils et équipements de protection du réseau électrique intelligent	Les auteurs ont proposé l'insertion d'un équipement d'isolation (le pare- feu ou firewall) pour séparer la partie interne du réseau de l'extérieur afin d'assurer la sécurité du réseau contre les attaques.
[12]	Gradient Ascent Algorithm for Enhancing Secrecy Rate in Wireless Communications for Smart Grid	Utilisation de l'algorithme d'ascension de gradient (*Gradient Ascent Algorithm),* qui est une technique d'apprentissage automatique.	Le niveau de confidentialité (le taux de secret) des communications sur le réseau électrique a été augmenté car selon les auteurs les réseaux électriques intelligents sont confrontés aux problèmes d'écoute clandestine (les attaquants tentent d'écouter silencieusement les communications qui se passent sur le réseau) et l'attaque par brouillage (l'attaquant perturbe les signaux reçus au niveau de récepteur). Cette technique permet de réduire l'effet des attaques par brouillage et par écoute clandestine.
[21]	Cyber security of smart grid: attacks and defenses	L'objectif était d'évaluer l'impact d'une cyberattaque sur les consommateurs d'électricité (clients) par rapport au système électrique. Donc les auteurs	Les résultats ont montré que les attaques sur les consommateurs sont plus élevées par rapport aux composants électriques. Il faut donc accorder désormais plus d'importance

		ont utilisé une méthode permettant de classer les utilisateurs (consommateurs) et les composants du système électrique avec l'utilisation de l'algorithme *Greedy Based Partition Algorithm* (GBPA)	sur l'impact des cyberattaques sur les clients dans les stratégies de sécurité
[22]	Cyber security for fog-based smart grid SCADA systems: Solutions and challenges	Revue documentaire sur les différentes solutions de cybersécurité existantes pour les SCADA dans les smart Grids.	Les résultats ont montré que les solutions de cybersécurité se classent en quatre catégories à savoir les solutions d'authentifications, les solutions de préservation de la vie privée, les systèmes de gestion des clés et les systèmes de détection des intrusions (IDS). Ces derniers se scindent en neuf (9) catégories à savoir les IDS basés sur: (i) l'apprentissage profond, (ii) les réseaux de neurones artificiels, (iii) les machines à vecteurs de support, (iv) les arbres de décision, (v) les règles, (vi) le filtre de Bloom, (vii) les forêts aléatoires, (viii) l'apprentissage de sous-espace aléatoire et (ix) les automates finis déterministes.
[23]	Security issues on smart grid and blockchain-based secure smart energy management system	Utilisation de la technologie blockchain	Les auteurs ont proposé utiliser la technologie *blockchain* comme solution pour assurer la sécurité et le stockage des données produites sur le réseau électrique intelligent car pour eux, cette technologie devrait assurer à la fois la transparence et la fiabilité des données.
[24]	Blockchain technology in the future smart grids: A comprehensive review and frameworks	Revue de littérature sur le domaine d'application de la technologie blockchain	Les résultats montrent que cette technologie peut être utilisée dans plusieurs domaines à savoir les contrats intelligents pour la réponse à la demande (DR) dans les *Smart Grids,* les véhicules intelligents (VEs), les technologies IoT, la gestion décentralisée de l'énergie, le commerce de l'énergie, les transactions financières, la cybersécurité, le banc d'essai, l'environnement.

5 DISCUSSIONS

Les résultats présentés ci-dessus montrent que plusieurs études ont été menées dans le but de détecter les intrusions (les cyberattaques) dans les systèmes industriels mais, peu sont orientées dans le sens de prévenir et de bloquer les cyberattaques dans les systèmes afin que celles-ci ne se propagent dans le réseau et causées des dysfonctionnements ou des *black-out*. C'est le cas des travaux de [5], [20], [9], [22] qui proposent l'installation d'un IDS et des pare-feu dans les sous stations électriques ainsi que des modèles de détection d'intrusion. Ces modèles ou propositions n'arrivent pas à bloquer les attaques. Ils ne sont que transparent et envoient seulement une alarme pour signaler que la menace a été détectée dans le réseau mais n'arrivent pas à l'éliminer. Le signal d'une attaque est une bonne alerte dans la gestion des systèmes de sécurité, mais ne constitue pas des mesures pour la maitriser. Leurs résultats sont similaires à ceux de [11], [13]. Donc, il vaut mieux orienter les recherches dans le sens des mesures anticipatives d'élimination et de prévention des attaques dans le réseau. La contribution dans ce sens pourrait aider vraiment à renforcer la sécurité des infrastructures électriques contre les cyberattaques. Les travaux de [19] devraient paraitre intéressants si les auteurs avaient pu passer à l'expérimentation sur l'approche proposée pour confirmer ou infirmer son efficacité. Aussi le fait de rapprocher le filtre compte-rendu des capteurs ne permet pas de distinguer les attaques des défaillances du système. Pour [13], le fait d'utiliser le firewall pour séparer le réseau interne de l'externe reste insuffisant car les intrusions et les attaques ne proviennent pas seulement de l'extérieur mais aussi de l'intérieur. Les résultats de [21] devraient interpeler puisque beaucoup d'études ont été avancées dans le sens de déterminer les points les plus critiques du

système électrique afin de mener des actions pour leurs protections car, la défaillance de ces points critiques peut entrainer une défaillance en cascade et une panne de l'ensemble du système sauf qu'on ignorait le plus souvent l'impact que ces attaques ont sur les consommateurs d'électricité. Or, la satisfaction des clients (consommateurs) pour la consommation d'électricité est l'un des principaux facteurs ayant un impact sur la façon dont nous comprenons la vulnérabilité du réseau électrique. Il est donc nécessaire d'accorder désormais d'importance sur l'impact des cyberattaques sur les clients dans les stratégies de sécurité. Pour [23], [24], la technologie blockchain est une solution pour assurer la sécurité et le stockage des données produites sur le réseau électrique intelligent. Puisqu'elle s'applique dans presque tous les domaines de l'économie, la blockchain est une technologie prometteuse dans le futur pour répondre à une variété de problèmes dans les réseaux électriques intelligents.

6 CONCLUSION

Cet article ressort les problèmes de cybersécurité auxquels sont confrontés aujourd'hui les systèmes industriels en général et celui de l'électricité avec l'intégration et l'évolution des TIC au sein de ce secteur en particulier. Une revue de littérature et des analyses critiques ont permis de voir les failles et les points de vulnérabilités des infrastructures électriques, le bilan des attaques dont ces dernières sont victimes ainsi que les différentes solutions et systèmes proposés par les chercheurs face à cette situation. Cependant, protéger le système électrique contre les menaces en temps réel s'avère être indispensable pour un système électrique dynamique tel que les *Smart Grids*. Pour cela, dans la suite de cette recherche, des nouveaux modèles ou algorithmes capables de pouvoir prendre en compte en temps réel les nouvelles attaques non encore connues doivent être développés ou conçus car, les méthodes et stratégies de sécurités utilisées habituellement sont principalement basées sur l'anticipation des cyberattaques déjà existantes et ne prennent pas en compte celles potentiellement prévisibles. Nous voulons à cet effet mettre en évidence, l'utilisation des techniques de machine learning (ML) et de l'intelligence artificielle (IA) dans la prévention des cyberattaques au regard des évolutions technologiques et assurer la sécurité des flux de données (consommations et productions) du réseau électrique. Notre motivation est que nous avions constaté dans la littérature que peu d'études sont allées dans le sens de bloquer l'intrusion (attaque) d'une cyberattaque dans l'infrastructure électroénergétique. Notre contribution est de développer un nouveau modèle capable de bloquer une cyberattaque avec l'utilisation des techniques de l'IA et de ML.

REMERCIEMENTS

La rédaction de ce manuscrit s'est effectuée grâce à la contribution de diverses personnes auxquelles nous tenons à adresser nos sincères remerciements.

Une marque particulière de reconnaissance au:

- **Pr AJAVON Ayité Sénah Akoda,** Ancien Directeur du Centre d'Excellence Régional pour la Maitrise de l'Electricité (CERME) pour son management au sein du centre et pour tous les efforts et sacrifices qu'il ne cesse de faire pour la réussite de ses étudiants et doctorants notamment le financement en totalité des frais de publication d'article;
- **Dr PALANGA Eyouléki Tchéyi Gnadi,** Maitre de conférences et directeur de thèse, qui consacre tout son temps jours et nuits malgré ses multiples occupations à encadrer nos travaux de recherche du début jusqu'à la publication de cet article. Qu'il trouve ici nos sincères remerciements pour la mobilisation des ressources matérielles, humaines et financières pour notre accompagnement;
- **Pr SALAMI Adekunlé Akim,** Directeur Adjoint de l'Ecole Polytechnique de Lomé (EPL) et co-directeur de thèse, pour sa disponibilité, ses conseils et orientations à encadrer nos travaux de recherches malgré ses multiples charges;
- **Dr OURO-GBELE Zoulkofoulou,** pour ses conseils, orientations, corrections et relecture de cet article.

Que toutes ces personnes, trouvent ici, l'expression courtoise de mes salutations distinguées. Leurs conseils, remarques et suggestions ont constitué pour moi un véritable point d'appui dans la rédaction de cet article. Je leur en sais vraiment gré et les en remercie vivement.

REFERENCES

[1] N. Rahman, I. Sairi, N. A. M. Zizi, et F. Khalid, « The importance of cybersecurity education in school«, *International Journal of Information and Education Technology,* vol. 10, nº 5, p. 378-382, 2020.

[2] K. Cacciapaglia, « Analyse sur les différentes cyberattaques informatiques«, Haute école de gestion de Genève, 2018.

[3] M. Gomes, « Analyse de cyberattaques et proposition de solution au travers du pentesting«, Haute école de gestion de Genève, 2021.

[4] M. Z. Gunduz et R. Das, « Cyber-security on smart grid: Threats and potential solutions », *Computer networks,* vol. 169, p. 107094, 2020.

[5] A. Stefanov et C.-C. Liu, « Cyber-power system security in a smart grid environment«, in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT),* 2012, p. 1-3.

[6] D. I. Dogaru et I. Dumitrache, « Cyber security of smart grids in the context of big data and machine learning«, in *2019 22nd International Conference on Control Systems and Computer Science (CSCS),* 2019, p. 61-67.

[7] ARSE - Autorité de reglémentation du secteur de l'électricité, « Rapport d'activité 2020«, Togo, Rapport annuel, 2020. [En ligne]. Disponible sur: https://www.arse.tg/

[8] International Energy Agency, « Electricity Market Report, July 2021«, OECD, juill. 2021. doi: 10.1787/f4044a30-en.

[9] L. Haghnegahdar et Y. Wang, « A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection«, *Neural computing and applications,* vol. 32, nº 13, p. 9427-9441, 2020.

[10] S. Iyer, « Cyber security for smart grid, cryptography, and privacy«, *International Journal of Digital Multimedia Broadcasting,* vol. 2011, 2011.

[11] G. Desarnaud, « Cyberattaques et systèmes énergétiques. Faire face au risque », *Etudes de l'Ifri,* p. 62, janv. 2017.

[12] N. Mensi, D. B. Rawat, et E. Balti, « Gradient Ascent Algorithm for Enhancing Secrecy Rate in Wireless Communications for Smart Grid«, *IEEE Transactions on Green Communications and Networking,* vol. 6, nº 1, p. 107-116, mars 2022, doi: 10.1109/TGCN.2021.3093821.

[13] G. Shen, G. Chen, X. Dong, A. Geng, L. Sun, et Y. Sun, « Architecture and Key Technology of Intelligent Energy Service System Based on Industrial Internet«, in *2020 IEEE Sustainable Power and Energy Conference (iSPEC),* 2020, p. 2077-2082.

[14] WAPP EEEOA, « Système d'Echanges d'Energie Electrique Ouest-Africain«, Rapport annuel, 2021. Consulté le: 9 août 2022. [En ligne]. Disponible sur: https://www.ecowapp.org/fr/documentation.

[15] « Statistiques, tendances et faits sur la cybersécurité qui comptent pour 2022«, *Website Rating,* 12 avril 2022. https://www.websiterating.com/fr/research/cybersecurity-statistics-facts/ (consulté le 17 juin 2022).

[16] H. Rebecca, « ÉVALUATION 2021 DES CYBERMENACES EN AFRIQUE«, p. 35, 2021.

[17] J.-M. Flaus, Cybersécurité des systèmes industriels. ISTE Group, 2019.

[18] J. R. Lindsay, « Stuxnet and the Limits of Cyber Warfare«, *Security Studies,* vol. 22, nº 3, p. 365-404, juill. 2013, doi: 10.1080/09636412.2013.816122.

[19] F. Sicard, É. Zamaï, et J.-M. Flaus, « Cyberdéfense des systèmes de contrôle-commande industriels: une approche par filtres basée sur la distance aux états critiques pour la sécurisation face aux cyberattaques«, 2017.

[20] S. Mocanu, « Cyberdéfense des infrastructures critiques«, COMMUNAUTÉ UNIVERSITÉ GRENOBLE ALPES, 2019.

[21] T. N. Nguyen, B.-H. Liu, N. P. Nguyen, et J.-T. Chou, « Cyber security of smart grid: attacks and defenses », in *ICC 2020-2020 IEEE International Conference on Communications (ICC),* 2020, p. 1-6.

[22] M. A. Ferrag, M. Babaghayou, et M. A. Yazici, « Cyber security for fog-based smart grid SCADA systems: Solutions and challenges«, *Journal of Information Security and Applications,* vol. 52, p. 102500, 2020.

[23] S. M. Kim, T. Lee, S. Kim, L. W. Park, et S. Park, « Security issues on smart grid and blockchain-based secure smart energy management system », in *MATEC Web of Conferences,* 2019, vol. 260, p. 01001.

[24] A. Hasankhani, S. M. Hakimi, M. Bisheh-Niasar, M. Shafie-khah, et H. Asadolahi, « Blockchain technology in the future smart grids: A comprehensive review and frameworks«, *International Journal of Electrical Power & Energy Systems,* vol. 129, p. 106811, 2021.

[25] A. Kpegouni, E. T. G. Palanga, et A. A. Salami, « Electricity Grids Facing Cyber Threats: What Approaches For Electricity Companies? », in *2022 V International Conference on High Technology for Sustainable Development (HiTech)*, oct. 2022, p. 1-4. doi: 10.1109/HiTech56937.2022.10145560.