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

Directives pour la sécurité des données des systèmes de mesure intelligents, annexe 2

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

RL-DSP – CH, annexe 2, 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

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, également souvent désigné «Exigences minimales» définit l'architecture d'un système de mesure intelligent (SMI) (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) En outre, des composants de sécurité et de protection des données doivent de plus être pris en compte pour le système global:

- Meter Data Management System
- Systèmes de visualisation
  - localement sur l'AMI (art. 8a, al. 1, let. a, 3.) en tant qu'interface
  - via une plateforme Web
- Appareil de lecture et de configuration
- Infrastructure de serveur, de réseau et de sécurité
- Système de gestion pour la clé cryptographique, etc. en tant qu'ancrage de sécurité centra
- Systèmes de niveau supérieur pour le traitement des données

(5) Aucun contrôle de sécurité des données n'est requis pour le gestionnaire de données, conformément à l'art. 8b. Les présentes exigences nécessitent toutefois un contrôle interne et externe dans des secteurs définis.

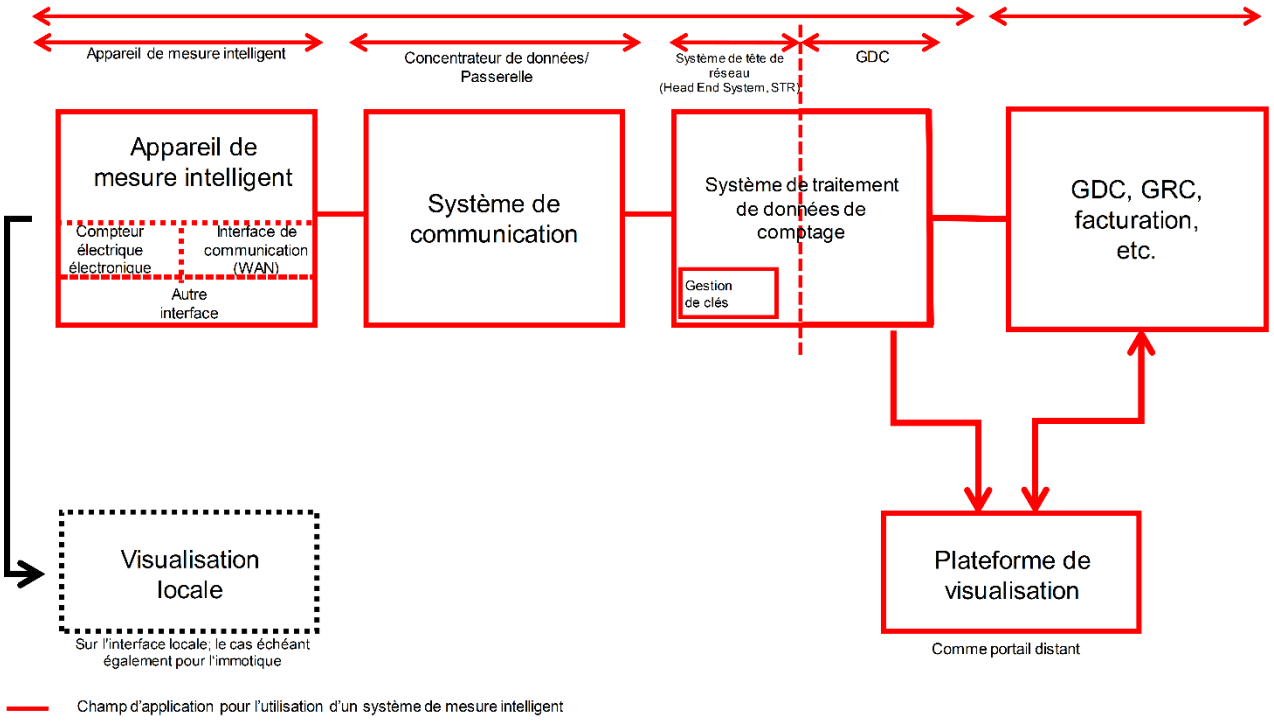

Figure 1 Champ d'application du système de mesure intelligent pour le gestionnaire de données

(6) Pour le système global représenté à la figure 1, il convient de garantir que le gestionnaire de données (les exploitants des systèmes de smart metering) puisse non seulement recourir à des composants principaux fiables du point de vue de la sécurité des données, mais qu'il dispose également de la qualification pour mettre en œuvre, déployer et exploiter de façon fiable les systèmes correspondants dans leur environnement informatique.

(7) Dans ce système global, aucune exigence de sécurité à l'échelle de l'entreprise n'est explicitement prise en compte, notamment les aspects de sécurité stratégiques, tactiques, organisationnels ou personnels.

1.1 Bases

Utilisation des documents

(1) Le présent document contient en principe des exigences sur la mise en œuvre, le déploiement et l'exploitation du système de mesure intelligent (SMI).

(2) L'annexe 1 contient en principe des exigences sur les composants principaux du SMI et donc directement sur les fabricants de ces derniers. Les exigences sont mises en œuvre dans l'architecture et la fonctionnalité des composants principaux, et l'exactitude et l'efficacité sont justifiés par un contrôle de conformité des données. Le contrôle de conformité validé des composants principaux appareil de

mesure intelligent, système de communication et STR indique que le gestionnaire de données peut exploiter de manière sécurisée les systèmes de mesure intelligents.

Aspects complémentaires

(1) La gestion de clés en guise de sous-système du système de traitement des données de comptage (STDC) est également contrôlée pour vérifier que les exigences formulées dans l'annexe 1 sont respectées. Les processus opérationnels de gestion de clés relèvent également de la responsabilité du gestionnaire de données.

(2) Le respect des exigences en matière de sécurité des données et de protection des données doit être garanti par l'exploitant de la visualisation à distance. Si la visualisation à distance présente un trafic de 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.

(3) La sécurité des données et de protection des données doit être garanti par l'éditeur d'une visualisation locale.

2. Les exigences traitent les objets de protection pertinents et les menaces

(1) Les composants principaux du système de mesure intelligent sont certifiés. Les exigences concernant la certification découlent de l'analyse des besoins de protection (ABP). Pour qu'une sécurité globale du système de mesure intelligent soit garantie de la même manière pendant la mise en service, l'exploitation et après la mise hors service des composants principaux, les exigences suivantes concernant le gestionnaire de données sont définies. Les exigences s'appliquent en outre, au sens de la sécurité des données et de la protection des données des systèmes de mesure intelligents, aux systèmes périphériques que le gestionnaire de données met en œuvre et exploite.

(2) Les exigences relatives au système de mesure intelligent traitent les risques exposés de l'ABP et ont été établies sur la base des normes de sécurité reconnues sur le plan international ISO/CEI 27002/27019. Les thèmes, contrôles et critères qui limitent les risques lors de la mise en œuvre, le déploiement et l'exploitation d'un système de mesure intelligent ont été sélectionnés. Les thèmes suivants font partie des exigences concernant le gestionnaire de données:

- Exigences relatives à la gestion des ressources
- Exigences relatives au contrôle d'accès
- Exigences relatives à la gestion de clés
- Exigences relatives à la sécurité physique et à la sécurité des appareils
- Exigences relatives à une exploitation des TIC sûre
- Exigences relatives à la sécurité de communication
- Exigences relatives aux relations des fournisseurs de systèmes
- Exigences relatives à la gestion des incidents relatifs à la sécurité des informations
- Exigences de conformité

(3) Les thèmes liés à la gouvernance à l'échelle de l'entreprise, qui limitent certes aussi les risques mais sont mis en œuvre par le gestionnaire de données également pour d'autres domaines pertinents pour la sécurité (gestion des données des collaborateurs ou protection de base des environnements de technologie opérationnelle p. ex.) ne font explicitement pas partie des exigences suivantes. Les thèmes ci-dessous ne font donc pas partie des exigences suivantes concernant le gestionnaire de données:

- Exigences relatives à la politique de sécurité des informations
- Exigences relatives à l'organisation de la sécurité des informations
- Exigences relatives à la sécurité du personnel
- Exigences relatives à le «Business Continuity Management»

(4) De plus, le développement sécurisé des systèmes n'est pas abordé puisque les composants principaux garantissant cet aspect sont fournis avec un certificat. En cas d'éventuels développements propres de systèmes périphériques, le gestionnaire de données doit définir des exigences complémentaires relatifs à la sécurité du développement.

(5) Les rôles génériques du gestionnaire de données sont définis ci-après. Ils sont à considérer comme des responsables de mise en œuvre possibles mais peuvent aussi, dans la pratique, porter d'autres noms ou être définis par un fournisseur:

- Responsable des ressources: comme son nom l'indique, ce rôle organisationnel est responsable d'une ressource ou d'un groupe de ressources. Les ressources, ou biens, peuvent être des composants techniques, mais aussi des informations ou des processus. Responsables des ressources typiques dans la sécurité des informations: le propriétaire des données ou le responsable des applications.
- Utilisateur: sur le principe, on fait la distinction entre les rôles des utilisateurs du côté du gestionnaire de données («utilisateurs»), des clients («utilisateurs finaux») et des administrateurs.
- Gestionnaire de coupe-circuit: le gestionnaire de coupe-circuit est un rôle technique. Ce rôle a le droit de commander les ordres de coupe-circuit. Dans le SMI, il s'agit d'une fonction privilégiée.
- Gestionnaire de relais: le gestionnaire de relais est un rôle technique. Ce rôle a le droit de régler et de commander les ordres de relais. Dans le SMI, il s'agit d'une fonction privilégiée.

(6) Le «Security Rational» détaillé, à savoir la justification détaillée du choix des thèmes, contrôles et critères sélectionnés pour les exigences suivantes et des risques issus de l'ABP ainsi traités, peut être consulté sur demande auprès de l'AES.

3. Exigences relatives à la gestion des ressources

3.1 Inventaire et responsabilité des ressources

Objectif:	Identification des ressources (informations, composants matériel et logiciel) dans le système de mesure intelligent et définition des tâches et responsabilités.

Inventaire des ressources

Control 3.1.1 **Smart meter**

(1) Tous les appareils de mesure intelligents doivent être identifiés par le gestionnaire de données et consignés dans un inventaire, qui doit être mis à jour en permanence.

Chaque smart meter doit être clairement identifiable.
L'inventaire doit au moins indiquer l'emplacement d'installation, la version du micrologiciel et le numéro de série.
L'inventaire doit être vérifié chaque année par échantillons.

Control 3.1.2 **Système de communication**

(1) Tous les composants des systèmes de communication doivent être identifiés par le gestionnaire de données et consignés dans un inventaire, qui doit être mis à jour en permanence. Les composants de communication du matériel relevant de la responsabilité opérationnelle du gestionnaire de données, comme *les modems PLC ou les modules de communication SIM* mais également les services de prestataires, doivent être ajoutés à l'inventaire.

a) Chaque élément doit être clairement identifiable.
b) L'inventaire doit au moins indiquer l'emplacement d'installation, la version du micrologiciel et le numéro de série.

Control 3.1.3 **Système de traitement des données de comptage**

(1) Tous les systèmes traitant les données de comptage doivent être identifiés par le gestionnaire de données et consignés dans un inventaire, qui doit être mis à jour en permanence. Les infrastructures de serveur, de sécurité et de réseau sous-jacentes doivent également être ajoutées à l'inventaire.

a) Chaque composant (matériel et logiciel) doit être clairement identifiable.
b) L'inventaire doit au moins indiquer la (les) version(s) du logiciel et du système d'exploitation.

Control 3.1.4 **Appareil de lecture et de configuration**

(2) Tous les appareils de lecture et de configuration doivent être identifiés par le gestionnaire de données et consignés dans un inventaire, qui doit être mis à jour en permanence.

a) Chaque appareil de lecture et de configuration doit être clairement identifiable.
b) L'inventaire doit au moins indiquer la version du logiciel et du système d'exploitation, le propriétaire (collaborateur) ainsi que le numéro de série.

Responsabilités des ressources

Control 3.1.5 **Smart meter**

(1) Chaque composant de l'inventaire des appareils de mesure intelligents doit disposer, en fonctionnement, d'un responsable des ressources.

a) Le responsable des ressources doit garantir que ses appareils de mesure intelligents ou les données sont correctement classifiés ou protégés.
b) Le responsable des ressources doit soumettre l'inventaire à une révision annuelle basée sur des échantillons.
c) Le responsable des ressources est responsable de la destruction correcte de ses appareils de mesure intelligents après leur mise hors service.

Control 3.1.6 **Système de communication**

(1) Chaque composant de l'inventaire du système de communication doit disposer, en fonctionnement, d'un responsable des ressources.

a) Le responsable des ressources doit garantir que ses ressources sont correctement classifiées ou protégées.
b) Le responsable des ressources doit soumettre l'inventaire à une révision annuelle basée sur des échantillons.
c) Le responsable des ressources est responsable de la destruction correcte de ses ressources après leur mise hors service.

Control 3.1.7 **Système de traitement des données de comptage**

(1) Chaque composant de l'inventaire du système des données de traitement des données de comptage doit disposer, en fonctionnement, d'un responsable des ressources.

a) Le responsable des ressources doit garantir que ses ressources sont correctement classifiées ou protégées.
b) Le responsable des ressources doit soumettre l'inventaire à une révision annuelle basée sur des échantillons.
c) Le responsable des ressources est responsable de la destruction correcte de ses ressources après leur mise hors service.

Control 3.1.8 **Appareil de lecture et de configuration**

(1) L'inventaire des appareils de lecture et de configuration doit disposer, en fonctionnement, d'un responsable des ressources.

a) Le responsable des ressources doit garantir que ses ressources sont correctement classifiées ou protégées.
b) Le responsable des ressources doit soumettre l'inventaire à une révision annuelle basée sur des échantillons.
c) Le responsable des ressources est responsable de destruction correcte de ses ressources après leur mise hors service.

Restitution des ressources

Control 3.1.9 **Système de communication**

(1) Les outils pour l'installation et l'exploitation de systèmes de communication et les informations utilisées à cet effet doivent être restitués après la cessation des rapports de travail et l'expiration des contrats.

a) La restitution doit être réalisée de façon avérée et doit être contrôlée par le responsable des ressources auprès du gestionnaire de données.
b) Un accord de restitution doit être signé par le propriétaire des informations et des outils.

Control 3.1.10 **Appareil de lecture et de configuration**

(1) Les appareils de lecture et de configuration pour l'installation et le paramétrage de l'appareil de mesure intelligent et les informations utilisées à cet effet doivent être restitués après la cessation des rapports de travail et l'expiration des contrats.

a) La restitution doit être réalisée de façon avérée et doit être contrôlée par le responsable des ressources auprès du gestionnaire de données.
b) Un accord de restitution doit être signé par le propriétaire de l'appareil.

3.2 Classification des informations

Objectif:	Garantir que les informations sont protégées en fonction de leur besoin de protection.

Classification des informations

Control 3.2.1 **Exigence de protection globale**

(1) Les gestionnaires de données en tant que responsables opérationnels de systèmes de mesure intelligents doivent classifier leurs informations confidentielles – notamment les informations personnelles.

a) La classification doit posséder une gradation claire des informations confidentielles et donc présenter des contrôles d'accompagnement en vue de la protection des informations.
b) La classification de toutes les informations doit être adaptée en cas de modifications dans le système (par exemple ajout de nouveaux cas d'usage).

Identification des informations

Control 3.2.2 **Exigence de protection globale**

(1) Les informations classifiées de manière confidentielle doivent être protégées en conséquence.

a) Les accès doivent être gérés conformément à la section *Exigences relatives au contrôle d'accès.*
b) Les données doivent être cryptées conformément à la section *Exigences relatives à la gestion de clés.*

Control 3.2.3 **Appareil de lecture et de configuration**

(2) Des informations classifiées de manière confidentielle doivent également être protégées en conséquence.

a) Les données classifiées de manière confidentielle doivent être enregistrées uniquement de façon cryptée sur les appareils de lecture et de configuration.
b) Les dispositifs doivent être protégés au moins avec un code PIN/mot de passe personnel.
c) Les dispositifs doivent être protégés par un compte individuel pour chaque utilisateur.
d) Les appareils doivent pouvoir être verrouillés individuellement, p. ex. avec un système de gestion des terminaux mobiles.

3.3 Gestion des supports amovibles et télétravail

Objectif:	Garantir que le besoin de protection défini des informations est également appliqué correctement sur les systèmes périphériques.

Utilisation de supports amovibles

Control 3.3.1 **Système de communication**

(1) Le gestionnaire de données doit définir les processus pour la gestion de dispositifs de stockage mobiles (p. ex. carte SIM des appareils de mesure intelligents ou clés USB).

a) Le processus doit être validé et appliqué.
b) Le processus doit être soumis à un contrôle annuel.

Télétravail, assistance et maintenance à distance

Control 3.3.2 **Exigence de protection globale**

(1) Le gestionnaire de données doit – dès lors qu'elles sont mises en œuvre –, définir et respecter une directive et des mesures de sécurité complémentaires pour le télétravail et l'assistance et la maintenance à distance.

a) Les mesures de sécurité doivent tenir compte de la classification des informations et de la criticité des systèmes auxquels on accède.
b) L'accès doit s'effectuer par une connexion contrôlée par le gestionnaire de données ou dont la sécurité est vérifiée.
c) L'accès doit être crypté et strictement authentifié.
d) Les mesures de sécurité doivent inclure la protection contre les logiciels malveillants et la protection et l'identification des attaques.
e) La lecture de données et l'utilisation de fonctions autorisées doivent être consignées et contrôlées, et la sortie de données et l'utilisation de fonctions non autorisées doivent être empêchées.
f) L'accès des tiers doit aussi être limité dans le temps et enregistré.

4. Exigences relatives au contrôle d'accès

4.1 Exigences commerciales relatives au contrôle d'accès

Objectif: Restriction de l'accès aux ressources (composants et données).

Règlementation du contrôle d'accès

Control 4.1.1 **Exigence de protection globale**

(1) Le gestionnaire de données doit définir et mettre en œuvre un concept d'habilitation en fonction des rôles:

a) Le principe *need-to-know* doit être mis en œuvre. Cela signifie que, pour le contrôle des droits d'accès, chaque utilisateur et chaque administrateur ne peut avoir recours qu'aux bases de données et ne peut exécuter que les programmes qui sont vraiment nécessaires pour le travail (tâche, rôle).

b) Les rôles techniques et non techniques suivants doivent être définis et mis en œuvre en substance dans le concept:

I. Rôles d'administrateurs pour le smart meter, les systèmes de communication, notamment le concentrateur de données et la passerelle, et pour le système de traitement des données de comptage, la visualisation et l'infrastructure informatique en aval, par exemple le serveur, les bases de données ou le pare-feu
II. Releveur de compteur local
III. Releveur de compteur à distance
IV. Gestionnaire de coupe-circuit et gestionnaire de relais
V. Assistance et maintenance fabricant (en fonction des besoins)
VI. Prosumer local
VII. Prosumer visualisation en ligne

c) Toutes les options de connexion sur les composants (au moins les interfaces définies par le fabricant) doivent être prises en compte dans un concept d'habilitation prévu à cet effet.

d) La séparation des pouvoirs entre l'attribution de l'autorisation et l'administration des droits d'accès doit être prise en compte en fonction des possibilités du gestionnaire de données.

e) Un processus pour l'autorisation formelle des requêtes d'habilitation doit être défini.

f) Les habilitations privilégiées peuvent uniquement être attribuées après un processus prédéfini. Une étape de validation supplémentaire doit être définie.

g) Les habilitations doivent être retirées après un processus prédéfini.

h) Les modifications des habilitations de l'utilisateur réalisées par les administrateurs et automatiquement par les systèmes doivent être contrôlées.

i) Le concept d'habilitation doit tenir compte du besoin de protection des informations de façon cohérente, via le système de mesure intelligent.

j) Les habilitations doivent être vérifiées chaque année sur la base d'un échantillon.

Control 4.1.2 **Visualisation**

(1) Le concept d'habilitation doit tenir compte des points suivants:

a) Les habilitations d'accès des utilisateurs finaux aux données de la plateforme de visualisation et de la visualisation locale ne doivent pas être moins restrictives que pour les autres composants sur lesquels se trouvent ces données classifiées (système de traitement des données de comptage p. ex.). Cela vaut pour tous les types d'accès, p.ex. via application Web, application ou dispositifs propriétaires.
b) Les accès des utilisateurs finaux doivent être consignés.

Accès aux réseaux et services réseau

Control 4.1.3 **Exigence de protection globale**

(1) Le gestionnaire de données doit définir et mettre en œuvre une directive pour l'utilisation des réseaux et de leurs services. En principe, les utilisateurs ont uniquement accès aux réseaux et interfaces s'ils y ont été autorisés au préalable.

a) Les accès pour le télétravail ainsi que l'assistance à distance et l'accès à la maintenance sont restreints et doivent être accordés uniquement suite à des requêtes correspondantes.
b) La directive doit définir:
   I. les réseaux, interfaces et services à utiliser
   II. la manière dont apparaît le processus de validation pour ces réseaux, interfaces et services pour les utilisateurs
   III. le mode de contrôle des accès
   IV. le mode d'accès des réseaux
   V. les mécanismes d'authentification et d'autorisation à utiliser
   VI. la surveillance des services réseau
   VII. La directive relative à l'utilisation des réseaux, interfaces ou de leurs services doit se combiner à la directive relative aux contrôles d'accès.

4.2 Administration de l'accès utilisateur

Control 4.2.1 **Exigence de protection globale**

(1) Un processus d'enregistrement des utilisateurs (attribution des rôles) des systèmes de mesure intelligents doit être défini afin que les habilitations correspondantes puissent être attribuées de façon avérée.

a) Les utilisateurs doivent être clairement identifiables (UID).
b) Exception: le rôle de releveur de compteur local (lecture seule) n'est pas impérativement attribué à un utilisateur clair, mais peut être défini via les appareils de lecture et de configuration identifiés (à des fins de lecture exclusivement). Dans ce cas, il faut pouvoir suivre quel utilisateur dispose de quel appareil à quel moment.

Control 4.2.2 **Smart meter**

(1) Le processus (voir 4.2.1) doit par ailleurs tenir compte des points suivants:

a) Les UID qui ne sont plus utilisés doivent être effacés dans le mois qui suit la cessation des rapports de travail.
b) Les habilitations doivent toujours être attribuées ou supprimées en deux étapes:

1. Les UID sont créés et attribués ou supprimés.
2. Les habilitations (rôles ou droits individuels) sont attribuées à ces UID ou supprimées.

Control 4.2.3 **Visualisation**

(1) Le processus doit par ailleurs tenir compte des points suivants:

a) Les UID qui ne sont plus utilisés doivent être effacés dans le mois qui suit la cessation des rapports de travail.
b) Les habilitations doivent toujours être attribuées ou supprimées en deux étapes:
   1. Les UID sont créés et attribués ou supprimés.
   2. Les habilitations sont attribuées à ces UID ou supprimées.

Attribution de droits d'accès

Control 4.2.4 **Exigence de protection globale**

(1) Les habilitations des utilisateurs pour les systèmes de mesure intelligents peuvent être attribuées uniquement selon un processus défini au préalable.

a) Le processus doit obtenir l'accord du responsable des ressources (selon l'inventaire).
b) Les droits attribués doivent être associés à la séparation des pouvoirs.

Control 4.2.5 **Smart meter**

(1) Le processus doit par ailleurs tenir compte des points suivants:

a) Les habilitations des utilisateurs ne peuvent pas être activées avant que l'accord du responsable des ressources n'ait été obtenu et consigné.
b) Une vue d'ensemble des habilitations doit exister pour chaque UID.

Control 4.2.6 **Système de traitement des données de comptage**

(1) Le processus doit par ailleurs tenir compte des points suivants:

a) Les habilitations des utilisateurs ne peuvent pas être activées avant que l'accord du responsable des ressources n'ait été obtenu et consigné.
b) Une vue d'ensemble des habilitations doit exister pour chaque UID.

Gestion des droits d'accès privilégiés (selon le concept d'habilitation basé sur les rôles)

Control 4.2.7 **Exigence de protection globale**

(1) L'attribution d'habilitations privilégiées pour les systèmes de mesure intelligents doit être soumise à un contrôle étendu.

a) Pour cela, un processus prédéfini contenant un niveau de validation supplémentaire doit être utilisé.
b) Pour les comptes d'administration techniques avec un mot de passe générique, les données d'accès doivent être protégées par un mot de passe modifié chaque année.

c) Les collaborateurs disposant d'habilitations privilégiées doivent signer un accord de confidentialité qui couvre également la période suivant la cessation des rapports de travail.
d) Les activités doivent être consignées.

Control 4.2.8 **Smart meter**

(1) Le contrôle étendu doit par ailleurs tenir compte des points suivants:

a) Les fonctions privilégiées doivent être identifiées et attribuées aux rôles correspondants. Des utilisateurs définis (UID) doivent se voir attribuer ces rôles.
b) Tous les rôles privilégiés doivent être examinés par le responsable des ressources (selon l'inventaire) chaque année (sur la base d'un échantillon).
c) Les habilitations privilégiées ne peuvent être attribuées qu'à des utilisateurs clairement identifiables (UID) avec le rôle correspondant, il en va de même pour les utilisateurs techniques.

Control 4.2.9 **Système de communication**

(1) Le contrôle étendu doit par ailleurs tenir compte des points suivants:

a) Les fonctions privilégiées (administration de pare-feu p. ex.) doivent être identifiées et attribuées aux rôles correspondants. Des utilisateurs définis (UID) doivent se voir attribuer ces rôles.
b) Toutes les habilitations privilégiées doivent être examinées par le responsable des ressources (selon l'inventaire) chaque année (sur la base d'un échantillon).

Control 4.2.10 **Système de traitement des données de comptage**

(1) Le contrôle étendu doit par ailleurs tenir compte des points suivants:

a) Les fonctions privilégiées (administration de base de données p. ex.) doivent être identifiées et attribuées aux rôles correspondants. Des utilisateurs définis (UID) doivent se voir attribuer ces rôles.
b) Toutes les habilitations privilégiées doivent être examinées par le responsable des ressources (selon l'inventaire) chaque année (sur la base d'un échantillon).
c) Les habilitations privilégiées ne peuvent être attribuées qu'à des utilisateurs clairement identifiables (UID) avec le rôle correspondant, il en va de même pour les utilisateurs techniques.

Control 4.2.11 **Visualisation**

(1) Le contrôle étendu doit par ailleurs tenir compte des points suivants:

a) Les fonctions privilégiées (administration de clients p. ex.) doivent être identifiées et attribuées aux rôles correspondants. Des utilisateurs définis (UID) doivent se voir attribuer ces rôles.
b) Toutes les habilitations privilégiées doivent être examinées par le responsable des ressources (selon l'inventaire) chaque année (sur la base d'un échantillon)
c) Les habilitations privilégiées ne peuvent être attribuées qu'à des utilisateurs clairement identifiables (UID) avec le rôle correspondant, il en va de même pour les utilisateurs techniques

Utilisation des mots de passe et moyens d'authentification

Control 4.2.12 **Exigence de protection globale**

(1) L'attribution de moyens d'authentification pour des systèmes de mesure intelligents doit être contrôlée.

a) Les mots de passe doivent être modifiés après la première connexion (cette mesure doit être requise techniquement).
b) Les mots de passe doivent être remplacés via des canaux cryptés. Cette mesure s'applique non seulement aux composants principaux, mais également pour les systèmes périphériques et les plateformes sous-jacentes.
c) Les utilisateurs doivent confirmer la réception des données d'accès.
d) Les mots de passe standard de fabricants / fournisseurs de systèmes doivent être modifiés lors de la première connexion.
e) Les accords de confidentialité de données d'accès doivent être signés par tous les utilisateurs.

Contrôle des droits d'accès

Control 4.2.13 **Exigence de protection globale**

(1) Toutes les habilitations d'utilisateurs du système de mesure doivent être examinées par le responsable des ressources (selon l'inventaire) chaque année (sur la base d'un échantillon).

a) Dès lors que la relation de travail des utilisateurs est modifiée (terme, promotion, changement de fonction), les habilitations doivent être adaptées en conséquence.
b) Les modifications apportées aux comptes utilisateurs privilégiés doivent être consignées.

Suppression ou modification des droits d'accès

Control 4.2.14 **Exigence de protection globale**

(1) Les habilitations d'accès du système de mesure intelligent des utilisateurs, dont le contrat de travail est arrivé à échéance, doivent être supprimées lors de leur départ.

a) Les habilitations d'accès doivent être retirées avant la cessation des rapports de travail dès lors que:
    I. un soupçon d'abus est justifié
    II. l'utilisateur dispose d'un rôle privilégié
    III. les informations présentent un besoin important de protection

4.3 Responsabilités des utilisateurs

Objectif: Les utilisateurs doivent être rendus responsables de la protection de leurs données d'accès.

Utilisation de données d'accès confidentielles

Control 4.3.1 **Exigence de protection globale**

(1) Les données d'accès pour les systèmes de mesure intelligents doivent être traitées de manière confidentielle.

a) Les mots de passe doivent être enregistrés uniquement dans des environnements sécurisés, notamment protégés par mot de passe.
b) Si l'on soupçonne que des personnes non habilitées connaissent un mot de passe, celui-ci doit être immédiatement modifié.
c) Les mots de passe doivent satisfaire aux exigences minimales suivantes (tel que déjà prescrit par les fabricants sur les composants principaux des systèmes):
    I. Le mot de passe utilisateur doit comprendre au moins 10 caractères.
    II. Les mots de passe triviaux comme l'ID utilisateur, le nom, le prénom, la date de naissance, etc., ne doivent pas être utilisés.
    III. Répétition du mot de passe: répétition après 10 changements réussis
    IV. Échecs: max. 10, puis l'ID utilisateur doit être verrouillé.
d) Le mot de passe est personnel et ne doit pas être transmis.
e) Les mots de passe pour les procédures de connexion automatisées doivent satisfaire aux mêmes règlementations de sécurité.

4.4 Contrôle d'accès au système et aux applications

Objectif: Empêcher tout accès non autorisé aux ressources.

Procédure de connexion sécurisée

Control 4.4.1 **Appareils de lecture et de configuration**

(1) L'accès aux appareils de lecture et de configuration doit s'effectuer par une procédure de connexion protégée.

a) 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).
b) Des mesures de sécurité protégeant des attaques de force brutale doivent être mises en œuvre.
c) Les tentatives de connexion réussies ou échouées doivent être enregistrées.
d) Les mots de passe doivent être masqués lors de la saisie.
e) Les mots de passe ne doivent pas être transférés en texte clair via des connexions réseau.
f) Les blocages d'accès au système doivent être activés automatiquement après maximum 15 minutes.

Control 4.4.2 **Smart meter**

(1) L'accès aux appareils de mesure intelligents doit s'effectuer via une procédure de connexion protégée. Pour ce composant principal, cette mesure est garantie par le fabricant.

Control 4.4.3 **Système de communication**

(1) L'accès aux composants du système de communication doit s'effectuer par une procédure de connexion protégée. Pour ce composant principal, cette mesure est garantie par le fabricant.

Control 4.4.4 **Système de traitement des données de comptage**

(1) L'accès aux systèmes de traitement des données de comptage doit s'effectuer par une procédure de connexion protégée. Pour la partie Système de tête de réseau (STR) de ce composant principal, cette mesure est garantie par le fabricant. Pour les parties restantes et les plateformes sous-jacentes, les opérations suivantes doivent se produire:

a) 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).
b) Des mesures de sécurité protégeant des attaques de force brutale doivent être mises en œuvre.
c) Les tentatives de connexion réussies ou échouées doivent être enregistrées.
d) Les mots de passe doivent être masqués lors de la saisie.
e) Les mots de passe ne doivent pas être transférés en texte clair via des connexions réseau.
f) Les blocages d'accès au système doivent être activés automatiquement après maximum 15 minutes.

Control 4.4.5 **Visualisation**

(1) L'accès aux visualisations en ligne doit s'effectuer par une procédure de connexion protégée.

a) Aucune information sensible ne doit être représentée avant la réussite de la procédure de connexion.
b) Les utilisateurs doivent avoir conscience que l'accès aux informations ne doit s'effectuer qu'avec une autorisation validée.
c) 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).
d) Des mesures de sécurité protégeant des attaques de force brutale doivent être mises en œuvre.
e) Les tentatives de connexion réussies ou échouées doivent être enregistrées.
f) Une fois la connexion établie, les informations suivantes doivent apparaître à l'utilisateur:
    I. la dernière connexion réussie
    II. les éventuels derniers échecs de connexion depuis la dernière connexion
g) Les mots de passe doivent être masqués lors de la saisie.
h) Les mots de passe ne doivent pas être transférés en texte claire via des connexions réseau.
i) Les blocages d'accès au système doivent être activés automatiquement après maximum 15 minutes.

Système de gestion des mots de passe

Control 4.4.6 **Exigence de protection globale**

(1) Pour la gestion des mots de passe dans le système de mesure intelligent, il convient d'utiliser des systèmes de gestion des mots de passe. Les systèmes périphériques et les plateformes sous-jacentes doivent respecter les critères suivants:

a) Les mots de passe doivent pouvoir être modifiés manuellement. Le processus doit inclure une confirmation de cette action.
b) Les mots de passe doivent satisfaire à la directive technique conformément au point 4.3.1.
c) Les mots de passe doivent être enregistrés de manière sécurisée.
d) Les mots de passe doivent être modifiés après la première connexion.

Utilisation de programmes utilitaires privilégiés

Control 4.4.7 **Système de traitement des données de comptage**

(1) L'utilisation d'un logiciel d'assistance sur des systèmes de traitement des données de comptage (utilitaires) doit être restreinte et contrôlée:

a) L'utilisation de programmes utilitaires doit être limitée au minimum et devrait être validée par le fabricant.
b) Tous les programmes utilitaires non nécessaires doivent être désactivés ou supprimés.
c) L'utilisation de programmes utilitaires doit être enregistrée.
d) Les processus de validation des programmes utilitaires et de blocage de ces programmes après utilisation doivent être formellement documentés et validés.

5. Exigences relatives à la gestion de clés

5.1 Mesures de contrôle cryptographiques

Objectif: Garantir que les mesures cryptographiques sont utilisées de manière correcte et efficace pour protéger le cryptage et ainsi la confidentialité des données personnelles et de profil, l'authentification des systèmes et l'intégrité des informations et fonctions.

Gestion de clés

Control 5.1.1 **Exigence de protection globale**

(1) L'utilisation et la protection de clés cryptographiques dans des systèmes de mesure intelligents doivent être conformes à une directive prédéfinie.

a) La directive réglemente la gestion des clés du SMI pendant tout le cycle de vie de toutes les clés cryptographiques. Et ce, de la génération au verrouillage, en passant par la répartition.
b) Les directives doivent être validées et appliquées, et être soumises à un contrôle annuel.
c) La directive doit définir concrètement les thèmes suivants:
   I. La génération de matériel-clé cryptographique pour les champs d'application définis
   II. L'utilisation de certificats ICP. L'intégralité des clés figurant dans un SMI doit être gérée par une gestion de clés.
   III. La répartition sécurisée des clés générées et leur activation, qui peuvent s'effectuer localement ou via la maintenance à distance.
   IV. Des fonctions de sécurité adaptées pour la protection contre tout accès non autorisé au matériel-clé sont mises en œuvre. La clé doit être enregistrée de sorte qu'elle ne puisse être lue avant l'activation.
   V. Les processus de modification des clés cryptographiques
   VI. L'utilisation des clés compromises
   VII. La désactivation des clés cryptographiques
   VIII. Le réapprovisionnement des clés perdues / corrompues
   IX. L'archivage des clés cryptographiques
   X. La suppression des clés devenues inutiles
   XI. L'enregistrement des activités dans système de gestion de clés
   XII. Outre l'utilisation de clés privées, la collaboration avec des fabricants / fournisseurs de systèmes de clés publiques doit également être définie.
   XIII. Un matériel clé préinstallé du fournisseur sur les composants principaux ou d'autres compteurs 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 opérationnellement lors de la mise en service.

6. Exigences relatives à la sécurité physique et à la sécurité des appareils

6.1 Espaces sécurisés

Objectif: Empêcher l'accès physique non autorisé pour éviter les dommages et attaques sur les ressources.

Mesures de contrôle d'accès physique

Control 6.1.1 **Exigence de protection globale**

(1) L'accès physique aux systèmes contenant des informations critiques (p. ex. concentrateurs de données) doit être restreint aux personnes habilitées par des contrôles de sécurité.

Control 6.1.2 **Système de traitement des données de comptage**

(1) Les systèmes de traitement des données de comptage doivent se trouver dans des zones protégées des personnes non autorisées au moyen de contrôles d'accès.

a) Le contrôle d'accès doit se composer d'une authentification stricte, p. ex. depuis une carte d'accès (batch), et d'un code PIN.
b) L'accès pour les collaborateurs d'assistance externes doit être limité, autorisé et consigné.
c) Toutes les habilitations d'accès pour les centres de données et les centres opérationnels doivent être contrôlés et adaptés annuellement (sur la base d'un échantillon).

Control 6.1.3 **Visualisation**

(1) Les systèmes de visualisation en ligne doivent se trouver dans des zones protégées des personnes non autorisées, au moyen de contrôles d'accès.

a) Le contrôle d'accès doit se composer d'une authentification stricte, p. ex. depuis une carte d'accès (batch), et d'un code PIN.
b) L'accès pour les collaborateurs d'assistance externes doit être limité, autorisé et consigné.
c) Toutes les habilitations d'accès pour les centres de données et les centres opérationnels doivent être contrôlés annuellement (sur la base d'un échantillon).

6.2 Appareils

Objectif: Empêcher des dommages, pannes, vols ou compromissions des ressources.

Control 6.2.1 **Smart meter**

(1) Le gestionnaire de données garantit que le smart meter ne peut être manipulé pendant le processus d'installation.

Maintenance des appareils

Control 6.2.2 **Exigence de protection globale**

(1) Les systèmes de mesure intelligents doivent être régulièrement soumis à une opération de maintenance afin de garantir leur confidentialité et leur intégrité.

a) Les indications des fabricants concernant les intervalles de maintenance, les exigences et l'étendue de cette dernière doivent être prises en compte.
b) Des travaux de maintenance doivent être réalisés exclusivement par des personnes formées à cet effet.
c) Des opérations de maintenance préventives et correctives, et les erreurs associées, doivent être documentées.
d) Si les composants des systèmes de mesure intelligents doivent être soumis à une maintenance réalisée par des collaborateurs externes, les contrôles en amont doivent garantir qu'aucune information critique ne se trouve plus dans l'appareil.
e) Les appareils doivent être contrôlés après la maintenance pour vérifier l'absence d'éventuelles erreurs de configuration avant de les réutiliser.
f) Cette mesure s'applique également lors de l'installation et de la mise en service de l'appareil de mesure intelligent.

Suppression des ressources

Control 6.2.3 **Exigence de protection globale**

(1) Les composants et informations des systèmes de mesure intelligents ne doivent pas être supprimés sans autorisation préalable, p. ex. à des fins de maintenance.

a) Les collaborateurs (y compris externes) qui sont habilités à disposer d'informations et de composants des systèmes de mesure intelligents doivent être identifiés et formés.
b) Il convient d'indiquer à quel moment les composants
    I. sont supprimés
    II. ont été restitués.

Élimination sécurisée ou réutilisation d'appareils

Control 6.2.4 **Exigence de protection globale**

(1) Avant l'élimination des composants, il convient de vérifier qu'aucune information sensible ne se trouve sur les dispositifs de stockage.

a) Les processus doivent être validés et appliqués, et être soumis à un contrôle annuel.
b) Les données vulnérables qui ont été enregistrées sur des supports de données sont rendues illisibles conformément à l'état de la technique. Les supports de données persistants sont rendus illisibles conformément à ces exigences.

7. Exigences relatives à une exploitation sûre des TIC

7.1 Processus opérationnels et responsabilités

Objectif: Garantir l'exploitation correcte et sûre du système de mesure intelligent.

Gestion des changements

Control 7.1.1 **Exigence de protection globale**

(1) Les modifications des processus et des composants du système de mesure intelligent doivent être contrôlées.

a) Les modifications significatives doivent être enregistrées.
b) Avant de procéder à des modifications dans la production, leur effet sur la sécurité des informations et sur la conformité des composants principaux doit être évalué.
c) La gestion des changements doit prévoir des processus de validation.
d) La gestion des changements doit définir les processus alternatifs et les responsabilités qui peuvent être utilisés si un changement n'est pas exécuté correctement par le gestionnaire de données.

Séparation de l'environnement de développement, de test et d'exploitation

Control 7.1.2 **Exigence de sécurité globale**

(1) Les environnements productifs doivent être séparés de l'environnement de test et d'intégration.

a) Les modifications apportées aux systèmes doivent être testées au préalable dans l'environnement de test avant de mettre en œuvre la modification dans l'instance productive.
b) Des données sensibles, notamment des données personnelles, peuvent être intégrées uniquement dans l'environnement de test si des contrôles de sécurité équivalents prévalent ou si les données ont été anonymisées.

7.2 Protection contre les attaques et logiciels malveillants

Objectif: Garantir la protection du système de mesure intelligent contre les attaques et logiciels malveillants.

Mesures de protection préventives et de détection

Control 7.2.1 **Exigence de protection globale**

(1) Le système de mesure intelligent doit être protégé à l'aide de mesures de prévention et de détection.

a) Les utilisateurs doivent être formés au moins tous les trois ans par des mesures de sensibilisation adaptées.
b) Le gestionnaire de données doit régulièrement compiler et évaluer des informations relatives aux points faibles et aux risques concrets des composants/technologies utilisés provenant de sources fiables et des fabricants.

c) Les informations et notifications relatives aux points faibles potentiels doivent être vérifiées par des processus prédéfinis.
d) Des processus et responsabilités doivent être définis pour le traitement des logiciels malveillants et des attaques. En font notamment partie l'utilisation correcte des mécanismes de protection et la réaction aux logiciels malveillants et aux attaques.

Control 7.2.2 **Smart meter**

(1) Les appareils de mesure intelligents doivent être protégés à l'aide de mesures de détection.

a) Les smart meters doivent être contrôlés périodiquement pour vérifier les fichiers, processus et connexions de communication non autorisés. Les modifications ainsi identifiées doivent être analysées et corrigées avec le fabricant.

Control 7.2.3 **Systèmes de communication**

(1) Les systèmes de communication doivent être protégés à l'aide de mesures détectrices, également sous la responsabilité du gestionnaire de données.

a) Les systèmes doivent être contrôlés périodiquement pour vérifier les fichiers, processus et connexions de communication non autorisés. Les modifications ainsi identifiées doivent être analysées et corrigées par le fabricant.

Control 7.2.4 **Système de traitement des données de comptage**

(1) Les systèmes de traitement des données de comptage doivent être protégés à l'aide de mesures de prévention et de détection.

a) L'utilisation du logiciel non autorisé doit être évitée grâce à des contrôles adaptés (liste blanche).
b) L'utilisation de services et téléchargements non sécurisés doit être évitée grâce à des contrôles adaptés (pare-feu).
c) Les systèmes doivent être contrôlés pour vérifier les fichiers, processus et connexions de communication non autorisés. Les modifications ainsi identifiées doivent être analysées et corrigées par le gestionnaire de données ou le fabricant.
d) Des solutions antivirus doivent être installées et régulièrement mises à jour.

Control 7.2.5 **Visualisations**

(1) La visualisation à distance doit être protégée à l'aide de mesures de prévention et de détection.

a) L'utilisation du logiciel non autorisé doit être évitée grâce à des contrôles adaptés (liste blanche).
b) L'utilisation de services Web non sécurisés doit être évitée grâce à des contrôles adaptés, notamment le pare-feu d'applications Web.
c) Les systèmes doivent être contrôlés pour vérifier les fichiers, processus et connexions de communication non autorisés. Les modifications ainsi identifiées doivent être analysées et corrigées.

7.3 Sauvegarde et récupération

Objectif: Une sécurisation et une récupération adaptées des systèmes, des applications, des configurations et des données pour la protection contre la perte et la garantie d'une récupération rapide.

Control 7.3.1 **Exigence supérieure**

(1) Un processus pour la sauvegarde et la récupération doit être défini.

a) Le processus doit définir la procédure de sauvegarde et de récupération pour les informations, les logiciels, les systèmes, les configurations et clés.
b) La durée de conservation et les exigences de sécurité doivent être définies et satisfaire aux exigences légales.
c) Des tests de récupération doivent être réalisés régulièrement.

7.4 Enregistrement et contrôle

Objectif:	L'identification des événements de sécurité doit être garantie pour pouvoir réagir rapidement aux événements.

Enregistrement des événements

Control 7.4.1 **Smart meter**

(1) Pour les appareils de mesure intelligents, le protocole de sécurité qui enregistre le moment, l'identification de l'utilisateur (UID) ou du système, l'interface concernée et l'événement, doit être activé. Les événements suivants doivent être enregistrés sous cette forme:

a) utilisation des habilitations d'utilisateurs
b) succès et échecs des mises à jour du logiciel
c) succès et échecs de l'authentification
d) tentatives de connexion locales
e) changements de configuration
f) modifications des habilitations
g) structure de connexion
h) manipulation physique
i) et autres événements de sécurité

Control 7.4.2 **Système de traitement des données de comptage**

(1) Pour les systèmes de traitement de données de comptage, le protocole de sécurité qui enregistre le moment, l'identification de l'utilisateur (UID) ou du système, l'interface concernée et l'événement, doit être activé. Les événements suivants doivent être enregistrés sous cette forme:

a) utilisation d'habilitations d'utilisateurs supérieures, notamment la fonction coupe-circuit
b) succès et échecs des mises à jour du logiciel
c) succès et échecs de l'authentification
d) tentatives de connexion locales
e) changements de configuration
f) modifications des habilitations
g) structure de connexion
h) et autres événements de sécurité

Control 7.4.3 **Visualisation**

(1) Pour la plateforme de visualisation, le protocole de sécurité qui enregistre le moment, l'identification de l'utilisateur (UID) ou du système, l'interface concernée et l'événement, doit être activé. Les événements suivants doivent être enregistrés sous cette forme:

a) succès et échecs de l'authentification
b) changements de configuration
c) modifications des habilitations
d) et autres événements de sécurité

Protection des informations de protocole

Control 7.4.4 **Smart meter**

(1) Les protocoles doivent être protégés contre toute modification non autorisée.

a) Les données de journal doivent être lues exclusivement par des utilisateurs autorisés à le faire.
b) Les fichiers de journal doivent être modifiés ou effacés uniquement par des actions autorisées.

Control 7.4.5 **Système de traitement des données de comptage**

(1) Les protocoles doivent être protégés contre toute modification non autorisée.

a) Les données de journal doivent être lues exclusivement par des utilisateurs autorisés à le faire.
b) Les fichiers de journal doivent être modifiés ou effacés uniquement par des actions autorisées.

Control 7.4.6 **Visualisation**

(1) Les protocoles doivent être protégés contre toute modification non autorisée.

a) Les données de journal doivent être lues exclusivement par des utilisateurs autorisés à le faire.
b) Les fichiers de journal doivent être modifiés ou effacés uniquement par des actions autorisées.

7.5 Contrôle du logiciel opérationnel

Objectif: Garantir l'intégrité lors de l'exploitation du système de mesure intelligent.

Installation du logiciel sur les systèmes opérationnels

Control 7.5.1 **Smart meter**

(1) L'installation du micrologiciel sur les appareils de mesure intelligents doit être contrôlée. À cet effet, les processus doivent être documentés et validés de manière formelle. Les points suivants doivent être abordés:

a) Les mises à jour du micrologiciel doivent être réalisées exclusivement par des administrateurs qualifiés avec une autorisation accordée au préalable.
b) Le micrologiciel doit être mis en œuvre dès lors qu'il a été testé sur un système-test séparé, conformément aux processus de gestion des changements.
c) Pour la protection des configurations et documentations, un système de contrôle des versions doit être utilisé.
d) Avant que les changements n'apparaissent sur les appareils productifs, une stratégie de retour en arrière (*rollback*) doit être définie.
e) Les versions précédentes du micrologiciel doivent être conservées en guise d'alternative de traitement de secours (*fallback*).
f) Un journal d'audit pour tous les changements apparaissant dans la production doit être réalisé.
g) Avant de procéder à une mise à niveau du micrologiciel, les exigences opérationnelles et l'effet sur la sécurité des informations doivent être contrôlés pour s'assurer de la sécurité des informations avec le fabricant.

Control 7.5.2 **Système de traitement des données de comptage**

(1) L'installation du logiciel et des systèmes d'exploitation sur les systèmes intelligents de traitement des données de comptage doit être surveillée. À cet effet, les processus couvrant les points suivants doivent être documentés et validés de manière formelle.

a) Les mises à jour du logiciel doivent être réalisées exclusivement par des administrateurs qualifiés avec une autorisation accordée au préalable.
b) Le logiciel ne peut être mis en œuvre qu'une fois qu'il a été testé sur un système-test séparé, conformément aux processus de gestion des changements.

7.6 Gestion des points faibles techniques

Objectif: Éviter l'utilisation des points faibles techniques.

Gestion des points faibles techniques

Control 7.6.1 **Objet de protection global**

(1) Il doit y avoir une surveillance et un contrôle actifs des informations concernant les éventuels points faibles dans les appareils de mesure intelligents par le fabricant et le gestionnaire de données (CERT).

a) Dès lors qu'une faiblesse a été identifiée, le risque y relatif doit être évalué et les correctifs correspondants doivent être installés. Si aucun correctif n'est encore disponible, des mesures de sécurité alternatives doivent être prises en compte et si possible mises en œuvre.
b) La stratégie de communication adaptée quant aux points faibles de sécurité doit être définie.
c) L'opérateur doit vérifier que le fournisseur entretient les processus de vulnérabilité et de gestion des correctifs appropriés.

Restrictions concernant l'installation du logiciel

Control 7.6.2 **Smart meter**

(1) Sur l'appareil de mesure intelligent, seules les fonctions et la configuration minimale requises dans le cas d'usage actuel, correspondantes pour exécuter les tâches, doivent être activées.

Control 7.6.3 **Système de traitement des données de comptage**

(1) Seul le logiciel requis pour exécuter les tâches doit être installé sur chaque système de traitement de données de comptage.

8. Exigences relatives à la sécurité de communication

8.1 Gestion de sécurité des réseaux

Objectif: Garantir la protection de la disponibilité et de l'intégrité des systèmes de communication.

Mesures de sécurité du réseau

Control 8.1.1 **Exigence de protection globale**

(1) Le gestionnaire de données et ses prestataires de services doivent garantir que leurs réseaux ou leurs services réseaux sont protégés contre les accès non autorisés.

a) Les processus et responsabilités pour la gestion des appareils réseau doivent être définis.
b) Les responsabilités pour les réseaux et l'utilisation des outils doivent si possible être dissociées.
c) Des contrôles dédiés pour la protection de la confidentialité et l'intégrité des informations qui sont envoyées via des réseaux publics ou des protocoles sans fil doivent être mis en œuvre (cela s'applique également pour les systèmes périphériques – pour les composants principaux, cela doit être garanti par la conception).
d) Les événements pertinents pour la sécurité des informations doivent être enregistrés et surveillés (enregistrement et contrôle).
e) Les systèmes périphériques doivent être authentifiés sur le réseau.
f) La connexion au réseau pour les composants qui ne sont pas utiles au SMI doit être restreinte.

Sécurité des services réseau

Control 8.1.2 **Exigence de protection globale**

(1) Toutes les interfaces spécifiées du système de mesure intelligent doivent être utilisées uniquement pour les fonctionnalités pour lesquelles elles sont définies;

a) L'utilisation des interfaces doit être surveillée.

Control 8.1.3 **Système de communication**

(1) Les services de communication et leur niveau de réalisation – en particulier pour les services de sécurité – doivent être surveillés, qu'on exécute le service soi-même ou par des tiers. Parmi les services de sécurité figurent:

a) les services d'authentification, le cryptage et les contrôles d'accès
b) les paramètres techniques pour les connexions sécurisées au prestataire

Segmentation des réseaux

Control 8.1.4 **Exigence de protection globale**

(1) Les réseaux doivent être segmentés:

a) Dans l'application dorsale du gestionnaire de données, les composants principaux, notamment le STR, doivent se trouver dans des segments dissociés de la visualisation et des clients.

8.2 Transfert d'informations

Objectif:	Garantir la sécurité des informations échangées via des systèmes externes.

Règlementations et procédures pour le transfert d'informations

Control 8.2.1 **Exigence de protection globale**

(1) Pour le transfert d'informations vers des systèmes externes, il convient de mettre en œuvre des contrôles:

a) Le trafic de données est crypté pour garantir la protection des informations à transférer avant leur interception par des tiers, la copie, la modification et la destruction.
b) Les informations qui sont échangées via des réseaux publics doivent être sécurisées au moyen d'un cryptage des données ou d'une protection de la connexion de données . Il convient ainsi de tenir compte des éléments suivants:
    I. Tous les partenaires de communication doivent être pris en compte.
    II. L'échange des clés requises doit être réalisé par un processus prédéfini.

9. Exigences relatives aux relations des fournisseurs de systèmes

9.1 Sécurité des informations dans le cadre des relations des fournisseurs de systèmes

Traitement des questions de sécurité dans les accords avec les fournisseurs de systèmes

Control 9.1.1 **Exigence de protection globale**

(1) Des accords de sécurité doivent être déterminés de manière formelle et documentés dans les accords de livraison, avec des fournisseurs de prestations externes qui exploitent, supportent ou entretiennent des appareils de mesure intelligents.

a) Les accords de sécurité doivent remplir les exigences légales, notamment les exigences en matière de protection des données.
b) Les accords de sécurité doivent remplir les exigences régulatoires (notamment les présentes exigences).
c) Il convient de déterminer la manière dont le fournisseur de prestations externe remplit ces exigences.
d) L'accord doit répertorier toutes les personnes du fournisseur de prestations externe qui ont accès aux données critiques ou aux composants principaux et décrire les exigences (de sécurité) établies posées aux personnes afin qu'elles aient accès aux informations.
e) L'accord doit définir les personnes à contacter en cas d'incidents de sécurité.
f) L'accord doit indiquer que le gestionnaire de données a le droit de contrôler les exigences de sécurité définies auprès du fournisseur de prestations externe (droit d'audit).
g) Le fournisseur de prestations externe doit être contraint de respecter les exigences de sécurité du fabricant ou gestionnaire de données des composants du système de communication.

9.2 Gestion d'exécution des prestations par des fournisseurs de systèmes

Objectif: Garantir que les fournisseurs respectent leurs engagements.

Surveillance et contrôle des prestations des fournisseurs de systèmes

Control 9.2.1 **Exigence de protection globale**

(1) Les prestations fournies par des fournisseurs externes et les éventuels sous-traitants doivent être surveillées et contrôlées annuellement. Les composants principaux ne sont donc pas concernés.

a) Le fournisseur de prestations externe doit publier les informations concernant les éventuels incidents de sécurité dans le cadre de ce contrôle. Ces informations doivent être contrôlées conformément aux exigences de sécurité définies.
b) Les problèmes identifiés lors du contrôle doivent être résolus et surveillés.

10. Exigences relatives à la gestion des incidents de sécurité des informations

10.1 Gestion des incidents de sécurité des informations et des améliorations y relatives

Objectif: Garantir une procédure cohérente et efficace quant à la gestion des incidents de sécurité, y compris la notification des événements de sécurité et les points faibles.

Responsabilités et procédures

Control 10.1.1 **Exigence de protection globale**

(1) Des responsabilités et procédures doivent être définies pour une réaction rapide et efficace aux éventuels incidents de sécurité qui surviennent.

a) Les processus doivent être validés et appliqués, et soumis à un contrôle annuel.

Notification des événements de sécurité des informations

Control 10.1.2 **Exigence de protection globale**

(1) Les incidents de sécurité, notamment le vol de données, les manipulations ou les pannes du SMI liées à la sécurité doivent être signalés à la direction et aux parties prenantes externes (p. ex. MELANI ou préposé cantonal à la protection des données).

a) À cet effet, les procédures et responsabilités correspondantes ainsi que les personnes à contacter doivent être définies au préalable.

Notification des points faibles en matière de sécurité des données

Control 10.1.3 **Exigence de protection globale**

(1) Les collaborateurs du gestionnaire de données doivent signaler tous les points faibles au niveau de l'AMI.

a) Une personne de contact ainsi qu'un processus clair ou efficace doivent être définis pour la notification de tels points faibles.

Réaction aux incidents de sécurité des informations

Control 10.1.4 **Exigence de protection globale**

(1) Des processus définis au préalable doivent permettre de réagir aux incidents de sécurité.

a) Les plans de relance doivent être préparés pour pouvoir réagir de façon adéquate en cas de logiciels malveillants et d'attaques.

11. Exigences de conformité

11.1 Conformité au regard des exigences légales et contractuelles

Objectif: Éviter les infractions contre les obligations légales, régulatoires ou contractuelles en matière de sécurité des informations et des autres exigences de sécurité.

Protection contre les enregistrements

Control 11.1.1 **Exigence de protection globale**

(1) Les informations issues des systèmes de mesure intelligents doivent être protégées contre tout accès non autorisé et contre toute publication, destruction ou perte.

a) Les mécanismes de protection mis en œuvre doivent tenir compte aussi bien de la classification des informations et des obligations légales et régulatoires.

Protection des données et protection des informations personnelles identifiables

Control 11.1.2 **Exigence de protection globale**

(1) La protection des données personnelles identifiables doit s'effectuer conformément aux règlementations légales en matière de protection des données, en complément des exigences présentées dans ce document.

11.2 Vérification de la sécurité des données

Objectif: Garantir que la sécurité des informations est exécutée et exploitée conformément aux prescriptions régulatoires et internes.

Vérification de la conformité technique

Control 11.2.1 **Exigence de protection globale**

(1) Le gestionnaire de données doit réaliser un contrôle technique annuel (sur la base d'un échantillon) des systèmes de mesure intelligents afin d'identifier s'ils sont conformes aux prescriptions régulatoires et internes, p. ex. si les configurations de sécurité respectent les prescriptions et meilleures pratiques.

a) La vérification doit, dans la mesure du possible, être automatisée. Les vérifications manuelles doivent être réalisées uniquement par des ingénieurs-système qualifiés et des experts en sécurité expérimentés.