Recommandation de la branche pour le marché suisse de l'électricité

Directives pour la sécurité des données des systèmes de mesure intelligents, annexe 1

Exigences de certification envers les systèmes de mesure intelligents pour la sécurité des données

RL-DSP – CH, annexe 1, Édition 2018

Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Téléphone +41 62 825 25 25, Fax +41 62 825 25 26, info@electricite.ch, www.electricite.ch

Impressum et contact

Éditeur
Association des entreprises électriques suisses AES
Hintere Bahnhofstrasse 10, case postale
CH-5001 Aarau
Téléphone +41 62 825 25 25
Fax +41 62 825 25 26
info@electricite.ch
www.electricite.ch

Auteurs de la première édition
Conformément au document principal

Imprimé n° 1045 / f, édition 2018

Sommaire

Liste des figures

1. Champ d'application

(1) Le document «Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse», OFEN, 11/2014, souvent aussi appelé «Exigences minimales», définit l'architecture d'un système de mesure intelligent (figure 1).

(2) Cette définition est formulée dans l'ordonnance sur l'approvisionnement en électricité (OApEl), modification du 1er novembre 2017, [6], art. 8a, al. 1:

> Pour les systèmes de mesure et les processus d'information, il convient d'utiliser des systèmes de mesure intelligents installés chez les consommateurs finaux et les producteurs. Ces systèmes comportent les éléments suivants:
>
> a. un compteur électrique électronique installé chez le consommateur final ou le producteur, qui:
>   1. enregistre l'énergie active et l'énergie réactive,
>   2. calcule les courbes de charge sur une période de quinze minutes et les enregistre pendant au moins soixante jours,
>   3. dispose d'interfaces, dont une est réservée à la communication bidirectionnelle avec un système de traitement des données et une autre permet au minimum au consommateur final ou au producteur de lire les valeurs de mesure lors de leur saisie et de consulter les courbes de charge visées au ch. 2, et
>   4. enregistre et consigne les interruptions de l'approvisionnement en électricité;
> b. un système de communication numérique garantissant la transmission automatique des données entre le compteur électrique et le système de traitement des données; et
>
> c. un système de traitement de données qui permet de consulter les données.

(3) Les définitions recouvrent l'appareil de mesure intelligent (art. 8a, al. 1, let. a), un système de communication (concentrateur de données ou passerelle) (art. 8a, al. 1, let. b) et un système de tête de réseau (art. 8a, al. 1, let. c).

(4) De plus, dans certaines circonstances, des composants pertinents pour la sécurité des données doivent être pris en compte pour le système global.

- Visualisation
  - localement sur l'AMI (art. 8a, al.1, let. a, 3.) en tant qu'interface
  - à distance en tant que plateforme de visualisation
- Système de gestion pour la clé cryptographique, etc. comme ancrage de sécurité central d'un SMI

(5) En conséquence, différents objets de vérification résultent de ces définitions pour un contrôle de sécurité des données, conformément à l'art. 8b. Les objectifs pour un contrôle de sécurité des données des éléments utilisés dans le cadre d'un SMI sont traitées (désignés «Composants principaux» dans [2] et dans ce document):

1 Seuls les systèmes de mesure intelligents dont les éléments ont été contrôlés avec succès pour s'assurer de la garantie de la sécurité des données peuvent être utilisés.

2 Les gestionnaires de réseau et fabricants adoptent, pour ce contrôle, sur la base d'une analyse des besoins de protection de l'OFEN, des directives qui déterminent les éléments à contrôler, les exigences les concernant et le type et le mode de contrôle.

3 Le contrôle est réalisé par l'institut fédéral de métrologie. Celui-ci peut confier à des tiers l'exécution de cette mission ou des parties de celle-ci.

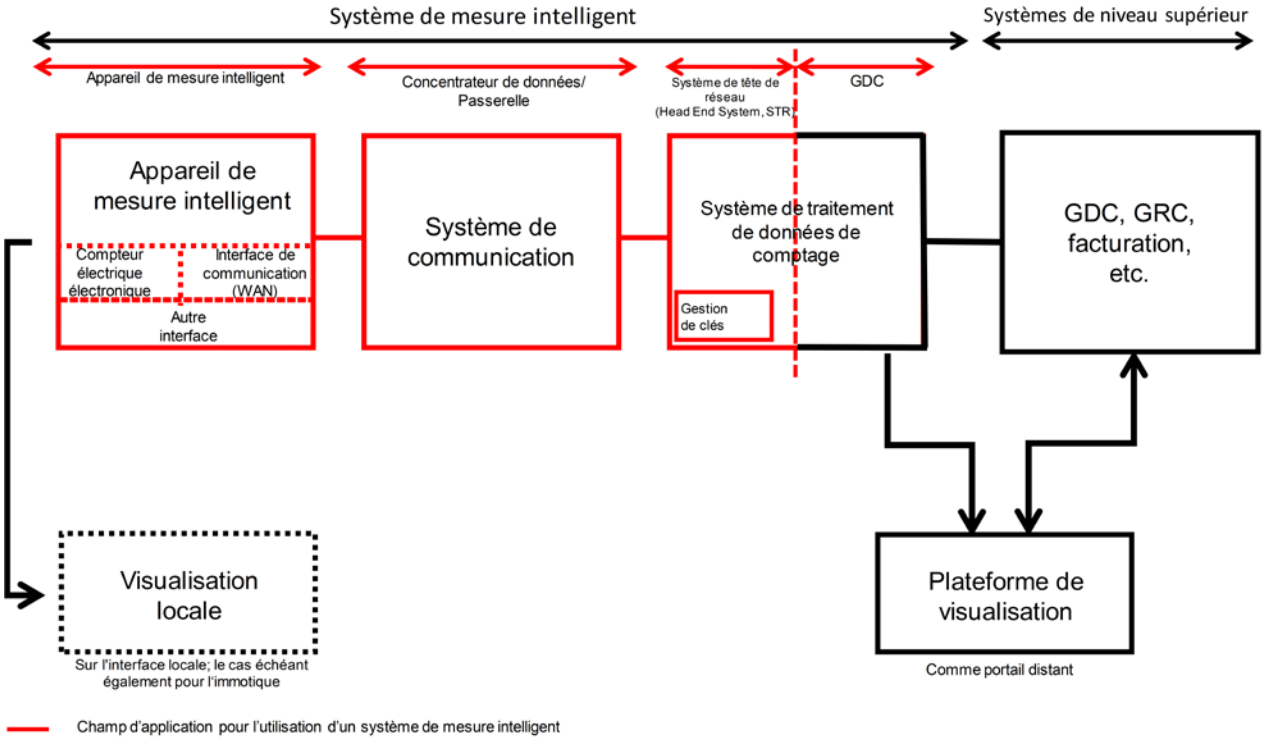

Figure 1: Systèmes et domaines pertinents

(6) Objets de vérification du contrôle de la sécurité des données:
Profils d'exigences génériques pour l'architecture et la fonctionnalité:

- Appareil de mesure intelligent: AMI
- Système de communication: concentrateur de données ou passerelle
- Système de tête de réseau

Profils d'exigences non génériques sur la base de solutions spécifiques au fabricant:

- Gestion de clés
- Plateformes de visualisation

(7) Pour le système complet représenté à la figure 1, il convient de garantir que les exploitants des systèmes de smart metering non seulement recourent, pour la sécurité des données, à des composants

fiables, mais qu'ils disposent également de la qualification pour exploiter les systèmes correspondants dans leur environnement informatique de façon fiable. Cela nécessite généralement d'utiliser des systèmes de gestion de la sécurité des informations (SGSI) correspondants, et est largement garanti par le recours à des systèmes informatiques sécurisés. En font notamment partie les processus suivants:

- Les responsabilités de gestion sont définies et mises en œuvre.
- Les directives de sécurité (Security Policies) sont mises en place et appliquées.
- Sécurité des informations et gestion du personnel: les mutations sont prises en compte.
- Le savoir-faire et la qualification sont d'un niveau suffisant et mis à jour grâce à une formation continue régulière.
- Le niveau suffisant de la sécurité des données est défini, mis en place et adapté en permanence.
- Les accès et droits d'accès sont structurés et gérés dans les meilleurs délais.

(8) Sont notamment compris les systèmes qui ne sont pas soumis à un contrôle de sécurité des données spécifique, ainsi que l'utilisation conforme aux spécifications des composants contrôlés:

- Systèmes de niveau supérieur de la gestion des données énergétiques
- L'ensemble du système de traitement des données de comptage (STDC) dont les objets de vérification ne constituent qu'une partie
- Composants de visualisation à distance, p. ex. basés sur le web
- Composants de visualisation laissés aux consommateurs finaux pour l'utilisation locale
- Utilisation du SMI

(9) À cet effet, un système de gestion doit être mis en place par les exploitants correspondants:

- Justification du fonctionnement sécurisé des composants principaux contrôlés (SMI)
- Justification du fonctionnement sécurisé du système de gestion de clés
- Justification du fonctionnement sécurisé du STDC
- Justification de la visualisation sécurisée
  - à distance
  - locale, UNIQUEMENT SI l'exploitant met à disposition des clients finaux un appareil de visualisation
- Justification du fonctionnement sécurisé des systèmes de niveau supérieur

(10) Le fabricant du STDC s'engage à consigner de manière suffisante la délimitation des objets de vérification «Système de tête de réseau» et «Gestion de clés».

1.1 Bases

a) Utilisation des annexes du document «Directives pour la sécurité des données des SMI»

(1) L'annexe 1 «Exigences de certification envers les systèmes de mesure intelligents pour la sécurité des données» contient les exigences relatives aux composants principaux du SMI et donc indirectement aux fabricants de ces derniers. Les exigences sont mises en œuvre dans l'architecture et la fonctionnalité des composants principaux, l'exactitude et l'efficacité sont justifiées par un contrôle de sécurité des données.

(2) L’annexe 2 «Exigences opérationnelles envers les systèmes de mesure intelligents pour la sécurité des données» contient les exigences concernant les exploitants du SMI.

b) Composants principaux

(1) Les fonctionnalités des composants principaux agissent contre les dangers des objets vulnérables issus de l’analyse des besoins de protection.

(2) Les composants principaux répondent aux exigences de procédure des exploitants dans le document exploitant.

c) Aspects complémentaires

(1) La gestion de clés en guise de sous-système du STDC est également contrôlée pour vérifier que les exigences formulées dans le document fabricant sont respectées.

(2) Le fabricant d’un STDC permet le transfert crypté sans canal de retour de données clients vers une plateforme de visualisation à distance, si son produit supporte cette fonction.

(3) Le respect des exigences en matière de sécurité des données et de protection des données doit être garanti par l’exploitant de la plateforme de visualisation à distance. Si la plateforme de visualisation à distance présente un trafic des données bidirectionnel avec l’un des «systèmes de niveau supérieur», le respect des exigences en matière de sécurité et de protection des données doit être garanti par les exploitants des deux systèmes.

(4) L’éditeur d’un appareil permettant la visualisation locale doit garantir à ses clients finaux le respect des exigences en matière de sécurité des données et de protection des données.

2. Description générique des composants principaux du système de mesure intelligent

(1) Les représentations suivantes utilisent des modules génériques logiques qui permettent de localiser les propriétés de sécurité et ne donnent aucune indication de construction aux fabricants.

(2) Si un composant principal (CP) contient des objets vulnérables, ceux-ci doivent être sécurisés en conséquence. Si un composant principal ne contient pas d'objet vulnérable, le module correspondant n'est pas nécessaire.

2.1 L'appareil de mesure intelligent (AMI)

2.1.1 L'AMI dans la configuration de base, comme système individuel

(1) L'AMI comprend plusieurs parties délimitables sur le plan fonctionnel, qui se composent du matériel informatique et du logiciel (figure 2). Sur le plan de la sécurité des données, leur interaction peut être représentée par la description modulaire de certaines fonctions, liens de communication, interfaces, sujets, objets et rôles. Par conséquent, le composant principal «appareil de mesure intelligent» est d'abord étudié en détail ci-après.

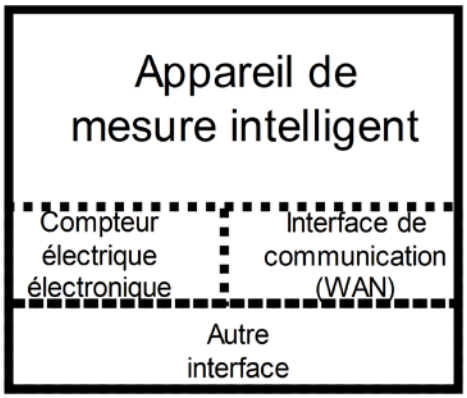

Figure 2: L'AMI en tant que composant principal du SMI

(2) L'AMI est en principe composé d'unités électromécaniques et électroniques (Figure 3). Il peut inclure un coupe-circuit qui coupe le courant entre le réseau électrique et le prosumer par un système à distance à partir d'instructions de contrôle envoyées. De même, des relais exécutant une fonction similaire à celle du récepteur de télécommande peuvent être montés. Évidemment, l'AMI contient, dans tous les cas, un compteur d'électricité et d'énergie vérifié. Il en résulte à cet effet des interfaces externes (IC0 à IC3) pour la communication avec des sujets en dehors de l'AMI et des interfaces internes pour la communication entre les composants partiels. Si un module de communication est insérable, les mêmes exigences s'appliquent par analogie à cet emplacement.

(3) Le micrologiciel de l'AMI comprend certains modules logiques auxquels sont attribuées certaines fonctionnalités pour la sécurité des données:

- interface externe: accès informatique logique au micrologiciel depuis l'extérieur de l'AMI
  - **IC3**: interface WAN pour le module de communication dans la tête de réseau ou dans un concentrateur de données ou une passerelle; en fonction de l'appareil: Ethernet, CPL, radio ou fibre optique, etc.
  - **IC0**: interface locale pour la configuration du système et la lecture du compteur
  - **IC2**: interface permettant de consulter les données de visualisation d'un prosumer
- interface interne: connexion aux autres systèmes montés dans l'AMI (compteur et le cas échéant un relais de disjoncteur ou un coupe-circuit, ou autres)
  - **Compteur:** compteur électronique d'électricité et d'énergie; partie métrologique de l'AMI
  - **Coupe-circuit** Relais de disjoncteur déclenché par un opérateur distant via l'AMI
  - **Relais** (au sens d'une télécommande centralisée)

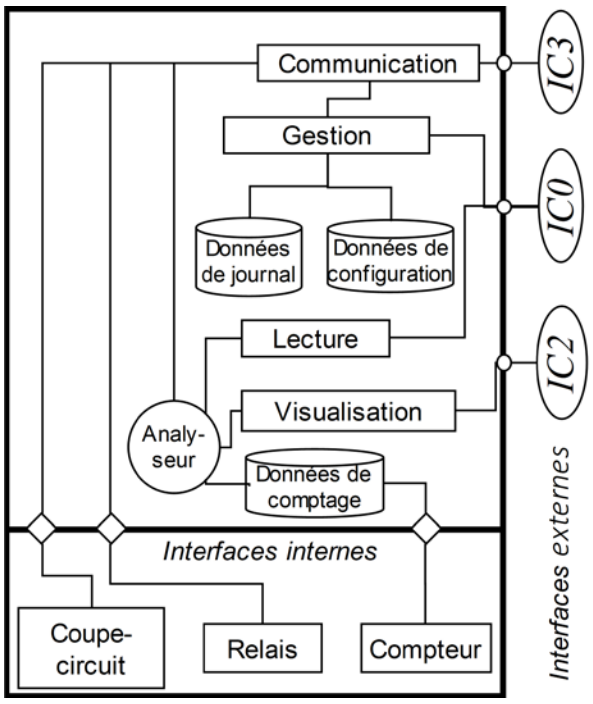

Figure 3: Architecture de base fonctionnelle de l'AMI

- Communication: module du micrologiciel qui commande la connexion des données par l'interface WAN (IC3) avec le système de tête de réseau.
- Gestion: module du micrologiciel qui commande la gestion des appareils de l'AMI par un administrateur local (via interface IC0) ou administrateur distant (via interface IC3)
  - Données de conf.: emplacement de stockage électronique des données de configuration
  - Données de journal: emplacement de stockage électronique des données de journal
- Lecture: module du micrologiciel qui commande la lecture locale du compteur sur place (via interface IC0)
- Visualisation: module du micrologiciel qui délivre localement des données de visualisation pour le prosumer (client final sans ou avec production d'électricité propre) via l'interface IC2 (lisible uniquement)
- Analyseur: module du micrologiciel qui prépare de manière adéquate les données de comptage pour la préparation aux interfaces correspondantes pour les rôles d'utilisateurs correspondants
- Données de comptage: emplacement de stockage électronique des données de comptage

2.1.2 L'AMI comme passerelle avec LMN

(1) Si d'autres compteurs doivent être raccordés à l'AMI et si les données de comptage doivent être transmises via son interface WAN IC3 à un système de tête de réseau, il doit disposer d'une autre interface externe IC1 au LMN (Local Metrological Network) (Figure 4).

(2) En principe, il conserve ses fonctions comme appareil de mesure intelligent, qui se limitent toutefois aux données de comptage du compteur monté. Les données de comptage des autres compteurs raccordés via l'IC1 et leurs données de configuration sont transmises uniquement à ces derniers ou transférées à une tête de réseau via l'interface IC3.

(3) En fonction de la technique de transmission utilisée dans le LMN, l'interface IC1 LMN peut supporter d'autres protocoles de communication que l'interface WAN IC3.
Les conditions marginales supplémentaires suivantes en résultent pour un AMI en tant que passerelle:

- Interface supplémentaire **IC1** pour le LMN
- Les données de comptage des appareils à l'interface **IC1** sont transmises par le module de communication uniquement via l'**IC3**, sans traitement des données dans l'AMI, mais avec conversion de protocole et cryptage, le cas échéant.
  - Si les données de comptage d'autres compteurs dans l'AMI sont stockées temporairement à d'autres fins, la gestion et le reconditionnement des espaces de stockage sont effectués.
  - Si les données de comptage de différents clients sont stockées temporairement, l'enregistrement est réalisé en mode multi-tenant (définition voir annexe)
- L'interface **IC1** prend en charge les protocoles de réseau de moindre portée.
- Si d'autres composants principaux dans le LMN utilisent cette interface, la communication est cryptée.

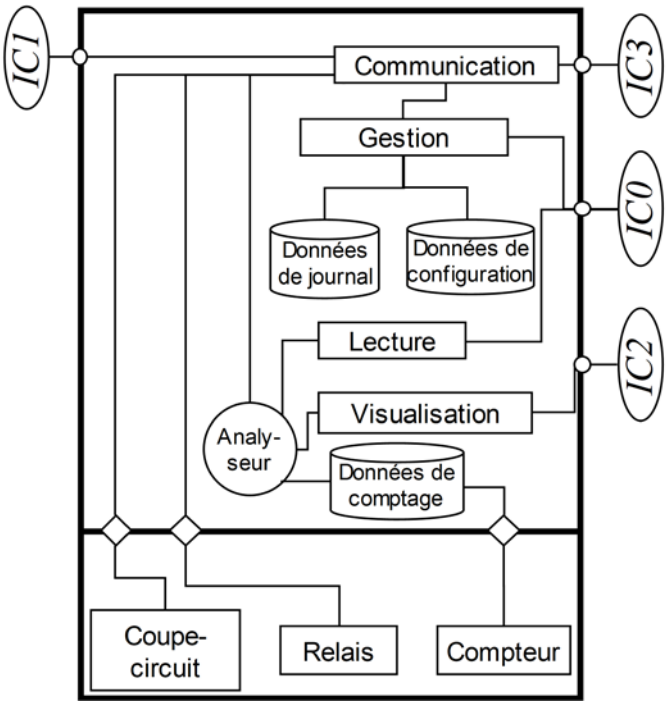

Figure 4: L'AMI comme passerelle avec un compteur propre

- Le module de communication isole le trafic des données depuis et vers les compteurs LMN de celui de son propre trafic, rapporté à ses données de comptage, données de configuration et utilisateur dans l'AMI.
- La lecture et la visualisation sont possibles uniquement pour les compteurs intégrés localement. Si l'AMI ne dispose pas de compteur propre, une série de modules internes est superflue, de sorte qu'il émerge une architecture simplifiée. Les exigences en matière de sécurité des données

relatives aux modules restants sont conservées.
Par conséquent, un profil d'exigences peut être déduit pour un concentrateur de données (CD) basé sur cette architecture ou pour une passerelle sans compteur.

(4) **Remarque:**
Pour les appareils de commutation de charge dédiés, les exigences figurant dans ce paragraphe s'appliquent, par analogie, à l'architecture des composants, aux fonctionnalités internes implémentées et aux interfaces externes.

2.2 Le système de communication

(1) Les composants principaux passerelle ou concentrateur de données en font partie. En fonction des modalités, ces composants transmettent uniquement les données de comptage de l'AMI raccordé au STR, ou permettent également un enregistrement local pour le traitement ultérieur. Les exigences de cette section s'appliquent donc uniquement aux fonctions mises en œuvre et ne concernent par conséquent pas l'ensemble des fonctions qui ne sont pas mises en œuvre.

2.2.1 La passerelle basée sur un AMI sans compteur propre

(1) Si une passerelle (Figure 5) traite, affiche et transmet exclusivement des données de comptage d'appareils LMN, son architecture logique correspond en principe à celle d'un AMI. Toutefois, certains des modules logiques correspondants doivent avoir des fonctionnalités partiellement étendues. Dans le cas où les données de comptage de différents clients sont traitées dans la même passerelle, les modules doivent être multi-tenant. Un composant de ce type est représenté dans la figure ci-dessous à titre d'exemple. Les conditions limites supplémentaires suivantes en résultent:

- Une architecture multi-tenant dans le cadre d'une exploitation pluripartite est garantie.
- Le module de communication sépare le trafic de données depuis et vers les compteurs LMN du trafic via l'IC3 selon le but (p. ex. données de configuration et accès utilisateur).
- Les données de comptage sont enregistrées en multi-tenant (voir section «Abréviations et définitions» en annexe).
- Si elles sont mises en œuvre, la visualisation et la lecture doivent être multi-tenant.
- Le transfert des données de comptage vers STR doit être multi-tenant.
- La fonction de l'analyseur doit être étendue à une fonctionnalité de filtre multi-tenant.

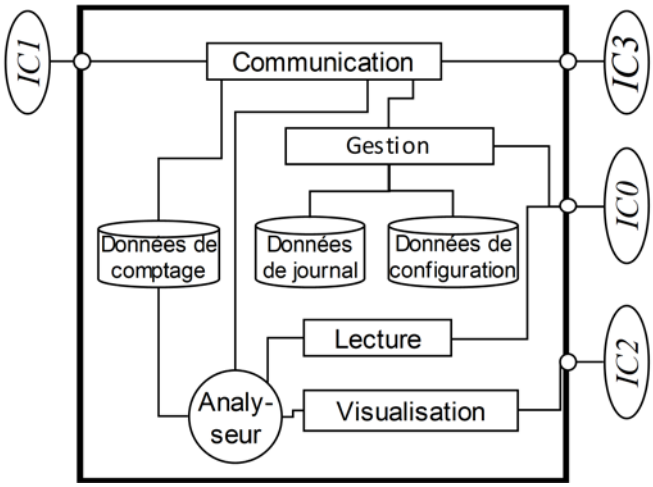

Figure 5: Passerelle sans compteur propre

2.2.2 La passerelle sans enregistrement des données de comptage

(1) Si une passerelle ne dispose pas d'un enregistrement local des données de comptage, les modules associés ne sont pas nécessaires (Figure 6). Des données de comptage à transférer peuvent être enregistrées provisoirement (données temp.).

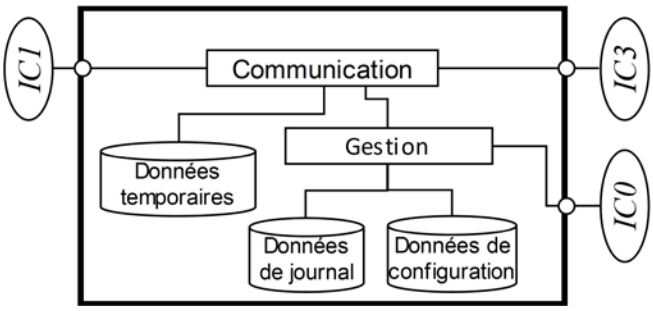

Figure 6: Passerelle sans enregistrement des données de comptage

2.2.3 Le concentrateur de données (CD)

(1) Le concentrateur de données est un composant principal du SMI comme système de communication (Figure 7). Il relie l'AMI et d'autres appareils avec le STR du gestionnaire de données. Il ne doit pas nécessairement être de conception identique ou dériver techniquement d'un AMI, mais les mêmes exigences s'appliquent par analogie pour les modules logiques spécifiés.

- Interfaces **IC0**, **IC1**, **IC3$_{CP}$** et **IC3$_{STR}$**
- Les données de comptage des appareils à l'interface **IC1** sont transmises au STR par le module de communication uniquement via l'**IC3$_{STR}$**, sans traitement des données dans le CD mais, le cas échéant, avec conversion de protocole et cryptage.
- L'interface **IC1** prend en charge les protocoles de réseau de moindre portée.
- L'interface **IC3$_{CP}$** prend en charge des protocoles de réseau de portée supérieure et est généralement reliée à plusieurs AMI (CP=composants principaux).
- Les données de comptage de l'AMI au niveau de l'interface **IC3$_{CP}$** sont transmises par le module de communication uniquement via l'**IC3$_{STR}$**, sans traitement des données dans le CD mais, le cas échéant, avec cryptage.

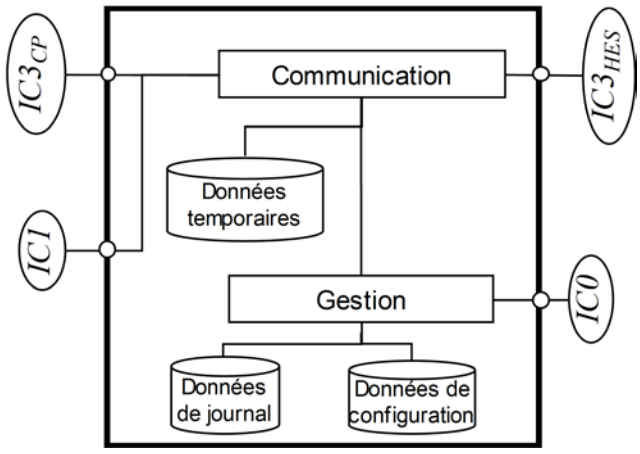

Figure 7: Le concentrateur de données

- Le CD peut enregistrer provisoirement des données de comptage à transférer (données temp.).
- Le module de communication sépare le trafic des données depuis et vers les compteurs LMN ou les composants principaux raccordés à l'**IC3$_{CP}$** du trafic via l'IC3 selon le but (p. ex. données de configuration et accès utilisateur).
- Le CD n'a pas d'interface locale pour la lecture ou la visualisation, mais pour l'administration locale (**IC0**).

2.3 Le système de tête de réseau (STR)

(1) Ce composant fait partie du composant principal du système de traitement des données de comptage (Figure 8). Il transmet les données de comptage au gestionnaire de données et permet aux administrateurs du système d'accéder à des composants principaux du SMI à distance. Pour cela, la tête de réseau dispose d'une interface WAN et d'interfaces locales correspondantes pour les rôles de ses utilisateurs. Quelle que soit la forme de ces interfaces (API, masques I&A, serveur Web, etc.), celles-ci remplissent les exigences de sécurité de façon adéquate et s'intègrent dans les processus de gestion de la sécurité des informations du gestionnaire de données. De la même manière que l'architecture logique des composants principaux, la tête de réseau comprend également des modules logiquement délimitables qui fournissent des fonctions spécifiques.

- **WAN**: interface avec un AMI ou un CD ou une passerelle; en fonction de l'appareil: Ethernet, CPL, radio ou fibre optique
- **Communication**: module du STR qui commande le transfert de données depuis et vers un AMI ou un CD
- **Gestion**: module du STR qui commande la gestion des appareils d'un AMI, d'un CD ou passerelle par un administrateur distant
- **Données de comptage**: module du STR qui transmet les données de mesure reçues par l'AMI au gestionnaire de données
- **Autres**: module de la tête de réseau qui prend en charge les fonctions spécifiques au fabricant, comme un technicien d'assistance d'un composant principal qui a accès aux composants principaux du SMI chez le gestionnaire de données
- **Interfaces locales**: interfaces fonctionnelles du système de tête de réseau qui sont utilisées par différents rôles ou différents systèmes chez le gestionnaire de données (accès utilisateur, transfert de données, API, etc.)

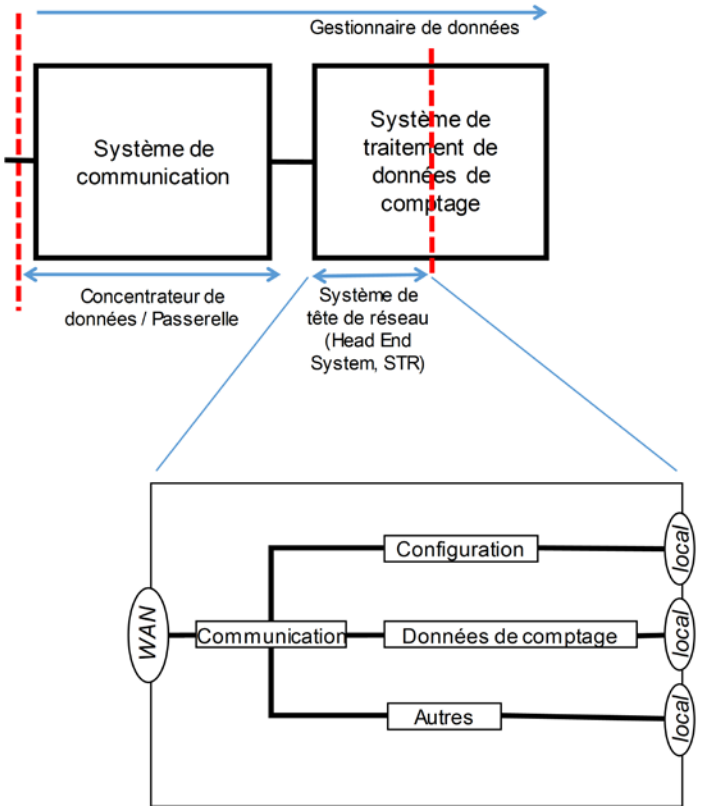

Figure 8: Le système de tête de réseau dans le domaine du gestionnaire de données

2.4 La plateforme de visualisation

(1) Ce composant principal permet la mise à disposition des données concernant la consommation d'énergie réelle, la production d'énergie réelle et d'informations concernant les tarifs pour les clients finaux.

(2) Toutefois, ces informations ne sont pas nécessairement mises à tout moment, dans leur ensemble, à la disposition des prosumers habilités à toutes les interfaces du SMI.

(3) Par conséquent, il convient de distinguer, pour ce composant principal, l'emplacement où il est utilisé et la nature des données qu'il rend accessibles au prosumer et au propriétaire des données.

(4) La distinction entre les sources de données repose au moins sur l'éventuelle granularité temporelle des données mises à disposition. Sur l'AMI, le prosumer peut accéder, en théorie, à ses données énergétiques actuelles, avant que l'AMI les enregistre ou les transmette de façon conjointe sur 15 minutes. Il s'agirait alors de la résolution temporelle la plus précise que pourrait proposer la plate-forme de visualisation à distance. De même, p. ex. il apparaît peu réaliste qu'un prosumer travaille activement sur l'interface locale de l'AMI avec des informations sur les tarifs (p. ex. tarif haut ou tarif bas), au-delà du tarif appliqué actuellement dans l'AMI.

2.4.1 Visualisation sur l'interface locale

(1) Les données de comptage de l'AMI sont préparées par le module d'analyseur en fonction des formats et filtres prévus, puis exportées depuis le module de visualisation, via l'interface **IC2**, vers le prosumer ou un autre sujet habilité. La propriété ne permettant la lecture des données que par des sujets habilités et ne permettant pas l'influence de l'AMI via cette interface est capitale. D'autres propriétés techniques restent à la discrétion du fabricant.

2.4.2 Visualisation sur l'interface distante

(1) L'interface distante permet de consulter les données de consommation et leur visualisation ainsi que les informations de tarif. Ces données proviennent de la gestion des données clients du gestionnaire de données et peuvent être mises à disposition directement par ce dernier ou par un autre prestataire de données énergétiques. Les propriétés permettant le transfert des données de façon confidentielle au prosumer authentifié ou à un autre sujet habilité sont capitales. Les accès non autorisés via cette interface à la gestion des données clients sont entravés par la gestion de la sécurité des informations du gestionnaire de données. D'autres propriétés techniques restent à la discrétion du gestionnaire de données.

2.5 Architectures

2.5.1 Appareils de mesure intelligents raccordés en parallèle

(1) Chaque AMI a une connexion WAN au STR ou au CD et utilise l'**IC3**. Il s'agit de l'architecture typique pour les solutions CPL à bande étroite. Le besoin de protection de l'**IC3**, toujours crypté, s'applique ici.

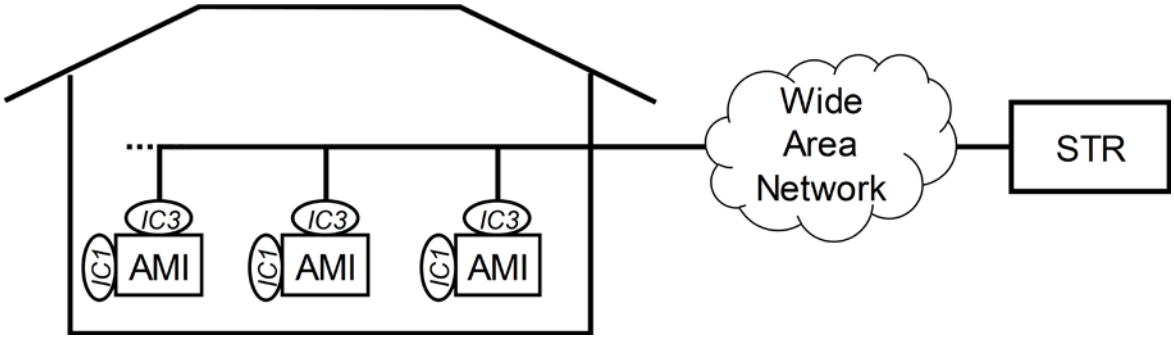

Figure 9: Appareils de mesure intelligents raccordés en parallèle

2.5.2 Appareil de mesure intelligent avec LMN

(1) Un AMI fonctionne également comme passerelle. Il a une connexion WAN au STR ou au CD et utilise **IC3**. D'autres AMI sont raccordés parallèlement dans son LMN via son **IC3** à l'**IC1** de l'AMI connecté au WAN. Le besoin de protection de l'**IC3**, toujours crypté, s'applique ici.

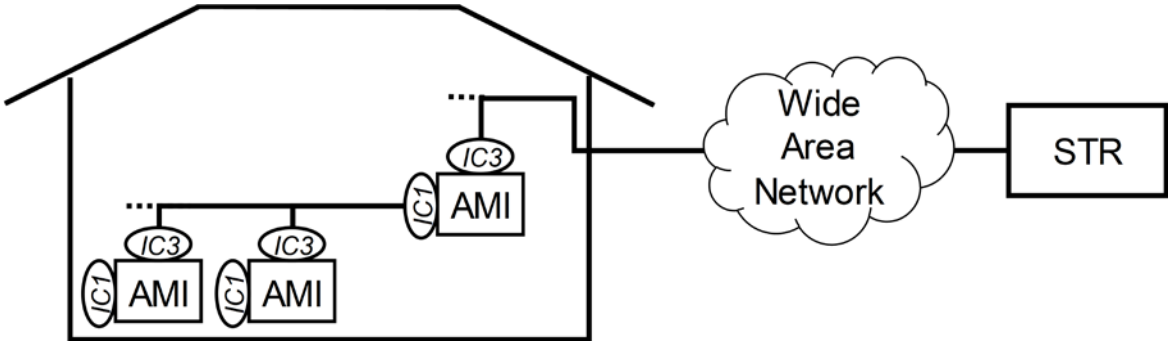

Figure 10: Appareil de mesure intelligent avec LMN

2.5.3 Appareil de mesure intelligent avec LMN en cascade

(1) Un AMI fonctionne également comme passerelle. Il a une connexion WAN au STR et utilise l'**IC3**. Au moins un autre AMI est raccordé dans son LMN via son **IC3** à l'**IC1** de l'AMI connecté au WAN. Le deuxième AMI dispose d'un (sous-)LMN propre au niveau de son **IC1,** etc. Le besoin de protection de l'**IC3**, toujours crypté, s'applique ici.

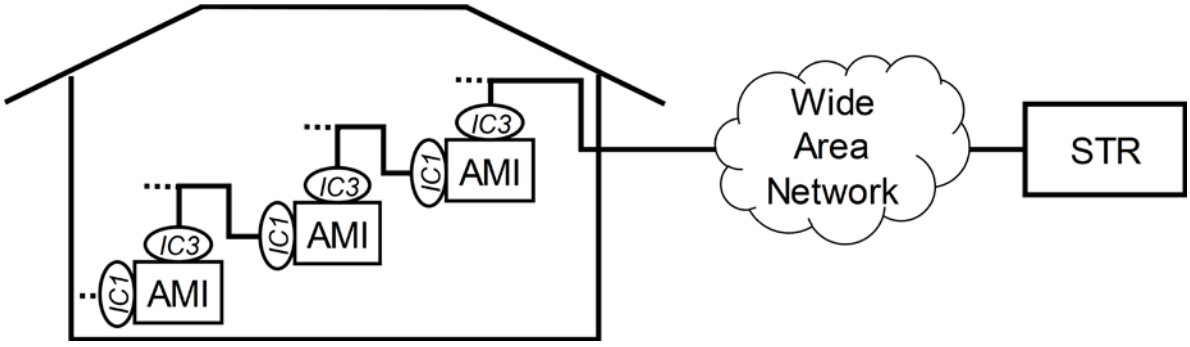

Figure 11: Appareil de mesure intelligent avec LMN en cascade

2.5.4 Passerelle avec LMN

(1) La passerelle/gateway (GW) a une connexion WAN au STR et utilise l'**IC3**. Les AMI sont raccordés parallèlement dans son LMN via l'**IC3** à l'**IC1** de l'AMI connecté au WAN. Le besoin de protection de l'**IC3**, toujours crypté, s'applique ici.

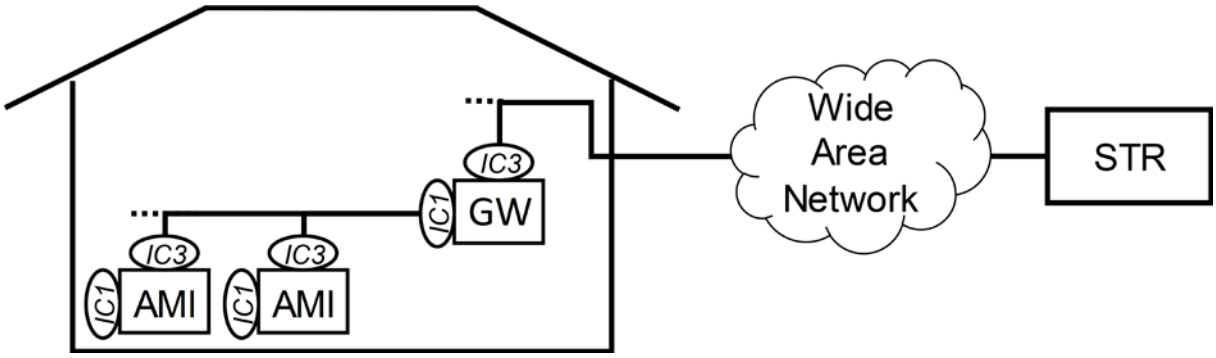

Figure 12: Passerelle avec LMN

2.5.5 Passerelle avec LMN en cascade

(1) La passerelle/gateway (GW) a une connexion WAN au STR et utilise l'**IC3**. Au moins un autre AMI est raccordé dans son LMN via l'**IC3** à l'**IC1** de l'AMI connecté au WAN. Le deuxième AMI dispose d'un (sous-)LMN propre sur son **IC1** etc. Le besoin de protection de l'**IC3**, toujours crypté, s'applique ici.

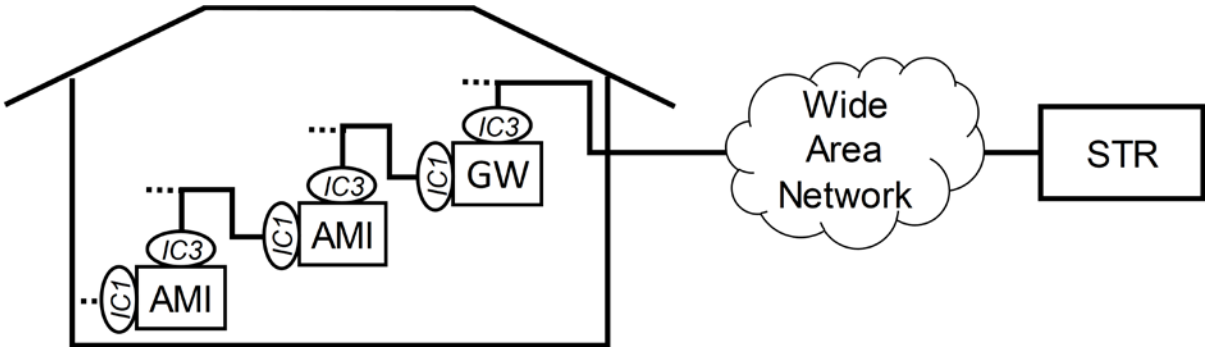

Figure 13: Passerelle avec LMN en cascade

3. Objets de protection pertinents

(1) Les objets vulnérables suivants résultent du document de base «Exigences minimales concernant le système de mesure intelligent» [2] et de l'analyse des besoins de protection [3]. Les exigences de sécurité à respecter sont spécifiées à la Section 5.

(2) Les «objets de protection subordonnés» répertoriés dans l'analyse des besoins de protection (ici: Section 4, Tableau 3) sont concrétisés dans cette section et représentés sur les composants principaux correspondants d'un SMI.

(3) Le besoin de protection résulte respectivement de la protection contre tout accès non autorisé résultant de la perte ou de l'altération de l'intégrité, la confidentialité ou la disponibilité des objets de protection.

3.1 Système de mesure intelligent

(1) Un système de mesure intelligent se compose au moins d'appareils de mesure intelligents et d'un système de tête de réseau.

(2) En règle générale, toutefois, les systèmes de communication procèderont au transfert de données entre l'appareil de mesure intelligent et le système de tête de réseau, et le système de tête de réseau est exploité comme un sous-système dans le STDC. Le STDC comprend donc également, comme objet du présent document, le composant principal «système de tête de réseau» du SMI et la gestion de clés cryptographique.

(3) Toutes les configurations des composants principaux forment respectivement un système fermé, dont les fonctions et les interfaces externes sont définies. Leurs architectures et processus sont documentés par les fabricants et spécifiés quant aux exigences de sécurité des données, et mises en œuvre conformément à ces exigences.

(4) En raison du caractère fermé de ce système, on suppose que les processus internes se déroulent conformément aux exigences et que seuls les sujets habilités ont pu avoir accès aux objets qui leur sont attribués via les interfaces externes, conformément à leurs profils de rôle.

(5) En outre, il convient de protéger:

- les interfaces externes contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon)
- l'intégrité physique (identification de manipulation)
- le démarrage fiable (p. ex. par un procédé de démarrage sécurisé)
- le fonctionnement fiable des fonctions mises en œuvre
- un auto-diagnostic fiable pour la détection d'éventuels accès compromettants

3.2 Plateforme de visualisation

(1) La plateforme de visualisation se trouve à différents emplacements avec différentes architectures et fonctionnalités. Elle peut être mise à la disposition de prosumers habilités, localement sur l'AMI ou à

distance. En outre, dans l'architecture logicielle des variantes de ce composant, il est prévu que différents jeux de données soient traités avec différentes exigences de sécurité.

3.2.1 Visualisation locale

(1) L'interface proposée à cet effet par l'AMI authentifie les sujets habilités et ne permet en outre aucune autre saisie, mais exporte les données de comptage à visualiser en lecture seule (read only).

3.2.2 Visualisation distante

(1) L'interface proposée à cet effet par le gestionnaire de données authentifie les sujets habilités et autorise la communication bidirectionnelle pour les données de comptage en lecture seule (read only), les données SIC, la tarification ou les autres transactions clients complexes.

3.3 Interfaces externes

3.3.1 Interface vers l'administration locale (IC0)

(1) Les composants principaux AMI et CD peuvent être administrés localement.

(2) Si un administrateur gère un composant principal localement, donc avec une connexion physique directe, il utilise l'interface **IC0**.

(3) Cette interface peut être mise à disposition exclusivement à cet effet (CD). Elle peut par ailleurs également prendre en charge une lecture du compteur locale (AMI ou passerelle).

(4) L'interface authentifie des sujets habilités et autorise ces accès sur la base des rôles des utilisateurs.

(5) La communication via cette interface est cryptée.

3.3.2 Interface IC3 (Wide Area Network)

3.3.2.1 Configuration de base de l'AMI

(1) Un AMI communique avec le STR, au-delà des limites du domaine, sur un réseau étendu (Wide Area Network) (Figure 14). Cela inclut le transfert des données de comptage (pour la consommation d'énergie, le statut de réseau, etc.) au gestionnaire de données et à l'administration de l'AMI (configuration, mises à jour, etc.) par des opérateurs habilités au niveau du gestionnaire de données. La communication est cryptée.

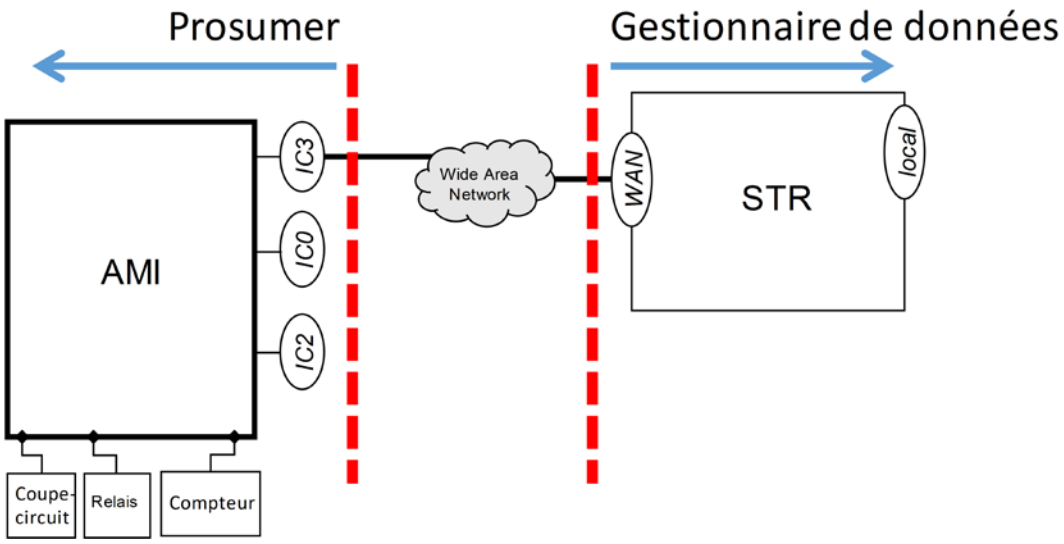

Figure 14: Configuration de base STR AMI

3.3.2.2 L'AMI comme passerelle

(1) Si un AMI est utilisé avec un compteur propre comme passerelle, les données de comptage des autres appareils qui sont raccordés à son interface **IC1** et celles du compteur dans l'AMI sont transférées au STR directement ou via un CD (Figure 15).

(2) Ce cas n'est pas à prendre en compte si l'AMI traite p. ex. les données énergétiques avec le compteur monté et doit transférer parallèlement d'autres données de consommation (eau, chauffage, gaz). Dans ce cas, l'AMI est localisé dans le domaine du prosumer.

(3) L'AMI en guise de passerelle transfère ses données de comptage et données de configuration ainsi que les données de comptage et données de configuration des appareils qui sont raccordés via son interface IC1, directement ou par l'intermédiaire d'un CD, du et vers le STR.

(4) Les interfaces des appareils raccordés établissent, si possible, une connexion cryptée à un niveau de protocole adapté, avec l'interface IC1 de l'AMI, en fonction de la technique de transfert et des protocoles de communication utilisés.

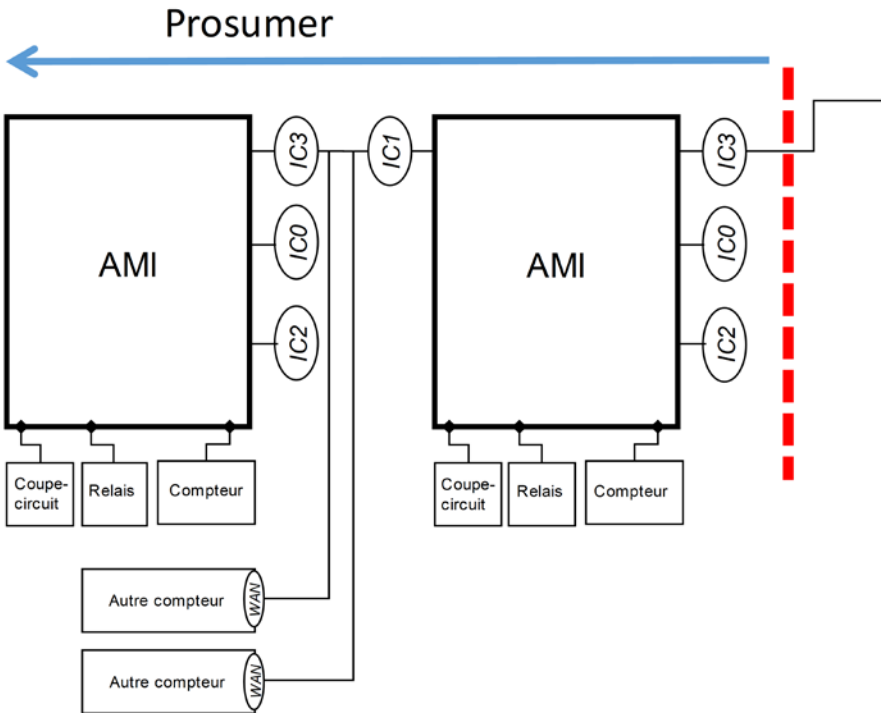

Figure 15: Configuration de l'AMI comme passerelle

3.3.2.3 Passerelle sans compteur propre

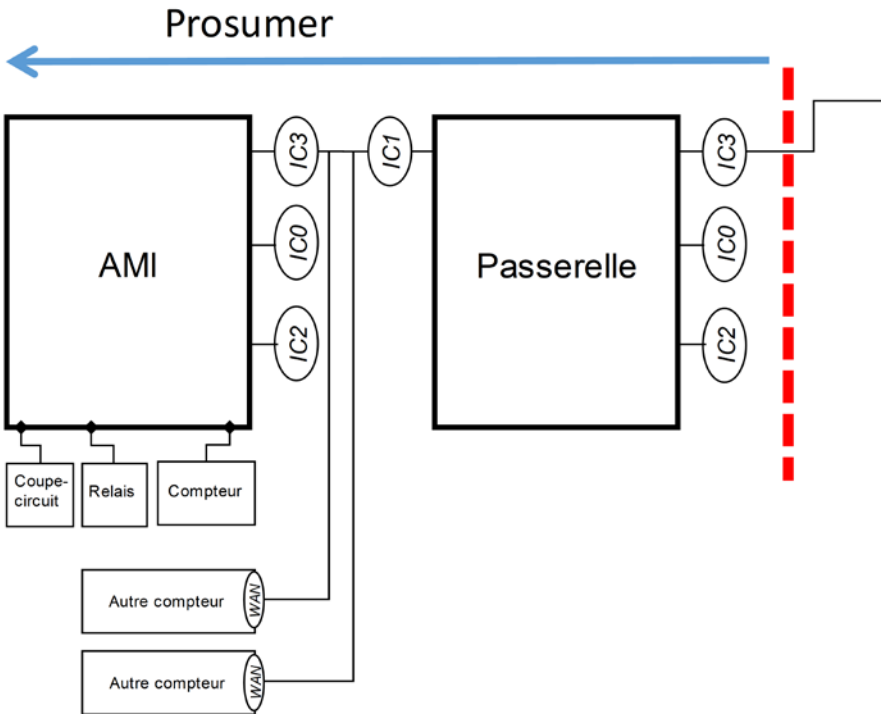

Figure 16: Architecture basée sur la passerelle dans l'environnement de prosumer

(1) Un appareil passerelle dédié peut être utilisé à la place d'un AMI servant de passerelle. Différents AMI peuvent être raccordés à cette passerelle via l'interface **IC1** (Figure 16).

(2) En fonction du modèle, une passerelle peut enregistrer et transmettre localement des données de comptage (similaire avec un AMI).

(3) Si aucun traitement local des données de comptage n'est réalisé, les exigences au sens du point 2.3.2.2 et l'interface **IC2** ne s'appliquent pas.

3.3.2.4 Concentrateur de données (CD)

(1) De la même manière, les exigences et les interfaces **IC1**, **IC3$_{CP}$** et **IC3$_{STR}$** s'appliquent également par analogie pour le CD, qui n'est généralement pas localisé dans le domaine du prosumer (Figure 17), p. ex. dans une station transformatrice. L'interface **IC3$_{CP}$** permet le raccordement de l'AMI via leurs interfaces **IC3**.

(2) Si un CD dispose également d'une interface **IC1**, de sorte que d'autres compteurs peuvent également être raccordés au CD (pas de composant principal du SMI), les exigences pour cette interface du CD s'appliquent également par analogie.

(3) Toutefois, contrairement à l'AMI, le CD transfère uniquement les données de comptage et les données de configuration des autres appareils.

(4) Il permet une gestion depuis un système distant via son interface **IC3$_{STR}$** et localement via son interface IC0.

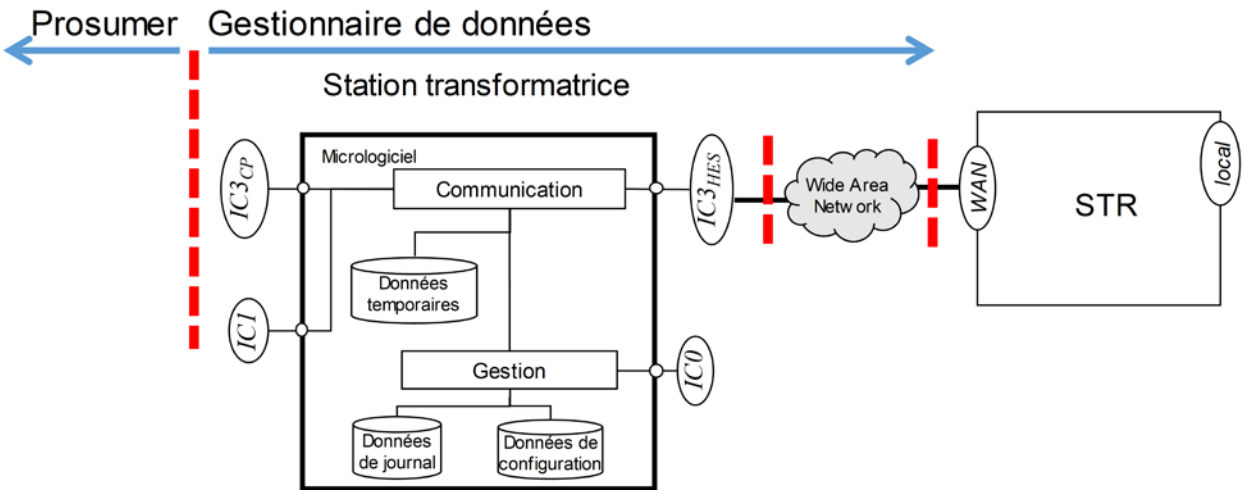

Figure 17: Configuration du concentrateur de données

3.3.3 Interface IC1 (Local Metrological Network)

(1) L'interface permet le raccordement d'autres appareils de mesure («autres compteurs», compteurs de secteurs étrangers qui ne sont pas des composants principaux du SMI) via leurs interfaces WAN au niveau d'un des composants principaux du SMI, qui prennent en charge une fonctionnalité de passe-

relle (AMI comme passerelle ou CD). Elle prend en notamment charge des protocoles de moindre portée, comme les courants porteurs en ligne (CPL, *powerline communication* – PLC).

(2) L'interface **IC1** permet, si possible, l'établissement d'une connexion cryptée entre un autre compteur et le composant principal agissant comme passerelle, et ne permet notamment pas d'accéder à d'autres fonctions internes de la passerelle.

(3) Les données de comptage et données de configuration des appareils à l'interface **IC1** sont transmises par le module de communication, sans traitement des données, mais avec conversion de protocole et cryptage, le cas échéant.

(4) Les commandes pour la consultation des données de comptage depuis des compteurs de secteurs étrangers raccordés qui sont mis en œuvre conformément à la protection des données (p. ex. consommation journalière, etc.) sont transférables uniquement aux compteurs correspondants via l'interface **IC1** et ne peuvent être modifiées dans l'AMI sans autorisation.

(5) Les commandes pour les appareils de courbe de charge externes raccordés peuvent être transférées uniquement via l'interface **IC1** et ne peuvent être modifiées dans l'AMI sans autorisation. La communication est cryptée.

3.3.4 Interface IC2 (HAN, Home Area Network)

(1) Un AMI permet au prosumer correspondant ou à un autre sujet habilité d'accéder, via cette interface, à une plateforme de visualisation locale.

(2) Les propriétés fondamentales de cette interface incluent l'authentification des utilisateurs auxquels les données de comptage sont transmises, et la garantie qu'il s'agit d'un export de données en lecture seule.

(3) Par conséquent, il y a au moins une option de raccordement locale pour un système ICT (Information and Communication Technology) adapté du prosumer.

3.4 Données dans les composants principaux

(1) Les principaux risques de perte de confidentialité, d'intégrité et de disponibilité des données s'appliquent respectivement dans une forme spécifique aux jeux de données correspondants et peuvent avoir des conséquences différentes. Il s'agit aussi bien de l'atteinte à la personnalité en matière de protection des données en cas de perte de confidentialité, ou de sanctions de droit civil ou pénal en cas de perte de disponibilité, qui peut provoquer, dans le pire des cas, une situation opérationnelle dangereuse.

(2) Cette section répertorie de manière structurée les données présentant un besoin de protection, en fonction des champs d'application. Les exigences de sécurité à respecter sont spécifiées à la Section 5, Exigences relatives au système de mesure intelligent.

3.4.1 Données de configuration

Micrologiciel

(1) Le système d'exploitation et les applications dans tous les composants principaux sont soumis à un contrôle de version, sont installés à la livraison et sont protégés contre toute mise en service non autorisée.
L'intégrité de ces données est la condition préalable pour un fonctionnement correct et fiable.

Mise à jour du micrologiciel:

(1) Le système d'exploitation et les applications dans tous les composants principaux sont soumis à un contrôle de version, sont installés dans les composants principaux en fonction du contrôle de version par des utilisateurs autorisés dans le rôle d'administrateurs, et sont mis en service.
L'intégrité de ces données est la condition préalable pour un fonctionnement correct et fiable.

Données de configuration de compteur

(1) Les données qui définissent le fonctionnement et le comportement d'un composant principal
L'intégrité de ces données est la condition pour un fonctionnement correct et fiable. Les modifications non autorisées menacent p. ex. la disponibilité des performances énergétiques pour le prosumer ou la tarification correcte.

Horloge du compteur

(1) Données de configuration spéciales
L'intégrité de ces données est la condition pour une indication correcte de l'heure dans les données de comptage, sa disponibilité doit être garantie pour l'indication permanente de l'heure.

Données de commutation

(1) Données de configuration spéciales
Si le composant principal AMI dispose d'une fonction de disjoncteur (coupe-circuit) qui peut être déclenchée à distance, une protection d'intégrité est mise en œuvre, avec une autorisation, pour les données qui déclenchent localement le processus correspondant.

(2) Cette mesure s'applique par analogie pour les données qui comprennent des commandes sur d'autres relais, fonctionnant p. ex. comme une télécommande centralisée.

(3) Les données de commutation pour un coupe-circuit doivent être clairement transférées pour une unité dédiée, et requièrent un opérateur autorisé au niveau du gestionnaire de données. Une diffusion pour le déclenchement simultané de plusieurs coupe-circuits n'est pas autorisée.

(4) Les données de commutation qui commandent les groupes de consommateurs peuvent être transférées automatiquement par diffusion.

Clé cryptographique

(1) Les jeux de données qui peuvent être utilisés pour le cryptage (confidentialité) et la protection de l'intégrité des données, et pour l'authentification
En fonction de l'utilisation, la clé commune d'un processus de cryptage symétrique ou la clé privée d'un processus asymétrique doit au moins être sécurisée contre la perte de confidentialité. La perte de l'intégrité de la clé publique est protégée par un certificat numérique.

(2) La compromission d'une clé ne doit pas entraîner celle des autres.

(3) La gestion de clés détermine la durée de vie des clés et garantit un renouvellement cyclique. De même, des algorithmes de cryptage, des longueurs de clés et d'autres processus (p. ex. fonctions de hachage) sont régulièrement contrôlés selon l'état de la technique, p. ex. au niveau de la durée restante et des réglementations légales nationales, et des mises à jour du micrologiciel sont mises en œuvre dans les délais.

Données clients:

(1) Les jeux de données contenant des informations qui permettent de tirer des conclusions sur des personnes, en tant que clients du gestionnaire du réseau.
Si des données de ce type existent dans les composants principaux, celles-ci doivent être protégées contre toute perte de confidentialité afin d'exclure toute atteinte à la personnalité.

3.4.2 Données réseau

(1) Les informations de statut utilisées par le gestionnaire de réseau de distribution pour la commande d'un réseau de distribution
Ces données mettent à disposition des informations actuelles. Pour garantir le fonctionnement correct, il convient de garantir l'intégrité des données.

3.4.3 Données de comptage

Courbe de charge, données de registre:

(1) Toutes les données de comptage issues de la consommation et l'injection dans l'AMI à des intervalles donnés
L'AMI dispose d'un compteur d'énergie intégré qui transmet régulièrement des valeurs de mesure à l'interface interne. Celles-ci doivent être protégées contre toute perte d'intégrité et de confidentialité à partir de l'interface interne. Une perte de disponibilité de ces valeurs doit être observée, et une entrée de journal ainsi qu'une signalisation au gestionnaire de données sont effectuées. En fonction des utilisateurs auxquels sont transmises les données de comptage via les interfaces externes de ce composant principal, l'AMI continue de préparer les données brutes reprises et traitées par le compteur. Les données exportées doivent également être protégées contre la perte d'intégrité et de confidentialité.

Informations sur le marché:

(1) Les informations quantifiables se trouvant dans un AMI au sens des considérations de l'Use Case 2 de l'ABP [3]
L'intégrité des informations sur le marché doit être généralement considérée comme critique, puisque des valeurs erronées (à grande échelle) pourraient entraîner un état critique du réseau. La disponibilité et la confidentialité des données du marché au sens décrit ici revêtent une importance moindre en termes de sécurité d'approvisionnement.

3.4.4 Données de journal

(1) Les données de journal sont des données nécessitant une protection. Le type et l'étendue des données à enregistrer ne sont pas l'objet du présent document. Ils sont plutôt définis par la mise en œuvre technique d'un SMI ou d'un composant principal, et notamment par la gestion du gestionnaire de données.

(2) Les fabricants doivent adapter l’étendue des données à enregistrer en fonction des exigences des exploitants.

4. Liste des menaces pertinentes

(1) L'ABP [3] s'appuie sur la prise en compte de certains scénarios de risques (SR). Elle comprend différents cas d'usage (*use cases*) et évalue leur risque d'exploitation propre, sur le plan de la sécurité informatique. Pour cela, 14 scénarios de risques sont spécifiés et des objets de protection, des faiblesses et des menaces sont indiqués. Les graphiques en annexe de l'ABP laissent clairement apparaître que les domaines «prosumer» et «gestionnaire de données», notamment, ont une importance capitale pour les cas d'usage présentés ici. Le présent document se focalise donc sur les composants principaux correspondants d'un SMI dans les domaines précités.

L'analyse des besoins de protection définit les menaces suivantes:

- Modification des données localement
- Modification des données à distance
- Modification des heures
- Accès non autorisé aux données localement
- Accès non autorisé aux données à distance
- Accès non autorisé aux données enregistrées sur l'appareil qui ne sont plus traitées
- Limitation de la disponibilité des données
- Commutation non autorisée du coupe-circuit
- Commutation non autorisée du relais dans le smart meter
- Démarrage non sécurisé

(2) Certaines menaces spécifiées dans l'ABP peuvent partiellement se répercuter directement sur la perte de confidentialité, d'intégrité et de disponibilité. La distinction entre «localement» et «à distance» est importante uniquement dans la mesure où ces menaces concernent les mêmes objets, mais résultent soit d'un défaut de résistance des appareils, soit d'un défaut de sécurité lors du transfert des données. S'agissant des composants principaux, la même fonctionnalité de protection doit être requise, mais pour les différentes interfaces externes, elle doit être mise en œuvre en conséquence.

(3) Une distinction en fonction de l'intégrité, la confidentialité et la disponibilité permet de regrouper les menaces de la façon suivante:

Perte d'intégrité	
– Modification des données localement – Modification des données à distance – Modification des heures	Cela peut se produire en cas d'accès en écriture non autorisé aux données enregistrées dans l'appareil ou pendant le transfert de données.

Perte de confidentialité	
– Accès non autorisé aux données localement	Cela peut se produire en cas d'accès en lecture non autorisé aux données enregistrées dans l'appareil ou pendant le transfert de données. Un éventuel accès aux espaces de stockage qui ont été utilisés au préa-

– Accès non autorisé aux données à distance – Accès non autorisé aux données enregistrées sur l'appareil qui ne sont plus traitées	lable pour le traitement des données nécessitant une protection peut notamment entraîner la perte de confidentialité.

Perte de disponibilité	
– Perte ou limitation de la disponibilité des données	Cela peut se produire en cas d'accès non autorisé aux processus traitant les données, de telle sorte qu'ils ne parviennent pas à procéder à l'enregistrement ou au transfert correct et reproductible.
– Commutation non autorisée du coupe-circuit – Commutation non autorisée du relais dans le smart meter	La commutation non autorisée du coupe-circuit ou du relais dans le smart meter entraîne, en règle générale, la perte de disponibilité de l'énergie électrique au point de mesure. À cela une condition: l'accès non autorisé aux parties du micrologiciel qui commandent le commutateur. Ce type de menace résulte, en fonction de la mise en œuvre, de la perte de confidentialité (p. ex. nom d'utilisateur/mot de passe) ou d'intégrité (modification non autorisée d'une variable de commande dans le logiciel)
– Démarrage non sécurisé	Il s'agit d'une lacune essentielle en matière de sécurité, dans la mesure où la menace atteint le système pendant le processus de démarrage, avant que les fonctions de sécurité, sous forme d'applications, ne soient activées. Les attaques peuvent aller jusqu'à la tentative d'accéder au menu démarrage par l'activation et la désactivation, ou au démarrage d'un système d'exploitation étranger.

5. Exigences relatives au système de mesure intelligent

5.1 Exigences globales

5.1.1 Modèle de rôle d'utilisateur

(1) En tenant compte des différents composants principaux et du GDC, trois catégories principales de rôles d'utilisateurs sont établies:

- Administrateur:
  Utilisateur qui assure l'installation, la maintenance et la gestion du système. L'administrateur a donc notamment l'autorisation de modifier la configuration de la sécurité et du système.
- Opérateur:
  Utilisateur qui exploite le système dans le cadre de l'utilisation prévue. Cela inclut également le droit de modifier les réglages opérationnels.
- Affichage de données:
  Utilisateur qui peut consulter le statut du système et lire les données opérationnelles définies, mais n'est pas habilité à effectuer des modifications.

(2) Pour répondre aux exigences d'un «contrôle d'accès granulaire» et de l'environnement-système complexe des différents composants principaux du SMI, il convient d'utiliser, au sens du principe du *need-to-know* (ou *need-to-use*), davantage de types d'utilisateur avec la même classification mais avec des droits d'accès différents configurés de manière adéquate.

Liste non exhaustive des utilisateurs SMI possibles:

- Administrateur AMI
  peut configurer un AMI localement ou à distance.
- Administrateur CD
  peut configurer un CD localement ou à distance.
- Administrateur STR
  peut configurer un STR chez le gestionnaire de données.
- Releveur de compteur
  peut lire localement les données de comptage sur l'AMI et synchroniser l'heure du compteur.
- Opérateur
  peut lire à distance les données de comptage (consommation ou réseau) depuis l'AMI via le STR.
- Gestionnaire de coupe-circuit
  peut déclencher un coupe-circuit à distance.
- Assistance fabricant
  correspond p. ex. à un technicien qui accède à distance à d'autres composants principaux depuis son domaine ou celui du gestionnaire de données.
- Prosumer local
  peut saisir des données de comptage uniquement en lecture via un composant de visualisation dans l'AMI.

– Prosumer à distance
peut recevoir des données de comptage du gestionnaire de données via un composant de visualisation et modifier, le cas échéant, des réglages dans le SIC du gestionnaire de données.

5.1.2 Contrôle d'accès

a) Sur les interfaces des composants principaux avec accès utilisateur, les droits d'accès respectifs sont définis pour tous les rôles en ce qui concerne les objets à protéger.
b) Le modèle de rôle à appliquer doit être défini par le fabricant.
c) Le modèle de rôle peut être complété par des utilisateurs autorisés.

5.1.3 Identification et authentification

a) Une solution est mise en œuvre avec au moins un nom d'utilisateur et un mot de passe aux interfaces des composants principaux avec un accès utilisateur local. Un accès protégé par un mot de passe à un rôle défini est possible au niveau de l'AMI.
b) Si un composant principal prend en charge le télétravail, des procédures d'authentification solides (basées sur la possession et les connaissances) doivent être mises en œuvre. Cela peut être le cas pour un STR et pour les accès à un composant principal via le STR.
c) Les mots de passe doivent être échangés via des canaux cryptés.
d) Les mots de passe standard doivent être modifiés à la première connexion.
e) Un contrôle de la complexité du mot de passe doit être réalisé selon l'état de la technique.
f) Si la procédure de connexion (log-in) n'est pas exécutée avec succès, le système ne doit donner aucun renseignement sur l'information qui n'était pas correcte (nom d'utilisateur ou mot de passe).
g) Les mots de passe doivent être masqués lors de la saisie.
h) Les mots de passe doivent pouvoir être modifiés manuellement. Le processus doit inclure une confirmation de cette action. La modification ou une tentative de modification entraîne une entrée de journal.
i) Si des mots de passe sont enregistrés, cela doit être fait de façon cryptée.

5.1.4 Cryptage

a) Le trafic de données entre les composants principaux est crypté.
b) Les données vulnérables doivent être enregistrées uniquement de manière cryptée dans le système de mesure intelligent. Celui-ci doit permettre la suppression sûre et sélective de certaines données, par exemple en écrasant les données aléatoires.
c) Lors de la sélection de normes de cryptage, les législations nationales doivent être prises en compte. Il ne faut utiliser que les procédures de cryptage et les longueurs de clé minimales reconnues qui sont considérées comme sûres selon l'état actuel de la technique également sur une durée prévisible. Les algorithmes de cryptage exclusifs ne sont pas autorisés. Lors de la mise en œuvre des procédures de cryptage, il convient, si possible, d'accéder à des bibliothèques de cryptage reconnues pour éviter les erreurs de mise en œuvre.
d) Les algorithmes utilisés doivent être indiqués.

5.1.5 Cycle de vie des composants principaux

(1) Le cycle de vie d'un composant principal comprend au moins sa spécification, son développement, sa livraison et sa mise en service ainsi que son élimination sûre. Les composants présentant une

fonctionnalité de sécurité informatique clôturée en matière de spécification et de développement peuvent toutefois être compromis dans toutes les phases de leur cycle de vie par des accès non autorisés.

a) Par conséquent, le fabricant garantit, dans les phases qu'il contrôle, la protection contre la perte de ou l'atteinte à l'intégrité, la confidentialité et la disponibilité de ses composants.
b) Ces mesures sont documentées par le fabricant et leur mise en œuvre peut être vérifiée par les exploitants de ses composants.
   Les exploitants respectent ainsi une approche procédurale pour l'acquisition, le développement et la maintenance de systèmes avec des prescriptions spécifiées dans le document exploitant. Les fabricants sont tenus d'adapter l'étendue des aspects à documenter en fonction des exigences des exploitants.
c) Si des points faibles critiques en matière de sécurité sont identifiés pendant le fonctionnement du CP, les mesures organisationnelles visant à mettre au jour, documenter et réparer les défauts entre les fabricants et les exploitants (*flaw remediation*, remédiation des points faibles) doivent être coordonnées.
d) La sécurité lors du développement et de la prise en charge des processus pour la livraison et la mise en service
e) Si un fabricant intègre des produits tiers ou des composants partiels dans ses produits, il exécute des contrôles à l'entrée au sens du a).
f) Si une élimination sûre des composants est requise, le fabricant contraint ses clients à documenter les composants restants ainsi que leur destruction, ou à les restituer sans pièce manquante.

5.2 Exigences relatives à l'AMI

5.2.1 Exigences relatives à un fonctionnement sûr

5.2.1.1 Livraison et première mise en service

a) Le fabricant livre en principe un AMI opérationnel, mais dans une configuration adaptée, de sorte qu'une première mise en service requiert au moins un enregistrement de l'appareil auprès du gestionnaire de données, avant que l'AMI n'autorise ses fonctions prévues.
b) L'identification des appareils et les numéros de version du micrologiciel (le cas échéant des composants individuels) sont documentés, et le certificat de livraison et les données qu'il contient sont déterminants.
c) Si l'appareil ne se trouve pas dans cet état de fonctionnement lors d'une première mise en service, cela doit pouvoir être constaté, afin que l'appareil puisse d'abord être reconfiguré.

5.2.1.2 Démarrage sécurisé de l'appareil

a) Après la première mise en service, un appareil est en mesure d'adopter le mode de fonctionnement prévu à chaque nouveau démarrage. Les menus de démarrage sont accessibles uniquement aux administrateurs habilités.
b) Le démarrage des supports de données externes est impossible.
c) Si l'appareil constate un redémarrage défectueux, un message d'erreur est émis, le cas échéant, une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et le démarrage des applications locales est empêché dans l'AMI.

d) Le système d'exploitation est en mesure d'exécuter un contrôle d'intégrité sur lui-même. Lors d'un contrôle d'intégrité défectueux, un message d'erreur est émis, et une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et le démarrage des applications locales est empêché dans le compteur.

5.2.1.3 Détection de sabotage

a) Un appareil qui fonctionne dans le mode de fonctionnement prévu peut reconnaître si l'intégrité du boîtier est compromise. Dans ce cas, un message d'erreur est délivré et une alarme est déclenchée auprès du gestionnaire de données.
b) Ces résultats sont repris dans les données de journal.

5.2.1.4 Protection de la mémoire

a) Le système d'exploitation permet la gestion de l'espace de stockage, de sorte que, dans la mémoire volatile de l'appareil, les espaces d'adressage sont réservés exclusivement pour les applications correspondantes.
b) Les espaces de stockage où sont enregistrées provisoirement les données de comptage ou les clés de cryptage sont récupérés après leur utilisation par un écrasement ciblé.

5.2.1.5 Journalisation

a) Tous les événements du système relevant de la sécurité des données sont repris dans les données de journal.
b) Les données de journal doivent être lues exclusivement par des utilisateurs autorisés à le faire.
c) Les données de journal sont sécurisées contre toute modification ou suppression non autorisée.
d) Le type et l'étendue des données à enregistrer ne sont pas l'objet du présent document. Ils sont plutôt définis par la mise en œuvre technique d'un SMI ou d'un composant principal de ce dernier, ainsi que par la gestion du gestionnaire de données. La journalisation permet au minimum de répondre aux exigences spécifiées au [4].

   Les fabricants sont tenus d'adapter l'étendue des données à enregistrer en fonction des exigences des exploitants.

5.2.1.6 Mise à jour du micrologiciel

a) Un administrateur autorisé peut uniquement lancer des mises à jour sur un appareil qui fonctionne dans le mode prévu.
b) Le système d'exploitation est en mesure d'exécuter un contrôle d'intégrité de la mise à jour (p. ex. par l'enregistrement temporaire et le test avec somme de contrôle).
c) Lors d'un contrôle d'intégrité défectueux, un message d'erreur est émis, le cas échéant, une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et la mise à jour est empêchée. Dans ce cas, le système d'exploitation est capable de démarrer à nouveau de façon fiable avec la version logicielle précédente.
d) Si une authentification de l'origine d'une mise à jour n'est pas possible avec les informations et fonctions conformément aux points a) et b), une authentification des mises à jour doit être mise en œuvre avec une autre fonctionnalité. L'échec d'une tentative d'authentification doit être traité conformément au point c).

e) La mise à jour de la partie métrologique de l'AMI est autorisée uniquement dans le cadre des objectifs MID (directive sur les instruments de mesure 2004/22/CE, Measuring Instruments Directive en anglais) et du METAS (Institut fédéral de métrologie).
f) La mise à jour du micrologiciel est possible uniquement via **IC0** et **IC3**.
g) Le micrologiciel de tous les composants principaux doit pouvoir être actualisé.

5.2.2 Interfaces

5.2.2.1 Interface IC0

a) Pour l'accès à cette interface, au moins les rôles d'utilisateurs «administrateur AMI», «releveur de compteur» et «opérateur_local» sont disponibles conformément aux droits d'accès correspondants.
b) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe.
c) L'interface offre au rôle de «releveur de compteur» un accès en lecture seule au relevé local des données de comptage prévues et la synchronisation de l'heure du compteur.
d) L'interface offre au rôle d'«opérateur_local» un accès en lecture seule aux données de comptage prévues pour le transfert à distance et aux données de réseau, ainsi que l'accès local aux relais et aux coupe-circuits.
e) Pour l'accès à la fonction de coupe-circuit, une authentification en deux étapes doit être prévue. Si cela n'est pas possible au niveau de la construction, la fonction est bloquée et doit être activée depuis le STR pour que l'«opérateur_local» y ait accès. Le blocage sera immédiatement réactivé après l'accès de l'«opérateur_local»,
f) Aucune connexion aux autres interfaces de l'AMI n'est possible via l'interface.
g) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
h) Une perturbation non autorisée de l'interface n'a aucune influence sur la partie métrologique ou sur les autres interfaces.
i) Les tentatives d'accès non autorisés et autres perturbations déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.2.2.2 Interface IC3

a) L'AMI se connecte via l'interface uniquement à l'interface WAN correspondante du STR ou à l'interface **IC3$_{CP}$** du CD et à l'**IC1** de la passerelle.
b) La communication est cryptée au niveau de protocole adapté. Les algorithmes utilisés sont régulièrement contrôlés selon l'état de la technique ou remplacés rapidement en cas de compromission identifiée.
c) Pour l'accès via cette interface, au moins les rôles d'utilisateurs «administrateur AMI» et «opérateur_télé» sont disponibles conformément aux droits d'accès correspondants.
d) Si l'AMI prend en charge le télétravail, des procédures d'authentification en deux étapes (basées sur la possession et les connaissances) doivent si possible être mises en œuvre. Cela peut être le cas pour les accès à l'AMI via le STR.
e) L'interface offre au rôle d'«opérateur_télé» auprès du gestionnaire de données un accès en lecture seule aux données de comptage prévues pour le transfert à distance et notamment aux données de réseau, ainsi que l'accès local aux relais et aux coupe-circuits.
f) Pour l'accès à la fonction de coupe-circuit, une authentification en deux étapes doit être prévue.

g) Aucune connexion aux autres interfaces de l'AMI n'est possible via l'interface. Le module de communication sépare le trafic de données depuis et vers les appareils raccordés via l'**IC1** ou l'**$IC3_{CP}$**.
h) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
i) Une perturbation de l'interface n'a aucune influence sur la partie métrologique ou sur les autres interfaces.
j) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.2.2.3 Interface IC2

a) Pour l'accès à cette interface, au moins le rôle d'utilisateur «prosumer» est disponible conformément aux droits d'accès correspondants.
b) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe.
c) L'interface offre au rôle de prosumer un accès en lecture seule aux données de comptage prévues pour la visualisation.
d) Aucune connexion aux autres interfaces de l'AMI n'est possible via l'interface.
e) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
f) Une perturbation de l'interface n'a aucune influence sur la partie métrologique ou sur les autres interfaces.
g) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du système GDC et ces résultats sont repris dans les données de journal.

5.2.2.4 Interface IC1

a) Via cette interface, l'AMI se connecte uniquement à l'interface WAN correspondante des autres appareils de mesure intelligents dans LMN.
b) La communication est si possible cryptée au niveau de protocole adapté. Les algorithmes utilisés sont régulièrement contrôlés selon l'état de la technique ou remplacés rapidement en cas de compromission identifiée.
c) Aucun rôle d'utilisateur n'est disponible pour l'accès à cette interface. L'administrateur AMI configure les connexions.
d) Les données de comptage des appareils à l'interface IC1 sont transmises par le module de communication uniquement via l'**IC3**, sans traitement des données dans l'AMI, mais avec conversion de protocole et cryptage, le cas échéant.
e) Aucune connexion aux autres interfaces de l'AMI n'est possible via l'interface.
f) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
g) Une perturbation de l'interface n'a aucune influence sur la partie métrologique ou sur les autres interfaces.
h) Les tentatives d'accès non autorisés et d'autres perturbations que peut détecter le composant principal correspondant dans le cadre des protocoles utilisés au niveau de l'interface, déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.2.3 Exigences spécifiques

5.2.3.1 Utilisation du cryptage

a) Chaque appareil reçoit une clé de livraison individuelle. Celle-ci est remplacée par une nouvelle clé à la première mise en service suivant l'enregistrement réussi.
b) Lors du remplacement d'un AMI (p. ex. démontage pour vérification), la clé de livraison peut être réactivée.
c) Le cryptage est réalisé avec une technologie considérée comme sûre au moment de la livraison.
d) La technologie de cryptage peut être mise à jour.
e) Les clés de cryptage sont protégées contre tout accès non autorisé dans tous les appareils et systèmes.

5.2.3.2 Réglages de l'heure

a) Pour l'accès à cet objet via l'interface IC0, les rôles d'utilisateurs «administrateur AMI» et «releveur de compteur» sont utilisés conformément aux droits d'accès correspondants.
b) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe.
c) La modification du réglage de l'heure dans l'AMI déclenche un message au gestionnaire de données et est reprise dans les données de journal.
d) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du système GDC et ces résultats sont repris dans les données de journal.

5.2.3.3 Coupe-circuit

a) Le coupe-circuit dans l'AMI peut être déclenché uniquement par un utilisateur habilité sur le STR, sur la passerelle, sur l'AMI via IC0 ou par les règles enregistrées dans l'AMI. Ce dernier doit donc également être autorisé en conséquence pour la réinitialisation d'un coupe-circuit déclenché.
b) Une fonction de coupe-circuit doit être déclenchée individuellement pour chaque coupe-circuit.
c) Une commande adressée simultanément à plusieurs coupe-circuits est exclue.
d) Le coupe-circuit doit être réactivé localement sur l'appareil après l'autorisation de mise hors tension.

5.2.3.3.1 Relais de commande

a) Un relais de commande peut être déclenché uniquement par un utilisateur habilité sur le STR, sur la passerelle, sur l'AMI via IC0 ou par les règles enregistrées dans l'AMI.
b) Plusieurs relais de commande peuvent être contrôlés par une diffusion.

5.3 Exigences relatives à la passerelle comme système de communication

5.3.1 Exigences relatives à un fonctionnement sûr

5.3.1.1 Livraison et première mise en service

a) Le fabricant livre en principe une passerelle opérationnelle, mais dans une configuration adaptée, de sorte qu'une première mise en service requiert au moins un enregistrement de l'appareil auprès du gestionnaire de données, avant que la passerelle n'autorise ses fonctions prévues.

b) L’identification des appareils et les numéros de version du micrologiciel (le cas échéant des composants individuels) sont documentés, et le certificat de livraison individuel et les données qu’il contient sont déterminants.
c) Si l’appareil ne se trouve pas dans cet état de fonctionnement lors d’une première mise en service, cela doit être constaté, afin que l’appareil puisse être reconfiguré.

5.3.1.2 Démarrage sécurisé de l’appareil

a) Après la première mise en service, un appareil est en mesure d’adopter le mode de fonctionnement prévu à chaque nouveau démarrage. Les menus de démarrage sont accessibles uniquement aux administrateurs habilités.
b) Le démarrage sur des supports de données externes est impossible.
c) Si l’appareil constate un redémarrage défectueux, un message d’erreur est émis, le cas échéant, une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et le démarrage des applications locales est empêché dans la passerelle.
d) Le système d’exploitation est en mesure d’exécuter un contrôle d’intégrité sur lui-même. Lors d’un contrôle d’intégrité défectueux, un message d’erreur est émis, et une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et le démarrage des applications locales est empêché dans le compteur.

5.3.1.3 Détection de sabotage

a) Un appareil qui fonctionne dans le mode de fonctionnement prévu peut reconnaître si l’intégrité du boîtier est compromise. Dans ce cas, un message d’erreur est émis et une alarme est déclenchée auprès du gestionnaire de données.
b) Ces résultats sont repris dans les données de journal.

5.3.1.4 Protection de la mémoire

a) Le système d’exploitation permet la gestion de l’espace de stockage, de sorte que, dans la mémoire volatile de l’appareil, les espaces d’adressage sont réservés exclusivement pour les applications correspondantes.
b) Les espaces de stockage où sont enregistrées provisoirement les données de comptage ou les clés de cryptage sont récupérés après leur utilisation par un écrasement ciblé.

5.3.1.5 Journalisation

a) Tous les événements du système relevant de la sécurité des données sont repris dans les données de journal.
b) Les données de journal doivent être lues exclusivement par des utilisateurs autorisés à le faire.
c) Les données de journal sont sécurisées contre toute modification ou suppression non autorisée.
d) Le type et l’étendue des données à enregistrer ne sont pas l’objet du présent document. Ils sont plutôt définis par la mise en œuvre technique d’un SMI ou d’un composant principal de ce dernier, et notamment par la gestion du gestionnaire de données. La journalisation permet au minimum de répondre aux exigences spécifiées au [4].

5.3.1.6 Mise à jour du micrologiciel

a) Un administrateur autorisé peut uniquement lancer des mises à jour sur un appareil qui fonctionne dans le mode prévu.

b) Le système d'exploitation est en mesure d'exécuter un contrôle d'intégrité de la mise à jour (p. ex. par le stockage temporaire et le test avec somme de contrôle).
c) Lors d'un contrôle d'intégrité défectueux, un message d'erreur est émis, le cas échéant, une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et la mise à jour est empêchée. Dans ce cas, le système d'exploitation est capable de démarrer à nouveau de façon fiable avec la version logicielle précédente.
d) Si une authentification de l'origine d'une mise à jour n'est pas possible avec les informations et fonctions, conformément aux points a) et b), une authentification des mises à jour doit être mise en œuvre avec une autre fonctionnalité. L'échec d'une tentative d'authentification doit être traité conformément au point c).
e) Le micrologiciel de tous les composants principaux doit pouvoir être actualisé.

5.3.2 Interfaces

5.3.2.1 Interface IC0

a) Pour l'accès à cette interface, au moins les rôles d'utilisateurs «administrateur de passerelle», «releveur de compteur» et «opérateur_local» sont disponibles conformément aux droits d'accès correspondants.
b) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe.
c) L'interface offre au rôle de «releveur de compteur» un accès en lecture seule au relevé local des données de comptage prévues et la synchronisation de l'heure de la passerelle.
d) L'interface offre au rôle d'«opérateur_local» un accès en lecture seule aux données de comptage prévues pour le transfert à distance et aux données de réseau, ainsi que l'accès local aux relais et coupe-circuits dans les AMI raccordés.
e) Pour l'accès à la fonction de coupe-circuit, une authentification en deux étapes doit être prévue. Si cela n'est pas possible au niveau de la construction, la fonction est bloquée et doit être activée depuis le STR pour que l'«opérateur_local» y ait accès. Le blocage sera immédiatement réactivé après l'accès de l'«opérateur_local»,
f) Aucune connexion aux autres interfaces de la passerelle n'est possible via l'interface.
g) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
h) Une perturbation non autorisée de l'interface n'a aucune influence sur les autres interfaces.
i) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.3.2.2 Interface IC3

a) Via cette interface, la passerelle se connecte uniquement à l'interface WAN correspondante du STR.
b) La communication est cryptée au niveau de protocole adapté. Les algorithmes utilisés sont régulièrement contrôlés selon l'état de la technique ou remplacés rapidement en cas de compromission identifiée.
c) Pour l'accès via cette interface, au moins les rôles d'utilisateurs «administrateur de passerelle» et «opérateur_télé» sont disponibles conformément aux droits d'accès correspondants.
d) Si la passerelle prend en charge le télétravail, des procédures d'authentification en deux étapes (basées sur la possession et les connaissances) doivent si possible être mises en œuvre. Cela peut être le cas pour les accès à la passerelle via le STR.

e) Le télétravail, p. ex. à des fins de maintenance des fabricants avec des procédures d'authentification «triviales» n'est pas autorisé.
f) L'interface offre au rôle d'«opérateur_télé» auprès du gestionnaire de données un accès en lecture seule aux données de comptage prévues pour le transfert à distance, ainsi que l'accès aux coupe-circuits et aux relais dans les AMI raccordés.
g) Pour l'accès à la fonction de coupe-circuit, une authentification en deux étapes doit être prévue.
h) Aucune connexion aux autres interfaces de la passerelle n'est possible via l'interface. Le module de communication sépare le trafic de données depuis et vers les appareils raccordés via l'**IC1** ou l'**IC3**.
i) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
j) Une perturbation de l'interface n'a aucune influence sur les autres interfaces.
k) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.3.2.3 Interface IC2

a) Pour l'accès à cette interface, au moins le rôle d'utilisateur «administrateur prosumer» est disponible conformément aux droits d'accès correspondants.
b) Si la passerelle traite les données de comptage de différents clients, la conservation des données doit être multi-tenant et peut permettre aux différents clients dans le rôle d'utilisateur «prosumer local» d'accéder exclusivement à leurs données correspondantes.
c) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe.
d) L'interface offre au rôle de prosumer un accès en lecture seule aux données de comptage prévues pour la visualisation.
e) Aucune connexion aux autres interfaces de la passerelle n'est possible via l'interface.
f) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
g) Une perturbation de l'interface n'a aucune influence sur les autres interfaces.
h) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du système GDC et ces résultats sont repris dans les données de journal.

5.3.2.4 Interface IC1

a) Via cette interface, la passerelle se connecte uniquement à l'interface WAN correspondante des autres appareils de mesure intelligents.
b) La communication est si possible cryptée au niveau de protocole adapté. Les algorithmes utilisés sont régulièrement contrôlés selon l'état de la technique ou remplacés rapidement en cas de compromission identifiée.
c) Aucun rôle d'utilisateur n'est disponible pour l'accès à cette interface. L'administrateur de passerelle configure les connexions
d) Les données de comptage des appareils à l'interface **IC1** sont transmises par le module de communication uniquement via l'**IC3**, sans traitement des données dans la passerelle, mais avec conversion de protocole et cryptage ou stockage temporaire, le cas échéant.
e) Aucune connexion aux autres interfaces de la passerelle n'est possible via l'interface.
f) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
g) Une perturbation de l'interface n'a aucune influence sur les autres interfaces.

h) Les tentatives d'accès non autorisés et d'autres perturbations que peut détecter le composant principal correspondant dans le cadre des protocoles utilisés sur l'interface, déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.3.3 Exigences spécifiques

5.3.3.1 Utilisation du cryptage

a) Chaque appareil reçoit une clé de livraison individuelle. Celle-ci est remplacée par une nouvelle clé à la première mise en service suivant l'enregistrement réussi.
b) Lors du changement de passerelle, la clé de livraison doit être réactivée.
c) Le cryptage est réalisé avec une technologie considérée comme sûre au moment de la livraison.
d) La technologie de cryptage peut être mise à jour.
e) Les clés de cryptage sont protégées contre tout accès non autorisé dans tous les appareils et systèmes.
f) Une interface au système ICP est nécessaire s'il ne s'agit pas d'une solution intégrée.

5.3.3.2 Réglages de l'heure

a) Pour l'accès à cet objet via l'interface **IC0**, les rôles d'utilisateurs «administrateur de passerelle» ou – s'il existe – «releveur de compteur» sont utilisés conformément aux droits d'accès correspondants.
b) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe.
c) La modification du réglage de l'heure dans la passerelle déclenche un message au gestionnaire de données et est reprise dans les données de journal.
d) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du système GDC et ces résultats sont repris dans les données de journal.

5.4 Exigences relatives au concentrateur de données comme système de communication

5.4.1 Exigences relatives à un fonctionnement sûr

5.4.1.1 Livraison et première mise en service

a) Le fabricant livre en principe un CD opérationnel, mais dans une configuration adaptée, de sorte qu'une première mise en service impose au moins un enregistrement de l'appareil auprès du gestionnaire de données, avant que le CD n'autorise ses fonctions prévues.
b) L'identification des appareils et les numéros de version du micrologiciel (le cas échéant des composants individuels) sont documentés, et si un certificat de livraison est utilisé, les données qu'il contient sont déterminantes.
c) Si l'appareil ne se trouve pas dans cet état de fonctionnement lors d'une première mise en service, cela doit pouvoir être constaté, afin que l'appareil puisse d'abord être reconfiguré.

5.4.1.2 Redémarrage sécurisé

a) Après la première mise en service, un appareil est en mesure d'adopter le mode de fonctionnement prévu à chaque nouveau démarrage. Les menus de démarrage sont accessibles uniquement aux administrateurs habilités.
b) Le démarrage des supports de données externes est impossible.
c) Si l'appareil constate un redémarrage défectueux, un message d'erreur est émis, le cas échéant, une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et le démarrage des applications locales est empêché dans le CD.
d) Le système d'exploitation est en mesure d'exécuter un contrôle d'intégrité sur lui-même. Lors d'un contrôle d'intégrité défectueux, un message d'erreur est émis, et une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et le démarrage des applications locales est empêché dans le compteur.

5.4.1.3 Démarrage sécurisé des applications GDC

a) Après la première mise en service, les applications GDC sont en mesure d'adopter à chaque nouveau démarrage le mode de fonctionnement prévu défini par les réglages de configuration.
b) Si l'application constate un redémarrage défectueux, un message d'erreur est émis, le cas échéant, une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal.
c) L'application GDC est en mesure d'exécuter un contrôle d'intégrité sur elle-même. En cas de contrôle d'intégrité erroné, un message d'erreur est émis, le cas échéant, une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal.

5.4.1.4 Détection de sabotage

a) Un appareil qui fonctionne dans le mode de fonctionnement prévu peut reconnaître si l'intégrité du boîtier est compromise. Dans ce cas, un message d'erreur est délivré et une alarme est déclenchée auprès du gestionnaire de données.
b) Ces résultats sont repris dans les données de journal.

5.4.1.5 Protection de la mémoire

a) Le système d'exploitation permet la gestion de l'espace de stockage, de sorte que, dans la mémoire volatile de l'appareil, les espaces d'adressage sont réservés exclusivement pour les applications correspondantes.
b) Les espaces de stockage où sont enregistrées provisoirement les données de comptage ou les clés de cryptage sont récupérés après leur utilisation par un écrasement ciblé.

5.4.1.6 Journalisation

a) Tous les événements du système relevant de la sécurité des données sont repris dans les données de journal.
b) Les données de journal doivent être lues exclusivement par des utilisateurs autorisés à le faire.
c) Les données de journal sont sécurisés contre toute modification ou suppression non autorisée.
d) Le type et l'étendue des données à enregistrer ne sont pas l'objet du présent document. Ils sont plutôt définis par la mise en œuvre technique d'un SMI ou d'un composant principal de ce dernier, et notamment par la gestion du gestionnaire de données. La journalisation permet au mini-

mum de répondre aux exigences spécifiées au [4].

Les fabricants sont tenus d'adapter l'étendue des données à enregistrer en fonction des exigences des exploitants.

5.4.1.7 Mise à jour du micrologiciel

a) Un administrateur autorisé peut uniquement lancer des mises à jour sur un appareil qui fonctionne dans le mode prévu.
b) Le système d'exploitation est en mesure d'exécuter un contrôle d'intégrité de la mise à jour (p. ex. par le stockage temporaire et le test avec somme de contrôle).
c) Lors d'un contrôle d'intégrité défectueux, un message d'erreur est émis, le cas échéant, une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal et la mise à jour est empêchée. Dans ce cas, le système d'exploitation est capable de démarrer de façon fiable avec la version logicielle précédente.
d) Si une authentification de l'origine d'une mise à jour n'est pas possible avec les informations et fonctions conformément aux points a) et b), une authentification des mises à jour doit être mise en œuvre avec une autre fonctionnalité. L'échec d'une tentative d'authentification doit être traité conformément au c).
e) Le micrologiciel de tous les composants principaux doit pouvoir être actualisé.

5.4.2 Interfaces

a) Avec le CD, les exigences de l'AMI ne s'appliquent pas en ce qui concerne

– la lecture du compteur locale à l'interface **IC0** et
– l'interface de visualisation **IC2**.

b) En principe, le scénario opérationnel du CD repose sur le récapitulatif de la communication des données de plusieurs AMI au gestionnaire de données correspondant. À cet effet, les interfaces **IC3$_{CP}$** et **IC3$_{STR}$** sont utilisées. Si le CD est utilisé dans une configuration qui permet également de raccorder d'autres compteurs dans un LMN, l'interface **IC1** est utilisée.

5.4.2.1 Interface IC0

a) Pour l'accès à cette interface, le rôle d'utilisateur «administrateur CD» est disponible conformément aux droits d'accès correspondants.
b) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe.
c) L'interface offre au rôle de releveur de compteur un accès en lecture seule au relevé local des données de comptage prévues et la synchronisation de l'heure du compteur.
d) Aucune connexion aux autres interfaces du CD n'est possible via l'interface.
e) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
f) Une perturbation non autorisée de l'interface n'a aucune influence sur les autres interfaces.
g) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.4.2.2 Interface IC3

a) Via cette interface, le CD se connecte uniquement aux interfaces WAN correspondantes de l'AMI et du STR.
b) La communication est cryptée au niveau de protocole adapté. Les algorithmes utilisés sont régulièrement contrôlés selon l'état de la technique ou remplacés rapidement en cas de compromission identifiée.
c) Pour l'accès via cette interface, au moins les rôles d'utilisateurs «administrateur CD» et «opérateur» sont disponibles conformément aux droits d'accès correspondants.
d) Pour le télétravail, des procédures d'authentification en deux étapes (basées sur la possession et les connaissances) devraient si possible être mises en œuvre. Cela peut être le cas pour les accès au CD via le STR.
e) Le télétravail, p. ex. à des fins de maintenance des fabricants avec des procédures d'authentification «triviales», n'est pas autorisé.
f) Aucune connexion aux autres interfaces du CD n'est possible via l'interface.
g) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
h) Une perturbation de l'interface n'a aucune influence sur les autres interfaces.
i) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.4.2.3 Interface IC1

a) Via cette interface, le CD se connecte uniquement à l'interface WAN correspondante des autres appareils de mesure dans le LMN.
b) La communication est si possible cryptée au niveau de protocole adapté. Les algorithmes utilisés sont régulièrement contrôlés selon l'état de la technique ou remplacés rapidement en cas de compromission identifiée.
c) Aucun rôle d'utilisateur n'est disponible pour l'accès à cette interface. L'administrateur de CD configure les connexions
d) Les données de comptage des appareils à l'interface **IC1** sont transmises par le module de communication uniquement via l'**IC3**, sans traitement des données dans le CD, mais avec conversion de protocole et cryptage le cas échéant.
e) Aucune connexion aux autres interfaces du CD n'est possible via l'interface.
f) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
g) Une perturbation de l'interface n'a aucune influence sur les autres interfaces.
h) Les tentatives d'accès non autorisés et d'autres perturbations que peut détecter le composant principal correspondant dans le cadre des protocoles utilisés au niveau de l'interface, déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.4.3 Exigences spécifiques

5.4.3.1 Utilisation du cryptage

a) Chaque appareil reçoit une clé de livraison individuelle. Celle-ci est remplacée par une nouvelle clé à la première mise en service suivant l'enregistrement réussi.
b) Lors du changement de CD, la clé de livraison doit être réactivée.

c) Le cryptage est réalisé avec une technologie considérée comme sûre au moment de la livraison.
d) La technologie de cryptage peut être mise à jour.
e) Les clés de cryptage sont protégées contre tout accès non autorisé dans tous les appareils et systèmes.

5.4.3.2 Réglages de l'heure

a) Pour l'accès à cet objet via l'interface IC0, le rôle d'utilisateur «administrateur CD» est utilisé conformément aux droits d'accès correspondants.
b) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe.
c) La modification du réglage de l'heure dans le CD déclenche un message au gestionnaire de données et est reprise dans les données de journal.
d) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du système GDC et ces résultats sont repris dans les données de journal.

5.5 Exigences relatives au STR

(1) Le système de tête de réseau est un composant principal du SMI au sens de la définition à la section 2.3. Il permet aux différents rôles et aussi aux processus automatisés du GDC chez le gestionnaire de données d'accéder aux composants principaux du SMI.

a) Par conséquent, des exigences de sécurité s'appliquent à ces interfaces externes proposées aux rôles chez le gestionnaire de données au même niveau que pour d'autres composants principaux.

(2) L'interface WAN du STR revêt une importance colossale. Elle relie le composant principal STR aux autres (AMI ou CD) via le transfert de données à distance.

b) Cette connexion doit présenter le niveau de sécurité des composants principaux.

(3) Le STR dispose de l'interface externe WAN et, le cas échéant, de plusieurs interfaces externes locales différentes:

- pour la configuration du système locale et à distance (fonctionnement régulier; interface homme-machine, MMI – Man Machine Interface)
- pour le transfert de données automatisé du SMI au gestionnaire de données (fonctionnement régulier; API, ou autres)
- pour les autres (p. ex. technicien d'assistance du fabricant, ou autres).

c) Les interfaces externes locales doivent présenter le même niveau de sécurité que les composants principaux.

(4) En fonction de l'étendue de la livraison du fabricant, le STR comprend au moins l'application STR, mais peut également se composer, en tant que système autonome, de matériel informatique, d'un système d'exploitation et d'une application.

5.5.1 Exigences relatives au fonctionnement sûr

5.5.1.1 Livraison et première mise en service

(1) Les numéros de version et les licences du logiciel (composants individuels le cas échéant) sont documentés.

5.5.1.2 Redémarrage sécurisé

a) Après la première mise en service, le système d'exploitation de la plateforme informatique du STR est en mesure d'adopter le mode de fonctionnement prévu à chaque nouveau démarrage.
b) Les menus de démarrage sont accessibles uniquement aux administrateurs habilités.
c) Le démarrage des supports de données externes est impossible.
d) Si le système constate un redémarrage défectueux, un message d'erreur est émis et une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal.

5.5.1.3 Démarrage sécurisé de l'application STR

a) Après la première mise en service, l'application STR est en mesure d'accéder au mode de fonctionnement prévu à chaque nouveau démarrage.
b) Si l'application constate un redémarrage défectueux, un message d'erreur est émis et une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal.
c) L'application STR est en mesure d'exécuter un contrôle d'intégrité sur elle-même. En cas de contrôle d'intégrité erroné, un message d'erreur est émis et une alarme est déclenchée auprès du gestionnaire de données, ces résultats sont repris dans les données de journal.

5.5.1.4 Protection de la mémoire

a) Le système d'exploitation de la plateforme informatique permet la gestion de l'espace de stockage, de sorte que, dans la mémoire volatile de cet ordinateur, les espaces d'adressage sont réservés exclusivement pour les applications correspondantes.
b) Les espaces de stockage où sont enregistrées provisoirement les données de comptage ou les clés de cryptage sont récupérés après leur utilisation par un écrasement ciblé.

5.5.1.5 Suppression sécurisée

a) Les données vulnérables qui ont été enregistrées sur des supports de données sont rendues physiquement illisibles par la réécriture multiple avec des données aléatoires, et ce via un processus conforme à l'état de la technique (BSI (Allemagne), DoD (États-unis) ou autres). Les supports de données persistants (p. ex. CD-ROM) sont rendus illisibles conformément à ces exigences.

5.5.1.6 Journalisation

a) Tous les événements du système relevant de la sécurité des données sont repris dans les données de journal.
b) Les données de journal peuvent être lues uniquement par des utilisateurs autorisés à le faire.
c) Les données de journal sont sécurisées contre toute modification ou suppression non autorisée.

d) Le type et l'étendue des données à enregistrer ne sont pas l'objet du présent document. Ils sont plutôt définis par la mise en œuvre technique d'un SMI ou d'un composant principal de ce dernier, et notamment par la gestion du gestionnaire de données. La journalisation permet au minimum de répondre aux exigences spécifiées au [4].

Les fabricants doivent adapter l'étendue des données à enregistrer en fonction des exigences des exploitants.

5.5.1.7 Mise à jour du micrologiciel

a) Pour la mise à jour d'une application STR, les droits d'administrateurs système (aucun rôle pris en compte dans le présent document) sont requis au niveau de la plateforme informatique correspondante.

5.5.2 Interfaces

5.5.2.1 Interface WAN

a) Via cette interface, le STR se connecte uniquement avec l'interface correspondante **IC3** de l'AMI et du DC ou de la passerelle.
b) La communication est cryptée au niveau de protocole adapté. Les algorithmes utilisés sont régulièrement contrôlés selon l'état de la technique ou remplacés rapidement en cas de compromission identifiée.
c) Aucun rôle d'utilisateur n'est défini pour l'accès à cette interface.
d) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
e) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès gestionnaire de données et ces résultats sont repris dans les données de journal.

5.5.2.2 Interfaces locales du STR

5.5.2.2.1 Homme-machine

a) Pour l'accès à ces interfaces, au moins les rôles d'utilisateurs «administrateur» et «opérateur» sont disponibles.
b) L'attribution des droits d'accès granulaires pour l'administrateur STR, l'administrateur AMI, l'administrateur CD, l'opérateur, le gestionnaire de coupe-circuit et l'assistance du fabricant doit être effectuée conformément à la topologie correspondante.
c) L'authentification s'effectue au minimum via le nom d'utilisateur et le mot de passe. Si un composant principal prend en charge le télétravail, des procédures d'authentification solides (basées sur la possession et les connaissances) doivent être mises en œuvre.
d) L'interface est renforcée contre les attaques, telles que le déni de service, le rejeu, le débordement de tampon, etc.
e) Les tentatives d'accès non autorisés et d'autres perturbations déclenchent une alarme auprès du gestionnaire de données et ces résultats sont repris dans les données de journal.

5.5.2.2.2 Machine-machine (SMI-GDC)

a) Puisque la forme de l'architecture du GDC est très différente en fonction du fabricant, les points suivants doivent être considérés comme des recommandations.

b) Cette interface permet le transfert automatisé des données de comptage depuis le SMI vers le STR du gestionnaire de données. En tant qu'interface externe du STR, l'exigence fondamentale consiste à empêcher tout accès non autorisé au STR.
c) Aucun rôle d'utilisateur n'est par conséquent défini pour l'accès à cette interface.
d) En fonction de la forme de l'interface, les données de comptage sont exportées dans un format configurable. Le transfert a lieu dans le domaine du gestionnaire de données. Les données transmises depuis le SMI sont donc protégées, sur le plan de la sécurité des données et de la protection des données, par les fonctions de protection des systèmes traitant les données pour le transfert et le traitement ultérieurs.

5.5.3 Exigences spécifiques

a) L'administrateur STR configure le STR.
b) L'administrateur AMI et l'administrateur CD (ou passerelle) configurent les composants principaux correspondants du SMI depuis le secteur du gestionnaire de données.
c) L'opérateur peut également accéder de manière ciblée aux données de comptage dans l'AMI déterminé pour le transfert des données automatisé.
d) Le gestionnaire de coupe-circuit supprime le coupe-circuit dans l'AMI du domaine du gestionnaire de données et prépare la réinitialisation.
e) L'assistance du fabricant configure les composants principaux correspondants hors du domaine du gestionnaire de données uniquement s'ils ne sont pas opérationnels.
f) En principe, les composants principaux sont configurés dans un état de fonctionnement régulier exclusivement par les rôles d'utilisateurs correspondants du gestionnaire de données.
g) Le STR peut avoir à transférer des messages d'autres composants principaux aux utilisateurs correspondants chez le gestionnaire de données, et ce sur la base des règles.

5.5.4 Exigences générales

5.5.4.1 Environnement opérationnel

a) En fonction de l'étendue de la livraison du STR (logiciel ou appareil (matériel et logiciel)), conformément à la section 5.5, un environnement d'exploitation fiable doit être garanti par le gestionnaire de données. Cela comprend la configuration de la plateforme informatique, la reprise des rôles d'utilisateurs spécifiques au STR et les attributions adaptées des rôles d'utilisateurs correspondants du gestionnaire de données.
b) Il est de la responsabilité du gestionnaire de données de garantir que les accès aux composants principaux à distance à des fins de maintenance par le fabricant présentent le même niveau de sécurité que ceux des accès à des fins de maintenance depuis le domaine du gestionnaire de données (idéalement: authentification à deux facteurs à un STR et connexion cryptée sans interruption aux composants principaux à distance).

5.5.4.2 GDC / GDE

a) Si le STR exporte des données de comptage de manière automatisée, les interfaces correspondantes vers les systèmes GDE doivent être supportées.
b) Cela ne doit pas entraîner une compromission du niveau de sécurité du STR.

5.6 Exigences relatives à la plateforme de visualisation

5.6.1 Interface des clients finaux (plateforme de visualisation locale)

5.6.1.1 Identification et authentification

a) Au moins une solution avec le nom d'utilisateur et le mot de passe est mise en œuvre sur l'AMI. Elle peut être conçue pour un auto-enregistrement du prosumer.

5.6.1.2 Contrôle d'accès

a) Les droits d'accès sont définis au niveau de l'interface concernant le rôle de prosumer pour tous les objets vulnérables.

5.6.1.3 Dissociation des interfaces

a) L'interface pour la plateforme de visualisation doit être dissociée des autres interfaces de l'AMI.
b) Les données de comptage pour la visualisation sont préparées de manière adaptée par l'AMI, et le rôle de prosumer n'a qu'un accès en lecture aux données à visualiser.

5.6.2 Plateforme de visualisation à distance

5.6.2.1 Identification et authentification

a) Pour tous les accès à la plateforme de visualisation, le prosumer s'authentifie sur le système correspondant du gestionnaire de données. Une procédure d'authentification en deux étapes (basée sur la possession et les connaissances) doit si possible être mise en œuvre.

5.6.2.2 Contrôle d'accès

a) Les droits d'accès sont définis au niveau de l'interface concernant le rôle de prosumer pour tous les objets vulnérables.

5.6.2.3 Cryptage

a) La communication entre le prosumer et la visualisation à distance est cryptée de bout en bout.

5.6.2.4 Architecture

a) Les données sont obtenues à partir de la GDC et un transfert sécurisé doit être établi entre la GDC (unilatéral) ou un composant des systèmes de niveau supérieur (bidirectionnel) et la plateforme de visualisation à distance.

5.6.2.5 Plateforme de visualisation à distance

(1) La plateforme de visualisation à distance offre au prosumer, le cas échéant, un accès interactif à son partenaire contractuel. Une partie de la fonctionnalité consiste toutefois dans la visualisation de données de consommation.

a) La personnalisation de ces données pour le prosumer autorisé en conséquence s'effectue dans le STDC, mais pas par le STR ou un autre composant principal.

b) Par conséquent, l’intégrité des données propres au prosumer doit être garantie depuis le STR.
c) Parallèlement, la visualisation des données doit être confidentielle pour le prosumer.
d) Toute modification non autorisée des données de consommation visualisées (p. ex. par le prosumer) est exclue.

6. Exigences relatives à la gestion de clés

(1) Les composants principaux du SMI ainsi que d'autres compteurs utilisent des clés cryptographiques pour protéger différents processus. Actuellement et pour une durée définie, beaucoup de ces appareils ne disposent pas de suffisamment de puissance de traitement ou d'espace de stockage pour les applications cryptographiques complexes ou la gestion de clés complète. Par conséquent, ils doivent être équipés d'une autre manière de clés adaptées correspondantes. L'intégralité des clés se trouvant dans un SMI doit être gérée notamment par une gestion de clés. Ce processus s'effectue en dehors de l'objet de contrôle «STR», mais dans le STDC. Il en résulte donc les exigences minimales suivantes. Selon l'architecture spécifique aux produits correspondante, un contrôle est réalisé, non pas en fonction d'une exigence générique, mais sur la base des informations des fabricants concernant les aspects suivants.

a) La gestion de clés couvre l'ensemble du cycle de vie de toutes les clés cryptographiques dans le système global:

   - Génération
   - Répartition
   - Verrouillage
   - ICP pour la cryptographie basée sur les certificats

b) Il doit y avoir une protection adaptée contre les accès non autorisés.
c) Un matériel-clé préinstallé sur les composants principaux sert exclusivement à la mise en service, il ne doit pas être appliqué en fonctionnement, et il doit être remplacé par des clés à appliquer de façon opérationnelle lors de la mise en service.
d) L'utilisation de clés triviales n'est pas admise.
e) L'utilisation de clés de groupes n'est pas admise, excepté lors de la diffusion.
f) Les rôles d'utilisateurs pour la gestion de clés doivent être définis par le fabricant correspondant, outre ceux présentés à la section 5.1.1. L'introduction de clés peut être réalisée par maintenance à distance ou localement sur les appareils. Des fonctions de sécurité adaptées pour la protection contre tout accès non autorisé au matériel-clé sont mises en œuvre.
g) Les algorithmes cryptographiques et les longueurs de clés correspondent respectivement à l'état de la technique. La durée de vie est également définie, et il existe un calendrier obligatoire pour les mises à jour et les mises à niveau. En cas de compromission connue des algorithmes ou des longueurs de clés, des mises à jour et des mises à niveau sont réalisées rapidement.
h) Les clés cryptographiques sont générées par des composants correspondants à l'état actuel de la technique.

Glossaire

Exemple de l'administration fédérale: Clés et algorithmes pour «INTERNE», état juillet 2017; source: Unité de pilotage informatique de la Confédération (UPIC)

Domaine	Application / Protocole	Algorithme /	Valeurs minimales	Remarques
Cryptage	symétrique	AES	128 bits	Cryptage de transport: Galois Counter Mode GCM Localement: Cipher Block Chaining Modus CBC Cryptage par flux: Counter Mode CTR
	asymétrique	RSA, ElGamal	2048 bits	ECC
Fonctions de hachage		SHA-2, SHA-3	Valeur H 256 bits	SHA-1 et MD5 non admis
Authentification des données	chiffré et authentifié	AES dans GCM		
	uniquement authentifié	HMAC avec SHA-2 ou SHA-3		Keyed-Hash Message Authentication Code
Signature électronique		RSA, DSA	2048 bits	Importance des paires de clés de niveau élevé
		ECDSA	256 bits	
Échange de clés	Diffie-Hellmann Ephemeral (DHE)	Perfect Forward Secrecy (PFS)	2048 bits	PFS contre les attaques par rejeu
Transport Layer Security (TLS)	Échange de clés	DHE	2048 bits	
		ECDHE	256 bits	
	Transfert de données	Authenticated Encryption with Additional Data (AEAD)		p. ex. AES dans GCM Secure Sockets Layer (SSL) uniquement dans des cas exceptionnels justifiés
Secure Shell (SSH)	Échange de clés DH avec Group-Exchange			Version 2 Version 1 uniquement dans des cas exceptionnels justifiés CTR et GCM CBC uniquement dans des cas exceptionnels justifiés
VPN	IPsec (Internet Protocol Security)	Internet Key Exchange (IKE)		Échange de clés IKEv2 IKEv1 uniquement dans des cas exceptionnels justifiés Pre-shared Keys 20 caractères avec caractère spéciaux
	OpenVPN			Basé TLS
WLAN	WPA2			WPA et WEP uniquement dans des cas exceptionnels justifiés Wi-Fi Protected Setup (WPS) non admis

Bluetooth				au moins la version 2.1 en mode Security 4 Bluetooth LE3 (ab v4.0) =Security Mode 1 Level 3 «Just Works» pour l'appariement non admis (attaque M-i-t-m)

Abréviations et définitions

ABP	Analyse des besoins de protection
AES	Association des entreprises électriques suisses
AMI	Appareil de mesure intelligent
API	*Application Programming Interface,* interface de programmation
BSI	Office fédéral allemand de la sécurité en matière de technologies de l'information
CD	Concentrateur de données
Coupe-circuit	Contact de disjoncteur dans l'AMI
CPL	Courants porteurs en ligne
DoD	United States Department of Defense, Département de la défense des États-Unis
DSsquare	DS désigne la protection des données et la sécurité des données; en anglais, *square* signifie entre autres «conforme»
GDC	Gestion des données de compteur; dans ce document: traitement des données de comptage au-delà du composant principal STR du SMI
GDE	Gestion des données énergétiques
GRD	Gestionnaire de réseau de distribution
HAN	*Home Area Network*, réseau domestique
I&A	Identification et authentification
ICP	Infrastructure à clés publiques (pour applications de cryptage asymétrique)
IPsec	*Internet Protocol Security*, communication sécurisée par le cryptage via les réseaux IP comme Internet
Journalisation	*Logging* en anglais: permet de conserver la trace de certains événements en vue de vérifications ultérieures et de reconstituer des informations et des traitements après une panne ou un autre dysfonctionnement.
LAN	*Local Area Network*, réseau local
LMN	*Local Metrological Network*, réseau métrologique local
METAS	Institut fédéral de métrologie
MID	Measuring Instruments Directive (Directive sur les instruments de mesure 2004/22/CE)
multi-tenant	Technique d'information qui peut servir plusieurs tenants, donc clients ou mandants, sur la même plateforme ou le même système logiciel, sans visualisation mutuelle de leurs données, de leur gestion des utilisateurs et similaires
OFEN	Office fédéral de l'énergie
Relais	Contact de commande dans l'AMI
RU	Royaume-Uni
SGD	Système de gestion de la distribution
SGSI	Système de gestion de la sécurité d'information
SIC	Système d'information de la clientèle
SMI	Système de mesure intelligent
SR	Scénario de risque
STR	Système de tête de réseau, *Head End System*
TB	Tarif bas
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP)
TH	Tarif haut
TI	Technique d'information
TIC	Technologies de l'information et de la communication
TLS	*Transport Layer Security* (anciennement: *Secure Sockets Layer*, SSL)
WAN	*Wide Area Network,* réseau étendu

WLAN	*Wireless LAN,* réseau local sans fil