Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1331

(03/2018)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité des réseaux électriques intelligents

Lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques (HAN) dans les réseaux électriques intelligents

Recommandation UIT-T X.1331

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	**X.1330–X.1339**
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1331

Lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques (HAN) dans les réseaux électriques intelligents

Résumé

Les réseaux domestiques (HAN) au sein des réseaux électriques intelligents sont des réseaux dans les locaux du client. Contrairement aux réseaux HAN classiques, les réseaux HAN dans les réseaux électriques intelligents comportent des dispositifs de réseau électrique intelligent, tels que des sources d'énergie réparties (DER), un chargeur pour véhicules électriques, un système domestique de gestion de l'énergie (HEMS) et un système d'affichage de l'énergie du client (CED). Les récepteurs d'électricité et les sources DER du client sont connectés au réseau HAN de façon à ce que le client puisse les activer et les désactiver en fonction des informations reçues du réseau général, afin que la consommation électrique soit la plus rationnelle possible. Un réseau HAN est généralement connecté à l'Internet, c'est pourquoi les auteurs d'attaques ont facilement accès à ces réseaux et aux dispositifs HAN. Par conséquent, ces dispositifs devraient être capables d'empêcher les auteurs d'attaques de porter atteinte aux réseaux et dispositifs HAN. La Recommandation UIT-T X.1331 fournit une analyse des menaces auxquelles sont exposés les réseaux HAN dans les réseaux électriques intelligents, les exigences de sécurité et les fonctions de sécurité. Le rôle et les fonctions de chaque dispositif HAN étant différents, les exigences de sécurité et les fonctions de sécurité sont fournies pour chaque dispositif.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1131	29.03.2018	17	11.1002/1000/13405

Mots clés

Réseau domestique, lignes directrices relatives à la sécurité, exigences de sécurité, réseau électrique intelligent.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1331

Lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques (HAN) dans les réseaux électriques intelligents

1 Domaine d'application

La présente Recommandation donne des lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques (HAN) dans les réseaux électriques intelligents. Il porte sur les points suivants:

– risques relatifs à la sécurité des dispositifs et des communications dans un réseau HAN;

– exigences de sécurité des dispositifs et des communications dans un réseau HAN;

– fonctions de sécurité pour les dispositifs et les communications dans un réseau HAN.

2 Références

Aucune.

3 Termes et définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 interface de services d'énergie (ESI) [b-UIT-T Y.2071]: ensemble de fonctions comprenant des fonctions de passerelle et des fonctions nécessaires pour permettre aux applications de réseau électrique intelligent de commander et de gérer les services de réseau électrique intelligent dans les locaux du client.

3.1.2 système de stockage de l'énergie (ESS) [b-UIT-T L.1430]: unité physique ou composant capable de stocker ou d'accumuler l'énergie produite par un générateur ou l'énergie obtenue auprès d'un consommateur.

NOTE – Un système ESS fournit des fonctions de stockage de l'électricité en utilisant différents types de batteries. On peut par exemple avoir recours au stockage d'énergie en cas de mise en œuvre d'un mécanisme de tarification dynamique dans un réseau de services collectifs. L'énergie électrique est stockée lorsque son coût est relativement bas et peut être utilisée ultérieurement lorsque le prix de l'électricité dans le réseau est plus élevé.

3.1.3 réseau domestique (HAN) [b-UIT-T G.9959]: réseau capable de connecter des dispositifs situés au domicile d'un particulier.

3.1.4 système domestique de gestion de l'énergie (HEMS) [b-UIT-T Y.4409]: système informatique composé d'une plate-forme logiciel fournissant des services d'appui de base et d'un ensemble d'applications fournissant les fonctionnalités nécessaires au fonctionnement efficace des équipements domestique, comme les appareils électroménagers et les batteries de stockage, afin d'assurer la sécurité adéquate de l'alimentation en énergie à un coût le plus bas possible.

NOTE – Un système HEMS est désigné par un réseau HAN dans un réseau électrique intelligent.

3.1.5 affichage à domicile (IHD) [b-UIT-T Y.4409]: dispositif utilisateur à écran servant à présenter les informations sur la consommation d'énergie de l'habitation. Les utilisateurs peuvent, à titre d'option, commander les appareils domestiques avec l'interface utilisateur de ce dispositif.

NOTE – Les informations de commande et d'utilisation sont transférées dans un environnement de système de communication HAN. Un téléphone mobile ou un téléphone intelligent, une télévision (utilisant le protocole Internet), un visiophone Internet, un ordinateur personnel, une tablette ou un boîtier mural peuvent servir de dispositif utilisateur à écran.

3.1.6 réseau étendu (WAN) [b-UIT-T Y.4409]: réseau de communication IP quelconque couvrant une grande zone géographique où l'Internet est disponible et prenant en charge des dispositifs et des réseaux locaux.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 véhicule électrique (EV): véhicule à moteur pouvant être rechargé sur une source extérieure d'électricité quelconque et également être utilisé comme système de fourniture d'énergie.

Il s'agit par exemple des véhicules tout électriques, des véhicules électriques fonctionnant sur batterie, des véhicules électriques hybrides rechargeables et des véhicules électriques hybrides transformés en véhicules rechargeables. Un véhicule électrique rechargeable est parfois appelé en anglais "grid enabled vehicle" (véhicule compatible à réseau intelligent) ou "electrically chargeable vehicle" (véhicule rechargeable à l'électricité).

3.2.2 réseau de proximité (NAN): réseau d'accès qui permet aux dispositifs terminaux des réseaux électriques intelligents et aux réseaux domestiques (HAN) de se connecter au réseau étendu (WAN).

NOTE – Adaptée de [b-Smart-O-33].

3.2.3 compteur intelligent: dispositif installé dans les locaux pour suivre et maîtriser la consommation électrique des dispositifs domestiques intelligents sur la base des informations de gestion active de la demande qu'ils reçoivent.

NOTE – Adaptée de [b-UIT-T Y.4409].

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AMI infrastructure de comptage évoluée (*advanced metering infrastructure*)

CED système d'affichage de l'énergie du client (*customer energy display*)

DER source d'électricité décentralisée (*distributed electricity resource*)

DG générateur décentralisé (*distributed generator*)

DoS déni de service (*denial of service*)

DTLS sécurité de la couche transport en mode datagramme (*datagram transport layer security*)

ESI interface de services d'énergie (*energy services interface*)

ESS système de stockage d'énergie (*energy storage system*)

EV véhicule électrique (*electric vehicle*)

G/W passerelle (*gateway*)

HAN réseau domestique (*home area network*)

HEMS système domestique de gestion de l'énergie (*home energy management system*)

HMAC code d'authentification de message par hachage (*hash-based message authentication code*)

ID identificateur (*identifier*)

IP protocole Internet (*Internet protocol*)

IHD affichage à domicile (*in-home display*)

NAN réseau de proximité (*neighbourhood area network*)

TLS sécurité dans la couche transport (*transport layer security*)

WAN réseau étendu (*wide area network*)

WPA accès protégé WiFi (*Wi-Fi protected access*)

5 Conventions

Aucune.

6 Modèle général de réseau domestique dans un réseau électrique intelligent

Un réseau électrique intelligent est un réseau d'énergie intelligent doté de technologies de communication des informations. Avec un réseau électrique intelligent, le fournisseur d'électricité peut estimer la demande en utilisant les informations sur la consommation électrique des clients transmises par les compteurs intelligents. Par conséquent, le fournisseur peut ensuite maîtriser les pointes de consommation à partir de cette estimation. Avant qu'une pointe se produise, le fournisseur réduit la consommation des clients ou fait basculer le client vers une source d'énergie décentralisée (DER) située dans les locaux du client, par exemple des dispositifs photovoltaïques installés sur le toit, des batteries électriques ou des véhicules électriques (EV). En outre, le client peut retarder ou avancer sa consommation d'électricité en fonction des informations relatives à l'heure de la pointe transmises par le fournisseur.

Pour permettre les échanges d'informations entre le fournisseur d'électricité et le client, le système d'estimation ou de gestion de la demande du fournisseur devrait être connecté aux dispositifs installés dans les locaux du client, comme le système domestique de gestion de l'énergie (HEMS) ou le système d'affichage de l'énergie du client (CED). La Figure 6-1 montre différents réseaux dans un environnement de réseau électrique intelligent. Comme on le voit, la connexion peut passer par plusieurs réseaux, comme un réseau HAN, un réseau d'accès [également appelé réseau de proximité (NAN)] ou un réseau étendu (WAN).

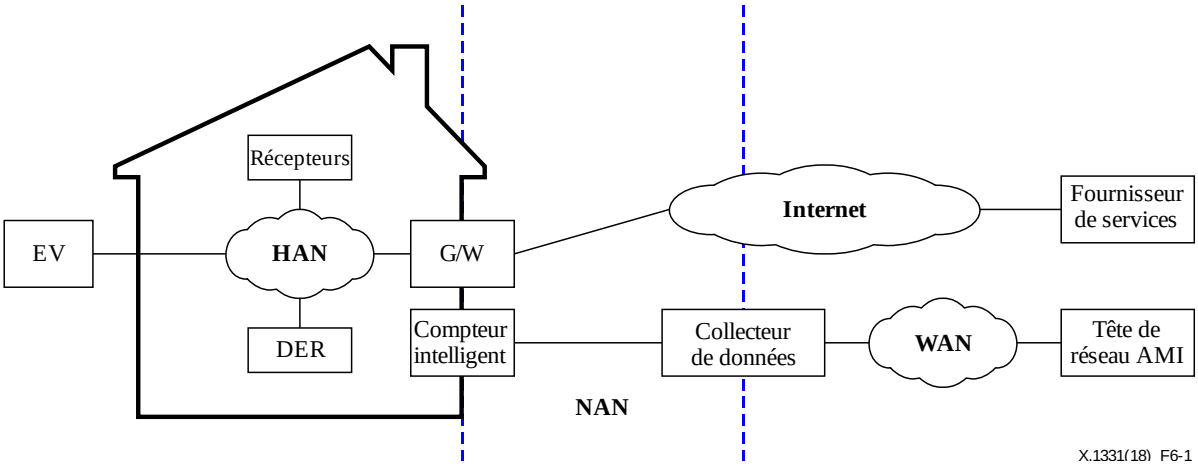

Figure 6-1 – Différents types de réseaux dans un réseau électrique intelligent

Un réseau HAN relie les récepteurs d'électricité et les sources d'électricité qui sont présents chez le client. Toutes les informations provenant des dispositifs HAN et destinées au système d'extrémité du fournisseur d'électricité, comme la tête de réseau d'une infrastructure de comptage évoluée (AMI), devraient partir du réseau HAN et toutes les informations provenant du fournisseur d'électricité devraient parvenir aux dispositifs du client en passant par le réseau HAN.

Un réseau HAN est accessible depuis l'Internet étant donné qu'il y est généralement connecté. Dès lors qu'un utilisateur malveillant peut accéder au réseau HAN, les dispositifs raccordés à ce réseau peuvent être compromis et des informations, comme les récepteurs d'électricité, peuvent être

modifiées de manière intentionnelle par l'auteur d'une attaque. Dans ce cas, l'auteur d'une attaque peut commander les dispositifs HAN à sa guise. Par conséquent, il convient d'envisager des mesures de sécurité au niveau des dispositifs connectés au réseau HAN et des communications qu'ils échangent.

Avant de décrire les menaces, les exigences et les technologies de sécurité, il convient d'élaborer un modèle général de réseau HAN dans un réseau électrique intelligent. Ce modèle général devrait indiquer toutes les entités et interfaces de communication associées afin de préciser leurs relations.

La Figure 6-2 montre un modèle général de réseau HAN dans un réseau électrique intelligent. Ce réseau HAN comprend de nombreux éléments, par exemple un récepteur d'électricité, une source DER, un système HEMS, un système CED [également appelé affichage à domicile (IHD)], une interface de services d'énergie (ESI) et un compteur intelligent.

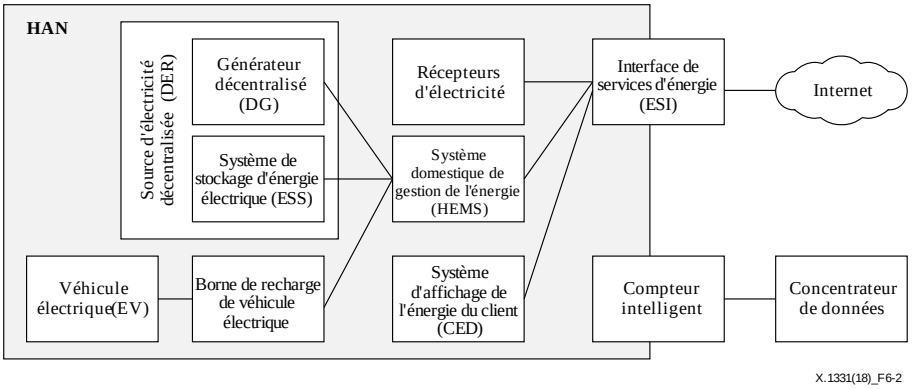

Figure 6-2 – Modèle général de réseau domestique dans un réseau électrique intelligent

- Les récepteurs d'électricité sont généralement des dispositifs qui consomment de l'électricité, par exemple les appareils électroménagers, les climatiseurs et les pompes à eau. Les récepteurs sont généralement de deux types: intelligents ou traditionnels. Les récepteurs intelligents ont des capacités de communication et de comptage que les récepteurs traditionnels n'ont pas. Néanmoins, il est possible de maîtriser la consommation d'électricité imputable aux récepteurs traditionnels grâce à un système HEMS si le dispositif est branché via une prise intelligente, laquelle est dotée de capacités de communication et de commutation. Par conséquent, la présente Recommandation porte sur les récepteurs intelligents et les prises intelligentes en tant que récepteurs d'électricité.
- Les sources DER, qui comprennent les générateurs décentralisés (DG) et les systèmes de stockage d'énergie électrique (ESS), sont des dispositifs qui fournissent de l'électricité pour les récepteurs. Les sources photovoltaïques sont des générateurs décentralisés couramment utilisés dans les réseaux HAN.
- Un véhicule électrique peut être à la fois un récepteur et une source DER. Le véhicule électrique est un récepteur dans le HAN lors de l'opération visant à le recharger et une source DER lorsqu'il fournit de l'électricité pour les appareils électroménagers.
- Un système HEMS commande les capacités des récepteurs et des sources DER en fonction du programme défini par le client ou de conditions définies au préalable. Les principaux critères associés aux conditions sont le prix de l'électricité et le signal de gestion active de la demande.
- Un système CED montre les statistiques de la consommation d'électricité en cours et les informations tarifaires, afin que les clients puissent réduire leur consommation ou modifier le plan de leurs activités consommant de l'électricité.

7 Menaces pour la sécurité des réseaux domestiques

On trouvera dans les paragraphes ci-après les principales menaces pour la sécurité des réseaux HAN. Il est à noter que ces paragraphes n'ont pas vocation à définir la taxonomie des menaces, mais à présenter les menaces que les opérateurs de réseau HAN doivent envisager au minimum.

7.1 Fuite de données

La divulgation d'informations stockées ou communiquées est une menace très courante pour les réseaux et les dispositifs. L'auteur d'une attaque peut épier de manière active les données transmises ou accéder physiquement à un dispositif pour obtenir des données stockées dans la mémoire. Si les données ne sont pas protégées, il peut alors les divulguer.

Etant donné qu'il y a de nombreuses communications hertziennes dans un réseau HAN, il peut être facile de procéder à des écoutes clandestines à l'intérieur ou à l'extérieur de ce réseau. En outre, dans la mesure où les entités dans un réseau HAN sont très souvent raccordées à l'Internet, une entité distante peut y accéder. En conséquence, l'auteur d'une attaque n'ayant aucune autorisation peut accéder aux données transmises et aux données stockées dans un environnement HAN.

Dans un réseau HAN, différents types de données relatives à la vie privée, par exemple les informations sur la consommation d'électricité, les informations de facturation et le plan de consommation électrique, sont stockées dans un système HEMS, dans un système CED ou dans le compteur intelligent. Ces données privées peuvent être transférées depuis ou vers un système HEMS ou un système CED via une interface ESI. La divulgation des données peut avoir de graves répercussions pour la vie privée d'un client. L'auteur de l'attaque connaîtrait alors les habitudes de vie du client.

En outre, les commandes contrôlant le fonctionnement des récepteurs, des sources DER et des bornes de recharge de véhicules électriques peuvent être transférées depuis un système HEMS et le système CED sur le réseau de communication. S'il a accès aux données, l'auteur d'une attaque peut trouver comment contrôler les récepteurs et les sources DER dans un réseau HAN, ce qui peut entraîner une autre menace, par exemple l'insertion de données malveillantes qui est décrite au § 7.2.

7.2 Falsification de données ou insertion de données malveillantes

L'auteur d'une attaque ne disposant d'aucune autorisation peut insérer, modifier ou supprimer des informations transmises entre des entités dans un réseau HAN ou stockées dans une entité HAN. L'auteur de l'attaque peut être une personne, un programme ou une entité HAN. Dans ce type d'attaque, l'intégrité des données peut être altérée. En outre, cette altération de l'intégrité des données peut entraîner un dysfonctionnement des dispositifs.

Etant donné qu'une entité anonyme quelconque peut avoir accès à un réseau de communication hertzien, cette entité peut envoyer des données malveillantes aux entités HAN. En outre, l'auteur d'une attaque peut ajouter des données à une connexion existante dans le but de détourner cette connexion ou d'envoyer des données à des fins malveillantes. De plus, il peut avoir accès à la mémoire de l'entité HAN, par exemple au système HEMS, et modifier les données stockées ou insérer des données malveillantes dans la mémoire.

Si le signal correspondant au prix de l'électricité est modifié pour indiquer une hausse, un système HEMS peut réduire la consommation électrique alors que le client ne souhaite pas. Par ailleurs, l'auteur d'une attaque peut envoyer un message de commande provoquant le déchargement d'un véhicule électrique ou d'un système ESS. On peut aussi citer comme exemples l'envoi d'un grand nombre de demandes à une entité pour créer un déni de service (DoS), la modification de valeurs dans un fichier de données ou l'altération d'un programme afin de modifier le comportement d'une entité HAN.

7.3 Interruption des communications

L'interruption des communications peut être provoquée par un brouillage volontaire ou involontaire qui perturbe l'émetteur ou le récepteur d'une liaison de communication et rend cette liaison de communication inutilisable. La surconsommation de bande passante due à l'envoi d'un très gros volume de données est un autre exemple d'interruption des communications.

Dans un réseau HAN, un système HEMS devrait rassembler les informations sur l'état des récepteurs et des sources DER liés à la consommation électrique, et recevoir les signaux de tarification et de contrôle envoyés par le fournisseur d'électricité ou de services, afin de répondre aux demandes d'ajustement adressées à ces récepteurs et sources DER. Ainsi, pour qu'un réseau HAN fonctionne correctement, ses capacités de communication devraient être correctement entretenues.

7.4 Accès non autorisé

Il peut y avoir accès non autorisé lorsque l'auteur d'une attaque obtient l'accès à des entités, par exemple aux sources DER, au système HEMS ou au système CED, en se faisant passer pour un utilisateur réel. Dès lors qu'une tentative d'accès non autorisé aboutit, l'auteur de l'attaque peut également accéder à d'autres dispositifs.

Pour ce faire, l'auteur d'une attaque doit s'identifier et s'authentifier. Pour y parvenir, il peut lancer une attaque par balayage des ports, qui consiste à déterminer quels ports vulnérables du dispositif HAN sont ouverts. Si des ports vulnérables sont ouverts, l'auteur de l'attaque peut exploiter la vulnérabilité du dispositif HAN. En outre, il peut accéder sans autorisation au service "invulnérable" en lançant une attaque consistant à deviner les mots de passe.

Les logiciels malveillants sont une autre grande menace. Ils peuvent infecter un dispositif HAN, par exemple un système CED, via un courrier électronique ou un service web, et ensuite se propager à d'autres dispositifs dans un réseau HAN. Une fois installé sur un dispositif HAN, un logiciel malveillant peut obtenir un accès non autorisé aux ressources du dispositif, risquant d'entraîner un dysfonctionnement du dispositif, ou une dégradation ou une perturbation de son fonctionnement.

7.5 Répudiation

Cette menace correspond au cas où l'auteur d'une attaque, un émetteur ou un récepteur, nie avoir émis ou reçu un message. Elle n'entraîne pas de détérioration ou de dysfonctionnement des dispositifs HAN, mais elle peut donner lieu à un conflit. Selon la nature de ce conflit, il est possible que la cause du dérangement ou du dysfonctionnement du service ne soit pas identifiée correctement.

7.6 Relations entre les menaces concernant la sécurité et le réseau domestique

Les menaces relatives à la sécurité décrites dans les paragraphes 7.1 à 7.5 concernent certaines entités ou communications du modèle général de réseau HAN. Les relations entre ces menaces et les entités HAN sont présentées dans le Tableau 7-1. La présence d'un cercle dans une cellule indique que cette menace existe pour l'entité considérée.

Tableau 7-1 – Relations entre les menaces relatives à la sécurité et le réseau domestique

Entités	Divulgation		Modification/ insertion		Interruption	Accès non autorisé	Répudiation
	Données stockées	Données transmises	Données stockées	Données transmises			
Récepteur		○		○	○		
Source DER		○		○	○	○	○
Borne de recharge de véhicule électrique		○		○	○		○
Système HEMS	○	○	○	○	○	○	○
Système CED	○	○	○	○	○	○	○
Interface ESI					○	○	
Communication		○		○	○		

8 Exigences de sécurité des réseaux domestiques

Les paragraphes ci-après décrivent les exigences de sécurité de haut niveau du point de vue de quatre principaux aspects de sécurité, à savoir la disponibilité, la confidentialité, l'intégrité et la non-répudiation.

8.1 Disponibilité

La disponibilité garantit qu'il n'y a pas de déni d'accès autorisé aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications en raison d'événements ayant une incidence sur le réseau. En d'autres termes, si une entité d'un réseau HAN qui en a la permission souhaite obtenir des informations sur un autre dispositif, l'entité devrait pouvoir accéder à ce dispositif immédiatement.

Un réseau HAN dans un réseau électrique intelligent devrait contrôler l'utilisation des récepteurs ainsi que la production ou le stockage de l'électricité par les sources DER en fonction des demandes envoyées par les réseaux. Lorsque le fournisseur d'électricité estime qu'il y a un pic de la demande, une demande de réduction de la consommation ou un signal indiquant qu'un nouveau tarif est appliqué devrait être transmis au système HEMS ou CED, pour que celui-ci puisse gérer les besoins d'électricité des dispositifs du client. La demande peut être acceptée ou non en fonction des conditions définies par le client.

Pour ce scénario, il est avant tout impératif que le réseau soit disponible et que les entités HAN soient en état de fonctionner. Si le réseau HAN n'est pas disponible lorsque la demande atteint son pic, il est possible que le système HEMS ne reçoive aucun signal du fournisseur d'électricité, d'où un coût plus élevé pour le client.

8.2 Confidentialité

La confidentialité garantit que le contenu des données ne peut être lu par des entités non autorisées. Même dans des cas où une partie des données a été interceptée dans le cadre d'écoutes clandestines des communications hertziennes, leur confidentialité peut être garantie, à moins que l'auteur de l'attaque ne puisse pas les divulguer.

La confidentialité doit être assurée pour les entités et les données de communication sensibles, qu'elles soient stockées ou transmises. Les données sensibles dans un réseau HAN sont les informations sur les relevés de consommation électrique, les messages de commande contrôlant le fonctionnement des récepteurs et des sources DER, les signaux relatifs à la tarification ou les demandes d'ajustement en fonction de la demande envoyés par le fournisseur d'électricité et les informations d'identification personnelle stockées dans le système CED.

8.3 Intégrité

L'intégrité garantit qu'après leur transfert, les données ne sont pas différentes de ce qu'elles étaient à la source. Récemment, la notion d'intégrité a été élargie pour s'appliquer à l'état du système ou du dispositif, qui ne doit pas avoir changé par rapport à la configuration de base. De même, les données originales stockées ne doivent pas avoir changé après une manipulation autorisée.

L'intégrité des informations de commande de contrôle et d'état transférées entre un système HEMS et d'autres entités, qui sont des récepteurs et des sources DER, doit être garantie. En outre, l'intégrité des données transmises depuis ou vers un système CED devrait être protégée. Par ailleurs, afin que le réseau soit en état de fonctionner, l'intégrité de la liste des programmes installés sur chaque dispositif HAN, ainsi que l'intégrité des programmes eux-mêmes, devraient être protégées.

8.4 Non-répudiation

La non-répudiation permet d'empêcher un individu ou une entité de nier avoir effectué telle ou telle action relative à des données en présentant la preuve numérique que cette action a bien eu lieu.

Dans un réseau HAN, les actions pouvant donner lieu à un conflit sont le contrôle des sources DER et des récepteurs, la réception des signaux de tarification et des demandes d'ajustement en fonction de la demande, ainsi que l'enregistrement du calendrier de consommation électrique via un système CED. Ainsi, les entités d'un réseau HAN ayant un lien avec ces actions devraient satisfaire l'exigence de non-répudiation. Toutefois, dans le cas des récepteurs, il se peut que la non-répudiation ne puisse être garantie en raison de leurs caractéristiques. Par exemple, une prise intelligente est un dispositif soumis à des contraintes qui ne dispose pas d'une mémoire et d'une puissance de calcul suffisantes.

8.5 Relations entre les exigences de sécurité et le réseau domestique

Les relations entre les exigences de sécurité et les menaces sont présentées dans le Tableau 8-1. La présence d'un cercle dans une cellule indique que cette exigence de sécurité devrait être respectée pour supprimer ou atténuer la menace considérée.

Tableau 8-1 – Relations entre les exigences de sécurité et les menaces

			Menaces relatives à la sécurité						
			Divulgation		Modification/ insertion		Interruption	Accès non autorisé	Répudiation
			Données stockées	Données transmises	Données stockées	Données transmises			
Exigences de sécurité	Confidentialité	Données stockées	○						
		Données transmises		○					
	Intégrité	Données stockées			○			○	
		Données transmises				○		○	
	Disponibilité						○		
	Non-répudiation								○

Etant donné que les menaces pour chaque entité d'un réseau HAN sont données dans le Tableau 7-1 et que les exigences pour chaque menace sont données dans le Tableau 8-1, les exigences de sécurité pour chaque entité d'un réseau HAN peuvent être établies en corrélant ces deux tableaux. Le Tableau 8-2 montre les exigences de sécurité à respecter pour les différentes entités d'un réseau HAN. La présence d'un cercle dans une cellule indique que cette exigence de sécurité devrait être respectée par l'entité pour supprimer ou atténuer la menace considérée.

Tableau 8-2 – Exigences de sécurité à respecter pour les différentes entités d'un réseau domestique

		Exigences de sécurité					
		Disponibilité	Confidentialité		Intégrité		Non-répudiation
			Données stockées	Données transmises	Données stockées	Données transmises	
Entités	Récepteur	○		○		○	
	Source DER	○		○		○	○
	Borne de recharge de véhicule électrique	○		○		○	○
	Système CED	○	○	○	○	○	○
	Système HEMS	○	○	○	○	○	○
	Interface ESI	○				○	
	Communication	○		○		○	

9 Relations entre les exigences de sécurité et les fonctions de sécurité

Pour répondre aux exigences de sécurité d'un réseau HAN et de ses dispositifs, il convient d'appliquer des fonctions de sécurité, par exemple: chiffrement ou déchiffrement, signature numérique, authentification des messages, authentification des entités, autorisation, contrôle d'accès, mesures de prévention des attaques par déni de service, audit et sécurité physique. Le Tableau 9-1 montre comment répondre aux exigences de sécurité grâce à des fonctions de sécurité. La présence d'un cercle dans une cellule indique que la fonction de sécurité en question peut être adoptée pour répondre à l'exigence de sécurité considérée. Il est à noter que chaque fonction de sécurité apparaissant dans le Tableau 9-1 est décrite dans la section 10.

Tableau 9-1 – Relations entre les exigences de sécurité et les fonctions de sécurité

			Fonctions de sécurité							
			Chiffr./ Déchiffr.	**Signature num.**	**Authentification**		**Contrôle d'accès**	**Anti-DoS**	**Audit**	**Sécurité physique**
					Msg.	**Entité**				
Exigences de sécurité	Confidentialité	Données stockées	○							
		Données transmises	○							
	Intégrité	Données stockées		○	○		○			
		Données transmises		○	○		○			
	Disponibilité					○		○	○	○
	Non-répudiation			○					○	○

10 Lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques dans les systèmes des réseaux électriques intelligents

10.1 Fonctions de sécurité pour les récepteurs

Le Tableau 10-1 donne les fonctions de sécurité pour les récepteurs dans un réseau HAN. Il indique les fonctions de sécurité correspondant à chaque exigence de sécurité et décrit les capacités nécessaires pour mettre en œuvre ces fonctions de sécurité.

Tableau 10-1 –Fonctions de sécurité pour les récepteurs dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Disponibilité	Mesures anti-DoS	Des capacités de détection et d'atténuation des attaques DoS devraient être envisagées.
	Sécurité physique	Des capacités permettant d'empêcher l'accès physique sans autorisation devraient être envisagées afin que les utilisateurs non autorisés ne puissent pas manipuler ou configurer les récepteurs.
Intégrité	Authentification des messages	Des capacités permettant de générer et de vérifier des données d'intégrité cryptographique devraient être envisagées afin de garantir l'intégrité des messages de rapport et de commande de contrôle. Les données d'intégrité cryptographique peuvent être générées par un mécanisme utilisant un code d'identification de message par hachage (HMAC).
Confidentialité	Chiffrement ou déchiffrement	Des capacités permettant de déchiffrer le message de commande chiffré envoyé par le système HEMS devraient être envisagées.

10.2 Fonctions de sécurité pour les sources d'électricité décentralisées

Le Tableau 10-2 donne les fonctions de sécurité pour les sources DER dans un réseau HAN. Il indique les fonctions de sécurité correspondant à chaque exigence de sécurité et décrit les capacités nécessaires pour mettre en œuvre ces fonctions de sécurité.

Tableau 10-2 – Fonctions de sécurité pour les sources d'électricité décentralisées dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Disponibilité	Mesures anti-DoS	Des capacités de détection et d'atténuation des attaques DoS devraient être envisagées.
	Sécurité physique	Des capacités permettant d'empêcher l'accès physique sans autorisation devraient être envisagées afin que les utilisateurs non autorisés ne puissent pas manipuler ou configurer les sources DER.
Intégrité	Authentification des messages	Des capacités permettant de générer et de vérifier des données d'intégrité cryptographique devraient être envisagées afin de garantir l'intégrité des messages de rapport et de commande. Les données d'intégrité cryptographique peuvent être générées par un mécanisme HMAC ou par un mécanisme utilisant la signature numérique.
	Authentification des entités	• Des capacités permettant d'authentifier les terminaux distants, qui envoient les messages de commande de contrôle, devraient être envisagées. La vérification d'un justificatif chiffré ou d'un certificat peut être envisagée comme méthode d'authentification. • Des capacités permettant d'authentifier les utilisateurs essayant de configurer ou de manipuler les sources DER devraient être envisagées. La vérification par mot de passe est une solution courante d'authentification des utilisateurs. Il est également possible de faire appel à des méthodes biométriques, par exemple la vérification d'empreintes.
	Contrôle d'accès	Des capacités permettant de faire en sorte que seuls des utilisateurs autorisés puissent modifier la configuration d'une source DER et la manipuler devraient être envisagées.

Tableau 10-2 – Fonctions de sécurité pour les sources d'électricité décentralisées dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Confidentialité	Chiffrement ou déchiffrement	Des capacités permettant de déchiffrer le message de commande chiffré envoyé par le système HEMS devraient être envisagées.
Non-répudiation	Signature numérique	Des capacités de vérification de la signature numérique figurant dans un métissage de commande de contrôle devraient être envisagées.
	Audit	Des capacités permettant de créer et de tenir à jour des enregistrements d'audit devraient être envisagées afin de garantir la transparence. La recharge et le déchargement du système ESS peuvent être des actions importantes qu'il convient d'enregistrer.

10.3 Fonctions de sécurité pour les bornes de recharge des véhicules électriques

Le Tableau 10-3 donne les fonctions de sécurité pour les bornes de recharge des véhicules électriques dans un réseau HAN. Il indique les fonctions de sécurité correspondant à chaque exigence de sécurité et décrit les capacités nécessaires pour mettre en œuvre ces fonctions de sécurité.

Tableau 10-3 – Fonctions de sécurité pour les bornes de recharge des véhicules électriques dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Disponibilité	Mesures anti-DoS	Des capacités de détection et d'atténuation des attaques DoS devraient être envisagées.
	Sécurité physique	Des capacités permettant d'empêcher l'accès physique sans autorisation devraient être envisagées afin que les utilisateurs non autorisés ne puissent pas manipuler ou configurer les bornes de recharge.
Intégrité	Authentification des messages	Des capacités permettant de générer et de vérifier des données d'intégrité cryptographique devraient être envisagées afin de garantir l'intégrité des messages de rapport et de contrôle. Les données d'intégrité cryptographique peuvent être générées par un mécanisme HMAC ou par un mécanisme utilisant la signature numérique.
	Authentification des entités	• Des capacités permettant d'authentifier les terminaux distants, qui envoient les messages de commande de contrôle, devraient être envisagées. La vérification d'un justificatif chiffré ou d'un certificat peut être envisagée comme méthode d'authentification. • Des capacités permettant d'authentifier les utilisateurs essayant de configurer ou d'utiliser les bornes de recharge devraient être envisagées. La vérification par mot de passe est une solution courante pour l'authentification des utilisateurs. Il est également possible de faire appel à des méthodes biométriques, par exemple la vérification d'empreintes.
	Contrôle d'accès	Des capacités permettant de faire en sorte que seuls des utilisateurs autorisés puissent modifier la configuration de la borne de recharge ou la manipuler devraient être envisagées.
Confidentialité	Chiffrement ou déchiffrement	Des capacités permettant de déchiffrer les messages de commande chiffrés envoyés par le système HEMS devraient être envisagées.

Tableau 10-3 – Fonctions de sécurité pour les bornes de recharge des véhicules électriques dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Non-répudiation	Signature numérique	Des capacités de vérification de la signature numérique figurant dans un message de commande de contrôle devraient être envisagées.
	Audit	Des capacités permettant de créer et de tenir à jour des enregistrements d'audit devraient être envisagées afin de garantir la transparence. Le lancement et l'arrêt de l'opération de recharge peuvent être des actions importantes qu'il convient d'enregistrer.

10.4 Fonctions de sécurité pour les systèmes d'affichage de l'énergie du client

Le Tableau 10-4 donne les fonctions de sécurité pour les systèmes CED dans un réseau HAN. Il indique les fonctions de sécurité correspondant à chaque exigence de sécurité et décrit les capacités nécessaires pour mettre en œuvre ces fonctions de sécurité.

Tableau 10-4 – Fonctions de sécurité pour les systèmes d'affichage de l'énergie du client dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Disponibilité	Sécurité physique	Des capacités permettant d'empêcher l'accès physique sans autorisation devraient être envisagées afin que les utilisateurs non autorisés ne puissent pas utiliser les systèmes CED.
Intégrité	Authentification des messages	Des capacités permettant de générer et de vérifier des données d'intégrité cryptographique devraient être envisagées afin de garantir l'intégrité des informations d'état venant d'un système HEMS et des messages de commande de contrôle envoyés à un système HEMS. Les données d'intégrité cryptographique peuvent être générées par un mécanisme HMAC ou par un mécanisme utilisant la signature numérique.
	Authentification des entités	• Des capacités permettant d'authentifier un système HEMS devraient être envisagées. La vérification d'un certificat peut être envisagée comme méthode d'authentification. • Des capacités permettant d'authentifier les utilisateurs essayant d'utiliser les systèmes CED devraient être envisagées. La vérification par mot de passe est une solution courante pour l'authentification des utilisateurs. Il est également possible de faire appel à des méthodes biométriques, par exemple la vérification d'empreintes.
	Contrôle d'accès	Des capacités permettant de faire en sorte que seuls des utilisateurs autorisés puissent modifier la configuration d'un système CED ou utiliser ses fonctions devraient être envisagées.
	Intégrité des applications	Des capacités permettant de garantir l'intégrité des applications devraient être envisagées afin de repérer les applications infectées par des logiciels malveillants ou modifiées par l'auteur d'une attaque. Les fichiers exécutables ou les bibliothèques peuvent être modifiés ou supprimés de manière intentionnelle par l'auteur d'une attaque, entraînant une instabilité de l'application. Grâce à ces capacités, les dispositifs HAN peuvent déterminer si l'application est modifiée. L'une des méthodes pour mettre en œuvre cette capacité peut consister à

Tableau 10-4 – Fonctions de sécurité pour les systèmes d'affichage de l'énergie du client dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
		vérifier le code d'intégrité cryptographique de l'application, qui est généré lors de l'installation ou de la mise à jour de cette application.
Confidentialité	Chiffrement ou déchiffrement	Des capacités permettant de chiffrer ou de déchiffrer les messages en provenance ou à destination d'un système HEMS devraient être envisagées afin de protéger les messages de commande et les messages comprenant des informations d'identification personnelle. Des capacités permettant de chiffrer ou de déchiffrer les données stockées dans un système CED devraient être envisagées afin de protéger les informations d'identification personnelle contenues dans le système CED.
Non-répudiation	Signature numérique	Des capacités de vérification de la signature numérique figurant dans un message de commande de contrôle devraient être envisagées.
	Audit	Des capacités permettant de créer et de tenir à jour des enregistrements d'audit devraient être envisagées afin de garantir la transparence.

10.5 Fonctions de sécurité pour un système domestique de gestion de l'énergie

Le Tableau 10-5 donne les fonctions de sécurité pour un système HEMS dans un réseau HAN. Il indique les fonctions de sécurité correspondant à chaque exigence de sécurité et décrit les capacités nécessaires pour mettre en œuvre ces fonctions de sécurité.

Tableau 10-5 – Fonctions de sécurité pour un système domestique de gestion de l'énergie dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Disponibilité	Mesures anti-DoS	Des capacités de détection et d'atténuation des attaques DoS devraient être envisagées. En particulier, un service utilisé par les clients pour commander les récepteurs et les sources DER devrait être protégé contre ce type d'attaque.
	Sécurité physique	Des capacités permettant d'empêcher l'accès physique sans autorisation devraient être envisagées afin que les utilisateurs non autorisés ne puissent pas utiliser un système HEMS.
Intégrité	Authentification des messages	Des capacités permettant de générer et de vérifier des données d'intégrité cryptographique devraient être envisagées afin de garantir l'intégrité des informations d'état venant d'autres dispositifs (récepteurs, sources DER et bornes de recharge des véhicules électriques) et des messages de commande de contrôle envoyés aux autres dispositifs (récepteurs, sources DER et bornes de recharge des véhicules électriques). Les données d'intégrité cryptographique peuvent être générées par un mécanisme HMAC ou par un mécanisme utilisant la signature numérique.
	Authentification des entités	• Des capacités permettant d'authentifier les terminaux distants devraient être envisagées. La vérification d'un certificat peut être envisagée comme méthode d'authentification. Pour les récepteurs ayant une faible puissance de calcul, l'authentification peut être assurée moyennant la vérification d'un justificatif généré à partir d'un secret prépartagé.

Tableau 10-5 – Fonctions de sécurité pour un système domestique de gestion de l'énergie dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
		• Des capacités permettant d'authentifier les utilisateurs essayant d'utiliser un système HEMS devraient être envisagées. La vérification par mot de passe est une solution courante pour l'authentification des utilisateurs. Il est également possible de faire appel à des méthodes biométriques ou à un code de réponse rapide.
	Contrôle d'accès	Des capacités permettant de faire en sorte que seuls des utilisateurs autorisés puissent modifier la configuration d'un système HEMS ou utiliser ses fonctions devraient être envisagées. Les comptes des administrateurs et des utilisateurs généraux devraient être séparés. Il convient de créer et d'utiliser des comptes séparés pour les différents objectifs, afin que l'auteur d'une attaque ait un accès limité aux informations sensibles, aux fonctions et aux autres comptes si un compte est compromis.
	Intégrité des applications	Des capacités permettant de garantir l'intégrité des applications devraient être envisagées afin de repérer les applications infectées par des logiciels malveillants ou modifiées par l'auteur d'une attaque. Les fichiers exécutables ou les bibliothèques peuvent être modifiés ou supprimés de manière intentionnelle par l'auteur d'une attaque, entraînant une instabilité de l'application. Grâce à ces capacités, les dispositifs HAN peuvent déterminer si l'application est modifiée. L'une des méthodes pour mettre en œuvre cette capacité peut consister à vérifier le code d'intégrité cryptographique de l'application, qui est généré lors de l'installation ou de la mise à jour de cette application.
Confidentialité	Chiffrement ou déchiffrement	• Des capacités permettant de chiffrer ou de déchiffrer les messages en provenance ou à destination d'une autre entité dans un réseau HAN devraient être envisagées afin de protéger les messages de commande de contrôle et les messages comprenant des informations d'identification personnelle. • Des capacités permettant de chiffrer ou de déchiffrer les données stockées dans un système HEMS devraient être envisagées afin de protéger les informations d'identification personnelle contenues dans un système HEMS si besoin est.
Non-répudiation	Signature numérique	Des capacités de vérification de la signature numérique figurant dans un message de commande de contrôle devraient être envisagées.
	Audit	Des capacités permettant de créer et de tenir à jour des enregistrements d'audit devraient être envisagées afin de garantir la transparence.

10.6 Fonctions de sécurité pour une interface de services d'énergie

Le Tableau 10-6 donne les fonctions de sécurité pour une interface ESI dans un réseau HAN. Il indique les fonctions de sécurité correspondant à chaque exigence de sécurité et décrit les capacités nécessaires pour mettre en œuvre ces fonctions de sécurité.

Tableau 10-6 – Fonctions de sécurité pour l'interface de services d'énergie dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Disponibilité	Sécurité physique	Des capacités permettant d'empêcher l'accès physique sans autorisation sont envisagées afin que les utilisateurs non autorisés ne puissent pas utiliser l'interface ESI.
Intégrité	Contrôle d'accès	• Des capacités permettant de faire en sorte que seuls les dispositifs locaux autorisés puissent accéder au réseau HAN devraient être envisagées. Pour les points d'accès WiFi, un accès protégé WiFi (WPA) de type II devrait être mis en œuvre, avec des mots de passe complexes afin d'éviter les attaques consistant à deviner les mots de passe. En outre, la fonction de transmission de l'identificateur (ID) d'ensemble de services devrait être désactivée. Pour les point d'accès Zigbee ou Bluetooth, toutes les fonctionnalités de sécurité prévues dans la spécification de chaque protocole devraient être appliquées pour satisfaire aux exigences de sécurité. • Des capacités de blocage du trafic non autorisé sur la base d'ID uniques devraient être envisagées. L'adresse de commande d'accès au support (MAC) ou l'adresse IP (protocole IP) du dispositif peut être utilisée comme ID unique.
	Intégrité des applications	Des capacités permettant de garantir l'intégrité des applications devraient être envisagées afin de repérer les applications infectées par des logiciels malveillants ou modifiées par l'auteur d'une attaque. Les fichiers exécutables ou les bibliothèques peuvent être modifiés ou supprimés de manière intentionnelle par l'auteur d'une attaque, entraînant une instabilité de l'application. Grâce à ces capacités, les dispositifs HAN peuvent déterminer si l'application est modifiée. L'une des méthodes pour mettre en œuvre cette capacité peut consister à vérifier le code d'intégrité cryptographique de l'application, qui est généré lors de l'installation ou de la mise à jour de cette application.

10.7 Fonctions de sécurité pour les communications

Le Tableau 10-7 donne les fonctions de sécurité pour les communications dans un réseau HAN. Il indique les fonctions de sécurité correspondant à chaque exigence de sécurité et décrit les capacités nécessaires pour mettre en œuvre ces fonctions de sécurité.

Tableau 10-7 – Fonctions de sécurité pour les communications dans un réseau domestique

Exigences de sécurité	Fonctions de sécurité	Description
Disponibilité	Mesures anti-DoS	Des capacités de détection et d'atténuation des attaques DoS devraient être envisagées.
Intégrité	Authentification des messages/ entités	Des capacités d'authentification mutuelle des entités de communication et des messages devraient être envisagées afin de garantir l'intégrité des données de communication. La mise en œuvre de la sécurité dans la couche transport (TLS) ou de la sécurité dans la couche transport en mode datagramme (DTLS) à l'aide de certificats peut être une solution adaptée. Un algorithme de chiffrement sécurisé devrait être choisi pour la sécurité TLS ou DTLS.
	Contrôle d'accès	• Des capacités permettant de faire en sorte que seuls les dispositifs locaux autorisés puissent accéder au réseau HAN devraient être envisagées. • Des capacités de blocage du trafic non autorisé sur la base d'ID uniques devraient être envisagées. L'adresse MAC ou l'adresse IP du dispositif peut être utilisée comme ID unique.
Confidentialité	Chiffrement ou déchiffrement	Des capacités permettant de chiffrer ou de déchiffrer les données stockées dans un système HEMS devraient être envisagées afin de protéger les informations d'identification personnelle contenues dans un système HEMS si besoin est.

Bibliographie

[b-UIT-T G.9959] Recommandation UIT-T G.9959 (2015), Emetteurs-récepteurs de radiocommunication numériques à bande étroite à courte portée – Spécifications des couches PHY, MAC, AR et LLC.

[b-UIT-T L.1430] Recommandation UIT-T L.1430 (2013), *Méthodologie d'évaluation de l'incidence environnementale des projets relatifs aux gaz à effet de serre et à la consommation d'énergie utilisant les technologies de l'information et de la communication*.

[b-UIT-T Y.2071] Recommandation UIT-T Y.2071 (2015), *Cadre applicable aux micro-réseaux électriques*.

[b-UIT-T Y.4409] Recommandation UIT-T Y.4409/Y.2070 (2015), *Exigences et architecture du système domestique de gestion de l'énergie et des services de réseau domestique*.

[b-UIT-T Smart-O-33] Groupe spécialisé de l'UIT-T sur les réseaux électriques intelligents: Smart-O-33Rev.6 (2011), *Architecture des réseaux électriques intelligents*; http://www.itu.int/en/ITU-T/focusgroups/smart/Documents/smart-o-0033r6_architecture_deliverable.doc

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changements climatiques, déchets d'équipements électriques et électroniques, efficacité énergétique, construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2018