Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 106 (2015)
Heft: 9

Artikel: Pistes vers l'avenir des réseaux électriques suisses
Autor: Le Roy, Bruno / Galus, Matthias
DOI: https://doi.org/10.5169/seals-856701

BRANCHE **SMART GRID**

Pistes vers l'avenir des réseaux électriques suisses

La protection et la sécurité des données, un défi identifié par la Feuille de route pour un réseau intelligent

Le développement des réseaux intelligents s'accompagnera d'un très fort accroissement de l'échange et de la collecte systématique de données numériques. Les questions de protection et de sécurité des données représentent donc un élément essentiel du développement des réseaux intelligents. La Feuille de route l'a clairement identifié.

Bruno Le Roy, Matthias Galus

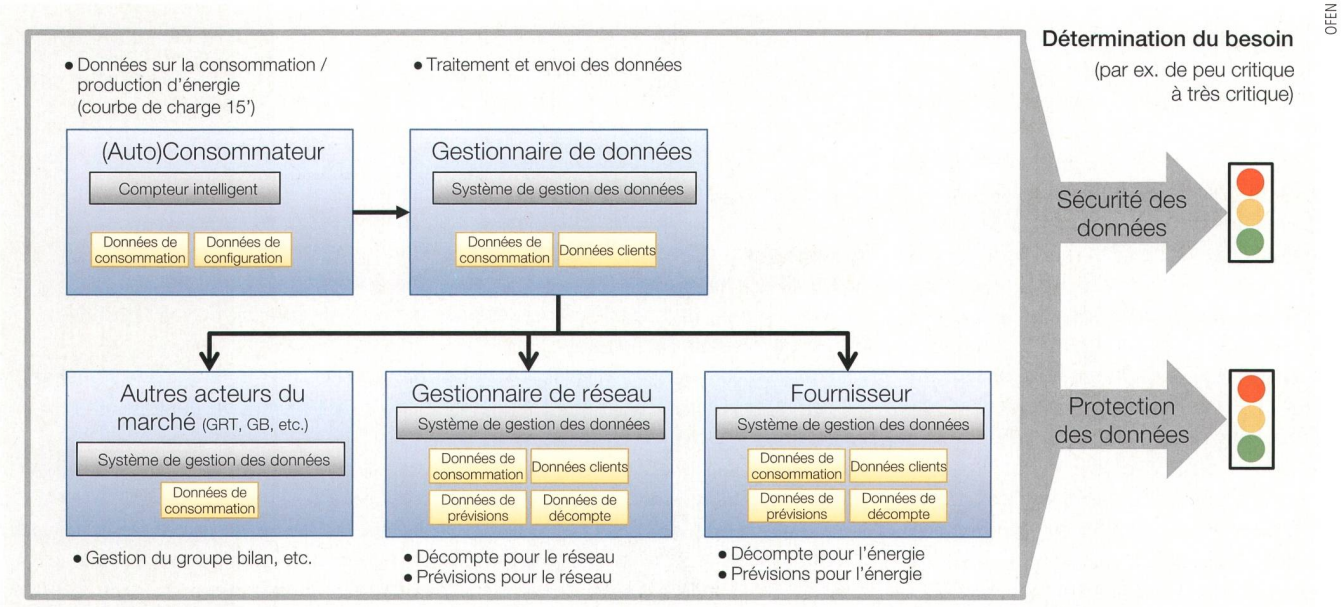
La Feuille de route pour un réseau intelligent [1] pose une vision à long terme concernant le développement des réseaux électriques intelligents en Suisse et présente un vaste panel des technologies appelées à être déployées à grande échelle pour leur réalisation. Bien plus que pour les réseaux « conventionnels », le développement des réseaux intelligents s'accompagnera d'un très fort accroissement de l'échange et de la collecte systématique de données numériques en recourant à des infrastructures basées sur les technologies de l'information et de la communication (TIC). Ces échanges de données contribueront à augmenter la pilotabilité et l'observabilité des réseaux électriques. Donnons ici deux exemples, traduisant des contextes de marché et de réseaux bien différents. Dans un cas, des données de mesures de consommation électrique enregistrées avec un pas de temps de 15 minutes auprès d'un consommateur [2] pourront être transmises quotidiennement à son fournisseur d'électricité. Dans un autre cas, un gestionnaire de réseau pourra envoyer à distance des ordres de pilotages aux différents transformateurs réglables de son réseau.

Problématique

Avec ces deux exemples, nous voyons poindre les problèmes relatifs à la protection et à la sécurité des données. Concernant le consommateur, il s'agit en particulier de lui assurer que ses données de mesures ne seront utilisées que par des tiers autorisés, dans le respect du principe de proportionnalité et sans violation de sa vie privée (thématique : protection des données). Quant au gestionnaire de réseau, il doit garantir que les TIC intégrées à son système de conduite de réseau se prémunissent contre toute menace ou toute nuisance externe pouvant entraver la gestion du réseau (thématique : sécurité des données).

La Feuille de route souligne ainsi que les questions de protection et de sécurité des données ne doivent donc pas être négligées lors du déploiement des réseaux intelligents :

- Protection : quelles règles doivent être définies pour protéger les données des personnes morales et physiques contre les abus et garantir que ces données ne soient exploitées que par des tiers autorisés ?
- Sécurité : quelles mesures techniques contribuent d'une part à assurer la protection des données et, d'autre part, à garantir l'exploitation d'un réseau intelligent sûr, performant et efficace, doté d'une infrastructure TIC robuste ?



OFEN

Déterminer le besoin de protection et de sécurité des données dans le cas du comptage intelligent.

BRANCHE **SMART GRID**

La Suisse n'est pas la seule à se pencher sur ces questions, de nombreux travaux sont déjà en cours au niveau européen. L'agence ENISA [3] ou le CENELEC [4] par exemple ont publié des guides méthodologiques afin que des mesures concrètes et adaptées puissent être prises par les gestionnaires des réseaux intelligents.

Quels modèles pour les réseaux intelligents ?

Afin de pouvoir définir des recommandations claires en termes de protection et de sécurité des données à l'échelle de la Suisse, il est au préalable nécessaire de définir précisément les cas d'utilisation (ou « use cases » en anglais) des réseaux intelligents. Autrement dit, il s'agit de pouvoir décrire sans ambiguïté le marché et ses différents acteurs, de séparer clairement leurs rôles et leurs obligations respectives et d'identifier les données et informations qui seront échangées. La figure s'appuie sur les travaux de la Feuille de route. Elle fournit, dans le cas précis du comptage intelligent, une illustration claire du modèle d'échange des données. On peut alors s'appuyer sur ce type de modèle bien établi pour traiter des problèmes de protection et de sécurité.

En marge de la Feuille de route, une étude publiée par l'OFEN [5] pose les grandes lignes de 12 cas d'utilisation des réseaux intelligents, en mettant l'accent sur l'utilisation des TIC. Ces cas constituent une première étape vers une future normalisation des cas d'utilisation ; ils doivent néanmoins être encore précisés, les acteurs mieux identifiés et leurs rôles plus concrètement définis.

Protection du consommateur final

Dans un premier temps, il s'agit d'identifier clairement tous les flux de données, et particulièrement celles se rapportant à des personnes. Pour chaque cas d'utilisation identifié, on peut ensuite déterminer si chaque acteur qui reçoit de telles données est autorisé à les traiter au sens de la loi fédérale de protection des données [6] et dans le respect du principe de proportionnalité qu'elle énonce. Dans le cas particulier du comptage intelligent, [5] montre qu'une unique législation au niveau fédéral concernant la protection des données dans les réseaux intelligents est souhaitable et juridiquement acceptable. Lors de travaux ultérieurs, il s'agirait de déterminer si les mêmes conclusions peuvent s'appliquer aux autres cas d'utilisation des réseaux intelligents.

Sécurité : déterminer les besoins

En s'appuyant sur des cas d'utilisation standard bien détaillés, on peut établir quel niveau de sécurité relatif aux TIC est nécessaire dans les réseaux intelligents. Pour cela, on peut recourir à une analyse du besoin de sécurité dont la méthodologie pourrait par exemple être la suivante :

- Définition et délimitation du système ou des sous-systèmes à protéger (par exemple un système de mesure intelligent [2], en tant que partie intégrante d'un réseau intelligent),
- Identification des vulnérabilités du système, des menaces pesant sur le système et des impacts associés,
- Identification et évaluation des risques associés (définis comme la résultante de la vulnérabilité, des menaces et des impacts ; ils peuvent être de nature opérationnelle, économique, environnementale, etc.),
- Détermination du besoin de sécurité correspondant pour l'infrastructure TIC du système. Le besoin de sécurité se déduit du niveau de risque résiduel acceptable.

Les résultats de l'analyse du besoin de sécurité peuvent ensuite servir à définir un cahier des charges en termes de sécurité TIC pour les réseaux intelligents.

Synthèse

L'utilisation des TIC dans les réseaux intelligents pose des questions cruciales pour la protection et la sécurité des données. Dans le domaine des réseaux intelligents, les travaux en la matière les plus avancés en Europe concernent le comptage intelligent. Il s'agirait dans un premier temps de travailler à définir plus précisément les cas concrets d'utilisation des réseaux intelligents, notamment pour mieux standardiser les flux d'informations entre les différents acteurs des réseaux intelligents. Sur cette base, des études d'analyses de besoin de sécurité pourront être menées. En fonction des résultats, les autorités nationales compétentes pourront définir des règles claires en termes de protection des données et des exigences pour la sécurité TIC des réseaux intelligents pourront être publiées.

Références

[1] Feuille de route suisse pour un réseau intelligent – Pistes vers l'avenir des réseaux électriques suisses OFEN, 2015.
[2] Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse – Exigences techniques minimales et modalités d'introduction, OFEN, 2014.
[3] Smart Grid Security Certification, ENISA, 2014.
[4] Smart Grid Coordination Group – Smart Grid Information Security, CEN-CENELEC-ETSI, 2012.
[5] Datensicherheit und Datenschutz für Smart Grids : Offene Fragen und mögliche Lösungsansätze, AWK-Vischer-FIR-HSG, 2014.
[6] 235.1 Loi fédérale du 19 juin 1992 sur la protection des données (LPD).

Lien

- www.bfe.admin.ch/smartgrids

Auteurs

Diplômé de l'École Polytechnique et de l'EPFL, **Bruno Le Roy** est spécialiste réseaux au sein de l'Office fédéral de l'énergie. Il traite notamment les sujets relatifs au comptage et aux réseaux électriques intelligents, ainsi que les aspects liés à la protection et à la sécurité des données.

Office fédéral de l'énergie, 3003 Berne
Bruno.Le-Roy@bfe.admin.ch

Dr **Matthias Galus** est spécialiste réseaux au sein de l'Office fédéral de l'énergie. Il a dirigé les travaux de la Feuille de route pour un réseau intelligent et l'élaboration des exigences minimales pour le comptage intelligent. Dr Matthias Galus est l'auteur de l'article précédent.

Matthias.Galus@bfe.admin.ch

Zusammenfassung **Zukunftsszenarien für die Schweizer Stromnetze**

Datenschutz und -sicherheit – eine Herausforderung, die aus der «Smart Grid Roadmap» hervorgeht

Die Entwicklung von Smart Grids führt – in einem weit grösseren Ausmass als bei den «konventionellen Netzen» – zu einer sehr starken Zunahme des Austauschs und der systematischen Sammlung von digitalen Daten mithilfe von Infrastrukturen, die auf Informations- und Kommunikationstechnologien (IKT) beruhen.

Datenschutz und Datensicherheit stellen daher ein grundlegendes Element bei der Entwicklung von Smart Grids dar – was die Smart Grid Roadmap (s. vorangehender Artikel) klar belegt. In Bezug auf die Verbraucher muss hauptsächlich gewährleistet werden, dass die Messdaten nur von autorisierten Dritten verwendet werden, unter Einhaltung des Grundsatzes der Verhältnismässigkeit und ohne Verletzung der Privatsphäre (Thema: Datenschutz). Der Netzbetreiber muss garantieren, dass die IKT, die in seinem Netzleitsystem eingesetzt werden, Schutz bieten vor jeglicher Bedrohung oder Belastung von aussen, die die Netzwerksteuerung beeinträchtigen könnte (Thema: Datensicherheit). Cr