

Réseaux d'eau potable : une infrastructure qui reste à sécuriser



Par Jacques-Olivier Baruch,
Technoscope

ABSTRACT

**Drinking water networks:
an infrastructure that remains
to be secured.**

Risk is defined as the probability of occurrence of a threat along with the extent of the impact it may generate. The drinking water network however, both as a whole and in terms of each of its components, contains a number of vulnerabilities that could constitute a weakness allowing a threat to occur. Even though contractor awareness is growing, the drinking water network remains to be secured.

Le risque est la combinaison de la probabilité de réalisation d'une menace avec la valorisation de l'impact qu'elle peut engendrer. Or, le réseau d'eau potable, dans son ensemble comme au niveau de chacun de ses constituants, recèle un certain nombre de vulnérabilités susceptibles de constituer une faiblesse de nature à permettre à une menace de se réaliser. Même si la prise de conscience progresse chez les exploitants, le réseau d'eau potable reste un ouvrage à sécuriser.

Usage sauvage en juillet 2015 des bouches d'incendie aux Essarts-le Roi, dans les Yvelines, intrusion au mois de mai dans le réservoir de l'Abyrne à Dreux, dans l'Eure-et-Loir, bouches d'incendies vandalisées à Lille

en septembre, pollution suspecte au sein d'un réseau d'eau potable en Haute-Loire en novembre, effraction l'année précédente de ceux de Florensac dans l'Hérault : les actes de malveillance se multiplient et concernent les réseaux d'eau potable

Composé d'un cylindre électronique et d'une clé intelligente mécatronique, abloy Protec2 Cliq est un système incrochetable et inviolable qui se caractérise par un double niveau de sécurité : variation mécanique et code électronique crypté.



Abloy

au même titre que n'importe quel autre type d'ouvrages. Sans compter les erreurs humaines comme la manœuvre malencontreuse des pompiers de Lyon en septembre dernier qui ont introduit un additif anti-incendie dans le réseau d'eau en s'étant trompé de sens de la pompe. Sous état d'urgence, le risque terroriste doit également être pris en compte. Erreur, malveillance voire attentat, comment se protéger et de quoi ?

Réduire les possibilités d'intrusion physique

La première des actions à mener consiste à réduire au maximum les risques d'intrusions physiques sur les sites liés au réseau d'eau potable, par nature très dispersés. Bien que la plupart soient désormais clos, il faut savoir qui peut entrer, quand, pourquoi, et qui ne le peut pas. Et, le cas échéant, en être avertis.

Trois solutions peuvent être retenues. La première concerne les transmissions d'alarmes IP via GPRS. Lacroix Sofrel, Aqualabo Perax ou Mios proposent ainsi des solutions très abouties intégrant des fonctions de sécurité avancées : contrôle d'accès avec lecteur de badge RFID, détection de présence, alarme et levée de doute avec Camera IP en cas d'intrusion.

La seconde repose sur une vidéosurveillance en circuit fermé avec une détection d'intrusion. Elle est assez simple à mettre en œuvre à partir de produits disponibles sur le marché et peut être customisée selon les besoins de chacun, mais elle requiert la surveillance d'un opérateur en permanence.

La troisième est le contrôle d'accès par clé

Optimiser les infrastructures techniques

Les exploitants d'infrastructures telles que les réseaux d'adduction en eau potable ou les réseaux d'assainissement recherchent en permanence une utilisation optimale de leurs ressources et de leurs équipements. Le logiciel de gestion Kanio®, développé par HST Systemtechnik, permet d'optimiser l'exploitation technique des infrastructures tout en réduisant au maximum les coûts

d'exploitation et de maintenance, en assurant une disponibilité maximale des systèmes et des équipes.



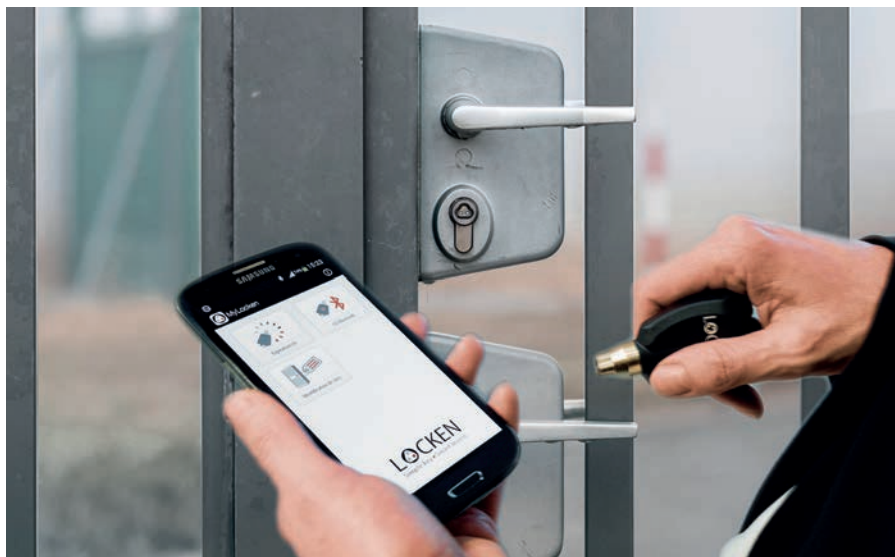
HST

ments. Interfaçable avec la plupart des SIG, PLS et systèmes ERP du marché, il s'intègre également de manière transparente dans les environnements systèmes existants. Kanio® s'architecture autour de cinq modules différents : la gestion des objets, la gestion de l'activité, la gestion des ressources, la gestion des commandes et le reporting. Des modules supplémentaires sont disponibles pour des applications mobiles et des représentations graphiques (cartes) des différents équipements.

électronique. Les serrures électroniques développées par Locken ou Abloy sont des outils assez simples à mettre en œuvre qui ne nécessitent pas de travaux importants. Un nouveau cylindre est inséré dans la porte existante et reçoit la clé électronique. Celle-ci est autonome en énergie et permet ou non l'accès à l'une des entrées du réseau. Mais il est possible d'aller bien plus loin. Avec l'application "MyLocken" de Locken, par exemple, l'utilisateur peut, en arrivant sur le site, se connecter au logiciel d'administration via son Smartphone pour récupérer ses droits d'accès. Ceux-ci sont alors transmis en temps réel à la clé grâce au module Bluetooth intégrée dans cette dernière. « Cela permet d'attribuer des droits d'accès pour une durée très courte en fonction des besoins et contribue à renforcer la sécurité sur des sites vulnérables » précise Catherine Laug chez Locken. Une autre solution consiste à utiliser

la nouvelle clé WiFi qui permet d'attribuer des droits d'accès, de transmettre des rapports d'activité en temps réel ainsi que de coordonner l'ensemble des opérations réalisées sur les sites avec un contrôle d'accès et des fonctionnalités qui, jusqu'à présent, étaient réservées aux solutions câblées. Les 64 stations de captage, les 86 réservoirs et les 42 stations de pompage de la régie d'agglomération de Charleville-Mézières-Sedan, dans les Ardennes, sont en train d'être équipés d'une solution de ce type. Ce type de système protège également les accès aux sites de production et de stockage d'eau potable de nombreuses agglomérations comme par exemple Châlons en Champagne mais aussi bien d'autres grandes villes françaises.

Mais pour que ces systèmes soient efficaces, les codes d'accès doivent être changés au maximum tous les trois mois, comme d'ailleurs tous les mots de passe



Locken

L'application de Locken, combinée à la clé Bluetooth, permet d'attribuer des droits d'accès en temps réel, seulement pour la durée de l'intervention sur un site. Cela est un facteur clé pour le renforcement de la sécurité.



ABLOY® PROTEC²

GARDEZ LE CONTRÔLE MÊME A DISTANCE



Web Manager

SYSTÈME DE CONTRÔLE D'ACCÈS SANS FIL

- Large gamme de cylindres incrochetables
- Longévité et haute résistance aux intempéries
- Energie contenue dans la clé
- Gestion des droits via un logiciel en ligne



Nouveau ! CLIQ™ CONNECT

Faites entrer votre système de verrouillage dans l'ère du mobile



Le système Copernic de Bayard permet d'avoir une connaissance de l'usage des poteaux d'incendie 24h/24, une évaluation des volumes puisés, des alertes en cas de fraude... en horodatant toute manipulation.

protégeant les différents processus de production et de distribution d'eau potable. « Ce n'est pas fait dans 95 % des cas, regrette Olivier Vallée, de Rockwell Automation. Comme dans tous les systèmes industriels, la routine prend le pas sur la sécurité. Il faudrait être plus vigilant ». Pour augmenter la sécurité, Abloy préconise de donner des droits d'accès à durée limitée à 24 heures et uniquement aux personnes autorisées à rentrer sur les lieux. « C'est ce que font la plupart de nos clients », souligne Mélanie Dubus chez Abloy. Ces droits sont chargés sur la clé via des bornes de rechargement qui existent sous plusieurs formes (murales, mobiles ou par téléphone) mais qui obligent les utilisateurs à revalider leurs droits pour limiter les risques liés aux pertes/vols/usages abusifs de clés.

De même, chez Locken, les droits d'accès peuvent être paramétrés de façon totalement personnalisée selon des plannings prédéfinis (plages horaires, durée...) ou avec attribution des droits sur site avec les nouvelles clés.

Le mode d'administration de ces droits et du niveau de sécurité de l'outil d'administration et des données associées est également essentiel. Chez Abloy, les droits sont administrés uniquement par des personnes habilitées sur un logiciel CLICK WEB Manager hébergé sur des serveurs sécurisés. Les données sont cryptées AES dans la base et lors de leur transfert entre les éléments du système.

Autre talon d'Achille de ces systèmes: en cas d'incendie, les portes s'ouvrent automatiquement afin de permettre au personnel de quitter le site. Rien n'empêche alors un tiers d'en profiter pour s'introduire à l'intérieur. Dans ce cas, la seule parade est la présence de gardiens. Les nouvelles technologies sont précieuses mais elles ne remplacent pas toujours et en tout lieu la présence humaine...

Protéger les ouvrages jugés annexes

Comme le montrent les types d'actes de malveillances recensés, ce sont les ouvrages annexes qui sont le plus souvent

le maillon faible de la chaîne.

Les châteaux d'eau, souvent excentrés, avec une vue imprenable sur les alentours, sont les premiers visés de par l'attrait qu'ils exercent. Du fait de leur position géographique, ils constituent des points hauts sur lesquels des concessions sont souvent faites aux opérateurs de télécommunications pour y installer leurs antennes. Avec les droits d'accès qui y sont afférents, ils ouvrent de nouveaux risques pour l'eau et à la garantie de sa qualité sanitaire.

Une solution est de séparer l'accès au château d'eau, c'est-à-dire au bâtiment lui-même, de l'accès à la cuve et son eau. C'est le principe du dispositif de protection et de sécurisation renforcée mis au point par Bertrand Vasconi, ingénieur, ancien cadre et ancien directeur adjoint d'agence chez Veolia Eau, qui repose sur l'installation, à proximité de la cuve, d'éléments mobiles (deux demi-

Le système de protection développé par Bertrand Vasconi fonctionne sans électronique ni énergie, et présente l'avantage de détecter l'intention volontaire, en cas d'effraction, en différenciant l'intrusion dans le château d'eau de l'accès aux cuves.



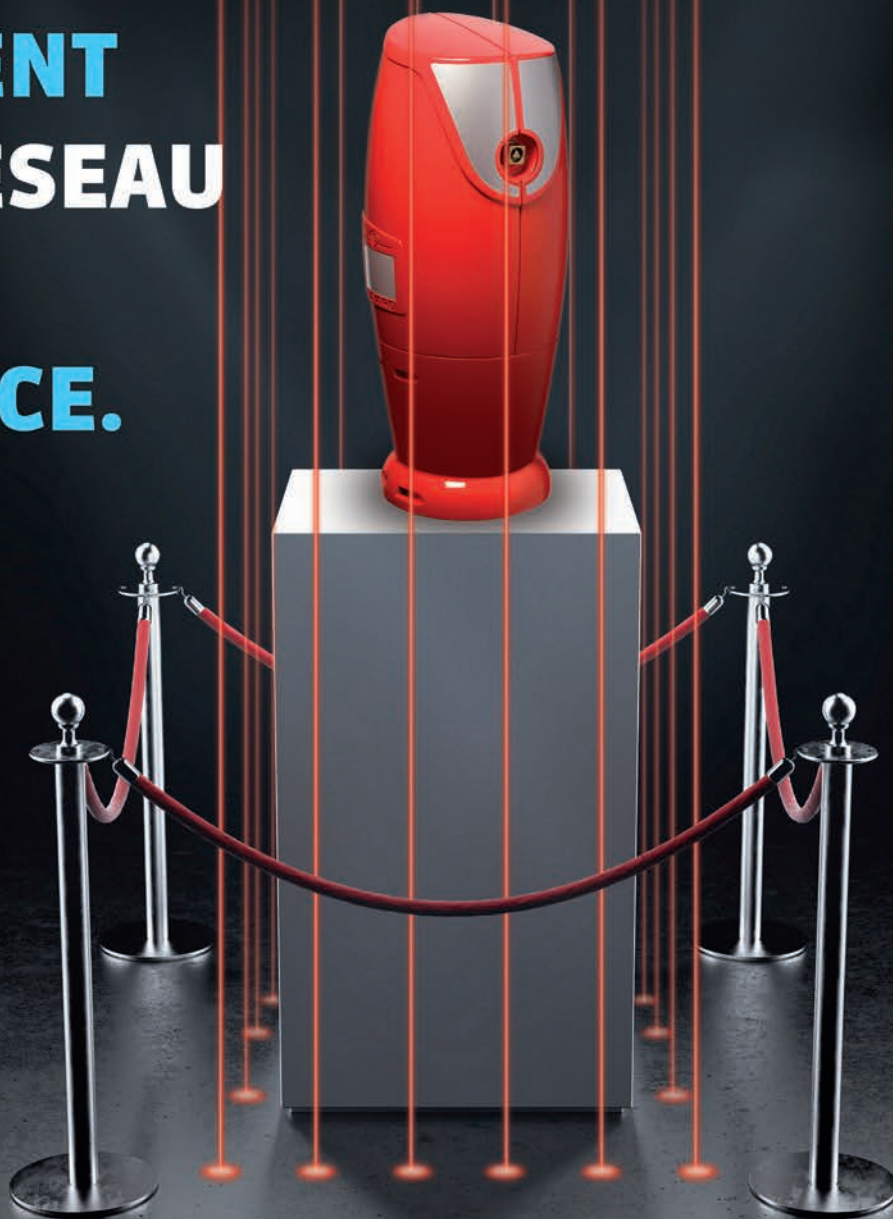
cylindres par exemple) qui se déplacent, se referment et bloquent ainsi tout accès à l'eau, y compris à ceux qui viennent procéder aux opérations d'entretien et de maintenance du château d'eau. Objectif: dissocier l'intrusion dans le château d'eau, ou le réservoir, de l'effraction réelle sur la cuve. « La sécurisation des réservoirs et des châteaux d'eau est une nécessité, explique-



L'omniprésence des capteurs sur un nombre et une variété croissante d'équipements associée à une multiplication des points de mesure génère une quantité impressionnante de données mais aussi d'alertes, rendant indispensable une analyse permanente des incidents et de leurs impacts en fonction des problèmes.

COPERNICTM

LE RENDEMENT DE VOTRE RÉSEAU SOUS HAUTE SURVEILLANCE.



Sécurisez la gestion de votre parc incendie.

Découvrez la dernière innovation BAYARD, un système de surveillance qui va révolutionner la gestion de votre parc incendie.

Sa mission : vous aider à booster le rendement de votre réseau en vous signalant en temps réel toutes les informations relatives à son fonctionnement. Connaissance de l'usage de vos poteaux 24h/24, évaluation des volumes puisés, alertes en cas de fraude, ... Grâce à Copernic, aucune information ne vous échappera.



 **BAYARD**
BY TALIS

«...il, mais sécuriser le périmètre extérieur ou installer une télésurveillance ne suffit pas. Il faut également protéger et isoler l'eau stockée dans la cuve. C'est exactement comme installer une porte mais ne pas l'équiper d'une serrure ». Le système développé, dont la solution standard de base fonctionne sans électronique ni énergie, présente l'avantage de différencier et détecter, en cas d'effraction, l'intrusion dans le réservoir, et la volonté d'accéder aux cuves.

« Du coup, les mesures adaptées comme par exemple l'isolement du réservoir ou la mise en fonctionnement du by-pass (si le réservoir en est équipé), peuvent être aussitôt déclenchés », explique Ber-

Le switch routeur Radiflow 3180 de Factory Systèmes est doté de mécanismes de sécurité intégrés spécialement conçus pour les applications SCADA. Il surveille les commandes SCADA via une inspection approfondie des paquets pour valider leur adéquation avec la logique de l'application pour des fonctions spécifiques.



trand Vasconi. Le dispositif préserve l'accessibilité du sommet de l'ouvrage pour des techniciens de maintenance sans qu'ils ne puissent pour autant accéder à l'eau s'ils n'y sont pas habilités. Eau et cuve(s) sont ainsi protégées des chutes volontaires ou involontaires de produits ou de matériels, de pollutions par des contaminants de toutes natures (terre, saletés, poussières, etc.), des projections ou écoulements divers, et même des pollutions imputables aux animaux volants ou rampants. « Le fait de connaître le motif de l'in-

trusion facilite les constats, favorise la continuité du service en évitant les nettoyages sans objet, voire une purge du réseau et de ses équipements, souligne Bertrand Vasconi. Il en résulte automatiquement des gains économiques directs

et indirects pour tous avec la diminution du nombre d'interventions sur site, la réduction du nombre d'analyses d'urgence, la baisse du nombre d'heures

L'eau, cibles des guerres modernes ?

La directive nationale de sécurité (DNS) relative au secteur de la gestion de l'eau prend en considération les risques liés à différents types d'événements : contamination volontaire, sabotage ou prise de contrôle d'une installation, agression du personnel, employé(s) désireu(x) de se venger, acte sectaire ou terroriste, etc... Sans entrer dans le détail des différents modes opératoires possibles, il apparaît que le réseau d'eau et ses organes associés font partie des cibles les plus vulnérables et paradoxalement les moins protégées dans notre pays. Pourtant, face à une contamination volontaire réalisée depuis la voie publique, le groupe de travail interministériel pour la préparation de la directive nationale de sécurité pour l'alimentation en eau potable des populations a estimé qu'une telle agression serait difficilement parable sans la mise en place de moyens de protection des hydrants implanté sur la voie publique¹.

1 : Source : Au « non » de Dieu, Max-Henri Boulois, Editions Acteurs de la Société, 2015;

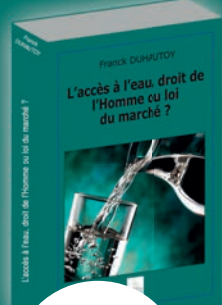
d'interventions en astreinte, mais aussi de la consommation de carburant, de l'usure des véhicules, des excès de vitesse, des risques d'accidents (trajets de nuit, période hivernale, ...) en plus de la diminution du nombre de lavages supplémentaires des cuves ». Ainsi, si une intrusion est détectée dans un ouvrage et retransmise par une alarme, il n'est plus nécessaire d'engager des mesures de sécurité excessives (arrêt complet, distribution d'eau en bouteilles, etc.) mais adaptées si l'eau stockée est touchée ou non par cette infraction. Avec ce dispositif, il n'est plus nécessaire d'interrompre la distribution de l'eau potable si aucun produit n'a pu être déversé dans la cuve.

Bertrand Vasconi a également développé un dispositif qui permet de protéger et de sécuriser les hydrants, ces multiples

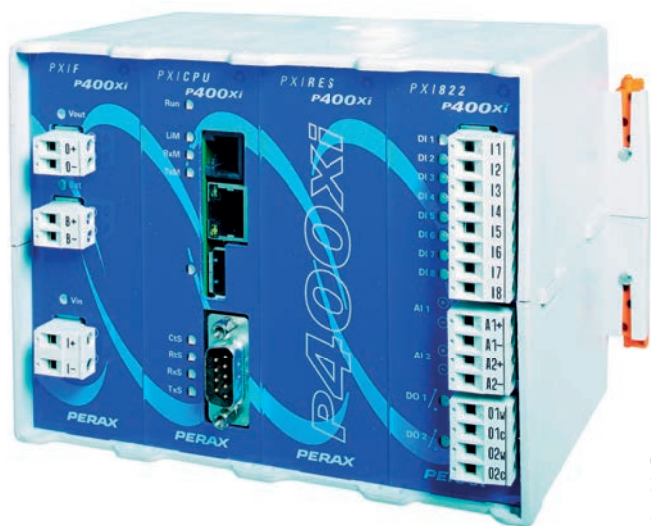
L'accès à l'eau, droit de l'Homme ou loi du marché

Franck DUHAUTOY

Historiquement, l'usage de l'eau ne correspond pas à un encadrement juridique unique. Il est des États et des situations où l'accès à l'eau s'approprie, donne lieu à un marché. Usage libre/usage approprié constituent les deux modèles historiques d'accès à la ressource hydrique. A l'image de sa nature physique, l'eau est ambivalente, renvoyant à deux fonctions : l'une vitale, l'autre économique. En effet, assurer la première par la potabilité a permis l'éclosion de la seconde, car l'absorption d'une eau saine a un coût, géré par des régies publiques ou des entreprises privées. A l'échelle internationale, le droit à l'eau repose seulement, pour l'instant, sur un corpus normatif très morcelé. Certains craignent que cette ressource vitale et les services d'accès en rapport ne soient pris en main par des groupes privés fondant leurs actions uniquement sur la loi de l'offre et de la demande. Cette crainte semble excessive car, en droit international, l'eau matière première n'est présentement pas reconnue comme un produit. De plus, même si tel était le cas, le GATT comporte des mécanismes juridiques autorisant un État en situation de nécessité à limiter ses exportations hydriques. Quant aux négociations de l'OMC permettant de libéraliser l'ensemble des services mondiaux liés à l'eau, elles sont gelées. Certes, le droit de l'investissement et ses techniques d'arbitrage avantagent les firmes hydriques multinationales mais, sociétés civiles voire gouvernements refusent toute atteinte au droit à l'eau par des prix élevés. Composant avec la double nature, économique et sociale, de cette ressource, les droits internes marient souvent non-gratuité et solidarité permettant un accès aux plus démunis. De nombreuses jurisprudences poussent également en ce sens. Parallèlement, le droit du développement durable et le concept de patrimoine commun de l'humanité, qui rend moins exclusif le droit de propriété, font progresser le droit à l'eau.



Format 16 x 24 cm
752 pages
ISBN 979-10-91089-15-9
Prix public : 56,00 euros TTC



Aqualabo Perax

Le réseau privé virtuel (VPN, virtual private network) proposé par Aqualabo Perax avec son automate P400Xi permet d'authentifier les accès et de crypter les échanges.

www.editions-johanet.com

60, rue du Dessous des Berges - 75013 Paris - Tél. +33 (0)1 44 84 78 78
Fax : +33 (0)1 42 40 26 46 - livres@editions-johanet.com

► Il fait tout...,
tout seul !



KROHNE

► measure the facts

► **Solutions complètes
pour la mesure de
Température, Pression,
Analyse, Niveau et Débit**

Compteur d'eau électro-magnétique autonome, le WATERFLUX 3070 assure une très bonne mesure à faible débit et convient même à une installation enterrée ou immergée (IP 68).

- Pour sectorisation, captage d'eau, réseaux de distribution, comptage, etc.
- Sans longueurs droites amont aval
- Capteurs de pression et de température intégrés
- Très faible consommation d'énergie



www.krohne.fr

SOFREL

Solutions de Télégestion et sectorisation

40 ans d'innovations
au service de vos
réseaux d'eau



► **Postes locaux
S500**

- Contrôle et alerte 24h/24
- Télécommande, automatisme
- Archivages et bilans
- Diagnostic permanent des réseaux
- Aide à la maintenance
- Réduction des coûts d'exploitation



► **Data logger LS/LT**

- Télérèlevé de compteurs réseau
- Suivi des volumes et des débits
- Diagnostic et amélioration du rendement du réseau
- Analyse des débits de nuit
- Alerte sur dérive et détection de fuites



Sofrel
LACROIX

www.lacroix-sofrel.fr
www.sectorisation.com

La Multi-Probe + d'EFS associe mesures physiques et analytiques au sein d'une sonde peu intrusive et autonome en énergie : vitesse d'écoulement, température, pression, débit, mais aussi pH, redox, conductivité, turbidité, taux de chlore.



EFS

points de vulnérabilité des réseaux, également sources de vol d'eau et de gaspillage : poteaux ou bouches d'incendie, bouches de lavage, ... Son système, breveté dès 2006 et primé au Salon des maires en 2009, en alliant mécanique et électronique, s'adapte sur tout type d'hydrants en bloquant - ou non - la rotation de la colonne de commande de l'équipement au moyen d'un dispositif amovible introduit dans la prise principale. Le coût de son déploiement sur le parc à l'échelle nationale est évalué à 3,50 € par an et par habitant sur 5 ans, l'équivalent annuel du prix d'un mètre cube d'eau. Avantage de ce dispositif, il ménage et garantit l'accessibilité directe des services d'incendie et de secours tout en empêchant l'accès au réseau à tout utilisateur non autorisé. Ce qui résout la question du vol d'eau récurrent et quotidien sur les poteaux d'incendie, les problèmes d'ouverture intempestive des bouches d'incendie, utilisées comme geysers urbains estivaux : des phénomènes accentués en cas de sécheresse et de canicule comme on en a observé durant les derniers étés chauds et secs. Mais surtout, il évite la possibilité d'injecter des produits nocifs ou contaminants dans le réseau, par des phénomènes de retour d'eau dus à des changements de

débit, de pression, de sens de circulation, involontaires ou non. Car sur les réseaux publics, le poteau d'incendie est l'un des équipements les plus sensibles. De par sa vulnérabilité d'abord, puisqu'il est piqué directement sur le réseau d'eau potable, constituant ainsi une émergence particulièrement sensible au plus près de la population. Par son accessibilité ensuite, qui doit, par principe, rester pleine et entière pour que l'appareil puisse être utilisé rapidement en cas d'accident ou de sinistre. Par leur nombre enfin, avec comme particularité d'avoir comme seuls utilisateurs les services incendie bien que propriété des collectivités. Une solution préventive efficace face à ces menaces, exactement comme une porte physique que l'on ferme véritablement à l'entrée d'un bâtiment stratégique, comparable à « un coffre-fort sur rue pour l'or bleu en quelque sorte », aime-il les comparer.

Raison pour laquelle les fabricants comme Bayard, Camene, Saint-Gobain PAM, SDI France, AVK ou VAG s'attachent eux aussi à développer en propre des solutions sans modifier pour autant les caractéristiques essentielles de l'équipement ni son utilisation comme le font les clés, badges, codes ... qui peuvent susciter une certaine

réticence de certains Services d'Incendies et de Secours, lesquels peuvent y voir des risques de ralentissement, voire de blocage, dans le déroulement des opérations de secours. C'est par exemple le cas du système Copernic de Bayard, une solution d'alerte en temps réel, autonome, qui permet d'avoir une connaissance de l'usage des poteaux 24h/24, une évaluation des volumes puisés, des alertes en cas de fraude comme en cas d'utilisation légitime... en horodatant toutes les manipulations, sans distinction. La carte électronique qui l'équipe sécurise la gestion des parcs incendie en signalant en temps réel toutes les informations relatives à tous ces fonctionnements. Sa communication est basée sur le réseau M2M SigFox présent sur tout le territoire.

Opérateurs d'importance vitale : vers de nouvelles obligations

La sécurisation des réseaux d'eau potable repose aujourd'hui en grande partie sur celle de toute cette intelligence embarquée au sein des différentes étapes de la production et de la distribution de l'eau potable et qui doit être protégée : capteurs, automates, analyseurs, postes de télégestion, superviseurs, etc...

En 2010, Stuxnet, le virus conçu par la national Security agency américaine, s'est répandu dans le réseau iranien pour perturber l'automate qui dirigeait les centrifugeuses de son industrie nucléaire, tout en affichant des données correctes aux opérateurs. Il a été introduit dans le système par un opérateur en interne avec clé USB. « Non seulement ces attaques informatiques occasionnent des pertes de production, donc d'argent, mais elles peuvent détériorer l'équipement, la qualité de l'eau et surtout l'image de l'entreprise qui aura alors beaucoup de mal à s'en sortir, prévient Olivier Vallée chez Rockwell Automation. C'est arrivé dans d'autres domaines industriels, pas encore dans le secteur de l'eau ». Le numérique est bien le point faible reconnu des réseaux. Une alerte que les professionnels du secteur, comme les autorités, prennent très au sérieux. Comme tous les opérateurs dits d'importance vitale (OIV), ils ont été réunis plusieurs fois ces derniers mois par l'Anssi, l'agence nationale de sécurité des systèmes d'information, un service du secrétariat général à

■ **Solutions pour la distribution
de l'eau potable.**



CAHORS propose une gamme complète de regards, coffrets et bornes de branchement qui se singularisent par une grande fiabilité et une maintenance minimale.



Conception, réalisation
et fabrication en France

www.groupe-cahors.com

La plateforme Wasmote Smart Water de Factory Systemes est la première plateforme de détection de la qualité de l'eau à distance capable de se connecter au cloud ou aux applications SCADA pour un contrôle de la qualité de l'eau en temps réel.

la Défense,

placé sous l'autorité du ministre. Résultat, après guides de bonnes pratiques ces dernières années, des arrêtés vont être publiés au Journal Officiel dans les prochaines semaines pour une application au 1^{er} juillet 2016. Même si l'on n'en connaît pas encore tous les détails, on sait qu'ils concernent la déclaration sans délai auprès de l'Anssi des constatations d'anomalies, des règles de sécurité sur l'accès à distance

(postes durcis tels

des disques

chiffrés, identification par un double facteur pour pouvoir se connecter) et les versions upgradées de logiciels. Un autre arrêté concernera le contrôle de ces règles, qui sera effectué par l'Anssi ou des prestataires délégués par l'Anssi, et la gestion de crises graves avec l'imposition, par le Premier ministre, de règles supplémentaires drastiques. De plus, l'opérateur devra établir un point de contact permanent avec l'Anssi. Les opérateurs industriels d'importance vitale, en particulier ceux des réseaux d'eau potable, auront entre 6 mois à deux ans pour s'y conformer. *« Le travail s'est fait en concertation durant l'année 2015 avec les opérateurs, tout en discutant avec les équipementiers, explique Yves Jussot, coordonnateur du groupe de travail sur l'eau potable à l'Anssi. Il n'y aura ainsi pas de problèmes d'application. Mais tout le monde devra s'y conformer car tous les opérateurs industriels, en particulier les acteurs des réseaux d'eau potable, sont sujets à des attaques informatiques ».*

Tout le monde, c'est-à-dire aussi bien les opérateurs eux-mêmes vis-à-vis des stations que des ouvrages annexes, mais aussi les fabricants de serrures, d'API, de RTU, de postes de télégestion, d'instruments analytiques, de logiciels de supervision... etc. Car aujourd'hui, grâce aux NTIC et à la banalisation du M2M et de l'Internet des objets (IoT), les vulnérabilités se sont multipliées. Chaque vanne, chaque organe réglant possède son capteur et son trans-

Premier
d e s
tiques



Factory Systemes

qui facilite le contrôle des installations et leur exploitation, mais avec une contrepartie: avec une telle avalanche d'informations, l'opérateur est submergé par les alarmes, plusieurs centaines pouvant se présenter quasi simultanément. Ce phénomène est dû au fait que très souvent une alarme en déclenche une autre et que tout n'est pas idéalement géré au moment de la mise en place des logiciels de supervision. *« Faute de se poser des questions très pointues sur comment inhiber une alarme à partir de telle autre et quel niveau de priorité attribuer à tel*

cas, toutes les alarmes sont remontées, reconnaissait Guy Gaudy, ingénieur informatique chez Suez, dans un précédent numéro de EIN. Autrement dit, on lègue le problème à l'exploitant ». Or, la multiplication des alarmes représente un réel problème de sécurité dans la mesure où celles qui sont vraiment critiques sont noyées dans la masse. Cette gestion des alarmes a amené l'EEMUA (Engineering Equipments & Materials Users' Association) à faire état de recommandations sur la gestion des alarmes en publiant sa directive 191, reprise par la norme industrielle ISA 18.02. Elle a établi le nombre d'alarmes susceptibles d'être traitées raisonnablement par un individu: une par dizaine de minutes. Beaucoup d'opérateurs en sont très loin!

Le problème étant clairement reconnu, de nombreux éditeurs comme Wonderware, Rockwell automation, Arc Informatique, Aréal, Prisma Instruments ou Codra incluent dans leur superviseur un logiciel permettant d'analyser les alarmes pour en faire le tri

metteur. Ce

en fonction du contexte et de les hiérarchiser selon leur criticité.

La question de l'entrée dans le réseau informatique par des clés USB est prise très au sérieux par les fabricants d'automates et de logiciels de supervision. Certains préconisent de simplement les désactiver. D'autres développent des solutions alternatives. Le scan antiviral de l'éditeur américain Bluecoat, proposé par Factory Systemes, permet de certifier les clés USB avant de pouvoir les utiliser sur les postes Scada de l'entreprise. L'idée est de créer des zones protégées pour les postes sans anti-virus. Factory Systemes propose aussi des pare-feu industriels, Radiflow et Tofino, dédiés aux systèmes très distribués et qui surveillent les protocoles utilisés sur le terrain, ainsi qu'une solution de protection par datadiode, Fox IT, qui permet de garantir une communication unidirectionnelle entre deux points et, par conséquent, l'impossibilité de prendre la main sur un poste fonctionnant en automatique la nuit par exemple.

Aéral développe de son côté des solutions logicielles destinées à protéger les communications avec l'extérieur. Il préconise de créer un sous-réseau isolé du reste de l'installation et auquel on accède par un serveur web avec un pare-feu et des filtres sur les flux de données entrant. Le logiciel permet d'entrer sur la machine mais ne permet pas d'aller plus loin. Aéral propose également des utilitaires pour verrouiller l'environnement Windows en fonction des droits d'accès pour différentes opérations (supervision, installation de nouveaux logiciels) et protéger les disques durs en écriture.

Autre contrepartie liée à la banalisation des technologies IP, les nouveaux services, très commodes, qui utilisent le web (télé-

gestion, télérelève, télémaintenance du logiciel de supervision) sont autant de points faibles pour



Rockwell Automation

Le routeur de services Stratix 5900™ de Rockwell Automation associe plusieurs fonctions de sécurité dans un seul et même dispositif afin de protéger les automatismes industriels et le réseau de systèmes de commande.



Solutions globales de contrôle/commande et télégestion

Vous recherchez performance & productivité de vos installations ; nous vous proposons des solutions optimales de gestion automatisée

- Acquisition et stockage des données
- Contrôle à distance
- IHM embarqué localement et accessible via un réseau Ethernet
- Maintenance à distance (application et IHM) via GPRS
- Gestion d'alarmes, envoi d'emails
- Envoi automatique de rapports quotidiens
- Supervision de l'ensemble de vos installations
- Pompage et ventilation à économie d'énergie

Hydraulique



Bioénergie



HAUTE TENSION



Photovoltaïque
BASSE TENSION

Eolien



Entrées/sorties sur Ethernet

- Connexion transparente à tous les systèmes SCADA
- Economie de 80% de largeur de bande réseau
- Réponses d'E/S sept fois plus rapides
- Large plage de température - 40 à +75°C
- 2 ports intégrés
- Anneau redondant Turbo Chain® (temps de cicatrisation < 20 ms)



Supervision et IHM

- Clients locaux IHM
- Supervision centralisée de l'ensemble de vos installations de 50 à 450 000 variables
- Gestion d'alarmes et de télésurveillance
- Rapports et liaison bases de données de gestion



Variateurs de vitesse

- Considérables économies d'énergie grâce à la technologie OEC
- Plateforme d'entraînement ouverte et modulable
- Une large gamme de produits adaptée aux besoins du marché
- Utilisation et mise en service simples
- Gestion et contrôle des données optimisés
- Des produits ultra fiables
- Conformité aux normes, standards et certificats mondiaux



Automates de télégestion

- Tout en un
- Automate programmable
- 4 ports de communication
- Serveur web embarqué
- Robuste et compact
- Gestion d'alarme

IP Systèmes

8, rue du Colonel Chambonnet
BP 67 - 69672 BRON

Tél : 04 72 14 18 00 - info@ip-systemes.fr

www.ip-systemes.fr - www.ip-online.fr

Le système d'analyse en ligne 8905 de Bürkert permet de surveiller tous les paramètres importants en gérant la fluidique et l'électronique dans un minimum d'espace.

des actions malveillantes ou simplement des perturbations dues à des négligences. De nombreux fabricants intègrent aujourd'hui cette contrainte avec, par exemple, le durcissement des mots de passe ou le filtrage des adresses IP (Lacroix Sofrel), le contrôle d'accès sur port USB (Rockwell Automation), des outils de surveillance des réseaux (Arc Informatique) ou des fonctions de cryptage (Aqualabo Contrôle). Mais la situation reste pour le moins critique. Les industriels, comme l'éditeur de logiciel de supervision Codra, travaillent déjà sur les exigences qui entreront bientôt dans la législation pour les plateformes industrielles.

Identifier toutes les vulnérabilités

Il faut donc choisir et installer des protections physiques ou logicielles en regard de chaque vulnérabilité identifiée. Il n'est cependant pas toujours possible d'adopter directement les recettes de l'informatique classique. Utiliser un anti-virus sur certaines stations par exemple dégraderait leur performance ou pourrait faire redémarrer une machine. Mais il existe sur le marché des solutions de protection adaptées aux contraintes du monde de l'eau. Le réseau privé virtuel (VPN, virtual private network) en est une. Aqualabo Perax le propose pour son automate P400Xi. Il permet d'authentifier les accès avec des certificats et de crypter les échanges. « Les échanges vers la supervision ainsi que les échanges entre P400XI seront



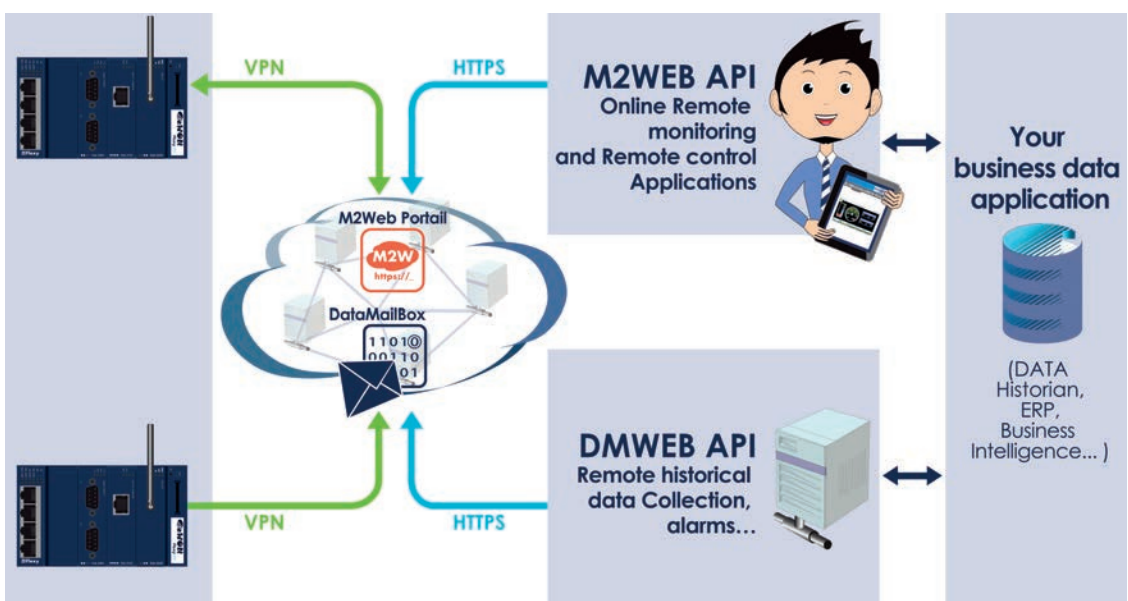
sécurisées de manière optimale », explique Frédéric Arbiol, d'Aqualabo Contrôle, propriétaire de la marque Perax. Le nouveau datalogger de la marque, le Smartlog, qui est associé à un capteur pour transmettre les données et qui communique en GPRS ou en SMS si le signal est trop faible, peut intégrer des cartes Sim sécurisées. Cette sécurisation provient du fait que les opérateurs

proposent à leurs clients des cartes Sim pouvant se connecter au réseau intranet de l'entreprise au travers d'un VPN de façon transparente. Le Smartlog peut ainsi bénéficier de cette sécurité optimisée pour transmettre les données en GPRS sur un serveur FTP, données que la supervision pourra ainsi récupérer sans risque. Autre exemple, un VPN est généré par le routeur Stratix 5900 de Rockwell Automation après qu'il se soit assuré de l'habilitation de la personne qui cherche à se connecter pour transférer ses données. De plus, il sert à l'intérieur du site, pour protéger des machines d'interférences de communication avec d'autres.

Un autre sujet sensible est le développement des objets connectés et l'utilisation des radiofréquences qui créent d'autres types de vulnérabilités. Factory Systems privilégie, sur des réseaux télécom ou classiques sur IP, le protocole sécurisé MQTT (message queue telemetry transfert), tel celui utilisé par ses capteurs Libellium. L'entreprise dispose également d'un modem Imsys qui fonctionne sur le réseau Ethernet ou avec une carte Sim sur un réseau d'opérateur télécom, et est géré, de façon centralisée et sans administration complexe, par un service hébergé dans le cloud (Imsys connectivity service). Ce service permet de créer une communication VPN très simplement entre un utilisateur et une application selon des règles définies par l'exploitant, par exemple, l'ouverture du tunnel sous condition d'autorisation d'accès seulement. Un autre moyen de surveillance consiste à mettre en place des analyseurs de réseau (sniffer) qui permettent de vérifier que les commandes transitant sur les réseaux entre supervision et automates sont bien autorisées par rapport aux droits d'accès utilisateurs.

Surveiller la qualité de l'eau en temps réel

Les capteurs intelligents permettant de surveiller la qualité de l'eau se développent. Actemium propose ainsi des dispositifs pour protéger les procédés essentiels de la



La passerelle de données eWON FLEXY est capable de se connecter à de nombreux équipements distants pour en assurer le monitoring et la gestion des données, dans tous formats (CSV, TXT, MySQL...) et de manière sécurisée (VPN, HTTPS)

FLOW LAB Technologies



Concepteur et fabricant français de débitmètres utilisant des technologies électromagnétiques et ultrasons, nous répondons à toutes les configurations hydrauliques et physiques. Nous savons modifier les produits de notre gamme standard pour les adapter à un site particulier, nous pouvons ainsi réduire de manière notable pour notre client les frais de montages et d'interfaçage cela en augmentant la fiabilité de la mesure finale. Pour ces raisons de nombreuses entreprises nous confient l'ingénierie complète du point de mesure.

FLOWLAB Technologies maîtrise la mesure de débit sur tout fluide liquide en canalisation forcée ou en canal ouvert – mesure en adduction en assainissement et rivière.



Fort d'une expérience de plus de 20 ans dans le domaine de la mesure des fluides, nos techniciens interviennent régulièrement dans le monde entier pour réaliser des diagnostics de réseaux, des formations techniques, des installations, des mises en services et des réparations. Grâce à l'expérience de nos techniciens et ingénieurs nous avons mis au point des produits qui utilisent des principes de mesures éprouvés mis en œuvre par les technologies les plus modernes. De ce fait nos capteurs et convertisseurs se trouvent être compatibles avec un grand nombre de marques dont le suivi n'est plus assuré par le fabricant initial.



FLOWLAB Technologies a développé ces dernières années son service de location de matériel.

Nous mettons à la disposition de nos clients un large choix de matériel :

- Débitmètre à ultrasons portables ;
- Débitmètre EM à insertion
- Télémètre ;
- Corrélateur...



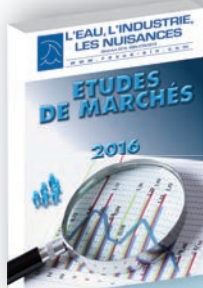
FLOW LAB TECHNOLOGIES
4 Le Pré de la Marquise, Av. du Roussillon
13109 SIMIANE COLLONGUE
Tél. : 04 42 90 01 16 • Fax : 04 42 90 00 15
www.flow-lab-france.com • email : contact@flow-lab-france.com

EN 389/2016

Vient de paraître !

Hors série « Etudes de marchés 2016 »

Un numéro exceptionnel de la revue **L'Eau, L'industrie, Les Nuisances** sur l'état de l'offre de biens et de services dans le secteur de l'eau.



- Les réseaux d'eau potable et d'assainissement
- La gestion des eaux pluviales
- La réutilisation des eaux usées
- L'assainissement non-collectif
- Les eaux récréatives ou de loisir
- L'eau potable
- Les eaux industrielles
- Les boues
- Méthanisation & biogaz
- Les pompes, compresseurs...
- Automatismes, télégestion
- Les sols pollués

Une série d'études technico-économiques pour appréhender le marché, ses tendances et ses évolutions prévisibles dans les domaines suivants :

Et bien d'autres analyses encore sur l'évolution du cadre institutionnel, de la réglementation, des services locaux de l'environnement, du prix du service de l'eau... etc.

Un numéro exceptionnel pour identifier les marchés porteurs, surveiller leurs évolutions, découvrir les nouvelles tendances, se situer dans un environnement fortement concurrentiel, décrypter les stratégies et anticiper les mutations à venir...

Disponible dès aujourd'hui au prix de 16 euros
<http://www.editions-johanet.com>

Éditions Johanet : 60, rue du Dessous des Berges • 75013 Paris
Tél. +33 (0)1 44 84 78 78 • Fax : +33 (0)1 42 40 26 46
livres@editions-johanet.com

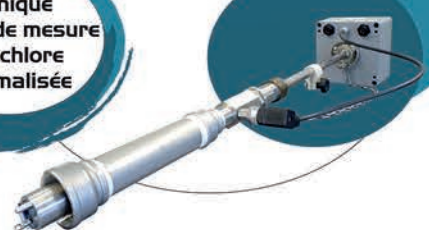


www.environnement.efs.fr

ANALYSE DE LA QUALITE DE L'EAU POTABLE

Sonde autonome à insertion pour connexion en charge

L'unique sonde de mesure du chlore normalisée



Multi-Probe+

Sonde multi-paramètres pour un contrôle en continu de la qualité de l'eau sur les réseaux de distribution d'eau potable.



- Surveillance en temps réel de 12 paramètres : turbidité, conductivité, pression, température, vitesse, pH, Redox, tension batterie, 2 entrées analogiques
- Mesure normalisée du chlore (ISO 7393)
- Mesure de débit à ultrason
- Fonctionnement en insertion jusqu'à 16 bars



Turbi-Probe 860+

Sonde de turbidité ultra-précise parfaitement adaptée aux eaux potables et effluents peu chargés.

- Mesure normalisée de la turbidité (ISO 7027)
- Précision de la mesure au centième de NTU
- Mesure sous pression
- Transmission numérique des données du capteur



Eaux potables - Eaux de surface - Eaux de station d'épuration - Eaux de process

EFS

192, allée des chênes
Parc d'activité du baconnet
Montagny - 69700 - France
sales_env@efs.fr
Tél. : 04 72 49 58 54



la station, par exemple pour détecter une modification anormale de la concentration de chlore en comparant des unités redondantes, en faisant remonter des alarmes en cas de modification inopinée de programme des automates, etc. Cette teneur en chlore devant être garantie dans le cadre du plan vigipirate, EFS propose sa sonde MultiProbe + dont les mesures, en temps réels et sur de nombreux paramètres, sont identiques à celles effectuées en laboratoire : elle intègre par exemple la mesure du chlore selon ISO 7393, la mesure de débit par ultrasons et la mesure de turbidité selon ISO 7027 avec une précision de mesure au centième de NTU. De même, la sonde ampérométrique Kapta 2000-AC2 de Veolia Water Solution Technologies utilise une membrane photo-polymérisée structurée, directement sur l'électrode, ce qui supprime les inconvénients des sondes ampérométriques à électrolyte. Elle peut ainsi être installée directement dans les conduites jusqu'à une pression de 10 bar sans contrôle de débit ou de pression et fournit une mesure précise de chlore libre actif.

Chez Factory Systèmes, la plateforme Waspnote Smart Water est la première plateforme de détection de la qualité de l'eau à distance capable de se connecter au cloud ou aux applications SCADA pour un contrôle de la qualité de l'eau en temps réel. Elle intègre un ensemble de capteurs ultra-basse puissance conçus pour être

exploités dans les environnements les plus difficiles. Les fonctions d'analyse en ligne progressent également grâce à la combinaison de différents capteurs de mesure sur une seule plateforme utilisant les nanotechnologies (MEMS). Le système d'analyse en ligne 8905 de Bürkert, qui repose sur ce principe, permet de surveiller tous les paramètres importants en gérant la fluide et l'électronique dans un minimum d'espace.

Protéger son réseau : un élément de la compétitivité

La télérelève, bien souvent en fin de chaîne des opérations sur un réseau d'eau potable, est également concernée, bien qu'elle ne commande directement aucun capteur, aucune vanne, aucun automate. Mais elle transmet des données. « En télérelève, le seul risque serait de perdre ou se faire subtiliser les données sur Internet, reconnaît Olivier Benas, de RG2i. Restent aux opérateurs à définir si c'est stratégique et critique ou non ». Les opérations de comptage de la consommation n'étant pas pilotées, leur éventuelle interception n'emporte pas de conséquence directe ou immédiate. Mais la gestion du Big Data est devenu un élément de compétitivité supplémentaire et protéger son réseau en garantissant la sécurité des données est essentiel. Or, la diversité des systèmes, des réseaux et des protocoles de communication utilisés en télérelève ne facilite pas les choses.

Même si la plupart des solutions proposées intègrent désormais nativement leurs propres fonctions de cybersécurité, beaucoup d'acteurs comme Phoenix Contact, IP Systèmes, RG2i, Factory Systèmes, Adeunis, Vertical M2M ou encore Ixel proposent des matériels, des modules de transmission ou des solutions radios capables de s'interfacer avec un grand nombre de standards pour sécuriser les réseaux et les communications. C'est par exemple le cas du routeur-passerelle eWON Flexy capable de se connecter à de nombreux équipements distants et de communiquer avec un large éventail d'équipements sur le terrain, où qu'ils soient et indépendamment du protocole utilisé. « Pour la transmission de données en toute sécurité, notre solution eWON FLEXY exploite les technologies HTTPS et VPN, qui permettent d'établir un tuyau sécurisé à l'intérieur duquel va pouvoir transiter les données de manière cryptée », souligne Olivier Benas.

Reste à bien mettre en place ces dispositifs et surtout, à respecter les règles. Nul doute que celles que va édicter l'Anssi très prochainement vont y contribuer. Mais même si les opérateurs devront, sans délai, avertir l'agence de sécurité des systèmes d'information de toute anomalie, celles-ci ne disparaîtront pas. La vigilance doit devenir le maître mot de la sécurisation des réseaux d'eau potable. C'est à une révolution des mentalités que nous assistons aujourd'hui. ■

Le statut juridique de l'eau à l'épreuve des exigences environnementales

Julia GUDEFIN



Que l'on soit un simple promeneur ou un fin observateur, l'eau est présente partout. Pourtant, l'atout qu'elle représente pour les activités anthropiques cache souvent sa réalité environnementale, celle de son cycle. Ce constat se reflète dans l'appréhension juridique de l'eau laquelle est conçue comme un bien ou une chose. Cette qualification l'assigne donc à un statut juridique dont les manifestations révèlent la fonction utilitariste de la ressource. Or, l'émergence des problématiques environnementales confronte le statut juridique de l'eau à sa réalité physique.

Ainsi, le droit et les exigences environnementales s'influencent réciproquement pour générer des règles protectrices de l'eau et des représentations juridiques du cycle hydrologique qui engendrent des évolutions du statut. Dès lors, ce dernier s'émancipe des catégories juridiques traditionnelles issues du droit des biens et s'habille d'une finalité protectrice dont les règles et les concepts qui s'attachent à la fonction écologique de l'eau et à la réalité environnementale du cycle hydrologique lui façonnent une autre condition juridique.

➡ www.editions-johanet.com

60, rue du Dessous des Berges - 75013 Paris - Tél. +33 (0)1 44 84 78 78 - Fax : +33 (0)1 42 40 26 46 - livres@editions-johanet.com

POUR UN AMENAGEMENT SUR DU FUTUR

Réservoirs d'eau de pluviale disposant d'équipements modernes qui se connectent entre eux grâce une technologie de procédés innovants. D'autres ouvrages peuvent avoir ainsi une interaction entre eux et se gérer selon les paramétrages intégrés. Dispositifs développés par la société HST permettant d'exécuter de manière automatisée, l'acquisition de données des différents processus de fonctionnement des ouvrages entre eux. Ceci est rendu possible grâce aux logiciels de la société HST contrôle de processus automatisé SCADA en liaison avec le logiciel de gestion d'opération automatisée KANiO®.

Avec ces équipements de haute technologie la société HST peut vous fournir cela selon vos besoins et contraintes. Avec toutes les exigences communales 4.0, pour un avenir sur et économique. Envoyez-nous vos documents de planification et nous vous ferons une proposition de conception.

