Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA
Swiss Gas and Water Industry Association SGWA

W1018 f Edition mars 2019

REGLEMENTAION

Recommandation

Norme minimale pour garantir les technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en eau

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie,
de la formation et de la recherche DEFR

Office fédéral pour l'approvisionnement économique du pays OFAE
Secrétariat domaine TIC

SSIGE, Grütlistrasse 44, case postale 2110, 8027 Zurich
Téléphone 044 288 33 33, Fax 044 202 16 33, www.ssige.ch

Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA
Swiss Gas and Water Industry Association SGWA

W1018 f Edition mars 2019

REGLEMENTATION

Recommandation

Norme minimale pour garantir les technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en eau

IMPRESSUM

Font foi les conditions générales publiées à l'adresse suivante :
www.sssige.ch/CGV

En vente auprès de l'Administration de la SSIGE
(support@svgw.ch)

SSIGE, Grütlistrasse 44, case postale 2110, 8027 Zurich
Téléphone 044 288 33 33, Fax 044 202 16 33, www.ssige.ch

Impressum

Editeur

Société Suisse de l'Industrie du Gaz et des Eaux (SSIGE)
Office fédéral pour l'approvisionnement économique du pays (OFAE)

Auteurs de la première édition

Nom	Prénom	Organisation	Fonction
Walder	Dario	OFAE	Auteur principal/responsable du projet
Schenker	Silvan	OFAE	Co-auteur/responsable du projet suppléant
Olschewski	André	SSIGE	Donneur d'ordre SSIGE/expert/fournisseur d'informations/assurance qualité
Domeniconi	Raffaele	SSIGE	Expert/fournisseur d'informations/assurance qualité
Carusone	Raffael	Energie Thun AG	Expert/fournisseur d'informations/assurance qualité
Garcia	Manuel	SIG	Expert/fournisseur d'informations/assurance qualité
Kasme	Samir	SIG	Expert/fournisseur d'informations/assurance qualité
Kegele	Karl	WWZ AG	Expert/fournisseur d'informations/assurance qualité
Maître	Nathalie	ESB	Experte/fournisseur d'informations/assurance qualité
Matt	Georg	WV Liechtensteiner Unterland e.G.	Expert/fournisseur d'informations/assurance qualité
Rickenbacher	Andreas	IWB	Expert/fournisseur d'informations/assurance qualité
Romano	Roberto	EW Rothrist AG	Expert/fournisseur d'informations/assurance qualité
Stöckli	Markus	Energie Thun AG	Expert/fournisseur d'informations/assurance qualité
Weyermann	Thomas	SWG	Expert/fournisseur d'informations/assurance qualité
Zberg	Leo	WV Sarnen	Expert/fournisseur d'informations/assurance qualité

Chronologie

Date	Intitulé raccourci
2016	Réalisation d'une analyse sur la vulnérabilité des TIC en lien avec l'approvisionnement en eau
Octobre 2017	Première discussion au sujet d'une norme minimale pour les TIC entre le DEFR et la SSIGE
Décembre 2017	Première discussion avant la réunion de lancement
Janvier 2018	Deuxième discussion avant la réunion de lancement
Janvier 2018	Début des travaux de l'équipe chargée du projet (lancement)
Février 2018	Discussion sur le sommaire commenté
Mars 2018	Examen de l'avant-projet par les experts
Avril 2018	Deuxième examen de l'avant-projet et validation par les experts
Mai 2018	Traduction en français
Mai 2015	Consultation de la SSIGE, constitution d'une commission principale
Mai – août 2018	Consultation par la SSIGE et élaboration d'exemples pour la mise en œuvre
Décembre 2018	Publication de la norme minimale en matière de TIC pour l'approvisionnement en eau

Ce document a été élaboré avec l'implication et le soutien de l'Office fédéral pour l'approvisionnement économique du pays (OFAE), de la Société Suisse de l'Industrie du Gaz et des Eaux (SSIGE) et d'experts de l'approvisionnement en eau.

SOMMAIRE

PREFACE

La généralisation et l'interconnexion des technologies de l'information et de la communication (TIC) dans tous les domaines de la vie courante offrent un potentiel économique et social incontournable pour un pays aussi développé et industrialisé que la Suisse. Parallèlement, la numérisation croissante génère de nouveaux risques, auxquels il convient de réagir rapidement et de façon appropriée. Le risque particulier lié aux cyberattaques visant les infrastructures informatiques ou à des dysfonctionnements ou erreurs de manipulation des systèmes TIC intervenant dans l'approvisionnement concerne des services publics au même titre que les gestionnaires d'infrastructures critiques et d'autres entreprises utilisant des informations particulièrement précieuses.

La norme minimale TIC s'applique là où une société moderne ne peut se permettre des défaillances des systèmes TIC utilisés par les organisations d'approvisionnement en eau. En tant que bien vital, l'eau mérite toute notre attention. La qualité, mais aussi la disponibilité de ce précieux liquide sont essentielles. Elles font d'ailleurs partie du mandat constitutionnel de l'AEP. Je suis donc très heureux qu'à travers la présente norme de la branche, l'AEP puisse contribuer, avec la SSIGE et des représentants du secteur, à améliorer la résilience de l'approvisionnement en eau.

La norme minimale TIC est recommandée par l'AEP et la SSIGE comme niveau de sécurité minimal en matière de TIC. L'adhésion de la branche à cette norme est primordiale pour l'AEP, L'approvisionnement économique du pays privilégie ainsi une collaboration étroite avec la branche et la fédération correspondante plutôt qu'une solution centralisée, comme le font d'autres pays.

La cybersécurité est désormais également reconnue en Suisse comme une tâche essentielle pour l'approvisionnement en eau potable et son infrastructure critique ». Il s'agit d'assurer une gestion minutieuse des mots de passe de systèmes informatiques de bureaux, tout en protégeant les systèmes SCADA ou les interfaces avec des systèmes installés à proximité. La cybersécurité n'est pas seulement incontournable pour les grands groupes, particulièrement exposés en tant que sociétés mixtes de distribution. Les organisations plus modestes doivent elles aussi se protéger, car elles exploitent souvent des installations complexes, afin de garantir l'approvisionnement en eau potable de la population et du secteur privé.

La présente Recommandation de branche (norme minimale TIC) a été rédigée par l'Office fédéral pour l'approvisionnement économique du pays et par la Société Suisse de l'Industrie du Gaz et des Eaux pour les systèmes d'approvisionnement en eau potable. Cette collaboration a permis de garantir une méthodologie intersectorielle homogène et tous les effets de synergies associés.

La recommandation pour la branche est conçue de façon modulable : elle sert de guide aux grands distributeurs d'eau comme, de manière concrète, aux entreprises de petite et moyenne taille. Nous remercions chaleureusement toutes les parties prenantes pour leur extraordinaire collaboration avec l'OFAE et la qualité élevée du produit. Nous espérons que la recommandation sera mise en œuvre rapidement par le plus grand nombre possible d'entreprises concernées pour rehausser nettement le niveau de cybersécurité, moyennant un coût raisonnable. La SSIGE sera ravie d'accompagner les services des eaux dans cette étape, en proposant des formations spécifiques.

Werner Meier
Délégué à l'approvisionnement
Économique du pays

Markus Küng
Président de la Société Suisse de l'Industrie
du Gaz et des Eaux (à partir de 2019)

Résumé

La numérisation et la professionnalisation croissantes de l'approvisionnement en eau améliorent certes l'efficacité du traitement et de la distribution d'eau potable, mais elles accroissent notre dépendance informatique. Les distributeurs d'eau utilisent par exemple des systèmes de gestion des processus (systèmes SCADA[1]) basés sur des TIC pour piloter le traitement et la distribution de l'eau.

Les systèmes SCADA font partie intégrante des infrastructures critiques qui facilitent la gestion des entreprises dans des secteurs importants comme l'approvisionnement en eau, en électricité, en pétrole et en gaz ou encore en logistique. L'importance accrue de la cybersécurité des systèmes TIC critiques est une évidence. Pour gérer efficacement la problématique de la cybersécurité, il faut bien connaître les enjeux actuels en matière de sécurité et les contre-mesures disponibles.

La présente norme minimale TIC constitue un cadre permettant aux distributeurs d'eau non seulement de se prémunir contre d'éventuelles attaques ou erreurs de manipulation, mais aussi de restaurer leurs systèmes le plus rapidement possible en cas d'incident. Ce cadre permet à l'entreprise d'évaluer elle-même le risque encouru et de mettre en œuvre les mesures appropriées.

La norme minimale TIC repose sur des bases concrètes et éprouvées comme le NIST Framework Core ou l'analyse des risques et de la vulnérabilité de l'approvisionnement en eau, menée par l'OFAE.[2] Cette norme permet de garantir une méthode uniforme débouchant sur des résultats comparables dans une branche et d'optimiser le niveau de sécurité des systèmes TIC requis pour l'approvisionnement en eau.

Pour les sociétés mixtes de distribution (par ex. gaz, eau, électricité, eaux usées, communication), il est crucial que les mêmes normes minimales TIC s'appliquent aux différents secteurs. La norme de l'Association des entreprises électriques suisses (AES) repose sur les mêmes prérequis que la présente norme minimale.

La présente norme comprend six parties. Ce document fait office d'élément principal, avec une introduction, des instructions et une initiation à l'approvisionnement en eau : il constitue la base de la mise en œuvre. Il est complété par quatre annexes (Défense en profondeur, Cadre de cybersécurité, Recommandations, Exemples de mise en œuvre) et un outil d'évaluation basé sur Excel (cf. chap. 2).

Exclusion de responsabilité

[1] SCADA: Supervisory control and data acquisition (système informatique pour surveiller et piloter des processus techniques)

[2] Analyse des risques et de la vulnérabilité relative à l'approvisionnement en eau. Office fédéral pour l'approvisionnement économique du pays (OFAE), Berne 2016 (n'existe qu'en allemand).

1 Introduction

1.1 Contexte et vue d'ensemble

L'Office fédéral pour l'approvisionnement économique du pays (OFAE) s'est intéressé à la vulnérabilité des TIC requis pour l'approvisionnement en eau dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyber-risques (SNPC). Cette analyse de vulnérabilité a été menée conjointement par la Confédération et les distributeurs d'eau. Elle s'est concentrée sur les processus assurant l'approvisionnement en eau de la population suisse.

Le plus souvent, l'approvisionnement en eau implique 4 processus centraux : l'eau est d'abord captée à la source, puisée dans les lacs et/ou les nappes phréatiques, puis transportée. Elle est ensuite soumise à un traitement variant selon sa qualité (aucun traitement, traitement simple ou plusieurs niveaux de traitement) avant d'être injectée dans le réseau/les réservoirs. De là, elle est ensuite acheminée vers le réseau qui assure sa distribution jusqu'au consommateur.

Le système nommé SCADA constitue la clé informatique centralisée de l'approvisionnement en eau pour les 4 processus centraux. Chaque centrale hydraulique exploite un système SCADA qui commande ses pompes, ses réservoirs ou ses installations de traitement. S'il tombait en panne, ces dernières ne pourraient plus tourner. De plus, les pompes seraient partiellement hors d'usage, dès lors qu'elles ne peuvent être actionnées manuellement. Cette panne peut aussi entraîner, dans certaines circonstances, l'impossibilité de recevoir les messages de perturbation et les alarmes.

Outre le système SCADA, les outils de communication comme la messagerie électronique, les terminaux mobiles, la VoIP[3], voire la radio, sont importants pour les distributeurs d'eau. Sans ces outils, les usines ne peuvent plus communiquer efficacement avec des installations décentralisées (stations de traitement d'eau de lac) ni remédier à leurs dysfonctionnements.

Intégrant l'analyse de vulnérabilité des TIC requis pour l'approvisionnement en eau, la présente norme formule des recommandations pour optimiser le niveau de sécurité informatique chez tous les acteurs du secteur[4]. Ils sont ainsi encouragés à évaluer eux-mêmes leur niveau de sécurité et à comparer le degré de maturité de leurs systèmes TIC avec la valeur-cible. En cas d'écarts, la présente norme sert (avec d'autres reconnues et citées en référence) de guide pour améliorer les aspects liés à la sécurité.

La loi sur l'approvisionnement du pays confère au Conseil fédéral la compétence de mettre en œuvre des mesures préventives pour favoriser la résilience des processus d'approvisionnement vitaux pour notre pays. La présente norme constitue une mesure de résilience que le secteur concerné est libre d'adopter ou non, au titre d'autorégulation de la branche. Ainsi la norme minimale en matière de TIC, élaborée en collaboration avec la SSIGE, se veut une recommandation pour la branche.

[3] VoIP : Voix sur IP (voice over IP)

[4] On a notamment utilisé les quatre documents suivants comme bases pour la présente norme minimale TIC :

1. Norme minimale TIC générale de l'approvisionnement économique du pays
2. Framework for Improving Critical Infrastructure Cybersecurity
3. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
4. Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME)

1.2 Situation initiale et objectifs

En analysant la vulnérabilité de l'approvisionnement en eau[5] (en 2016), on a révélé une dépendance croissante de l'informatique dans l'approvisionnement en eau potable. La numérisation poursuit son chemin chez les fournisseurs d'eau, ce qui augmente l'efficacité mais aussi la complexité de l'approvisionnement. La défaillance des systèmes TIC critiques peut avoir des répercussions considérables sur l'approvisionnement en eau potable, en eaux industrielles ou en eaux d'extinction.

La présente Recommandation de l'Office fédéral pour l'approvisionnement économique du pays (OFAE) et de la SSIGE adopte l'approche d'une défense en profondeur (Defense in Depth)[6], qui retient un large éventail de menaces pour la sécurité des TIC. L'objectif est de mettre à la disposition des informaticiens travaillant chez les fournisseurs d'eau un outil pratique pour évaluer et optimiser la cybersécurité dans leur entreprise. La finalité est d'améliorer la résilience des fournisseurs d'eau face aux risques liés aux TIC et, à terme, d'augmenter la sécurité globale de l'approvisionnement.

Les menaces liées aux TIC sont comprises de manière globale : elles vont des dégâts concrets aux cyberattaques à visée destructrice, en passant par la perte ou la manipulation de données. Les risques identifiés lors de l'analyse de vulnérabilité, menée dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyber-risques sont également pris en compte.

Outre les mesures techniques, la présente recommandation pour la branche englobe la formation des collaborateurs et la gouvernance afin d'améliorer la résilience des systèmes informatiques importants. Nous recommandons une approche à plusieurs niveaux pour assurer la disponibilité, l'intégrité et la confidentialité des informations :

- **Disponibilité**
  Garantir la disponibilité des informations lorsque c'est nécessaire. Cela suppose que les systèmes de traitement et de transmission soient opérationnels et disponibles
- **Intégrité**
  Faire en sorte que les informations soient à tout moment complètes et exactes.
- **Confident**
  Garantir que les informations sont accessibles uniquement aux personnes ou aux systèmes autorisés.

[5] Analyse des risques et vulnérabilités du sous-secteur approvisionnement en eau. Effectué par l'approvisionnement économique du pays (https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ncs_strategie/stand_der_umsetzungsarbeiten.html) [état au 07.09.2018]

[6] Voir aussi annexe 1.

1.3 Champ d'application et délimitations

La présente recommandation de branche émane de l'OFAE et de la SSIGE. Elle se concentre sur les processus dans l'entreprise qui ont une influence directe sur l'approvisionnement de la population suisse en eau potable. La portée de ce document est définie comme suit :

Champ d'application

- La présente norme englobe toutes les technologies de l'information et de la communication nécessaires à l'exploitation des systèmes et réseaux d'approvisionnement en eau potable.
- La résilience des systèmes doit être améliorée dans toute la branche. L'objectif du niveau minimal de protection doit permettre de limiter les effets d'un cyber-incident sur l'approvisionnement en eau.
- Nous nous sommes notamment concentrés sur les systèmes suivants : SCADA, ERP[7] et de communication. Sont également concernés les ordinateurs portables et les postes de travail avec PC, les téléphones mobiles, les logiciels de maintenance, les interfaces SCADA, le Smart Metering, ainsi que les réseaux et systèmes installés dans des bâtiments autres que ceux de l'entreprise (installations du client).
- La recommandation se concentre sur les entreprises de distribution d'eau fortement tributaires des systèmes TIC pour maintenir leur activité.

Délimitation

- Dans cette recommandation, nous n'avons pas abordé le cas où une entreprise peut aussi faire fonctionner son système d'approvisionnement en eau sans systèmes TIC, soit en mode manuel, en cas de cyberattaque par exemple. Nous recommandons cependant de sauvegarder ou de (ré)introduire cette possibilité si les conditions s'y prêtent. Pour les infrastructures critiques, le mode manuel est capital – a minima, la déconnexion en bon ordre des infrastructures devrait toujours être possible.
- Cette norme minimale pour les TIC ne concerne pas l'approvisionnement en électricité. Il est néanmoins recommandé de prévoir pour chaque système d'approvisionnement, un plan d'urgence afin d'affronter une pénurie ou une panne généralisée. La dépendance vis-à-vis de la fourniture d'électricité est très importante. Sans électricité, les stations de pompage, les systèmes de traitement de l'eau brute, de transport et de collecte ne peuvent être mis en œuvre que partiellement, voire pas du tout. Les captages d'eau de source peuvent, eux, être en grande partie maintenus, même sans électricité (sans désinfection). Plus de 40 % de l'eau potable proviennent des nappes phréatiques. Par conséquent, au niveau local, une quantité d'eau considérable d'eau potable peut être collectée sans électricité. Dans certaines zones de desserte, la distribution d'eau de source peut aussi s'effectuer sans électricité. D'autres fournisseurs d'eau sont équipés de groupes électrogènes pour collecter et distribuer l'eau de source et notamment l'eau souterraine. Ces mesures permettent de garantir, dans une certaine mesure, l'approvisionnement en eau, y compris en cas de pénurie d'électricité ou de panne générale.
- L'ordonnance sur la garantie de l'approvisionnement en eau potable en temps de crise (voir chapitre 5.1) n'est pas intégrée dans la présente norme. Elle est néanmoins considérée comme une mesure de résilience générale pour l'approvisionnement en eau.
- La présente recommandation ne comporte pas de mesures concernant la sécurité au travail.

[7] Système Enterprise Ressource Planning : le système ERP est une application complexe voire une multitude de systèmes informatiques ou de logiciels d'application en interaction, aidant à planifier les ressources dans toute l'entreprise.

1.4 Nécessité d'avoir une norme minimale pour les TIC

Dans le domaine des TIC, en constante évolution les menaces qui pèsent sur les petits et grands distributeurs d'eau évoluent constamment elles aussi. Les cyberattaques n'ont rien à voir avec la taille de l'entreprise et résultent souvent d'un concours de circonstances ou d'un effet d'aubaine. Ces situations se multiplient avec la généralisation de la numérisation. Les services des eaux sont de plus en plus nombreux à connecter leurs systèmes de commande à Internet pour faire des économies ou gagner en flexibilité grâce à la télésurveillance. Cela entraîne de nouveaux types de vulnérabilité, ces failles pouvant, par exemple, être exploitées par des pirates pour voler des données, utiliser des ressources TIC externes voire prendre le contrôle d'infrastructures critiques.

De telles menaces sont bel et bien réelles. En cas d'attaque de rançongiciels (ransomware), par exemple, les réseaux informatiques ou les systèmes de contrôle sont bloqués et ne sont libérés que contre le paiement d'une rançon. Aux États-Unis, des entreprises d'approvisionnement en eau ont d'ores et déjà été infectées par ce biais, mais seul un petit nombre a versé une rançon. La plupart ont récupéré en remplaçant leur système ou en restaurant une version sauvegardée[8]. Néanmoins, ces attaques produisent des dommages colossaux, avec des pertes financières importantes.

D'autres attaques ont visé directement les systèmes de commande. En 2016, des pirates ont visé une compagnie des eaux (Kemuri Water Company, KWC), manipulant les systèmes de contrôle-commande de ses processus pour traiter les eaux et contrôler le débit[9]. Le fournisseur de service Internet Verizon a indiqué que Kemuri Water Company avait une architecture de sécurité insuffisante, que ses systèmes connectés à Internet présentaient des faiblesses et qu'ils étaient donc très vulnérables[10]. Le système de contrôle-commande des processus a été compromis pour gérer l'ajout de produits chimiques. Les pirates sont ainsi parvenus à influencer le débit et la teneur de l'eau en produits chimiques. Dans deux cas au moins, ils ont réussi à manipuler le système de façon à bloquer les capacités de traitement et de production de l'eau. Fort heureusement, grâce à une fonction d'alarme, KWC a pu détecter rapidement les modifications chimiques et les variations du débit. Elle a pu y remédier, minimisant largement les conséquences pour ses clients.

Afin de limiter au maximum ce type de risque et d'autres, les TIC requis pour l'approvisionnement en eau doivent présenter un niveau de sécurité élevé. L'instauration d'une procédure normalisée en matière de cybersécurité permet aux entreprises d'optimiser la protection de leurs TIC et d'améliorer la protection en continu. La présente norme fournit des instructions pratiques pour la mettre en œuvre.

Les entreprises de distribution d'eau sont encouragées à identifier elles-mêmes les risques auxquels elles sont exposées ainsi qu'à évaluer leur propension au risque. Elles peuvent adapter la présente norme en fonction de leur taille, de leurs ressources et de l'état actuel des connaissances (approche basée sur les risques). C'est en fonction de ces considérations qu'elles établiront ce que leur coûtera la mise en œuvre.

En finalité, c'est au distributeur d'eau d'assumer ses responsabilités quant à la sécurité de fonctionnement de ses installations.

[8] WaterNews - Water Sector Prepares for Cyberattacks. 9 juin 2016/dans Infrastructure, United States, Water Management, Water News/de Brett Walton, dans : http://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks/ [consulté le 22.02.2018].

[9] Verizon, Data Breach Digest 2016, dans : http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf [consulté le 22.02.2018].

[10] Security Week Online: https://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report [consulté le 22.02.2018].

2 Consignes d'application de la norme minimale TIC

2.1 Aperçu des documents contenus dans la norme

La norme minimale TIC comprend plusieurs parties (fig. 1), le présent document constituant le document principal, soit la base de la mise en œuvre. Il comprend aussi une introduction, des instructions et une initiation à l'approvisionnement en eau. Il s'accompagne de 4 annexes et d'un outil d'évaluation basé sur Excel.

Fig. 1 Vue d'ensemble des documents constitutifs de la norme minimale TIC

Document principal (présent document) (requis)
La présente norme minimale TIC (Recommandation OFAE/SSIGE pour la branche) comprend une introduction au sujet et des instructions pour mettre en œuvre de la norme.

1) Annexe 1 – Défense en profondeur (facultatif)
Il permet de s'initier aux fondements (défense en profondeur) de la norme.

2) Annexe 2 – Cadre de cybersécurité (facultatif)
Présente le cadre de cybersécurité utilisé par l'outil d'évaluation et comprend des informations utiles pour noter son niveau de maturité (cf. échelle de 0 à 4). Offre également une vue d'ensemble des résultats affichés dans l'outil d'évaluation.

3) Annexe 3 – Recommandations aux petits distributeurs d'eau (requis pour les ces derniers)
Fournit des recommandations spécifiques aux distributeurs d'eau dont la zone de desserte couvre moins de 5000 habitants.

4) Annexe 4 – Exemples de mise en œuvre (facultatif)
Contient des exemples de mise en œuvre anonymisés pouvant servir de référence pour répondre à d'éventuelles interrogations dans le cadre de la mise en application de la norme minimale TIC.

5) Outil d'évaluation (basé sur Excel - requis pour les distributeurs d'eau dont la zone de desserte couvre 5000 habitants ou plus)
L'outil d'évaluation basé sur Excel constitue une aide à la mise en œuvre de la norme minimale en matière de TIC. Il permet d'évaluer la maturité de la cybersécurité de l'approvisionnement en eau. L'utilisation de l'outil d'évaluation est recommandée pour tous les distributeurs d'eau dont la zone de desserte couvre 5000 habitants ou plus.

2.2 Mise en œuvre de la norme minimale TIC

2.2.1 Procédure différenciée

Le secteur de l'approvisionnement en eau est très hétérogène, question taille des entreprises. Cette norme minimale TIC a pour vocation de couvrir l'ensemble de la branche. Cela impose une procédure différenciée (tab. 1). Les distributeurs d'eau dont la zone de desserte couvre 5000 habitants ou plus doivent appliquer la norme minimale TIC dans son intégralité. Ils sont encouragés à déterminer leur degré de maturité avec l'outil d'évaluation et à l'améliorer en continu. En Suisse, les plus grands distributeurs d'eau devraient notamment viser un niveau de maturité supérieur au minimum recommandé.

Pour les entreprises qui desservent moins de 5000 habitants, il serait disproportionné d'investir dans l'outil d'évaluation. Des recommandations spécifiques ont été formulées à leur attention (cf. annexe 3). Elles constituent les exigences minimales à remplir (et remplacent l'outil d'évaluation).

Habitants approvisionnés	Recommandation pour la mise en œuvre
≥ 5000	Norme minimale TIC complète, outil d'évaluation compris
< 5000	Recommandations (voir annexe 3)

Tab. 1 Mise en œuvre de la norme minimale en matière de TIC

2.2.2 Préparation

Le processus (diagramme de flux) ci-après peut servir de base pour mettre en œuvre la norme minimale TIC (fig. 2). Si le service informatique du distributeur d'eau est relié à celui de la commune, la mise en œuvre peut se faire à un niveau supérieur et inclure d'autres processus d'approvisionnement. Si tel n'est pas le cas, ou si vous souhaitez sécuriser votre installation à titre individuel, vous devez d'abord déterminer sa taille. Les distributeurs d'eau qui desservent moins de 5000 habitants appliquent les recommandations fournies à l'annexe 3. Ceux qui alimentent 5000 habitants ou plus appliquent la norme minimale TIC dans son intégralité, en utilisant l'outil d'évaluation.

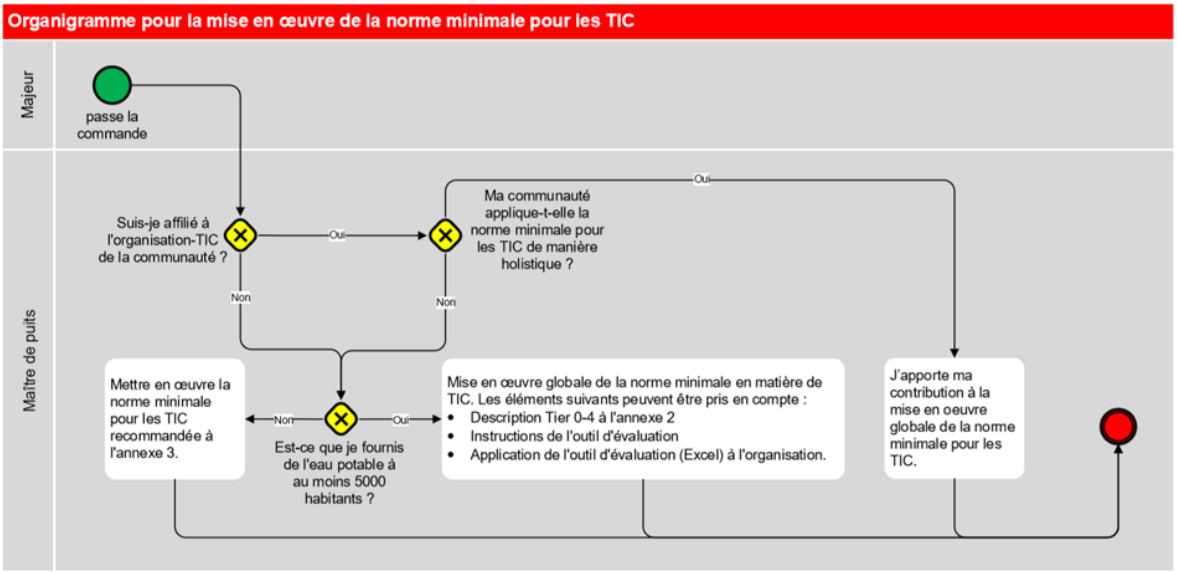

Fig. 2 Processus d'aide à la mise en œuvre de la norme minimale TIC

2.2.3 Instructions aux distributeurs d'eau desservant moins de 5000 habitants

Les distributeurs d'eau dont la zone de desserte couvre moins de 5000 habitants sont également soumis à la présente norme minimale sur les TIC, mais seulement de façon partielle. L'annexe 3 de cette norme de la branche comprend une liste de recommandations qui se substituent à l'outil d'évaluation. L'état actuel de la mise en œuvre des recommandations doit être évalué sur la base de l'aide fournie à l'annexe 3, Cela permettra ainsi de mettre en évidence les domaines dans lesquels des mesures sont nécessaires. L'annexe 4 propose un exemple de mise en œuvre chez un petit distributeur d'eau.

Le niveau minimum pour les petits distributeurs d'eau est considéré comme atteint quand toutes les recommandations formulées à l'annexe 3 sont mises en œuvre.

2.2.4 Instructions aux distributeurs d'eau desservant 5000 habitants ou plus

Les distributeurs d'eau dont la zone de desserte couvre 5000 habitants ou plus doivent appliquer la norme minimale TIC dans son intégralité. Le présent document sert de guide de procédure et d'aide à la mise en œuvre. Le niveau minimum est considéré comme atteint si la notation globale de la maturité en matière de cybersécurité (cf. outil d'évaluation) correspond au moins aux valeurs minimales prescrites conformément à leur propre approche basée sur les risques.

Généralement, l'approche basée sur les processus est recommandée notamment pour les grands distributeurs d'eau. Dans ce cas, la cybersécurité n'est pas considérée ni abordée comme un état, mais comme un processus, et doit être dynamique. La sécurité des TIC n'est jamais acquise. Elle constitue un objectif permanent, qui doit faire l'objet de contrôles réguliers (par ex. annuels) et d'un processus d'amélioration continue. Ceux-ci doivent reposer sur la norme minimale TIC. La SSIGE proposera des formations et une assistance spécifique sur ces points.

L'outil d'évaluation reprend pour l'essentiel les exigences du NIST Framework Core[11]. Il permet une auto-évaluation à partir de cinq fonctions (identifier, protéger, détecter, réagir et récupérer). Ces fonctions sont ensuite réparties en 23 catégories, elles-mêmes subdivisées en 106 activités (fig. 3).

[11] NIST Framework Core: https://www.nist.gov/framework [consulté le 26.03.2018].

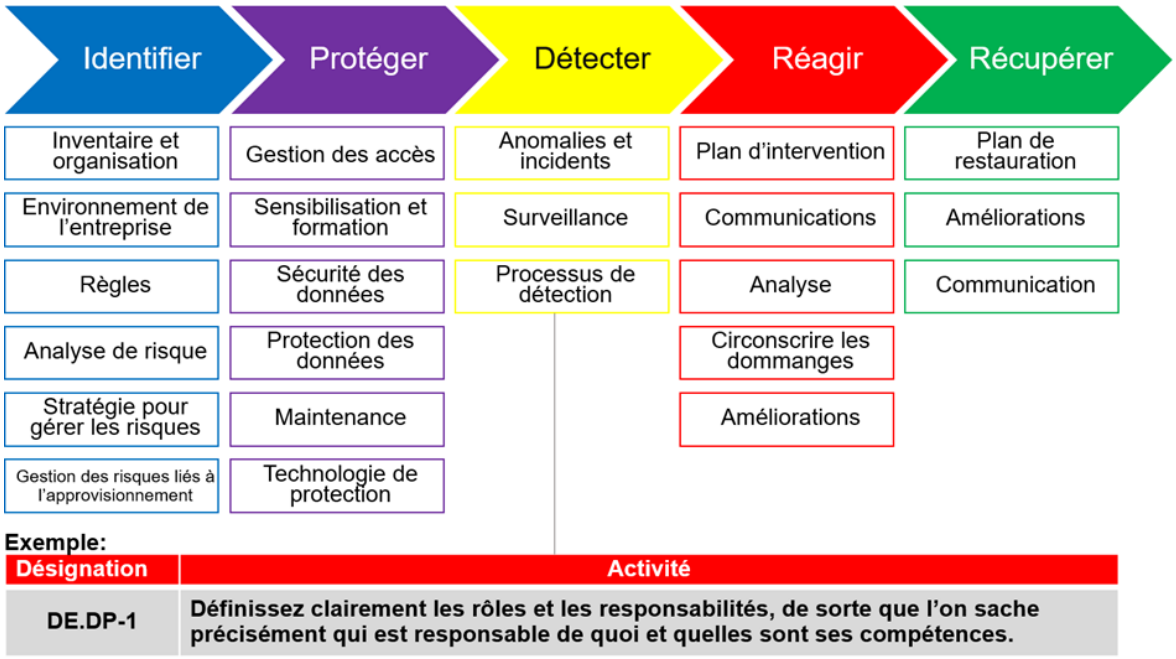

Fig. 3 Fonctions, catégories et exemple d'activité du « cadre de cybersécurité »

L'annexe 2 présente le cadre de cybersécurité. Ce dernier est mis à disposition pour servir de support d'information et de discussion. Le cadre de cyber sécurité peut être mis en œuvre à l'aide de l'outil d'évaluation. Celui-ci comprend et présente les cinq fonctions, 23 catégories et 106 activités de façon à ce qu'elles puissent être évaluées et commentées.

Avant de commencer à utiliser l'outil d'évaluation, les fonctions et les catégories du cadre de cybersécurité peuvent être priorisées en fonction de la propension au risque de l'organisation. À cet effet, conformément à l'approche basée sur les risques, une note est attribuée à chacune des cinq fonctions et 23 catégories. Les distributeurs d'eau déterminent quelles sont les fonctions et les catégories qui revêtent une importance particulière pour leur organisation (priorité élevée), et celles qui sont moins pertinentes.[12] Certaines catégories mobilisent plus ou moins de ressources. Cette approche offre, comparée à la méthode sans priorisation, un gain d'efficacité pour évaluer les 106 activités. Elle intéressera plus particulièrement les distributeurs d'eau de taille moyenne (zone de desserte comprise entre 5000 et 15000 habitants). Il est recommandé aux grandes compagnies suisses (grandes villes) de mettre en œuvre l'ensemble des 106 activités du cadre de cybersécurité avant de procéder à l'évaluation à l'aide de l'outil et d'y saisir les réponses.

L'évaluation peut ensuite être effectuée à l'aide de l'outil d'évaluation, dans lesquels les réponses seront saisies. Pour toutes questions sur les activités, se reporter aux normes de référence indiquées (cf. outil d'évaluation) ou à la partie théorique de l'annexe 2 à la norme minimale TIC. De plus, les exemples fournis à l'annexe 4 pourraient se révéler particulièrement utiles.

[12] L'approche basée sur les risques peut par exemple s'appuyer sur la gestion des risques de l'entreprise. Voir également les exemples de mise en œuvre à l'annexe 4.

3 Présentation générale du secteur de approvisionnement en eau

3.1 Structure de la branche

Plus de 2500 distributeurs d'eau desservent la population résidante en Suisse en eau potable. La majorité d'entre elles est composée de petites et micro-entreprises. Le nombre élevé de fournisseurs d'eau indépendants s'explique par le fait qu'en Suisse, l'approvisionnement en eau potable relève de la compétence des cantons. Ces derniers délèguent le mandat d'approvisionnement aux communes, en leur donnant une marge de manœuvre décisionnelle importante. Les communes assurent généralement l'approvisionnement en eau. Il arrive cependant que cette tâche soit confiée à des sociétés anonymes. Le plus souvent, il s'agit de collectivités de droit public. Dans de nombreuses régions, on assiste aussi au regroupement de plusieurs communes, qui assurent ensemble l'approvisionnement en eau. On compte en outre de nombreuses entreprises organisées sous forme de sociétés mixtes de distribution, qui endossent ainsi simultanément différentes missions d'approvisionnement (p. ex. gaz et eau ou gaz, eau et électricité). Il n'existe cependant pas de modèle unique pour l'approvisionnement en eau en Suisse.

3.2 Service d'approvisionnement

L'eau est utilisée à de nombreuses fins en Suisse, par les ménages, mais aussi par l'artisanat, l'industrie et l'agriculture. Les Suisses et les Suissesses consomment chaque jour quelque 142 litres d'eau potable pour cuisiner, boire, laver leur linge et faire leur toilette. La consommation des ménages représente environ un quart de la consommation totale. L'agriculture, quant à elle, en absorbe 20 %. Près de la moitié de la consommation d'eau imputée à l'agriculture reste cependant inexploitée et alimente des fontaines. L'artisanat et l'industrie totalisent la moitié de la consommation d'eau (fig. 4).

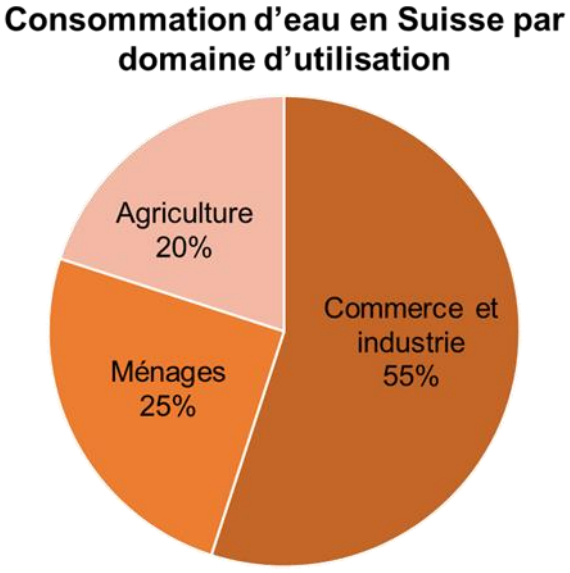

Fig. 4 Consommation d'eau en Suisse

Les trois quarts de l'eau consommée par le secteur agricole suisse sont requis pour élever le bétail et fournir des produits laitiers ainsi que de la viande de bœuf et de porc. Contrairement à ceux d'origine animale, les produits d'origine végétale sont majoritairement importés. Une part conséquente de l'eau consommée par l'agriculture, l'industrie et l'artisanat provient non des services des eaux (publics), mais de captages privés concessionnaires dont le volume dépasse même celui du secteur public. Outre son importance dans le secteur productif, l'eau potable sert également à éteindre les incendies.

3.3 Présentation générale des systèmes critiques

L'approvisionnement en eau est fortement tributaire des systèmes TIC. Sans eux (par ex. systèmes SCADA ou moyens de communication), le traitement de l'eau et le processus de communication ainsi que la surveillance de la zone de desserte ne peuvent que partiellement être maintenus. Le tableau ci-dessous présente les principaux systèmes pour les processus-clés de l'approvisionnement en eau :

Liste des principaux systèmes TIC pertinents pour le sous-secteur de l'approvisionnement en eau	
Processus clés Approvisionnement en eau	Principaux systèmes TIC
Collecte des eaux	Système SCADA*
Traitement	Système SCADA*
Transport	Système SCADA*
Stockage	Système SCADA*
Distribution	Système SCADA*
Processus de communication	Téléphonie mobile et fixe, VoIP, E-Mail
Processus de pilotage	Système SCADA*

Tab. 2 Principaux systèmes TIC utilisés pour approvisionner en eau la population suisse

* Le système SCADA englobe les systèmes de commande de la distribution d'eau. Il peut s'agir, par exemple, du système de commande d'une station de traitement d'eau de lac, modules de commande API de l'installation y compris le système de contrôle-commande.

4 Conclusions

L'eau potable est à la fois un élément vital pour les humains ou organismes vivants et un moyen de production essentiel dans diverses branches économiques. Ce qui caractérise le système suisse de distribution d'eau, ce sont les différentes formes d'organisation et le nombre élevé d'acteurs impliqués. À l'heure actuelle en Suisse, l'approvisionnement en eau potable est assuré par 2500 fournisseurs. Ils obtiennent souvent l'eau auprès de différentes sources aux ressources hydriques différentes et de qualité parfois variable. En Suisse, l'eau potable est constituée à 80 % d'eau de source ou souterraine et à 20 % d'eaux de surface. Le traitement des eaux de surface est un processus complexe, qui implique généralement le réglage précis de plusieurs étapes de filtration et de désinfection. En cas de défaillance des systèmes TIC utilisés pour commander ces processus, le traitement de l'eau ne peut plus s'effectuer en toute sécurité. Compte tenu de la grande complexité du processus, un pilotage manuel n'est possible que de façon très limitée.

Une défaillance de l'approvisionnement en eau sur une large zone suite à une ou plusieurs cyberattaques aurait des conséquences désastreuses pour les populations concernées et l'économie. Il existe différentes façons de parer à une défaillance de systèmes TIC jouant un rôle clé dans la distribution d'eau, des installations individuelles, voire même de l'approvisionnement en électricité. Un contrôle périodique des processus et installations sur la base de la présente norme minimale est ici primordial. En tant que recommandation pour la branche, elle constitue en effet un outil pratique permettant à toute entreprise de distribution d'eau de relever son niveau de sécurité TIC au minimum standard. L'outil d'évaluation est destiné aux distributeurs d'eau dont la zone de desserte couvre 5000 habitants ou plus. Les très grandes compagnies, dont la zone de desserte couvre plus de 50000 habitants approvisionnés, doivent viser un niveau de sécurité nettement supérieur aux exigences minimales. Les distributeurs d'eau desservant moins de 5000 habitants peuvent appliquer les recommandations spécifiques fournies à l'Annexe 3, pour une mise en œuvre simplifiée de la norme.

La méthode de défense en profondeur (Defense in Depth) appliquée par cette norme minimale privilégie une approche basée sur les risques. Elle n'offre pas de solutions standard, mais encourage les différents acteurs de l'approvisionnement en eau à analyser et à évaluer leur situation en matière de cybersécurité à l'aide d'une approche basée sur les risques. La norme minimale TIC permet à chaque entreprise ou organisation de définir elle-même sa propension au risque, ainsi que d'élaborer et de prioriser les mesures d'amélioration qui s'imposent. La responsabilité de la cybersécurité relève systématiquement de la compétence du distributeur d'eau (et éventuellement aux responsables politiques).

À travers l'outil d'évaluation basé sur Excel, cette norme minimale TIC permet aux acteurs du secteur de l'approvisionnement en eau de relever leur niveau de sécurité simplement, mais de façon systématique, et d'atteindre un niveau minimum élevé homogène. La sécurité des TIC n'est pas abordée comme un état, mais comme un processus itératif dynamique. Cette norme minimale repose sur une méthode éprouvée d'incitation à une mise en œuvre efficace de ce processus. D'autres secteurs d'approvisionnement, comme celui de l'électricité, utilisent les mêmes principes et méthodes, ce qui favorise les effets de synergie, notamment pour les sociétés mixtes de distribution.

La SSIGE communiquera largement sur la norme minimale TIC au sein du secteur, afin de permettre la diffusion et l'application maximales des connaissances nécessaires au respect de cette Recommandation de la branche. Elle accompagnera ses membres pour l'introduction et la mise en œuvre de la norme minimale à travers des formations et des conseils spécifiques.

5 Appendice

5.1 Documents de référence et normes

Le présent document intègre des plans, recommandations et mesures issus de diverses normes et d'autres documents normatifs (cf. tableau ci-dessous).

Titre	Année	Éditeur(s) et description
Mesures de protection des systèmes de contrôle industriels (SCI)	2013	Éditeur : **Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI** Basées sur des documents américains de l'Industrial Control Sys-tems Cyber Emergency Response Team (SCADA-CERT) du Département de la Sécurité intérieure (DHS) ainsi que du National Institute of Standards and Technology (NIST), ces instructions décrivent en huit pages, de façon succincte et pragmatique, les onze principales mesures à mettre en œuvre par les exploitants de systèmes SCADA.
Analyse des risques et des vulnérabilités du sous-secteur de l'approvisionnement en eau	2016	Éditeur : **Office fédéral pour l'approvisionnement économique du pays (OFAE)** Cette analyse des risques et des vulnérabilités repose sur la Stratégie nationale de protection de la Suisse contre les cyber-risques (SNPC) et sur la Stratégie nationale pour la protection des infrastructures critiques (PIC). Elle a pour but d'analyser la vulnérabilité aux défaillances ou aux perturbations des TIC dans le sous-secteur critique de l'approvisionnement en eau.
Guide pour la protection des infrastructures critiques (guide PIC)	2015	Éditeur : **Office fédéral de la protection de la population (OFPP)** Ce guide constitue un instrument d'examen et, le cas échéant, d'amélioration de la résilience des infrastructures critiques. Il est notamment conçu pour être utilisé dans des sous-secteurs (aussi appelés secteurs partiels) critiques par les exploitants, les associations sectorielles et les autorités compétentes. Le guide décrit pour l'essentiel une procédure potentielle de gestion des risques : analyse (identification des ressources, vulnérabilités, risques), évaluation, mesures et leur garantie (mise en œuvre, contrôle et amélioration). Cette procédure peut tout à fait ou devrait être intégrée même aux processus de gestion existants ou exécutée sur la base de ces derniers.
Stratégie nationale pour la protection des infrastructures critiques (PIC)	2012 et 2018	Éditeur : **Office fédéral de la protection de la population (OFPP)** La stratégie décrit le champ d'application, désigne les infrastructures critiques (notamment d'approvisionnement en eau) et fixe les principes directeurs de la protection des infrastructures critiques. La stratégie nationale PIC s'adresse à tous les services qui ont des responsabilités dans ce domaine, en particulier aux différentes autorités concernées, aux responsables politiques et aux exploitants d'infrastructures critiques.
Stratégie nationale de protection de la Suisse contre les cyber-risques (SNPC)	2012	Éditeur : **Unité de pilotage informatique de la Confédération (UPIC)** La protection des infrastructures d'information et de communication contre les cyber-risques représentant un intérêt majeur pour la Suisse, le Conseil fédéral a ordonné l'élaboration d'une stratégie nationale visant à protéger notre pays contre de tels risques. Cette stratégie a pour but de dresser un panorama actuel de ces risques et de montrer les moyens dont dispose la Suisse pour y faire face, où se situent les lacunes et comment y remédier le plus efficacement possible. La stratégie identifie les structures existantes et définit des objectifs ainsi que sept champs d'action assortis de mesures ad hoc (p. ex. analyses des risques et des vulnérabilités d'un sous-secteur tel que l'approvisionnement en eau – cf. ci-dessus).

Titre	Année	Éditeur(s) et description
Loi fédérale sur l'approvisionnement économique du pays (Loi sur l'approvisionnement du pays, LAP)	État 2016	Éditeur : **Assemblée fédérale de la Confédération suisse** La présente loi régit les mesures visant à garantir l'approvisionnement du pays en biens et services vitaux lors d'une pénurie grave à laquelle les milieux économiques ne peuvent pas faire face par leurs propres moyens. La Confédération peut encourager, dans les limites des fonds octroyés, des mesures prises par des entreprises de droit privé ou public pour assurer l'approvisionnement économique du pays, dès lors que ces mesures contribuent, dans le cadre de la préparation à une situation de pénurie grave, à renforcer substantiellement les systèmes d'approvisionnement et infrastructures vitaux. L'une de ces mesures constitue la présente norme minimale TIC pour l'approvisionnement en eau.
Étude sectorielle KRITIS sur l'alimentation et l'eau (en allemand uniquement)	État 2015	Éditeur : **Bundesamt für Sicherheit in der Informationstechnik (BSI)** L'Office fédéral – allemand – chargé de sécuriser les technologies de l'information est l'un des principaux interlocuteurs en Allemagne parmi les autorités compétentes en matière de protection d'infrastructures critiques. À travers différentes activités, comme l'organisation d'échanges entre professionnels de la branche, la mise à disposition de normes et de guides sur les grands thèmes liés à la sécurité informatique, des projets nationaux et la coordination de l'initiative nationale UP KRITIS, le BSI soutient la mise en œuvre des stratégies nationales pour la protection des infrastructures critiques (stratégie KRITIS) et la cybersécurité. Pour ses travaux, le BSI a besoin d'informations précises sur les fonctions des prestations critiques et l'importance associée de certains équipements et installations (KRITIS).
OAEC – Ordonnance sur la garantie de l'approvisionnement en eau potable en temps de crise	État 2017	Éditeur : **Conseil fédéral suisse** Cette ordonnance vise à garantir l'approvisionnement en eau potable en temps de crise. Les mesures prévues doivent être de nature à assurer : a. l'approvisionnement normal en eau potable aussi longtemps que possible, b. la réparation rapide des dérangements, c. la mise à disposition, en tout temps, de l'eau potable indispensable à la survie.
DVGW W 1060 (M) – Notice technique, aide-mémoire	2017	Éditeur : **Deutscher Verein des Gas- und Wasserfaches** Le DVGW a rédigé plusieurs règlements et guides sur la sécurité informatique dans le domaine de l'approvisionnement en eau. Sa fiche technique W1060 offre une vue d'ensemble des règlements existants et des outils d'aide à leur mise en œuvre.
Process Control System Security Guidance for the Water Sector	2017	Éditeur : **American Water Works Association (AWWA)** L'objectif du guide de l'AWWA est de fournir aux propriétaires/exploitants d'entreprises d'approvisionnement en eau une recommandation de procédure cohérente et répétable pour réduire la vulnérabilité aux cyberattaques.
SCADA Security Good Practices for the Drinking Water Sector – TNO Report	2008	Éditeur : **TNO Defence, Security and Safety** Ces bonnes pratiques du secteur néerlandais de l'approvisionnement en eau potable sont destinées à augmenter la résilience de l'ensemble de la branche face aux cybermanipulations frauduleuses des systèmes de surveillance et de saisie de données (SCADA), ainsi que d'autres outils et logiciels du domaine des TIC.
Produits de sécurité qualifiés – ANSSI (France)	2017	Éditeur : **ANSSI (Agence nationale de la sécurité des systèmes d'information)** La qualification d'un produit de sécurité est prévue par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Titre	Année	Éditeur(s) et description
Guide d'hygiène informatique – ANSSI (France)	2017	Éditeur : **ANSSI (Agence nationale de la sécurité des systèmes d'information)** Guide d'hygiène informatique : 42 mesures essentielles pour assurer la sécurité de votre système d'information et les moyens de les mettre en œuvre, outils pratiques à l'appui.
Les règles de sécurité – ANSSI (France)	2017	Éditeur : **ANSSI (Agence nationale de la sécurité des systèmes d'information)** Les règles de sécurité sont à la fois organisationnelles et techniques. Elles doivent, pour la plupart, être déjà appliquées par l'ensemble des opérateurs pour sécuriser efficacement leurs systèmes d'information d'importance vitale. Ces règles de sécurité s'appliquent notamment aux SIIV opérés par les sous-traitants.
10 Steps to Cyber Security – NCSC (UK)	2016	Éditeur : **NCSC (National Cybersecurity Centre, UK)** Guide expliquant comment les organisations peuvent se protéger dans le cyberespace. • introduction à la cybersécurité pour les personnels dirigeants, • livre blanc qui explique à quoi ressemble une cyberattaque ordinaire et le mode opératoire des cyberpirates, • dix fiches de conseils techniques que vous devriez envisager de mettre en place.
ISO 27001:2013 Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences ISO 27002:2013 Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information	2013	Éditeur : **International Standard Organization (ISO)** Cette norme détaille les exigences relatives à un système de gestion de la sécurité de l'information (SMSI). La suite ISO/CEI 27 000 (ou ISO 27k) comprend une série de normes concernant la sécurité de l'information, dont les suivantes présentent un intérêt ici : • 27000:2016 Vue d'ensemble et vocabulaire (:2016 indique l'année de publication) • 27001:2013 Exigences: principes de base avec contrôles et objectifs de contrôle en annexe • 27002:2013 Exigences: principes de base avec contrôles et objectifs de contrôle en annexe • 27003:2010 Lignes directrices pour la mise en œuvre • 27005:2011 Gestion des risques Désormais les plus répandues, les normes de sécurité ISO 27000 devraient s'avérer décisives dans les années à venir. Aujourd'hui déjà, la bonne approche consiste à observer les normes de sécurité ISO. Contrairement à d'autres textes normatifs d'IT-Grundschutz, de l'ANSI/ISA ou du NIST, elles sont moins détaillées, utilisables de manière flexible et peuvent être améliorées et étendues en continu sur une plus longue période.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev.2	2015	Éditeur : **National Institute of Standards and Technology (NIST)** Ce guide fournit une introduction complète au système SCADA, aux topologies et aux architectures, identifie les menaces et les vulnérabilités, et formule des recommandations pour les contre-mesures et l'atténuation des risques. Des contrôles spécifiques aux systèmes SCADA, basés sur le cadre 800-53 du NIST, sont également présentés.
ISA 62443 Industrial communication networks – Network and system security	2009 ss	Éditeur : **International Society of Automation (ISA)** Série d'un total de 13 normes de sécurité et rapports techniques en matière de systèmes de contrôle-commande industriels (IACS). Ces normes sont généralement applicables dans le domaine de l'automatisation industrielle et ne sont pas spécifiques à l'approvisionnement en électricité. Elles se basent sur les normes ISO 27000 et les étoffent par l'ajout de différences et de particularités propres à l'automatisation industrielle. Il convient de mentionner notamment le traitement de l'architecture réseau et zonale, qui n'est guère ou pas aussi détaillé dans d'autres normes.

Titre	Année	Éditeur(s) et description
Recommended Practice: Improving Industrial Control System Cyber Security with Defense in Depth Strategies	**2016**	Éditeur : **Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** Édition revue et corrigée d'une précédente publication datant de 2006. Introduction complète à la stratégie de défense en profondeur dans le cadre de la sécurité des systèmes de contrôle industriels.
Catalogues « IT-Grundschutz » du BSI 15. Version de 2016 Certification du BSI suivant la norme ISO 27001 sur la base de l'IT-Grundschutz BSI – Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz	2016	Éditeur : **Bundesamt für Sicherheit in der Informationstechnik (BSI)** À l'aide des normes 100-1 à 100-4 du BSI, l'« IT-Grundschutz » (méthodologie de protection de base des technologies de l'information) décrit une procédure pour mettre en place et de maintenir un système gérant la sécurité de l'information (SMSI). Les catalogues de l'IT-Grundschutz détaillent la mise en œuvre des mesures et des objectifs qui en découlent. Le SMSI ainsi créé satisfait aux exigences de la norme ISO 27001 et dispose d'un équivalent aux recommandations de la norme ISO 27002. La sécurité peut être introduite et contrôlée selon les procédures de l'IT-Grundschutz developpées par le BSI, mais aussi conformément aux normes de la famille ISO 27000. Ces deux options sont compatibles dans leur approche. Elles sont utilisées pour mettre en place et exploiter un SMSI, qui identifie les risques dans le domaine de la sécurité de l'information et les réduit à un niveau acceptable par le biais de mesures appropriées. Alors que l'analyse et l'évaluation des risques constituent un élément essentiel d'un SMSI conforme à la norme ISO 27001, cette analyse n'est requise que dans certains cas particuliers pour l'IT-Grundschutz du BSI. Les catalogues de cette protection de base décrivent par le menu la procédure permettant de réduire au maximum les risques. Quant aux normes ISO, elles laissent davantage de place à l'interprétation et offrent une plus grande souplesse, mais fournissent également des instructions et un soutien moins détaillé. À l'inverse, l'approche de l'IT-Grundschutz, comme son nom l'indique, offre une « protection de base ». L'effort requis pour obtenir la certification ISO est moindre.
BSI ICS Security – Kompendium	2013	Éditeur : **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Ce compendium est un ouvrage de référence destiné à faciliter l'accès à la sécurité informatique dans les systèmes SCADA. Les bases SCADA nécessaires, les processus y afférents, les normes pertinentes et un lien concret avec l'IT-Grundschutz y sont expliqués, les différences et lacunes des normes établies, et en particulier de l'IT-Grundschutz dans le domaine de la sécurité SCADA étant mises en lumière.
Norme BSI 100-1 Managementsysteme für Informationssicherheit (ISMS)	2008	Éditeur : **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Cette norme décrit les méthodes, les tâches et les activités pertinentes qui font le succès d'un SMSI et précise les tâches qui incombent à la direction. La méthodologie de l'IT-Grundschutz, qui explique comment développer, pas à pas un SMSI dans la pratique et mentionne des mesures concrètes pour tous les aspects relevant de la sécurité de l'information, favorise la mise en œuvre des recommandations. La norme 100-1 s'adresse aux responsables de l'exploitation informatique, aux délégués à la sécurité, ainsi qu'aux experts et conseillers en sécurité chargés de la gestion de la sécurité de l'information.

Titre	Année	Éditeur(s) et description
Norme BSI 100-2 IT-Grundschutz Vorgehens-weise	2008	Éditeur : **Bundesamt für Sicherheit in der Informations-technik (BSI)** La procédure de l'IT-Grundschutz décrit, étape par étape, comment mettre en place et exploiter un système de management de la sécurité de l'information dans la pratique et à l'aide des catalogues de cette protection de base. Elle se penche de façon très approfondie sur la manière d'élaborer en pratique un concept de sécurité, sur le choix des mesures de sécurité adéquates, ainsi que sur les éléments à prendre en compte lors de la mise en œuvre.
Norm BSI 100-3 Risikoanalyse	2008	Éditeur : **Bundesamt für Sicherheit in der Informations-technik (BSI)** Ce document décrit une méthodologie pour réaliser des analyses de risques, qui complètent un concept de sécurité existant en matière de protection de base des technologies de l'information. Les dangers présentés dans les catalogues de l'IT-Grundschutz sont utilisés comme outils. Une différence essentielle par rapport à la plupart des autres méthodes d'analyse de risques est l'omission totale de la probabilité de survenance des dommages.
BSI-Standard 100-4 Notfallorganisation	2008	Éditeur : **Bundesamt für Sicherheit in der Informations-technik (BSI)** Ce document décrit une méthodologie pour mettre en place un système de gestion des cas d'urgence fondée sur les procédures figurant dans la norme 100-2 et les complétant. Il présente tous les processus au sein d'une organisation pour cas d'urgence, de l'analyse d'impact sur les affaires à la gestion de crise, en passant par le retour à l'exploitation normale et les activités continues de processus en dehors des situations de crise.
ISA 95 / ISO 62264 Intégration du système de commande d'entreprise	2010 ss	Éditeur : **International Society of Automation (ISA)** Série de cinq normes relatives à l'intégration des systèmes informatiques d'entreprise et de contrôle-commande.
Framework for Improving Critical Infrastructure Cyber Security	2014	Éditeur : **National Institute of Standards and Technology (NIST)** Ce cadre découle de l'exigence posée par le décret présidentiel américain intitulé « Improving Critical Infrastructure Cyber Security » (Améliorer la cybersécurité des infrastructures critiques), datant de 2013. Il s'agit d'une compilation de différentes orientations visant à déterminer le statut actuel d'une entreprise et à définir une feuille de route pour l'amélioration des pratiques de cybersécurité en se référant à d'autres cadres et normes tels que ISO 27001, ISA 62443, NIST 800-53 et COBIT.
Communication network dependencies for ICS/SCADA Systems	2016	Éditeur : **European Union Agency for Network and Information Security (ENISA)** Ce rapport se focalise sur les aspects des réseaux de communication et de l'intercommunication entre les systèmes ICS/SCADA et l'identification des vulnérabilités, des risques, des menaces et des conséquences en matière de sécurité pouvant être causés par les systèmes cyber-physiques. Il comporte également un certain nombre de recommandations destinées à réduire les risques détectés. La principale conclusion de l'étude préliminaire est une liste de pratiques et de directives éprouvées visant à limiter autant que possible la surface des systèmes ICS/SCADA exposée aux attaques. Le document a pour objectif principal de fournir un aperçu des dépendances des réseaux de communication des systèmes ICS/SCADA et d'identifier les ressources critiques en matière de sécurité et les scénarios d'attaques et menaces réalistes contre ces réseaux de communication.

Titre	Année	Éditeur(s) et description
Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME). Une protection accrue grâce au programme en dix points élargi	2005	Éditeur : **InfoSurance** L'Association InfoSurance s'occupe depuis plusieurs années des risques liés à l'utilisation de l'informatique dans les petites et moyennes entreprises. Pour aider les entreprises à mettre en œuvre un système de protection adéquat, InfoSurance a publié en 2005 un programme en dix points pour la mise en place d'une protection de base efficace en informatique.

Tab. 3 Normes nationales et internationales relatives à la sécurité des TIC

5.2 Glossar

Abréviation	Description
API	Automate programmable industriel, cf. SCADA
AEP	Approvisionnement économique de pays
BSI	Bundesamt für Sicherheit in der Informationstechnik (Office fédéral allemand chargé de sécuriser les technologies de l'information)
Contrôle-commande	Système de contrôle-commande de réseaux, de stations et de centrales
DMZ	Demilitarized Zone (zone démilitarisée). Désigne un réseau d'ordinateurs avec des possibilités d'accès contrôlées du point de vue de la sécurité (souvent utilisé pour la séparation logique de deux zones de réseau)
DNS	Domain Name System (système de noms de domaine)
eDec	Déclaration électronique de données. Système utilisé par l'Administration fédérale des douanes pour les déclarations d'importation en douane
ENISA	Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)
ERP	Enterprise Ressource Planning, progiciel de gestion intégré
Facility Control	Technique du bâtiment, commande et surveillance des installations
Field	Niveau terrain
FINMA	Autorité fédérale de surveillance des marchés financiers
HIDS	Host Intrusion Detection System (système de détection d'intrusions machine)
HMI	Human Machine Interface (interface homme-machine). Désigne une interface ou une procédure permettant à l'homme d'entrer en contact avec une machine.
IaaS	Infrastructure as a Service (infrastructure en tant que service)
ICS	Voir SCADA
IDS	Intrusion detection system (système de détection d'intrusions)
Inf.	Informatique
IP	Internet Protocol
IPS	Intrusion prevention system, système de prévention des intrusions
ISA	International Society of Automation
ISO	Organisation internationale de normalisation
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Unité de pilotage informatique de la Confédération)
MOU/MOA	Memorandum of Understanding / Agreement, protocole d'accord
MPLS	Multiprotocol Label Switching, technologie utilisée pour le transfert de communication de données
MPLS-TP	Multiprotocol Label Switching Transport Profile, variante du protocole MPLS

NAC	Network access control
NIST	National Institute of Standards and Technology
OAEC	Ordonnance sur la garantie de l'approvisionnement en eau potable en temps de crise
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFPP	Office fédéral de la protection de la population
PaaS	Platform as a Service (plate-forme en tant que service)
PC	Personal Computer (ordinateur personnel)
PDH	Plesiochronous Digital Hierarchy (hiérarchie numérique plésiochrone). Technologie utilisée pour la communication vocale et de données
Private range	Les adresses IP privées (private IP en abrégé) sont les adresses IP qui ne sont pas allouées sur Internet par l'IANA. Elles ont été retirées de l'espace public pour un usage privé, afin de pouvoir être utilisées sur des réseaux locaux sans surcharge administrative (enregistrement des adresses IP).
PRTG Network Monitor	Solution de surveillance complète permettant de surveiller les temps de disponibilité/d'arrêt, le trafic et l'utilisation d'un réseau.
Réseau de communication	Réseau de communication interne des données et vocale
SaaS	Software as a Service (logiciel en tant que service)
SCADA	Supervisory Control and Data Acquisition (système d'acquisition et de contrôle des données). Désigne un système de surveillance et de pilotage de processus techniques. Comprend des capteurs, des conduites, des ordinateurs et un poste de conduite du système (de production). Concerne essentiellement les systèmes de mise en service, de pilotage de la production des processeurs, mais aussi les systèmes de caisse des commerces de détail. Synonyme d'ICS. Comprend également les API.
SDH	Synchronous Digital Hierarchy. Désigne une technologie utilisée pour le transfert de la communication vocale et de données
SIEM	Security Incident and Event Management (gestion des événements et incidents de sécurité)
SLA	Service level agreement, accord sur le niveau de service
SMSI	Système de management de la sécurité de l'information
SQL	Désigne un langage informatique servant à définir des bases de données relationnelles. Il permet aussi de traiter (ajouter, modifier ou supprimer) et de rechercher des informations dans lesdites bases de données.
Thin client	Un thin client, lean client ou slim client (client léger) est un client, c'est-à-dire un ordinateur ou un programme, qui dépend de l'aide d'un serveur pour effectuer ses tâches.
TI	Technologies de l'information
TIC	Technologies de l'information et de la communication (informatique)
TO	Technologie opérationnelle (systèmes SCADA notamment)
UPIC	Unité de pilotage informatique de la Confédération
VoIP	Voix sur IP (voice over IP)
VPN	Virtual private network
WAN	Wide area network

Tab. 4 Table des abréviations

5.3 Liste des figures

5.4 Liste des tableaux