Nations Unies ECE/ENERGY/GE.6/2023/3–ECE/ENERGY/GE.5/2023/3

Conseil économique et social

Distr. générale
27 juillet 2023
Français
Original : anglais

Commission économique pour l'Europe

Comité de l'énergie durable

Groupe d'experts des systèmes de production moins polluante d'électricité
Dix-neuvième session
Genève, 3 et 4 octobre 2023
Point 7 de l'ordre du jour provisoire
Fiabilité et cyber-résilience des systèmes énergétiques intégrés intelligents

Groupe d'experts de l'efficacité énergétique
Dixième session
Genève, 5 et 6 octobre 2023
Point 6 de l'ordre du jour provisoire
Transition numérique et résilience des systèmes énergétiques

Principales considérations relatives à la cyber-résilience des systèmes énergétiques intégrés intelligents et solutions pour la garantir

Note du secrétariat

Résumé

La transition numérique, c'est-à-dire l'application des technologies et modèles d'activité numériques aux procédés existants, suscite un intérêt croissant, étant donné qu'elle pourrait accompagner la transition énergétique et lui être complémentaire. Toutefois, l'intégration de plusieurs sources d'énergie et l'interconnexion des différents composants d'un système énergétique intégré intelligent nécessitent l'échange de grandes quantités de données, ce qui augmente l'exposition à des risques de cybersécurité.

La présente note a été élaborée dans le cadre de l'Équipe spéciale de la transition numérique dans le domaine de l'énergie, par le Groupe d'experts de l'efficacité énergétique et le Groupe d'experts des systèmes de production moins polluante d'électricité, conformément à leur plan de travail respectif pour la période 2022-2023 et compte tenu des menaces grandissantes qui pèsent sur la sécurité de l'information à mesure que la transition numérique du système énergétique s'accélère. L'Équipe spéciale a en outre conscience qu'il est important que tous les organes subsidiaires du Comité de l'énergie durable collaborent afin que les aspects propres aux différents éléments de la chaîne de valeur de l'énergie soient pris en compte.

On trouvera dans le présent document des considérations générales sur le sujet, ainsi qu'un recensement et une classification des types de cyberattaques qui peuvent toucher les composants vulnérables des systèmes énergétiques et des conséquences qu'elles peuvent avoir. À titre de conclusion, un ensemble de mesures à mettre en place, au niveau de la gestion et sur le plan technique, et de recommandations à suivre afin d'atténuer les risques de cybersécurité est proposé.

I. Introduction

1. L'intégration croissante d'énergies renouvelables à production variable rend les excédents et les pénuries d'énergie plus fréquents. C'est pour remédier à ce problème de fiabilité qu'est apparu le concept de « systèmes énergétiques intelligents » intégrant différentes sources d'énergie et solutions de stockage et ouvrant la voie à un rôle actif du prosommateur[1].

2. En plus d'intégrer différentes sources d'énergie, les systèmes intelligents comportent plusieurs composants connectés, qui permettent la collecte détaillée et en temps réel de données sur la production, la transmission, la distribution et la consommation d'énergie, ainsi que l'analyse de ces données grâce à des outils tels que l'intelligence artificielle (IA). Il est ainsi possible de produire de nouvelles informations utiles qui conduisent à de meilleures prévisions et facilitent la prise de décisions en matière de planification, d'exploitation et de maintenance. En raison de cette interconnexion multidirectionnelle, des systèmes plus intelligents reposant davantage sur les technologies numériques ont été mis au point et sont désignés par l'expression « réseaux électriques intelligents » (*smart grid*s en anglais). Ils peuvent être unidirectionnels (les données sont collectées sans que les informations qui en sont extraites ne soient remobilisées) ou bidirectionnels (les données collectées sont analysées et utilisées pour contrôler, faire fonctionner ou gérer certains équipements ou dispositifs). Ils peuvent également permettre de coordonner les besoins et les capacités de l'ensemble des producteurs, gestionnaires réseau, utilisateurs finaux et parties prenantes du marché de l'électricité. Il est ainsi possible d'assurer une exploitation du système la plus efficace, fiable, résiliente, flexible et stable possible et de réduire au minimum les coûts et les effets sur l'environnement.

3. Grâce au recours accru aux technologies numériques dans des systèmes plus intelligents, il est possible de proposer différentes solutions, notamment en ce qui concerne la gestion de la demande, l'écrêtement des pointes de consommation (privilégier la consommation d'énergie pendant les périodes où la demande est plus faible) et le stockage de l'énergie excédentaire. En outre, la transition numérique donne les moyens de prévoir les flux énergétiques et de modifier le comportement des fournisseurs d'électricité, des consommateurs et des prosommateurs par le recours à des taxes, à des signaux tarifaires ou à d'autres mesures.

4. L'adoption d'un système énergétique intégré intelligent présente de nombreux avantages, mais elle comporte également son lot de défis à relever. Parmi eux, l'exposition accrue aux risques de cyberattaques. Il s'agit là d'une conséquence inévitable du passage de composants physiques indépendants à des dispositifs intelligents et des équipements intégrés reliés par des réseaux.

5. En général, les cyberattaques visent à prendre le contrôle du système ou des données, ou à endommager du matériel, et donc à nuire à la réputation d'une entité ou à saper la confiance qu'elle inspire. Lorsqu'elles ciblent un système énergétique intégré intelligent, elles servent donc à prendre le contrôle du système d'une manière qui entrave sa capacité à fournir de l'énergie.

6. L'augmentation du nombre de dispositifs rend les cyberattaques plus probables. Cette situation s'explique par le fait que les capteurs, les relais, les commandes de machine, les dispositifs de commande et autres ont tous une surface d'attaque différente. On entend par « surface d'attaque » la somme de tous les points d'entrée que les cybercriminels peuvent emprunter pour prendre le contrôle d'un système, y compris le réseau utilisé pour connecter tous ses composants. Dans le cas d'un système énergétique intégré intelligent, la surface d'attaque correspond au moins aux composants liés aux réseaux de production, de transport, de transmission et de distribution d'énergie, aux dispositifs de stockage, aux équipements qui consomment de l'énergie et à un réseau de communication numérique.

[1] GEEE-7/2020/INF.3 (https://unece.org/sites/default/files/2020-12/GEEE-7.2020.INF_.3.pdf).

A. Cyberattaques menées sur des composants d'un système énergétique intégré intelligent et exemples de conséquences qu'elles peuvent avoir

7. Le système énergétique faisant partie des infrastructures critiques et l'énergie étant un pivot de la société, les cyberattaques peuvent être lourdes de conséquences, notamment économiques, sociales et environnementales. On observe, à partir de quelques exemples récents de cyberattaques par logiciel rançonneur menées sur des infrastructures critiques, qui ont entraîné des coupures temporaires et des pertes de données, une tendance à la hausse : si les attaques de ce type ont presque doublé en 2022, les six derniers mois de l'année ont à eux seuls été marqués par une augmentation de 35 % des familles de rançongiciels visant des infrastructures industrielles et par une hausse de 53 % des logiciels malveillants et des *wipers* (programme dont l'objectif est d'effacer les données)[2].

8. Cette tendance n'a rien de surprenant, étant donné que la prévention des cyberattaques et l'atténuation de leurs conséquences n'est pas chose aisée. À cela s'ajoute le fait que la cybersécurité n'est souvent pas prise en compte dès la conception et jusqu'à l'exploitation des systèmes énergétiques intégrés intelligents, et ce, malgré leur très grande surface d'attaque. Le tableau 1 comprend une liste des composants vulnérables de ces systèmes qui servent à la production, à la transmission et à la distribution d'énergie.

Tableau 1
Composants des systèmes énergétiques intégrés intelligents servant à la production, la transmission et la distribution d'énergie, et leur fonction (liste non exhaustive)

Production	*Transmission*	*Distribution, ressources énergétiques décentralisées et consommateurs*
Dispositifs de suivi des équipements Systèmes de commande Dispositifs de protection (relais, etc.) Appareils enregistreurs Interfaces des systèmes de gestion de l'énergie, des systèmes de surveillance et d'acquisition de données, des consoles de maintenance, etc.	Transformateurs s'appuyant sur la technologie optique Dispositifs de suivi des équipements Dispositifs de protection (relais, etc.) Synchrophaseurs Systèmes de commande Appareils enregistreurs Interfaces des systèmes de gestion de l'énergie, des systèmes de surveillance et d'acquisition de données, des consoles de maintenance, etc. Dispositifs servant à l'automatisation des postes électriques Unités de terminal à distance	Dispositifs avancés de mesure (compteurs intelligents) Dispositifs servant à l'automatisation (réenclencheurs automatiques, feeders, etc.) Dispositifs de protection Dispositifs d'aide à la mobilité Dispositifs de suivi et de contrôle des éléments suivants : • Panneaux solaires • Batteries (stockage) • Véhicules électriques et chargement • Bâtiments intelligents • Microréseau Gestion de la charge Interaction avec le consommateur

[2] Fortinet, Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs (février 2023).

9. Les dispositifs, serveurs, ordinateurs et systèmes connectés et intelligents utilisés dans les systèmes énergétiques intégrés intelligents sont composés de plusieurs éléments qui peuvent tous potentiellement être attaqués par les moyens exposés ci-après :

a) Serveurs : recours à des services qui ne devraient pas être accessibles de l'extérieur, exploitation des vulnérabilités connues de logiciels obsolètes, exploitation de paramètres de configuration non sécurisés (par exemple, mots de passe par défaut) et obtention d'un accès non autorisé à des données sensibles ;

b) Réseaux : contournement de l'authentification, surcharge du réseau au point d'en altérer le fonctionnement normal, exploitation de paramètres de configuration non sécurisés (par exemple, chiffrement faible) et obtention d'un accès non autorisé aux données de communication d'autres utilisateurs ;

c) Sites Web : utilisation de fonctionnalités qui ne devraient pas être accessibles, exploitation de vulnérabilités connues, exploitation de paramètres de configuration non sécurisés (par exemple, mots de passe par défaut), obtention d'un accès non autorisé à des données sensibles (par exemple, base de données dorsale ou communications non chiffrées), obtention d'un accès non autorisé au serveur dorsal, attaque visant d'autres utilisateurs et introduction d'un logiciel malveillant ;

d) Applications mobiles : utilisation de fonctionnalités qui ne devraient pas être accessibles, exploitation de vulnérabilités connues, exploitation de paramètres de configuration non sécurisés (par exemple, mots de passe par défaut), obtention d'un accès non autorisé à des données sensibles (par exemple, base de données dorsale ou communications non chiffrées), et obtention d'un accès non autorisé à l'appareil mobile associé ;

e) Logiciels et micrologiciels : contournement de l'authentification, exploitation de vulnérabilités connues, exploitation de paramètres de configuration non sécurisés (par exemple, mauvaise gestion des droits) et obtention d'un accès non autorisé à des données sensibles (par exemple, code source) ;

f) Services Web : exploitation de vulnérabilités connues, exploitation de paramètres de configuration non sécurisés (par exemple, authentification sans mot de passe), obtention d'un accès non autorisé à des données sensibles (par exemple, données d'autres utilisateurs) et obtention d'un accès non autorisé au serveur dorsal ;

g) Nuages : obtention d'un accès non autorisé aux données d'autres utilisateurs (par exemple, dossiers), obtention d'un accès non autorisé au serveur dorsal, exploitation de paramètres de configuration non sécurisés (par exemple, authentification en devinant le mot de passe), obtention d'un accès non autorisé à des données sensibles (par exemple, mots de passe ou clefs d'accès) et exploitation de vulnérabilités connues ;

h) Capteurs, moteurs, relais, etc. : exploitation de vulnérabilités connues des logiciels, exploitation de paramètres de configuration non sécurisés, altération des données envoyées par un capteur, moteur, relais ou autre, modification des fonctionnalités d'un capteur, moteur, relais ou autre, désactivation du capteur, et obtention d'un accès non autorisé à des données ;

i) Matériel informatique : altération du matériel, introduction sur le réseau de matériel infecté par un logiciel malveillant, attaque visant les interfaces de détection des problèmes, altération des données transférées ;

j) Utilisateurs : envoi de courriers électroniques malveillants (par exemple, courriers de hameçonnage, invitant les destinataires à fournir des données sensibles, ou pièces jointes contenant un logiciel malveillant), manipulation des utilisateurs destinée à leur causer une frayeur pour qu'ils effectuent une action qui leur est nuisible sans s'en rendre compte, désinformation visant à les inciter à communiquer des informations sensibles.

10. Il existe de nombreux autres types d'attaques possibles, qui peuvent être classées selon les quatre types suivants :

a) Les attaques physiques (visant les composants physiques du système), notamment :

i) Les attaques occasionnant des dommages physiques : l'attaque vise un composant et lui occasionne des dommages physiques, provoque son dysfonctionnement ou l'empêche de fonctionner ;

ii) Les attaques d'ingénierie sociale : l'attaque consiste à tromper et à manipuler des utilisateurs pour qu'ils communiquent des informations sensibles pouvant être utilisées pour mener d'autres attaques ;

iii) Les attaques consistant à falsifier un nœud ou à ajouter un nœud malveillant au réseau : dans un système énergétique intégré intelligent, on désigne par « nœud » un composant qui relie un appareil physique à Internet et qui permet la collecte, le traitement ou le contrôle des données. On entend par « falsification » le fait d'accéder aux données, mais aussi de les altérer. Ce type d'attaques peut cibler un nœud existant, mais peut aussi consister à ajouter un nœud au système.

b) Les attaques logicielles (visant les programmes informatiques exécutés par les dispositifs physiques du système énergétique intégré intelligent), notamment :

i) Les codes malveillants : l'attaque consiste à ajouter des fonctions nuisibles à un logiciel existant, par exemple afin de voler des données de connexion ;

ii) Les logiciels malveillants : l'attaque consiste à installer un logiciel permettant diverses activités nuisibles, par exemple un logiciel espion servant à voler des données, un virus destiné à endommager ou modifier des fichiers ou des données, un *wiper* permettant d'effacer des données et des logiciels, ou un rançongiciel visant à chiffrer des données ;

iii) Les attaques par saturation : l'attaque vise à rendre indisponible un dispositif ou un logiciel, par exemple en surchargeant ce dernier de requêtes ou en provoquant son arrêt. Lorsqu'une attaque de ce type est menée simultanément depuis de nombreux ordinateurs, on l'appelle attaque par déni de service distribué.

c) Les attaques réseau (visant à obtenir un accès non autorisé au réseau et à y effectuer des actions non autorisées), notamment :

i) Les attaques par analyse du trafic : l'attaque vise à extraire des renseignements à partir des caractéristiques d'un flux de données qui peuvent être observées, même si le contenu de ce dernier n'est pas visible ;

ii) Les attaques par redirection d'informations : l'attaque consiste à intercepter, modifier ou détourner les données envoyées par le réseau, par exemple pour les surveiller ou les voler, ou pour perturber les services fournis par le système énergétique ;

iii) Les attaques *Sinkhole* : l'attaque consiste à ajouter un nœud compromis dans le réseau pour qu'il envoie de faux messages aux autres nœuds et les incite à lui envoyer des informations ;

iv) Les attaques par accès non autorisé : l'attaque consiste à obtenir un accès au réseau sans y être autorisé.

d) Les attaques par chiffrement (visant à contourner la sécurité par l'ajout d'un chiffrement, qui rend nécessaire une clef pour retransformer le code en informations ou données lisibles), notamment :

i) Les attaques reposant sur la cryptanalyse : l'attaque consiste à déduire les informations ou données chiffrées sans posséder la clef de chiffrement ;

ii) L'attaque par canal auxiliaire : l'attaque consiste à exploiter des informations qui sont fournies de manière non intentionnelle par un système informatique au cours d'opérations cryptographiques afin d'obtenir un accès à des informations chiffrées ;

iii) L'attaque de l'homme du milieu : l'attaque consiste à compromettre le canal de communication entre deux composants, de manière à intercepter, voire modifier, les messages chiffrés qu'ils s'échangent.

11. On observe souvent plusieurs types de cyberattaques déployés simultanément, ce qui entraîne un cumul de défis à relever et de perturbations pour les victimes potentielles. En outre, les cyberattaques peuvent être utilisées en complément d'autres types d'attaques physiques.

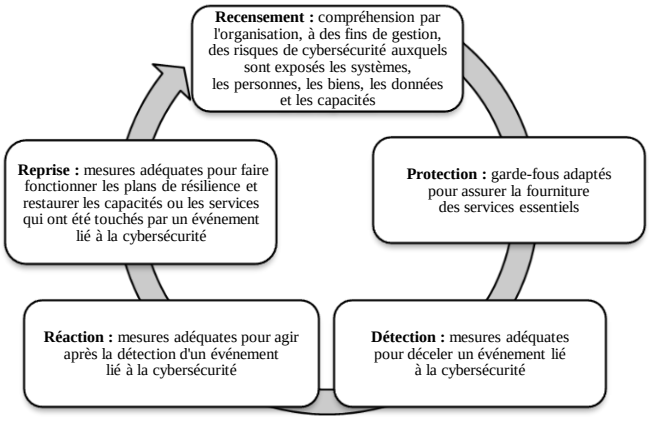
B. Mesures visant à prévenir les cyberattaques visant les composants de systèmes énergétiques intégrés intelligents

12. Les systèmes énergétiques intégrés intelligents faisant partie des infrastructures critiques, il est essentiel de prévenir les cyberattaques qui les visent. Lorsque celles-ci ne peuvent pas être empêchées, il convient d'en atténuer les conséquences. Pour ce faire, il y a lieu de mettre en place des solutions variées afin d'établir une stratégie globale et cohérente, parfois désignée sous le terme de « défense en profondeur ».

13. De nombreux cadres et normes, tels que le cadre du National Institute of Standards and Technology (Institut des normes et de la technologie des États-Unis) visant à améliorer la cybersécurité des infrastructures critiques et la série de normes 62443 de la Commission électrotechnique internationale (CEI)[3], constituent de très bons points de départ à l'élaboration et à l'application de programmes de cybersécurité efficaces.

14. Par exemple, le cadre du National Institute of Standards and Technology contient une liste d'activités classées selon cinq fonctions d'élaboration et d'application essentielles (voir la figure ci-dessous). Il porte également sur les ressources (humaines, matérielles et financières), le contrôle de supervision (gouvernance), les procédures et les technologies.

Figure
Cadre du National Institute of Standards and Technology



Source : adapté de National Institute of Standards and Technology, « NIST Releases Version 1.1 of its Popular Cybersecurity Framework », 16 avril 2018.

15. En outre, les activités destinées à la prévention, à l'atténuation et à la reprise doivent être menées au niveau de la gestion, mais aussi sur le plan.

[3] Série ISA/IEC 62443 définissant des normes de cybersécurité des systèmes d'automatisation et de commande.

Tableau 2
Activités destinées à la prévention, à l'atténuation et à la reprise pour les programmes de cybersécurité (liste non exhaustive)

Niveau	*Prévention*	*Atténuation*	*Reprise*
Gestion (approche descendante) : les stratégies et les réglementations établies sont à destination de la main-d'œuvre*.	i) Gestion des risques : recenser les actifs numériques (c'est-à-dire tout élément numérique qui a de la valeur), tels que les photos, les vidéos, les fichiers audio, et les textes. ii) Gestion des actifs : évaluer les mesures de sécurité existantes et mettre en place des nouvelles mesures. iii) Gestion des mises à jour ou des correctifs : dans le cadre établi, informer les administrateurs de l'installation ou du déploiement de mises à jour, les logiciels obsolètes ayant une plus grande surface d'attaque. iv) Systèmes de cybersécurité : utiliser des pare-feu pour contrôler le trafic entrant du réseau selon des règles de sécurité prédéfinies, ce qui permet de garantir que seules les personnes autorisées ont accès au réseau ou à un segment de celui-ci. Un contrôleur d'accès au réseau permet de veiller à ce que l'accès soit autorisé aux seuls utilisateurs authentifiés et appareils autorisés qui respectent les règles de sécurité. v) Ségrégation des réseaux : séparer les réseaux, en particulier un réseau d'importance stratégique, d'Internet et d'autres réseaux moins importants tels que les réseaux administratifs, afin de réduire la probabilité d'accès non autorisé. vi) Gestion des droits d'accès (dont gestion de l'authentification et gestion des clefs) : stocker et gérer les noms d'utilisateurs, mots de passe et autres moyens d'authentification comme les clefs (ces activités comprennent la création, l'attribution, le stockage et la mise à jour). Afin que les différentes parties du système énergétique intégré intelligent aient des effets complémentaires, les méthodes d'authentification utilisées dans chacune d'entre elles doivent être identiques. Le choix de la méthode la plus adaptée dépend de différents facteurs, tels que l'extensibilité et la sécurité.	i) Système de détection des intrusions : surveiller en permanence le système et repérer les éventuelles anomalies. Une anomalie peut prendre de nombreuses formes, par exemple un nombre anormal de tentatives de connexion sur un compte, un trafic réseau inhabituel depuis un ordinateur ou un appareil supplémentaire sur le réseau. Lorsqu'une anomalie est détectée, elle est isolée. Lorsque le trafic émanant d'un ordinateur est anormalement élevé, cet ordinateur est bloqué. La plupart du temps, l'administrateur du réseau est prévenu de l'anomalie afin que des mesures adéquates puissent être prises. Les faux positifs étant possibles, l'apprentissage automatique et l'intelligence artificielle peuvent être utilisés pour améliorer la détection.	Les réglementations fondées sur ces normes peuvent prévoir des mesures destinées à la reprise, y compris la planification de cette dernière, à savoir les processus et procédures à mettre en place pour permettre la restauration de systèmes ou d'actifs touchés par un cyberincident. Ces processus et procédures doivent être suivis dans le cadre de la gestion de la continuité des opérations afin de revenir à un fonctionnement normal le plus rapidement possible.

* *Note* : les types de stratégies de prévention et d'atténuation doivent être précisés. Ces stratégies doivent de préférence être définies dans des règlements. Ces derniers peuvent par exemple être appliqués sur la base de la série de normes IEC 62443 et de la norme ISO/IEC 27032:2012 (Technologies de l'information − Techniques de sécurité − Lignes directrices pour la cybersécurité, accessible à l'adresse suivante : https://www.iso.org/fr/standard/44375.html). La première concerne la cybersécurité de la technologie opérationnelle dans les systèmes d'automatisation et de commande, tandis que la seconde s'applique à la protection des données, des systèmes et des opérations et activités en ligne sensibles, afin d'éviter qu'ils soient piratés, sabotés ou modifiés. Afin de renforcer encore davantage la sécurité en travaillant au niveau de l'information, on peut envisager d'appliquer la norme ISO/IEC 27001:2022 (Systèmes de management de la sécurité de l'information, accessible à l'adresse suivante : https://www.iso.org/fr/standard/27001), qui aide les organisations à gérer la sécurité informatique à l'échelle des personnes, des procédures et des technologies.

Niveau	*Prévention*	*Atténuation*	*Reprise*
	vii) Attestation d'intégrité : vérifier l'intégrité du logiciel et veiller à ce qu'il n'ait pas été compromis. Analyse de code : vérifier la qualité du code et s'assurer de l'absence de failles de sécurité que des hackers pourraient exploiter. Le modèle zero trust constitue une autre solution permettant de garantir la sécurité d'un système. viii) Sécurité des appareils et des logiciels : vérifier la sécurité des composants du système énergétique intégré intelligent, par exemple grâce à des tests d'intrusion. ix) Cryptographie : vérifier que les données peuvent être échangées en toute sécurité et demeurent invisibles aux utilisateurs non autorisés. Selon le critère de sécurité et le contexte, il est possible d'utiliser différents algorithmes et méthodes afin de transformer des données en codes indéchiffrables. La puissance de l'algorithme est également importante à cet égard. x) Sensibilisation : entretenir une culture de la cybersécurité ou promouvoir la cyberhygiène au moyen, par exemple, de démonstrations de piratages, afin d'illustrer comment les cybercriminels attaquent différents composants. Ces activités ne sont pas destinées uniquement au personnel technique, elles peuvent aussi être utilisées pour sensibiliser le personnel non technique aux moyens dont il dispose pour renforcer la cybersécurité. xi) Programmes de cybersécurité et mentalité : rassurer les organisations sur le fait que tous les aspects de la cybersécurité sont couverts en tenant compte des risques économiques, sociétaux et environnementaux. xii) Stratégie zero trust : appliquer le principe « Never trust, always verify », selon lequel aucun utilisateur ou appareil ne doit recevoir de confiance par défaut, même s'il est connecté à un réseau autorisé.	ii) Techniques de prévention de la perte de données : prévenir la perte d'informations et empêcher que des données infectées par un virus soient transmises. Ces techniques sont utilisées lorsqu'un virus essaye d'utiliser ou d'envoyer des informations confidentielles. Pour éviter cela, il est possible d'isoler un appareil infecté ou de bloquer l'accès aux appareils non autorisés.	
Technique (approche ascendante) : les problèmes rencontrés sont signalés aux gestionnaires, qui reçoivent également un retour d'informations afin d'améliorer les stratégies et les réglementations.	a) Analyse de code (pas nécessairement envisageable pour tous les dispositifs en fonctionnement) : analyser le code source d'une application afin de détecter des vulnérabilités. Cette analyse peut être statique ou dynamique. Lorsqu'elle est statique, l'analyste a un accès complet au code source et recherche les vulnérabilités dans les lignes de code. Lorsqu'elle est dynamique, l'analyste n'a pas accès au code source et exécute le programme informatique en le passant au crible à la recherche de vulnérabilités. b) Recours à un scanner de vulnérabilités : évaluer automatiquement les problèmes de sécurité des systèmes ainsi que le logiciel exécuté sur ces systèmes. Ces analyses sont utiles, car elles permettent de détecter les points d'entrée que les hackers peuvent emprunter pour pénétrer dans un système et qu'ils peuvent utiliser comme des tremplins pour mener d'autres attaques.	Centre des opérations de sécurité : désigner une équipe de professionnels qui supervise toute l'infrastructure des systèmes d'information de l'organisation, afin de détecter en temps réel tout événement constituant une menace pour la cybersécurité et de réagir aussi rapidement et efficacement que possible. Le centre est chargé de choisir, d'exécuter et de tenir à jour les technologies de cybersécurité de l'organisation	a) Criminalistique numérique : collecte de preuves permise par le recensement des appareils susceptibles de fournir des informations sur une cyberattaque et la collecte et l'analyse des données qu'ils contiennent. Elle fournit également des indications

Niveau	*Prévention*	*Atténuation*	*Reprise*
	c) Test d'intrusion : évaluer le niveau de sécurité d'un réseau, système, appareil ou logiciel en lançant une cyberattaque autorisée. L'objectif de ce test est de rechercher un large éventail de problèmes de sécurité. d) Équipe rouge : trouver un exemple illustrant les conséquences profondes d'une cyberattaque, plutôt que de chercher à détecter une grande variété de problèmes de sécurité comme dans un test d'intrusion. Cette technique est semblable au test d'intrusion, puisqu'il s'agit de cyberattaques autorisées, la principale différence étant une différence d'échelle − le test est généralement mené à l'échelle d'une entreprise.	et d'améliorer la détection des menaces, l'ensemble des mesures de sécurité ainsi que les capacités de réaction et de prévention en coordonnant l'ensemble des technologies et des opérations de cybersécurité. Pour remplir ce mandat, il analyse les données provenant de différentes sources, notamment les renseignements communiqués par les autorités et les professionnels du secteur, au moyen en particulier d'un système de gestion des événements et des informations de sécurité (SIEM), qui permet d'analyser les anomalies comportementales au moyen de l'IA afin de détecter automatiquement les cyberattaques et de réagir.	précieuses sur les moyens d'éviter les cyberattaques à l'avenir. b) Élimination : élimination de la source de l'incident et reconstruction des systèmes ayant subi l'attaque afin de revenir à un fonctionnement normal (grâce aux sauvegardes, plans de reprise et plans de continuité des opérations).

III. Recommandations

16. Compte tenu des indications contenues dans le présent document sur la cybersécurité des systèmes énergétiques intégrés intelligents, les conclusions, mesures et recommandations ci-après sont proposées pour examen :

a) Niveau réglementaire : veiller à l'application des normes et lignes directrices relatives au renforcement de la cybersécurité de la technologie opérationnelle dans les systèmes d'automatisation et de commande et à la cybersécurité des infrastructures critiques ;

b) Niveau financier : prévoir des mesures d'incitation fiscale pour les entreprises qui appliquent les normes pertinentes en matière de cybersécurité, et allouer des fonds aux initiatives relatives à la cybersécurité, telles que les activités de recherche-développement et de sensibilisation en lien avec la cybersécurité ;

c) Niveau structurel :

i) Établir des stratégies nationales de cybersécurité qui expliquent comment prévenir et gérer les cyberattaques ciblant les systèmes énergétiques intégrés intelligents et qui définissent les attributions des différentes parties prenantes, notamment celles des organismes publics, des entreprises et des individus ;

ii) Collaborer avec d'autres pays à des fins de mise en commun des normes et communiquer des informations sur les acteurs malveillants potentiels afin de pouvoir gérer plus efficacement les risques liés à la cybersécurité ;

iii) Appliquer des plans de gestion de la continuité des opérations décrivant la manière de faire face aux incidents de cybersécurité, notamment ceux qui entraînent des coupures de courant ;

iv) Assurer une répartition adéquate des responsabilités en matière de cybersécurité dans le secteur de l'énergie (gouvernance) entre les parties prenantes aux niveaux national et supranational ;

d) Communication d'informations : demander que les informations concernant la protection des données et la cybersécurité soient communiquées aux organismes officiels afin de stimuler les stratégies ascendantes ;

e) Sensibilisation : déterminer quels sont les chefs de file du secteur qui peuvent montrer l'exemple, et former les entreprises et les organismes publics sur les aspects théoriques et pratiques afin de les aider à appliquer les mesures de cybersécurité tant au niveau de la gestion que sur le plan technique.