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

Directives pour la sécurité des données des systèmes de mesure intelligents

pour la certification et l'exploitation de systèmes de mesure intelligents

RL-DSP – Édition CH 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 (Groupe de travail Sécurité des données dans le cadre du smart metering)

Maurus Bachmann	VSGS	
Francis Beyeler	AES	
Andreas Eilingsfeld	EWZ	
Roman Gmür	Enpuls AG	
Stéphane Henry	Romande Energie SA	
Patrick Inderkum,	e-lynx (ASUT)	
Roland Kiefer	Stadtwerk Winterthur	
Andreas Kölliker	Infoquard AG	Responsable du GT
Andy Kreuzer	IDS Schweiz AG (swissmig)	
Thomas Mettler	Arbon Energie AG	
Hendrik la Roi	AES	Secrétaire
Tom Ruef	BKW Energie SA	
Yves Senn	Encontrol AG	
David Spale	Avectris SA	
Michael Staudinger	Landis+Gyr SA (ISSS)	

Conseil
Infoguard AG, Baar
VZsecurITy, Laupersdorf

Responsabilité commission
La Commission Données énergétiques de l'AES, en collaboration avec les auteurs, est désignée responsable de la tenue à jour et de l'actualisation du document.

Ce document est un document de la branche sur le marché de l'électricité. Il constitue une directive au sens de l'art. 27, al. 4 de l'Ordonnance sur l'approvisionnement en électricité.

Chronologie

Janvier 2016	Début des travaux du GT Sécurité des données dans le cadre du smart metering
Juin 2016	Publication de l'analyse des besoins de protection de l'OFEN
Novembre 2017	Adoption de la révision des ordonnances relatives à la Stratégie énergétique 2050 par le Conseil fédéral avec le nouvel art. 8b OA-pEl «Vérification de la sécurité des données»
Avril 2018	Finalisation du document
Mai/juin 2018	Procédure de consultation au sein de la branche
24 octobre 2018	Approbation par le Comité de l'AES

Ce document a été élaboré avec l'implication et le soutien de l'AES et de représentants de la branche.

L'AES approuve ce document à la date du 24.10.2018.

Imprimé n° 1045 / f, édition 2018

Sommaire

Liste des figures

Abréviations et définitions

ABP	Analyse des besoins de protection
AES	Association des entreprises électriques suisses
AMI	Appareil de mesure intelligent. «Compteur électrique électronique» selon art. 8a OApEl
CD	Concentrateur de données
CRM	Customer Relationship Management.
EAE	Entreprise d'approvisionnement en énergie
GDC	Gestion des données de compteur
GDE	Gestion des données énergétiques
GRD	Gestionnaire de réseau de distribution
METAS	Institut fédéral de métrologie
OFEN	Office fédéral de l'énergie
SMI	Système de mesure intelligent
STDC	Système de traitement des données de comptage. Ces systèmes proposent des fonctions pour administrer les appareils de mesure ou pour traiter les données brutes enregistrées par les appareils de mesure, comme p. ex. le paramétrage des appareils, l'administration des appareils ou l'administration des séries chronologiques.
STR	Système de tête de réseau, *Head End System*
TIC	Technologies de l'information et de la communication
WAN	Wide Area Network

Liste des sources

	Titre	Éditeur
[1]	Ordonnance sur l'approvisionnement en électricité (OApEl) du 14 mars 2008 (avec adaptations pour le 1er janvier 2018)	Confédération
[2]	Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse; 11/2014	OFEN
[3]	Approches garantissant la sécurité des TIC des systèmes de mesure intelligents installés chez le consommateur final; 10/2015	OFEN
[4]	Étude «Analyse des besoins de protection du smart metering en Suisse» de juin 2016	OFEN

Avant-propos

Le présent document est un document de la branche publié par l'AES. Il fait partie d'une large réglementation relative à l'approvisionnement en électricité sur le marché ouvert de l'électricité. Les documents de la branche contiennent des directives et des recommandations reconnues à l'échelle de la branche concernant l'exploitation des marchés de l'électricité et l'organisation du négoce de l'énergie, répondant ainsi à la prescription donnée aux entreprises d'approvisionnement en électricité (EAE) par la Loi sur l'approvisionnement en électricité (LApEl) et par l'Ordonnance sur l'approvisionnement en électricité (OApEl).

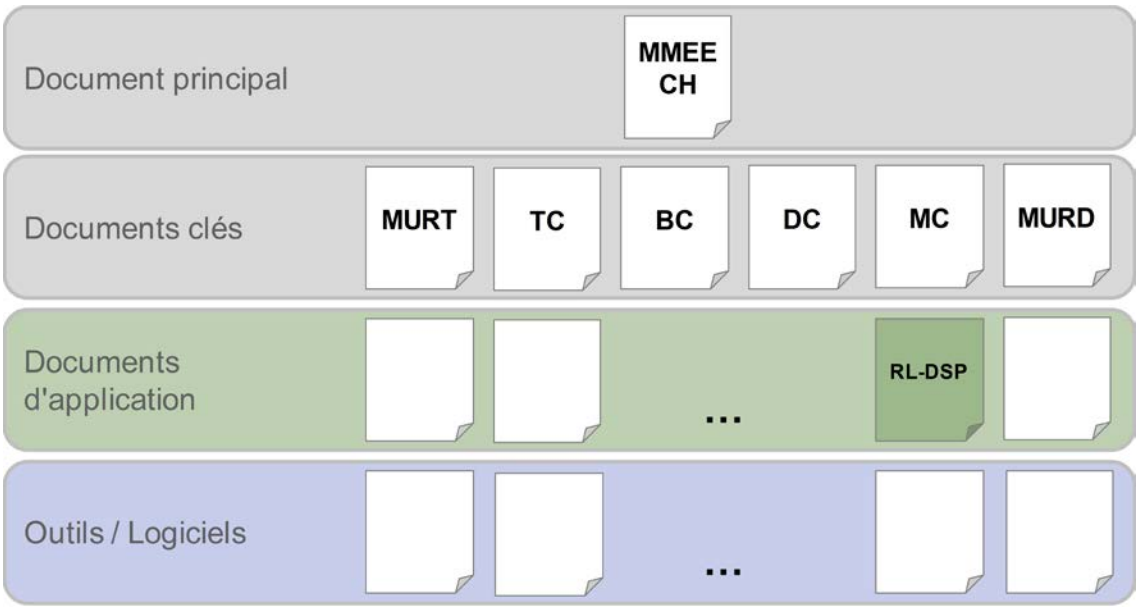
Les documents de la branche sont élaborés par des spécialistes de la branche selon le principe de subsidiarité; ils sont régulièrement mis à jour et complétés. Les dispositions qui ont valeur de directives au sens de l'OApEl sont des normes d'autorégulation. En principe, les documents de la branche font foi pour toutes les personnes impliquées ayant déclaré que lesdits documents faisaient partie intégrante d'un contrat donné.

Les documents sont répartis en quatre catégories hiérarchisées:

- Document principal: Modèle de marché pour l'énergie électrique (MMEE)
- Documents clés
- Documents d'application
- Outils / Manuels

Le présent document «Directives pour la sécurité des données des systèmes de mesure intelligents», est un Document d'application.

Structure des documents



1. Introduction

1.1 Objectif du document

(1) Le présent document de la branche s'appuie sur l'analyse des besoins de protection (ABP) de l'OFEN [4] pour fixer des directives et exigences pour la mise en œuvre d'un contrôle de la sécurité des données pour des systèmes de mesure intelligents installées chez les consommateurs finaux.

(2) Les directives visent à définir, à l'aide de l'évaluation des risques dans l'ABP, des exigences contrôlables en matière de sécurité, qui présentent un niveau de détail adapté et permettent d'obtenir des résultats reproductibles dans le cadre d'une vérification.

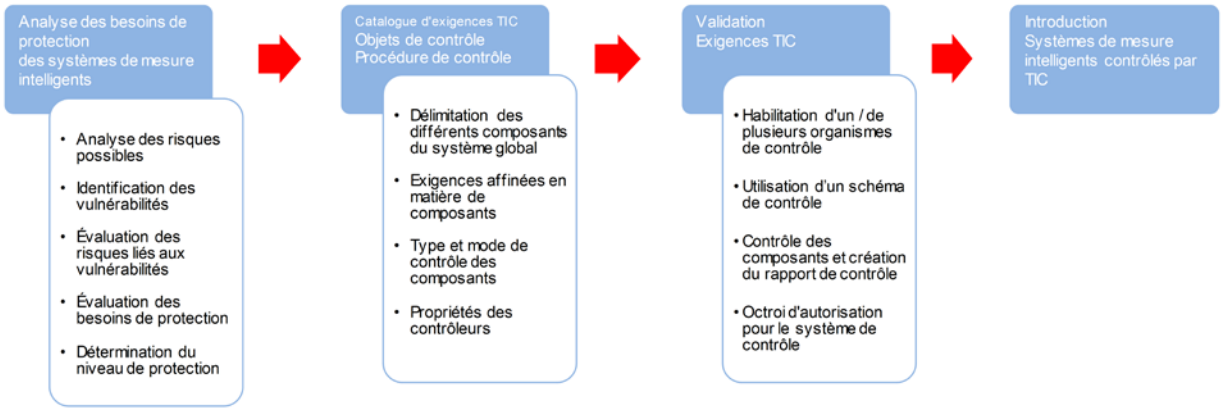


Figure 1: Étapes du processus garantissant la sécurité des données des systèmes de mesure intelligents installés chez le consommateur final (Source: Réf. [3], Illustration 8)

(3) La figure 1 présente les étapes de processus importantes pour la garantie de la sécurité des données des systèmes de mesure intelligents:

- Analyse des besoins de protection (ABP)
- Définition du catalogue d'exigences (ce document et ses annexes)
- Validation des exigences de sécurité (via le METAS)
- Introduction du système de mesure intelligent (par le gestionnaire de réseau de distribution)

(4) Outre les exigences de mise en œuvre du contrôle de la sécurité des données du SMI, le document de la branche comprend des recommandations sur la manière dont un SMI peut être utilisé en toute sécurité.

1.2 Structure des documents

(1) Le document se compose d'un document de directives définissant l'ensemble du processus ainsi que les rôles et responsabilités de chaque acteur. Le chapitre 3 donne un aperçu des directives pour la certification d'un SMI et le chapitre 4 des recommandations pour l'utilisation sûre d'un SMI. Les exigences de sécurité sont décrites dans deux annexes au document.

- Annexe 1 «Exigences de certification envers les systèmes de mesure intelligents pour la sécurité des données» avec des exigences pour la sécurité contrôlable des composants d'un SMI (pour le contrôle de la sécurité des données selon l'art. 8b OApEl).
- Annexe 2 «Exigences opérationnelles envers les systèmes de mesure intelligents pour la sécurité des données» des exigences et recommandations pour le gestionnaire de réseau et le prestataire en vue de l'exploitation d'un SMI. Cette annexe est à considérer, indépendamment de la vérification de la sécurité des données selon l'art. 8b OApEl, comme recommandation de la branche indiquant comment le GRD peut assumer sa responsabilité pour l'exploitation sûre d'un SMI.

2. Rôles

(1) **Fabricant**: Le rôle de «fabricant» inclut le fabricant de logiciels et de matériel informatique des composants des systèmes de mesure intelligents. Ils fournissent des produits pour le SMI. Ils sont chargés de faire contrôler les composants du SMI avant leur commercialisation. De plus, ils garantissent que les appareils peuvent continuer d'être utilisés de façon sûre pendant la phase d'exploitation, p. ex. à l'apparition de nouveaux risques, au moyen de mises à jour de logiciels et de micrologiciels.

(2) **Gestionnaire de réseau de distribution:** Le gestionnaire de réseau de distribution est responsable de la fourniture des prestations de métrologie (utilisation de places de mesure et service de mesure). Il veille à ce que seuls les composants contrôlés soient utilisés. Par ailleurs, il est chargé de l'utilisation sûre du SMI. Les exigences pour l'utilisation sûre d'un SMI sont formulées pour le rôle du gestionnaire de données. Le gestionnaire de réseau de distribution peut fournir lui-même les prestations de métrologie en tant que gestionnaire des données ou sous-traiter les missions correspondantes à des tiers.

(3) **Gestionnaire de données**: L'ABP [4] regroupe les rôles de «gestionnaire de places de mesure» et de «prestataire de mesure» sous le terme de «gestionnaire de données». Le gestionnaire de places de mesure est généralement responsable des processus d'assistance, comme l'installation et l'exploitation ainsi que la vérification et la maintenance de l'AMI. Le prestataire de mesure prend habituellement en charge la lecture et le relevé du dispositif de mesure ainsi que d'autres prestations pour le consommateur final, comme le traitement ultérieur des données, la facturation, la prise en charge ou le conseil des clients.

(4) **Prosumer / consommateur final**: Le prosumer peut aussi bien être producteur dans le réseau électrique que consommateur final de ce réseau, et se trouve normalement au niveau de réseau 5 ou 7, dans de rares cas au niveau de réseau 3.

(5) **Organisme de contrôle**: L'organisme de contrôle est chargé de valider les exigences de sécurité. Il vérifie si les exigences de sécurité des données ont été mises en œuvre de façon exhaustive et efficace. L'organisme de contrôle transmet les résultats de contrôle au fabricant, sous la forme d'un rapport de contrôle, une fois le contrôle exécuté. L'art. 8b, al. 3 OApEl mentionne le METAS comme organisme de contrôle unique. Celui-ci peut confier à des tiers l'exécution de cette mission ou des parties de celle-ci.

(6) **Autorité de contrôle / autorité de certification**: L'autorité de contrôle attribue au fabricant, après évaluation de la procédure ou du rapport de contrôle, une autorisation d'exploitation du produit – appelée «habilitation» –, ainsi qu'un sigle d'homologation (certificat). Le METAS endosse le rôle de l'autorité de contrôle, conformément à la formulation de l'art. 8b, al. 3 OApEl.

(7) D'autres rôles sont répertoriés dans le document «MMEE – CH».

3. Directives pour le contrôle de la sécurité des données du SMI

(1) L'art 8b OApEl du 1er novembre 2017 détermine que seuls les SMI qui ont été soumis à un contrôle de sécurité des données au préalable peuvent être utilisés. Le présent chapitre décrit «les éléments à contrôler» (chapitre 3.1), «les exigences y relatives» (annexe 1) ainsi que «le type et le mode de contrôle» (chapitre 3.3). Le chapitre 3.2 donne un aperçu du processus et des rôles impliqués dans le contrôle de la sécurité des données.

3.1 Champ d'application du SMI pour le contrôle de sécurité des données

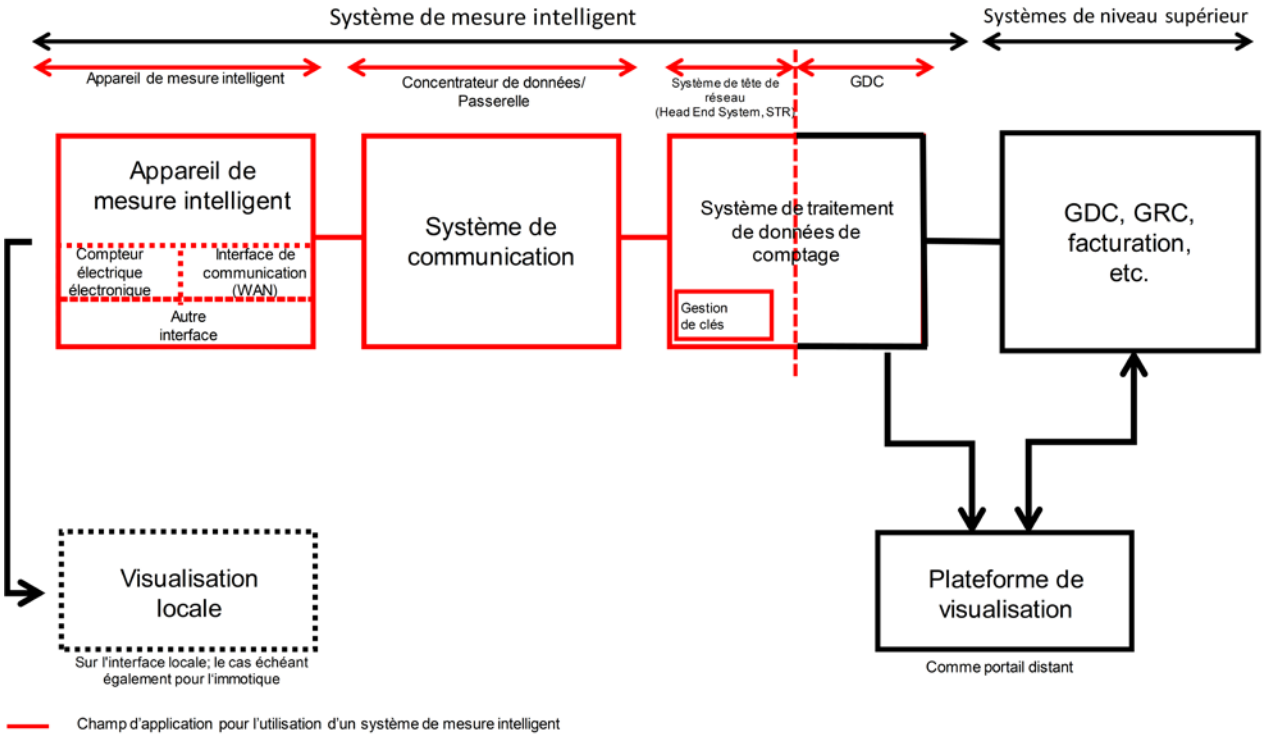


Figure 2: Champ d'application du SMI pour le contrôle de sécurité des données

(1) Le champ d'application pour le contrôle de sécurité des données du SMI est représenté (en rouge) à la figure 2. Il inclut trois composants principaux: l'AMI, le système de communication et le STR.

(2) La visualisation locale ainsi que tous les systèmes en aval du STR ne sont pas concernés par le champ d'application du contrôle de sécurité des données, en raison de leur mise en œuvre différente (GDC, STDC, GDE, GRC, système de facturation, plateforme de visualisation, etc.). Pour la même raison, l'interface entre le STR et le GDC ne fait partie du contrôle de sécurité des données. L'interface permettant la visualisation locale sur l'AMI est toutefois comprise dans le champ d'application.

3.2 Processus de contrôle de sécurité des données – Étape par étape

(1) Les étapes suivantes[1] décrivent l'exécution du contrôle de sécurité des données, illustrée par la figure 3. La description de ce processus s'appuie sur la répartition des rôles présentés ci-dessus des acteurs correspondants, mais concrétise ses missions lorsque cela s'avère nécessaire.

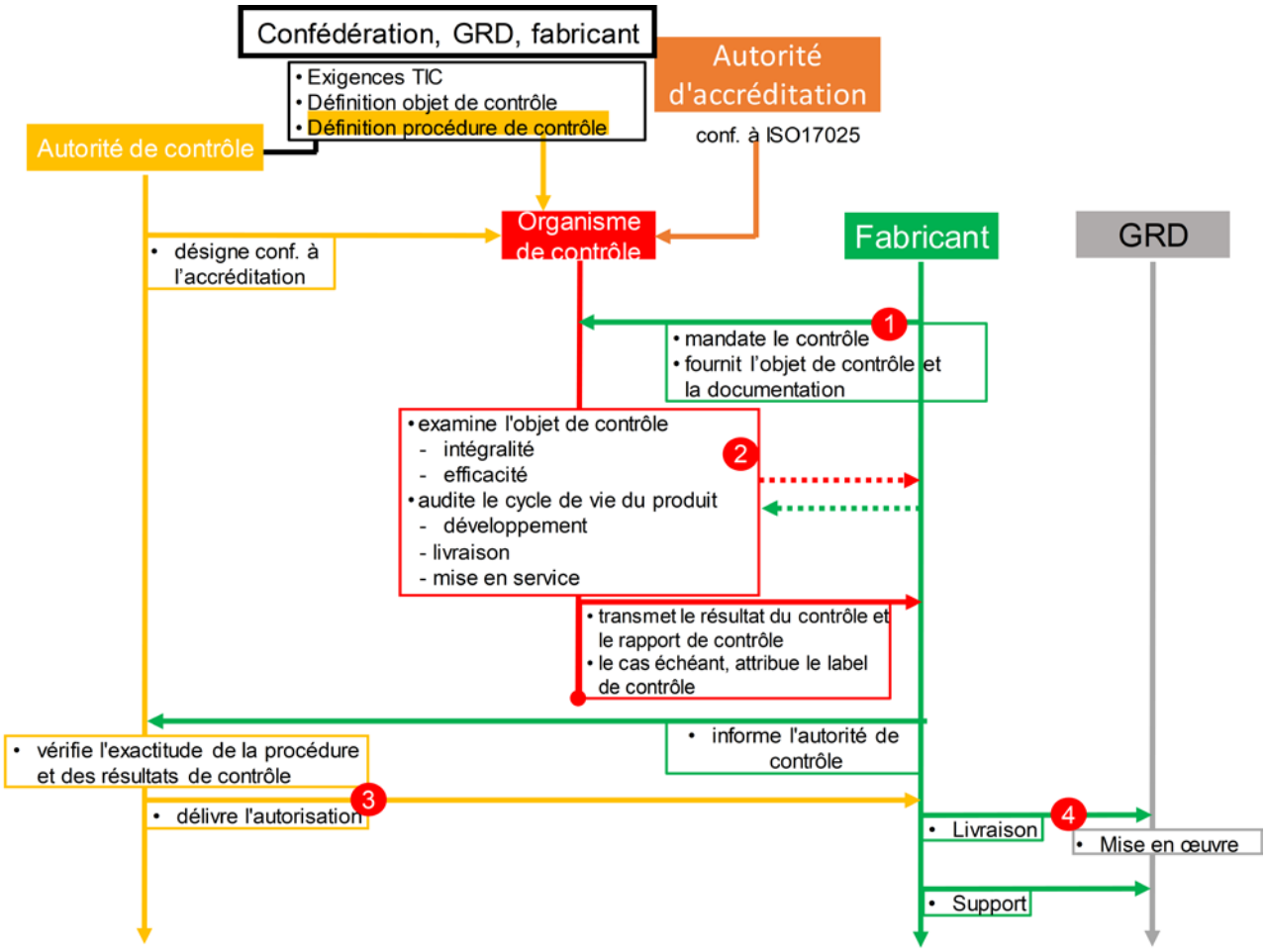


Figure 3: Processus de validation de la sécurité des TIC (Source: Réf. [3], figure 10)

Étape 1: Mission de contrôle du fabricant pour un produit confiée à l'organisme de contrôle

(2) Un organisme de contrôle accrédité est mandaté par le fabricant (ou par ex. par l'exploitant qui intervient comme «sponsor» pour la prise en charge des coûts du contrôle) pour examiner un SMI sous l'angle du contrôle de sécurité des données et sur la base du catalogue d'exigences connu. Les objets de vérification font partie d'un SMI; leurs fonctionnalités de sécurité requises sont détaillées dans le catalogue d'exigences (voir annexe 1: «Exigences de certification envers les systèmes de mesure intelligents pour la sécurité des données»).
Le fabricant met à la disposition de l'organisme de contrôle son produit, la documentation y afférente et la documentation technique requise, ainsi que d'autres informations relatives aux processus de sécurité (conformément au catalogue d'exigences). L'identification produit (par ex. numéro de série, version du système de contrôle de configuration, etc.), la documentation produit ainsi que toutes les

[1] La figure originale dans réf. [3] décrit également l'étape 5 «Surveillance du fonctionnement et des échantillons». Il n'existe actuellement aucune base légale pour le contrôle du fonctionnement. C'est pour cette raison qu'elle n'apparaît pas dans cette figure.

spécifications techniques englobant les fonctionnalités de sécurité des TIC. En outre, les processus relatifs à la sécurité dans le cycle de vie d'un objet de contrôle sont contrôlés par le fabricant pour l'organisme de contrôle (sécurité dans le développement, lors de la livraison, de la mise en service, fonctionnalités de mise à jour).

Étape 2: Produit soumis à l'organisme de contrôle

(3) Le contrôle se déroule, de manière interactive le cas échéant, entre l'organisme de contrôle et le fabricant. Les phases de contrôle détaillées dans le schéma de contrôle pour les objets de vérification distincts sont exécutées étape par étape, à l'aide de documents fournis par le fabricant, et les fonctionnalités de sécurité définies dans le catalogue d'exigences sont vérifiées. Pendant le contrôle, le fabricant assiste l'organisme de contrôle par des informations complémentaires qui peuvent être requises par l'organisme de contrôle, dans certains cas justifiés. L'organisme de contrôle détermine donc l'exhaustivité et l'efficacité des fonctionnalités de sécurité. Par ailleurs, il audite le cycle de vie du produit, en vérifiant autant que possible le développement, la livraison, la mise en service et les fonctionnalités de mise à jour. Il peut p. ex. le faire sur la base de procédures documentées. En cas de défauts constatés, le contrôle peut également autoriser des cycles de révision de l'objet du contrôle par le fabricant pour la réparation. L'organisme de contrôle transmet le résultat au fabricant, sous la forme d'un rapport de contrôle, une fois le contrôle exécuté.

Étape 3: Contrôle par l'autorité de contrôle et habilitation

(4) L'autorité de contrôle reçoit le rapport de contrôle du fabricant du SMI et enregistre le produit concerné dans un répertoire. Elle contrôle le rapport pour vérifier l'exactitude de la procédure et des résultats. En cas d'irrégularités ou de contrôles insatisfaisants, elle demande des améliorations ou des contrôles à un autre organisme de contrôle. L'autorité de contrôle attribue, après évaluation de la procédure ou du rapport de contrôle, une autorisation d'exploitation du produit – appelée «habilitation» –, ainsi qu'un sigle d'homologation.

Étape 4: Livraison du produit et mise en service

(5) Le fabricant fournit un produit validé par l'autorité de contrôle à l'exploitant, qui l'installe dans son environnement d'exploitation, conformément aux réglementations de sécurité liées au contrôle de sécurité des données. Le label de contrôle et l'autorisation de l'autorité de contrôle offrent une transparence pour le contrôle des coûts réalisé par le régulateur, et garantissent ainsi l'imputabilité.

3.3 Type et mode de contrôle de sécurité des données

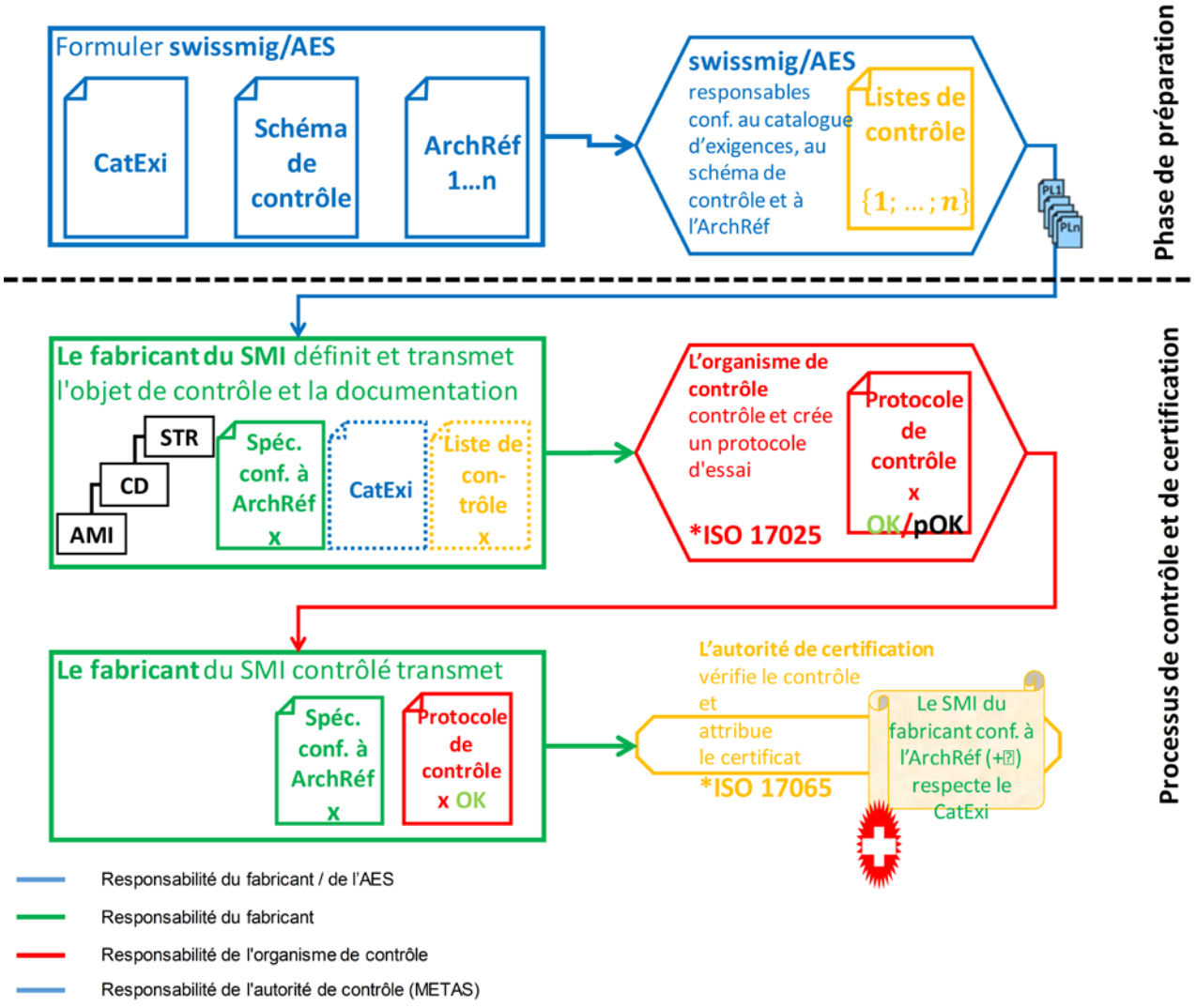


Figure 4: Schéma de contrôle avec les domaines de compétences des acteurs impliqués

(1) Le contrôle de sécurité des données s'appuie sur ces directives, qui se composent d'un catalogue d'exigences, du schéma de contrôle et des listes de contrôle. À l'aide de ces réglementations, le fabricant de l'organisme de contrôle explique la manière dont il a mis en œuvre les exigences avec ses produits.

(2) L'organisme de contrôle vérifie les produits présentés et résume ses résultats dans un protocole de contrôle. Une fois le contrôle de sécurité des données effectué, l'autorité de contrôle attribue l'autorisation des produits sur la base du protocole de contrôle.

3.3.1 Interopérabilité lors du contrôle de la sécurité des données

(1) Tous les éléments d'un SMI doivent être soumis à un contrôle de la sécurité des données, conformément à l'art. 8b OApEl, et être certifiés. La certification concernant la sécurité des données se fait sur la base de différents éléments. Tout nouvel élément ajouté dans un SMI doit faire l'objet d'une

certification. Les corrections d'erreurs pertinentes pour la sécurité réalisées sur des éléments déjà certifiés doivent faire l'objet d'une certification ultérieure au plus tard après un (1) an. Cette certification ultérieure doit être réalisée au niveau du fabricant. Ainsi, un SMI composé d'éléments certifiés qui est agrandi par un nouvel élément certifié (d'un autre fabricant) continue de satisfaire à l'art. 8b OApEl (contrôle de la sécurité des données).

4. Le fonctionnement sécurisé d'un SMI

(1) L'utilisation d'objets de protection sûrs et contrôlés ne suffit pas pour faire face aux risques de l'ABP. Les gestionnaires de données doivent également garantir qu'après la mise en service, les appareils sont utilisés de la manière prévue dans la vérification du contrôle des données.
L'annexe 2 «Exigences opérationnelles envers les systèmes de mesure intelligents pour la sécurité des données» inclut également des exigences qui garantissent que la sécurité des données puisse être assurée lors de l'exploitation d'un SMI.

(2) Le chapitre 4.1 montre les composants-système impliqués dans l'exploitation d'un SMI. La sécurité des données doit être garantie pour ce champ d'application.

4.1 Champ d'application pour l'utilisation sûre d'un SMI

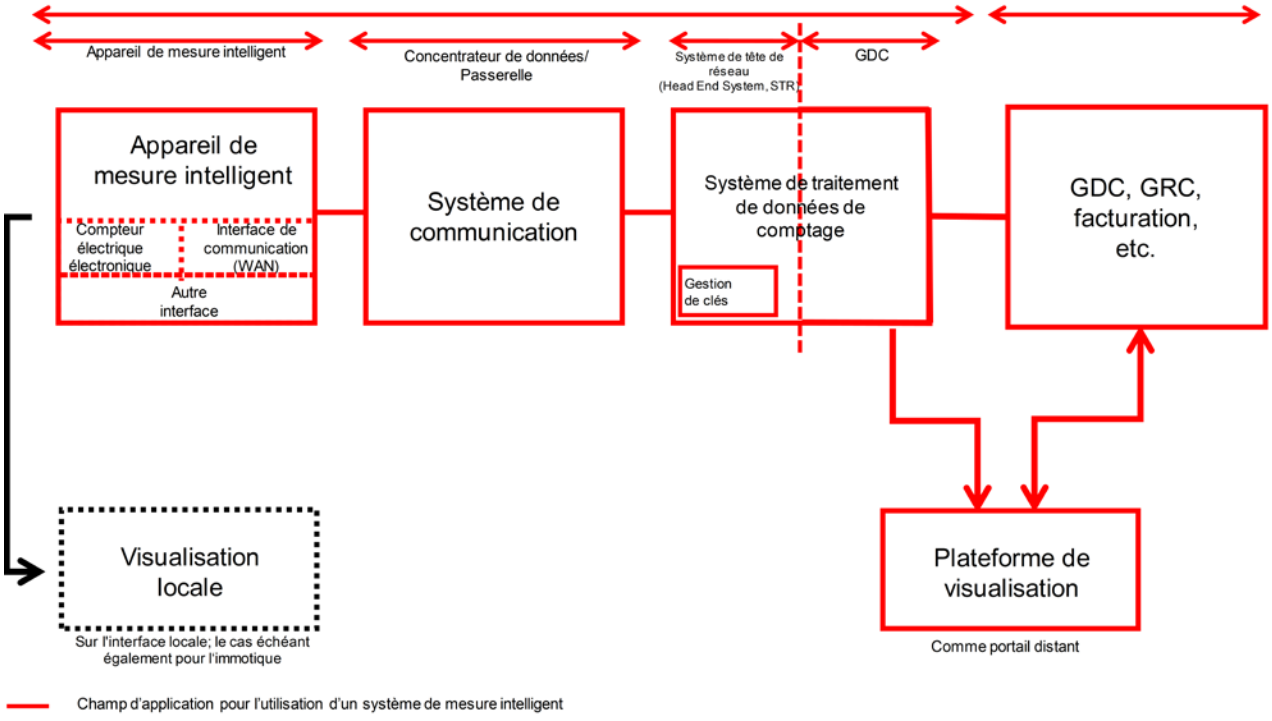


Figure 5: Champ d'application pour l'utilisation sûre d'un SMI

(1) La figure 5 montre (en rouge) le champ d'application pour l'utilisation d'un SMI. Outre les composants principaux de l'AMI, le système de communication et le STR du contrôle de la sécurité des données, elle inclut également tous les systèmes en aval du STR (GDC, STDC, GDE, GRC, système de facturation, plateforme de visualisation, etc.). Les interfaces permettant la visualisation locale sur l'AMI et entre le STR et le GDC sont incluses. La visualisation locale est exclue de la sphère d'influence du gestionnaire de données et donc du champ d'application.

4.2 Contrôle de sécurité pour l’utilisation d’un SMI

(1) Les exigences à l’annexe 2 «Exigences opérationnelles envers les systèmes de mesure intelligents pour la sécurité des données» sont très complètes: elles incluent p. ex. les exigences relatives à la gestion des ressources, au contrôle des accès, à la cryptographie, à la sécurité d’exploitation et de communication, à la gestion des incidents affectant la sécurité, au développement et à la maintenance, et enfin à la conformité (compliance). Le choix des exigences peut s’effectuer sur la base d’une évaluation des risques propre du gestionnaire des données.

(2) Le catalogue d’exigences contient des exigences et recommandations quant à la manière d’utiliser un SMI de manière sécurisée. Le respect des exigences garantit que le gestionnaire des données exploite le SMI de la façon requise lors de l’exécution du contrôle de la sécurité des données.

(3) La mise en œuvre des exigences aide le gestionnaire de données dans sa responsabilité pour l’utilisation sûre d’un SMI. Avec un audit de sécurité des données périodique sur la base du catalogue d’exigences présenté, le gestionnaire de données peut vérifier et améliorer en permanence la sécurité des données du fonctionnement de l’installation. L’exécution d’audits de sécurité est donc recommandée.

5. Annexe 1: Exigences de certification envers les systèmes de mesure intelligents pour la sécurité des données

6. Annexe 2: Exigences opérationnelles envers les systèmes de mesure intelligents pour la sécurité des données